

SonicOS Enhanced EFT 4.0.1.0 Release Notes For TZ 180 and TZ 190 Series

SonicWALL, Inc.

Firmware Release: November 9, 2007

CONTENTS

PLATFORM COMPATIBILITY
KNOWN ISSUES
RESOLVED KNOWN ISSUES
KEY FEATURES
ENHANCEMENTS
UPGRADING SONICOS STANDARD/ENHANCED IMAGE PROCEDURES
RELATED TECHNICAL DOCUMENTATION

PLATFORM COMPATIBILITY

SonicOS Enhanced version 4.0.1.0 is a supported release for the following platforms:

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

Strong SSL and TLS Encryption Required in Your Browser

The internal SonicWALL Web server now 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 these 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, click on the Advanced tab, and scroll to the bottom of the Settings menu. In Firefox, go to Tools > Options, click on the Advanced tab, and then click on the Encryption tab.

KNOWN ISSUES

The following are known issues in SonicOS Enhanced 4.0.1.0:

Network

- **52578: Symptom:** The status of the WWAN does not change from 'Available - Active' back to 'Failover' after failing back to the WAN. **Condition:** Occurs when using the Modem as the WWAN failover interface when Preempt is enabled.
- **52539: Symptom:** A PPPoE client always uses the same DNS server as the PPPoE server, even when a different DNS server is specified. **Condition:** Occurs when PPPoE is selected as the IP Assignment for the WAN interface in the Network > Interfaces page, and a different DNS server is specified for the Specify DNS Server setting.
- **50917: Symptom:** The Web management connection can be lost even though ports 80 and 443 still allow HTTP or HTTPS connections. **Condition:** Occurs when IPS is enabled on the LAN/WAN zone while a medium/high level of detectable scans or attacks is running.

Wireless

- **51557: Symptom:** On the Wireless > Security page, after configuring WEP Encryption and clicking Apply, the page indicates that WPA encryption is configured. **Condition:** Occurs when using the Firefox browser, apparently due to a Firefox caching issue.
- **50134: Symptom:** Association to a SonicPoint with WPA-EAP security fails. **Condition:** Occurs when RADIUS requests from the SonicPoint to LAN RADIUS server are dropped. **Workaround:** Manually create the related access rule to all the RADIUS traffic from the SonicPoint to the LAN RADIUS server.

VPN

- **50411: Symptom:** When using DHCP over VPN, a client computer on the remote VPN network cannot renew its DHCP lease after the gateway is restarted. **Condition:** Occurs when the gateway on the DHCP server side is restarted after the VPN tunnel is established.
- **50257: Symptom:** "Remote VPN Networks" are not advertised on corresponding interfaces when using summary addresses. **Condition:** Occurs when individual local subnets are not manually defined, but instead are defined through summary addresses. Summarized subnets are not advertised even when the "Advertise Remote VPN Network" option is enabled.

Apple Macintosh Users and Single Sign-On

- Single Sign-On utilizes Windows APIs that are not supported by the Apple Macintosh, hence Mac users in a Windows environment will not get authenticated automatically by Single Sign-On. Mac users must log in to the appliance using a Web browser in order to get access when authentication is required. Note that this may require setting additional policy rules that would not otherwise be required with Single Sign-On, such as to allow access to external DNS servers.

Anti-Spyware

- **46218: Symptom:** Anti-Spyware enforcement fails when spyware traffic is passed from DMZ to WLAN. **Condition:** Occurs when Anti-Spyware service is enabled on both WLAN and DMZ zones.

CLI

- **45309: Symptom:** An SSH session with an invalid IP address cannot be removed. **Condition:** Occurs when using SSH to attempt a connection with an invalid IP address. Specifically, this can occur when using Tera Term Pro 3.1 to connect and disconnect. The session cannot be removed by **clear ssh all**, **clear ssh ID** or **disable ssh**, **enable ssh**.

GAV

- **46355: Symptom:** GAV IMAP sometimes fails to catch virus attached to email. **Condition:** Occurs when GAV IMAP fails to catch the virus when bad email (with virus attached) sits between good emails.

Networking

- **49411: Symptom:** In transmitted IP packets that are subject to QoS control, the packet classification field is not set to the right value by the SonicWALL. **Condition:** Occurs when DCSP marking is set to Preserve, and the 802.1p marking is set to Map in a LAN > WAN rule. The DCSP value in the packets that are sent from the LAN is set to 8, Class Selector = 1. VLAN user priority = 4. Packets captured on the WAN show VLAN priority 4. The VLAN priority is not changed to 1 as it should be according to the QoS mapping table.
- **49099: Symptom:** The number of dropped packets can be incorrectly displayed as 11922944 when bandwidth management is enabled. **Condition:** Occurs when only outbound bandwidth management is configured on the Ethernet BWM tab in the Firewall > Access Rules > Add Rule dialog box.
- **48977: Symptom:** After changing the LAN IP address and subnet, the DHCP server configuration for the LAN zone is not updated accordingly, preventing a client computer from receiving a DHCP address on the LAN. **Condition:** Occurs when the changes are made while connected to the X0 (LAN zone) interface. **Workaround:** Make the LAN IP address and subnet changes while connected to the WAN interface using HTTP/HTTPS management.
- **45010: Symptom:** One-to-one NAT policy works with LAN but doesn't work with DMZ interface. **Condition:** Occurs when using LAN-DMZ mixed bridge mode.
- **44972: Symptom:** Primary and secondary interfaces can have sub-interfaces configured with the same VLAN ID. **Condition:** Occurs when creating a sub-interface for both interfaces in a bridged pair, and then assigning the same VLAN ID to both sub-interfaces. The bridged pair might be WAN-LAN (X1-X2) or LAN-DMZ (X3-X4).

RESOLVED KNOWN ISSUES

The following issues are resolved in SonicOS Enhanced 4.0.0.2:

Networking

- **51172: Symptom:** Tasks are suspended and the firewall may restart when long value is configured in a DHCP Option object that is bound to the DHCP server. **Condition:** Occurs when a DHCP client attempts to obtain an IP address from a DHCP server that has a DHCP Option object with a long host name (255 characters).

Users

- **51677: Symptom:** SonicOS reports a critical warning: "VPN Client entry is not in tree", followed by a General Protection Fault. **Condition:** Occurs when LAN/WLAN-side GVC clients are triggered to automatically connect when a Web browser request is made to the WAN.

Wizards

- **51550: Symptom:** The error log pop-up window displays "Data out of bounds" errors when an attempt is made to edit or disable certain NAT policies. **Condition:** Occurs when the NAT policies were created by the Public Server Wizard, for example when creating an FTP Server behind the firewall.

The following issues were resolved in SonicOS Enhanced 4.0.0.1:

CFS

- **50341: Symptom:** The SonicWALL sometimes reboots unexpectedly. **Condition:** Occurs when allocating or freeing memory from the heap during HTTPS access. May be related to use of Application Firewall feature.

CLI

- **50453: Symptom:** Attempting to change the SSH port causes the SonicWALL to reboot. **Condition:** Occurs when attempting to change the SSH port either in the CLI or on the System > Administration page in the user interface. After rebooting, the SSH port is changed if the CLI was used, but not if the UI was used.
- **49918: Symptom:** In the CLI, the command **show address-object** will cause the SonicWALL to reboot. **Condition:** Occurs when the command is executed right after uploading firmware and clicking the boot icon for **Uploaded Firmware with Factory Default Settings**.

Users

- **50489: Symptom:** Single sign-on users may get redirected to log in to the appliance when the agent is using WMI on a busy network. **Condition:** Occurs when the network response time is slow and the default Single Sign-On timeout is set. **Workaround:** Increase the SSO timeout to something longer than the default of 3 seconds.
- **50118: Symptom:** Some features are not working properly for Limited or Non-Config mode admin users. **Condition:** Occurs when a Limited Admin attempts to make a change on the Log > Automation or Log > Syslog pages, or clicks **Flush ARP Cache** on the Network > ARP page, and when a Non-Config Admin clicks **Flush ARP Cache** on the Network > ARP page. An error message saying "not allowed in current mode" will be reported, and the operation may or may not be successful.

- **50108: Symptom:** User sessions are sometimes disconnected after only one or two minutes for users who are members of a local group that corresponds to an Active Directory group and has a group-based access policy for another LAN segment. **Condition:** Occurs when Single Sign-On is being used.

VoIP

- **49914: Symptom:** Back to Back User Agent: SonicOS Enhanced 4.0 firmware cannot consistently handle transfer calls and conference calls in different network zones. **Condition:** Occurs when more than two calls are transferred or conferenced to a different zone.
- **49912: Symptom:** Back to Back User Agent: A “Network Busy” error message may be displayed, or a call may be connected to the recipient’s voicemail rather than ringing their phone when making phone calls. **Condition:** Occurs when calls are made using IP phones between one LAN and another LAN interface.
- **49884: Symptom:** Back to Back User Agent: Outgoing calls result in a “Network Busy” error message, and incoming calls may be connected to the recipient’s voicemail rather than ringing their phone. **Condition:** Occurs when calls are made using IP phones with SIP (Session Initiation Protocol) in the following cases:
 - Outgoing calls from the LAN to the DMZ
 - Incoming calls from the DMZ to the LAN

KEY FEATURES

This section describes key features in SonicOS Enhanced 4.0.0.2, including features that were introduced in SonicOS Enhanced 4.0.0.0 and 4.0.0.1.

The following feature was introduced in SonicOS Enhanced 4.0.0.1:

- Password Constraint Enforcement** – Password Constraint Enforcement provides the ability to set and enforce constraints on user and administrator passwords and allows users to change their own passwords. The Password Constraint Enforcement feature meets requirements for both Common Criteria and the Payment Card Industry Data Security Standard.

SonicOS provides configuration settings for password expiration, minimum length, complexity (use of numeric or symbolic characters), and reuse. The constraints apply only to local users and administrators whose passwords are configured on the appliance rather than through LDAP or RADIUS. Once the settings are configured, the built-in administrator password must meet the requirements. Administrators can set non-conforming passwords for other local users, but those users will be prompted to change their passwords upon their next login.

New fields in the SonicOS management interface have been added to support Password Constraint Enforcement, as shown below.

The System > Administration page contains the following new fields:

The Enforce password complexity drop-down list includes the following options:

The Add User / Edit User dialog box contains the following new checkbox to force users to change their passwords the next time they log in:

Settings Groups VPN Access

User Settings

Name:

Password:

Confirm Password:

User must change password

Comment:

For Web users, a **Change Password** button has been added to the User Login screen and User Login Status windows.

User Login screen:

SonicWALL - User Password Update

SONICWALL COMPREHENSIVE INTERNET SECURITY™

Password update needed!

Your password has expired and must be changed before you can log in.
Please enter a new password.

New Password:

Confirm New Password:

Change Password Cancel

Administrative user login status window:

SonicWALL - User Login Status - Microsoft I...

Bob, you now have access to privileged services.
- You have limited firewall management capabilities

Clicking the logout button below will terminate those privileges. You have a maximum login session time of 30 minutes. For security reasons you may choose to limit your remaining session time to a lower value below.

Limit remaining login time to (mins) 30 Update

Login session time remaining (mins): 30

SONICWALL Change Password Manage Logout

Non-administrative user login status window:



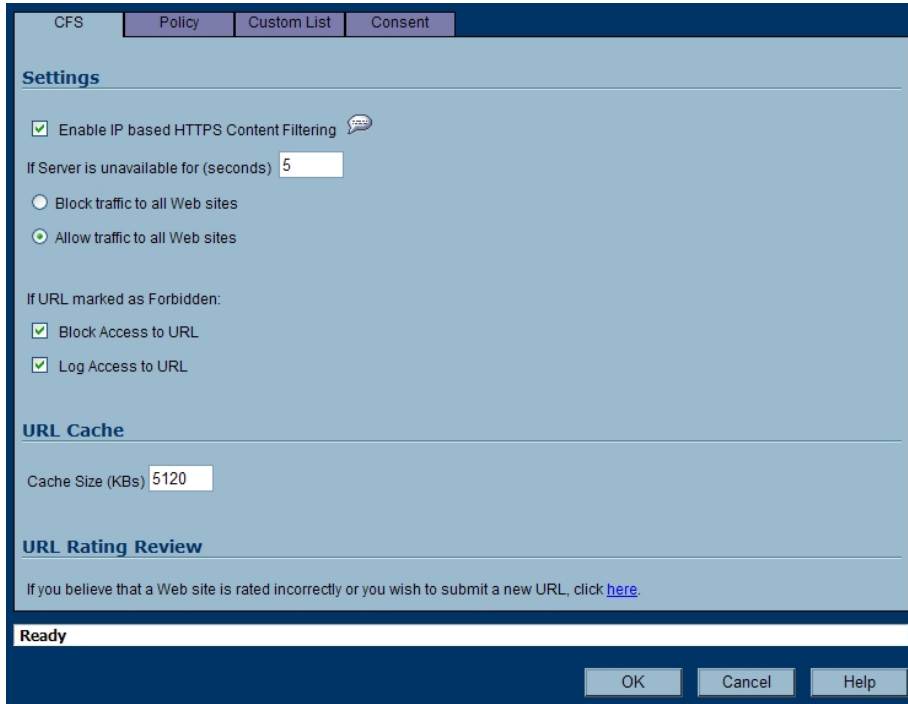
The following features were introduced in SonicOS Enhanced 4.0.0.0:

- **Single Sign-On User Authentication** – Single Sign-On User Authentication provides privileged access to multiple network resources with a single workstation login. Single Sign-On uses the SonicWALL SSO Agent to identify user activity based on workstation IP addresses. Access to resources is based on policy for the group to which the user belongs.
- **HTTPS Filtering** – HTTPS Filtering allows 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 that 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.



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

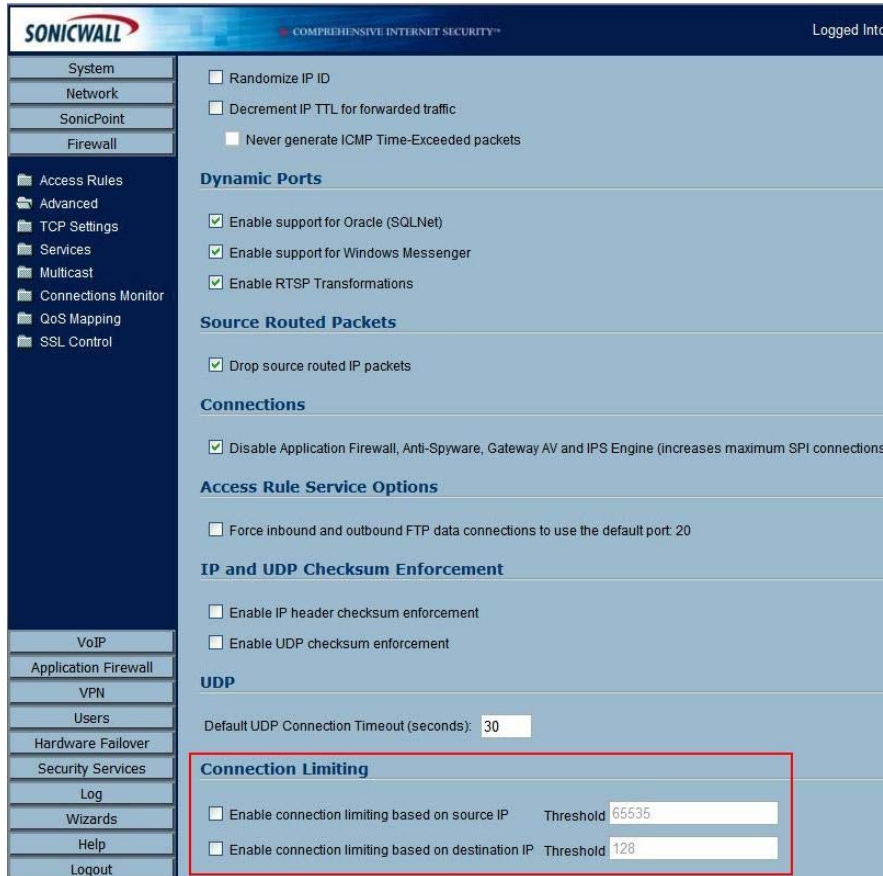


- **SSL Control** – SSL Control is a system that provides visibility into the handshake of Secure Socket Layer (SSL) sessions, and a method for configuring policies to control the establishment of SSL sessions.



- **Certificate Blocking** – Certificate Blocking in SonicOS Enhanced provides a way to specify which HTTPS certificates to block. This feature is closely integrated with SSL Control.
- **Inbound NAT Load Balancing with Server Monitoring** – Inbound NAT Load Balancing with Server Monitoring detects when a server is unavailable and stops forwarding requests to it. Inbound NAT Load Balancing spreads the load across two or more servers. When Stateful High Availability (Stateful Hardware Failover) is configured in the environment, during a failover SonicOS forwards all requests to the alternate server(s) until it detects that the offline server is back online. Additionally, inbound NAT Load Balancing can be used to provide redundancy or load balancing for multiple SonicWALL SSL-VPN appliances.
- **Security Dashboard Web Page** – The Security Dashboard page in the user interface displays a summary of threats stopped by the SonicWALL security appliance. The Security Dashboard shows two types of reports:
 - A Global Report that displays a summary of threat data received from all SonicWALL security appliances worldwide.
 - An Individual Appliance Report that displays a summary of attacks detected by the local SonicWALL security appliance.
- **License Wizard** – As part of the Security Dashboard, the License Wizard is available for both firewall registration and the purchase of security service licenses. The available security services are the same as those that enable Global Reports by providing threat data from SonicWALL devices around the world.
- **Multiple SSH Support** – Multiple concurrent SSH sessions are supported on the SonicWALL security appliance. When connected over SSH, you can run command line interface (CLI) commands to monitor and manage the device. The number of concurrent SSH sessions is determined by device capacity. Note that only one session at a time can configure the SonicWALL, whether the session is on the GUI or the CLI (SSH or serial console). For instance, if a CLI session goes to the config level, it will ask you if you want to preempt an administrator who is at config level in the GUI or an SSH session.
- **Multiple and Read-only Administrator Login** – Multiple Administrator Login provides a way for multiple users to be given administration rights, either full or read-only, for the SonicOS security appliance. Additionally, multiple users can concurrently manage the appliance, but only one user at a time can be in config mode with the ability to change configuration settings. This feature applies to both the graphical user interface (GUI) and the command line interface (CLI).

- IP-Based Connection Limit** – The IP-Based Connection Limit feature provides a way to limit the number of connections on a per-source or per-destination IP address basis. This feature protects against worms on the LAN side that initiate large numbers of connections in denial of service attacks.



- IKEv2 Secondary Gateway Support** – IKEv2 Secondary Gateway Support provides a way to configure a secondary VPN gateway to act as an alternative tunnel end-point if the primary gateway becomes unreachable. While using the secondary gateway, SonicOS can periodically check for availability of the primary gateway and revert to it, if configured to do so. Configuration for the secondary VPN gateway is available under VPN > Settings > Add Policy in the management interface.

- **IKEv2 Dynamic Client Support** – IKEv2 Dynamic Client Support provides a way to configure the Internet Key Exchange (IKE) attributes rather than using the default settings. Previously, only the default settings were supported: Diffie-Hellman (DH) Group 2, the 3DES encryption algorithm, and the SHA1 authentication method. SonicOS now allows the following IKE Proposal settings:
 - DH Group: 1, 2, or 5
 - Encryption: DES, 3DES, AES-128, AES-192, AES-256
 - Authentication: MD5, SHA1

These settings are available by pressing the Configure button in the VPN > Advanced screen of the management interface. However, if a VPN Policy with IKEv2 exchange mode and a 0.0.0.0 IPsec gateway is defined, you cannot configure these IKE Proposal settings on an individual policy basis.

Note that the VPN policy on the remote gateway must also be configured with the same settings.

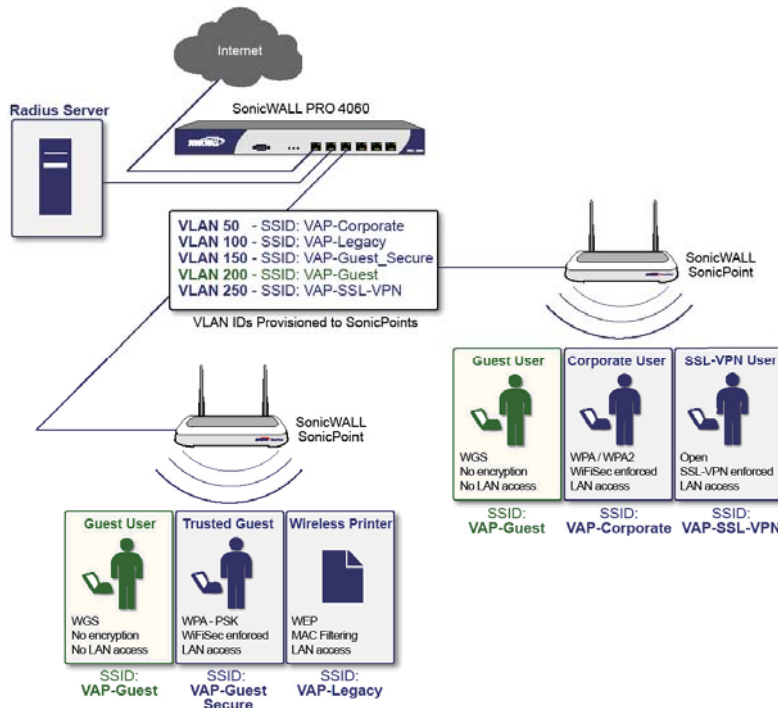
- **Wireless IDS Rogue Detection** – Wireless intrusion detection is supported on SonicPoint devices. Wireless IDS Rogue Detection allows you to configure a set of authorized access points, defined by address object groups. If contact is attempted from an unauthorized access point, SonicOS generates an alert.
- **RF Management** – Radio Frequency Management is supported on SonicPoint devices. RF Management provides detection of eleven types of wireless threats:
 - Long duration attack
 - Management frame flood
 - Null probe request
 - Broadcasting de-authentication
 - Valid station with invalid SSID
 - Ad-Hoc station
 - Unassociated station
 - Wellenreiter attack
 - NetStumbler attack
 - EAPOL packet flood
 - Weak WEP IV
- **SMTP Authentication** – SMTP Authentication as detailed in RFC 2554 defines an SMTP service extension that allows the SMTP client to indicate an authentication method to the server, perform an authentication protocol exchange, and optionally negotiate a security layer for subsequent protocol interactions. This feature helps prevent viruses that attack the SMTP server on port 25.
- **Generic DHCP Option Support** – Generic DHCP configuration allows vendor-specific DHCP options in DHCP server leases.
- **DHCP Server Lease Cross-Reboot Persistence** – DHCP Server Lease Cross-Reboot Persistence provides the ability to record and return to DHCP server lease bindings across power cycles. The SonicWALL security appliance does not have to depend on dynamic network responses to regain its IP address after a reboot or power cycle. This feature is supported on all SonicWALL PRO platforms. It is not supported on SonicWALL TZ platforms.
- **Custom IP Type Service Objects** – Support for Custom IP Type Service Objects allows administrators to augment the pre-defined set of Service Objects.

- **Dynamic Address Objects** – Two changes to Address Objects are supported:
 - **MAC** – SonicOS Enhanced will resolve MAC AOs to an IP address by referring to the ARP cache on the SonicWALL.
 - **FQDN** – Fully Qualified Domain Names (FQDN), such as ‘www.sonicwall.com’, will be resolved to their IP address (or IP addresses) using the DNS server configured on the SonicWALL. Wildcard entries are supported through the gleaning of responses to queries sent to the sanctioned DNS servers.

- **Virtual Access Points** – A “Virtual Access Point” (VAP) is a multiplexed instantiation of a single physical Access Point (AP) so that it presents itself as multiple discrete Access Points. To wireless LAN clients, each Virtual AP appears to be an independent physical AP, when there is actually only a single physical AP. Before Virtual AP feature support, wireless networks were relegated to a one-to-one relationship between physical Access Points and wireless network security characteristics, such as authentication and encryption. For example, an Access Point providing WPA-PSK security could not simultaneously offer Open or WPA-EAP connectivity to clients. If Open or WPA-EAP were required, they would need to have been provided by a separate, distinctly configured APs. This forced WLAN network administrators to find a solution to scale their existing wireless LAN infrastructure to provide differentiated levels of service. With the Virtual APs (VAP) feature, multiple VAPs can exist within a single physical AP in compliance with the IEEE 802.11 standard for the media access control (MAC) protocol layer that includes a unique Basic Service Set Identifier (BSSID) and Service Set Identified (SSID). This allows segmenting wireless network services within a single radio frequency footprint of a single physical access point device.

In SonicOS Enhanced 4.0.0.0 and higher, VAPs allow the network administrator to control wireless user access and security settings by setting up multiple custom configurations on a single physical interface. Each of these custom configurations acts as a separate (virtual) access point, and can be grouped and enforced on single or multiple physical SonicPoint access points simultaneously.

You can configure up to eight VAPs per SonicPoint access point.



ENHANCEMENTS

The following enhancements are included in SonicOS Enhanced 4.0.0.0 and higher:

- **Enhanced Packet Capture** – Enhanced Packet Capture contains improvements in both functionality and flexibility, including the following:
 - Capture control mechanism with improved granularity for custom filtering
 - Display filter settings independent from capture filter settings
 - Packet status indicating dropped, forwarded, generated, or consumed
 - Three-window output in the user interface that provides the packet list, decoded output of selected packet, and hexadecimal dump of selected packet
 - Export capabilities that include text, HTML, hex dump, and CAP file format
 - Automatic buffer export to FTP server when full
 - Bidirectional packet capture based on IP address and port
 - Configurable wrap-around of capture buffer when full
- **User Authentication** – There are a number of enhancements to user authentication, including optional case-sensitive user names, optional enforcement of unique login names, support for MSCHAP version 2, and support for VPN and L2TP clients changing expired passwords (when that is supported by the back-end authentication server and protocols used). Note that for this purpose there is a new setting on the VPN > Advanced page to cause RADIUS to be used in MSCHAP mode when authenticating VPN client users.
- **IP Helper Scalability** – Enhancements to the IP Helper architecture support large networks. Improvements include changes to DHCP relay and Net-BIOS functionality. DHCP relay over VPN is now fully integrated.
- **Diagnostics Page Tool Tips** – Self-documenting mouse-over descriptions for diagnostic controls are provided in the graphical user interface.
- **BWM Rate Limiting** – The Bandwidth Management feature is enhanced to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables modem bandwidth management in cases where the primary WAN link fails over to a secondary modem connection that cannot handle as much traffic.
- **DHCP Client Reboot Behavior Control** – Enhancements to DHCP Client Reboot Behavior controls allow you to configure the WAN DHCP client to perform a DHCP RENEW or a DHCP DISCOVERY query when attempting to obtain a lease. The previous behavior was to always perform a RENEW, which caused lease failures on some networks, particularly certain cable modem service providers. The new behavior is to perform a DISCOVERY, but it is configurable. A checkbox has been added to the Network > Interfaces > WAN > DHCP Client page:
 - **Enabled:** when the appliance reboots, the DHCP client performs a DHCP RENEW query.
 - **Disabled:** (Default) when the appliance reboots, the DHCP client performs a DHCP DISCOVERY query.
- **Dynamic Route Metric Recalculation Based on Interface Availability** – To better support redundant or multiple path Advanced Routing configurations, when a default-route's interface is unavailable (due to no-link or negative WAN LB probe response), that default route's metric will be changed to 255, and the route will be instantly disabled. When a default-route's interface is again determined to be available, its metric will be changed back to 20, and the route will be non-disruptively enabled.

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

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.

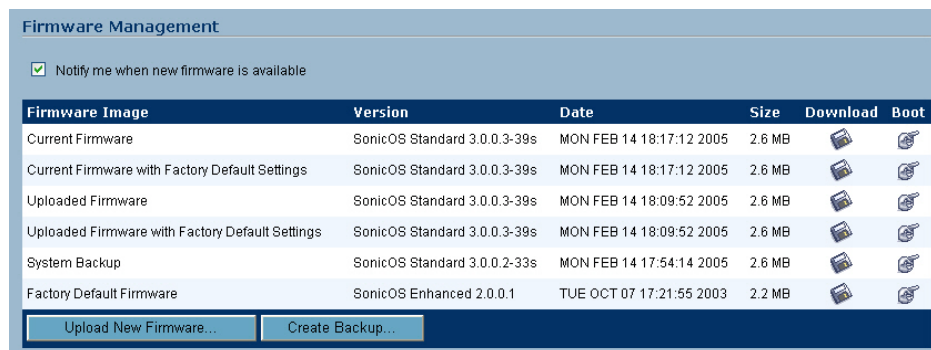
Saving a Backup Copy of Your Configuration Preferences


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 PRO 2040, SonicWALL PRO 3060, SonicWALL PRO 4060, SonicWALL PRO 4100, or SonicWALL PRO 5060, 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.




- 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.



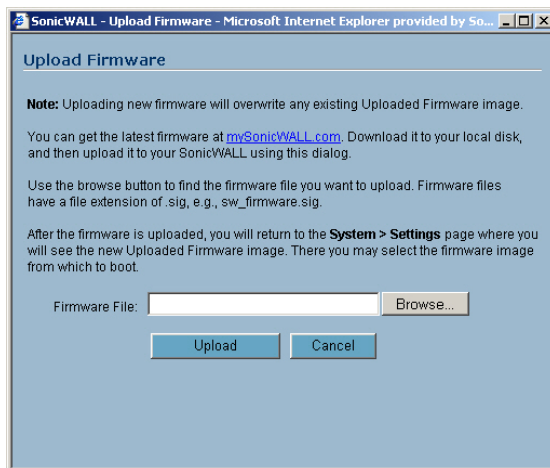
Tip: Rename the .exp file to include the version of the SonicOS Standard/Enhanced image from which you are exporting the settings. For example, if you export the settings from the SonicOS Standard 3.0 image, rename the file using the format: [date]_[version]_[mac].exp to "021605_3.0.0.6-27s_000611223344.exp"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

- Download the SonicOS Standard/Enhanced image file from mysonicwall.com and save it to a location on your local computer.
- 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.



- 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!

- 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.

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:

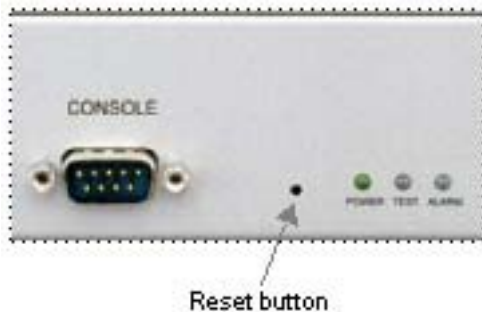
1. Connect your management station to a LAN port on the SonicWALL security appliance and configure your management station IP address with an address on the 192.168.168.0/24 subnet, such as 192.168.168.20.



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.*

- 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.

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

System Information



Product Name:	PRO 4060
Serial Number:	0006B1026C78
Authentication Code:	78CR-SAEF
ROM Version:	SonicROM 3.1.0.2
CPU Type:	2.0GHz Intel Processor
Total Memory:	256MB RAM, 64MB Flash
Uptime:	0 Days 00:00:24
System Time:	WED JAN 31 22:05:39 2007 GMT

[Run Diagnostics...](#) [View Boot Log...](#)

Firmware Management

Firmware Image	Version	Date	Size	Download	Boot
Current Firmware	SonicOS Enhanced 4.0.0.0-21e	WED JAN 31 22:05:39 2007 GMT	4.86 MB		
Current Firmware with Factory Default Settings	SonicOS Enhanced 4.0.0.0-21e	WED JAN 31 22:05:39 2007 GMT	4.86 MB		
Uploaded Firmware	SonicOS Enhanced 4.0.0.0-21e	WED JAN 31 16:44:04 2007 GMT	4.86 MB		
Uploaded Firmware with Factory Default Settings	SonicOS Enhanced 4.0.0.0-21e	WED JAN 31 16:44:04 2007 GMT	4.86 MB		
System Backup	SonicOS Enhanced 4.0.0.0-3e	MON NOV 06 23:00:50 2006 GMT	4.79 MB		
Factory Default Firmware	SonicOS Enhanced 2.5.0.1	WED JUN 16 04:00:51 2004 GMT	3.45 MB		

[Upload New Firmware...](#) [Create Backup...](#)

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**.

RELATED TECHNICAL DOCUMENTATION

SonicWALL user guide 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.

WORLDWIDE | NORTH AMERICA SEARCH SITE MAP

SONICWALL

HOME PRODUCTS SOLUTIONS HOW TO BUY SUPPORT COMPANY PARTNERS MY SONICWALL

« GO BACK TO

TZ 190 SERIES APPLIANCES PRODUCT SUPPORT

SUPPORT RESOURCES

SELF-SERVE HELP

- » Downloads
 - Firmware
 - Setup Tool
 - Signatures
- » User Forums
- » Knowledge Portal

OPEN A SUPPORT CASE

- » Web
- » Telephone
- » Partner

REFERENCE LIBRARY

- » Product Guides
- » Tech Notes
- » FAQs
- » Release Notes

OTHER SERVICES

- » Support Services
 - Support & Consulting Services
 - Dynamic Support Reference Guide
- » Training & Certification
- » Consulting Services

STAY IN TOUCH

RECENT PRODUCT GUIDES

#	Date	Description
1	19 Jun 2007	SonicOS Enhanced 3.8 Administrator's Guide
2	14 May 2007	SonicWALL TZ 190 Getting Started Guide
3	13 Nov 2006	SonicOS Enhanced 3.6 Administrator's Guide
4	10 Mar 2006	Configuring VoIP for SonicOS Enhanced 3.2

RECENT TECHNICAL NOTES

#	Date	Description
---	------	-------------

RECENT SERVICE BULLETINS

#	Date	Description
---	------	-------------

RECENT FAQs

#	Date	Description
---	------	-------------

RECENT RELEASE NOTES

#	Date	Description
1	25 Jun 2007	SonicOS Enhanced 3.8.0.4 TZ 190 Series Release Notes
2	10 May 2007	SonicOS 3.6.0.4 Enhanced Release Notes
3	06 Mar 2007	SonicOS Enhanced 3.6.0.2 Release Notes
4	08 Dec 2006	SonicOS Enhanced 3.6.0.1 Release Notes
5	08 Nov 2006	SonicOS Enhanced 3.6.0.0 Release Notes

Document Version: November 9, 2007

Page 20 of 20

