Release Notes

SonicOS | **SonicOS 6.1.1.4 NSA 3600/4600/5600/6600 Release Notes**

Contents

Release Purpose

SonicOS 6.1.1.4 is a maintenance release that fixes a number of known issues.

Platform Compatibility

The SonicOS 6.1.1.4 release is supported on the following Dell SonicWALL appliances:

- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600

The Dell SonicWALL WXA series appliances (WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are supported for use with Dell SonicWALL NSA appliances running 6.1.1.4. The recommended WXA firmware version is WXA 1.2.1.

WXA 1.1.1 will work with SonicOS 6.1.1.4, but you will not be able to see or use the new features in WXA 1.2.1.

Upgrading Information

For information about obtaining the latest firmware, upgrading the firmware image on your Dell SonicWALL appliance, and importing configuration settings from another appliance, see the *SonicOS 6.1 Upgrade Guide* available on MySonicWALL or on the www.sonicwall.com Product Documentation page for the NSA series:

http://www.sonicwall.com/us/en/support/3643.html

Browser Support

SonicOS uses advanced browser technologies such as HTML5, which are supported in most recent browsers. Dell SonicWALL recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of SonicOS. This release supports the following Web browsers:

- Chrome 18.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 16.0 and higher
- Internet Explorer 8.0 and higher (do not use compatibility mode)
- Safari 5.0 and higher

Mobile device browsers are not recommended for Dell SonicWALL appliance system administration.

Known Issues

This section contains a list of known issues in the SonicOS 6.1.1.4 release.

Certificates

Symptom	Condition / Workaround	Issue
Auto-import CRL via http does not work for revoking certificates.	Occurs when you add a certificate, then on the import CRL popup page, select **Periodically auto-import CRL via HTTP**, enter a valid HTTP URL for CRL download, and click the **Apply** button.	129379

DPI-SSL

Symptom	Condition / Workaround	Issue
The CFS block page is not displayed for a blocked HTTPS website, although the site is correctly blocked and the attempt is logged.	Occurs when **Enable SSL Client Inspection** and **Content Filter** are selected on the DPI-SSL > Client SSL page, and a Content Filter policy is configured to block a site category that uses HTTPS, such as for online banking. When a user accesses a banking website, it is blocked and the attempt is logged, but the CFS block page does not appear.	123676
DPI-SSL does not take effect for a wireless guest user. The certificate from the remote server is not rewritten using the designated certificate.	Occurs when guest services are enabled on the WLAN zone and a guest user logs in and attempts to access a website using HTTPS, such as https://mail.google.com.	123097

High Availability

Symptom	Condition / Workaround	Issue
The Active firewall in a Stateful HA pair does not synchronize all VPN connections to the Standby firewall.	Occurs when many VPN tunnels are up, all bound to a certain interface, and fully synchronized, then the interface goes down on the Primary firewall. The Primary firewall begins deleting the tunnels and also synchronizing with the Secondary, then a failover occurs before all tunnels are deleted and the Stateful Sync finishes. The Primary continues deleting the rest of the tunnels, but cannot sync with the Secondary because it is no longer the Active firewall. The Secondary is left with a number of active VPN tunnels, but does not sync them to the Primary unless the tunnel configuration is changed.	131211

Log

Symptom	Condition / Workaround	Issue
The first two pages of log events are not displayed in the Log View table.	Occurs when the Items count above the Log View table indicates that many items exist, such as a hundred or more, and Items per Page is set to show 50 at a time. The appliance is configured with an imported OCSP certificate, WANGroupVPN enabled, and third party with OCSP enabled.	132048

Networking

Symptom	Condition / Workaround	Issue
The firewall cannot connect with the PPTP server.	Occurs when configuring a WAN zone interface in PPTP mode, and a wrong password is entered along with other correct settings. After correcting the password, the PPTP connection still fails.	134038
FTP connections fail after a Stateful HA failover when using Wire Mode over Link Aggregation. The FTP session will time out or can be flushed from the Dashboard > Connections Monitor page, then a new FTP session can be established.	Occurs when Wire Mode over Link Aggregation (such as X6(X7) to X10(X11)) is configured on a Stateful HA pair, and a failover occurs while FTP traffic is running. One switch is connected to X6(X7) and another switch is connected to X10(X11), with PC's connected to both switches and FTP traffic running between the PC's. After the failover, the FTP session hangs when any command is entered.	132278
A test virus is logged, but not blocked when using Wire Mode over Link Aggregation.	Occurs when an anchor port is down, in Secure mode. Wire Mode is configured from LAN to LAN, X2 and X8. Link Aggregation (LAG) configuration is: X2: X3,X6,X7 and X8: X9,X10,X11, with static LAG between two switches connected to these ports. Initially, a virus sent from a PC on one switch to a PC on the other switch is blocked. After X2 is shut down administratively, the next virus transfer is logged, but not blocked.	129955

System

Symptom	Condition / Workaround	Issue
Certain buttons on the AppFlow > Dashboard and System > Diagnostics screens do not function correctly.	Occurs when viewing Intrusions on AppFlow > Dashboard and clicking the IPS signature for details. The details are blank. On the System > Diagnostics screen with Connections Monitor selected, clicking the button to display the connections also displays a blank area.	133816
A 3rd party certificate cannot be selected, and the VPN tunnel that uses the 3rd party certificate for authentication cannot come up.	Occurs when the VPN Policy is configured and then the appliance is upgraded to 6.1.1.4. After upgrading, the Local Certificate drop-down list is empty in the VPN Policy screen, preventing the local certificate from being selected.	133697

User Interface

Symptom	Condition / Workaround	Issue
A JavaScript error window is displayed by the browser during GMS management configuration.	Occurs when using Internet Explorer 9 to manage the appliance, with the “Display a notification about every script error” option enabled under Internet Options > Advanced. After selecting “Enable management using GMS” on the SonicOS System > Administration page, clicking the Configure button causes the error window to display.	131990

Users

Symptom	Condition / Workaround	Issue
For Single Sign-On authentication, NTLM does not work on Linux (Fedora and Firefox) computers. Instead of NTLM prompting for name and password, the browser redirects to the user authentication page.	Occurs when NTLM is configured to be tried before the Single Sign-On agent, or NTLM is selected as the only SSO method. The **Simple usernames in local database** checkbox is enabled. With no user logged in through the appliance, a new browser is used to browse to a WAN-side web server. The user should be prompted for credentials, but is not.	129835
The LDAP User/Group Trees Auto-configure request fails and the console prints a stack trace.	Occurs when you open the LDAP configuration window from the “LDAP is selected for user group lookup for RADIUS/SSO users:” side, and then click the **Auto-configure** button and select **Append to existing trees**/**Replace existing trees**. **Workaround**: Open the LDAP configuration window from the User authentication method.	129383

VoIP

Symptom	Condition / Workaround	Issue
The firewall drops SIP packets from WAN to LAN (on a bridged LAN interface).	Occurs when: 1. X0 was already configured as LAN with default gateway IP of 192.168.50.1 2. Configure X5(LAN) to X0 in L2 bridge mode 3. Connect a Cisco phone on the LAN side of the X5 interface with IP 192.168.50.13(gateway is 192.168.50.1) 4. As the proxy is already on WAN, make a call from Cisco phone connected to the bridged LAN interface(X5) to a phone on the WAN side. 5. The call should be established, but WAN to Bridged LAN(X5) SIP packets are dropped by the firewall.	128225

VPN

Symptom	Condition / Workaround	Issue
VPN tunnels associated through a port redundancy group on an HA pair go down when the primary interface in the port redundancy group fails.	Occurs when the tunnels are initiated from an HA pair which is also configured for port redundancy using X4(WAN) and X6. While traffic is passing through the tunnels from the remote end LAN to the head end LAN, the X4 interface is shut down on the Active firewall on the head end side. Although traffic is switched to X6, the tunnels remain down for an extended period. **Workaround**: Select the **Enable Load Balancing** checkbox on the Network > Failover & LB page.	131162

Resolved Issues

This section contains a list of issues that are resolved in the SonicOS 6.1.1.4 release.

Log

Symptom	Condition / Workaround	Issue
Syslog messages are not formatted correctly in the display.	Occurs when using an Arcsight syslog server to format and display the messages.	131995
Only the first three syslog servers added in the Log > Syslog page can receive syslog messages from the appliance.	Occurs when more than three syslog servers are configured. SonicOS allows up to seven syslog servers to be added.	131988

Networking

Symptom	Condition / Workaround	Issue
The Edit Interface screen displays a “Default Gateway (Optional)” field for non-WAN interfaces, but configuring it does not cause the interface to be used as a gateway.	Occurs when configuring a non-WAN interface from the Network > Interfaces screen. This field is removed in the SonicOS 6.1.1.4 release.	133560
Default service group objects are missing for Active Directory Server, AD Directory Services, and AD NetBios.	Occurs when viewing the default service group objects on the Network > Services page.	132830
Address objects cannot be added to, or removed from, an address object group, and the OK button is disabled (grey).	Occurs when attempting to edit an address object group.	132827

System

Symptom	Condition / Workaround	Issue
An appliance restarts frequently and displays a message containing “Reboot due to DP Core[1] hang”.	Occurs when High Availability is enabled, and a user changes his password.	132896
The firewall cannot boot with firmware diagnostics enabled. After selecting this option, the Status line displays the message “The configuration has been updated”, but the checkbox is cleared.	Occurs when the "Boot with firmware diagnostics enabled" checkbox is selected on the System > Settings page.	129648

User Interface

Symptom	Condition / Workaround	Issue
HTTPS management of the appliance sometimes loses the connection, while ping to the interface succeeds.	Occurs when the internal web server stops listening while the appliance is being managed over HTTPS.	132366

Users

Symptom	Condition / Workaround	Issue
An LDAP User/Group Trees auto-configure request fails and the console prints a stack trace.	Occurs when using "LDAP is selected for user group lookup for RADIUS/SSO users" and then the LDAP configuration button is clicked. Specifically, in the LDAP Configuration screen, on the Directory tab, enter the Primary domain and click the auto-configure button. In the LDAP User/Group Trees Auto-configure screen, select Append to existing trees/Replace existing trees, and click OK.	129383

VPN

Symptom	Condition / Workaround	Issue
After modifying a VPN policy, the message “Error: OCSP Responder URL is invalid” is displayed.	Occurs when Enable OCSP Checking is selected and the OCSP Responder URL is entered for a site-to-site VPN policy using IKE with third party certificates, and then the VPN policy is modified to use IKE with a preshared secret. After the preshared secret is saved, the error message is displayed.	132054

Last updated: 8/20/2013