



# Dell SonicWALL™ SonicOS 5.8.1.15

## Release Notes

### August 2015

These release notes provide information about the Dell SonicWALL™ SonicOS 5.8.1.15 release.

- [About SonicOS 5.8.1.15](#)
- [Supported platforms](#)
- [Resolved issues](#)
- [Known issues](#)
- [Supported features by model](#)
- [Key features in SonicOS 5.8](#)
- [System compatibility](#)
- [Product licensing](#)
- [Upgrading SonicOS image procedures](#)
- [Technical support resources](#)
- [About Dell](#)

## About SonicOS 5.8.1.15

SonicOS 5.8.1.15 resolves a number of issues found in earlier releases. See [Resolved issues](#).

SonicOS 5.8.1.15 provides all the features and contains all the resolved issues that were included in previous releases of SonicOS 5.8.1.x. For detailed information, see the previous release notes, available on <https://mysonicwall.com/> or on <https://support.software.dell.com/release-notes-product-select>.

## Supported platforms

The SonicOS 5.8.1.15 release is supported on the following Dell SonicWALL network security appliances:

- |             |                            |                         |
|-------------|----------------------------|-------------------------|
| • NSA E8510 | • NSA 5000                 | • TZ 215 / 215 Wireless |
| • NSA E8500 | • NSA 4500                 | • TZ 210 / 210 Wireless |
| • NSA E7500 | • NSA 3500                 | • TZ 205 / 205 Wireless |
| • NSA E6500 | • NSA 2400                 | • TZ 200 / 200 Wireless |
| • NSA E5500 | • NSA 240                  | • TZ 105 / 105 Wireless |
|             | • NSA 250M / 250M Wireless | • TZ 100 / 100 Wireless |
|             | • NSA 220 / 220 Wireless   |                         |

# Resolved issues

This section contains a list of issues that are fixed in the SonicOS 5.8.1.15 release.

## DPI-SSL

Resolved issue	Issue ID
HTTPS Web sites cannot be accessed in Wire mode. Occurs when Wire mode is in secure mode and Client DPI-SSL enabled.	134703
Excluding a User Object or User Group for Server DPI-SSL causes Client DPI-SSL to not work properly. Occurs when accessing HTTPS websites from a client computer without logging in as a user on the client computer. Client DPI-SSL does not change the site certificate to the SonicWALL certificate.	118962

## Firewall

Resolved issue	Issue ID
Action objects and App Rules that are not selected are deleted. Occurs when another App Rule is deleted.	132232

## GMS

Resolved issue	Issue ID
GMS cannot acquire the remote firewall. Occurs when GMS tries to connect to the remote firewall over a VPN Tunnel through the firewall's L2 Bridge (X1-X0).	126247

## High Availability

Resolved issue	Issue ID
The bandwidth of the HA L2 Bridge suddenly goes to almost zero and stays there for one to five minutes. Occurs when the primary firewall is running at 500 to 750 Megabytes of bandwidth. If the Active unit is rebooted, the Secondary unit takes over and the bandwidth returns to normal.	137367

## Log

Resolved issue	Issue ID
The firewall does not send the connection report to the collector. Occurs when the "Report ONCE" option is selected for "Report Connection On Kilo BYTES Exchanged" on the AppFlow > Flow Reporting page.	143005

## Networking

Resolved issue	Issue ID
SSH Management does not respond. Occurs when SSH Management is configured on a subinterface. If SSH Management is configured on the parent interface, it works fine. <b>Workaround:</b> Enable SSH Management on the parent physical interface.	133992
The configured web proxy cannot resolve the FQDN server name. Occurs after the firewall firmware is upgraded.	131893

NetBIOS packets are dropped due to "Invalid Connection Cache". Occurs when the VPN policy is bound to an interface on a L2 Bridge.	131035
MAC based address objects lose their bindings to the IP addresses assigned by DHCP. Occurs intermittently at random 2 or 3 times a day. <b>Workaround:</b> Flush the firewall's ARP cache.	98946

## Security Services

Resolved issue	Issue ID
No inbound emails are received. Occurs when Anti-Spam is enabled.	134223

## SSL VPN

Resolved issue	Issue ID
The firewall does not release the client login session and the client cannot log back in. Occurs when the client is logged in using NetExtender over an SSL VPN and the connection is lost. <b>Workaround:</b> Reboot the firewall.	119678

## System

Resolved issue	Issue ID
The SonicOS management interface is slow to respond, or does not respond for a brief period of time. Occurs when the WebListener task is in a loop waiting for more SSL data until it eventually times out. During this period, the tWebListen task may take 100% of the CPU time. <b>Note:</b> As a best practice, configure Access Control of the management interface on the WAN.	144909
Exporting a certificate on the System > Certificate page displays the error - "Page redirected HTTP 404 page not found". Occurs when the certificate name contains periods.	127719
The System Backup on the System > Settings page shows that the file size is zero bytes, even though the System Backup can be uploaded fine. Occurs after upgrading the firmware.	78393

## Users

Resolved issue	Issue ID
The firewall displays the error message: "Failed to decrypt password." Occurs when the administrator's password is changed to include French special characters such as an accent. Then, the administrator reboots the firewall and tries to add a Local User.	143665

## VoIP

Resolved issue	Issue ID
VoIP traffic that is not allowed by the Access Rule is still entering the customer network. Occurs when the "SIP Media inactivity time out (seconds)" is not specified on the VoIP > Settings page.	139977

## VPN

Resolved issue	Issue ID
VPN tunnels cannot be established successfully. Occurs when attempting to configure a VPN tunnel for Amazon Web Services (AWS) in an Amazon Virtual Private Cloud (VPC).	138998
NAT traffic is sent to WXA on the remote node. Occurs when NAT traffic is sent over a VPN tunnel interface.	137694
Multiple L2TP clients cannot maintain connections to the firewall simultaneously. Occurs when multiple clients are connected to the firewall via an L2TP from behind the same gateway (public IP).	128382

# Known issues

This section contains a list of known issues in the SonicOS 5.8.1.15 release.

## DPI-SSL

Known issue	Issue ID
Excluding a User Object or User Group for Server DPI-SSL causes Client DPI-SSL to not work properly. Occurs when accessing HTTPS websites from a client computer without logging in as a user on the client computer. Client DPI-SSL does not change the site certificate to the SonicWALL certificate.	118962

## High Availability

Known issue	Issue ID
The firmware cannot be upgraded on the primary firewall of an HA pair. Occurs when the Primary firewall is active. When the Standby firewall is active, the firmware can be upgraded successfully.	144573
Traffic is going to the Primary unit when it should be going to the Backup unit. This issue is specific to the NSA 2400 appliance. Occurs when the Primary unit is rebooted and a failover occurs, making the Backup unit become the Active unit. Then, when the Primary unit is fully back online again, traffic is switched from the backup unit back to Primary unit automatically.	141439

## Networking

Known issue	Issue ID
Under certain customer deployment conditions there could be temporary link instability experienced by physical interfaces on NSA 2400 units. This is an intermittent condition that is resolved in the majority of cases when using SonicOS 5.8.1.15 and newer. However, it may still persist in a very small number of units.	145764
DDNS cannot connect to Dyn.com and returns a certificate error. Occurs when the DDNS certificate is using SHA2. <b>Workaround:</b> Contact Dell SonicWALL Technical Support for the Hot Fix.	144834

The L2TP client on the WAN interface of the firewall gets disconnected every two minutes. Occurs when the WAN interface IP Assignment is L2TP and the WAN interface is connected to an L2TP/PPP server. When PPP messages are exchanged, there is no magic number negotiation on the client side during the Link Control Protocol (LCP) configuration request. Only the server attempts to negotiate the magic numbers. The LCP echo reply from the firewall has the same magic numbers as the server. After 4 attempts, the server terminates the connection, but the firewall continues to retry the connection every 2 minutes.	143953
FTP or HTTP traffic cannot pass through a pair of interfaces configured in Wire Mode and set to Secure. Occurs when using a Stateful High Availability pair and Active-Active DPI is enabled.	101359

## Users

Known issue	Issue ID
A limited administrator can log out the firewall administrator on the Users > Status page. Occurs when a limited administrator is in non-configuration mode.	145005

## VPN

Known issue	Issue ID
The tunnel interface is bound to X0, but IKE traffic is allowed on X1 through the remote firewall that is reachable on X1. Occurs when trying to establish a tunnel interface VPN between two firewalls discovered by the router. When trying to connect Firewall1 X0 to Firewall2 X0, when the IPsec Phase2 security association (SA) is accepted, but the VPN is down, the policy is bound to X0. Although the remote firewall is reachable through X1, no IKE packet should go through the X1 interface.	121966

## Wireless

Known issue	Issue ID
Wireless PCs connected via SonicPoint cannot communicate with other PCs on the SonicPoint. Occurs when the X3 WLAN zone is configured as a Layer 2 Bridge to X0, and the "Allow Interface Trust" option is enabled in the Add Zone dialog under the General tab, and the "Only allow traffic generated by a SonicPoint / SonicPointN" option is disabled in the Add Zone dialog under the Wireless tab.	142815

# Supported features by model

The following tables list the key features in SonicOS 5.8 and which appliance models support them. Blank table cells indicate that the feature is not supported. Features that are affected by licensing status are also listed.

- [NSA E-Class, NSA Series, TZ 210/200/100 Series](#)
- [TZ 205 Series and TZ 105 Series](#)
- [NSA 250M Series, NSA 220 Series, TZ 215 Series](#)
- [Supported features and licensing](#)

## NSA E-Class, NSA Series, TZ 210/200/100 Series

Specifically, this table indicates supported features for:

- NSA E-Class Series — E8510 / E8500 / E7500 / E6500 / E5500
- NSA Series — 5000 / 4500 / 3500 / 2400 / 240
- TZ 210 Series — 210 / 210 Wireless
- TZ 200 Series — 200 / 200 Wireless
- TZ 100 Series — 100 / 100 Wireless

Feature/Enhancement	NSA E-Class Series	NSA Series	TZ 210 Series	TZ 200 Series	TZ 100 Series
Accept Multiple VPN Client Proposals.	Supported	Supported	Supported	Supported	Supported
App Control Advanced	Supported	Supported	Supported	Supported	Supported
App Control Policy Configuration via App Flow Monitor	Supported	Supported	Supported	Supported	Supported
App Rules	Supported	Supported	Supported		
AppFlow > Flow Reporting	Supported	Supported	Supported		
AppFlow Dash	Supported	Supported	Supported		
AppFlow Monitor	Supported	Supported	Supported		
AppFlow Reports	Supported	Supported	Supported		
Application Usage and Risk Report	Supported	Supported	Supported		
Auto-Configuration of URLs to Bypass User Authentication	Supported	Supported	Supported	Supported	Supported
Browser NTLM Authentication	Supported	Supported	Supported	Supported	Supported
CASS 2.0	Supported	Supported	Supported	Supported	Supported
CFS Enhancements	Supported	Supported	Supported	Supported	Supported
Cloud GAV	Supported	Supported	Supported	Supported	Supported
Connection Monitor	Supported	Supported	Supported	Supported	Supported
Current Users and Detail of Users Options for TSR	Supported	Supported	Supported	Supported	Supported
Customizable Login Page	Supported	Supported	Supported	Supported	Supported
DHCP Scalability Enhancements	Supported	Supported	Supported	Supported	Supported
DPI-SSL	Supported	Supported			
Dynamic WAN Scheduling	Supported	Supported	Supported	Supported	Supported
Enhanced Connection Limit	Supported	Supported	Supported	Supported	Supported
Geo-IP Filtering and Botnet Command & Control Filtering	Supported	Supported	Supported		
Global BWM Ease of Use Enhancements	Supported	Supported	Supported	Supported	Supported
IKEv2	Supported	Supported	Supported	Supported	Supported
IPFIX & NetFlow Reporting	Supported	Supported	Supported		

Feature/Enhancement	NSA E-Class Series	NSA Series	TZ 210 Series	TZ 200 Series	TZ 100 Series
LDAP Primary Group Attribute	Supported	Supported	Supported	Supported	Supported
Link Aggregation	Supported				
Log Monitor	Supported	Supported	Supported	Supported	Supported
Management Traffic Only Option for Network Interfaces	Supported	Supported	Supported	Supported	Supported
NTP Authentication Type	Supported	Supported	Supported	Supported	Supported
Packet Monitor Enhancements	Supported	Supported	Supported	Supported	Supported
Port Redundancy	Supported				
Preservation of Anti-Virus Exclusions After Upgrade	Supported	Supported	Supported	Supported	Supported
Real-Time Monitor	Supported	Supported	Supported		
SIP Application Layer Enhancements	Supported	Supported	Supported	Supported	Supported
SonicPoint N DR	Supported	Supported	Supported	Supported	Supported
SonicPoint Ne/Ni	Supported	Supported	Supported	Supported	Supported
SonicPoint VAPs	Supported	Supported	Supported	Supported	Supported
SSL VPN NetExtender Client Update	Supported	Supported	Supported	Supported	Supported
SSO User Import from LDAP	Supported	Supported	Supported	Supported	Supported
Stateless High Availability	Supported	Supported	Supported	Supported	Supported
Top Global Malware	Supported	Supported	Supported	Supported	Supported
User Monitor Tool	Supported	Supported	Supported		
VLAN Subinterfaces	Supported	Supported	Supported	Supported	Supported
WAN Acceleration	Supported	Supported	Supported	Supported	Supported
Wire and Tap Mode	Supported	NSA 3500 and above			
Wireless Client Bridge Support			Supported	Supported	Supported
YouTube for Schools	Supported	Supported	Supported	Supported	Supported

## TZ 205 Series and TZ 105 Series

Specifically, this table indicates supported features for:

- TZ 205 Series — 205 / 205 Wireless
- TZ 105 Series — 105 / 105 Wireless

Feature / Enhancement	TZ 205 Series	TZ 105 Series
Accept Multiple VPN Client Proposals	Supported	Supported
App Control Advanced	Supported	Supported
App Control Policy Configuration via App Flow Monitor		
App Rules	Supported	Supported
AppFlow > Flow Reporting		
AppFlow Dash		
AppFlow Monitor		
AppFlow Reports		
Application Usage and Risk Report		
Auto-Configuration of URLs to Bypass User Authentication	Supported	Supported
Browser NTLM Authentication	Supported	Supported
CASS 2.0	Supported	Supported
CFS Enhancements	Supported	Supported
Cloud GAV	Supported	Supported
Connection Monitor	Supported	Supported
Current Users and Detail of Users Options for TSR	Supported	Supported
Customizable Login Page	Supported	Supported
DHCP Scalability Enhancements	Supported	Supported
DPI-SSL		
Dynamic WAN Scheduling	Supported	Supported
Enhanced Connection Limit	Supported	Supported
Geo-IP Filtering and Botnet Command & Control Filtering		
Global BWM Ease of Use Enhancements	Supported	Supported
IKEv2	Supported	Supported
IPFIX & NetFlow Reporting		
LDAP Primary Group Attribute	Supported	Supported
Link Aggregation		
Log Monitor	Supported	Supported
Management Traffic Only Option for Network Interfaces	Supported	Supported
NTP Authentication Type	Supported	Supported
Packet Monitor Enhancements	Supported	Supported
Port Redundancy		
Preservation of Anti-Virus Exclusions After Upgrade	Supported	Supported



Feature / Enhancement	TZ 205 Series	TZ 105 Series
Real-Time Monitor		
SIP Application Layer Enhancements	Supported	Supported
SonicPoint N DR	Supported	Supported
SonicPoint Ne/Ni	Supported	Supported
SonicPoint VAPs	Supported	Supported
SSL VPN NetExtender Client Update	Supported	Supported
SSO User Import from LDAP	Supported	Supported
Stateless High Availability	Supported	
Top Global Malware		
User Monitor Tool	Supported	Supported
VLAN Subinterfaces	Supported	Supported
WAN Acceleration Support	Supported	Supported
Wire and Tap Mode		
Wireless Client Bridge Support	Supported	Supported
YouTube for Schools	Supported	Supported

## NSA 250M Series, NSA 220 Series, TZ 215 Series

Specifically, this table indicates supported features for:

- NSA 250M Series — 250M / 250M Wireless
- NSA 220 Series — 220 / 220 Wireless
- TZ 215 Series — 215 / 215 Wireless

Feature / Enhancement	NSA 250M Series	NSA 220 Series	TZ 215 Series
Accept Multiple VPN Client Proposals	Supported	Supported	Supported
App Control Advanced	Supported	Supported	Supported
App Control Policy Configuration via AppFlow Monitor	Supported	Supported	Supported
App Rules	Supported	Supported	Supported
AppFlow > Flow Reporting	Supported	Supported	Supported
AppFlow Dash	Supported	Supported	Supported
AppFlow Monitor	Supported	Supported	Supported
AppFlow Reports	Supported	Supported	Supported
Application Usage and Risk Report	Supported	Supported	Supported
Auto-Configuration of URLs to Bypass User Authentication	Supported	Supported	Supported
Browser NTLM Authentication	Supported	Supported	Supported
CASS 2.0	Supported	Supported	Supported
CFS Enhancements	Supported	Supported	Supported
Cloud GAV	Supported	Supported	Supported

Feature / Enhancement	NSA 250M Series	NSA 220 Series	TZ 215 Series
Connection Monitor	Supported	Supported	Supported
Current Users and Detail of Users Options for TSR	Supported	Supported	Supported
Customizable Login Page	Supported	Supported	Supported
DHCP Scalability Enhancements	Supported	Supported	Supported
DPI-SSL	Supported	Supported	
Dynamic WAN Scheduling	Supported	Supported	Supported
Enhanced Connection Limit	Supported	Supported	Supported
Geo-IP Filtering and Botnet Command & Control Filtering	Supported	Supported	Supported
Global BWM Ease of Use Enhancements	Supported	Supported	Supported
IKEv2	Supported	Supported	Supported
IPFIX & NetFlow Reporting	Supported	Supported	Supported
LDAP Primary Group Attribute	Supported	Supported	Supported
Link Aggregation			
Log Monitor	Supported	Supported	Supported
Management Traffic Only Option for Network Interfaces	Supported	Supported	Supported
NSA Modules	Supported		
NTP Authentication Type	Supported	Supported	Supported
Packet Monitor Enhancements	Supported	Supported	Supported
Port Redundancy			
Preservation of Anti-Virus Exclusions After Upgrade	Supported	Supported	Supported
Real-Time Monitor	Supported	Supported	Supported
SIP Application Layer Enhancements	Supported	Supported	Supported
SonicPoint N DR	Supported	Supported	Supported
SonicPoint Ne/Ni	Supported	Supported	Supported
SonicPoint VAPs	Supported	Supported	Supported
SSL VPN NetExtender Client Update	Supported	Supported	Supported
SSO User Import from LDAP	Supported	Supported	Supported
Top Global Malware	Supported	Supported	Supported
User Monitor Tool	Supported	Supported	Supported
VLAN Subinterfaces	Supported	Supported	Supported
WAN Acceleration Support	Supported	Supported	Supported
Wire and Tap Mode			
Wireless Client Bridge Support	Supported	Supported	Supported
YouTube for Schools	Supported	Supported	Supported

## NSA 250M Series module support

The following SonicWALL NSA modules are supported on the NSA 250M series appliances:

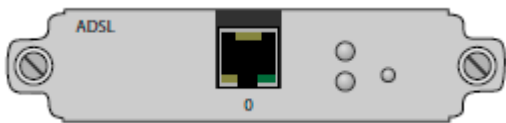


**WARNING:** You MUST power down the appliance before installing or replacing the modules.

- **1 Port ADSL (RJ-11) Annex A** - Provides Asymmetric Digital Subscriber Line (ADSL) over plain old telephone service (POTS) with a downstream rate of 12.0 Mbit/s and an upstream rate of 1.3 Mbit/s.



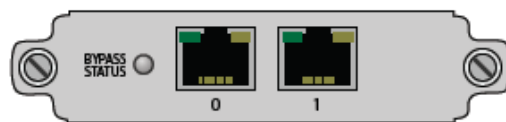
- **1 Port ADSL (RJ-45) Annex B** - Provides Asymmetric Digital Subscriber Line (ADSL) over an Integrated Services Digital Network (ISDN) with a downstream rate of 12.0 Mbit/s and an upstream rate of 1.8 Mbit/s.



- **1-port T1/E1 Module** - Provides the connection of a T1 or E1 (digitally multiplexed telecommunications carrier system) circuit to a SonicWALL firewall using a RJ-45 jack.



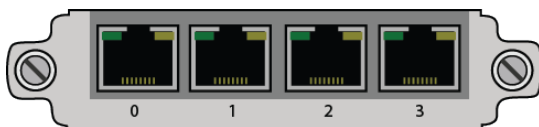
- **2-port LAN Bypass Module** - Removes a single point of failure so that essential business communication can continue while a network failure is diagnosed and resolved.



- **2-Port SFP Module** - This small form-factor pluggable (SFP) network interface module offers a fiber alternative to the 4-Port GbE Module, enabling more flexible and scalable deployments in a wide range of environments. Note that port 0 (802.3at) is disabled by default and should be enabled manually from the SonicOS management interface.



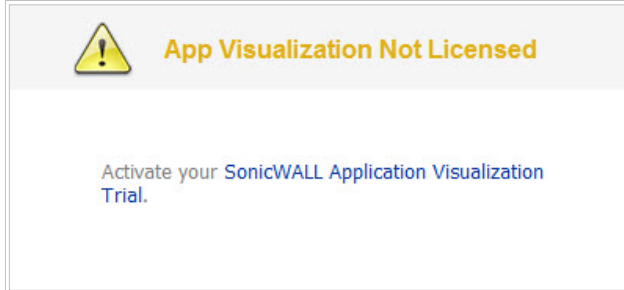
- **4-Port Gigabit Ethernet Module** - Expands port density of a SonicWALL NSA 250M Series firewall by adding four 1-Gbps Ethernet networking interfaces that negotiate the best Ethernet speeds available.



## Supported features and licensing

Some pages in the SonicOS management interface do not display if the license is not activated for the feature on that page.

Here is an example of the **Dashboard > Real-Time Monitor** page with App Visualization not licensed:



The following table lists the key features in SonicOS 5.8 that depend on licenses and other settings for the related management interface pages to display and function properly:

SonicOS Feature	No license (SGSS)	With license and disabled in flow reporting	With license and enabled in flow reporting
Dashboard > Real-Time Monitor	Blocks the page with a license popup window.	All charts are independently enabled or disabled from the <b>AppFlow &gt; Flow Reporting</b> page. It is not dependent on Visualization being enabled.	All charts are enabled. The App charts content depends on whether <b>Visualization</b> or <b>App Control Advanced</b> is enabled with zone settings.
Dashboard > AppFlow Monitor/Dash/Reports	Blocks the page with a license popup window.	The <b>AppFlow Monitor</b> page displays the message "flow reporting and visualization is disabled". Content is not shown.	All tabs are visible and fully operational.
Dashboard > BWM Monitor	Blocks the page with a license popup window.	Always on if <b>Global BWM</b> and <b>Interface</b> are enabled.	Always on if <b>Global BWM</b> and <b>Interface</b> are enabled.
AppFlow > Flow Reporting	Available and displays a statement that App Visualization is not licensed.	Available	Available
Security Services > GeoIP Filter	Blocks the page with a license popup window.	Not available	Available
Security Services > Botnet Filter	Blocks the page with a license popup window. * This is a separate license and is not part of the Comprehensive Gateway Security Suite (CGSS).	Available	Available

# Key features in SonicOS 5.8

This section describes the key features in SonicOS 5.8.

- YouTube for School Content Filtering Support
- IKEv2 Support
- SNMP for VLAN Interfaces
- SonicOS Management Interface HTTPS Default
- Real-Time Monitor
- Dashboard and AppFlow Enhancements
- Wire Mode / Inspect Mode
- Application Intelligence & Control
- Global Bandwidth Management
- Geo-IP/Botnet
- WXA 1.3 Support
- SonicPoint-N Dual Radio Support
- Accept Multiple Proposals for Clients Option
- ADTRAN Consolidation
- Deep Packet Inspection of SSL encrypted data (DPI-SSL)
- Gateway Anti-Virus Enhancements (Cloud GAV)
- NTP Authentication Type
- Link Aggregation
- Port Redundancy
- Content Filtering Enhancements
- IPFIX and NetFlow Reporting
- VLAN Support for TZ Series
- SonicPoint Virtual Access Point Support for TZ Series
- LDAP Primary Group Attribute
- Preservation of Anti-Virus Exclusions After Upgrade
- Comprehensive Anti-Spam Service (CASS) 2.0
- Enhanced Connection Limiting
- Dynamic WAN Scheduling
- NTLM Authentication with Mozilla Browsers
- Single Sign-On Import Users from LDAP Option
- SSL VPN NetExtender Update
- DHCP Scalability Enhancements
- SIP Application Layer Gateway Enhancements
- Management Traffic Only Option for Network Interfaces
- Auto-Configuration of URLs to Bypass User Authentication

# YouTube for School Content Filtering Support

YouTube for Schools is a service that allows for customized YouTube access for students, teachers, and administrators. YouTube Education (YouTube EDU) provides schools access to hundreds of thousands of free educational videos. These videos come from a number of respected organizations. You can customize the content available in your school. All schools get access to all of the YouTube EDU content, but teachers and administrators can also create playlists of videos that are viewable only within their school's network. Before configuring your SonicWALL security appliance for YouTube for Schools, you must first sign up at <http://www.youtube.com/schools>.

The configuration of YouTube for Schools depends on the method of Content Filtering you are using, which is configured on the **Security Services > Content Filter** page.

## Membership in Multiple Groups

- If a user is a member of multiple groups where one policy allows access to any part of YouTube and the other policy has a YouTube for Schools restriction, the user will be filtered by the YouTube for Schools policy and not be allowed unrestricted access to YouTube.
- A user cannot be a member of multiple groups that have different YouTube for School IDs. While the firewall will accept the configuration, this is not supported.



**NOTE:** For more information on the general configuration of CFS, refer to the **Security Services > Content Filter** section in the *SonicOS Administration Guide*.

*When the CFS Policy Assignment pulldown menu is set to Via Application Control, YouTube for Schools is configured as an App Control Policy.*

- 1 Navigate to **Firewall > Match Objects** and click **Add New Match Object**.

**Match Object Settings**

Object Name:

Match Object Type:

Match Type:

Input Representation: ☒ Alphanumeric ☐ Hexadecimal

Content:

List:

**Ready**

- 2 Type in a descriptive name, and then select **CFS Allow/Forbidden List** as the **Match Object Type**.
- 3 Select **Partial Match** for the **Match Type**.
- 4 In the **Content** field, type in "youtube.com" and then click **Add**.
- 5 Type in "yting.com" and then click **Add**.
- 6 Click **OK** to create the Match Object.

- 7 Navigate to the **Firewall > App Rules** page and click **Add New Policy**.

**App Control Policy Settings**

Policy Name:

Policy Type:

Address:

Exclusion Address:

Match Object:

Action Object:

Users/Groups:  Included:  Excluded:

Schedule:

Enable flow reporting: ☐

Enable Logging: ☒

Log using CFS message format: ☒

Log Redundancy Filter (seconds): ☐ Use Global Settings

Zone:

CFS Allow/Excluded List:

CFS Forbidden/Included List:

Enable Safe Search Enforcement: ☐

Enable YouTube for Schools: ☒

School ID:

**Note:** BWM Type: Advanced; To change go to [Firewall Settings > BWM](#)

**Ready**

- 8 Type in a descriptive **Policy Name**.
- 9 For the **Policy Type**, select **CFS**.
- 10 Select the appropriate settings for **Match Object** and **Action Object**, based on your environment.
- 11 For **CFS Allow/Excluded List**, select the Match Object you just created (our example uses “CFS Allow YT4S”).
- 12 Select the **Enable YouTube for Schools** checkbox.
- 13 Paste in your **School ID**, which is obtained from <http://www.youtube.com/schools>.
- 14 Click **OK** to create the policy.

**NOTE:** Once the policy has been applied, any existing browser connections will be unaffected until the browser has been closed and reopened. Also, if you have a browser open as administrator on the firewall, you will be excluded from CFS policy enforcement unless you configure the firewall specifically not to exclude you (select the Do not bypass CFS blocking for the Administrator checkbox on the Security Services > Content Filter page).

*When the CFS Policy Assignment drop-down menu is set to **Via User and Zone Screens**, YouTube for Schools is configured as part of the Content Filter policy.*

- 1 On the Security Services > Content Filter page, select **Content Filter Service** from the **Content Filter Type** drop-down menu.

- 2 Click the **Configure** button.
- 3 On the **Policy** tab, click the **Configure** icon for the CFS policy on which you want to enable YouTube for Schools.
- 4 Click on the **Settings** tab, and select the **Enable YouTube for Schools** checkbox.
- 5 Paste in your School ID, which is obtained from <http://www.youtube.com/schools>.

The screenshot shows the 'Custom List Settings' tab with the following sections:

- Custom List Settings**
  - Source of Allowed Domains: Global
  - Source of Forbidden Domains: Global
  - Source of Keyword: Global
- Safe Search Enforcement Settings**
  - ☐ Enable Safe Search Enforcement
- YouTube for Schools** (highlighted with a red box)
  - ☒ Enable YouTube for Schools
  - School ID: Lj3Q2GVaHbr3k\_yiY2lhkQ
- Filter Forbidden URLs by time of day**
  - Always on

- 6 Click **OK**.
- 7 On the **Custom List** tab, click the **Add** button for **Allowed Domains**.
- 8 In the dialog box, type "youtube.com" into the **Domain Name** field and click **OK**.
- 9 Click **Add** again.
- 10 Type "yting.com" into the **Domain Name** field and click **OK**.

The screenshot shows the 'Custom List' tab with the following sections:

- Allowed Domains**
  - youtube.com
  - yting.com
  - Buttons: Add..., Edit..., Delete, Delete All
- Forbidden Domains**
  - Buttons: Add..., Edit..., Delete, Delete All
- Keyword Blocking**
  - Buttons: Add..., Edit..., Delete, Delete All



11 Click **OK**. These settings will override any CFS category that blocks YouTube.

**NOTE:** Once the policy has been applied, any existing browser connections will be unaffected until the browser has been closed and reopened. Also, if you have a browser open as administrator on the firewall, you will be excluded from CFS policy enforcement unless you configure the firewall specifically not to exclude you (select the Do not bypass CFS blocking for the Administrator checkbox on the Security Services > Content Filter page).

## IKEv2 Support

Beginning in SonicOS 5.8.1.8, Internet Key Exchange version 2 (IKEv2) is the default proposal type for new Site-to-Site VPN policies when clicking the Add button from the VPN > Settings screen.

IKEv2 is a protocol for negotiating and establishing a security association (SA). IKEv2 provides improved security and a simplified architecture. Compared to IKEv1 Main Mode, using IKEv2 greatly reduces the number of message exchanges needed to establish an SA, while IKEv2 is more secure and flexible than IKEv1 Aggressive Mode. This reduces the delays during re-keying.

IPsec Secondary Gateway is supported with IKEv2. DHCP over VPN is not supported with IKEv2. IKEv2 is not compatible with IKEv1. When IKEv2 is used, all nodes in the VPN must use IKEv2 to establish the tunnels.

IKEv2 has the following advantages over IKEv1:

- More secure
- More reliable
- Simpler
- Faster
- Extensible
- Fewer message exchanges to establish connections
- EAP Authentication support
- MOBIKE support
- Built-in NAT traversal
- Keep Alive is enabled as default

## SNMP for VLAN Interfaces

In SonicOS 5.8.1.11 and higher, SNMP MIB-II statistic counters are supported for VLAN interfaces on the following appliances:

- SonicWALL NSA E8510
- SonicWALL NSA E8500
- SonicWALL NSA E7500
- SonicWALL NSA E6500
- SonicWALL NSA E5500
- SonicWALL NSA 5000
- SonicWALL NSA 4500
- SonicWALL NSA 3500
- SonicWALL NSA 2400
- SonicWALL NSA 240
- SonicWALL TZ 210 Series

- SonicWALL TZ 200 Series
- SonicWALL TZ 100 Series

In SonicOS 5.8.1.12 and higher, SNMP MIB-II statistic counters are supported for VLAN interfaces on the following appliances:

- SonicWALL NSA 250M Series
- SonicWALL NSA 220 Series
- SonicWALL TZ 215 Series
- SonicWALL TZ 205 Series
- SonicWALL TZ 105 Series

## SonicOS Management Interface HTTPS Default

HTTP access to the SonicOS web-based management interface is disabled by default. When running SonicOS with factory defaults, the administrator can log into the management interface using HTTPS at <https://192.168.168.168>.

HTTP management is still allowed when upgrading from prior firmware versions, when already enabled in the previous configuration settings.



**NOTE:** HTTP management must be enabled when the firewall is being managed by SonicWALL GMS via a VPN tunnel. This applies when using either a GMS Management Tunnel or an existing VPN tunnel.

The System > Administration page has an **Allow management via HTTP** checkbox to allow the administrator to enable/disable HTTP management globally.

**Web Management Settings**

☐ Allow management via HTTP

HTTP Port:  Delete cookies

HTTPS Port:  End config. mode

Certificate Selection: Use Selfsigned Certificate

Certificate Common Name:

Default Table Size:  items per page

Auto-updated Table Refresh Interval:  in seconds

☐ Use System Dashboard View as starting page

☒ Enable Tooltip

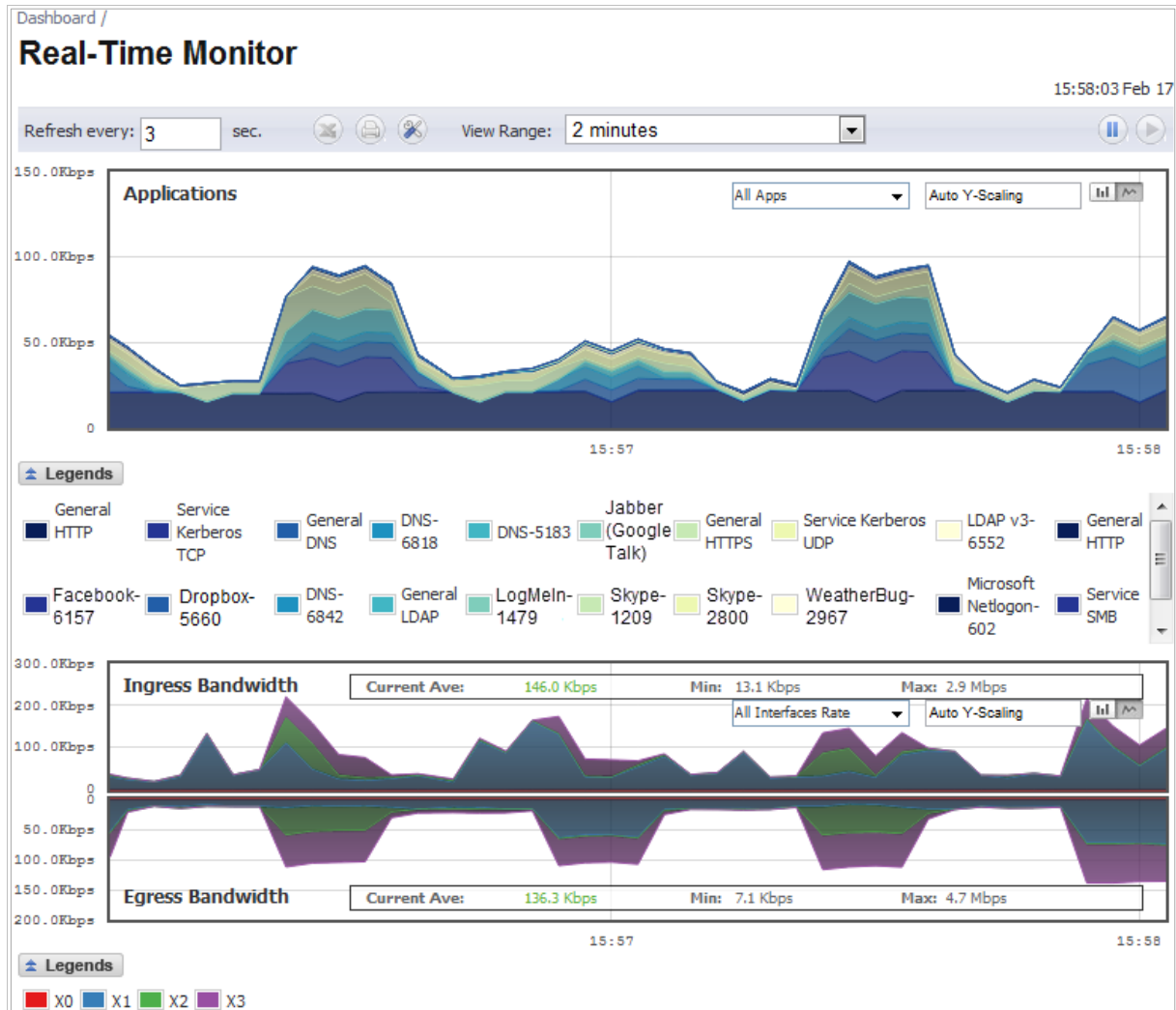
Form Tooltip Delay:  in msec

Button Tooltip Delay:  in msec

Text Tooltip Delay:  in msec

# Real-Time Monitor

The real-time visualization dashboard monitoring feature allows administrators to respond quickly to network security vulnerabilities and network bandwidth issues. Administrators can see what websites their users are accessing, what applications and services are being used in their networks and to what extent, in order to police content transmitted in and out of their organizations.



New appliances running SonicOS 5.8.1.15 receive an automatic 30-day free trial for App Visualization upon registration.

SonicWALL appliances upgrading from a pre-SonicOS 5.8 release and already licensed for GAV/IPS/AS, Total Secure, or Comprehensive Gateway Security Suite (CGSS) automatically receive a complimentary App Visualization license for the Real-Time Visualization Dashboard.

To populate the Real-Time Monitor with data, navigate to the **AppFlow > Flow Reporting** page, then click the **Enable Real-Time Data Collection** and **Enable AppFlow To Local Collector** checkboxes. In the **Collect Real-Time Data For** drop-down list, click the checkboxes for the types of data you wish to collect. You can then view real-time application traffic on the Dashboard > Real-Time Monitor page.

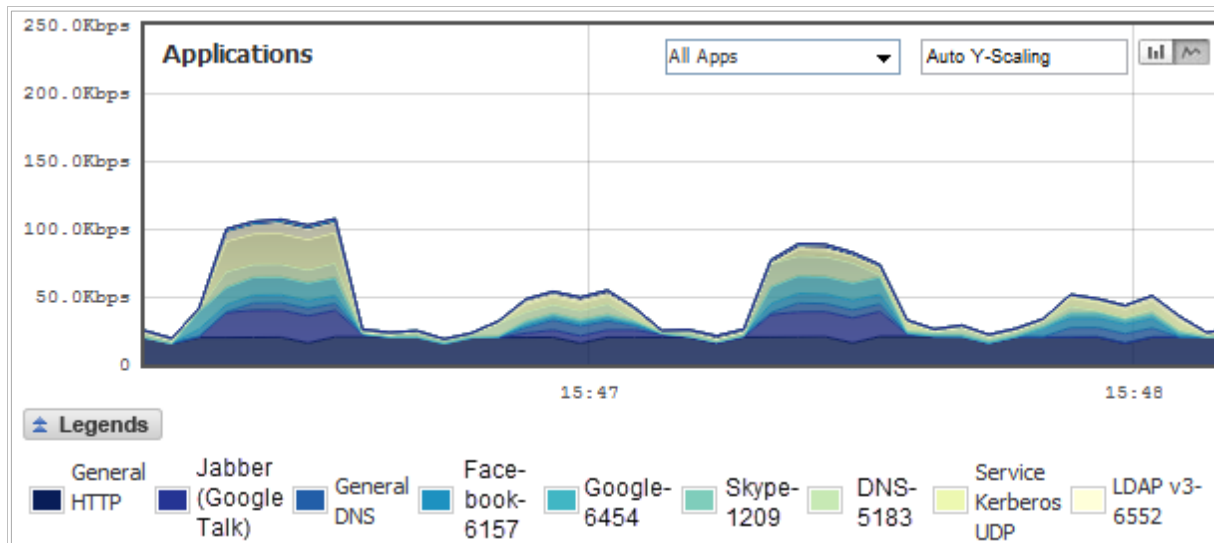



**NOTE:** Clicking the **Enable AppFlow to Local Collector** checkbox may require rebooting the device.

<b>Settings</b>	
Enable AppFlow To Local Collector <sup>[*]</sup>	<input checked="" type="checkbox"/>
Enable Real-Time Data Collection	<input checked="" type="checkbox"/>
Collect Real-Time Data For	Top apps, Bits per sec., Packets per sec., Average packet size, Connections per

All Real-Time Monitor application legends are hidden by default from the Application and Bandwidth charts.

To view the legends, click the  **Legends** icon.



To relocate the legends into the Application or Bandwidth charts, click the  icon, then select the desired checkbox(s).

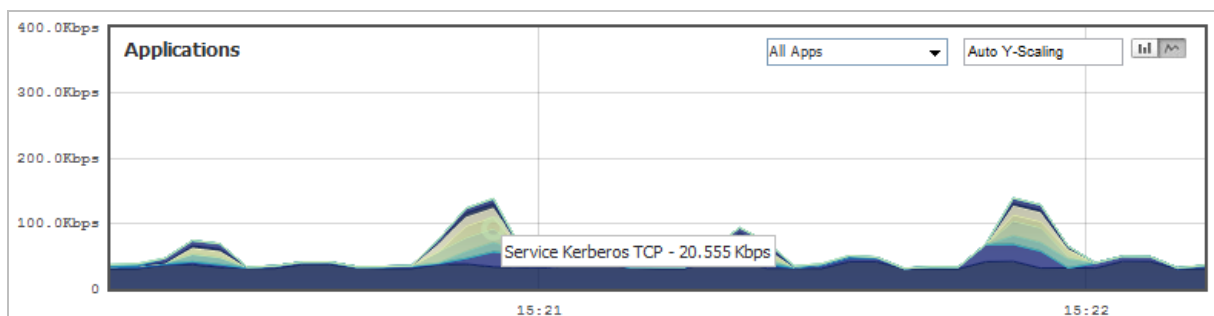


The dialog box contains the following options:

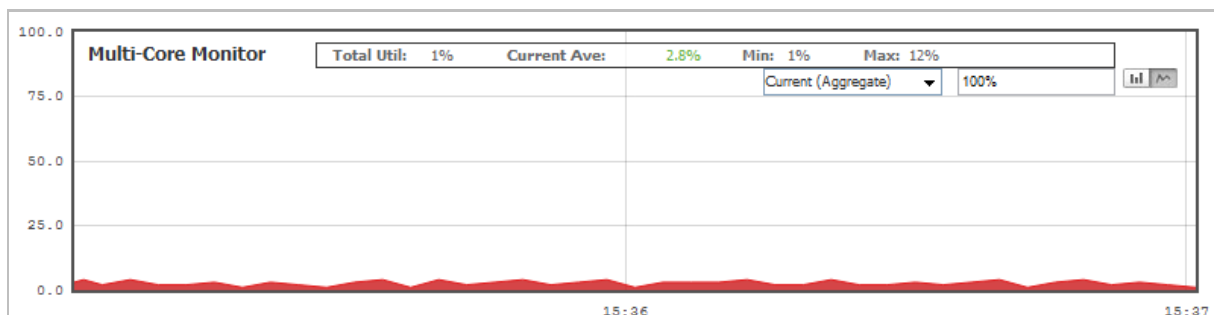
- ☒ Use Gradient
- ☐ Put legends inside Application Chart
- ☐ Put legends inside Bandwidth Chart

Buttons at the bottom: Default, Generate, Cancel, Save.

To view individual application information, hover the mouse over the real-time visualization graph to display a tooltip.



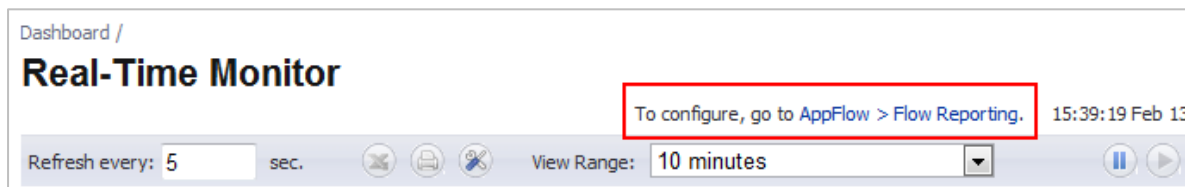
By default, the Multi-Core Monitor displays as a stack chart, rather than as a bar graph, to easily show its relation to the other charts on this screen.



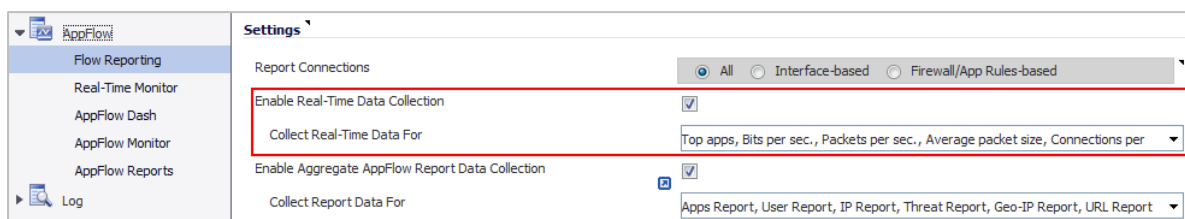
**NOTE:** The Multi-Core Monitor only shows the processor load for the cores of the managing firewall. If operating in Active-Active DPI mode, the core load for the standby firewall does not display.

## Link to Flow Reporting

The Dashboard > Real-Time Monitor page provides a link to the AppFlow > Flow Reporting page, where you can enable/disable each chart in the Real-Time Monitor page.

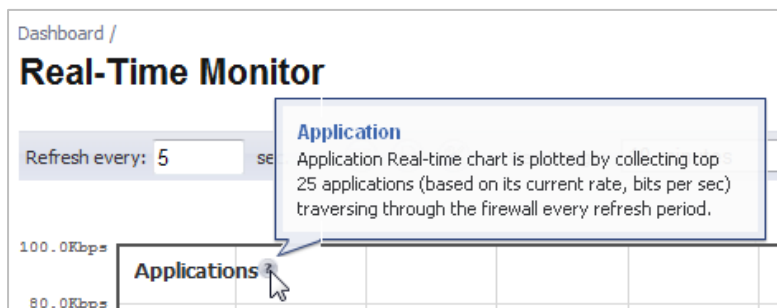


To enable/disable each chart in the Real-Time Monitor page, use the **Enable Real-Time Data Collection** option and associated drop-down list.



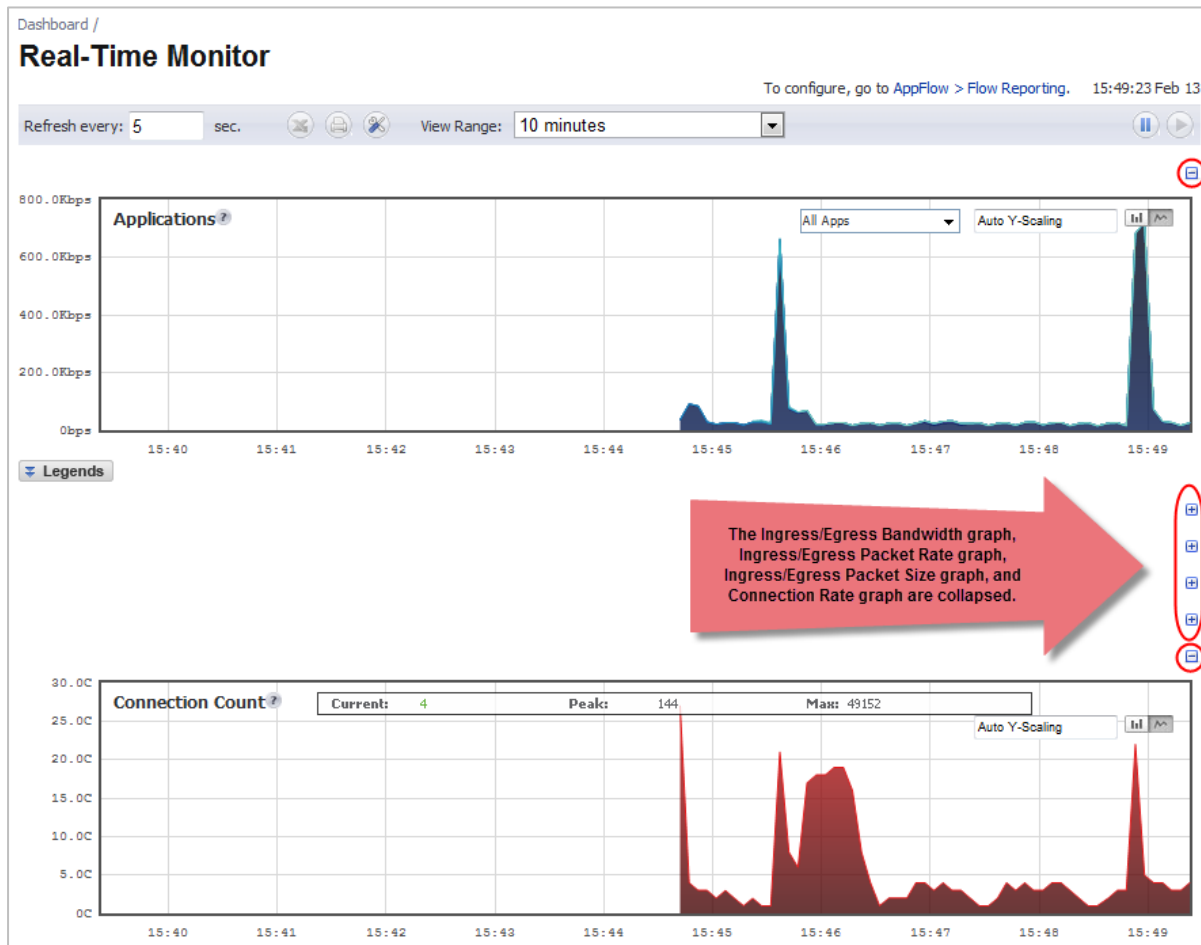
## Real-Time Monitor Tooltips

The Dashboard > Real-Time Monitor page provides a tooltip with useful information next to each chart title.



## Real-Time Monitor Collapse/Expand Options

The Dashboard > Real-Time Monitor page provides a collapse/expand button for each chart. This allows the administrator to juxtapose two charts for comparison, even if they are normally far apart on the page.

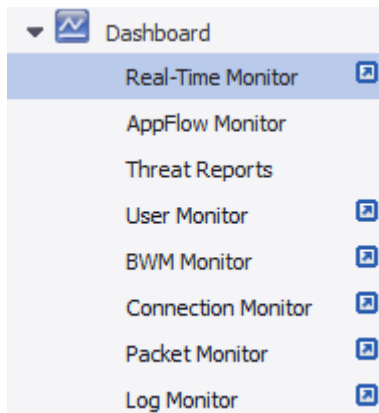


## Dashboard and AppFlow Enhancements

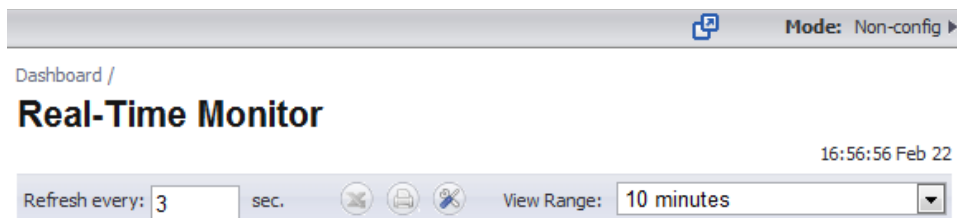
- [Standalone Dashboard Page](#)
- [AppFlow > Flow Reporting](#)
- [Dashboard > AppFlow Dash](#)
- [Dashboard > AppFlow Monitor](#)
- [Dashboard > AppFlow Reports](#)

## Standalone Dashboard Page

Several of the SonicOS Visualization Dashboard pages contain a blue pop-up button that will display the dashboard in a standalone browser window that allows for a wider display. Click on the blue pop-up icon to the right of the page name in the left-hand navigating bar to display a dashboard page as a standalone page.



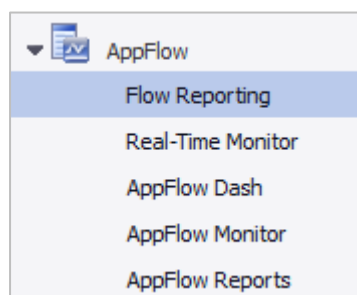
The pop-up button is also available at the top right of the individual dashboard pages, as shown below:



## AppFlow > Flow Reporting

The **AppFlow > Flow Reporting** page provides the information previously displayed in the **Log > Flow Reporting** page, such as detailed external and internal flow statistics. In SonicOS 5.8.1.11 and higher, the **Log > Flow Reporting** page is removed, and its elements are now displayed in the **AppFlow > Flow Reporting** page.

The **AppFlow** menu in the left navigation pane contains five pages. The lower four **AppFlow** pages display the corresponding **Dashboard** pages of the same names.



A number of enhancements have been added to the **AppFlow** and **Dashboard** pages.

More sections have been added to the **AppFlow > Flow Reporting** page, and some elements have been rearranged and placed under one of the three tabs:

- Statistics
- Settings
- External Collector

The **Statistics** section is shown below.

**Flow Reporting**

Accept Cancel Clear Default

Statistics Settings External Collector

**External Flow Reporting Statistics**

Connection Flows Enqueued:	0
Connection Flows Dequeued:	0
Connection Flows Dropped:	0
Connection Flows Skipped Reporting:	0
Non-Connection data Enqueued:	42
Non-Connection data Dequeued:	42
Non-connection data Dropped:	0
Non-connection related static data Reported:	0

**Internal AppFlow Reporting Statistics**

Data Flows Enqueued:	64337
Data Flows Dequeued:	64337
Data Flows Dropped:	0
Data Flows Skipped Reporting:	0
General Flows Enqueued:	42
General Flows Dequeued:	42
General Flows Dropped:	0
General Static Flows Dequeued:	135723
AppFlow Collector Errors:	0
Total Flows in DB:	11519

**Total IPFIX Statistics**

Total NetFlow/IPFIX Packets Sent:	0
NetFlow/IPFIX Packets Sent to External Collector:	0
Netflow/IPFIX Templates sent:	0
Connection Flows Sent to External Collector:	0

**Total IPFIX Statistics**

Non-Connection related Dynamic Flows Sent to External Collector:	0
Non-Connection related Static Flows Sent to External Collector:	0

The **Settings** section is shown below.

**Flow Reporting**

Accept Cancel Clear Default

Statistics Settings External Collector

**Settings**

Report Connections: ☒ All ☐ Interface-based ☐ Firewall/App Rules-based

Enable Real-Time Data Collection: ☒

Collect Real-Time Data For: Top apps, Bits per sec., Packets per sec., Average packet size, Connections per

Enable Aggregate AppFlow Report Data Collection: ☒

Collect Report Data For: Apps Report, User Report, IP Report, Threat Report, Geo-IP Report, URL Report

**Local Server Settings**

Enable AppFlow To Local Collector [\*]: ☒

**Other Report Settings**

Report DROPPED Connection: ☒

Skip Reporting STACK Connections: ☐

Include Following URL Types: Gifs, Jpegs, Pngs, Htmls, Aspx

Enable Geo-IP Resolution: ☒

AppFlow Report Upload Timeout (sec): 30

The options from the previous **Connection Report Settings** section are merged into the **External Collector Settings** section, except for the **Report Connections** option which is moved to the **Settings** section of the **AppFlow > Flow Reporting** page.

The **Settings** section provides options to control the reporting content by interface or rules, to control which graphs to display on the **Real-Time Monitor** page, and to control which graphs to display on the **AppFlow Monitor** page. The **Settings** area has an **Enable Aggregate AppFlow Report Data Collection** option and associated **Collect Report Data For** drop-down list. This allows the administrator to select the specific report types to be included in AppFlow reports. The functionality is very similar to the control over the Real-Time



Monitor charts provided by the **Enable Real-Time Data Collection** option and drop-down list, also in the **Settings** section. Some other options under **Settings** are:

- **Enable Geo-IP Resolution** — AppFlow Monitor groups flows based on country under initiator and responder tabs.
- **AppFlow Report Upload Timeout (sec)** — Specifies the timeout in seconds when connecting to the AppFlow upload server. The minimum value is 5, the maximum is 120, and the default is 30.

The **Enable Domain Resolution** option and the **Enable Domain Resolution for Private IPs** option have been removed from the **Settings** section.

The former **Generate All Templates** and **Generate Static AppFlow Data** buttons, which were at the top of the **Log > Flow Reporting** page, have been moved to the **Actions** option at the bottom of the **External Collector Settings** section of the page.

External Collector Settings

Send AppFlow and Real-Time Data To External Collector [\*]

☐

External AppFlow Reporting Format

Netflow version-5

External Collector's IP address

0.0.0.0

Source IP To Use For Collector On A VPN tunnel

0.0.0.0

External Collector's UDP Port Number

2055

Send IPFIX/Netflow Templates At Regular Interval

☐

Send Static AppFlow At Regular Interval

☐

Send Static AppFlow For Following Tables

Applications, Viruses, Spyware, Intrusions, Services, Rating Map

Send Dynamic AppFlow For Following Tables

Connections, Users, URLs, URL ratings, VPNs, VOIPs

Include Following Additional Reports via IPFIX

Report On Connection OPEN

☒

Report On Connection CLOSE

☒

Report Connection On Active Timeout

☐

Number Of Seconds

60

Report Connection On Kilo BYTES Exchanged

☐

Kilobytes Exchanged

100

Report ONCE

☐

Report Connections On Following Updates

threat detection, application detection, user detection, VPN tunnel detection

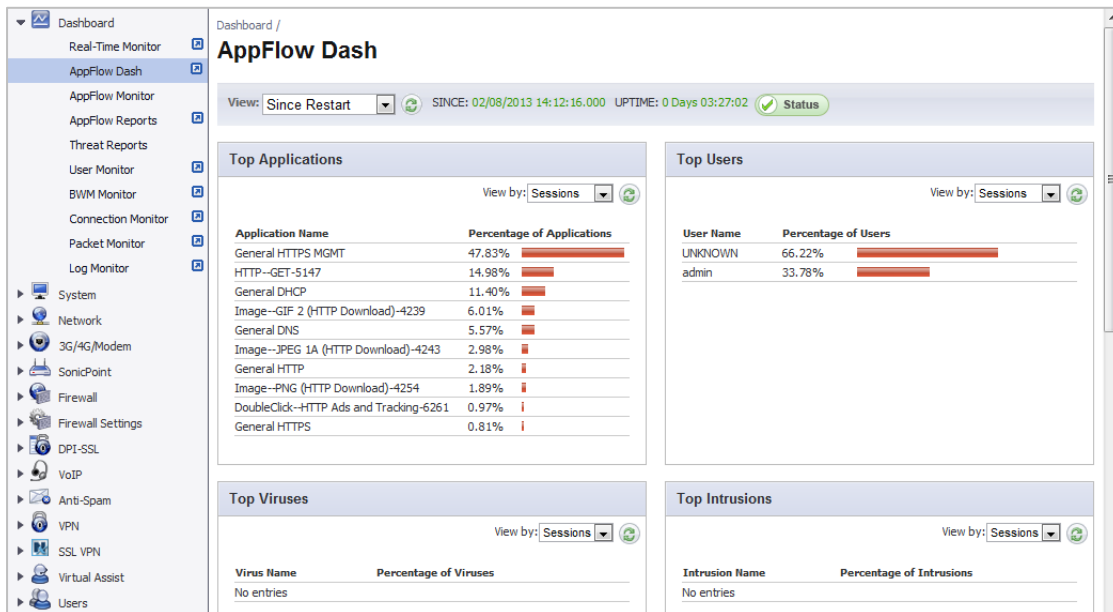
Actions

Generate ALL Templates

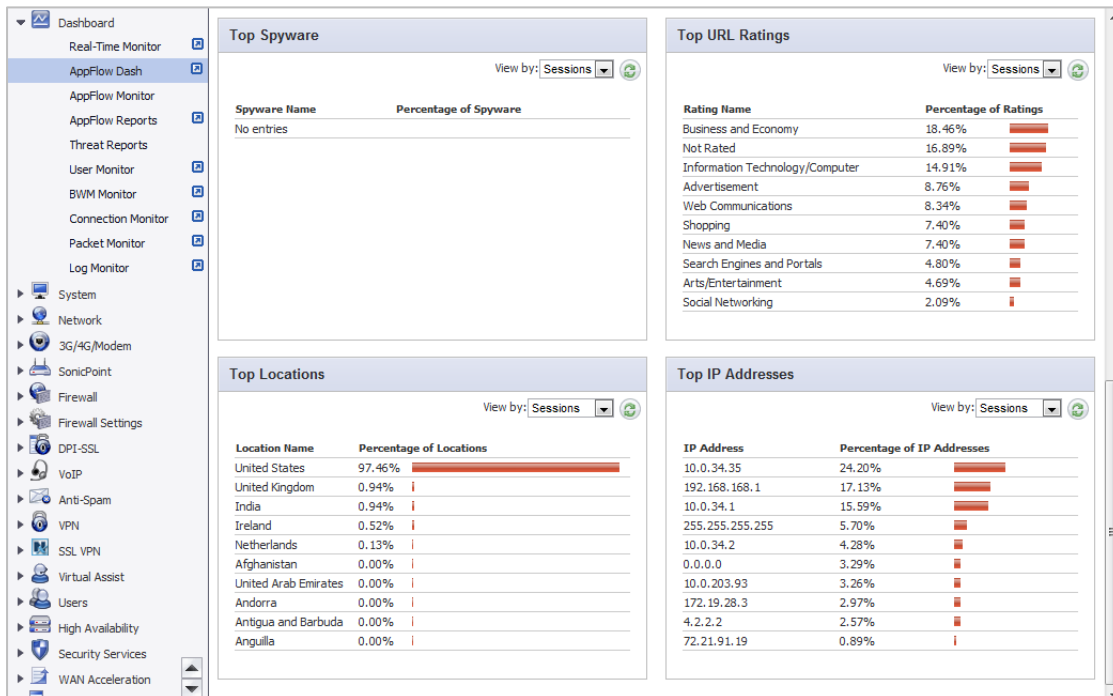
Generate Static AppFlow Data

## Dashboard > AppFlow Dash

The Dashboard > AppFlow Dash page provides graphs for Top Applications, Top Users, Top Viruses, Top Intrusions, Top Spyware, Top URL Ratings, Top Locations, and Top IP Addresses that are tracked with AppFlow. The top four graphs from the AppFlow Dash page are shown below:



The bottom four graphs from the AppFlow Dash page are shown below:



## Dashboard > AppFlow Monitor

The toolbar categories display Total Packets, Total Bytes, and Average Rate, providing the user with a specific view of data being transferred.

	Application	Sessions	Total Packets	Total Bytes ▼	Ave Rate (KBps)	Threats
<input type="checkbox"/>	Dropbox	3	91	50,046	0.817	0
<input type="checkbox"/>	Service Kerberos TCP	7	76	21,168	2.953	0
<input type="checkbox"/>	BitTorrent/uTorrent	186	186	16,678	-	0
<input type="checkbox"/>	DNS	8	98	9,167	1.071	0
<input type="checkbox"/>	HTTP	4	142	7,482	0.970	0
<input type="checkbox"/>	LDAP v3	1	18	5,093	4.974	0

In the Flow Table, clicking on the number specified under the Sessions category of any Application, a Flow Table displays with Application-specific data, including the Rate in KBps.

Flow Table															
Start Time	Last Update	Init MAC	Resp MAC	Init IP	Resp IP	Proto	Init Port	Resp Port	Init Iface	Resp Iface	Init Bytes	Resp Bytes	Rate (KBps)	Status	
15:24:34 Jan 12	15:24:34 Jan 12	00:06:B1:10:4E:06	00:06:B1:10:4E:07	172.16.0.9	172.16.5.35	6	2854	80	X2	X3	23506	101000	-	Active	
15:24:41 Jan 12	15:24:46 Jan 12	00:06:B1:10:4E:06	00:06:B1:10:4E:07	172.16.0.3	172.16.5.35	6	2854	80	X2	X3	46424	202048	425.906	Active	

The Dashboard > AppFlow Monitor page has several updates for enhanced usability:

- **AppFlow Monitor Filter** — A Filter text box provide a way to enter a text string to use for filtering the displayed information.

Dashboard / **AppFlow Monitor**

Load Filter: -- Select/Input Filter --

+ Filter View x

Filter:

Applications Users URLs Initiators Responders Threats VoIP VPN Devices Contents

Create Rule Filter View Interval: Last 60 seconds Group: Application

#	Application	Sessions	Total Packets	Total Bytes ▼	Ave Rate (KBps)
1	General HTTPS MGMT	20	314	95.37K	4.657
2	General DNS	2	4	354	0.173
3	General DHCP	1	1	328	-

Status

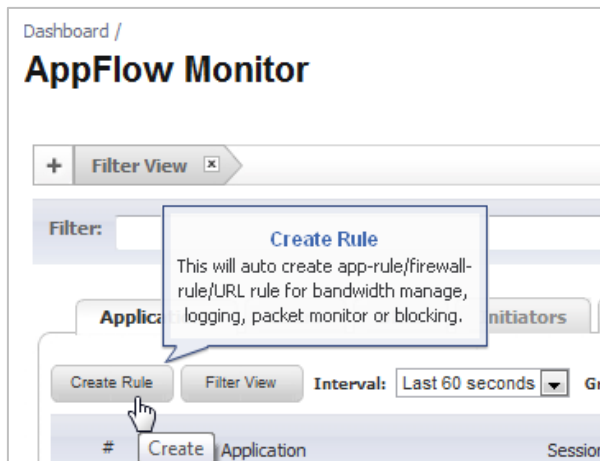
The Filter field is used to search for specific values in the main column, similar to this function on the Dashboard > AppFlow Reports page. The main column is the column to the right of the number (#) column, and its contents change depending on which tab is selected. For example, when the Applications tab is selected, you can filter on text strings that appear in the Application column.

If another tab is selected, the main column changes accordingly and the search values would be different.

- **Link to AppFlow > Flow Reporting** — A link to the AppFlow > Flow Reporting page is provided at the bottom of the Dashboard > AppFlow Monitor page.

- **Local Collector Status** — A green or red status line at the bottom of the Dashboard > AppFlow Monitor page shows whether AppFlow to Local Collector is enabled (green) or disabled (red).

- **Tooltips** — Additional tooltips are available on the **Dashboard > AppFlow Monitor** page for the Create Rule button, Filter View button, and other elements.



- **Numbering and Auto-Scrolling** — Numbering is added in the left-most column of each table on the **Dashboard > AppFlow Monitor** page, along with an auto-scroll feature, which automatically loads more rows as you scroll down. This allows you to keep track of where you are in the list while scrolling down, and avoids delays from loading large amounts of data at once. The total number of items is always displayed.

The screenshot shows the 'AppFlow Monitor' dashboard with a table of responders. The table has columns: #, Responder, Sessions, Total Packets, Total Bytes, and Ave Rate (Kbps). The table is auto-scrolling, and the total number of items (372) is displayed at the bottom. The table is filtered by 'IP Address' and 'Last 24 hours'.

#	Responder	Sessions	Total Packets	Total Bytes	Ave Rate (Kbps)
76	223.165.26.46	2	105	82.4K	-
77	74.125.224.44	8	246	79.15K	-
78	69.171.224.42	5	197	78.82K	-
79	69.172.216.56	11	168	77.20K	-
80	23.21.208.110	6	168	76.21K	-
81	216.36.248.222	8	138	75.63K	-
82	67.195.146.230	1	86	75.07K	-
83	69.171.237.40	3	186	73.44K	-
84	69.171.234.34	4	188	71.14K	-
85	206.160.170.26	5	231	69.35K	-
86	65.54.87.125	1	95	69.09K	-
87	23.11.15.139	3	120	68.44K	-
<b>Total:</b>	<b>372 item(s)</b>	<b>9.09K</b>	<b>129.13K</b>	<b>94.94M</b>	

## Dashboard > AppFlow Reports

The **Dashboard > AppFlow Reports** page provides aggregate AppFlow reports for the following cases:

- Since the last firewall restart
- Since the last reset of the counter; administrators can reset the counter manually

- Scheduled reports; administrators can set a start and end time for data to be collected, and can configure the reports to be sent either via email or to an FTP server once the period ends. This is done via scheduled objects.

Dashboard /

## AppFlow Reports

Filter String:

Applications Users IP Viruses Intrusions Spyware Location Botnets URL Rating

View: Since Restart Limit: 50 SINCE: 02/08/2013 14:12:16.000 UPTIME: 0 Days 03:33:49 Status

#	Name	Sessions	Init Bytes	Resp Bytes	Access Rules Block	App Rules Block	Location Block	BotNet Block	Viruses	Intrusions	Spyware
1	General HTTPS MGMT	4.71K	14.37M	17.82M	0	0	0	0	0	0	0
2	HTTP-GET-5147	1.44K	2.72M	11.10M	0	3	3	0	0	0	0
3	General DHCP	1.13K	358.84K	0	1,133	0	0	0	0	0	0
4	Image-GIF 2 (HTTP Download)-423	579	2.75M	3.10M	0	2	2	0	0	0	0
5	General DNS	539	57.82K	79.11K	0	0	0	0	0	0	0
6	Image-JPEG 1A (HTTP Download)-4	287	961.32K	9.71M	0	0	0	0	0	0	0
7	General HTTP	210	75.26K	450.60K	0	24	24	0	0	0	0
8	Image-PNG (HTTP Download)-4254	182	497.65K	5.60M	0	0	0	0	0	0	0
9	DoubleClick-HTTP Ads and Tracks	93	217.42K	379.15K	0	0	0	0	0	0	0
<b>Total: 50 item(s)</b>		<b>9.74K</b>	<b>23.55M</b>	<b>61.26M</b>	<b>1.13K</b>	<b>29</b>	<b>29</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>

up times: 0 Days 03:34:57 last update: 17:46:01 Feb 08

Aggregate AppFlow reporting is enabled. Apps Reporting is enabled. To configure, go to AppFlow > Flow Reporting.

The Filter String field at the top of the page is used to search for specific values in the main column. The main column is the column to the right of the number (#) column, and its contents change depending on which tab is selected. For example, when the Applications tab is selected, you can filter on text strings that appear in the Name column:

Dashboard /

## AppFlow Reports

Filter String: google

Applications Users IP Viruses Intrusions Spyware Location Botnets URL Rating

View: Since Restart Limit: 50 SINCE: 02/08/2013 14:12:16.000 UPTIME: 0 Days 03:40:36 Status

#	Name	Sessions	Init Bytes	Resp Bytes	Access Rules Block	App Rules Block	Location Block	BotNet Block	Viruses	Intrusions	Spyware
1	Google-SSL Any Google Domain 2-9379	14	29.51K	164.14K	0	0	0	0	0	0	0
2	Google Analytics-HTTP 2-2226	7	56.66K	1.17M	0	0	0	0	0	0	0
3	Google Safe Browsing--Traffic 1-707	7	12.64K	7.14K	0	0	0	0	0	0	0
4	Google Safe Browsing--Traffic 2-708	7	17.20K	42.62K	0	0	0	0	0	0	0
5	Google Analytics-HTTP 4-7885	2	18.65K	372.66K	0	0	0	0	0	0	0

When the **IP** tab is selected, the contents in the **Filter String** box are cleared, and you can enter an appropriate value to search for in the **IP Address** column:

Dashboard / **AppFlow Reports**

Filter String: 206

Applications Users **IP** Viruses Intrusions Spyware Location Botnets URL Rating

View: Since Restart Limit: 50 SINCE: 02/08/2013 14:12:16.000 UPTIME: 0 Days 03:47:57

#	IP Address	Sessions	Bytes Rcvd	Bytes Sent	Blocked	Virus	Spyware	Intrusion
1	206.160.170.43	164	<1%	281.81K	<1%	997.03K	1%	0
2	206.160.170.35	45	<1%	252.74K	<1%	857.58K	<1%	0
3	206.160.170.11	44	<1%	235.43K	<1%	1.86M	2%	0
4	206.160.170.18	38	<1%	78.22K	<1%	522.68K	<1%	0
5	206.160.170.16	37	<1%	223.99K	<1%	3.82M	4%	0
6	206.191.168.170	35	<1%	120.67K	<1%	110.67K	<1%	0

## Wire Mode / Inspect Mode

When **Inspect Mode (Passive DPI)** is selected as the **Wire Mode Setting**, a **Restrict analysis at resource limit** checkbox appears. This checkbox is selected by default. The behavior of this option is as follows:

- **Enabled** - Scan only the amount of packets that the device can handle.
- **Disabled** - Throttle the traffic to be able to scan all packets.

General Advanced

**Interface 'X2' Settings**

Zone: LAN

Mode / IP Assignment: Wire Mode (2-Port Wire)

Wire Mode Setting: Inspect Mode (Passive DPI)

☒ Restrict analysis at resource limit

Paired Interface: -- Select an Interface --

## Application Intelligence & Control

This feature has two components for more network security:

- **Identification** — Identify applications and track user network behaviors in real-time.
- **Control** — Allow/deny application and user traffic based on bandwidth limiting policies.

Administrators can easily create network policy object-based control rules to filter network traffic flows based on:

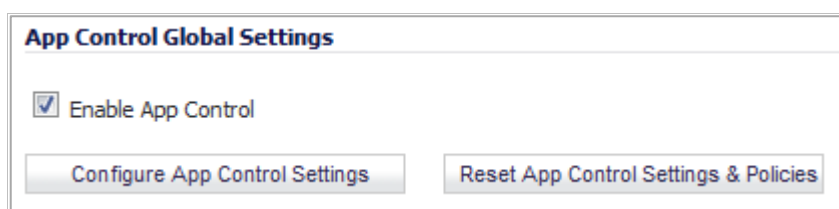
- Blocking signature-matching **Applications**, which are notoriously dangerous and difficult to enforce
- Viewing the real-time network activity of trusted **Users and User Groups** and guest services
- Matching **Content-rated categories**

Network security administrators now have application-level, user-level, and content-level real-time visibility into the traffic flowing through their networks. Administrators can take immediate action to re-traffic engineer their networks, quickly identify Web usage abuse, and protect their organizations from infiltration by malware. Administrators can limit access to bandwidth-hogging websites and applications, reserve higher priority to critical applications and services, and prevent sensitive data from escaping the SonicWALL secured networks.

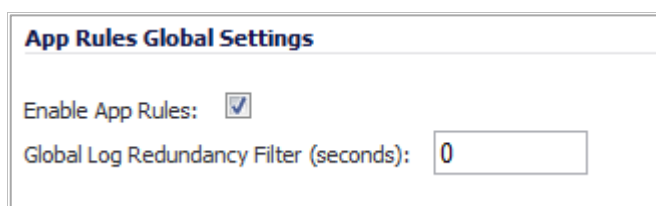
New appliances running SonicOS 5.8.1 and higher receive an automatic 30-day free trial for App Control upon registration.

SonicWALL appliances upgrading from a pre-SonicOS 5.8 release *and* already licensed for GAV/IPS/AS, Total Secure, or Comprehensive Gateway Security Suite (CGSS) automatically receive a complimentary App Control license, required for creating Application Control policies.

Select the **Enable App Control** option on the Firewall > App Control Advanced page to begin using the App Control feature.



To create policies using App Rules (included with the App Control license), select **Enable App Rules** on the Firewall > App Rules page.



## Global Bandwidth Management

Global Bandwidth Management improves ease of use for bandwidth management (BWM) configuration, and increases throughput performance of managed packets for ingress and egress traffic on all interfaces, not just WAN. The Firewall Settings > BWM page allows network administrators to specify guaranteed minimum bandwidth, maximum bandwidth, and control the number of different priority levels for traffic. These global settings are used in firewall access rules and application control policies. Global BWM provides:

- Simple bandwidth management on all interfaces.
- Bandwidth management of both ingress and egress traffic.
- Support for specifying bandwidth management priority per firewall rules and application control rules.
- Default bandwidth management queue for all traffic.
- Support for applying bandwidth management directly from the Dashboard > App Flow Monitor page.

Global bandwidth management provides 8 priority queues, which can be applied to each physical interface.

The Firewall Settings > BWM page is shown below:

Firewall Settings /

## BWM

**Bandwidth Management Type:**
☐ WAN
☒ Global
☐ None

Priority	Enable	Guaranteed	Maximum\Burst
0 Realtime	<input type="checkbox"/>	0 %	100 %
1 Highest	<input type="checkbox"/>	0 %	100 %
2 High	<input checked="" type="checkbox"/>	30 %	100 %
3 Medium High	<input type="checkbox"/>	0 %	100 %
4 Medium	<input checked="" type="checkbox"/>	50 %	100 %
5 Medium Low	<input type="checkbox"/>	0 %	100 %
6 Low	<input checked="" type="checkbox"/>	20 %	100 %
7 Lowest	<input type="checkbox"/>	0 %	100 %
<b>Total:</b>		<b>100</b>	

You can select either WAN or Global as the Bandwidth Management Type.

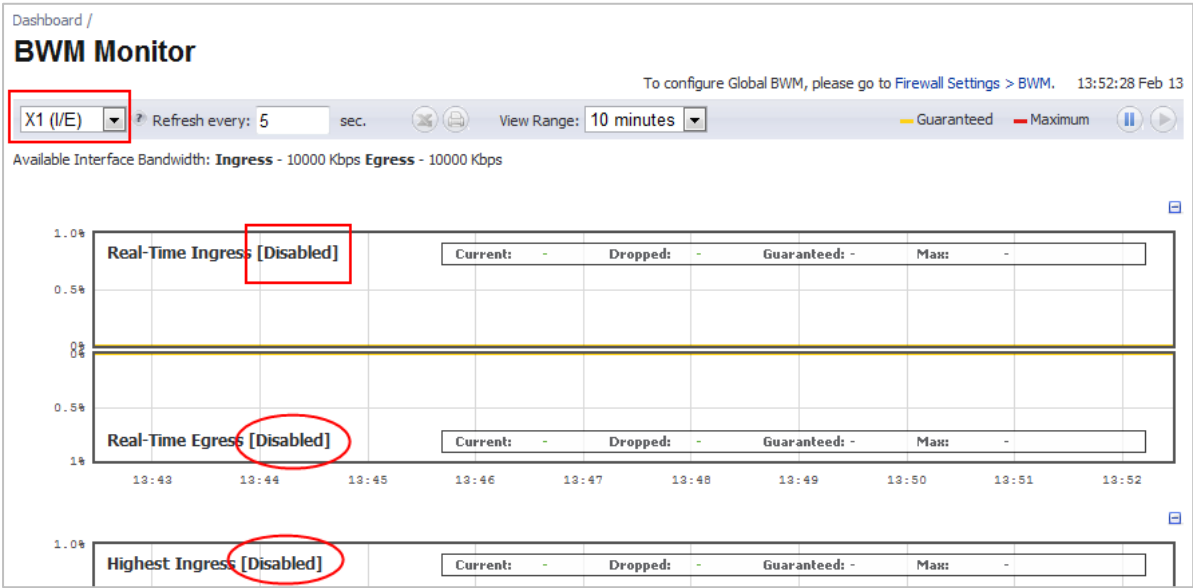
**NOTE:** When switching between bandwidth management modes, all bandwidth management settings in firewall access rules are set back to defaults and any custom settings must be reconfigured. Default BWM actions in Application Control policies are automatically converted to WAN BWM or Global BWM, using default priority levels.

In the global priority queue table, you can configure the **Guaranteed** and **Maximum\Burst** rates for each **Priority** queue. The rates are specified as a percentage. The actual rate is determined dynamically while applying BWM on an interface. The configured bandwidth on an interface is used in calculating the absolute value. The sum of all guaranteed bandwidth must not exceed 100%, and guaranteed bandwidth must not be greater than maximum bandwidth per queue.

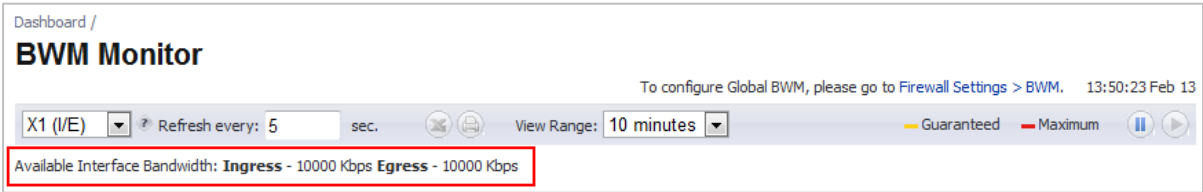
The **BWM Monitor** page displays per-interface bandwidth management for ingress and egress network traffic. The BWM monitor graphs are available for real-time, highest, high, medium high, medium, medium low, low and lowest policy settings. The view range is configurable in 60 seconds, 2 minutes, 5 minutes, and 10 minutes (default). The refresh interval rate is configurable from 3 to 30 seconds. The bandwidth management priority is depicted by guaranteed, maximum, and dropped.



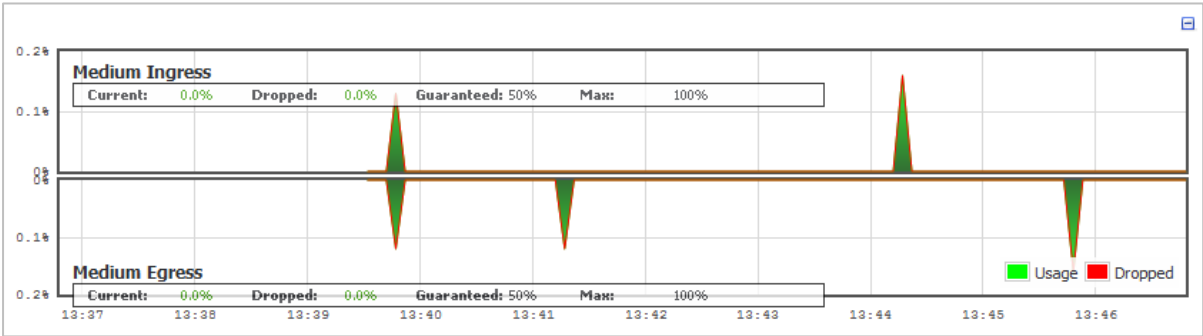
The Dashboard > BWM Monitor page displays a chart for each possible BWM setting for the selected interface, and displays [Disabled] unless BWM is enabled.



A text line is added near the top of the page showing the available bandwidth for the interface selected in the drop-down list at the top left.



In each chart, an information box now shows the values for Current bandwidth, Dropped bandwidth, Guaranteed bandwidth, and Max bandwidth for the interface selected at the top of the page.



The Firewall Settings > BWM page has usability enhancements. An Interface BWM Settings tooltip displays all network interfaces and shows whether bandwidth management is enabled for them.

Firewall Settings /

BWM

Accept

Cancel

Restore Defaults...

Bandwidth Management Type: ☐ WAN ☒ Global ☐ None

Interface BWM Settings

Interface Bandwidth Settings

Name	Ingress	Egress
X0	Disabled	Disabled
X1	Enabled / 10000 Kbps	Enabled / 10000 Kbps
X2	Disabled	Disabled
X3	Disabled	Disabled
X4	Disabled	Disabled
X5	Disabled	Disabled
U0	Disabled	Disabled
U1	Disabled	Disabled

Priority			Maximum\Burst
0	Realtime		
1	Highest		
2	High		
3	Medium High		
4	Medium		
5	Medium Low	<input type="checkbox"/>	0 %

The following note is displayed at the bottom of the Firewall Settings > BWM page:

**Note:** This priority table is used only when global bandwidth management is selected. (When using legacy BWM, values can be set independently in Firewall Access Rules and Action Objects.)

In global BWM mode, all traffic (by default) is marked as "medium" priority unless configured via firewall rule/app firewall rule.

## Geo-IP/Botnet

The System > Diagnostics page has a Geo-IP/Botnet Cache checkbox. If selected, the Geo-IP and Botnet cached information is included when generating a Tech Support Report (TSR). If not selected, this lengthy data will not be included in the TSR.

System /

Diagnostics

Accept

Cancel

Refresh

Tech Support Report

Include: ☒ VPN Keys ☒ ARP Cache ☒ DHCP Bindings ☒ IKE Info ☒ SonicPointN Diagnostics ☒ Current users ☒ Detail of users

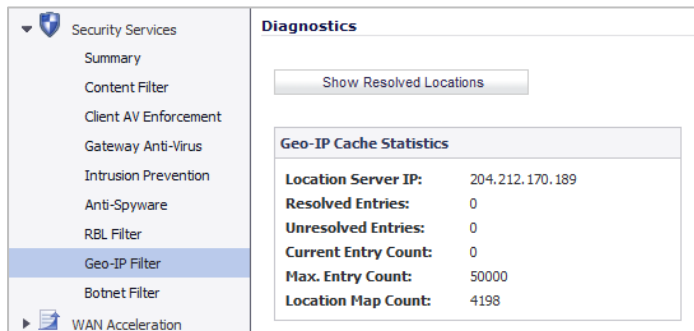
☐ Geo-IP/Botnet Cache

Download Report

Send Diagnostic Reports to Support

# Geo-IP Filter

The Geo-IP Filter page has a **Diagnostics** section containing a **Show Resolved Locations** button and a table displaying cache statistics.

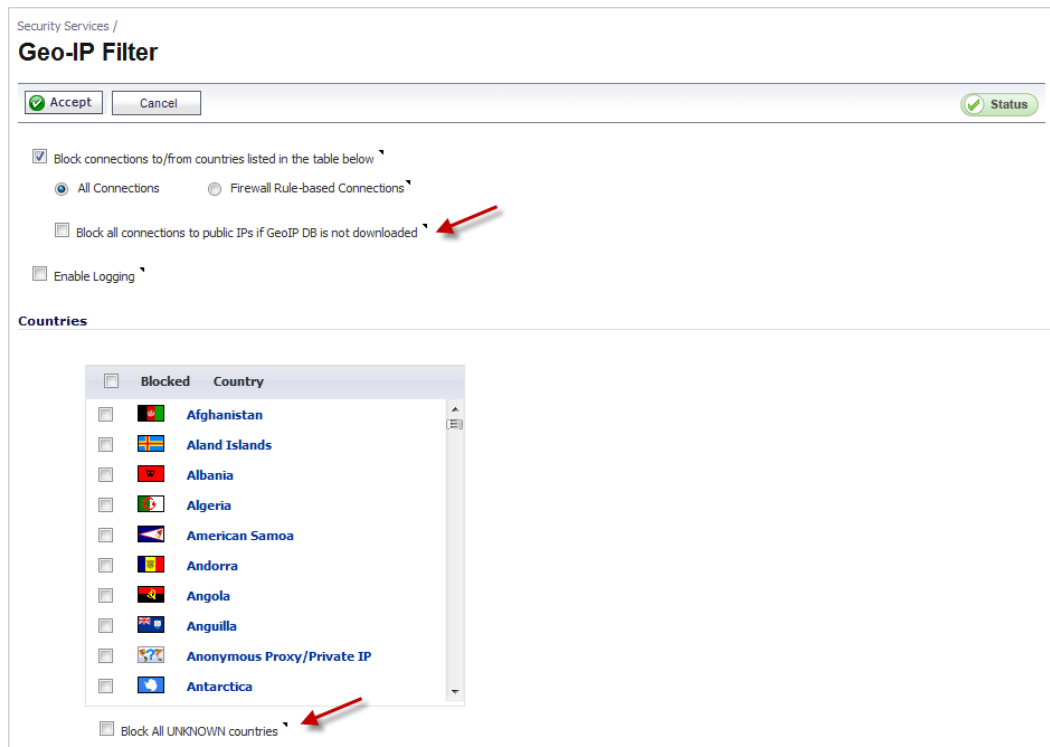


The Geo-IP Filter page includes several options, including **Block Connections to/from Following Countries**, **Block all connections to public IPs if GeoIP DB is not downloaded**, **Block ALL UNKNOWN countries**, and a checkbox for **Enable Logging**.

The **Block Connections to/from Following Countries** checkbox provides options to block **All Connections** or block **Firewall Rule-Based Connections**.

Select the **Block all connections to public IPs if GeoIP DB is not downloaded** option if you want all countries to be blocked whenever the firewall cannot download the Geo-IP database that contains the list of countries to be blocked. For selected countries to be blocked, the Geo-IP database must be downloaded from the Internet. The firewall must be able to resolve the address "gbdata.global.sonicwall.com" to download the country database. If the Geo-IP database is not downloaded successfully, the firewall cannot block selected countries.

Some countries may not be listed in the Geo-IP database. Select the **Block ALL UNKNOWN countries** option if you want all countries not listed in the Geo-IP database to be blocked.



# Botnet Filter

The **Botnet Filter** feature is available as a free trial and can be activated by navigating to the **Security Services > Botnet Filter** page. The Botnet Filter page provides configuration options for **Block connections to/from Botnet Command and Control Services**, **Block all connections to public IPs if BOTNET DB is not downloaded**, **Enable Logging**, defining Botnet exclusion objects, and checking Botnet server lookup.

Select the **Block all connections to public IPs if BOTNET DB is not downloaded** option if you want all public IP addresses to be blocked whenever the firewall cannot download the Botnet database that contains the list of Botnet IP addresses to be blocked. For selected IP addresses to be blocked, the Botnet database must be downloaded from the internet. If the Botnet database is not downloaded successfully, the firewall cannot block Botnet IP addresses.

The Botnet page also has a **Diagnostics** section containing a **Show Resolved Locations** button and a table displaying cache statistics.

Botnet Cache Statistics	
Location Server IP:	173.240.214.190
Resolved Entries:	52
Unresolved Entries:	0
Current Entry Count:	52
Max. Entry Count:	50000
Location Map Count:	253

## WXA 1.3 Support

SonicOS 5.8.1.15 supports WXA 1.3 and is only compatible with WXA 1.2.2 and newer. Earlier versions of WXA are not supported.

SonicWALL WXA 1.3 provides the following enhancements:

- **Increased Supported Connections**—WXA 1.3 runs as a 64-bit system, offering significant increases in concurrent connections over a 32-bit system.
- **Extended Support for Localization**—Firmware support for Brazilian Portuguese, Japanese, Simplified Chinese, and Korean languages is available.
- **Web Cache Data Improvements**—Additional data fields are added to the Web Cache statistics.
- **Manual Server Entry for Signed SMB**—The option to manually enter a server or share name is added to the Signed SMB Advanced configuration.

SonicWALL WXA 1.2.2 provides the following enhancements:

- **Unsigned SMB Acceleration**—In previous versions of WXA, SMB signing was the only supported method for shared access to files, which required joining the WXA series appliance to the domain and manually configuring shares. However, some networks do not need to use SMB signing. For these types of network environments, WXA 1.2 introduces support for Unsigned SMB, which allows the WXA series appliance to

accelerate traffic without joining the domain. This greatly simplifies the configuration procedure for WFS Acceleration. Just click the **Unsigned SMB** checkbox, apply the changes, and shared files start accelerating between sites.

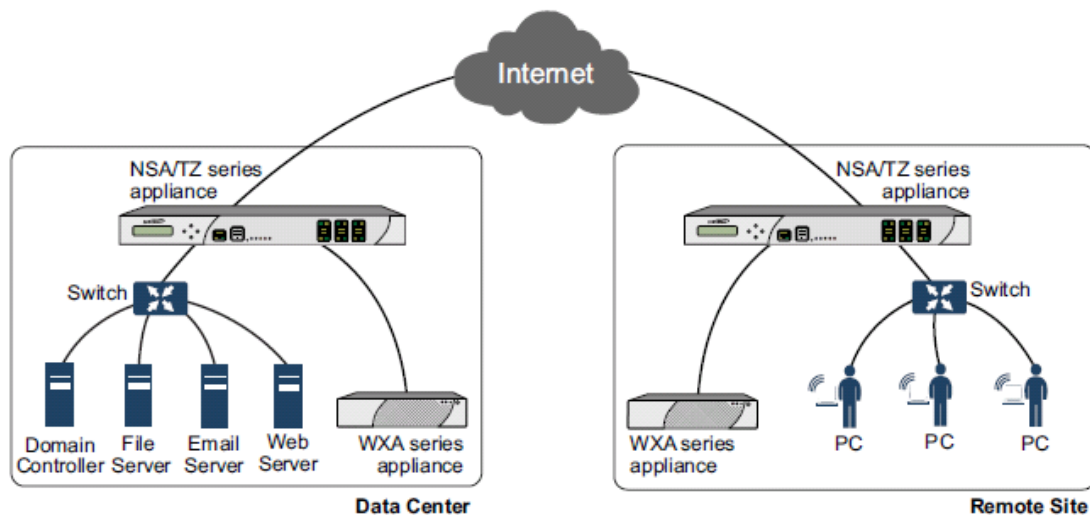
If your network uses unsigned and signed SMB traffic, the **Unsigned SMB** and **Support SMB Signing** checkboxes can be enabled to use both features simultaneously.

- **Web Cache**—The Web Cache feature stores copies of frequently and recently requested Web content as it passes through the network. When a user requests this Web content, it is retrieved from the local web cache instead of the Internet, which can result in significant reductions in downloaded data and bandwidth usage.
- **YouTube Web Caching**—The Web Cache feature also provides caching for YouTube content. This feature is only available when using Moderate (default) and Aggressive web caching strategies.

For more information about WAN Acceleration, see the *WXA 1.3 User's Guide*.

### About WAN Acceleration

The **WAN Acceleration** service allows network administrators to accelerate WAN traffic between a central site and a branch site by using Transmission Control Protocol (TCP), Windows File Sharing (WFS), and a Web Cache. The Dell SonicWALL WXA series appliance is deployed in conjunction with a Dell SonicWALL NSA/TZ series appliance. In this type of deployment, the NSA/TZ series appliance provides dynamic security services, such as attack prevention, Virtual Private Network (VPN), routing, and Web Content Filtering. The WAN Acceleration service can increase application performance.



## SonicPoint-N Dual Radio Support

The SonicWALL **SonicPoint-N Dual Radio** appliance (SonicPoint-N DR) is supported by all SonicWALL NSA and TZ platforms when running SonicOS 5.8.0.3 or higher.

With support for two wireless radios at the same time, you can use **SonicPoint-N DR Clean Wireless** access points to create an enterprise-class secure wireless network. The SonicPoint-N DR uses six antennas to communicate with wireless clients on two frequency ranges: 2.4 GHz and 5 GHz. You can install and configure a SonicPoint-N DR access point in about an hour.

**NOTE:** The SonicPoint-N DR cannot broadcast the same Service Set Identifiers (SSID) when using Virtual Access Points (VAP) on 2.4 and 5 GHz frequency ranges.

For more information, see the *SonicWALL SonicPoint-N DR Getting Started Guide*, at: <https://support.software.dell.com/>



## Accept Multiple Proposals for Clients Option

The **Accept Multiple Proposals for Clients** checkbox allows multiple VPN or L2TP clients using different security policies to connect to a firewall running SonicOS 5.8.0.3 or higher. This option is on the **Advanced** tab when configuring a GroupVPN policy from the **VPN > Settings** page in SonicOS.

The screenshot shows the SonicOS configuration interface with four tabs: General, Proposals, Advanced, and Client. The 'Advanced' tab is selected. Under the 'Advanced Settings' section, there are three checkboxes: 'Enable Windows Networking (NetBIOS) Broadcast', 'Enable Multicast', and 'Accept Multiple Proposals for Clients'. The 'Accept Multiple Proposals for Clients' checkbox is currently unchecked.

The client policy is still strictly checked against the configured proposal in the Proposals tab, as with clients connecting with SonicWALL GVC. This option has no effect on GVC.

If the **Accept Multiple Proposals for Clients** option is selected, SonicOS allows connections from other L2TP clients, (such as Apple OS, Windows, or Android), whose proposals are different from the configured proposal in the Proposals tab. These proposals are accepted under the following conditions:

- If the offered algorithm matches one of the possible algorithms available in SonicOS.
- If the offered algorithm is more secure than the configured algorithm in the SonicOS proposal.

If this option is not selected, SonicOS requires the client to strictly match the configured policy. This option allows SonicWALL to support heterogeneous environments for Apple, Windows, and Android clients. Using this option, SonicOS can work with these clients if their proposal includes a combination of algorithms which are supported in SonicOS, but are not configured in the policy to prevent other clients like GVC from failing.

## ADTRAN Consolidation

In SonicOS 5.8.1.11 and higher, ADTRAN NetVanta units run the same SonicOS firmware as SonicWALL units. Upon upgrading a NetVanta unit to SonicOS 5.8.1.11 or higher, the management interface will change from the previous NetVanta look and feel (color scheme, icons, logos) to the standard SonicWALL SonicOS look and feel. The Content Filter block page will look the same as that used by SonicWALL models.

In SonicOS 5.8.1.11 and higher, ADTRAN NetVanta units have the following capabilities:

- **Additional Features** — ADTRAN NetVanta units support the following additional features:
  - SonicPoint
  - Comprehensive Anti-Spam Service
  - WAN Acceleration
  - Enforced Client AV with Kaspersky Anti-Virus

- Solera
- Firmware Auto Update
- **Feature Capabilities** — On ADTRAN NetVanta units, the following features provide the same capabilities as the equivalent SonicWALL units:
  - DHCP Server Leases
  - Maximum Schedule Object Group Depth
  - Maximum SonicPoints per Interface
  - SSLVPN Licenses
  - Virtual Assist Licenses
- **Product Names** — On ADTRAN NetVanta units, the product name appears as the SonicWALL model name followed by “OEM” as follows:
  - NetVanta 2830 now appears as NSA 2400 OEM
  - NetVanta 2730 now appears as NSA 240 OEM
  - NetVanta 2730 EX now appears as NSA 240 OEM EX
  - NetVanta 2630 now appears as TZ 210 OEM
  - NetVanta 2630W now appears as TZ 210 wireless-N OEM
- **URLs** — ADTRAN NetVanta units use the same URLs as SonicWALL units.
- **WLAN SSID** — ADTRAN NetVanta units use “adtran” for the default Internal WLAN SSID.
- **HTTPS Certificates** — ADTRAN NetVanta units use an ADTRAN-specific HTTPS management self-signed certificate.

## Deep Packet Inspection of SSL encrypted data (DPI-SSL)

DPI-SSL provides the ability to transparently decrypt HTTPS and other SSL-based traffic, scan it for threats using SonicWALL’s Deep Packet Inspection technology, then re-encrypt (or optionally SSL-offload) the traffic and send it to its destination if no threats or vulnerabilities are found. This feature works for both client and server deployments. It provides additional security, application control, and data leakage prevention functionality for analyzing encrypted HTTPS and other SSL-based traffic. The following security services and features are capable of utilizing DPI-SSL: Gateway Anti-Virus, Gateway Anti-Spyware, Intrusion Prevention, Content Filtering, Application Control, Packet Monitor and Packet Mirror. DPI-SSL is supported on SonicWALL NSA models 240 and higher.

## Gateway Anti-Virus Enhancements (Cloud GAV)

The Cloud Gateway Anti-Virus feature introduces an advanced malware scanning solution that compliments and extends the existing Gateway AV scanning mechanisms present on SonicWALL firewalls 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 engine capabilities by consulting with the data center 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.

## NTP Authentication Type

When adding a Network Time Protocol server, the Add NTP Server dialog box provides a field to specify the NTP authentication type, such as MD5. Fields are also available to specify the trust key ID, the key number and the password.

## Link Aggregation

Link Aggregation provides the ability to group multiple Ethernet interfaces to form a trunk which looks and acts like a single physical interface. This feature is useful for high end deployments requiring more than 1 Gbps throughput for traffic flowing between two interfaces. This functionality is available on all NSA E-Class platforms.

Static Link Aggregation with the ability to aggregate up to 4 ports into a single link is supported in SonicOS 5.8. A round-robin algorithm is used for load balancing traffic across the interfaces in an aggregated link.

## Port Redundancy

Port Redundancy provides the ability to configure a redundant physical interface for any Ethernet interface in order to provide a failover path in case a link goes down. Port Redundancy is available on all NSA E-Class platforms.

When the primary interface is active, it handles all traffic from/to the interface. When the primary interface goes down, the backup interface takes over and handles all outgoing/incoming traffic. When the primary interface comes up again, it takes over all the traffic handling duties from the backup interface.

When Port Redundancy, High Availability and WAN Load Balancing are used together, Port Redundancy takes precedence followed by High Availability, then followed by WAN Load Balancing.

## Content Filtering Enhancements

The CFS enhancements provide policy management of network traffic based on Application usage, User activity, and Content type. Administrators can create multiple CFS policies per user group and set restrictive 'Bandwidth Management Policies' based on CFS categories.

## IPFIX and NetFlow Reporting

This feature enables administrators to gain visibility into traffic flows and volume through their networks, helping them with tracking, auditing and billing operations. This feature provides standards-based support for NetFlow Reporting, IPFIX, and IPFIX with extensions. The data exported through IPFIX with extensions contains information about network flows such as applications, users, and URLs extracted through Application Intelligence, along with standard attributes such as source/destination IP address (includes support for IPv6 networks), source/destination port, IP protocol, ingress/egress interface, sequence number, timestamp, number of bytes/packets, and more.

## VLAN Support for TZ Series

SonicOS 5.8.1.11 and higher provides VLAN support for SonicWALL TZ 210/200/100 Series appliances, including wireless models. The TZ 210 and 200 Series support up to 10 VLANs, the TZ 100 Series supports up to 5 VLANs.



# SonicPoint Virtual Access Point Support for TZ Series

Virtual Access Points (VAPs) are supported when one or more SonicWALL SonicPoints are connected to a SonicWALL TZ 210/200/100 Series appliance. The TZ 210 and 200 Series support up to 8 VAPs, the TZ 100 Series supports up to 5 VAPs.

## LDAP Primary Group Attribute

To allow Domain Users to be used when configuring policies, membership of the Domain Users group can be looked up via an LDAP "Primary group" attribute. Beginning in 5.8.1.0, SonicOS provides an attribute setting in the LDAP schema configuration for using this feature.

## Preservation of Anti-Virus Exclusions After Upgrade

SonicOS includes the ability to detect if the starting IP address in an existing range configured for exclusion from anti-virus enforcement belongs to either LAN, WAN, DMZ or WLAN zones. After upgrading to a newer firmware version, SonicOS applies the IP range to a newly created address object. Detecting addresses for other zones not listed above, including custom zones, is not supported.

Anti-virus exclusions which existed before the upgrade and which apply to hosts residing in custom zones will not be detected. IP address ranges not falling into the supported zones will default to the LAN zone. Conversion to the LAN zone occurs during the restart process. There is no message in the SonicOS management interface at login time regarding the conversion.

## Comprehensive Anti-Spam Service (CASS) 2.0

The Comprehensive Anti-Spam Service (CASS) feature provides a quick, efficient, and effective way to add anti-spam, anti-phishing, and anti-virus capabilities to your SonicWALL security appliance. This feature increases the efficiency of your SonicWALL security appliance by providing you the ability to configure user view settings and filter junk messages before users see it in their inboxes. The following capabilities are available with CASS 2.0:

- The Email Security Junk Store application can reside outside the Exchange Server system, such as on a remote server.
- Dynamic discovery of Junk Store user interface pages feature allows the Junk Store to inform SonicOS of a list of pages to display under Anti-Spam in the SonicOS left hand navigation pane. For example, the pane might show Junk Box View, Junk Box Settings, Junk Summary, User View Setup, and/or Address Books.
- User-defined Allow and Deny Lists can be configured with FQDN and Range address objects in addition to Host objects.
- A GRID IP Check tool is available in the Anti-Spam > Status page. The SonicWALL administrator can specify (on-demand) an IP address to check against the SonicWALL GRID IP server. The result will either be LISTED or UNLISTED. Connections from a LISTED host will be blocked by the SonicWALL security appliance running CASS (unless overridden in the Allow List).
- A parameter to specify the Probe Response Timeout is available in the Anti-Spam > Settings page Advanced Options section. This option supports deployment scenarios where a longer timeout is needed to prevent a target from frequently being marked as Unavailable. The default value is 30 seconds.

## Enhanced Connection Limiting

Connection Limiting enhancements expand the original Connection Limiting feature which provided global control of the number of connections for each IP address. This enhancement is designed to increase the granularity of this kind of control so that the SonicWALL administrator can configure connection limitation

more flexibly. Connection Limiting uses Firewall Access Rules and Policies to allow the administrator to choose which IP address, which service, and which traffic direction when configuring connection limiting.

## Dynamic WAN Scheduling

SonicOS 5.8 supports scheduling to control when Dynamic WAN clients can connect. A Dynamic WAN client connects to the WAN interface and obtains an IP address with the PPPoE, L2TP, or PPTP. This enhancement allows the administrator to bind a schedule object to Dynamic WAN clients so that they can connect when the schedule allows it and they are disconnected at the end of the configured schedule. In the SonicOS management interface, a Schedule option is available on the WAN interface configuration screen when one of the above protocols is selected for IP Assignment. Once a schedule is applied, a log event is recorded upon start and stop of the schedule.

## NTLM Authentication with Mozilla Browsers

As an enhancement to Single Sign-On, SonicOS can now use NTLM authentication to identify users who are browsing using Mozilla-based browsers (including Internet Explorer, Firefox, Chrome and Safari). NTLM is part of a browser authentication suite known as “Integrated Windows Security” and should be supported by all Mozilla-based browsers. It allows a direct authentication request from the SonicWALL appliance to the browser with no SSO agent involvement. NTLM authentication works with browsers on Windows, Linux and Mac PCs, and provides a mechanism to achieve Single Sign-On with Linux and Mac PCs that are not able to interoperate with the SSO agent.

## Single Sign-On Import Users from LDAP Option

An **Import from LDAP** button on the Users > Local Users page allows you to configure local users on the SonicWALL by retrieving the user names from your LDAP server. This allows SonicWALL user privileges to be granted upon successful LDAP authentication. For ease of use, options are provided to reduce the list to a manageable size and then select the users to import.

## SSL VPN NetExtender Update

This enhancement supports password change capability for SSL VPN users, along with various fixes. When the password expires, the user is prompted to change it when logging in via the NetExtender client or SSL VPN portal. It is supported for both local users and remote users (RADIUS and LDAP).

## DHCP Scalability Enhancements

The DHCP server in SonicWALL appliances has been enhanced to provide between 2 to 4 times the number of leases previously supported. To enhance the security of the DHCP infrastructure, the SonicOS DHCP server now provides server side conflict detection to ensure that no other device on the network is using the assigned IP address. Conflict detection is performed asynchronously to avoid delays when obtaining an address.

## SIP Application Layer Gateway Enhancements

SIP operational and scalability enhancements are provided in SonicOS 5.8. The SIP feature-set remains equivalent to previous SonicOS releases, but provides drastically improved reliability and performance. The SIP Settings section under the VoIP > Settings page is unchanged.

SIP ALG support has existed within SonicOS firmware since very early versions on legacy platforms. Changes to SIP ALG have been added over time to support optimized media between phones, SIP Back-to-Back User Agent (B2BUA), additional equipment vendors, and operation on a multi-core system.

The SIP protocol is now in a position of business critical importance - protecting the voice infrastructure, including VoIP. To accommodate the demands of this modern voice infrastructure, SIP ALG enhancements include the following:

- **SIP Endpoint Information Database** - The algorithm for maintaining the state information for known endpoints is redesigned to use a database for improved performance and scalability. Endpoint information is no longer tied to the user ID, allowing multiple user IDs to be associated with a single endpoint. Endpoint database access is flexible and efficient, with indexing by NAT policy as well as by endpoint IP address and port.
- **Automatically Added SIP Endpoints** - User-configured endpoints are automatically added to the database based on user-configured NAT policies, providing improved performance and ensuring correct mappings, as these endpoints are pre-populated rather than "learnt."
- **SIP Call Database** - A call database for maintaining information about calls in progress is implemented, providing improved performance and scalability to allow SonicOS to handle a much greater number of simultaneous calls. Call database entries can be associated with multiple calls.
- **B2BUA Support Enhancements** - SIP Back-to-Back User Agent support is more efficient with various algorithm improvements.
- **Connection Cache Improvements** - Much of the data previously held in the connection cache is offloaded to either the endpoint database or the call database, resulting in more efficient data access and corollary performance increase.
- **Graceful Shutdown** - Allows SIP Transformations to be disabled without requiring the firewall to be restarted or waiting for existing SIP endpoint and call state information to time out.

## Management Traffic Only Option for Network Interfaces

Beginning in 5.8.1.0, SonicOS provides a **Management Traffic Only** option on the **Advanced** tab of the interface configuration window, when configuring an interface from the **Network > Interfaces** page. When selected, this option prioritizes all traffic arriving on that interface. The administrator should enable this option **ONLY** on interfaces intended to be used exclusively for management purposes. If this option is enabled on a regular interface, it will still prioritize the traffic, but that may not be the desired result. It is up to the administrator to limit the traffic to just management; the firmware does not have the ability to prevent pass-through traffic.

The purpose of this option is to provide the ability to access the SonicOS management interface even when the appliance is running at 100% utilization.

## Auto-Configuration of URLs to Bypass User Authentication

Beginning in 5.8.1.0, SonicOS includes an auto-configuration utility to temporarily allow traffic from a single, specified IP address to bypass authentication. The destinations that traffic accesses are then recorded and used to allow that traffic to bypass user authentication. Typically this is used to allow traffic such as anti-virus updates and Windows updates. To use this feature, navigate to **Users > Settings** and click the **Auto-configure** button in the Other Global User Settings section.

# System compatibility

This section provides additional information about hardware and software compatibility with this release.

## WAN Acceleration (WXA) support

The Dell SonicWALL WXA series appliances (WXA 6000 Software, WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are supported for use with Dell SonicWALL NSA E-Class, NSA, and TZ products running 5.8.1.15. The recommended firmware version for the WXA series appliances is 1.3. SonicOS 5.8.1.15 is only compatible with WXA 1.2.2 and newer. Earlier versions of WXA are not supported.

## Browser support



SonicOS with Visualization uses advanced browser technologies such as HTML5, which are supported in most recent browsers. SonicWALL recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of SonicOS.

This release supports the following Web browsers:

- Chrome 18.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 16.0 and higher
- Internet Explorer 8.0 and higher (do not use compatibility mode)
- Safari 5.0 and higher



**NOTE:** On Windows machines, Safari is not supported for SonicOS management.



**NOTE:** Mobile device browsers are not recommended for Dell SonicWALL appliance system administration.

## Product licensing

Dell SonicWALL network security appliances must be registered on MySonicWALL to enable full functionality and the benefits of Dell SonicWALL security services, firmware updates, and technical support. Log in or register for a MySonicWALL account at <https://mysonicwall.com/>.

A number of security services are separately licensed features in SonicOS. SonicOS periodically checks the license status with the SonicWALL License Manager. When a service is licensed, full access to the functionality is available.

The System > Status page displays the license status for each security service.

# Upgrading SonicOS image procedures

The following procedures are for upgrading an existing SonicOS image to a newer version:

- [Obtaining the latest SonicOS image version](#)
- [Creating a system backup and exporting your settings](#)
- [Upgrading firmware with current settings](#)
- [Upgrading firmware with factory default settings](#)
- [Using SafeMode to upgrade firmware](#)
- [Importing configuration settings](#)
- [Importing settings from SonicOS Standard to SonicOS 5.8.1.15 Enhanced](#)

## Obtaining the latest SonicOS image version

To obtain a new SonicOS firmware image file for your SonicWALL security appliance:

- 1 Connect to your mysonicwall.com account at <http://www.mysonicwall.com>.
- 2 In MySonicWALL, click **Downloads** in the left navigation pane to display the Download Center screen.
- 3 Select your product in the **Software Type** drop-down list to display available firmware versions.
- 4 To download the firmware to your computer, click the link for the firmware version you want. You can download the Release Notes and other associated files in the same way.

You can update the SonicOS image on a SonicWALL security appliance remotely if the LAN interface or the WAN interface is configured for management access.

## Creating a system backup and exporting your settings

### Create Backup

Before beginning the update process, you can use the **Create Backup** button to make a system backup on your Dell SonicWALL appliance.

On Dell SonicWALL NSA 2400 and above, the backup feature saves a copy of the current system state, firmware, and configuration settings on your appliance, protecting all your existing settings in the event that it becomes necessary to return to a previous configuration state.



**NOTE:** The TZ series, NSA 220 series, NSA 240, and NSA 250M series do not support a full firmware image backup.

### Create Backup Settings

On TZ 105 series, TZ 205 series, TZ 215 series, NSA 220 series, NSA 240, and NSA 250M series, you can use the **Create Backup Settings** button to save a copy of the configuration settings locally on the firewall. The saved settings can be used with the current firmware version or with a newly uploaded firmware version.



**NOTE:** The TZ 100 series and TZ 200 series do not support saving a copy of the settings directly on the unit.

## Export Settings

On all appliance platforms, you can export the appliance configuration settings to a file on your local management station. This file serves as an external backup of the configuration settings, and can be imported into another appliance or into the same appliance if it is necessary to reboot the firmware with factory default settings.

*To save a system backup on your appliance and export configuration settings to a file on your local management station:*

- 1 To save a system backup or backup settings in the System > Settings page, do one of the following:
  - On an NSA 2400 or above, click **Create Backup**. SonicOS takes a “snapshot” of your current system state, firmware, and configuration preferences, and makes it the new System Backup firmware image. Clicking **Create Backup** overwrites the existing System Backup image, if any. The System Backup entry is displayed in the Firmware Management table.
  - On a TZ, NSA 220, NSA 240, or NSA 250M, click **Create Backup Settings**. SonicOS saves a small file on the appliance with all your configuration settings. Any previous backup settings file is overwritten. The Firmware Management table displays the **Current Firmware with Backup Settings** entry.
- 2 To export your settings to a local file, click **Export Settings** and then click **Export** in the popup window that displays the name of the saved file.
- 3 On the System > Diagnostics page, under **Tech Support Report**, select the following checkboxes and then click the **Download Report** button:
  - VPN Keys
  - ARP Cache
  - DHCP Bindings
  - IKE Info
  - SonicPointN Diagnostics
  - Current users
  - Detail of users

**NOTE:** A Download button is displayed in the Firmware Management table for System Backup and for Current/Uploaded Firmware with Backup Settings. However, the downloaded files cannot be imported into another appliance, nor can they be uploaded like firmware. Use **Export Settings** to save your configuration settings for import into another appliance.


The information is saved to a “techSupport\_” file on your management computer.

## Upgrading firmware with current settings

You can update the SonicOS image on a Dell SonicWALL security appliance by connecting your computer to the LAN (X0) port or you can update it remotely if the LAN or WAN interface is configured for remote management access.


*To upload new firmware to your Dell SonicWALL appliance and use your current configuration settings upon startup:*


- 1 Download the SonicOS firmware image file from mysonicwall.com and save it to a location on your local computer.
- 2 Point your browser to the appliance IP address, and log in as an administrator.
- 3 On the System > Settings page, click **Upload New Firmware**.
- 4 Browse to the location where you saved the SonicOS firmware image file, select the file, and click **Upload**. After the firmware finishes uploading, it is displayed in the Firmware Management table.

- 5 On the System > Settings page, click the Boot icon  in the row for **Uploaded Firmware - New!**
- 6 In the confirmation dialog box, click **OK**. The SonicWALL restarts and then displays the login page.
- 7 Enter your user name and password. Your new SonicOS image version information is listed on the System > Settings page.

## Upgrading firmware with factory default settings

*To upload new firmware to your Dell SonicWALL appliance and start it up using the default configuration:*

- 1 Download the SonicOS firmware image file from [mysonicwall.com](http://mysonicwall.com) and save it to a location on your local computer.
- 2 Point your browser to the appliance IP address, and log in as an administrator.
- 3 On the System > Settings page, click **Upload New Firmware**.
- 4 Browse to the location where you saved the SonicOS firmware image file, select the file, and click **Upload**.
- 5 On the System > Settings page, click the Boot icon  in the row for **Uploaded Firmware with Factory Default Settings**.
- 6 In the confirmation dialog box, click **OK**. The appliance restarts and then displays the options to launch the Setup Wizard or go to the login page of the SonicOS management interface.  



**NOTE:** The IP address for the X0 (LAN) interface reverts to the default, 192.168.168.168. You can log into SonicOS by connecting to X0 and pointing your browser to <https://192.168.168.168>.
- 7 Enter the default user name and password (admin / password) to access the SonicOS management interface.

## Using SafeMode to upgrade firmware

If you are unable to connect to the SonicOS management interface, you can restart the Dell SonicWALL security appliance in SafeMode. The SafeMode feature allows you to quickly recover from uncertain configuration states with a simplified management interface that includes the same settings available on the System > Settings page.


The SafeMode procedure uses a recessed reset button in a small pinhole for which the location varies:

- On the NSA models, the button is near the USB ports on the front.
- On the TZ models, the button is next to the power connection on the back.

*To use SafeMode to upgrade firmware on a Dell SonicWALL security appliance:*

- 1 Connect your computer to the X0 port on the appliance and configure your computer with an IP address on the 192.168.168.0/24 subnet, such as 192.168.168.20.
- 2 Do one of the following to restart the appliance in SafeMode:
  - Use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the reset button on the security appliance for more than 20 seconds.
  - On platforms with an LCD screen and control buttons on the front bezel, you can use the LCD control buttons to set the appliance to SafeMode. Once selected, the LCD displays a confirmation prompt. Select **Y** and press the **Right** button to confirm. The Dell SonicWALL security appliance changes to SafeMode.

The Test light starts blinking when the appliance has rebooted into SafeMode.

 **NOTE:** Holding the reset button for two seconds will send a diagnostic snapshot to the console. Holding the reset button for six to eight seconds will reboot the appliance in regular mode.

- 3 Point the browser on your computer to 192.168.168.168. The SafeMode management interface displays.
- 4 Click **Upload New Firmware**, and then browse to the location where you saved the SonicOS firmware image, select the file, and click **Upload**.
- 5 Click the Boot icon in the row for one of the following:
  - **Uploaded Firmware - New!**  
Use this option to restart the appliance with your current configuration settings.
  - **Uploaded Firmware with Factory Default Settings - New!**  
Use this option to restart the appliance with factory default configuration settings.
- 6 In the confirmation dialog box, click **OK** to proceed.
- 7 If you booted with current configuration settings, reconfigure your computer as needed to automatically obtain an IP address and DNS server address, or reset it to its normal static values.
- 8 Connect the computer to your network or leave it connected to the X0 (LAN) interface of the appliance, and point your browser to the WAN or LAN (depending on how you are connected) IP address of the Dell SonicWALL appliance.

After successfully booting the firmware, the login screen is displayed. If you booted with factory default settings, enter the default user name and password (admin / password) to access the SonicOS management interface. The default IP address of the X0 interface is 192.168.168.168.

## Importing configuration settings

You can import configuration settings from one appliance to another, which can save a lot of time when replacing an older appliance with a newer model. This feature is also useful when you need multiple appliances with similar configuration settings.

Importing configuration settings, or preferences ("prefs"), to Dell SonicWALL network security appliances running SonicOS 5.8.1 is generally supported from the following Dell SonicWALL appliances:

- NSA E-Class Series
- NSA Series
- TZ 215/210/205/200/105/100/190/180/170 Series
- PRO Series

There are certain exceptions to preferences importing on these appliances running the SonicOS 5.8.1.15 release. Preferences cannot be imported in the following cases:

- Settings files containing Portshield interfaces created prior to SonicOS 5.x
- Settings files containing VLAN interfaces are not accepted by the TZ 100/200 Series firewalls
- Settings files from a PRO 5060 with optical fiber interfaces where VLAN interfaces have been created

Full support for preferences importing from these appliances is targeted for a future release. At that time, you will need to upgrade your firmware to the latest SonicOS maintenance release available on MySonicWALL.



# Importing settings from SonicOS Standard to SonicOS

## 5.8.1.15 Enhanced

The SonicOS Standard to Enhanced Settings Converter is designed to convert a source Standard Network Settings file to be compatible with a target SonicOS Enhanced appliance. Due to the more advanced nature of SonicOS Enhanced, its Network Settings file is more complex than the one SonicOS Standard uses. They are not compatible. The Settings Converter creates an entirely new target Enhanced Network Settings file based on the network settings found in the source Standard file. This allows for a rapid upgrade from a Standard deployment to an Enhanced one with no time wasted in re-creating network policies.



**NOTE:** SonicWALL recommends deploying the converted target Network Settings file in a testing environment first and always keeping a backup copy of the original source Network Settings file.

The SonicOS Standard to Enhanced Settings Converter is available at:

<https://convert.global.sonicwall.com/>

If the preferences conversion fails, email your SonicOS Standard configuration file to [settings\\_converter@sonicwall.com](mailto:settings_converter@sonicwall.com) with a short description of the problem. In this case, you may also consider manually configuring your SonicWALL appliance.

To convert a Standard Network Settings file to an Enhanced one:

- 1 Log in to the management interface of your SonicOS Standard appliance, navigate to **System > Settings**, and save your network settings to a file on your management computer.
- 2 On the management computer, point your browser to <https://convert.global.sonicwall.com/>.
- 3 Click the **Settings Converter** button.
- 4 Log in using your MySonicWALL credentials and agree to the security statement.

The source Standard Network Setting file must be uploaded to MySonicWALL as part of the conversion process. The Setting Conversion tool uses MySonicWALL authentication to secure private network settings. Users should be aware that SonicWALL retains a copy of their network settings after the conversion process is complete.

- 5 Upload the source Standard Network Settings file:

- Click **Browse**.
- Navigate to and select the source SonicOS Standard Settings file.
- Click **Upload**.
- Click the right arrow to proceed.

- 6 Review the source SonicOS Standard Settings Summary page.

This page displays useful network settings information contained in the uploaded source Network Settings file. For testing purposes, the LAN IP and subnet mask of the appliance can be changed on this page in order to deploy it in a testing environment.

- (Optional) Change the LAN IP address and subnet mask of the source appliance to that of the target appliance.
- Click the **right arrow** to proceed.

- 7 Select the target SonicWALL appliance for the Enhanced deployment from the available list.

SonicOS Enhanced is configured differently on various SonicWALL appliances, mostly to support different interface numbers. As such, the converted Enhanced Network Settings file must be customized to the appliance targeted for deployment.

- 8 Complete the conversion by clicking the **right arrow** to proceed.
- 9 Optionally click the **Warnings** link to view any differences in the settings created for the target appliance.
- 10 Click the **Download** button, select **Save to Disk**, and click **OK** to save the new target SonicOS Enhanced Network Settings file to your management computer.

- 11 Log in to the management interface for your SonicWALL appliance.
- 12 Navigate to **System > Settings**, and click the **Import Settings** button to import the converted settings to your appliance.

## Support matrix for importing preferences

### Legend

This legend defines the letter-codes used in the tables below.

Y	Supported
N	Unsupported. While importing the settings file may be successful, firewall limitations may result in the removal of items such as DHCP scopes, VPN settings, etc.
B	Portshield interfaces prior to SonicOS 5.x are not supported.
C	Configuration information from extra interfaces will be removed. NAT policies, Firewall access rules and other interface-dependent configuration will also be removed.
D	When importing from non-SonicOS 5.x devices, the X2 interface will be configured in the DMZ zone.
E	VLANs created as sub-interfaces of the fiber interfaces will be renamed.

Tables:

- [NSA / E-Class NSA configuration import support](#)
- [TZ / NSA configuration import support](#)

## NSA / E-Class NSA configuration import support

The following matrix shows the Dell SonicWALL firewalls whose configuration settings can be imported to Dell SonicWALL NSA and E-Class NSA platforms. The source firewalls are in the left column, and the destination firewalls are listed across the top.

		DESTINATION FIREWALLS									
		NSA 2400	NSA 2400MX	NSA 3500	NSA 4500	NSA 5000	NSA E5500	NSA E6500	NSA E7500	NSA E8500	NSA E8510
S O U R C E  F I R E W A L L S	PRO 1260	N	N	N	N	N	N	N	N	N	N
	PRO 2040	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	PRO 3060	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	PRO 4060	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	PRO 4100	C	Y	C	C	C	C	C	C	C	C
	PRO 5060	C,E	E	C,E	C,E	C,E	C,E	C,E	C,E	C,E	C,E
	TZ 170	N	N	N	N	N	N	N	N	N	N
	TZ 170W	N	N	N	N	N	N	N	N	N	N
	TZ 170SP	N	N	N	N	N	N	N	N	N	N
	TZ 170SPW	N	N	N	N	N	N	N	N	N	N
	TZ 180	N	N	N	N	N	N	N	N	N	N
	TZ 180W	N	N	N	N	N	N	N	N	N	N
	TZ 190	N	N	N	N	N	N	N	N	N	N
	TZ 190W	N	N	N	N	N	N	N	N	N	N
	TZ 100/TZ 200	N	N	N	N	N	N	N	N	N	N
	TZ 100W/TZ 200W	N	N	N	N	N	N	N	N	N	N
	TZ 105/TZ 205	N	N	N	N	N	N	N	N	N	N
	TZ 105W/TZ 205W	N	N	N	N	N	N	N	N	N	N
	TZ 210	N	N	N	N	N	N	N	N	N	N
	TZ 210W	N	N	N	N	N	N	N	N	N	N
	TZ 215	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	TZ 215W	N	N	N	N	N	N	N	N	N	N
	NSA 220	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	NSA 220W	N	N	N	N	N	N	N	N	N	N
	NSA 240	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	NSA 250M	N	N	N	N	N	N	N	N	N	N
	NSA 250MW	N	N	N	N	N	N	N	N	N	N
	NSA 2400	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	NSA 2400MX	C	Y	C	C	C	C	C	C	C	C
	NSA 3500	C	Y	Y	Y	Y	Y	Y	Y	Y	Y
	NSA 4500	C	Y	Y	Y	Y	Y	Y	Y	Y	Y
	NSA 5000	C	Y	C	C	Y	Y	Y	Y	Y	Y
	NSA E5500	C	Y	C	C	C	Y	Y	Y	Y	C
	NSA E6500	C	Y	C	C	C	Y	Y	Y	Y	C
	NSA E7500	C	Y	C	C	C	Y	Y	Y	Y	C
	NSA E8500	C	Y	C	C	C	Y	Y	Y	Y	C
	NSA E8510	Y	Y	Y	Y	Y	C	C	C	C	Y

## TZ / NSA configuration import support

The following matrix shows the Dell SonicWALL firewalls whose configuration settings can be imported to Dell SonicWALL TZ 100/200/105/205/210/215 series and NSA 220/240/250M series platforms. The source firewalls are in the left column, and the destination firewalls are listed across the top.

		DESTINATION FIREWALLS												
		TZ100/ TZ200	TZ100w/ TZ200w	TZ105/ TZ205	TZ105w/ TZ205w	TZ210	TZ210w	TZ215	TZ215w	NSA 220	NSA 220W	NSA 240	NSA 250M	NSA 250MW
S O U R C E	PRO 1260	B,D	B,D	B,D	B,D	B,D	B,D	B,D	B,D	N	N	B,D	N	N
	PRO 2040	N	N	N	N	N	N	N	N	N	N	C	N	N
	PRO 3060	N	N	N	N	N	N	N	N	N	N	C	N	N
	PRO 4060	N	N	N	N	N	N	N	N	N	N	C	N	N
	PRO 4100	N	N	N	N	N	N	N	N	N	N	C	N	N
	PRO 5060	N	N	N	N	N	N	N	N	N	N	C,E	N	N
	TZ 170	B,D	B,D	B,D	B,D	B,D	B,D	B,D	B,D	N	N	B,C,D	N	N
	TZ 170W	B,C,D	B,D	B,C,D	B,D	B,C,D	B,D	B,C,D	B,D	N	N	B,C,D	N	N
	TZ 170SP	B,C,D	B,C,D	B,C,D	B,C,D	B,C,D	B,D	B,C,D	B,D	N	N	B,C,D	N	N
	TZ 170SPW	C,D	B,C,D	C,D	B,C,D	B,C,D	B,D	B,C,D	B,D	N	N	B,C,D	N	N
	TZ 180	C,D	C,D	C,D	C,D	C,D	C,D	C,D	C,D	N	N	B,D	N	N
	TZ 180W	C,D	C,D	C,D	C,D	C,D	C,D	C,D	C,D	N	N	B,C,D	N	N
	TZ 190	C,D	C,D	C,D	C,D	C,D	C,D	C,D	C,D	N	N	B,D	N	N
	TZ 190W	C,D	C,D	C,D	C,D	C,D	C,D	C,D	C,D	N	N	B,C,D	N	N
	TZ 100/TZ 200	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	TZ 100W/TZ 200W	C	Y	C	Y	C	Y	C	Y	N	N	Y	N	Y
	TZ 105/TZ 205	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	TZ 105W/TZ 205W	C	Y	C	Y	C	Y	C	Y	N	N	Y	N	Y
	TZ 210	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N
	TZ 210W	C	Y	C	Y	C	Y	C	Y	C	Y	Y	N	N
	TZ 215	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N
	TZ 215W	C	Y	C	Y	C	Y	C	Y	C	Y	N	N	N
D E S T I N A T I O N	NSA 220	N	N	N	N	N	N	N	N	Y	Y	Y	N	N
	NSA 220W	N	N	N	N	N	N	N	N	C	Y	N	N	N
	NSA 240	N	N	N	N	N	N	N	N	N	N	Y	C	C
	NSA 250M	N	N	N	N	N	N	N	N	N	N	N	Y	Y
	NSA 250MW	N	N	N	N	N	N	N	N	N	N	N	N	Y
	NSA 2400	N	N	N	N	N	N	N	N	C	N	C	N	N
	NSA 2400MX	N	N	N	N	N	N	N	N	C	C	C	C	C
	NSA 3500	N	N	N	N	N	N	N	N	C	N	C	N	N
	NSA 4500	N	N	N	N	N	N	N	N	C	N	C	N	N
	NSA 5000	N	N	N	N	N	N	N	N	C	N	C	N	N
	NSA E5500	N	N	N	N	N	N	N	N	C	N	C	N	N
	NSA E6500	N	N	N	N	N	N	N	N	C	N	C	N	N
	NSA E7500	N	N	N	N	N	N	N	N	C	N	C	N	N
	NSA E8500	N	N	N	N	N	N	N	N	C	N	C	N	N
	NSA E8510	N	N	N	N	N	N	N	N	C	N	Y	N	N

# Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the portal provides direct access to product support engineers through an online Service Request system. To access the Support Portal, go to <http://software.dell.com/support/>.

The site enables you to:

- View Knowledge Base articles at:  
<https://support.software.dell.com/kb-product-select>
- View instructional videos at:  
<https://support.software.dell.com/videos-product-select>
- Engage in community discussions
- Chat with a support engineer
- Create, update, and manage Service Requests (cases)
- Obtain product notifications

SonicOS Administration Guides and related documents are available on the Dell Software Support site at <https://support.software.dell.com/release-notes-product-select>.

## About Dell

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

## Contacting Dell

Technical support:

[Online support](#)

Product questions and sales:

(800) 306-9329

Email:

[info@software.dell.com](mailto:info@software.dell.com)

© 2015 Dell Inc.  
ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Dell Inc.

The information in this document is provided in connection with Dell 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 Dell products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES 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 DELL 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 DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes 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. Dell does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Dell Inc.  
Attn: LEGAL Dept.  
5 Polaris Way  
Aliso Viejo, CA 92656

Refer to our web site ([software.dell.com](http://software.dell.com)) for regional and international office information.

## Patents

For more information about applicable patents, refer to <http://software.dell.com/legal/patents.aspx>.

## Trademarks

Dell, the Dell logo, and SonicWALL are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.

## Legend



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



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



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

---

Last updated: 8/6/2015

232-002983-00 Rev A