

Release Notes

Contents

Platform Compatibility	1
Known Issues	2
Resolved Known Issues	3
Upgrading SonicOS Standard/Enhanced Image Procedures	4
Related Technical Documentation	8

Platform Compatibility

The SonicOS Enhanced 4.0.1.1 release is supported on the following SonicWALL appliances:

- SonicWALL TZ 190 Wireless
- SonicWALL TZ 190
- SonicWALL TZ 180 Wireless
- SonicWALL TZ 180

This release supports the following Web browsers:

- Microsoft Internet Explorer 6.0 and higher
- Mozilla Firefox 2.0 and higher
- Netscape 9.0 and higher
- Opera 9.10 and higher for Windows
- Safari 2.0 and higher for MacOS

Strong SSL and TLS Encryption Required in Your Browser

The internal SonicWALL Web server only supports SSL version 3.0 and TLS with strong ciphers (128 bits or greater) when negotiating HTTPS management sessions. SSL implementations prior to version 3.0 and weak ciphers (symmetric ciphers less than 128 bits) are not supported. This heightened level of HTTPS security protects against potential SSLv2 roll-back vulnerabilities and ensures compliance with the Payment Card Industry (PCI) and other security and risk-management standards.

TIP: By default, Mozilla Firefox 2.0 and Microsoft Internet Explorer 7.0 enable SSL 3.0 and TLS, and disable SSL 2.0. SonicWALL recommends using the most recent Web browser releases. If you are using a previous release of these browsers, you should enable SSL 3.0 and TLS and disable SSL 2.0. In Internet Explorer, go to Tools > Internet Options on the Advanced tab and scroll to the bottom of the Settings menu. In Firefox, go to Tools > Options on the Advanced tab, and then select the Encryption tab.

Release Notes

Known Issues

This section contains a list of known issues in the SonicOS Enhanced 4.0.1.1 release.

Firewall

Symptom	Condition / Workaround	Issue
Users are allowed access without being required to authenticate when the CFS exclusion list is enabled.	Occurs when the CFS exclusion list is enabled and users attempt to access the network from the IP address range specified for the CFS exclusion list. Workaround: Disable the CFS exclusion list.	70797
Bandwidth management rates that are configured as limits in Kbps are saved in the UI as percentage limits.	Occurs when configuring bandwidth management on access rules and the bandwidth rates are configured as percentage limits. Workaround: Configure bandwidth management rates as Kbps limits.	70782

Networking

Symptom	Condition / Workaround	Issue
Configuring the link speed for an interface doesn't work on the Network > Interfaces page.	Occurs when trying to configure the link speed on the Advanced tab of an interface configuration window. Workaround: Configure the Link speed on the Network > SwitchPorts page.	70647

System

Symptom	Condition / Workaround	Issue
Users with Limited Admin privileges cannot configure an NTP server on the System > Time page. Instead of displaying the Configure NTP Server page, the UI displays the System > Status page.	Occurs when a Limited Admin user attempts to configure an NTP server. This problem only affects Limited Admin users.	70494
The SonicWALL GMS Synchronize Now command fails to retrieve Local Certificates.	Occurs when performing the Synchronize Now command for a SonicWALL security appliance that has Local Certificates configured.	70625

VPN

Symptom	Condition / Workaround	Issue
L2TP clients cannot connect to the L2TP server when the firewall is behind a NAT device.	Occurs when a Windows XP client attempts to establish an L2TP tunnel to a firewall behind a NAT device. Workaround: Remove the NAT device.	52890
A Windows L2TP IPsec client is logged out unexpectedly.	Occurs when the L2TP IPsec client is running FTP traffic through the tunnel.	70789

Release Notes

Resolved Known Issues

This section contains a list of resolved issues in the SonicOS Enhanced 4.0.1.1 release.

Content Filtering

Symptom	Condition / Workaround	Issue
The CFS block page executes JavaScript code that is appended to a blocked URL.	Occurs when a user connected to the SonicWALL visits a URL that contains a malicious script within the URL itself, and also triggers the CFS block page.	70676

Log

Symptom	Condition / Workaround	Issue
Checksum error messages need to include the word "dropped" for compliance with ICSA Certification V01:LO2H.	Occurs when checksum errors are logged.	53434

Networking

Symptom	Condition / Workaround	Issue
DNS attacks and cache poisoning are possible using some methods of port translation when designating the source port.	Occurs when sequential NAT port translation instead of random port translation is used for outgoing DNS queries.	70927

Release Notes


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.....	4
Saving a Backup Copy of Your Configuration Preferences	4
Upgrading a SonicOS Standard/Enhanced Image with Current Preferences	5
Upgrading a SonicOS Standard/Enhanced Image with Factory Defaults.....	6
Resetting the SonicWALL Security Appliance Using SafeMode.....	6

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.

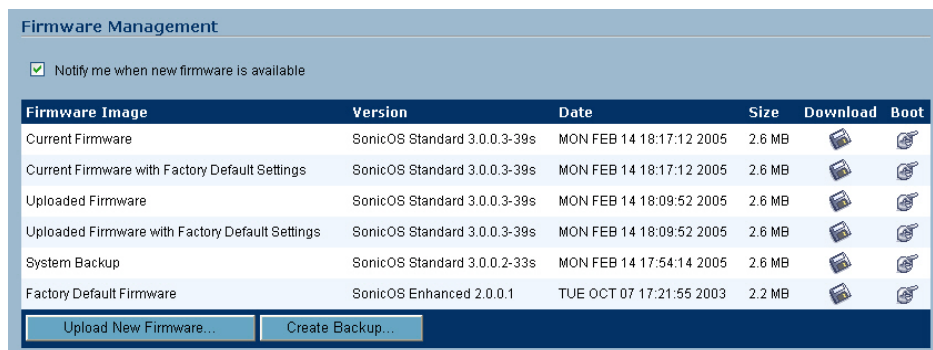
Saving a Backup Copy of Your Configuration Preferences

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. To save a backup of your settings on a SonicWALL TZ 180/180W or SonicWALL TZ 190/190W, click the **Create Backup Settings** button on 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.



Release Notes


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 extension.



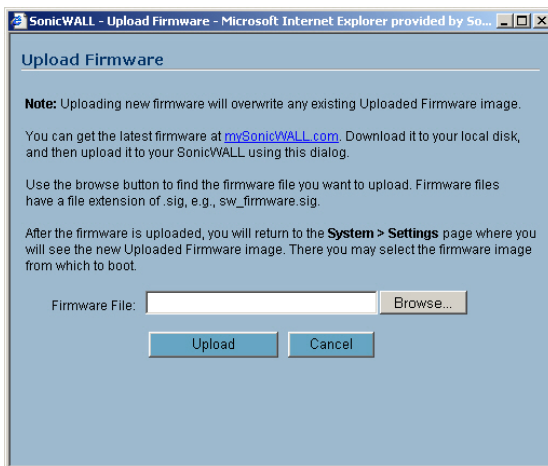
Tip: Rename the .exp file to include the version of the SonicOS Standard/Enhanced image from which you are exporting the settings. For example, if you export the settings from the SonicOS Standard 3.0 image, rename the file using the format: [date]_[version]_[mac].exp to “021605_3.0.0.6-27s_000611223344.exp” (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 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.



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 that the image update booting process will take between one and two minutes, and a warning is displayed that warns you 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.

Release Notes

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 one 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 that the firmware booting process will take between one and two minutes, and a warning is displayed that warns you 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.



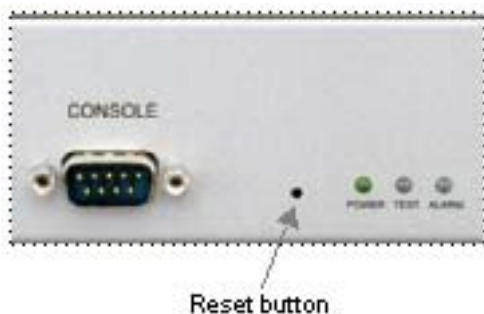
Note: *The SonicWALL security appliance can also respond to the last configured LAN IP address in SafeMode. This is useful for remote management recovery or hands off recovery in a datacenter.*

Release Notes



2. Use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the reset button on the security appliance for 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.

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**.

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 Web site.

The screenshot displays the SonicWALL support website interface. At the top, there is a navigation menu with links for HOME, PRODUCTS, SOLUTIONS, HOW TO BUY, SUPPORT (highlighted), TRAINING & EVENTS, COMPANY, and PARTNERS. A "Login to MySonicWALL" button is located in the top right corner. The main content area features a large banner for "TZ 180 SERIES APPLIANCES" with the text "PRODUCT SUPPORT" overlaid. Below the banner, there are several sections of support resources:

- SUPPORT RESOURCES**
- SELF-SERVE HELP**
- Downloads**
 - Firmware
 - Setup Tool (PC)
 - Setup Tool (Mac)
 - Signatures
- User Forums**
- Knowledge Portal**
- OPEN A SUPPORT CASE**
- Web**
- Telephone**
- Partner**
- REFERENCE LIBRARY**
 - Product Guides
 - Technical Notes
 - FAQs
 - Release Notes
- OTHER SERVICES**
 - Support Services**
 - Support and Consulting Services Brochure
 - E-Class Support
 - Global Support Services Reference Guide
 - Training & Certification**
 - Consulting Services**
- STAY IN TOUCH**

Below the navigation and banner, there are four tables of recent resources:

- Recent PRODUCT GUIDES**

#	Date	Title
1	26 Jun 2008	SonicWALL TZ 180 Wireless Getting Started Guide
2	26 Jun 2008	SonicWALL TZ 180 Getting Started Guide
3	25 Jun 2008	SonicOS Enhanced 4.0 TZ 180 & 190 Series Administrator's Guide
4	20 Jun 2008	TZ 4.0 Documents Zip File
5	16 Jun 2008	TZ 3.9 Documents Zip File
- Recent TECHNICAL NOTES**

#	Date	Title
1	22 Mar 2008	Lightweight Hotspot Messaging Scripts
- Recent SERVICE BULLETINS**

#	Date	Title
---	------	-------
- Recent FAQs**

#	Date	Title
---	------	-------
- Recent RELEASE NOTES**

#	Date	Title
1	28 May 2008	SonicOS Standard 3.9.0.1 Release Notes
2	28 May 2008	SonicOS Enhanced 3.9.0.3 Release Notes
3	20 Mar 2008	SonicOS Enhanced 3.9.0.1 Release Notes
4	03 Mar 2008	SonicOS Standard 3.9.0.0 Release Notes
5	03 Mar 2008	SonicOS Enhanced 3.9.0.0 Release Notes

Last updated: 8/27/2008