

# Release Notes

## Contents

Platform Compatibility .....	1
Browser Support .....	1
Supported Features by Appliance Model .....	2
Supported SonicWALL NSA Modules .....	3
Enhancements .....	4
Licensing Geo-IP and Botnet Filtering .....	8
Known Issues .....	10
Resolved Issues .....	12
Upgrading SonicOS Image Procedures .....	17
Related Technical Documentation .....	22

## Platform Compatibility

The SonicOS 5.8.1.4 release is supported on the following SonicWALL Deep Packet Inspection (DPI) security appliances:

- SonicWALL NSA 250M / 250M Wireless
- SonicWALL NSA 220 / 220 Wireless

The SonicWALL WAN Acceleration Appliance Series (WXA 500 Live CD, WXA 2000 appliance, WXA 4000 appliance, WXA 5000 Virtual Appliance) are also supported for use with NSA appliances running 5.8.1.4. The minimum recommended Firmware version for WXA Series is 1.0.18.

## 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 11.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 4.0 and higher
- Internet Explorer 8.0 and higher (do not use compatibility mode)
- Safari 5.0 and higher

Mobile device browsers are not recommended for SonicWALL appliance system administration.

# Release Notes

## Supported Features by Appliance Model

The following table lists the supported / not supported key features in SonicOS 5.8 for the SonicWALL NSA 220 and 250M series appliances.

Features Supported on NSA 220 and NSA 250M Series	Features Not Supported on NSA 220 and NSA 250M Series
DPI-SSL	Link Aggregation
NSA Modules (supported only on NSA 250M Series)	Port Redundancy
Wireless Client Bridge Support	Wire Mode
App Flow Monitor	
Real-Time Monitor	
Top Global Malware	
Log Monitor	
Connection Monitor	
Packet Monitor	
Log > Flow Reporting	
App Control Advanced	
App Rules	
Cloud GAV	
NTP Auth Type	
CFS Enhancements	
IPFIX & NetFlow Reporting	
VLAN	
SonicPoint VAPs	
CASS 2.0	
Enhanced Connection Limit	
Dynamic WAN Scheduling	
Browser NTLM Auth	
SSO Import from LDAP	
SSL VPN NetExtender Update	
DHCP Scalability Enhancements	
SIP Application Layer Gateway Enhancements	
SonicPoint-N DR	
Accept Multiple Proposals for Clients	
WAN Acceleration Support	
App Control Policy Configuration via App Flow Monitor	
Global BWM Ease of Use Enhancements	

# Release Notes

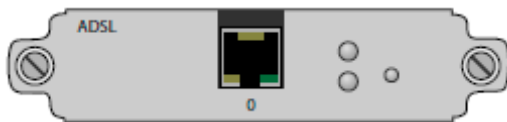
Features Supported on NSA 220 and NSA 250M Series	Features Not Supported on NSA 220 and NSA 250M Series
Application Usage and Risk Report	
Geo-IP Filtering and Botnet Command & Control Filtering	
Customizable Login Page	
LDAP Primary Group Attribute	
Preservation of Anti-Virus Exclusions After Upgrade	
Management Traffic Only Option for Network Interfaces	
Current Users and Detail of Users Options for TSR	
User Monitor Tool	
Auto-Configuration of URLs to Bypass User Authentication	

## Supported SonicWALL NSA Modules

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

**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.

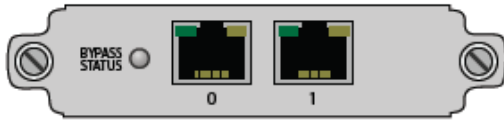


- **1-port T1/E1 Module** – Provides the connection of a T1 or E1 (digitally multiplexed telecommunications carrier system) circuit to a SonicWALL firewall using a RJ-45 jack.

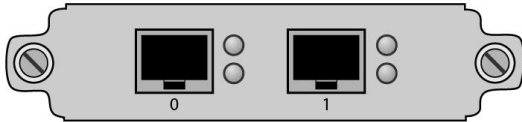


# Release Notes

- **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** – A small form-factor pluggable (SFP) network interface module.

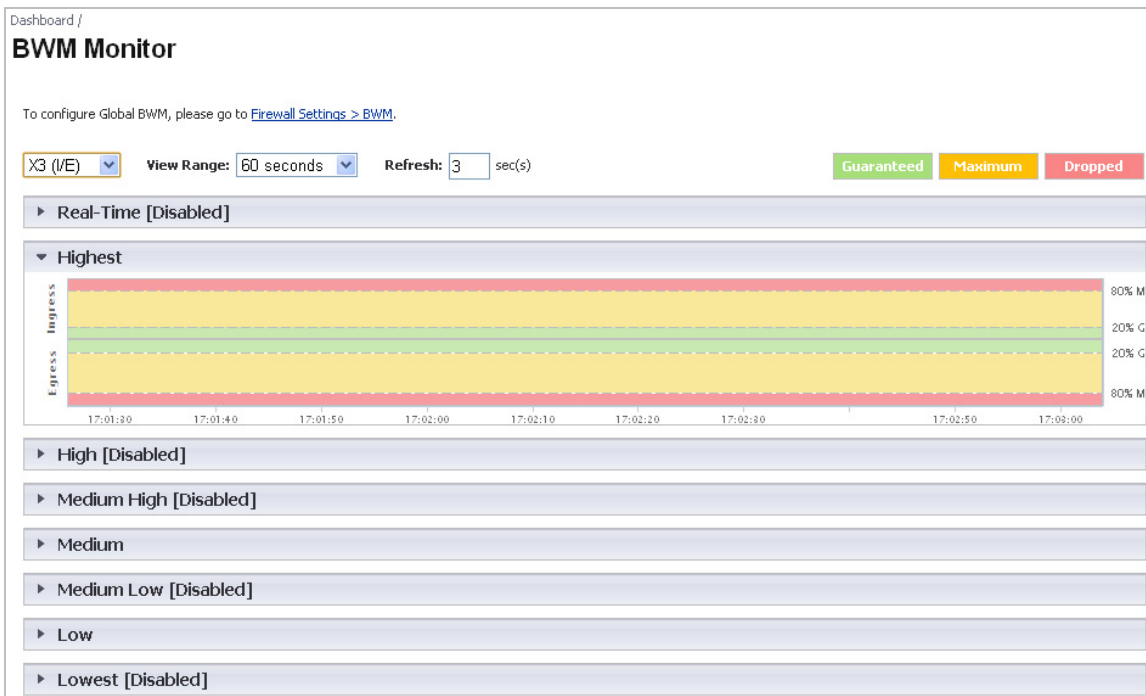


## Enhancements

SonicOS 5.8.1.4 includes several enhancements that involve changes to the SonicOS management interface. These changes are described in this section.

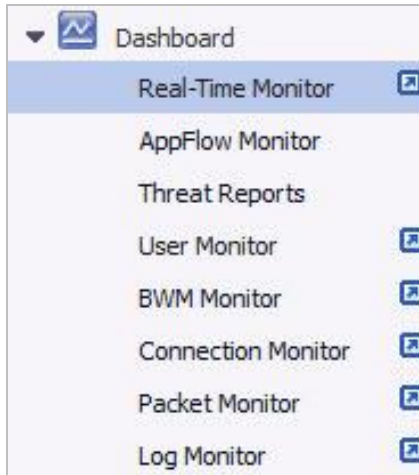
### *Dashboard Updates*

- **Bandwidth Management Monitor Page**—The new **Dashboard > 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.



# Release Notes

- **Pop-Up Visualization Dashboard Displays**— Several of the SonicWALL Visualization Dashboard pages now 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.



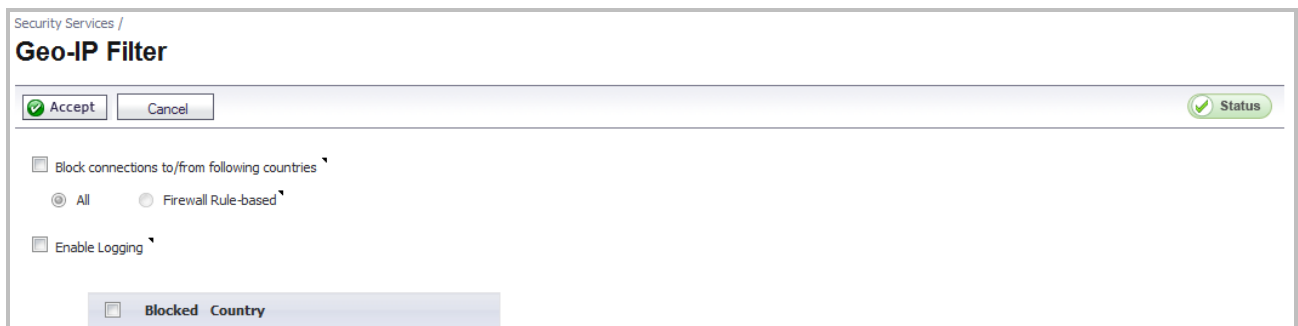
The pop-up button is also available at the top right of the individual dashboard pages, as shown below:



## Geo-IP and Botnet Filtering Updates

- **Geo-IP Filter**— The Geo-IP Filter feature is now on its own page in the management interface and is no longer shared with the Botnet Filter feature. The management interface has new features for the **Block Connections to/from Following Countries** checkbox and a new checkbox for **Enable Logging**.

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



# Release Notes

- **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 is now separate from the Geo-IP Filter page, offering configuration options for blocking all or firewall rule-based connections to/from Botnet Command and Control Services, enabling logging, Botnet exclusion objects, and checking Botnet server lookup.

Security Services /  
**Botnet Filter**

Accept  Cancel

Block connections to/from Botnet Command and Control Servers  
 All  Firewall Rule-based

Enable Logging

**Botnet Exclusion Object:**  
Default Geo-IP and Botnet Exclusion Group

**Check BOTNET Server Lookup**

DNS Server 1: 10.50.129.148  
DNS Server 2: 10.50.129.149  
DNS Server 3: 4.2.2.2  
Lookup IP:

## Log > Flow Reporting

- The Log > Flow Reporting page is updated to include new settings and information. The statistics at the top of the page show the same information, but are renamed for better clarity:

Log /  
**Flow Reporting**

External Flow Reporting Statistics		Internal AppFlow Reporting Statistics	
NetFlow/IPFIX Packets Sent:	1131943	Data Flows Enqueued:	1071483
Connection Flows Enqueued:	1079318	Data Flows Dequeued:	1071483
Connection Flows Dequeued:	1079313	Data Flows Dropped:	0
Connection Flows Dropped:	0	Data Flows Skipped Reporting:	0
Connection Flows Skipped Reporting:	0	General Flows Enqueued:	69
Non-Connection data Enqueued:	36	General Flows Dequeued:	69
Non-Connection data Dequeued:	69	General Flows Dropped:	0
Non-connection data Dropped:	0	General Static Flows Dequeued:	769617
Netflow/IPFIX Templates sent:	677677	AppFlow Collector Errors:	0
Non-connection related static data Reported:	8435157	Total Flows in DB:	24123

# Release Notes

- The **Settings** area is updated to provide a way to enable AppFlow to Local Collector and Real-Time Data Collection, as well as to allow the selection of data type for real-time collection. **External Collector Settings** are moved to their own area for better clarity.

The screenshot shows two configuration panels. The top panel, titled "Settings", includes a checkbox for "Enable AppFlow To Local Collector[\*]" which is checked, and another for "Enable Real-Time Data Collection" which is unchecked. Below these is a dropdown menu for "Collect Real-Time Data For" with the selection "Top apps, Bits per sec., Packets per sec., Average packet size, Connections per". The bottom panel, titled "External Collector Settings", includes a checked checkbox for "Send AppFlow and Real-Time Data To EXTERNAL Collector [\*]". It features several input fields: "External Flow Reporting Format" (dropdown: "IPFIX with extensions"), "External Collector's IP address" (text: "10.128.1.105"), "Source IP To Use Uor Collector On A VPN tunnel" (text: "0.0.0.0"), and "External Collector's UDP Port Number" (text: "2055"). There are also two checked checkboxes for "Send IPFIX/Netflow Templates At Regular Interval" and "Send Static AppFlow At Regular Interval". Below these are two dropdown menus: "Send Static AppFlow For Following Tables" (selection: "Location Map, Rating Map, Table Map, Column Map") and "Send Dynamic AppFlow For Following Tables" (selection: "Connections, Users, URLs, URL ratings, VPNs, Devices, SPAMs, VOIPs"). The final dropdown is "Include Following Additional Reports via IPFIX" (selection: "Top 10 Apps").

- Report Settings are split into two sections, one for **Connection Report Settings** with new options for reports about connections, and the other for **Other Report Settings** with additional new options including a way to specify URL types to include and an option to control the grouping of flows by domain or country.

The screenshot shows two configuration panels. The top panel, titled "Connection Report Settings", includes a radio button group for "Report Connections" with "Interface-based" selected. Below are checkboxes for "Report On Connection OPEN" (checked), "Report On Connection CLOSE" (checked), and "Report Connection On Active Timeout" (unchecked). There are two input fields: "Number Of Seconds" (text: "60") and "Report Connection On Kilo BYTES Exchanged" (text: "100"). There is also a checkbox for "Report ONCE" (unchecked) and a dropdown menu for "Report Connections On Following Updates" (selection: "threat detection, application detection, user detection, VPN tunnel detection"). The bottom panel, titled "Other Report Settings", includes a checked checkbox for "Report DROPPED Connection", an unchecked checkbox for "Skip Reporting STACK Connections", a dropdown menu for "Include Following URL Types" (selection: "Gifs, Jpegs, Pngs, Js, Xmls, Jsons, Css, Htmls, Aspx, Cms"), and a checked checkbox for "Enable Geo-IP And Domain Resolution". At the bottom of the panel, a note states: "[\*]: May need rebooting the device to completely disable/enable these features."

# Release Notes

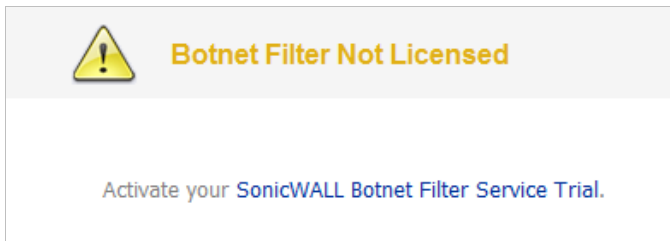
## Licensing Geo-IP and Botnet Filtering

The Geo-IP and Botnet Filter features are licensed services. The Geo-IP Filter is licensed along with other Security Services (Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, App Control, and App Visualization) in a Comprehensive Gateway Security Services (CGSS) license bundle, and renews / expires along with these services. Once the appliance is registered and licensed for Geo-IP, the country database is automatically downloaded.

### Botnet Filtering

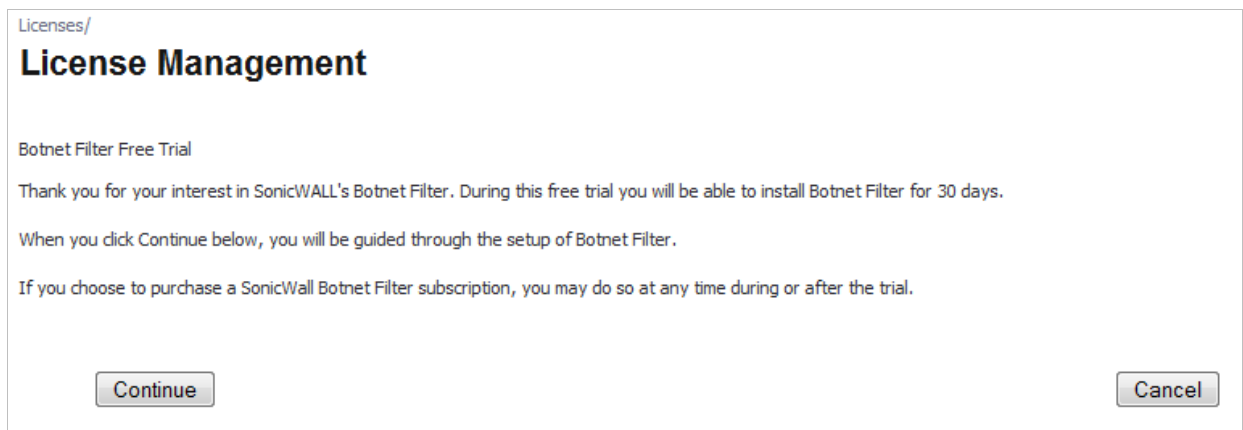
The Botnet Filtering feature is currently available on a free trial license basis. Perform the following steps to activate your Botnet Filter free trial:

1. Navigate to the **Security Services > Botnet Filter** page.



2. Click the **Activate your SonicWALL Botnet Filter Service Trial** link.
3. Enter your MySonicWALL.com **username** and **password**. This redirects you to the **Licenses > License Management** page.
4. Click the **Try** link in the Botnet Filter row.

The Botnet Filter Free Trial window displays:



5. Click the **Continue** button.



# Release Notes

## Geo-IP Filtering

Perform the following steps to activate Geo-IP Filtering:

1. Navigate to the **System > Licenses** page.

Comprehensive Gateway Security Suite Upgrade		<a href="#">Upgrade</a> <a href="#">Renew</a>
Gateway Anti-Virus, Anti-Spyware & Intrusion Prevention Service	Licensed	<a href="#">Renew</a>
Premium Content Filtering Service	Not Licensed	<a href="#">Try</a> <a href="#">Activate</a>
ViewPoint	Not Licensed	<a href="#">Try</a> <a href="#">Activate</a>

2. Activate the **CGSS** license bundle.
3. Register your appliance.
4. Navigate to the **Security Services > Geo-IP** page. A green status icon displays, confirming the Geo-IP Filter is licensed and ready to use.

The screenshot shows the 'Geo-IP Filter' configuration page. At the top, there are 'Accept' and 'Cancel' buttons, and a 'Status' button with a green checkmark. Below this, there are several checkboxes: 'Block connections to/from following countries', 'Block connections to/from following domains', and 'Enable Logging'. A large green message box is overlaid on the page, stating 'Country Database: Downloaded' and 'Geo Enforcement Available' with a green checkmark. A 'close' button is visible in the top right corner of the message box.

# Release Notes

## Known Issues

This section contains a list of known issues in the SonicOS 5.8.1.4 release.

### Application Control

Symptom	Condition / Workaround	Issue
App Control advanced signatures are applied to traffic from and to the VPN zone, rather than the WAN zone only.	Occurs when enabling the App Control service on the WAN zone, and then enabling the logging or blocking action for any signature. After traffic is generated from the LAN to the VPN, the App control signatures are applied to VPN traffic.	107296
App rules remain in effect even when disabled globally.	Occurs when the Enable App Rules checkbox is cleared to disable these policies globally, then an app rule is created. When traffic on the WAN interface matches the rule, the configured policy action is applied.	101194
Related traffic configured in an application rule is blocked even though the <b>Enable App Rules</b> checkbox is not selected.	Occurs when an application rule is created using Create Rule on the App Flow Monitor page and the Enable App Rules checkbox is not selected, which is the factory default setting. The app rule is created and functions properly, even though the <b>Enable App Rules</b> checkbox is disabled.	100120

### Bandwidth Management

Symptom	Condition / Workaround	Issue
Traffic is dropped when the ingress or egress values for an interface are modified and traffic is passing through that interface.	Occurs when modifying the ingress or egress interface values while the interface is passing traffic. <b>Workaround:</b> Stop traffic on the interface, and then modify the values.	101286
Bandwidth management application rules are sometimes mapped to the wrong global BWM priority queue.	Occurs when creating a bandwidth management rule on the <b>App Flow Monitor</b> page and setting the priority to <b>High</b> . The <b>App Flow Monitor</b> page displays the created rule with a <b>Medium</b> priority setting, even though <b>High</b> was selected.	100116

### Module

Symptom	Condition / Workaround	Issue
The LAN Bypass module's Bypass Status LED indicates that bypass mode is active during the boot process, then changes to the normal mode in which bypass is ready, but not active.	Occurs when configuring an SFP module in Layer 2 Bridge Mode, then replacing it with a LAN Bypass module.	108416

### Networking

Symptom	Condition / Workaround	Issue
Configuring more than one remote appliance with a tunnel interface and OSPF could result in dropped routes.	Occurs when an additional remote appliance is configured with a tunnel interface and OSPF is enabled.	102961

# Release Notes

## System

Symptom	Condition / Workaround	Issue
After importing preferences from another appliance model, the X5 interface is configured with the same IP address as the W0 interface.	Occurs when importing preferences from a SonicWALL TZ 200W or TZ 100W to a SonicWALL NSA 220W.	110699 110697
The MO/M1 status LED does not indicate the presence of a module.	Occurs when inserting a module into the appliance and booting the system. The MO/M1 status LED should be on when a valid module is detected in the slot and blink if a module is present but not supported.	107620
The system preferences do not import correctly. The LAN IP address is changed to 192.168.168.168 and the user cannot log in.	Occurs when importing preferences from a TZ 200 appliance into a NSA 250M appliance, then performing a restart.	107209

## ViewPoint

Symptom	Condition / Workaround	Issue
The ViewPoint service appears to be available for activation and free trial on the System > Licenses page, although it is no longer supported.	Occurs when the appliance is running SonicOS 5.8.1.4, which does not support ViewPoint because ViewPoint is being replaced with a new reporting service.	110425

## Visualization

Symptom	Condition / Workaround	Issue
The NetFlow EndTime timestamp results in 0.00000 for valid and allowed TCP packets.	Occurs when the NetFlow collector's logging is enabled on Applicable Interfaces and Rules, and TCP traffic is sent to the allowed destination. Upon checking the packet capture details, the EndTime timestamp displays as 0.00000.	102961

## VPN

Symptom	Condition / Workaround	Issue
Sometimes, the secondary IPSec gateway is unable to establish a tunnel with a peer if the primary gateway is unreachable.	Occurs when there are two SonicWALL devices with VPN configured and the cable from the secondary gateway is unplugged.	103935
Having multiple tunnel interface policies with the same IPSec gateway but different ports configured on the firewall can cause only one tunnel to be active.	Occurs when there are two or more tunnel interface policies using the same IPSec gateway and those interfaces are bound to different ports.	103398

# Release Notes

## Resolved Issues

This section contains a list of resolved issues in the SonicOS 5.8.1.4 release.

### Bandwidth Management

Symptom	Condition / Workaround	Issue
The ingress/egress rate per interface is not accurately controlled by the bandwidth management settings.	Occurs when Global BWM is enabled and 400 Mbps of UDP traffic (1518 bytes) is passing from the X5 (DMZ) interface to X0 (LAN). With no BWM rate configured on X5, the received rate on X0 is the full 400 Mbps. When a 200, 300, or 400 Mbps ingress rate is configured on X5, the received rate on X0 is 135, 140, or 146 Mbps.	108199

### Content Filtering System

Symptom	Condition / Workaround	Issue
The SonicWALL CFS block page does not display when a blocked page is accessed, but the user sees a "page cannot be displayed" message instead.	Occurs when users are connecting via Layer 2 Tunneling Protocol and the L2TP server is configured in route-all mode, and a user browses to a website that is blocked by the CFS policy.	92539

### Dashboard

Symptom	Condition / Workaround	Issue
The NSA 250 M Wireless-N security appliance M0:E1T10 interface ingress / egress bandwidth does not display on the Real-Time Monitor page.	Occurs when passing traffic through the M0:E1T10 interface, and then viewing the Real-Time Monitor page.	109751
The Bandwidth Management icon does not display anything after clicking it.	Occurs when navigating to the <b>Firewall Settings &gt; BWM</b> page, then clicking the BWM icon.	109663
Changing the View Style, Vertical Access, or Show options on the <b>Dashboard &gt; Use Monitor</b> page does not work.	Occurs when navigating to <b>Dashboard &gt; Use Monitor</b> , then clicking the icon next to <b>Use Monitor</b> . A separate Dashboard > Use Monitor tab is displayed in the browser. Changing the View Style, Vertical Axis, or Show options does not work. Refresh the browser page and the options still do not work.	109634

# Release Notes

## Firmware

Symptom	Condition / Workaround	Issue
An iPad client fails to connect to the L2TP server if MSCHAPv2 authentication is set as the first order authentication method.	Occurs when GroupVPN is enabled and configured for an L2TP. The iPad can successfully connect if PAP authentication is set as the first order authentication method, but fails if MSCHAPv2 is preferred. A Windows XP client can successfully connect using MSCHAPv2. <b>Workaround:</b> Move MSCHAPv2 to the bottom of the authentication protocol list (by clicking on the Down Arrow button).	106801
The Geo-IP and Botnet Exclusion Objects do not take effect, causing DNS query packets to be incorrectly dropped.	Occurs when enabling the checkbox for <b>Block All Connections to/from Following Countries</b> , selecting all countries, and entering DNS Servers into the <b>Exclusion Object</b> . When a web page is accessed and the packet monitor is used to capture packets, you can see that all DNS query packets are dropped by the Geo-IP filter.	100010

## Log

Symptom	Condition / Workaround	Issue
Syslog messages are sent with a source IP address of 0.0.0.0 out the wrong interface.	Occurs when attempting to send syslog messages to an internal Viewpoint server, but they are sent out the WAN interface with the source IP of 0.0.0.0 instead.	106271

## Module

Symptom	Condition / Workaround	Issue
The LAN bypass primary interface displays incorrectly in the management interface.	Occurs when configuring the LAN M0:X0 interface and M0:X1 interface in Layer 2 Bridge Mode, and then enabling the Bypass feature. View the X1 management interface and see that it is displayed incorrectly.	107713

# Release Notes

## Networking

Symptom	Condition / Workaround	Issue
SonicOS drops fragmented packets when Kerberos authentication is based on UDP.	Occurs when the firewall is configured in Routed Mode between a Cisco MPLS Router and the LAN at the remote locations and LAN users are trying to access remote computers over the MPLS link with Kerberos authentication. The SonicWALL drops the fragmented return traffic from the Cisco MPLS router.	108049
Link status does not match the configured link speed and duplex settings on the SonicWALL appliance.	Occurs when the SonicWALL is connected to a peer device such as a third-party switch, and the link speed and duplex settings are manually set on both sides, rather than being auto-negotiated.	105576
The Dynamic DNS agent does not automatically update dynamic DNS records, although the new IP address is reflected in the online status and the WAN interface IP address.	Occurs when using a DynDNS.com free account with a TTL set to 60 seconds, and the Dynamic DNS profile is added to the firewall and bound to the WAN interface using DSL/PPPoE and service type Dynamic, and then renewal of the dynamic WAN IP address is triggered by disconnecting and reconnecting the WAN PPPoE interface, by restarting, or by upgrading the firewall.	104539
The information displayed by the MIB Browser on a SNMPc server is not accurate for the interfaces of the connected SonicWALL appliance.	Occurs when an SNMPc server is connected to the secondary WAN interface on a SonicWALL NSA appliance and configured with read/write access using SNMPv2. SNMP management is enabled on the connected interface.	89533

## SSL VPN

Symptom	Condition / Workaround	Issue
Logging into the SSL VPN portal from the WAN or WLAN zone of the NSA 250M security appliance does not work.	Occurs when the SSL VPN service and HTTPS management/user logins are enabled on the WAN and WLAN zones, and a typical "Route All" VPN NAT Policy is configured on the firewall with Original Source = Any, rather than specifying the source, such as Original Source = SSLVPN IP Pool.	109737

## System

Symptom	Condition / Workaround	Issue
Automatic adjustment for daylight savings time does not occur for Australian time zones.	Occurs when the SonicWALL appliance is set to use the Sydney/Melbourne (GMT +10:00) time zone and the "Automatically adjust clock for daylight saving time" checkbox is selected, and then the date of the time change arrives.	95748

# Release Notes

## **Users**

Symptom	Condition / Workaround	Issue
The NT LAN Manager (NTLM) cannot be enabled until RADIUS is enabled, but RADIUS cannot be enabled until NTLM is enabled.	Occurs when setting the authentication method to LDAP, the single-sign-on method to SSO Agent, and then enabling NTLM and RADIUS.	109247

## **User Interface**

Symptom	Condition / Workaround	Issue
HTTP(S) management login or user login on the LAN is not possible and an error message is displayed: "Sorry, but either the maximum number of users are already logged in, or too many users are simultaneously trying to log in. Try again shortly or contact your firewall administrator." Login via SSH is still possible.	Occurs when more than 210 HTTP(S) connections to the appliance are opened, but then stop in the middle of the connection process, possibly to wait for something from the browser.	100106

## **VoIP**

Symptom	Condition / Workaround	Issue
Inbound SIP audio cannot be heard after answering a call placed on hold.	Occurs when the existing SIP media connection being re-used, rather than re-negotiated, after coming off hold.	108339

# Release Notes

## VPN

Symptom	Condition / Workaround	Issue
A misconfigured VPN policy allows a phase 2 tunnel to be established instead of logging an error for the mismatched proposal.	Occurs when two VPN policies are configured on the local firewall and one VPN policy is configured on the remote firewall to match one of the local policies. When the remote firewall starts the tunnel negotiation, it establishes phase 1 to the matching policy, but if the phase 2 proposal matches the other policy, it establishes a tunnel with that policy rather than logging an error for the mismatched proposal.	107806
The Layer 2 Tunneling Protocol (L2TP) allows iOS / MAC users to connect without authentication (only using a pre-shared key).	Occurs when enabling the RSA SecureID option, then authenticating with an invalid username and a pre-shared key. The firewall should require proper authentication and not allow remote clients which have RSA SecureID enabled to connect to L2TP with only the pre-shared key.	107803
A user on a remote DHCP client machine cannot connect to the central firewall using HTTP.	Occurs when the remote and central gateways are configured to allow the remote network to obtain IP addresses via DHCP through the VPN tunnel, which automatically adds access rules on the central gateway. After these access rules are edited via the Firewall > Access Rules page to set the Users Allowed field to Everyone, and the IP address is renewed for the DHCP client on the remote network, the user cannot connect from that client machine.	107637
DHCP (unicast) packets are dropped on the central gateway as IP spoofed packets.	Occurs when IP Helper is enabled on the remote site in the DHCP policy, and the DHCP server is enabled on the central site, and IP Helper sends DHCP relay packets over the VPN tunnel interface.	105924

## WAN Acceleration

Symptom	Condition / Workaround	Issue
The TCP Acceleration Service Object configuration is lost after rebooting the SonicWALL WXA. The field is reverted back to the default value of "HTTP" after the reboot.	Occurs when the TCP Acceleration Service Object field on the WAN Acceleration > TCP Acceleration configuration page in SonicOS is set to a non-default value, the configuration is saved, and then the WXA appliance is rebooted.	108197
SonicOS retains the previous IP address for a SonicWALL WXA even after the WXA appliance is replaced by another one.	Occurs when a SonicWALL WXA is connected to the SonicWALL firewall and is configured to use a static DHCP lease for the IP address, and then the WXA appliance is replaced by another WXA.	107384

## Wireless

Symptom	Condition / Workaround	Issue
After being redirected to the Policy page and clicking <b>Accept</b> , the Android device's stock browser displays a browser error message, but the user can still access the Internet.	Occurs when enabling the guest service's <b>Policy Page Without Authentication</b> feature, clicking <b>Accept</b> on the Policy page, and then connecting to the web using the Android's stock browser.	108398



# Release Notes

## Upgrading SonicOS Image Procedures

---

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

<i>Obtaining the Latest SonicOS Image Version.....</i>	<i>17</i>
<i>Saving a Backup Copy of Your Configuration Preferences.....</i>	<i>17</i>
<i>Upgrading a SonicOS Image with Current Preferences.....</i>	<i>18</i>
<i>Importing Preferences to SonicOS 5.8.....</i>	<i>18</i>
<i>Importing Preferences from SonicOS Standard to SonicOS 5.8 Enhanced.....</i>	<i>19</i>
<i>Support Matrix for Importing Preferences.....</i>	<i>20</i>
<i>Upgrading a SonicOS Image with Factory Defaults.....</i>	<i>21</i>
<i>Using SafeMode to Upgrade Firmware.....</i>	<i>21</i>

### **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. Copy the new SonicOS image file to a directory on your management station.

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.

### **Saving a Backup Copy of Your Configuration Preferences**

Before beginning the update process, make a system backup of your SonicWALL security appliance configuration settings. The backup feature saves a copy of your current configuration settings on your SonicWALL security appliance, protecting all your existing settings in the event that it becomes necessary to return to a previous configuration state.

In addition to using the backup feature to save your current configuration settings to the SonicWALL security appliance, you can export the configuration preferences file to a directory on your local management station. This file serves as an external backup of the configuration preferences, and can be imported back into the SonicWALL security appliance.

Perform the following steps to save a backup of your configuration settings and export them to a file on your local management station:

1. On the System > Settings page, click **Create Backup**. Your configuration preferences are saved. The System Backup entry is displayed in the Firmware Management table.
2. To export your settings to a local file, click **Export Settings**. A popup window displays the name of the saved file.

# Release Notes

## ***Upgrading a SonicOS Image with Current Preferences***

Perform the following steps to upload new firmware to your SonicWALL appliance and use your current configuration settings upon startup:

1. Download the SonicOS firmware image file from [mysonicwall.com](http://mysonicwall.com) and save it to a location on your local computer.
2. On the System > Settings page, click **Upload New Firmware**.
3. Browse to the location where you saved the SonicOS firmware image file, select the file, and click **Upload**.
4. On the System > Settings page, click the **Boot** icon in the row for **Uploaded Firmware**.
5. In the confirmation dialog box, click **OK**. The SonicWALL restarts and then displays the login page.
6. Enter your user name and password. Your new SonicOS image version information is listed on the **System > Settings** page.

## ***Importing Preferences to SonicOS 5.8***

Preferences importing to the SonicWALL UTM appliances is generally supported from the following SonicWALL appliances running SonicOS:

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

There are certain exceptions to preferences importing on these appliances running the SonicOS 5.8 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.

# Release Notes

## **Importing Preferences from SonicOS Standard to SonicOS 5.8 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 will retain 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.

# Release Notes

## Support Matrix for Importing Preferences

		DESTINATION FIREWALLS																																				
		TZ100/	TZ100w/																	PRO	PRO	PRO	PRO	PRO	PRO	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA
		TZ200	TZ200w	TZ210	TZ210w	TZ170	TZ170w	TZ170SP	TZ170SPw	TZ180	TZ180w	TZ190	TZ190w	1260	2040	3060	4060	4100	5060	220	220W	240	250M	250MW	2400	3500	4500	5000	E5500	E6500	E7500	E8500	E8510					
S	TZ100/TZ200	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗		
O	TZ100w/TZ200w	C	✓	C	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗		
U	TZ 210	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗		
R	TZ 210W	✓	✓	C	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗		
C	TZ 170	B,D	B,D	B,D	B,D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
E	TZ 170W	B,C,D	B,D	B,C,D	B,D	C	✓	✓	✓	C	✓	C	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	TZ 170SP	B,C,D	B,C,D	B,C,D	B,D	C	C	✓	✓	C	C	C	✓	C	C	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	
F	TZ 170SPW	C,D	B,C,D	B,C,D	B,D	C	C	C	✓	C	C	C	✓	C	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	
I	TZ 180	C,D	C,D	C,D	C,D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
R	TZ 180W	C,D	C,D	C,D	C,D	C	✓	✓	✓	C	✓	C	✓	C	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
E	TZ 190	C,D	C,D	C,D	C,D	C	C	✓	✓	C	C	✓	✓	C	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
W	TZ 190W	C,D	C,D	C,D	C,D	C	✓	✓	✓	C	✓	C	✓	C	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
A	PRO 1260	B,D	B,D	B,D	B,D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
L	PRO 2040	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	
L	PRO 3060	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
S	PRO 4060	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	PRO 4100	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	PRO 5060	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	NSA 220	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	NSA 220W	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	NSA 240	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	NSA 250M	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	NSA 250MW	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	NSA 2400	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	NSA 3500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	NSA 4500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	NSA 5000	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	NSA E5500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	NSA E6500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	NSA E7500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	NSA E8500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	NSA E8510	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

Notes:

- A - When VLANs are present, the settings file will not be accepted.
- 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.

✓	Supported
✗	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.



# Release Notes

## Upgrading a SonicOS Image with Factory Defaults

Perform the following steps to upload new firmware to your 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. On the System > Settings page, click **Create Backup**.
3. 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 SonicWALL restarts and then displays the Setup Wizard, with a link to the login page.
7. Enter the default user name and password (admin / password) to access the SonicWALL management interface.

## Using SafeMode to Upgrade Firmware



The SafeMode procedure uses a reset button in a small pinhole, whose 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 cord on the back. If you are unable to connect to the SonicWALL security appliance's management interface, you can restart the 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.

To use SafeMode to upgrade firmware on the SonicWALL security appliance, perform the following steps:

1. Connect your computer to the X0 port on the SonicWALL appliance and configure your IP address with an 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 front of the security appliance for more than 20 seconds.
  - Use the LCD control buttons on the front bezel to set the appliance to Safe Mode. Once selected, the LCD displays a confirmation prompt. Select **Y** and press the **Right** button to confirm. The SonicWALL security appliance changes to SafeMode.

The **Test** light starts blinking when the SonicWALL security 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 Web browser on your computer to **192.168.168.168**. The SafeMode management interface displays.
4. If you have made any configuration changes to the security appliance, select the **Create Backup On Next Boot** checkbox to make a backup copy of your current settings. Your settings will be saved when the appliance restarts.
5. Click **Upload New Firmware**, and then browse to the location where you saved the SonicOS firmware image, select the file, and click **Upload**.
6. Select 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 Defaults – New!**   
Use this option to restart the appliance with default configuration settings.
7. In the confirmation dialog box, click **OK** to proceed.
8. 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 SonicWALL management interface.

# Release Notes

## Related Technical Documentation

SonicWALL user guides and reference documentation is available at the SonicWALL Technical Documentation Online Library: <http://www.sonicwall.com/us/Support.html>

For basic and advanced deployment examples, refer to SonicOS Guides and SonicOS TechNotes available on the Website.

The screenshot shows the SonicWALL Support website. The top navigation bar includes the SonicWALL logo, links for Products, Solutions, How to Buy, Support, and Sign In/Register, and a search box. A left sidebar menu lists various support resources. The main content area features a 'Support for SonicWALL® Products and Services' header, a 'Service Bulletins' section with a recent entry about vulnerabilities, a 'Knowledge Base Search' section with a search input and button, and a row of service icons for Network Security, SSL VPN, Email Security, Backup & Recovery, Endpoint Security, and Management & Reporting. Below these are sections for 'Top Support Topics' (a list of articles) and 'Recent Video Tutorials' (a video player for 'How to Configure Standard Ports on a SonicWALL Firewall').

Last updated: 12/21/2011