Release Notes

SonicOS

SonicOS 6.1.1.5 NSA 3600/4600/5600/6600 Release Notes

Contents

Release Purpose

SonicOS 6.1.1.5 is a maintenance release that fixes a number of known issues.

Platform Compatibility

The SonicOS 6.1.1.5 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 6.1.1.5. The recommended WXA firmware version is WXA 1.2.1.

WXA 1.1.1 will work with SonicOS 6.1.1.5, 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 6.1.1.5 release.

Firewall

Symptom	Condition / Workaround	Issue
The Enable Egress Bandwidth Management option and the Enable Ingress Bandwidth Management option in the Edit interface dialog (Advanced tab) cannot be selected.	Occurs when the Bandwidth Management Type is set to Global.	140553

Network

Symptom	Condition / Workaround	Issue
The Use Password option cannot be disabled in the RIP Configuration dialog.	Occurs when you enable the Use Password option and then try to disable it by unchecking the box.	140592
When Guest Services on the customer's WiFi zone are deleted, the Access Rules for the customer's Wireless to WAN connection are deleted.	Occurs when the customer settings have been imported, but does not occur when the default settings are used.	135345

Security Services

Symptom	Condition / Workaround	Issue
The Anti-Spam service becomes disabled.	Occurs after importing the settings on the System > Settings page and rebooting the firewall.	140587
Anti-spyware is still active after it is disabled.	Occurs when the Enable Anti-Spyware Service option has been enabled and then is disabled by unchecking the Enable Anti-Spyware Service checkbox. Spyware can still be downloaded.	140543

Users

Symptom	Condition / Workaround	Issue
Adding a Terminal Services Agent (TSA) displays "Error: Host name/IP address."	Occurs when the host name begins with a number.	140030
Users are not logged out of the firewall automatically.	Occurs when users log out of the Terminal Server using the Remote Desktop Protocol (RDP).	139917

VPN

Symptom	Condition / Workaround	Issue
Two VPN policies can be added to the same gateway.	Occurs when you add two VPN policies to the same gateway using the CLI. This cannot be done using the Web Management Interface.	139967
VPN tunnels in port redundancy groups are failing.	Occurs when the primary interface in the port redundancy group fails. **Workaround:** Enable Load Balancing on the Network > Failover & LB page.	131162

Resolved Issues

This section contains a list of issues that are resolved in the SonicOS 6.1.1.5 release.

CLI

Symptom	Condition / Workaround	Issue
The system settings file exported using the CLI command, "export current-config sonicos ftp" is corrupted.	Occurs when trying to import the system settings file into the Web Management Interface.	137285

Firewall

Symptom	Condition / Workaround	Issue
The destination address objects in Access Rules are modified.	Occurs after rebooting the firewall.	139587

DPI-SSL

Symptom	Condition / Workaround	Issue
The DPI-SSL server sends an error, "Certificate is not trusted", and the SSL testing tools fail.	Occurs when importing a wild card certificate to the firewall, and there are intermediate certificates in the certificate chain.	139379

High Availability

Symptom	Condition / Workaround	Issue
The primary appliance stops responding, and failover to the secondary appliance never occurs.	Occurs at random intervals during the week if the Watchdog task times out.	136958
The firewall displays the following error: "Firmware upload failed – Cannot upload firmware to idle unit."	Occurs when upgrading the firmware if the firewall is in an Active/Standby HA pair or if the firewall is in Active/Active clustering mode. **Workaround:** Boot each unit to Safemode, then upgrade the firmware.	141413

Log

Symptom	Condition / Workaround	Issue
The Log View panel on the Log > Monitor page does not show the first two pages.	Occurs when the Log View panel is refreshed.	132048

Network

Symptom	Condition / Workaround	Issue
LAN to WAN Access Rules do not block traffic.	Occurs when the LAN to WAN interfaces are a wire mode pair.	138944
Some packets have an 802.1q VLAN tag added to them.	Occurs when packets with 802.1q VLAN tags arrive on an interface that is not in wire mode. Packets traversing the wire mode pair are randomly tagged with the same VLAN.	134072
Users cannot connect to the Point to Point Tunneling Protocol (PPTP) server after typing the correct password.	Occurs when a user types the wrong password on the first try and then enters the correct password on the second try.	134038
FTP connections fail and new FTP connections cannot be established.	Occurs after a Stateful Failover on a Stateful Failover pair in Wiremode in a Link Aggregation Group (LAG).	132278
Some packets have an 802.1q VLAN tag added to them.	Occurs when packets with 802.1q VLAN tags arrive on an interface that is not in wire mode. Packets traversing the wire mode pair are randomly tagged with the same VLAN.	136251

Security Services

Symptom	Condition / Workaround	Issue
Content Filtering Service (CFS) schedules do not start working automatically.	Occurs after the schedule is configured. They start working only if the user logs out and then logs in again. **Workaround:** Use CFS with App Rules.	137889
HTTP POST (ACK PSH) packets associated with AirPlay are being dropped, causing AirPlay to fail.	Occurs when Content Filtering Service (CFS) is enabled. **Workaround:** Disable CFS on the zone, or add the AirPlay server to the CFS Exclusion List.	136107

SSL VPN

Symptom	Condition / Workaround	Issue
A semicolon is added to end of the Connect DNS Domain.	Occurs when a client is obtaining an IP address from a server.	134583

System

Symptom	Condition / Workaround	Issue
A Java script error is displayed on the System > Administration page.	Occurs when you select the “Enable management using GMS” option and then click the Configuration button.	131990
The Auto-import CRL via HTTP option is very slow and times out.	Occurs when trying to revoke certificates via HTTP.	129379

Users

Symptom	Condition / Workaround	Issue
Guest Services is using the Public WAN zone instead of the private IP address of the user.	Occurs when the user is logging in via HTTPS.	137127
Guest Services HTTPs Redirect redirects to the IP address of the user after initially redirecting to the FQDN.	Occurs when the user is logging in via HTTPS.	134851
The LDAP User/Group Trees Auto Configuration request fails. The console print stacktrace command also fails.	Occurs when trying to configure LDAP in the LDAP Configuration dialog on the Users > Settings page.	129383
Some problems exist in identifying users via SSO, which is causing the Users > Status page to show the incorrect user information for the user IP address, resulting in the wrong CFS policies, etc. being applied to the users.	Occurs randomly, usually when the SSO agent(s) are overloaded.	139144

VPN

Symptom	Condition / Workaround	Issue
A VPN tunnel interface routed over an MPLS Link stops passing traffic intermittently until the VPN is renegotiated.	Occurs after upgrading the firewall.	133996
The Local Certificate menu is blank in the VPN Policy dialog.	Occurs after upgrading the firewall.	133697
The following error is displayed: “OCSP Responder URL is invalid when change VPN policy from IKE 3rd certificates to IKE preshared secret mode.”	Occurs when OCSP Checking is enabled and the Authentication Method in the VPN Policy dialog is changed from “IKE using 3rd Party Certificates” to “IKE using Preshared Secret.”	132054

Last updated: 1/30/2014