

Release Notes

Contents

Platform Compatibility	1
Known Issues	2
Resolved Issues	5
Upgrading SonicOS Enhanced Image Procedures.....	7
Related Technical Documentation	12

Platform Compatibility

The SonicOS Enhanced 5.5.2.0 release is supported on the following SonicWALL UTM appliances:

- SonicWALL TZ 100
- SonicWALL TZ 100 Wireless-N
- SonicWALL TZ 200
- SonicWALL TZ 200 Wireless-N
- SonicWALL TZ 210
- SonicWALL TZ 210 Wireless-N
- SonicWALL NSA 240
- SonicWALL NSA 2400
- SonicWALL NSA 3500
- SonicWALL NSA 4500
- SonicWALL NSA 5000
- SonicWALL NSA E5500
- SonicWALL NSA E6500
- SonicWALL NSA E7500

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

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 higher, and Microsoft Internet Explorer 7.0 and higher 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 5.5.2.0 release.

Command Line Interface

Symptom	Condition / Workaround	Issue
On SonicWALL TZ Series and NSA 240 appliances, the X2-X8 interfaces cannot be configured from the CLI. An error may be reported, and the interfaces remain configured with the previous settings when viewed in the Web management interface.	Occurs when the X2-X6 interfaces are configured as "PortShield to X0", and then the CLI is used to modify their IP address or zone settings. Workaround: Use the Web management interface to configure X2-X8.	80208

Log

Symptom	Condition / Workaround	Issue
A UTM appliance no longer records log information after hitting a maximum number of entries.	Occurs when a UTM appliance records 400 log entries from various traffic types and the log cannot be cleared from the Log > View page.	87138

Networking

Symptom	Condition / Workaround	Issue
Select traffic types are not given access to pass networks.	Occurs when non-HTTP(S) types of traffic attempt to access a site that has been identified and enabled as set for pass network accessibility.	86539
Variable file traffic is allowed when Performance Optimization is set for GAV.	Occurs when Performance Optimization is set in the Security Services menu, and inbound/outbound HTTP and outbound TCP is enabled for GAV.	86451
In a few reported cases, RIPv2 routing information is not recorded into the internal routing table of a UTM appliance.	Occurs when RIPv2 is used for routing in a High Availability environment and some routing information is lost during failover.	86290
OSPF cannot be disabled within any OS interface.	Occurs when a user attempts to disable OSPF on an interface and receives an error claiming, "Configuration Locked by OSPF cli."	84786
RIP is disabled on an interface, and the published network is not updated on the router.	Occurs when RIPv2 is enabled on a LAN interface and then the interface IP address is changed to a different subnet.	83512
SonicWALL security services fail to display block pages when blocking Web sites designated as Spyware, and the appliance becomes inaccessible from LAN interfaces configured for L2 Bridge mode.	Occurs only in an asymmetric routing configuration. Occurs when the firewall ARP table includes an entry for the LAN host. Workaround: Delete the LAN host entry from the ARP table.	79478
Changing the zone assignment of an interface leads to the user being unable to edit the DHCP relay policy for that interface.	Occurs when an interface is assigned to a customized zone and then a DHCP relay policy is configured with the customized zone as the source. If the interface is then assigned to a different interface, the DHCP relay policy can no longer be edited.	79363

Release Notes

In a two-firewall configuration with asymmetric routing, TCP connections are dropped with TCP handshake violation errors related to stateful inspection.	Occurs when the Disable Stateful inspection on this bridge-pair checkbox is selected, but fails to override TCP stateful inspection settings.	79353
The Default Gateway and Secondary Gateway address objects are always shown as 0.0.0.0. They can still be selected, but do not work.	Occurs when attempting to use the Default Gateway or Secondary Gateway address object in SonicOS Enhanced release 5.5. Note that the address objects are shown as 0.0.0.0 when booted to factory default settings, or if the gateways are not configured upon upgrade.	79059

SSL VPN

Symptom	Condition / Workaround	Issue
Attempts to login to the SSL VPN portal fail, and a "Login screen timed out" message is repeatedly displayed.	Occurs when attempting to login as a local user to the SSL VPN portal of a firewall over a wireless connection after first attempting to log in as admin over HTTP on the wireless and not being allowed. Workaround: Log in as admin over HTTPS, then log out. You will then be able to log in to the SSL VPN portal.	82120

VPN

Symptom	Condition / Workaround	Issue
In a site-to-site VPN tunnel, traffic from the remote to the local is occasionally dropped.	Occurs when an ICMP request is dropped by the firewall due to policy enforcement, when the local is in Layer 2 bridge mode through the X1 interface.	88379
A VPN tunnel ceases to work after connecting through a secondary WAN interface.	Occurs when a VPN tunnel using a secondary WAN fails to maintain connectivity when the primary WAN returns to service. Workaround: Manually renegotiate the VPN tunnel from the remote unit.	87500
H.323 endpoint calls made through Route-Based VPN with Tunnel Interface configured cannot be established.	Occurs when attempting to make H.323 calls from a NetMeeting client on the LAN of firewall A to the Polycom client or to the NetMeeting client on the LAN of firewall B.	81549
The Enable Windows Networking (NetBIOS) Broadcast option for a VPN Policy does not automatically create an IP Helper policy. The IP Helper policy must be added manually.	Occurs when adding a Tunnel Interface VPN Policy and selecting the Enable Windows Networking (NetBIOS) Broadcast option.	79952

Release Notes

Wireless

Symptom	Condition / Workaround	Issue
SSL VPN enforcement is disregarded for HTTPS traffic.	Occurs when HTTPS traffic is allowed from WLAN to WAN, while other traffic is denied by WLAN SSL VPN enforcement policies. Workaround: Create a WLAN to WAN HTTPS deny rule, or change the default allow rule to deny and create an allow rule for DNS.	85827

WWAN

Symptom	Condition / Workaround	Issue
Dial-on-Data profile does not work after Connection Model is changed.	Occurs when configuring a WWAN profile Dial-on-Data. Although the Network Connection Model is set to Ethernet with WWAN failover, the WWAN connection is invalid and all traffic is dropped. Note that this occurs occasionally, and can only be seen on failover from Ethernet WAN. Workaround: Reboot the device after changing the connection type or the WAN connection model. Only reboot if the 3G interface fails to appear or cannot obtain an IP address after a failover.	81148

Release Notes

Resolved Issues

This section contains a list of resolved issues in the SonicOS Enhanced 5.5.2.0 release.

Anti-Spam

Symptom	Condition / Workaround	Issue
In rare cases, Anti-Spam service appears as unavailable.	Occurs when the Anti-Spam service shows as "Unknown" on the management interface's Anti-Spam > Status screen.	87075
The Anti-Spam service cannot perform IP reputation DNS lookups, or log events are created when it does so.	Occurs when DNS Rebinding attack prevention is enabled for either blocking or logging.	83648

Modem

Symptom	Condition / Workaround	Issue
A modem connected to the USB port fails to connect after the SonicWALL security appliance is rebooted.	Occurs if there is an active VPN tunnel when the appliance is rebooted.	81720

Multiple WAN Interfaces

Symptom	Condition / Workaround	Issue
In an active-passive load balancing configuration with probe monitoring, the secondary WAN interface is unable to maintain a steady connection after failover from the primary WAN interface.	Occurs when DNS resolution is being used. If a static IP address is set, this issue does not occur.	82779

Networking

Symptom	Condition / Workaround	Issue
A user is unable to modify or delete access rules.	Occurs when a UTM's bandwidth management settings are not correctly initialized for dial-up interfaces.	85096
A UTM appliance drops some management traffic when coming through a tunnel interface.	Occurs when management traffic such as "HTTP Management" and "HTTPS User Login" are dropped by the UTM, when the user attempts to manage the UTM through a tunnel interface.	82326

Release Notes

Single Sign On

Symptom	Condition / Workaround	Issue
The Single Sign-On (SSO) configuration is not synchronized from the primary appliance to the backup appliance in a Stateful High Availability (HA) pair.	Occurs when failover occurs in a HA pair where the primary appliance has SSO configured.	82791
SSO fails to work after new firmware is uploaded to the appliance.	Occurs when uploading new firmware to an appliance with SSO enabled. Workaround: Disable SSO before booting the new firmware and then re-enable it afterwards.	82781

SSL VPN

Symptom	Condition / Workaround	Issue
The UTM should disable TLS renegotiation based on an SSL VPN issue.	Occurs when the HTTPS server enables TLS renegotiation for SSL VPN traffic.	85724

VoIP

Symptom	Condition / Workaround	Issue
VoIP calls occasionally drop after reaching 10 minutes in length.	Occurs when a SonicWALL log shows a VoIP call disconnecting due to a SIP update method that was previously not supported.	85724
Some VoIP calls cannot last more than 30 seconds.	Occurs when a call is placed from an Avaya IP PBX using two record routes and is sent out through a SonicWALL UTM.	83381

Wireless

Symptom	Condition / Workaround	Issue
SonicPoint device continues to display "reboot" status after reboot is completed.	Occurs when a profile is not provisioned to a SonicWALL device, preventing the device status from progressing past initialization.	84899
Additional radio types can associate when radio mode "N-only" is set in the management interface.	Occurs when 802.11 b/g clients are still able to associate even with the radio type set to "N-only."	83537
Clients lose connection to a SonicPoint after a number of days.	Occurs when the SonicPoint-N is running an outdated version of the OS. The SonicPoint-N must be rebooted after losing client associations.	83390
Wireless clients sometimes do not receive DHCP leases.	Occurs when a DHCP offer is sent by the UTM, but is not received by the client, when the SonicPoint is in b/g/n mixed mode with auto-channel.	82239

Release Notes

Upgrading SonicOS Enhanced Image Procedures

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

Obtaining the Latest SonicOS Enhanced Image Version.....	7
Saving a Backup Copy of Your Configuration Preferences.....	7
Upgrading a SonicOS Enhanced Image with Current Preferences.....	7
Importing Preferences to SonicOS Enhanced 5.5.....	8
Importing Preferences from SonicOS Standard to SonicOS Enhanced 5.5	8
Support Matrix for Importing Preferences.....	10
Upgrading a SonicOS Enhanced Image with Factory Defaults.....	11
Using SafeMode to Upgrade Firmware	11

Obtaining the Latest SonicOS Enhanced Image Version

To obtain a new SonicOS Enhanced 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 Enhanced image file to a directory on your management station.

You can update the SonicOS 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 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.

Upgrading a SonicOS Enhanced 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 Enhanced firmware image file from 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 Enhanced 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 Enhanced image version information is listed on the System > Settings page.

Release Notes

Importing Preferences to SonicOS Enhanced 5.5

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

- 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 a SonicOS Enhanced 5.5.1.x 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 Enhanced maintenance release available on MySonicWALL.

Importing Preferences from SonicOS Standard to SonicOS Enhanced 5.5

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 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.

Release Notes

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

Upgrading a SonicOS Enhanced 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 Enhanced firmware image file from 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 Enhanced 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 login page.
7. Enter the default user name and password (admin / password) to access the SonicWALL management interface.

Using SafeMode to Upgrade Firmware



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. The reset button is in a small hole next to the USB ports.
 - 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 Enhanced 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 Web site.

The screenshot shows the SonicWALL Support Documentation website. The header includes the SonicWALL logo and the tagline "PROTECTION AT THE SPEED OF BUSINESS.™". A navigation menu contains links for HOME, PRODUCTS, SOLUTIONS, HOW TO BUY, SUPPORT (highlighted), TRAINING & EVENTS, COMPANY, and PARTNERS. A "Login to MySonicWALL" button is in the top right. The main content area features a large heading "SUPPORT DOCUMENTATION" and a sub-heading "PRODUCT GUIDES, TECH NOTES, FAQs & SUPPORT RELEASE NOTES". Below this is a "START" button and a navigation bar with "DOCUMENTATION" (highlighted), "SUPPORT CASES", "DOWNLOADS", "USER FORUMS", and "KNOWLEDGE BASE". A "Documentation by Product" section has a dropdown menu. Two tables list "Recent PRODUCT GUIDES" and "Recent TECHNICAL NOTES". A left sidebar contains various support resources and services.

Documentation by Product

Select a product to view its available documentation...

Recent PRODUCT GUIDES [more Product Guides >>](#)

#	Date	Description
1	16 Sep 2009	SonicOS Enhanced 5.5 Active/Active UTM Feature Module
2	14 Aug 2009	SonicWALL SSL VPN 3.5 User's Guide
3	13 Aug 2009	SonicWALL SSL VPN 3.5 Administrator's Guide
4	09 Aug 2009	SonicOS Enhanced 5.5 Single Sign-On Feature Module
5	06 Aug 2009	SonicOS Enhanced 5.5 Layer 2 Bridge Bypass Feature Module

Recent TECHNICAL NOTES [more Technical Notes >>](#)

#	Date	Description
1	22 Jul 2009	GMS Licensing for Windows and UMA EM5000
2	02 Jul 2009	Leveraging LDAP Groups/ Users with SonicWALL UTM Appliance
3	01 Jun 2009	SonicWALL TZ 100/200 Safety and Regulatory Information
4	26 Feb 2009	Transferring SonicWALL GMS from a Windows server to a SonicWALL UMA
5	05 Dec 2008	CDP 5.0 SQL Backup and Restore
6	05 Dec 2008	CDP 5.0 SQL Backup and Restore
7	05 Dec 2008	CDP 5.0 Authorative Restore
8	05 Dec 2008	CDP 5.0 Demonstration of Backing up and Restoring SQL
9	02 Dec 2008	Creating a Database Maintenance Plan for SQL Server 2005
10	22 Nov 2008	CDP 5.0 Active Directory Backup Algorithm
11	22 Nov 2008	CDP 5.0 AB CDP Exchange Error

Last updated: 3/16/2010