Release Notes

SonicOS

SonicOS Standard 3.1.6.6 Release Notes

Contents

Platform Compatibility

SonicOS Standard version 3.1.6.6 is a supported release for the following platforms:

- SonicWALL TZ 150 Series
- SonicWALL TZ 170
- SonicWALL TZ 170 SP
- SonicWALL TZ 170 Wireless
- SonicWALL PRO 1260
- SonicWALL PRO 2040
- SonicWALL PRO 3060

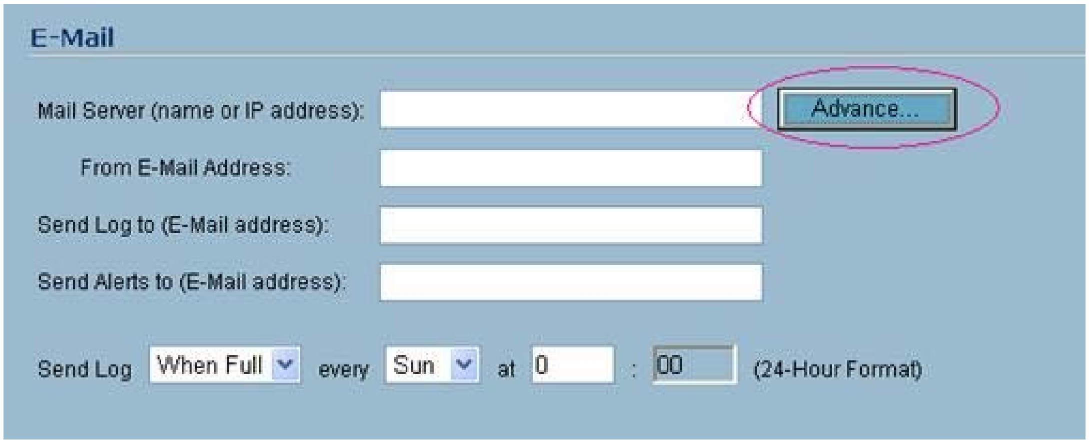
Key Features in SonicOS Standard 3.1.6.6

SonicOS Standard 3.1 Feature Highlights

The following list provides feature highlights:

- **Anti-Spyware**—Analyzes inbound connections for ActiveX-based component installations, the most common method of spyware delivery. It also examines inbound setup executables and cabinet files crossing the gateway, and resets the connections that are streaming spyware setup files to the LAN. If spyware was installed on a LAN workstation prior to SonicWALL Anti-Spyware activation, the service examines outbound traffic for streams originating at spyware infected clients and resets those connections. The SonicWALL Anti-Spyware Service provides the following protection:
    - Blocks spyware delivered through auto-installed ActiveX components, the most common vehicle for distributing malicious spyware programs.
    - Scans and logs spyware threats that are transmitted through the network and alerts administrators when new spyware is detected and/or blocked.
    - Stops existing spyware programs from communicating in the background with servers on the Internet, preventing the transfer of confidential information.
    - Provides granular control over networked applications by enabling administrators to selectively permit or deny the installation of spyware programs.
    - Prevents e-mailed spyware threats by scanning and then blocking infected e-mails transmitted either through SMTP, IMAP or Web-based e-mail.
    - Works with other anti-spyware programs, such as applications that remove existing spyware applications from hosts, to provide an added measure of defense against spyware.

- **Connection Limitation**—Gives the administrator the ability to place a limit on the number of connections client computers on a LAN can open up. This limit is set by defining a maximum quota on the source IP or destination IP numbers passing through the firewall. This feature mitigates the impact of worms by preventing them from overloading the firewall through opening an excessive number of connections.
- **Mail Authentication**— Implements an extension to the SMTP protocol.
    - The SMTP service extension [ESMTP] focuses on authentication. It requires an SMTP client to authenticate itself to the server. Authentication is accomplished by username and password exchange, and optional negotiation of a security layer for subsequent protocol interactions.
    - Customers can now configure the port to use when exporting local firewall logs over SMTP, rather than always using port 25. Note that port 25 must still be used when an SMTP-based email is initiated from a host on the LAN and passes through the firewall to the destination. The SMTP server can authenticate the log transaction over PLAIN as well as LOGIN protocols.
    - SMTP settings can be configured on the Log > Automation page, by clicking on the **Advance** button. The log email setting supports changing the SMTP port, as well as setting credentials for Mail Authentication.



E-Mail

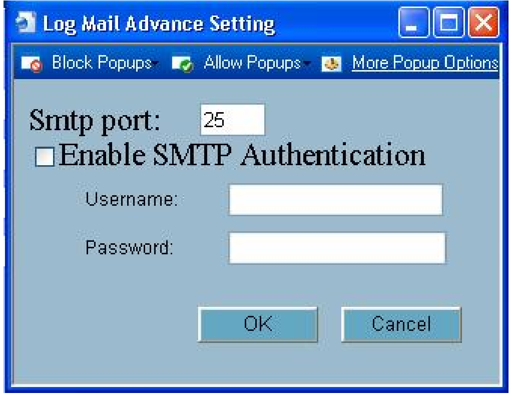
Mail Server (name or IP address):

From E-Mail Address:

Send Log to (E-Mail address):

Send Alerts to (E-Mail address):

Send Log When Full every Sun at 0 : 00 (24-Hour Format)



Log Mail Advance Setting

Smtp port: 25

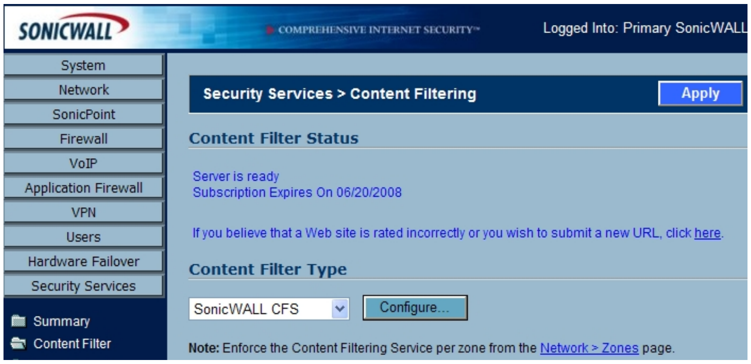
□Enable SMTP Authentication

Username:

Password:

- **HTTPS Filtering— HTTPS Filtering** – SonicOS Standard 3.1.6.6 uses HTTPS Filtering to allow administrators to control user access to Web sites when using the encrypted HTTPS protocol. HTTPS Filtering is based on the ratings of Web sites, such as Gambling, Online Banking, Online Brokerage and Trading, Shopping, and Hacking/Proxy Avoidance.

  Note: HTTPS Filtering is IP-based, so IP addresses must be used rather than domain names in the Allowed or Forbidden lists. You can use the **nslookup** command in a DOS cmd window to convert a domain name to its IP address(es). There may be more than one IP address associated with a domain, and if so, all must be added to the Allowed or Forbidden list.



Security Services > Content Filtering

Content Filter Status

Server is ready
Subscription Expires On 06/20/2008

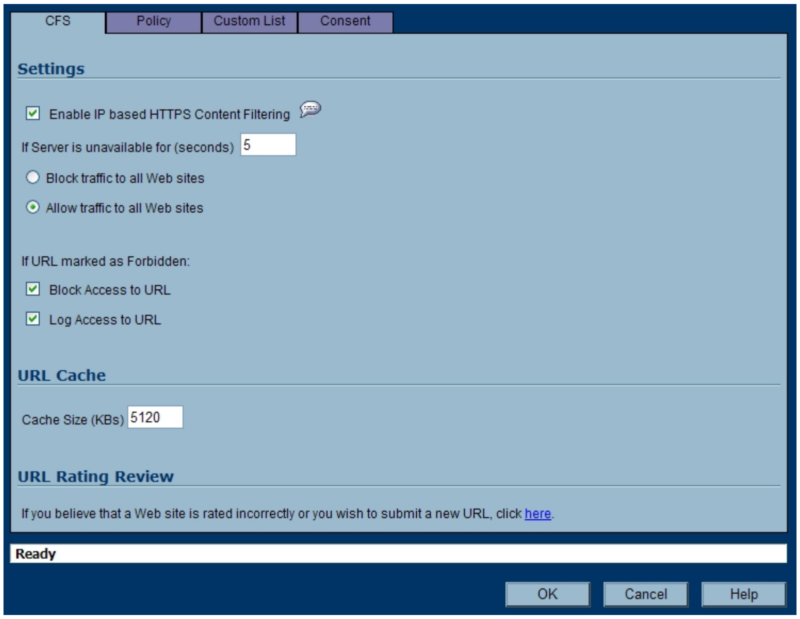
If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click here.

Content Filter Type

SonicWALL CFS

Note: Enforce the Content Filtering Service per zone from the Network > Zones page.

  Press the **Configure** button to display the following screen where you can enable IP based HTTPS content filtering:



Settings

☑ Enable IP based HTTPS Content Filtering

If Server is unavailable for (seconds) 5

○ Block traffic to all Web sites

● Allow traffic to all Web sites

If URL marked as Forbidden:

☑ Block Access to URL

☑ Log Access to URL

URL Cache

Cache Size (KBs) 5120

URL Rating Review

If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click here.

Ready

- **New SonicOS Settings** — SonicOS Standard 3.1.6.6 supports the following “Tivo Services” Service Group:
  - TCP 2190: “Tivo TCP Beacon”
  - UDP 2190: “Tivo UDP Beacon”
  - TCP 8080-8089: “Tivo TCP Data”
  - TCP 8101-8102, 8200 “Tivo TCP Desktop”

Known Issues

This section contains a list of known issues in the SonicOS Standard 3.1.6.6 release.

Networking

Symptom	Condition / Workaround	Issue
Management of a SonicWALL security appliance from the WAN side is possible only by using HTTPS.	A network access rule allowing HTTP management from the WAN is configurable, but the administrator will not be able to log in to the SonicWALL security appliance.	34022

Security Services

Symptom	Condition / Workaround	Issue
Only Microsoft Outlook Express client implementation of Internet Message Access Protocol (IMAP) supported.	Occurs when specifying the IMAP option on 'Security Services' > 'Gateway Anti-Virus' only supports scanning of the Microsoft Outlook Express client implementation of IMAP.	34617
Gateway Anti-Virus fails to detect a virus transmitted through a VPN tunnel.	Occurs when running SonicOS Standard 3.0 with Gateway Anti-Virus enabled, by default Gateway Anti-Virus does not detect the virus through a VPN tunnel. **Workaround**: Enable NAT and firewall rules.	34503
Intrusion Prevention Service classifies IM, P2P as Multimedia traffic as Low Priority Attacks.	Occurs when prevention is enabled for all Low Priority Attacks, certain types of valid traffic will be blocked, such as Instant Messenger (IM) protocols, and other protocols such as Apple iChat. This is by design. **Workaround**: To stop detecting or preventing these 'valid' traffic types, disable Detection, Prevention, or both for the IM, P2P, and Multimedia categories.	34460

Users

Symptom	Condition / Workaround	Issue
URLs that can bypass ULA in rules will not work with a proxy Web server.	URLs that can bypass ULA in rules only work for traffic to the default HTTP port 80. **Workaround**: If the SonicWALL security appliance is configured to use an external proxy server and ULA is enforced and configured with some URLs to bypass this ULA in your network access rules, the Proxy server should be configured on the default port number 80.	34310

VPN

Symptom	Condition / Workaround	Issue
The SonicWALL security appliance does not propose static routes to GVC.	Single-arm mode deployments: Enable SonicWALL security appliances to be deployed downstream from an edge routing device or aggregation switch.	36185
When management from the Central Gateway's LAN is attempted, the Remote Gateway prints the log message: Incompatible IPSec Security Association.	The Remote Gateway log message includes a source IP address of the host on the Central Gateway's LAN and a destination – the Relay IP address.	35100
If you try to use Dynamic DNS to update the DYN record for a dynamic IP client and you are using the hostname to establish a VPN tunnel to another SonicWALL security appliance, the VPN connection drops and will not be able to be reestablished.	Pushing all traffic through a VPN from a dynamic IP to a static IP causes this problem.	34987

Resolved Issues

The following issue is resolved in the SonicOS 3.1.6.6 release.

Symptom	Condition / Workaround	Issue
SonicOS management SessionID brute force vulnerability when attempted from the same source IP as a legitimate administrator's active management session.	Occurs when the brute force attacker finds the legitimate SessionID, which is valid for use only from the source IP of the legitimate administrator during an active session, from one of 4,294,967,296 possible SessionIDs (a session is active between the time legitimate administrator logs on and off). The SessionID security enhancement requires the attacker to guess the legitimate SessionID from one of 340,282,366,920,938,463,463,374,607,431,768,211,456 possible SessionIDs, and therefore requiring an attack on an active administrative session, from the same source IP of the administrator, to last 2,697,570,767,701,495,615,277,217,349,632 years. Please see this document for further analysis: SonicWALL Analysis of PenTest Vulnerability Reports	108138

This section describes an issue resolved in the SonicOS Standard 3.1.6.5 release.

Networking

Symptom	Condition / Workaround	Issue
The connection to License Manager fails and the following error message is displayed: "Connection Failure - SSL negotiation with the license manager server has failed. This could be caused by an incorrect date/time setting on your firewall." This impacts product registration, service activations, license updates, and signature downloads.	Occurs when the SonicWALL License Manager passes a 2048-bit keyed Verisign certificate while the admin is attempting to manage licenses on the SonicWALL appliance.	98228

Upgrading SonicOS Standard/Enhanced Image Procedures

The following procedures are for upgrading an existing SonicOS Standard or SonicOS Enhanced image to a newer version.

Obtaining the Latest SonicOS Standard/Enhanced Image Version

1. To obtain a new SonicOS Standard/Enhanced image file for your SonicWALL security appliance, connect to your mySonicWALL.com account at <http://www.mysonicwall.com>.

   Note: *If you have already registered your SonicWALL security appliance, and you selected **Notify me when new firmware is available** on the **System > Settings** page, you are automatically notified of any updates available for your model.*

2. Copy the new SonicOS Standard/Enhanced image file to a directory on your management station.

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

Upgrading a SonicOS Standard Image to SonicOS Enhanced Image

SonicOS Enhanced is available as an upgrade for the following SonicWALL security appliances running SonicOS Standard:

- SonicWALL TZ 150
- SonicWALL TZ 150 Wireless
- SonicWALL TZ 170
- SonicWALL TZ 170 SP
- SonicWALL TZ 170 Wireless
- SonicWALL PRO 1260
- SonicWALL PRO 2040
- SonicWALL PRO 3060

Note: *Refer to the Upgrading SonicOS Standard to SonicOS Enhanced document for complete upgrade procedures, available on the SonicWALL documentation Web site: <http://www.sonicwall.com/us/support/2134_3372.html >.*

⚠ **Alert**: You must use **Uploaded Firmware with Factory Defaults – New!** when upgrading from SonicOS Standard to SonicOS Enhanced and then manually reconfigure all settings on the SonicWALL security appliance. The **Uploaded Firmware – New!** will use the current SonicOS Standard configuration preferences, which are not compatible with SonicOS Enhanced. This also prohibits performing a remote upgrade to SonicOS Enhanced.

Saving a Backup Copy of Your Configuration Preferences

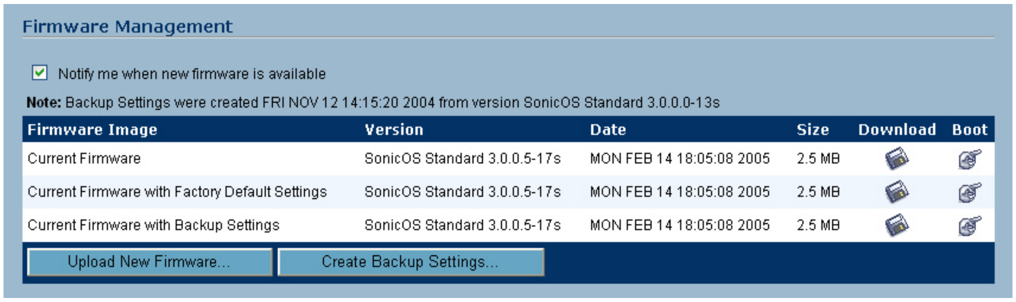
Before beginning the update process, make a system backup of your SonicWALL security appliance configuration settings. The backup feature saves a copy of your current configuration settings on your SonicWALL security appliance, protecting all your existing settings in the event it becomes necessary to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

In addition to using the backup feature to save your current configuration state 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 procedures to save a backup of your configuration settings and export them to a file on your local management station:

1. Depending on the SonicWALL security appliance model you are using, perform one of the following procedures:

   - If you are using a **SonicWALL TZ 150**, **SonicWALL TZ 150 Wireless**, **SonicWALL TZ 170**, **SonicWALL TZ 170 SP**, **SonicWALL TZ 170 Wireless**, or **SonicWALL PRO 1260**, click the **Create Backup Settings** button on the **System > Settings** page. Your configuration preferences are saved. The last backup settings information is displayed in the **Note** area above the **Firmware Management** table on the **System > Settings** page.



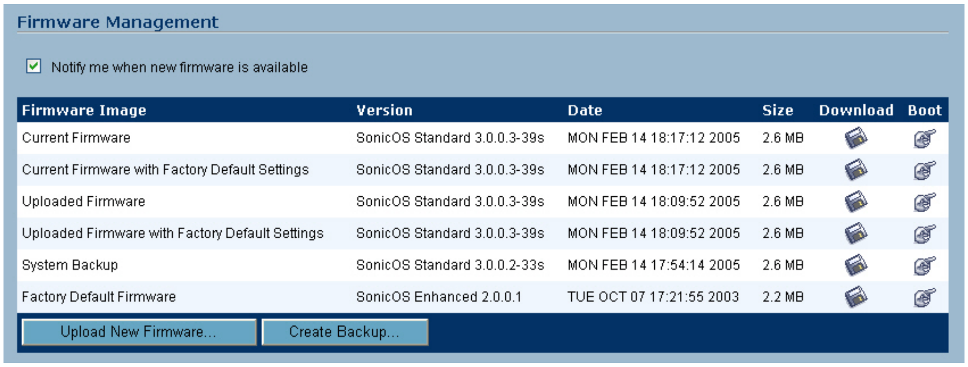
Firmware Management

☑ Notify me when new firmware is available

Note: Backup Settings were created FRI NOV 12 14:15:20 2004 from version SonicOS Standard 3.0.0.0-13s

Firmware Image	Version	Date	Size	Download	Boot
Current Firmware	SonicOS Standard 3.0.0.5-17s	MON FEB 14 18:05:08 2005	2.5 MB		
Current Firmware with Factory Default Settings	SonicOS Standard 3.0.0.5-17s	MON FEB 14 18:05:08 2005	2.5 MB		
Current Firmware with Backup Settings	SonicOS Standard 3.0.0.5-17s	MON FEB 14 18:05:08 2005	2.5 MB		

   - If you are using a **SonicWALL PRO 2040**, **SonicWALL PRO 3060**, **SonicWALL PRO 4060**, or **SonicWALL PRO 5060**, click the **Create Backup Settings** button on from the **System > Settings** page of the SonicWALL management interface. When you select **Create Backup**, SonicOS saves both the current SonicOS Standard/Enhanced image and your current configuration preferences.



Firmware Management

☑ Notify me when new firmware is available

Firmware Image	Version	Date	Size	Download	Boot
Current Firmware	SonicOS Standard 3.0.0.3-39s	MON FEB 14 18:17:12 2005	2.6 MB		
Current Firmware with Factory Default Settings	SonicOS Standard 3.0.0.3-39s	MON FEB 14 18:17:12 2005	2.6 MB		
Uploaded Firmware	SonicOS Standard 3.0.0.3-39s	MON FEB 14 18:09:52 2005	2.6 MB		
Uploaded Firmware with Factory Default Settings	SonicOS Standard 3.0.0.3-39s	MON FEB 14 18:09:52 2005	2.6 MB		
System Backup	SonicOS Standard 3.0.0.2-33s	MON FEB 14 17:54:14 2005	2.6 MB		
Factory Default Firmware	SonicOS Enhanced 2.0.0.1	TUE OCT 07 17:21:55 2003	2.2 MB		

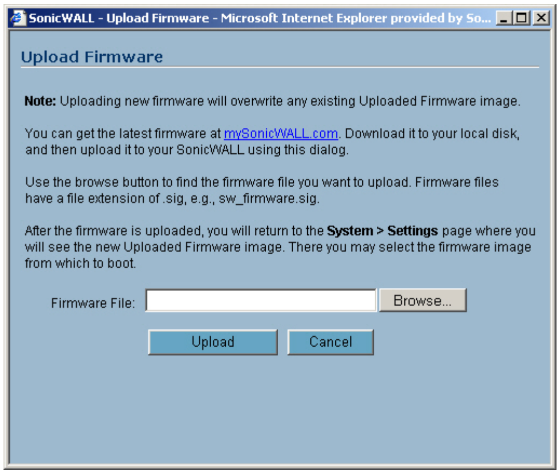
2. On the **System > Settings** page, click the **Export Settings...** button and save the preferences file to your local machine. The default preferences file is named *sonicwall.exp*. You can rename the file but you should keep the .exp extension.

Tip: *Rename the .exp file to include the version of the SonicOS Standard/Enhanced image from which you are exporting the settings. For example, if you export the settings from the SonicOS Standard 3.1.5.0 image, rename the file using the format: [date]_[version]_[mac].exp to "021605_3.1.5.0s_000611223344.exp" (the [mac] format entry is the serial number of the SonicWALL security appliance). Then if you need to roll back to that version of the SonicOS Standard/Enhanced image, you can correctly choose the file to import.*

Upgrading a SonicOS Standard/Enhanced Image with Current Preferences

Note: *SonicWALL security appliances do not support downgrading a SonicOS Standard/Enhanced image and using the configuration preferences file from a higher version. If you are downgrading to a lower version of a SonicOS Standard/Enhanced image, you must select* ***Uploaded Firmware with Factory Defaults – New!*** ☞. *You can import a preferences file previously saved from the downgrade version or reconfigure manually. Refer to "Updating SonicOS Standard/Enhanced with Factory Default Settings."*

1. Download the SonicOS Standard/Enhanced image file from mysonicwall.com and save it to a location on your local computer.
2. Select **Upload New Firmware** from the SonicWALL's **System > Settings** page. Browse to the location where you saved the SonicOS Standard/Enhanced image file, select the file, and click the **Upload** button. The upload process can take up to one minute.


SonicWALL - Upload Firmware - Microsoft Internet Explorer provided by So...

Upload Firmware

Note: Uploading new firmware will overwrite any existing Uploaded Firmware image.

You can get the latest firmware at mySonicWALL.com. Download it to your local disk, and then upload it to your SonicWALL using this dialog.

Use the browse button to find the firmware file you want to upload. Firmware files have a file extension of .sig, e.g., sw_firmware.sig.

After the firmware is uploaded, you will return to the **System > Settings** page where you will see the new Uploaded Firmware image. There you may select the firmware image from which to boot.

Firmware File: [ ] Browse...

3. When the upload is complete, you are ready to reboot your SonicWALL security appliance with the new SonicOS Standard/Enhanced image. From the SonicOS **System > Settings** page, select the boot icon for the following entry:

   Uploaded Firmware – New! ☞

4. A message dialog is displayed informing you the image update booting process will take between one and two minutes, and a warning not to power off the device while the image is being uploaded to the flash memory. Click **OK** to proceed.
5. After successfully uploading the image to your SonicWALL security appliance, the login screen is displayed. Enter your user name and password. Your new SonicOS Standard/Enhanced image version information is listed on the **System > Settings** page.

Upgrading a SonicOS Standard/Enhanced Image with Factory Defaults

1. Download the SonicOS Standard/Enhanced image file from mysonicwall.com and save it to a known location on your local computer.
2. Make a system backup of your SonicWALL security appliance configuration settings by selecting **Create Backup Settings** or **Create Backup** from the **System > Settings** page of the SonicWALL management interface.
3. Select **Upload New Firmware** from the SonicWALL's **System > Settings** page. Browse to the location where you saved the SonicOS Standard/Enhanced image, select the file, and click the **Upload** button. The upload process can take up to 1 minute.
4. When the upload is complete, you are ready to reboot your SonicWALL security appliance with the new SonicOS Standard/Enhanced image. From the SonicWALL's **System > Settings** page, select the boot icon for the following entry:

   Uploaded Firmware with Factory Defaults – New! ☞

5. A message dialog is displayed informing you the firmware booting process will take between one and two minutes, and a warning not to power off the device while the image is being uploaded to the flash memory. Click **OK** to proceed.
6. After successfully uploading the firmware to your SonicWALL security appliance, the login screen is displayed. Enter your user name and password to access the SonicWALL management interface. Your new firmware is listed on the **System > Settings** page.

Resetting the SonicWALL Security Appliance Using SafeMode

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.

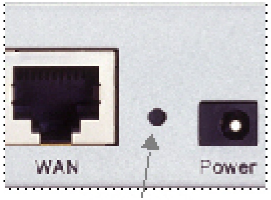
To reset the SonicWALL security appliance, perform the following steps:

1. Connect your management station to a LAN port on the SonicWALL security appliance and configure your management station IP address with an address on the 192.168.168.0/24 subnet, such as 192.168.168.20.

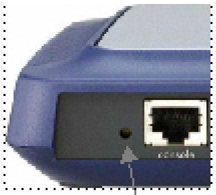
   Note: *The SonicWALL security appliance can also respond to the last configured LAN IP address in SafeMode. This is useful for remote management recovery or hands off recovery in a datacenter.*

2. Use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the reset button on the back of the security appliance for more than 20 seconds. The reset button is in a small hole next to the console port or next to the power supply, depending on your SonicWALL security appliance model.

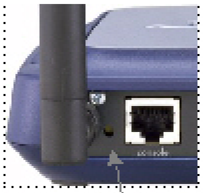
   Tip: *If this procedure does not work while the power is on, turn the unit off and on while holding the reset button until the Test light starts blinking.*



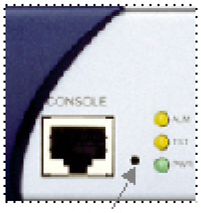
Reset button
TZ 150, TZ 150 Wireless



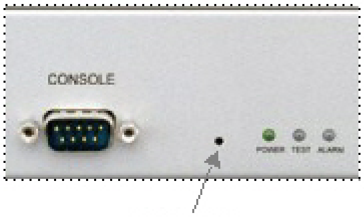
Reset button
TZ 170, TZ 170 SP



Reset button
TZ 170 Wireless



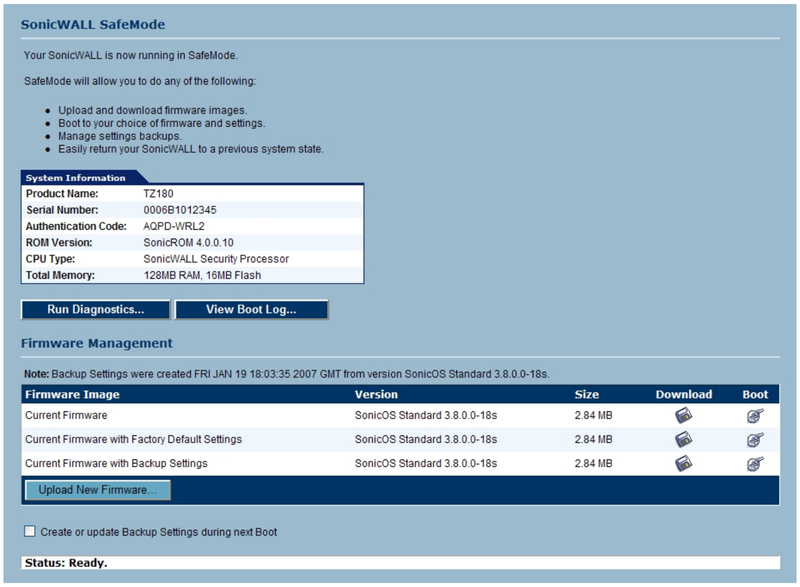
Reset button
PRO 1260



Reset button
PRO 2040, PRO 3060
PRO 4060, PRO 5060

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

3. Connect to the management interface: Point the Web browser on your Management Station to **192.168.168.168**. The SafeMode management interface displays.



SonicWALL SafeMode

Your SonicWALL is now running in SafeMode.

SafeMode will allow you to do any of the following:

- Upload and download firmware images.
- Boot to your choice of firmware and settings.
- Manage settings backups.
- Easily return your SonicWALL to a previous system state.

System Information	
Product Name:	TZ180
Serial Number:	0006B1012345
Authentication Code:	AQPD-WRL2
ROM Version:	SonicROM 4.0.0.10
CPU Type:	SonicWALL Security Processor
Total Memory:	128MB RAM, 16MB Flash

Firmware Management

Note: Backup Settings were created FRI JAN 19 18:03:35 2007 GMT from version SonicOS Standard 3.8.0.0-18s.

Firmware Image	Version	Size	Download	Boot
Current Firmware	SonicOS Standard 3.8.0.0-18s	2.84 MB		
Current Firmware with Factory Default Settings	SonicOS Standard 3.8.0.0-18s	2.84 MB		
Current Firmware with Backup Settings	SonicOS Standard 3.8.0.0-18s	2.84 MB		

☐ Create or update Backup Settings during next Boot

Status: Ready.

4. If you have made any configuration changes to the security appliance, make a backup copy of your current settings. Click **Create Backup Settings**.

5. Try rebooting the SonicWALL security appliance with your current settings. Click the boot icon in the same line with **Current Firmware**.

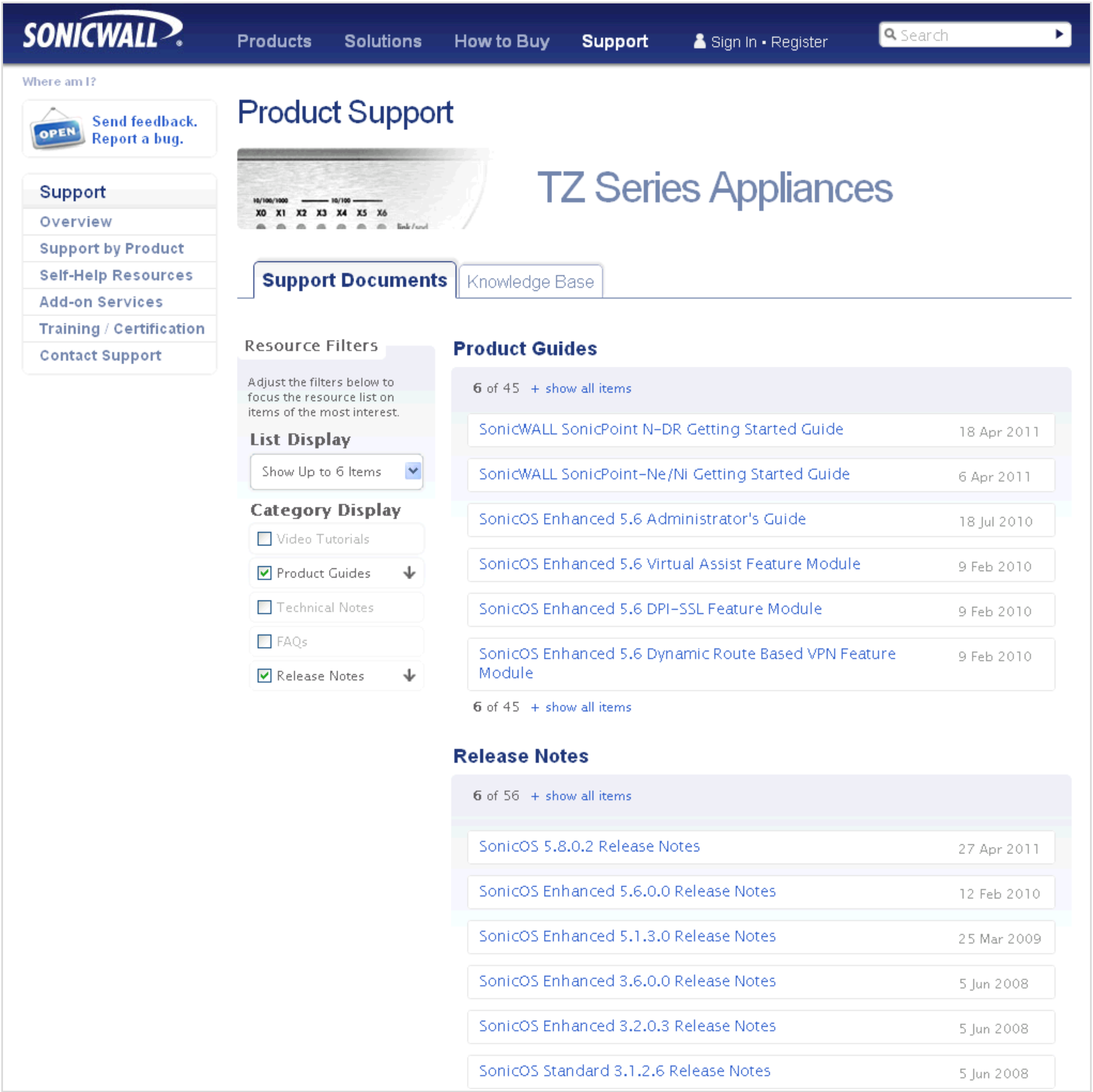
6. After the SonicWALL security appliance has rebooted, try to open the management interface again. If you still cannot open the management interface, use the reset button to restart the appliance in SafeMode again. In SafeMode, restart the SonicOS image with the factory default settings. Click the boot icon in the same line with **Current Firmware with Factory Default Settings**.

7. After the SonicWALL security appliance has rebooted, try to open the management interface again. If you are able to connect, you can recreate your configuration or try to reboot with the backup settings: Restart the security appliance in SafeMode again, and click the boot icon in the same line with **Current Firmware with Backup Settings**.

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.



Product Support

TZ Series Appliances

Resource Filters

Adjust the filters below to focus the resource list on items of the most interest.

List Display

Show Up to 6 Items

Category Display

□ Video Tutorials
☑ Product Guides
□ Technical Notes
□ FAQs
☑ Release Notes

Product Guides

6 of 45 + show all items

SonicWALL SonicPoint N-DR Getting Started Guide	18 Apr 2011
SonicWALL SonicPoint-Ne/Ni Getting Started Guide	6 Apr 2011
SonicOS Enhanced 5.6 Administrator's Guide	18 Jul 2010
SonicOS Enhanced 5.6 Virtual Assist Feature Module	9 Feb 2010
SonicOS Enhanced 5.6 DPI-SSL Feature Module	9 Feb 2010
SonicOS Enhanced 5.6 Dynamic Route Based VPN Feature Module	9 Feb 2010

6 of 45 + show all items

Release Notes

6 of 56 + show all items

SonicOS 5.8.0.2 Release Notes	27 Apr 2011
SonicOS Enhanced 5.6.0.0 Release Notes	12 Feb 2010
SonicOS Enhanced 5.1.3.0 Release Notes	25 Mar 2009
SonicOS Enhanced 3.6.0.0 Release Notes	5 Jun 2008
SonicOS Enhanced 3.2.0.3 Release Notes	5 Jun 2008
SonicOS Standard 3.1.2.6 Release Notes	5 Jun 2008

Last updated: 10/18/2011