SonicOS Standard 3.1.2.5 Release Notes

SonicWALL, Inc.
Software Release: March 7, 2006

CONTENTS

PLATFORM COMPATIBILITY

SonicOS Standard version 3.1.2.5 is a supported release for the following platforms:

SonicWALL TZ 50
SonicWALL TZ 50 Wireless

KEY FEATURES

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.

P/N 232-000991-00
Rev A 3/06
3125s96

ENHANCEMENTS

- **New SonicOS Settings**:
  Added "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

Network

- **34022**: **Symptom**: Management of a SonicWALL security appliance from the WAN side is possible only by using HTTPS. **Condition**: 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.

Security Services

- **34460**: **Symptom**: Intrusion Prevention Service classifies IM, P2P as Multimedia traffic as Low Priority Attacks. **Condition**: If 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.
- **34503**: **Symptom**: Gateway Anti-Virus fails to detect a virus transmitted through a through VPN tunnel. **Condition**: 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.
- **34617**: **Symptom**: Only Microsoft Outlook Express client implementation of Internet Message Access Protocol (IMAP) supported. **Condition**: Specifying the IMAP option on 'Security Services' > 'Gateway Anti-Virus' only supports scanning of the Microsoft Outlook Express client implementation of IMAP.

Users

- **34310**: **Symptom**: URLs that can bypass ULA in rules will not work with a proxy Web server. **Condition**: 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.
- **35458**: **Symptom**: UserLoginStatus window displays an incorrect warning message about inactivity timer expiration. **Condition**: Inactivity Remaining for the user in the Active Sessions table on the 'Users' > 'Status' page always displays 0 if the activity timeout is set to a large value.

P/N 232-000991-00
Rev A 3/06
3125s96

VPN

- **34987**: **Symptom**: 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. **Condition**: Pushing all traffic through a VPN from a dynamic IP to a static IP causes this problem.
- **35100**: **Symptom**: When management from the Central Gateway's LAN is attempted, the Remote Gateway prints the log message: Incompatible IPSec Security Association. **Condition**: 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.
- **36185**: **Symptom**: The SonicWALL security appliance does not propose static routes to GVC. **Condition**: Single-arm mode deployments: Enable SonicWALL security appliances to be deployed downstream from an edge routing device or aggregation switch.

P/N 232-000991-00
Rev A 3/06
3125s96

RESOLVED KNOWN ISSUES FOR SONICOS STANDARD 3.1.2.5

This section contains a list of resolved known issues provided by the SonicOS Standard 3.1.2.5 release, which was released on March 7, 2006.

GUI

- **40451**: **Symptom**: The firmware image is not shown on the **System > Settings** page, and the SonicWALL security appliance prompts the user for the SonicOS Enhanced activation key (when SonicOS Enhanced has already been activated). **Condition**: Occurs when GAV, IPS, and Anti-Spyware are enabled using the **Manage Licenses** feature on the **Security Services** page.

Networking

- **40286**: **Symptom**: The Startup wizard misconfigures the DHCP Server. **Condition**: Occurs when DHCP is configured using the Startup wizard, and a PC attempts to obtain a lease outside of the DHCP range configured on the SonicWALL security appliance.

P/N 232-000991-00
Rev A 3/06
3125s96

RESOLVED KNOWN ISSUES FOR SONICOS STANDARD 3.1.0.15

This section contains a list of resolved known issues provided by the SonicOS Standard 3.1.0.15 and earlier releases. SonicOS Standard 3.1.0.15 was released on December 30, 2005.

Email Filtering

- **35597**: **Symptom**: Emails passing through a SonicWALL security appliance are garbled. C**ondition**: Occurs when Email Filtering is enabled.

Firewall

- **30085**: The option to force inbound and outbound FTP data connections to use the default port 20 is now available on the 'Firewall' > 'Advanced' display page.

GMS Filtering

- **37217**: **Symptom**: SNMP traps are sent when the SA lifetime expires and the tunnel renegotiates, and when users manually renegotiate the tunnel. **Condition**: Occurs when the SA lifetime expires or when the tunnel is manually renegotiated, and when users have the VPNTUNNELDOWN alert enabled in the SonicWALL Global Management System.

Log

- **34605**: **Symptom**: Unable to control 'Unknown protocol dropped' log messages. **Condition**: Log entry not being categorized in SonicOS Standard.
- **34762**: **Symptom**: Log messages appear for all traffic that is dropped, regardless of the logging setting for that service. **Condition**: 'Packet dropped' messages will appear for traffic configured to be dropped by an Access Rule, even if the 'Logging' checkbox on the service is disabled.
- **35330**: **Symptom**: Log displayed in UTC (Coordinated Universal Time) instead of local time. **Condition**: UTC time is displayed in log even when 'Display UTC in logs' on the 'System' > 'Time' page is not selected.
- **36051**: **Symptom**: SonicWALL security appliance may cease to operate at random times when the Data collection feature is enabled on the Log -> Reports page. Condition: In the SonicWALL Management interface under LOG -> Reports page, when the data collection feature is enabled, the SonicWALL security appliance—while collecting the data on the various sites visited by the hosts on the LAN—may cease to operate at random times.
- **37547**: **Symptom**: A SonicWALL security appliance reports "Possible Port Scan Dropped" alert messages. **Condition**: Occurs when the connection from a LAN to a WAN is terminated by the WAN host.
- **37595**: **Symptom**: A SonicWALL security appliance drops TCP reset packets from a web server because it classifies them as possible port scans. **Condition**: Occurs when the SonicWALL security appliance has several TCP connections on its DMZ interface to a web server. When the web server attempts to reset the connections, the SonicWALL security appliance drops the reset packets.

P/N 232-000991-00
Rev A 3/06
3125s96

N/A

- **38048**: **Symptom**: A SonicWALL security appliance reboots approximately once ever two hours. **Condition**: Occurs when the SonicWALL security appliance receives email containing unrecognized EIGRP packets.

N2H2 & Websense

- **37523**: **Symptom**: The SonicWALL security appliance repeatedly reboots. **Condition**: Occurs when enabling Websense on the Filter page.

Network

- **32289**: An issue with out-of-order packets in the FTP service when a client sent data first followed by the server sending data. Previously, if the client connected on TCP port 21 and sent data first, the SonicWALL security appliance blocked all client data. In addition, the SonicWALL security appliance logged an "Out-of-order command packet dropped" log event message and dropped the FTP service data.
- **32627**: An issue with TCP connections being reset when you enabled Content Filtering Services (CFS) on the LAN. Previously, when a user logged out of the SonicOS management interface, FTP and HTTP downloads currently in progress and any other persistent TCP connections were stopped.
- **33081**: **Symptom**: PPPoE negotiation delays for random periods of time before successfully connecting to the ISP. **Condition**: PPPoE continues to attempt negotiations without server response until finally an offer is received the server.
- **33808**: When User-Level Authentication (ULA) is enforced, the user has 60 seconds to authenticate with the username/password credentials. Otherwise, the login authentication window times out after 60 seconds.
- **34467**: **Symptom**: Dynamic DNS (DDNS) updates can take a few minutes to propagate. **Condition**: Specifying 'Specify IP Address Manually' for DDNS off-line configuration.
- **34539**: **Symptom**: DDNS records are only updated with the DDNS provider when an IP change occurs so as to prevent abuse charges. **Condition**: Changing the backup MX field by itself will not force an update to the record.
- **35220**: **Symptom**: E-mail from select ISPs using PPPoE is not delivered to mail server behind SonicWALL security appliance. **Condition**: An incorrect TCP MSS is being used for the SMTP session.
- **35400**: **Symptom**: FTP throughput performance on SonicWALL security appliance is low. **Condition**: SonicWALL security appliances may be incorrectly negotiating Ethernet link speed and duplex mode.
- **35727**: **Symptom**: SonicWALL security appliance ceases to operate when a DHCP client sends multiple DHCP requests with the same ID. **Condition**: The first IP address the SonicWALL DHCP Server wanted to hand out was already taken by a host with static IP on the network. By the time the SonicWALL security appliance responds with a new IP address, the DHCP Client sends a second DHCP request using the same ID as the previous one rather than incrementing the ID, which causes the SonicWALL security appliance to cease operation.
- **35754**: **Symptom**: PPPoE client is disconnected when inactivity timer is enabled even when there is LAN to WAN traffic. **Condition:** Enabling ‘Inactivity Disconnect’ on the ‘General’ tab for PPPoE displays the message ‘Disconnecting the PPPoE due to traffic timeout message’ and causes LAN to WAN traffic to be stopped.

P/N 232-000991-00
Rev A 3/06
3125s96

- **35759**: **Symptom**: DHCP clients on the WLAN interface are failing to renew the IP Lease after random periods of time. Condition: The SonicWALL security appliance stops answering DHCP requests. A power cycle of the SonicWALL security appliance temporarily resolves the issue.
- **36059**: **Symptom**: Network inactivity timers are not working properly with Oracle server. **Condition**: SonicWALL security appliance is resetting TCP connections at different idle times than specified in access rules.
- **36318**: **Symptom**: A proper PPPoE termination signal causes a delay (less than 20 seconds) to the SonicWALL security appliance PPPoE Active Discovery recovery. **Condition**: Occurs on SonicWALL security appliances receiving regularly service provider sent PPPoE termination signals.
- **36503**: **Symptom**: PPTP clients cannot establish connections to the PPTP server located behind a SonicWALL security appliance on the LAN Interface. **Condition**: This issue exists only when the SonicWALL is configured in the Transparent Mode.
- **37133**: **Symptom**: A SonicWALL security appliance does not automatically attempt to reconnect to an ISP. **Condition**: Occurs after the ISP rejects SonicWALL PPPoE negotiation.
- **37449**: **Symptom**: WPA will not work when enabled after WEP configuration. **Condition**: Wireless clients cannot be associated with SonicWALL security appliances after switching authentication type from WEP to WPA.
- **37662**: **Symptom**: A SonicWALL TZ 170 SP fails to restore the primary PPPoE aDSL connection when the connection is restored. **Condition**: Occurs when the PPPoE aDSL connection on a SonicWALL TZ 170 SP goes down, the TZ 170 SP fails over to the backup dial-up line, and the PPPoE aDSL connection is then restored.
- **37790**: **Symptom**: The “Error: Invalid DMZ Private Address” error message is displayed. **Condition**: Occurs when entering a valid IP address on the OPT / DMZ port in transparent mode.
- **37791**: **Symptom**: DHCP ranges are not imported. **Condition**: Occurs when importing an .exp file containing DHCP ranges after the SonicWALL security appliance reboots with factory settings.
- **38148**: **Symptom**: A SonicWALL TZ 150 intermittently loses Internet connectivity. **Condition**: Occurs when the SonicWALL TZ 150 is configured for NAT with DHCP on the WAN interface.
- **38625**: **Symptom**: A DDNS update message hangs. **Condition**: Occurs when the WAN IP address is changed.
- **38674**: **Symptom**: When the WAN interface on a SonicWALL security appliance is configured in NAT with PPPoE client mode, the PPPoE connection does not timeout and automatically disconnect—even when there is no traffic going from the LAN to WAN interfaces. **Condition:** Occurs when the PPPoE client is configured to timeout with an inactivity timeout period.

Policies Panel

- **38610**: **Symptom**: The VPN Configuration mode (Main or Aggressive mode) does not match with the firewall configuration, even after they have been synchronized. **Condition**: Occurs when the mode of an existing VPN SA is changed from Main mode to Aggressive mode.

P/N 232-000991-00
Rev A 3/06
3125s96

Security Services

- **35597: Symptom**: E-Mail Filtering can cause garbled Smart tags in attached Microsoft Office 2003 files. **Condition**: Microsoft Office 2003 output files (.ppt, .doc, .xls) with Smart tagging are filtered as .com file type attachments. If .com file type filtering is enabled, Microsoft Office 2003 files are blocked.

System/GUI

- **35225**: **Symptom**: Special characters like HTML bracket and double quote malfunction in IKE secret key fields. **Condition**: This issue occurs only with HTML-relevant special characters. Any characters following a double quote are erased. If a closing HTML bracket character > appears after a double quote, the content after the bracket is displayed as raw HTML code on the form container.
- **35799**: **Symptom**: The Acceptable Use Policy does not save configuration and displays incorrectly. **Condition**: Occurs after you have enter text, save, and revisit and view the text; text appears truncated.
- **36451**: **Symptom**: Scripts or HTML strings entered in the username field of the SonicOS management login appear in the Log > View page. **Condition**: Occurs when you enter a script or HTML string in the username field in the SonicOS management login page, access is denied. User then enters proper administrator credentials and views the Log > View page that the script and HTML string is displayed.
- **37789**: **Symptom**: A SonicWALL TZ 170 reboots because the tNTP task is suspended. **Condition**: Occurs when no NTP server responds to the SonicWALL TZ 170.

Users

- **35459**: **Symptom**: The browser is not redirected to <http://<addr>/userLogin2.html> when remote user logs into the VPN zone, and the User Login Status window is not displayed. **Condition**: From a remote VPN host, the user browses to the LAN IP of the local firewall, and enters a user name and password. Traffic is passed through the tunnel, and the user is shown in the Active User Session table.
- **37296**: RADIUS servers cannot be authenticated using RSA tokens.
- **39678**: **Symptom**: A SonicWALL TZ 170 SP Wireless fails to authenticate client session. C**ondition**: Occurs when clients are using the SonicWALL Global VPN Client configured for DHCP over VPN.

VPN

- **32863**: An issue where a SonicWALL security appliance configured in Single ARM Mode proposed the *host mask* instead of *network mask* during IPSec negotiations.
- **32925**: An issue where tunnel negotiation on the secondary VPN gateway fails when the unit is configured for GMS management using HTTPS over an existing tunnel.
- **35756**: **Symptom**: SonicWALL security appliance displays an incorrect VPN proposal for local network behind a LAN gateway when using Aggressive Mode for IKE. **Condition**: Add route on SonicWALL security appliance to point to the network behind the LAN router, create an Aggressive Mode VPN to another SonicWALL security appliance, and initiate a tunnel from the network behind the LAN router.

P/N 232-000991-00
Rev A 3/06
3125s96

- **35997**: **Symptom**: SonicWALL security appliance malfunctions when Bandwidth Management (BWM) and WAN GroupVPN are enabled. **Condition**: Enable BWM on the WAN interface and then enable WAN GroupVPN.
- **36287**: **Symptom**: When a site-to-site VPN Tunnel is setup between a Zultys VoIP Phone and SonicWALL security appliance, ESP packets pertaining to an old Phase2 SA were being dropped by SonicWALL security appliance. **Condition**: This happens on a re-key, the SonicWALL security appliance expects the Zultys VoIP phone to send the subsequent ESP packets on the new Phase2 SA, whereas the Zultys VoIP Phone is still sending the packets using the old phase2 SA until the hard lifetime expires.
- **36379**: **Symptom**: The SonicWALL security appliance does not allow more than two site-to-site VPN Policies even when the unit is licensed for 10 VPN policies. **Condition:** This happens on a SonicWALL TZ 170/W/SP 10 node product after a node upgrade from 10 nodes to 25 or unlimited nodes.
- **36585**: **Symptom**: Manual Key SA using ESP Null cannot be added and is deleted upon an upgrade from earlier firmware versions. **Condition**: During an upgrade, if you have 'Phase 2 Authentication for Manual Key VPNs' specified to anything other than 'None', the SA will be deleted after upgrade.
- **39312**: **Symptom**: A SonicWALL TZ series security appliance stops passing traffic even though the VPN tunnel appears to remain active. **Condition**: Occurs under moderate to heavy traffic conditions when the crypto hardware security association (SA) fails (because of a queue overflow, for example) and the crypto hardware SA driver does not switch over to an uninitialized SA.
- **39611**: **Condition**: A VPN-enabled SonicWALL security appliance stops passing traffic, stops processing VPN traffic, or spontaneously restarts when subjected to the PROTOS test suite (http://www.ee.oulu.fi/research/ouspg/protos/testing/c09/isakmp/) or derivative Denial of Service attack.

Wireless

- **34695**: **Symptom**: When Wireless Guest Services is configured to use External Guest Authentication where the External Web Server is connected by a VPN tunnel, authentication will fail. **Condition**: The WAN IP address is being used as the mgmtBaseURL instead of the LAN IP, which should be used because the user is connecting through the tunnel.
- **37449**: **Symptom**: Wireless clients cannot connect to a SonicWALL security appliance using the WPA authentication method. **Condition**: Occurs when the authentication method is changed from WEP to WPA.
- **38540**: **Symptom**: NetBIOS traffic is unable to traverse from the LAN side to the WLAN side. **Condition**: Occurs whenever NetBIOS attempts to traverse from the LAN side to the WLAN side.
- **38931**: **Symptom**: A SonicWALL TZ 170 wireless hangs. **Condition**: Occurs when a WEP key is added when wireless is disabled.
- **39021**: **Symptom**: Unauthorized and unassociated wireless clients can prevent authorized clients from connecting to a SonicWALL security appliance. **Condition**: Occurs when WGS is first enabled and then later disabled.
- **39170**: **Symptom**: Connections to a SonicWALL TZ 170 SP Wireless are dropped and the clients cannot reconnect. **Condition**: Occurs when clients are using the SonicWALL Global VPN Client over a wireless connection.

P/N 232-000991-00
Rev A 3/06
3125s96

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
- SAVING A BACKUP COPY OF YOUR CONFIGURATION PREFERENCES
- UPGRADING A SONICOS STANDARD/ENHANCED IMAGE WITH CURRENT PREFERENCES
- UPGRADING A SONICOS STANDARD/ENHANCED IMAGE WITH FACTORY DEFAULTS
- RESETTING THE SONICWALL SECURITY APPLIANCE USING SAFEMODE
- UPGRADING A SONICOS STANDARD IMAGE TO A SONICOS ENHANCED IMAGE

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.

P/N 232-000991-00
Rev A 3/06
3125s96

Saving a Backup Copy of Your Configuration Preferences

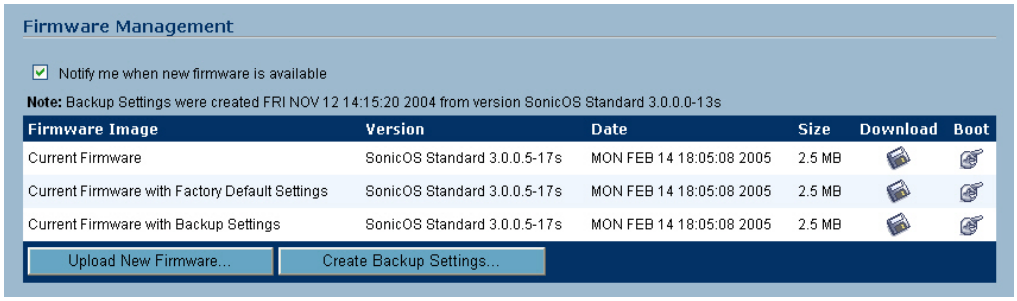
Before beginning the update process, make a system backup of your SonicWALL security appliance configuration settings. The backup feature saves a copy of your current configuration settings on your SonicWALL security appliance, protecting all your existing settings in the event it becomes necessary to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

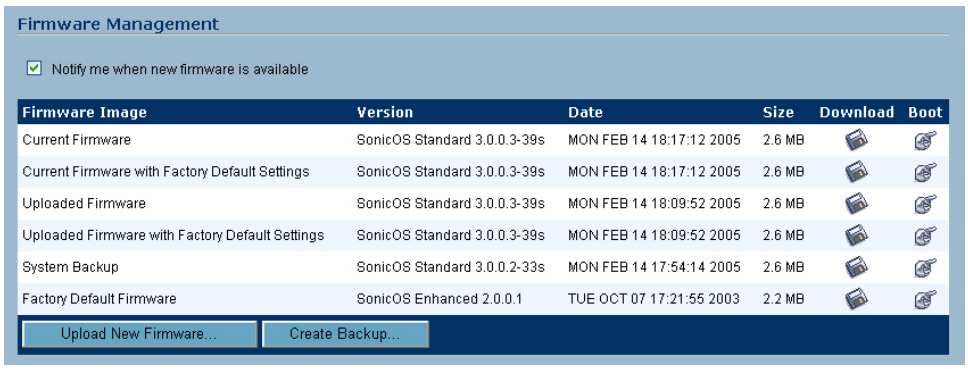
Perform the following procedures to save a backup of your configuration settings and export them to a file on your local management station:

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

   - If you are using a **SonicWALL TZ 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.



   - 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.



2. On the **System > Settings** page, click the 

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 filename.

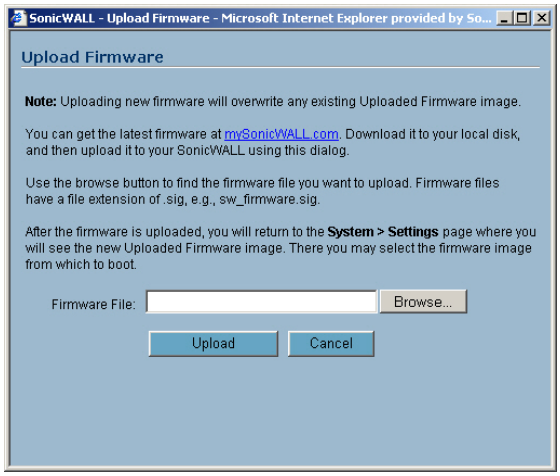
P/N 232-000991-00
Rev A 3/06
3125s96

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 3.0 image, rename the file using the format: [date]_[version]_[mac].exp to "021605_3.0.0.6-27s_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 mage, 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.



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.

P/N 232-000991-00
Rev A 3/06
3125s96

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.

P/N 232-000991-00
Rev A 3/06
3125s96

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.

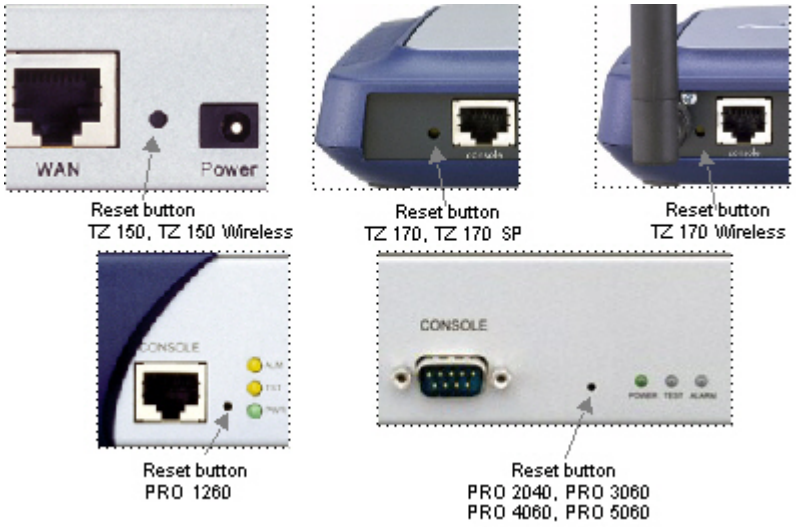
To reset the SonicWALL security appliance, perform the following steps:

1. Connect your management station to a LAN port on the SonicWALL security appliance and configure you management station IP address to **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 five to ten 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.

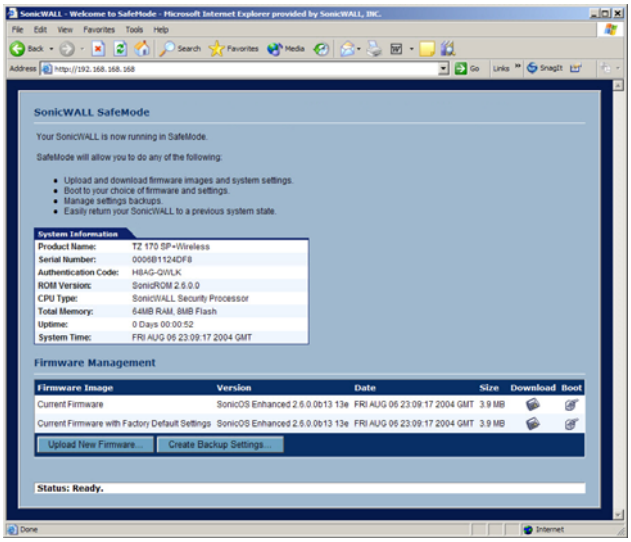
   Tip: *If this procedure does not work while the power is on, turn the unit off and on while holding the reset button until the Test light starts blinking.*



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

P/N 232-000991-00
Rev A 3/06
3125s96

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



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 Standard 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**.

P/N 232-000991-00
Rev A 3/06
3125s96

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 170	SonicWALL PRO 1260
SonicWALL TZ 170 SP	SonicWALL PRO 2040
SonicWALL TZ 170 Wireless	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/support/SonicOS_FW_documentation.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.

P/N 232-000991-00
Rev A 3/06
3125s96

RELATED TECHNICAL DOCUMENTATION

SonicWALL user guide reference documentation is available at the SonicWALL Technical Documentation Online Library:
http://www.sonicwall.com/support/documentation.html

- *SonicOS Standard 3.1 Administrator's Guide*
- *SonicOS Enhanced 3.1 Administrator's Guide*
- *SonicOS Log Event Reference Guide*
- *SonicOS CLI Reference Guide*

For basic and advanced deployment examples,
refer to SonicOS Feature Modules and Deployment TechNotes:

SonicOS Feature Modules

SonicOS Enhanced

- NEW! Configuring Quality of Service and Bandwidth Management
- NEW! Configuring Portshield Interfaces
- NEW! Configuring VLANs

SonicOS TechNotes

SonicOS Upgrades

- SonicOS Standard to Enhanced Upgrade (SonicOS 3.0)
- SonicOS Standard to Enhanced Upgrade (SonicOS 2.0)

General Configuration

- NEW! VPN Interoperability Between SonicWALL Security Appliances and Cisco 3000
- NEW! VPN Interoperability Between SonicOS 3.1 Enhanced and Microsoft ISA Server 2004
- NEW! IP Helper on SonicOS Enhanced
- Transparent Mode Support on SonicOS Enhanced
- Using VLANs with SonicWALLs
- Cisco Catalyst Switch Configuration for SonicWALL Device
- NEW! Online Certificate Status Protocol in SonicOS Enhanced 3.1
- NEW! Using SYN Flood Protection in SonicOS Enhanced
- SonicOS Enhanced Wizards

Document Version: March 7, 2006

P/N 232-000991-00
Rev A 3/06
3125s96