Dell™ SonicWALL™ SonicOS 6.2.6.1

Release Notes

November 2016

These release notes provide information about the Dell™ SonicWALL™ SonicOS 6.2.6.1 release.

Topics:

About SonicOS 6.2.6.1

SonicOS 6.2.6.1 extends support for SonicWALL Capture ATP to the SuperMassive 9600, TZ300/TZ300W, and TZ400/TZ400W. This release also resolves a number of issues found in previous releases.

This release provides all the features and contains all the resolved issues that were included in previous releases of SonicOS 6.2. For more information, see the previous release notes, available on MySonicWALL or on the Support Portal at: https://support.software.dell.com/release-notes-product-select.

TZ Series / SOHO Wireless feature support

Dell SonicWALL SOHO Wireless and TZ series appliances running SonicOS 6.2.6.1 support most of the features available for other platforms. Only the following features are *not* supported on the TZ series or SOHO Wireless appliances:

- Active/Active Clustering
- Advanced Switching
- Jumbo Frames
- Link Aggregation
- Port Redundancy
- Wire Mode

In addition, SOHO Wireless appliances do not support the following features:

- App Visualization (Real-Time Monitor and AppFlow)
- Capture ATP
- Geo-IP Filtering
- Botnet Filtering
- High Availability

Supported platforms

SonicOS 6.2.6.1 is supported on the following Dell SonicWALL network security appliances:

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2600
- TZ600
- TZ500 and TZ500 Wireless
- TZ400 and TZ400 Wireless
- TZ300 and TZ300 Wireless
- SOHO Wireless

Resolved issues

The following issues are resolved in this release.

Capture ATP

Resolved issue	Issue ID
Some file uploads result in a “highly delayed acks” response and do not receive the expected receipt confirmation from the cloud servers. Occurs when the number of files uploaded for analysis exceeds the concurrent files limit for the platform. On a platform supporting 25 concurrent files, if 50 files are uploaded for analysis, a “highly delayed acks” response is received for two of them.	175967 / 176496

CFS

Resolved issue	Issue ID
The Syslog server log or SonicWALL GMS/Analyzer Syslog server log for the firewall displays an extremely large number of received bytes, such as `rcvd=5367667152344055808` for the **rcvd** field in a log entry containing the key/value pairs `c=1024 m=97`. Occurs when Content Filtering (CFS 4.0) is enabled under Security Services on the firewall and then users visit some web sites.	176616

System

Resolved issue	Issue ID
Sending diagnostic reports to Support can cause the SonicOS management interface to become unresponsive for up to 15 minutes. Occurs when the **Send Diagnostic Reports to Support** button is clicked on the System > Diagnostics page.	175969
For some GMS managed units, the Network > Interfaces page is not displayed after synchronizing. Occurs when synchronizing at the group level, but works fine when synchronizing at the unit level.	172638

Users

Resolved issue	Issue ID
After enabling One-Time Password for some groups, the setting is not saved. Occurs when the **Require one-time passwords** option is enabled in the configuration dialog for imported Local Groups or LDAP Groups, then saved by clicking **OK**, and then the configuration dialog is opened again.	178877
Expired local user accounts are sometimes not automatically pruned (deleted). The user is shown in strikethrough text showing that the account is expired, but the edit page is blank and membership lists are empty. Occurs when a local user account has the auto-prune option enabled and the user is referenced in an access rule.	177686

VPN

Resolved issue	Issue ID
Traffic over a numbered tunnel interface fails after upgrading the appliance firmware. Occurs when the firewall is upgraded from SonicOS 6.2.4.2 to 6.2.5.1 or 6.2.6.0. **Workaround**: After importing configuration settings from a firewall running 6.2.4.2 to a firewall running 6.2.5.1 or 6.2.6.0, manually recreate the VPN Tunnel Interface (numbered tunnel interface), the route entries, and the firewall access rules.	175845

Known issues

This section contains a list of known issues in this release.

3G/4G

Known issue	Issue ID
The Connect on Data mode is not working for 3G cards, causing traffic to stop passing and no Internet access due to an unsuccessful failover to WWAN after the WAN interface is disconnected. Occurs when a 3G card is connected to the U0 port, U0 is configured in Connect on Data mode as the final backup for the WAN (X1) interface, traffic is passing from a client system on the LAN side to the WAN and then the X1 interface is disconnected.	175877

Known issue	Issue ID
Some China-Huawei 3G cards do not connect after the primary WAN interface goes down. Occurs when 3G is configured as final backup in DoD mode, while using a China-Huawei 3G card, including the Huawei E398 card with China Unicom SIM card and the Huawei EC169C card with China Telecom SIM card.	175146
Website access over AT&T Beam and AT&T Momentum 4G USB modem cards fails with a connection reset page. Other traffic types succeed, including ping, telnet, and nslookup. Occurs when accessing the Internet over the WWAN interface while either of these AT&T cards is connected to the U0 port. This issue occurs because the Maximum Transmission Unit (MTU) changed from 1500 to 40 in the AT&T network.	168487

AppFlow

Known issue	Issue ID
The **GMSFlow Server** option is available as a selection for **Data Source**, but should be dimmed or greyed out. Using the option results in the error message, “Error or no response from the server.” Occurs when an external collector is configured in the AppFlow > Flow Reporting screen and the **GMSFlow Server Address** field is set to 0.0.0.0 in the AppFlow > GMSFlow Server screen, and then the admin navigates to a related screen such as AppFlow Monitor.	178854

App Rules

Resolved issue	Issue ID
Policies with match objects are not enforced. Occurs when the match object size is greater than 150 bytes.	173739

Capture ATP

Known issue	Issue ID
The scanned files are truncated and the firewall log shows “File truncated due to highly delayed acks”, but the scan history shows all 45 files scanned with result clean. Occurs when sending a PDF file with IMAP protocol as an attachment through a VPN tunnel interface.	176213
The Gateway Anti-Virus status says, “Gateway Anti-Virus Status: File sent to Sandbox, but could not confirm receipt due to highly delayed acks”. Occurs after sending a file to the Capture ATP cloud servers for analysis.	175415

DPI-SSL

Known issue	Issue ID
The HTTPS service object is not correctly excluded by Client DPI-SSL. Occurs when the firewall is deployed between an HTTPS proxy server and a client system, the proxy server is configured in the client browser, Client DPI-SSL is enabled along with the **Deployments wherein the Firewall sees a single server IP for different server domains, ex: Proxy setup** option, HTTPS is selected in the Client DPI-SSL Exclude drop-down for Service Object/Group, and then the user accesses some online banking websites which are not excluded as expected, but are decrypted by DPI-SSL and the certificates are re-issued by SonicWALL. If proxy is not set in the client browser, those sites are correctly excluded from DPI-SSL.	175696

Log

Known issue	Issue ID
The Web Site Hits table is always empty in the Log > Reports page. Occurs when clicking the Start Data Collection button on the Log > Reports page and then running LAN to WAN HTTP/HTTPS web browsing traffic.	176224

Networking

Known issue	Issue ID
The tunnel interface name is not displayed in the connection monitor table after traffic passes through an unnumbered VPN tunnel interface. Occurs when a tunnel interface VPN policy is added and a static route going through this VPN tunnel interface is added, and then traffic is sent to the destination.	175449
Traffic fails on 10Gb interfaces that are changed from Wiremode in a High Availability pair. Occurs when X18 and X19 are configured as Wiremode pair interfaces in inspect mode and traffic is passing, and then X18 is unassigned, then assigned to the LAN zone as a static interface and a DHCP server is bound to it. After a client PC connected to X18 renews its DHCP lease, traffic to the WAN fails and pings from the client PC are not received.	175333
The link status between a TZ appliance and a Dell X-Series switch displays “no link”. Occurs when changing the link settings to 100 Mbps Full-Duplex with one switch using an Isolated Link configuration or with two switches using a Common Link configuration.	175205
The FQDN resolved results are not synchronized on the firewalls in an HA pair. Occurs when a firewall in an HA pair is idle and Stateful Synchronization is enabled.	174716
Auto-added route entries for the WAN are disabled and dimmed in a firewall configured with a redundant WAN port. Occurs when WAN port goes down but its redundant port is still up, and then the firewall is restarted.	173703

Security Services

Known issue	Issue ID
Workstations cannot communicate with Windows Shared Folders. Files cannot be copied, and this GAV alert is generated, “SMB out of order read/write”. Occurs when the CIFS/Netbios option is enabled on the Security Services > Gateway Anti-Virus page. Communication works after disabling CIFS/Netbios.	175366
Gateway Anti-Virus does not correctly block a malicious email attachment. Occurs when using Thunderbird as the email client to download email from an IMAP server on the WAN, and email with a malicious attachment is downloaded.	174499

Switching

Known issue	Issue ID
The L2 LAG members are not aggregated on the VLAN trunk ports, and traffic is blocked. Occurs when PortShield and L2 LAG are configured on the VLAN trunk, and the firewall is restarted.	175363
A VLAN interface bound to a Trunk interface cannot be deleted, and the Switching > VLAN Trunking page only shows the first 32 configured VLAN interfaces. Occurs when more than 32 VLAN interfaces are configured on the Trunk interface, and the	175229

Known issue	Issue ID
one to be deleted is not displayed on the Switching > VLAN Trunking page.	
The L2 Link Aggregation Group (LAG) function does not respond. Occurs when creating a new LAG group, and the aggregator port link is down, and the primary WAN is in Round Robin mode.	175152

Syslog

Known issue	Issue ID
Syslog messages for both admin and user login sessions show “dur=0”, instead of the actual duration of the login. This causes SonicWALL GMS to display zeros for the login session duration. Occurs when capturing and viewing the syslog messages that are sent to GMS, and when viewing the login durations in GMS.	175823

System

Known issue	Issue ID
The **Enable FTP 'REST' requests with Gateway AV** option in the Gateway Anti-Virus settings is not turned on after enabling DPI and Stateful Firewall Security. Occurs when GAV is licensed but disabled with all options disabled, and then the **DPI and Stateful Firewall Security** button is clicked on the System > Settings page and the firewall restarts.	175100
The **Enable HTTP Byte-Range requests with Gateway AV** option in the Gateway Anti-Virus settings is not turned on after enabling DPI and Stateful Firewall Security. Occurs when GAV is licensed but disabled with all options disabled, and then the **DPI and Stateful Firewall Security** button is clicked on the System > Settings page and the firewall restarts.	175098
Connections do not update their configurations. Occurs when Enable Stealth Mode and Randomize IP ID are enabled, and Decrement IP TTL for forwarded traffic is disabled, and Maximum DPI Connections is set with DPI services enabled.	175006

Users

Known issue	Issue ID
Local users with Limited Administration rights and local users who are part of the Read-only Administrators group cannot access the SonicOS management page, but are redirected to an authentication page. Occurs when the local users also belong to the Guest Services group, and Guest Services is enabled in the LAN zone, and the user attempts to log into the appliance and clicks the Manage button.	175973
RADIUS or LDAP authenticated user sessions remain active after clicking the Logout button. Occurs when a user on the LAN side attempts to access the Internet through the firewall and logs in when the login redirect window is displayed and then clicks the Logout button. When the Users > Status page is checked, the Active User Sessions table still shows the user session as active, and the user can continue to access the Internet from the same computer without being required to log in again.	175765

VPN

Known issue	Issue ID
SonicWALL GMS, while running behind a gateway firewall, does not acquire a firewall for management, although an active VPN tunnel is created in the gateway device. Occurs when **IPSEC Management Tunnel** is selected as the **Management Mode** in the GMS settings configured from the System > Administration page on the managed firewall.	178775
The **Apply NAT Policies** option cannot be enabled in a VPN policy of type Tunnel Interface, preventing NAT policies from being applied over the unnumbered tunnel interface. Occurs when the VPN policy is added with the Apply NAT Policies option enabled, but when verifying it, the checkbox for Apply NAT Policies is not selected and it cannot be enabled.	175882
Connecting via SSH to a firewall with a VPN tunnel set up results in the error message, “maximum number of ssh sessions are active, please try again later”. Occurs when a site-to-site VPN tunnel is active between two firewalls and four SSH sessions are started on one of the firewalls, then the VPN tunnel is disabled followed by exiting all SSH sessions, and then the VPN tunnel is reconnected and the administrator attempts to connect via SSH again.	175610

Wireless

Known issue	Issue ID
The beacon interval for a SonicPoint Virtual Access Point (VAP) is affected by the beacon interval set for an internal wireless VAP. The error message “Error: Too small 802.11 Beacon Interval for Virtual Access Point” is displayed upon moving more than four VAP objects into a Virtual Access Point Group. Occurs when a SonicPoint is connected to a TZ Wireless appliance which has its wireless radio enabled with the Internal AP Group configured as the Virtual Access Point Group, and the beacon interval is set to a value such as 400 milliseconds on the Wireless > Advanced page. The SonicPoint is connected to a WLAN interface of the TZ and its beacon interval is set to a different value, such as 600 milliseconds, and then five VAP objects are added on the SonicPoint > Virtual Access Point page. Next, a Virtual Access Point Group is added and the five VAP objects are moved to it, resulting in the error message.	175891

System compatibility

This section provides additional information about hardware and software compatibility with this release.

Wireless 3G/4G broadband devices

SonicOS 6.2.6.1 provides support for a wide variety of PC cards, USB devices and wireless service providers. For the most recent list of supported devices, see http://www.sonicwall.com/supported-wireless-broadband-cards-devices/.

GMS support

Dell SonicWALL Global Management System (GMS) management of Dell SonicWALL security appliances running SonicOS 6.2.6.1 requires GMS 8.2 for management of firewalls using Capture ATP and Content Filter Service 4.0 (CFS 4.0). GMS 8.1 SP1 supports management of all other features in SonicOS 6.2.6.1 and earlier releases.

WXA support

The Dell SonicWALL WXA series appliances (WXA 6000 Software, WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are supported for use with Dell SonicWALL security appliances running SonicOS 6.2.6.1. The recommended firmware version for the WXA series appliances is WXA 1.3.2.

Browser support

SonicOS with Visualization 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 9.0 and higher
- Safari 5.0 and higher running on non-Windows machines

ⓘ **NOTE:** On Windows machines, Safari is not supported for SonicOS management.

ⓘ **NOTE:** Mobile device browsers are not recommended for Dell SonicWALL appliance system administration.

Product licensing

The Capture ATP license requires that Gateway Anti-Virus (GAV) is also licensed. You must enable Gateway Anti-Virus (GAV) and Cloud Anti-Virus before you can use Capture ATP. See the *SonicOS 6.2.6 Capture ATP Feature Guide* for details on licensing Capture ATP.

Dell SonicWALL network security appliances must be registered on MySonicWALL to enable full functionality and the benefits of Dell SonicWALL security services, firmware updates, and technical support. Log in or register for a MySonicWALL account at https://mysonicwall.com/.

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 6.2 Upgrade Guide* available on MySonicWALL at https://mysonicwall.com/ or on the Support portal at https://support.software.dell.com/.

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the portal provides direct access to product support engineers through an online Service Request system. To access the Support Portal, go to http://software.dell.com/support/.

The site enables you to:

- View Knowledge Base articles at:

  https://support.software.dell.com/kb-product-select

- View instructional videos at:

  https://support.software.dell.com/videos-product-select

- Engage in community discussions
- Create, update, and manage Service Requests (cases)
- Obtain product notifications

SonicOS Administration Guides and related documents are available on the Dell Software Support site at https://support.software.dell.com/release-notes-product-select.

About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit http://www.software.dell.com.

Contacting Dell

For sales or other inquiries, visit http://software.dell.com/company/contact-us.aspx or call 1-949-754-8000.

Legend

△ **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

⚠ **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

ⓘ **IMPORTANT**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Last updated: 10/31/2016

232-003407-00 Rev A