

## SonicOS Enhanced 3.1.0.14 Release Notes

SonicWALL, Inc.

Software Release: December 30, 2005

### CONTENTS

---

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

### PLATFORM COMPATIBILITY

---

SonicOS Enhanced version 3.1.0.14 is a supported release for the following platforms:

SonicWALL PRO 5060
SonicWALL PRO 4100
SonicWALL PRO 4060
SonicWALL PRO 3060
SonicWALL PRO 2040
SonicWALL PRO 1260
SonicWALL TZ 170 SP
SonicWALL TZ 170 W
SonicWALL TZ 170 SPW
SonicWALL TZ 170

SonicWALL Secure Wireless features are supported on the SonicOS Enhanced version 3.1.0.14 release for management of the following SonicWALL Wireless access points.

- SonicWALL SonicPoint
- SonicWALL SonicPoint G

The SonicOS Enhanced 3.1.0.6 release was the initial software release to support management of the SonicWALL SonicPoint G platform.

### KEY FEATURES

---

#### SonicOS Enhanced 3.1 Feature Highlights

The following list provides feature highlights:

- **Anti-Spyware**—Analyzes inbound connections for the most common method of spyware delivery, ActiveX-based component installations. 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 reset 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.
  - Operates with other anti-spyware programs, such as applications that remove existing spyware applications from hosts, to provide an added measure of defense against spyware.
- **SYN Flood Protection**—SYN Floods are a common form of denial of service attack launched against IP-based hosts. They are designed to incapacitate the target by exhausting its resources with illegitimate TCP connections. SonicOS Enhanced provides improved SYN Flood protection engine to safeguard protected systems from such attacks.  
Key features of SonicWALL's SYN Flood protection engine include:
    - **Layer 2 SYN Flood Protection (SYN-Blacklisting)**—Applies to all interfaces, and is designed to protect internally launched SYN Flood attacks, as well as severe attacks from higher-speed WAN networks.
    - **Layer 3 SYN Flood Protection (SYN-Proxy)**—Applies to WAN interfaces to defend internal public systems from attacks launched by Internet-based hosts.
    - **Automatically Computed and Continuously Updated Thresholds for Detection and Dynamic, Event-Triggered Defense Fortification**—SYN-Proxy mode can be dynamically activated in response to a recognized attack, ensuring that legitimate traffic is processed even in the midst of an attack.
    - **SonicWALL Management Traffic Prioritization**—Ensures SonicWALL security appliances can always process inbound management traffic (i.e. Web management GUI, GMS, dynamic routing information) even while attack countermeasures are being taken.
    - **Precise Controls**—Provides precise controls of TCP MSS (Maximum Segment Size) and SACK (Selective ACKnowledgement) TCP options when operating in SYN-Proxy mode.
    - **Extensive Statistical Reporting and Event Logging**—SYN Flood Protection provides extensive event logging information for generating reports and administrator alerts.
  - **Source-Destination IP Persistence for WAN Load Balancing**—Provides granular WAN load balancing based on the source and destination IP. The SonicWALL security appliance determines which WAN to use for communication from one PC to a given destination IP address emanating from the same WAN.
  - **SonicPoint Dynamic Subnet Addressing**—Allows more flexible IP subnet masking by specifying the number of SonicPoints that will be connected to an interface assigned to the WLAN. This declaration will then dynamically determine the maximum allowable subnet mask size.
  - **Online Certificate Status Protocol (OCSP) Support**—Allows the SonicWALL security appliance to use the newer, real-time scheme for maintaining digital certificate status. The OCSP standard supersedes the Certificate Revocation List (CRL).

## ENHANCEMENTS

---

- **37364:** Added CFS IP Exclusion list to exclude individual IP addresses or ranges of IP addresses from CFS enforcement.
- **36546:** Added new checkbox to the VPN > Certificates page to invalidate certificates and SAs if CRL fetch or processing fails.
- **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

---

### Log

- **37135: TCP IP Layered-Data Packet Processing and SonicOS Log Event Handling**  
In specific cases of multi-layer packet processing, a TCP connection initially logged as "open," will be rejected by a deeper layer of packet processing. In these cases, the connection request has not been forwarded by the SonicWALL security appliance, and the initial Connection Open SonicOS log event message should be ignored in favor of the TCP Connection Dropped log event message.

### CLI

- **34019:** Known issue with the Command-Line Interface (CLI) not supporting all the sections of the Technical Support Report (TSR) using the **show tsr** command.

### Network

- **37307: Symptom:** TCP connections are dropped during session establishment. **Condition:** When TCP Stateful inspection is enabled, the SonicWALL will only allow perfectly ordered 3 way handshakes. Any deviation from this, such as retransmitted packets during the handshake, will result in the connection being dropped. **Workaround:** From the 'Firewall > TCP Settings' page, disable TCP Stateful Inspection.
- **37213: Symptom:** After enabling OSPF on a secondary LAN, the primary LAN behind the SonicWALL security appliance becomes inaccessible. **Condition:** Occurs when OSPF settings are configured for redistribution of network routes.
- **37362: Symptom:** A host relocated from the WAN segment to a transparently configured segment will fail to communicate with the upstream router. **Condition:** if a host is connected to the WAN segment, and is in the ARP cache of the upstream router (or other WAN segment device) relocating that host to a segment behind the SonicWALL that is configured for transparent operation will result in a stale entry in the ARP cache of the upstream router. This is because the SonicWALL does not pass the gratuitous ARP that is generated by the client. **Workaround:** Flush the ARP cache (or remove the relevant individual ARP cache entry) on the upstream router.

- **39327: Symptom:** Enabling IP Helper on a SonicWALL 170 Wireless when the WAN interface is configured for DHCP might prevent the WAN interface from obtaining a DHCP lease. **Condition:** Occurs when IP Helper is enabled on a SonicWALL 170 Wireless and the device is rebooted. **Workaround:** Assign a static IP address to the interface, apply the settings, and then change it back to DHCP.

## Services

- **37205: Symptom** – Access to certain web-sites is blocked when the Gateway Anti Virus “Restrict Transfer of password protected ZIP files” option is enabled. **Condition:** It is possible for the Gateway Anti Virus password protected Zip detection to classify gzip compressed HTTP content as password protected ZIP content. **Workaround:** Disable “Restrict Transfer of password protected ZIP files”.

## System

- **36706: Symptom:** The diagnostic tool, Active Connections Monitor causes a SonicWALL security appliance to lock up. **Condition:** Occurs on a SonicWALL security appliance running 40,000 TCP connections when the administrator goes to System>Diagnostics>Active Connections Monitor. **Workaround:** Avoid using the Active Connections Monitor in deployments with a large number of simultaneous TCP connections.
- **39350: Symptom:** Enabling IP Helper with a NetBIOS policy configured for a destination on the Encrypted Zone (VPN) might cause a SonicWALL 4060 to become unresponsive or to reboot several times a day. **Condition:** Occurs when VPN hardware acceleration is disabled, or when VPN processing is assumed by software due to excessive traffic loads. **Workaround:** Disable the VPN bound IP Helper NetBIOS policy.

## VPN

- **27863:** If a VPN policy uses “Any Address” as the local network, and the corresponding VPN policy uses “Route All” as the destination network, then the Internet traffic cannot pass through the VPN tunnel.
- **28427:** The SonicWALL security appliance may not be able to consistently send an IKE SA Delete message when an Active VPN Policy is disabled.
- **30232:** Mismatched IKE IDs on two peers configured for Main Mode IKE VPN Policies will not properly log an Invalid ID Info event.
- **30245: Symptom:** Missing access rule for VPN connection. **Condition:** Occurs when two VPN policies are configured on the SonicWALL security appliance. The local network for both policies is the same group address object, Local LAN and Custom Zone. Originally the VPN policies had destination networks selected, but the configuration was modified for DHCP relay, selected the ‘Destination network obtains IP addresses using DHCP through VPN tunnel’ checkbox. The only auto-added access rule was for VPN > LAN, with source ‘VpnDhcpClients’ and destination ‘LAN and Custom Zone.’ When the VPN policies were reconfigured to have destination networks again, only one auto-added access rule was listed in VPN > LAN and LAN > VPN.
- **34115:** If the remote gateway of a DHCP over VPN setup has DHCP clients on an interface other than X0, inbound DHCP over VPN connections for remote gateway DHCP clients fail.

- **35883: Symptom:** When SonicWALL security appliance receives a QM request from a Site-to-Site VPN gateway peer, it also initiates a QM itself. Both QMs are negotiated resulting in traffic being dropped. **Condition:** The local gateway receives the IPSec Del message and QA request from the remote gateway and initiates a QM as well, which results in two Phase 2 negotiations and the traffic from the local gateway being dropped.
- **36456: Symptom:** If you define an address object after you add a VPN policy, newly created access rules are not created. **Condition:** Load SonicOS Enhanced 3.1.0.11 firmware and boot with factory default settings, configure LAN and WAN interfaces, add a Site-to-Site VPN policy, select Firewalled Subnets as your local network. Configure a subinterface with the DMZ zone assignment and configure the OPT interface with Custom zone assignment. The DMZ > VPN, VPN > DMZ, Custom > VPN, and VPN > Custom access rules are not created.

## Wireless/SonicPoints

- **31592:** In accordance with the Transmit Power Control (TPC) and Dynamic Frequency Selection (DFS) requirements mandated by the European Telecommunications Standards Institute (ETSI) 301-893 for countries in the European Union, International versions of the SonicPoint will experience boot times of approximately 5 minutes as the SonicPoint scans for radio interference along the available 5GHz frequency spectrum.

## RESOLVED KNOWN ISSUES FOR SONICOS ENHANCED 3.1.0.14

---

This section contains a list of resolved known issues provided by the SonicOS Enhanced 3.1.0.14 release, which was released on December 30, 2005.

### Detection and Prevention

- **37218: Symptom:** SonicWALL security appliances did not block Skype's asymmetric key exchange over HTTP. **Condition:** Occurs when Skype's 3-way handshake fails.

### System

- **39312: Symptom:** A SonicWALL TZ series security appliance stops passing traffic even through 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.

### Users

- **39396: Symptom:** GVC cannot negotiate a DHCP lease, but the user session remains active. **Condition:** Occurs when connecting GVC from behind a NAT device to a peer gateway that is configured for PPPoE.

## RESOLVED KNOWN ISSUES FOR SONICOS ENHANCED 3.1.0.12

---

This section contains a list of resolved known issues provided by the SonicOS Enhanced 3.1.0.12 release, which was released on December 12, 2005.

### High Availability

- **39127: Symptom:** A device configured for WAN Load Balancing experiences intermittent spontaneous restarts. **Condition:** WAN Load Balancing statistic calculations are being performed on an invalid interface.

### Log

- **37547: Symptom:** The SonicWALL security appliance reports a "Possible Port Scan Dropped" message. **Condition:** Occurs when a connection from a LAN to a WAN is terminated by the WAN host.
- **38858: Symptom:** Manual changes to the system clock are not reported in the log. **Condition:** Occurs when NTP is disabled and the time and date is manually changed.
- **38859: Symptom:** A SonicWALL security appliance logs traffic on IP protocols that should not be allowed as being allowed; however, the traffic is not allowed. **Condition:** Occurs when traffic is received on IP protocols 2, 47, 88, 89, and 103.
- **38900: Symptom:** ICMP "TTL exceeded" packets are incorrectly logged as if the ICMP packet is a DNS packet from the router. **Condition:** Occurs when ICMP "TTL exceeded" packets are generated by a router in response to a DNS packet with a short TTL.

## Networking

- **37474: Symptom:** A SonicWALL PRO 4060 drops inbound ESP packets. **Condition:** Occurs when inbound ESP packets pass through an access rule that allows a group service containing ESP.
- **38051: Symptom:** A SonicWALL PRO 5060 locks up and stops passing traffic. **Condition:** Occurs when the IP Helper is enabled with NetBios and DHCP, and no NetBios policy is configured.
- **38861: Symptom:** A SonicWALL security appliance inappropriately allows SYN+PSH+RST packet, which is in invalid combination. **Condition:** Occurs when a valid SYN packet is received followed by an invalid SYN+PSH+RST packet.
- **38542: Symptom:** Windows Active Directory GPO Propagation fails over a Site-to-Site VPN connection. **Condition:** Occurs when at least one of the SonicWALL security appliances in a Site-to-Site VPN uses a PPPoE DSL connection.
- **38863: Symptom:** ICMP "TTL exceeded" packets can be captured and replayed through the SonicWALL security appliance. Only one ICMP "TTL exceeded" packet should be allowed through for each outbound packet. **Condition:** Occurs when multiple ICMP "TTL exceeded" packets are sent to the SonicWALL security appliance.
- **38864: Symptom:** When an outbound TCP packet is sent with a spoofed source IP address, the SonicWALL security appliance replies with an RST packet to the spoofed IP address. **Condition:** Occurs when outbound rules are set to "discard."
- **39148: Symptom:** A SonicWALL SonicPoint crashes in standalone mode. **Condition:** Occurs when a SonicWALL SonicPoint in stand-alone mode is managed by its web GUI from a host connected over a VPN tunnel.
- **39211: Symptom:** DNS queries from LAN to DMZ configured for Transparent mode fail to receive replies under heavy DNS traffic loads. **Condition:** Occurs when SIP Transformation are enabled.

## Services

- **35730: Symptom:** When the HTTP escape sequences are used, keywords within the URL are not blocked. **Condition:** The SonicWALL CFS Forbidden Keywords blocking feature does not filter keywords within the URL.
- **36265: Symptom:** Firmware upgrade fails, SonicOS management UI becomes unresponsive and selected firmware file for upload does not display. **Condition:** Firmware upgrade fails if the SonicWALL security appliance has multiple services enabled (including GMS, Network Anti-Virus, IPS, and Content Filtering Service (CFS)).

## System

- **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.

## VPN

- **37412: Symptom:** 'IPSec Replay Detected' message are logged, and VPN connections are dropped and re-established. **Condition:** Under extremely heavy VPN loads, the hardware accelerated VPN queue could become full, and VPN packets will begin taking a synchronous software path until the hardware queue is available. This could result in VPN packets being delivered out of order, and if this extends beyond the order window threshold of 64 packets, the packets will be dropped as replay packets.
- **38300: Symptom:** VPN fails to reestablish after changing the dynamic WAN IP address during renegotiation of the PPPoE session after being disconnected. **Condition:** Occurs after a PPPoE connection is established with a dynamic IP address and then attempting to create a VPN connection to a remote location.
- **39019: Symptom:** A SonicWALL security appliance incorrectly drops a quick mode negotiation message and sends an INVALID-COOKIE message. **Condition:** Occurs when the peers' lifetime for the IKE SA is set higher than the SonicWALL's.
- **39079: Symptom:** DHCP packets relayed over a VPN tunnel from a remote network connected by a non-SonicWALL VPN device could cause the SonicWALL device to stop passing traffic.
- **39247: Symptom:** IKE negotiations do not begin when the SonicWALL security appliance transitions from HA idle to HA active. **Condition:** Occurs when a SonicWALL security appliance with keepalives enabled transitions from the backup state (HA idle) to the primary state (HA active.)
- **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/SonicPoints

- **39020: Symptom:** When attempting to import a preference file into a SonicWALL with SonicPoints attached to it, the import operation fails. **Condition:** This occurs when the SonicPoint Profile configured with a schedule object or Access Control List (ACL) object.

## RESOLVED KNOWN ISSUES FOR SONICOS ENHANCED 3.1.0.11

---

This section contains a list of resolved known issues provided by the SonicOS Enhanced 3.1.0.11 release, which was released on October 7, 2005.

### Log

- **37780: Symptom:** Syslog packets generated from the secure appliance have Time To Live (TTL) values that are too low. **Condition:** The TTL value for these packets was increased from 15 to 64.
- **37780: Symptom:** Syslog packets generated from the SonicWALL security appliance do not reach the Syslog server if the server is located more than 15 hops away. **Condition:** Previously, the Syslog packets have a Time To Live (TTL) value of 15 and this value has been increased to 64 to cover the cases where the Syslog server is located more than 15 hops away from the SonicWALL.

## Network

- **38807: Symptom:** After you initially configure the WAN Interface to use PPTP, any subsequent attempts to modify Point-to-Point Protocol (PPTP) settings (username, password, IP addressing, etc) results in the unit locking up when you try to apply the changes. Changing PPTP WAN settings caused the secure appliance to lock or reboot. **Condition:** This occurs after you initially configure the WAN interface and attempt to modify PPTP settings.
- **38393: Symptom:** An interoperability failure occurs between a SonicWALL secure appliance and an LDAP server that uses the Samba schema. **Condition:** This occurs when an LDAP server is configured to use a Samba schema.
- **37724: Symptom:** While trying to enable the Hardware Failover feature with the Static PPPoE WAN Connections, the system displays an incorrect error message:

### **HF is not supported with dynamic WAN IP assignment or transparent mode.**

**Condition:** This occurs while trying to enable the Hardware Failover feature on a SonicWALL that has a Static PPPoE WAN connection. Currently, the Hardware Failover feature is supported when the SonicWALL is configured in NAT mode with a static IP address. The Hardware Failover feature cannot be enabled when the WAN interface is configured with dynamic IP address assignment: PPPoE (dynamic/static) or in Transparent Mode.

- **37708: Symptom:** An L2TP/IPSec client coming from behind a NAT device fails to negotiate the quick mode connection with the SonicWALL. **Condition:** This occurs because a misaligned access when processing the NAT 0A payload when an L2TP/IPSec client coming from behind a NAT device tries to negotiate a quick mode tunnel.
- **37660: Symptom:** A Bandwidth Management-enabled traffic stream receives less bandwidth than the expected value in instances when the configured guaranteed bandwidth value is less than the Maximum Bandwidth value. **Condition:** This occurs in instances where a single Bandwidth Management enabled rule is configured for the FTP traffic with a guaranteed bandwidth value of 2 percent and a maximum bandwidth value of 100 percent. In this scenario, the traffic without the Bandwidth Management enabled receives more bandwidth than the FTP traffic with the bandwidth management enabled. With this configuration, FTP should be receiving 100 percent bandwidth at all times since it is the only traffic for which bandwidth management is enabled.
- **37482: Symptom:** The SonicWALL does not send an ARP for an IP address which was on the DMZ port when the WAN – DMZ port is in transparent mode. **Condition:** This occurs when the WAN – DMZ port is in transparent mode.
- **37277: Symptom:** A Cisco VPN Client version 4.0.2 coming from behind a SonicWALL cannot connect to the Cisco concentrator. **Condition:** This occurs when the NAT traversal is enabled on the SonicWALL and the Cisco client behind the SonicWALL tries to connect to the Cisco concentrator. During this process, the response packets are fragmented and arrive out of order. Also the IP reassembly is not performed properly, leading to failure of connection cache entry and subsequent NAT translation.

- **37133: Symptom:** The SonicWALL WAN interface configured with the PPPoE client does not automatically reconnect once the connection is rejected by the PPPoE server. **Condition:** This occurs when the PPPoE authentication fails during the process of PPPoE connection establishment. The timer which forces the PPPoE client to reconnect gets stopped after the PPPoE Active Discovery session confirmation packet is received. In instances when the authentication fails, the retry does not occur. However, if there is traffic from the LAN interface, the PPPoE client tries to reconnect again and the PPPoE connection is established.
- **37217: Symptom:** A security appliance incorrectly sends SNMP traps after renegotiating a tunnel. Activant expects SNMP traps to be sent only when a tunnel is truly down and not just when the user renegotiates it. **Condition:** This occurs after the security appliance renegotiates a tunnel. This behavior has been corrected, and so now the unit sends SNMP traps only when the tunnel is truly down and not when it is renegotiated.
- **36172: Symptom:** A management session generated from behind a NAT device is redirected to a valid SonicWALL management IP address and port number. **Condition:** This scenario occurs when a user behind a NAT device using HTTP requires the HTTPS login for LDAP/RADIUS authentication. Then this user was redirected to HTTPS on the SonicWALL's Local (private) IP address and the session failed.

## Services

- **38662: Symptom:** Users behind the SonicWALL with the Content Filtering System (CFS) enabled are unable to access Hotmail and few other sites. **Condition:** This occurs when CFS is enabled on the SonicWALL and is then configured to use an external Web Proxy Server which does not comply with TCP RFC 1323.
- **38776: Symptom:** Some PRO 5060 and PRO 4060 secure appliances could not download the latest GAV signatures. **Condition:** This can occur in instances when the SonicWALL WAN IP address is changing and at the same time, the unit tries to download the signatures.
- **37393: Symptom:** A distributed policy associated with an active Global Security Client (GSC) connection incorrectly becomes Active on the LAN hosts causing the disconnection of the applications running on these hosts. **Condition:** This occurs when the GSC is enforced on the VPN Zone and the SonicWALL Security Appliance is rebooted.
- **35597: Symptom:** When enabling the Email Filtering feature, the emails become garbled or encoded. When you disable the feature, the emails appear correctly. **Condition:** This issue occurs in Microsoft Word 2.0.0.3, which has smart tags enabled.
- **36750: Symptom** – Password protected ZIP files are allowed through even when disabled on Gateway Anti Virus. **Condition:** The Zip 2.0 encryption method is not currently recognized by Gateway Anti Virus. (*Standard and Enhanced*).

## System

- **38048: Symptom:** SonicWALL reboots automatically and the log page displays a Diagnostics Code A error with tNetTask in the Notes column. **Condition:** This occurs when the Email Filtering feature is enabled on the SonicWALL, and during the process of Email scanning, an empty boundary string is encountered.

- **38002: Symptom:** When preferences are imported into both the TZ 170 SP and TZ 170 SPW, the modem interface zone assignment incorrectly changes from WAN to Unassigned. **Condition:** This occurs when the preferences are imported onto the TZ 170 SP and TZ 170 SPW running former versions 3.0.0.7 to 3.1.0.7.
- **37581: Symptom:** Creation of more than four users in GMS sometimes does not work properly. When users are successfully created in GMS, the passwords may not work. **Condition:** These problems are caused by the handling of passwords that are encrypted in preferences.
- **33481: Symptom:** SonicWALL security appliance locks up after manually loading the Certificate Revocation List (CRL) and then adding a local certificate. **Condition:** If the uploaded CRL size is larger than 2K, attempting to add a local certificate larger than this size locks the unit.

## Users

- **38525: Symptom:** When the SonicWALL is configured to use RADIUS, the user privilege attributes are not correctly reported in the RADIUS test that appears in the RADIUS Configuration Window in the **User > Settings** page. **Condition:** This occurs only in a RADIUS test after configuring user privileges on a RADIUS server.
- **37296: Symptom:** Users cannot authenticate to the RADIUS server using RSA tokens. **Condition:** This occurs when the User Level Authentication (ULA) is enabled and the users are configured to be authenticated from a RADIUS server with SecureID. This fails because the SonicWALL is not sending back the new PIN challenge response.
- **35236: Symptom:** When the user authentication occurs through the Novell LDAP Server 6.5, the group membership attributes for a user are not returned properly. **Condition:** This occurs when the User Level Authentication (ULA) is enabled on the SonicWALL and the authentication occurs through the Novell LDAP Server 6.5.

Note that the SonicWALL GUI is now updated to better support the Novell LDAP Server. On the Schema page, there is now an entry to select Novell eDirectory Schema. If the Novell eDirectory is selected, the domain component in entries on the Directory page is automatically changed to "o=". When changing from Novell back to any other schema, this value is changed to ".com".

## VPN

- **37922: Symptom:** DHCP-based Site-to-Site VPN tunnels, after a rekey, have an ARP management issue which affects access to hosts with static DHCP leases behind the remote secure appliance. **Condition:** The ARP management issue occurs only with hosts that have static DHCP leases and only after a rekey session.
- **37922: Symptom:** In the DHCP over VPN configuration the hosts behind the remote secure appliance loses network connectivity to the head-end secure appliance. **Condition:** This issue occurs when the hosts behind the remote site have Static DHCP leases and at the end of the IPsec Phase 2 lifetime.
- **37765: Symptom:** The head-end SonicWALL displays duplicate VPN security associations and Global VPN Client users with session times longer than the actual session time. **Condition:** This occurs when the remote SonicWALLs or the Global VPN clients which support only NAT Traversal draft version v00 coming from behind a NAT device are connected to the head-end SonicWALL.

- **37755: Symptom:** In a Site-to-Site DHCP over VPN configuration, the DHCP client behind the remote gateway cannot obtain an IP Lease if there are multiple networks in the list. **Condition:** This issue occurs when the DHCP server is located on a routed network on the head-end secure appliance, and when DHCP relay VPN uses the hub and spoke VPN type.
- **37288: Symptom:** If a Global VPN Client is configured with static IP, sometimes the connection creating the client applications running on the GVC host cannot connect to the server applications. **Condition:** This occurred when the GVC client is configured with static IP and the server application tries to connect to the client after a rekey because of an incorrect connection cache entry on the SonicWALL.
- **36628: Symptom:** Disconnected GVC remote VPN users remain in the Currently Active VPN Tunnels table. **Condition:** If a GVC session is not properly disconnected, the session might remain in the 'VPN > Settings > Currently Active VPN Tunnels' table. This is because GVC sessions, by design, do not time out. This condition should not affect performance unless there are thousands of orphaned sessions.
- **36890: Symptom:** VPN traffic is unaffected, but the SonicOS management UI displays more than one instance of the same SA under different VPN policies. **Condition:** When a VPN policy has more than one NAT-T SA and if the NAT-T port changes during the lifetime of the SA, the corresponding SA appears under multiple VPN policies.

## Wireless

- **38459: Symptom:** Wireless connectivity completely fails when the standalone SonicPoint device uses WEP. **Condition:** This occurs when the SonicPoint is in standalone mode.

## RESOLVED KNOWN ISSUES FOR SONICOS ENHANCED 3.1.0.8

---

This section contains a list of resolved known issues provided by the SonicOS Enhanced 3.1.0.8 release, which was released on September 15, 2005.

### High Availability

- **36338: Symptom:** Resolved an issue related to GUI allowing you to configure the HF Feature when the SonicWALL is in the Transparent Network Mode. **Condition:** This issue occurs when the SonicWALL is configured in the Transparent Network Mode and if trying to enable the Hardware Failover Feature. In the current firmware release, if the SonicWALL is configured in Transparent Network Mode, Hardware Failover Feature is not supported.
- **36904: Symptom:** When the SonicWALL security appliances are configured for Hardware Failover, the Backup SonicWALL (in idle state) eventually begins to lose memory over a period of time. **Condition:** Small portions of system memory are leaked out when the Primary SonicWALL (in Active state) attempts to perform a full synchronization of the preference files to the Backup SonicWALL in Idle state.

### Log

- **37164: Symptom:** Received the following SonicOS log event message:  

```
Reboot due to task suspension
```

**Condition:** Occurs during the syslog rendering of an IP address when you specify DNS name resolution to convert an IP address into a domain name.

### Network

- **37851: Symptom:** When Bandwidth Management (BWM) is enabled on a SonicWALL security appliance, disabling BWM results in an unresponsive and un-pingable SonicWALL security appliance. **Condition:** Occurs when BWM is enabled on the WAN interface, and BWM is disabled.
- **37287: Symptom:** Interface IP addresses are displaying 0.0.0.0. **Condition:** Occurs when configuring a Hardware Failover pair and rebooting to factory default settings.
- **37147: Symptom:** Oracle Dynamic Ports are unable to send traffic from DMZ to LAN zones. **Condition:** Occurs in network deployments where servers in the DMZ are sitting behind a SonicWALL security appliance in NAT mode. Configure Firewall > Access Rules > Advanced and select the Dynamic Oracle Ports checkbox.
- **36469: Symptom:** The NetBios broadcast packet TTL is set to 4 in the IP helper code if the TTL value is less than 4. **Condition:** Occurs when you enable a LAN to WAN NetBios broadcast IP helper policy. On the LAN, configure 'nbtstat -R' and 'nbtstat -a' on the host on the WAN. The TTL value of the NetBios outgoing packet displays 4. The TTL value of the same packet on LAN displays 128.
- **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.

- **36465: Symptom:** After disabling ingress Bandwidth Management (BWM) for a WAN interface the SonicWALL security appliance enters a deadlock state. **Condition:** Occurs while an administrator is configuring the SonicWALL security appliance to disable WAN ingress BWM from the SonicOS management console and ingress WAN traffic is coming in at the same time.
- **36582: Symptom:** Creating an AH Protocol object contains a defaults out of bounds error message:  
Error: . Data out of bounds (min = 1, max = 65535)  
**Condition:** Occurs when you configure Firewall > Services > Add Service, enter an object name, and select AH for the protocol.**36582: Symptom:** Creating an AHProtocol object contains a defaults out of bounds error message: **Condition:** Occurs when you configure Firewall > Services > Add Service, enter an object name, and select AH for the protocol.
- **36318: Symptom :** Resolved an issue where the SonicWALL PPPoE client is getting out of sync with the PPPoE Server when a PADT packet is being sent from the PPPoE Server. **Condition:** This issue occurs when the PPPoE server sends a PADT packet to terminate the PPPoE connection.
- **36313: Symptom:** Unable to nest MAC groups when access-control list (ACL) enforcement is enabled on SonicPoints. **Condition:** Occurs when you configure a MAC-based address object for a WLAN client, create an address object group, and assign the address object to this newly created address object group, enable ACL enforcement and allow the newly created address object group, and connect the WLAN client. Moving the address object to a nested group does not allow the WLAN client to associate.
- **36221: Symptom:** Deleting a PortShield interface whose auto-created address objects are being actively reference could result in an orphaned address object. **Condition:** Deleting a PortShield interface that is being reference by a VPN policy will result in a residual address object for "PortShield-<name> Subnet" that cannot be deleted.
- **33126: Symptom:** EIGRP inbound traffic failed despite correctly configured network access rule. **Condition:** After creating an EIGRP (IP Protocol 88) Service Object and creating a matching network access rule to allow EIGRP ingress traffic from WAN to LAN, the SonicWALL security appliance dropped the traffic even though Multicast traffic support is enabled.

## Services

- **37100: Symptom:** The SonicOS administration page is slow to respond with CFS Premium enabled on the SonicWALL security appliance. **Condition:** Occurs in extreme high traffic conditions, such as over 100 user Web usage, with content filtering enabled to block all site categories.
- **36700: Symptom:** In some situations SonicWALL GAV, Anti-Spyware, IPS security services signature updates fail to download. **Condition:** Occurs when there is a temporary disconnection from the Internet on the management network while a signature update download is in progress.
- **36121: Symptom:** Access to Websites is not blocked by CFS Category 49: Freeware/Software Download. **Condition:** After enabling CFS Premium security service, check the 'All Categories' checkbox to filter selected categories, visit <http://www.download.com/>. This site is not blocked by Category 49.
- **36509: Symptom:** Tarantella client applications are not able to connect to servers behind a SonicWALL security appliance. **Condition:** Occurs when CFS is enabled.

- **36341: Symptom:** CFS is not displaying a blocked site message entry to MAC OSX users. **Condition:** Occurs when you attempt to visit a CFS configured blocked site, such as <http://www.playboy.com>, CFS blocks the user from visiting the forbidden site, but does not display a blocked site message on browsers running on MAC OSX systems.
- **36243: Symptom:** GMS management tunnels to remote SonicWALL security appliances are not sending traffic across the VPN tunnel, but instead the traffic is being sent to non-management VPN tunnels where the remote SonicWALL security appliance is terminating the tunnel. **Condition:** Occurs when managing SonicWALL security appliances with GMS Proxy settings for remote devices.

## System

- **37118: Symptom:** After rebooting the SonicWALL security appliance, no syslog or SonicOS log events are displayed. **Condition:** Occurs during syslog encryption from the SonicWALL security appliance to the GMS server using HTTPS management.
- **36946: Symptom:** After enabling HTTPS management for the SonicWALL security appliance and then rebooting the system, the system is not manageable through HTTPS. **Condition:** Loss of the HTTPS management rule configuration occurs after a system reboot.
- **36122: Symptom:** Resolved an issue where the Primary SonicWALL while in Active state, goes into an idle state for a few seconds. **Condition:** This occurs during the process when the Active SonicWALL is trying to synchronize the full preferences to the Backup SonicWALL, which is in the Idle state.

## Users

- **36995: Symptom:** LDAP Authentication fails when using full Active Directory login names, for example, user@test.company.com. **Condition:** This issue occurs in situations where both parent and the child domains users have the same Active Directory Login name.
- **37007:** After configuring a URL to bypass user authentication in the User < Settings access rules page, TCP terminations are not completed properly to the external side. This results to systems on the external side to wait for a last TCP ACK message.
- **35866: Symptom:** Received the following SonicOS log event message:  
User login denied - LDAP schema mismatch  
**Condition:** Enter an invalid entry in your hierarchy tree of users, such as an invalid user name or password, and click the **Test** button.
- **36096: Symptom:** After reboot, configurations for User session settings are lost. **Condition:** Occurs when you configure the Users > Settings page, select the 'Enable login session limit' checkbox, click the Apply button, unselect the 'Show users login status' checkbox, and click the Apply button. When you refer back to the User > Settings page, the configured settings are not saved.

## VoIP

- **35554: Symptom:** SIP endpoints experience one-way media for inbound calls. **Condition:** Occurs when the SIP endpoint has not previously been registered with a SIP proxy.

## VPN

- **37187: Symptom:** ESP packets are sent with TCP header containing DF bit set. **Condition:** Configure a VPN tunnel as ESP with NULL encryption, and send traffic with DF bit set.
- **36566: Symptom:** The System > Certificates page displays imported and built-in CA certificates. This issue is specific to built-in CA certificates containing unintended, imported CA information details. **Condition:** Import CA certificates, import CRLs for the CA certificate, and mouse-over the pop-up for Certificate Details.
- **35755: Symptom:** Global VPN Clients trying to connect gets an error "failed to convert peer name to IP address." **Condition:** Occurs with preference files taken from SonicWALL 6.x.x.x firmware version.
- **36584: Symptom:** XAUTH fails when you configure GroupVPN policies and enable XAUTH for third-party VPN clients. **Condition:** Third party VPN clients using XAUTH fails if its public IP address is less than the SonicWALL WAN IP address.
- **36773: Symptom:** FTP sessions across zones, including VPN, fail. Other TCP sessions involving certain hosts intermittently fail. **Condition** – FTP stateful inspection incorrectly calculating the checksum on FTP retransmission packets, causing them to be dropped by certain FTP clients and servers. The intermittent failure of other TCP sessions is caused by TCP stateful inspection enforcing proper TCP handshake sequences. **Workaround** – Some TCP implementations do not employ proper TCP handshaking. To support these devices, disable 'TCP Stateful Inspection' on the 'Firewall > TCP Settings page'. **Enhancement** – A series of descriptive log events have been added to indicate when TCP stateful inspection drops aberrant TCP traffic.
- **36569: Symptom:** DHCP client becomes unresponsive after retransmitting a DHCP REQUEST message. **Condition:** Occurs when you have configured the DHCP client on the WAN interface of the SonicWALL security appliance. After the DHCP client acquires a DHCP lease, disconnect the DHCP server from the network, when the DHCP client tries to renew the lease by sending a DHCP REQUEST on 50% of the lease time. The first DHCP REQUEST message is sent properly, but subsequent retransmitted messages caused the DHCP client to become unresponsive.
- **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.
- **36434: Symptom:** SonicWALL security appliances unexpectedly reboots after the administrator deletes or adds unused auto-created network address objects and static routes. **Condition:** Occurs when adding or deleting network address objects assigned to a group object that is used with VPN destination targets.

## Wireless

- **36464: Symptom:** Traffic from a wireless client is unable to reach the SonicPoint connecting to the PortShield WLAN interface if ingress BWM management is enabled. **Condition:** Occurs when egress and ingress BWM is enabled on the WAN interface.

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

### Obtaining the Latest SonicOS Enhanced Image Version

1. To obtain a new SonicOS 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 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 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:

- 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.

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

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

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

- 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.



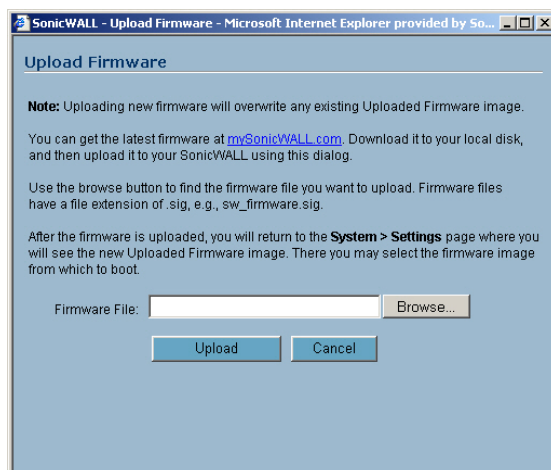
**Tip:** Rename the .exp file to include the version of the SonicOS Standard/Enhanced image from which you are exporting the settings. For example, if you export the settings from the SonicOS Standard 3.0 image, rename the file using the format: [date]\_[version]\_[mac].exp to "021605\_3.0.0.6-27s\_000611223344.exp" (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 the image update booting process will take between one and two minutes, and a warning not to power off the device while the image is being uploaded to the flash memory. Click **OK** to proceed.
5. After successfully uploading the image to your SonicWALL security appliance, the login screen is displayed. Enter your user name and password. Your new SonicOS Standard/Enhanced image version information is listed on the **System > Settings** page.

## Upgrading a SonicOS Standard/Enhanced Image with Factory Defaults

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

### Uploaded Firmware with Factory Defaults – New!


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

## Resetting the SonicWALL Security Appliance Using SafeMode


If you are unable to connect to the SonicWALL security appliance's management interface, you can restart the SonicWALL security appliance in SafeMode. The SafeMode feature allows you to quickly recover from uncertain configuration states with a simplified management interface that includes the same settings available on the **System > Settings** page.

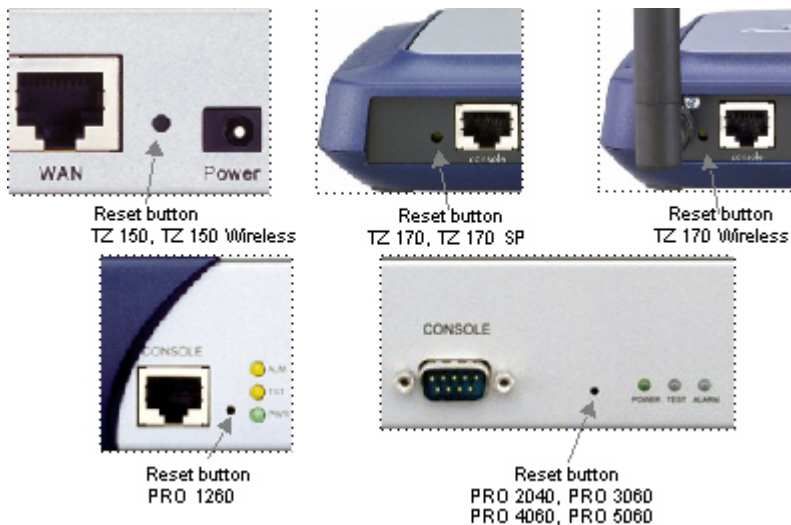
To reset the SonicWALL security appliance, perform the following steps:

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

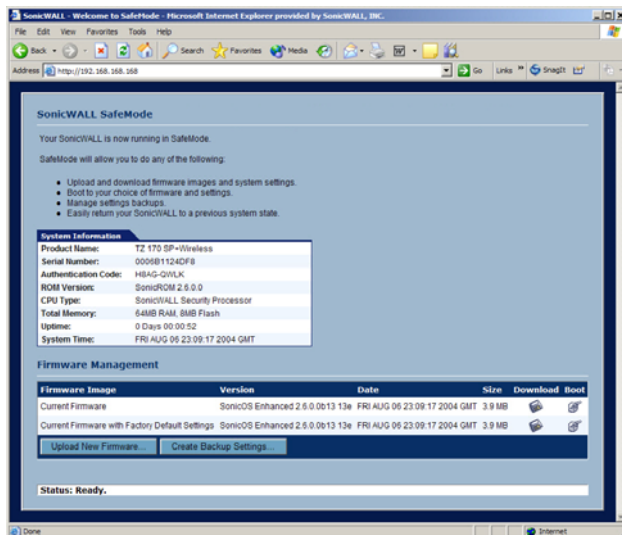
2. Use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the reset button on the back of the security appliance for five to ten seconds. The reset button is in a small hole next to the console port or next to the power supply, depending on your SonicWALL security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

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**.

## 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 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:** December 30, 2005