Dell SonicWALL™ SonicOS 6.2.2.2

Release Notes

June 2015

These release notes provide information about the Dell SonicWALL SonicOS 6.2.2.2 release.

- About SonicOS 6.2.2.2
- Supported platforms
- Enhancements
- Resolved issues
- Known issues
- System compatibility
- Product licensing
- Upgrading information
- Technical support resources
- About Dell

About SonicOS 6.2.2.2

SonicOS 6.2.2.2 is a maintenance release that fixes a number of issues found in previous releases. See Resolved issues. It also provides enhancements for supporting international Dell SonicPoint wireless access points. See Enhancements.

This release provides all the features and contains all the resolved issues that were included in the SonicOS 6.2.0.0, 6.2.0.1, 6.2.2.0, and 6.2.2.1 releases. For more information, see the release notes for these releases, available at https://support.software.dell.com/release-notes-product-select.

**IMPORTANT:** Note the following recent design changes for the treatment of traffic over VPN tunnel interfaces:

- In SonicOS 6.2.0.0, and in SonicOS 6.1.1.9 and earlier 6.1.1.x releases, traffic over VPN tunnel interfaces is *exempt* from NAT policies.

- In SonicOS 6.2.0.1 and 6.1.1.10, NAT policies are applied by *default* to traffic over VPN tunnel interfaces. Upgrading to 6.2.0.1 or 6.1.1.10 may require configuration changes.

- Beginning in SonicOS 6.2.2.0, NAT policies can optionally be applied to this traffic by selecting the Apply NAT Policies checkbox when configuring the VPN tunnel interface. *By default, this option is disabled.*

Upgrading from SonicOS 6.2.0.1 or 6.1.1.10 to 6.2.2.2 may require configuration changes if you are using VPN tunnel interfaces.
Supported platforms

The SonicOS 6.2.2.2 release 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

Enhancements

- Dell SonicPoint support for Japan
- International Dell SonicPoint support

Dell SonicPoint support for Japan

SonicOS 6.2.2.2 supports Dell SonicPoint ACe, ACi, and N2 wireless access points for deployment in Japan.

International Dell SonicPoint support

SonicOS 6.2.2.2 supports international Dell SonicPoint ACe, ACi, and N2 wireless access points. An international SonicPoint is one that is deployed and operating in a country other than the United States or Japan.

When an international Dell SonicPoint is connected to a Dell SonicWALL network security appliance, SonicOS displays a Register button on the SonicPoint > SonicPoints page. Clicking Register brings up a dialog box in which you can select the appropriate Country Code.

**NOTE:** Be sure to select the country code for the country in which the Dell SonicPoint will be deployed, even if you are not in that country while registering the SonicPoint.

For international SonicPoints registered with country codes other than Canada, the country code can be changed in the SonicPoint profile on the SonicPoint > SonicPoints page.

**IMPORTANT:** Once the SonicPoint is registered with the country code for Canada, the country code cannot be changed except by contacting Dell SonicWALL Support.
Resolved issues

The following issues are resolved in this release.

### CFS

<table>
<thead>
<tr>
<th>Resolved issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>After configuring a per IP address range CFS policy, it is not properly added and is not displayed in the SonicOS management interface. Occurs when the administrator selects the Enable Policy per IP Address Range checkbox on the Security Services &gt; Content Filter page and clicks the Add button, configures the policy, and then clicks OK.</td>
<td>156374</td>
</tr>
</tbody>
</table>

### Log

<table>
<thead>
<tr>
<th>Resolved issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Some raw IP protocols not correctly reported in the log. Occurs when raw IP protocols 47 and 103 are sent inbound or outbound through the firewall. Protocol 47 is labeled as &quot;proto=1/1&quot; and protocol 103 is labeled as &quot;proto=88/88&quot;.</td>
<td>161165</td>
</tr>
<tr>
<td>Syslog messages for ICMP packets do not include the “type=” field. Occurs when syslog messages are logged for ICMP type 0 packets passing through the firewall either inbound or outbound.</td>
<td>160682</td>
</tr>
</tbody>
</table>

### Wireless

<table>
<thead>
<tr>
<th>Resolved issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>A deleted and resynchronized SonicPoint ACe, ACi, or N2 uses the wrong country code. Occurs when a SonicPoint is registered with a country code, then the country code is changed in the SonicPoint profile, and then the unit is deleted and resynchronized. It should use the registered country code, not the one from the profile change.</td>
<td>160692</td>
</tr>
</tbody>
</table>

Known issues

The following is a list of known issues in this release.

### High Availability

<table>
<thead>
<tr>
<th>Known issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>After enabling the Preempt mode, IPv6 VPN SA cannot be established. Occurs after setting up the appliance and the Preempt mode has been enabled with an IPv6 manual key VPN policy. After checking the VPN SA traffic, a failover occurs by cutting the primary XO. The backup boots up ready, but after reconnecting the XO and waiting for the preempting to occur, the traffic fails.</td>
<td>152565</td>
</tr>
</tbody>
</table>

### Log

<table>
<thead>
<tr>
<th>Known issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>The source and destination of the App Rules log messages are opposite. The source is the real destination, and the destination is the real source. Occurs when viewing the App Rules log messages.</td>
<td>149458</td>
</tr>
</tbody>
</table>
### Networking

<table>
<thead>
<tr>
<th>Known issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>The network interface cannot be edited or unassigned and error messages appear. Occurs when the interface configuration is changed from L2TP, PPTP, or PPPOE mode to L2 Bridged mode.</td>
<td>156477</td>
</tr>
<tr>
<td>The firewall cannot enable OSPF through the console. Occurs when trying to enable the OSPF through the firewall console. The network needs to first match the OSPF wildcard bits.</td>
<td>153350</td>
</tr>
<tr>
<td>The firewall cannot enable RIPv2 through the console. Occurs when trying to enable RIPv2 through the firewall console and the subnet is not set, or when the subnet is 32-bit as with 10.8.109.0 where the last byte of the IP address is 0.</td>
<td>153267</td>
</tr>
<tr>
<td>The firewall learns OSPF routes from areas other than area0. Occurs when the network topology includes 3 firewalls with 3 areas, all with VLANs configured, and the OSPF routes are checked on the area1 firewall.</td>
<td>153096</td>
</tr>
<tr>
<td>There is no option to originate a default route for dynamic IPv6 routing via OSPFv3. Occurs when configuring OSPFv3 from the Network &gt; Routing page. IPv6 default route origination via OSPFv3 is currently not supported.</td>
<td>150771</td>
</tr>
</tbody>
</table>

### SSL VPN

<table>
<thead>
<tr>
<th>Known issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP traffic between different SSL VPN clients works for a while, then fails with a message, “couldn’t connect to host.” Occurs when 10 SSL VPN clients are passing TCP traffic for several hours to a server that is also connected to the firewall via SSL VPN.</td>
<td>154958</td>
</tr>
</tbody>
</table>

### System

<table>
<thead>
<tr>
<th>Known issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attempting to log into the SonicOS management interface results in the error message, “---error code: ssl_error_no_cipher_overlap”. Occurs when logging in over HTTPS from a Firefox 37.0.1 browser.</td>
<td>161354</td>
</tr>
<tr>
<td>Cannot ping IPv6 hosts using Diagnostic Tools. Occurs when specifying MGMT as the outgoing interface.</td>
<td>155988</td>
</tr>
</tbody>
</table>

### VoIP

<table>
<thead>
<tr>
<th>Known issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsequent inbound calls from a VoIP client on the WAN side of the firewall to a VoIP client on the LAN side fail after a successful first call. If using NetMeeting, the WAN side client gets the error message, “The other party did not accept your call.” Occurs when both clients are using the H.323 standard and both are registered to the same gatekeeper, which is located on the WAN side. Workarounds: Re-register the LAN side client with the gatekeeper to allow one more inbound call.</td>
<td>161392</td>
</tr>
</tbody>
</table>
System compatibility

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

- Dell SonicWALL WXA support
- Browser support

Dell SonicWALL WXA support

The Dell SonicWALL WX series appliances (WXA 6000 Software, WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are also supported for use with Dell SonicWALL security appliances running SonicOS 6.2.2.2. The recommended firmware version for the WX series appliances is WXA 1.3.1.

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 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.

Product licensing

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.

For Dell SonicPoint ACi, ACi, or N2 units purchased in the United States or Japan, after your SonicPoint is connected to a registered Dell SonicWALL network security appliance, SonicOS will automatically register the SonicPoint on MySonicWALL, if connected to the Internet. It may take up to 24 hours for your SonicPoint to be automatically registered. Optionally, you can manually register your SonicPoint on MySonicWALL by logging into your account at: http://www.mysonicwall.com.

For Dell SonicPoints purchased in other countries, after your SonicPoint is connected to a Dell SonicWALL network security appliance, SonicOS displays a Register button on the SonicPoint > SonicPoints page. Clicking Register brings up a dialog box in which you can select your Country Code.

All Dell SonicPoint wireless access points include an initial subscription to Dell SonicWALL 24x7 Support. In order to receive technical support, your SonicPoint must have an active Support subscription.
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 or on the Dell Software Support page for SonicWALL NSA or SuperMassive appliances at https://support.software.dell.com/release-notes-product-select.

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. To access the Support Portal, go to http://software.dell.com/support/.


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.

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
- Chat with a support engineer
- Create, update, and manage Service Requests (cases)
- Obtain product notifications

About Dell

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

Contacting Dell

Technical support:
Online support
Product questions and sales:
(800) 306-9329
Email:
info@software.dell.com
© 2015 Dell Inc.
ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser’s personal use without the written permission of Dell Inc.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:
Dell Inc.
Attn: LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

Refer to our web site (software.dell.com) for regional and international office information.

Patents

Trademarks
Dell, the Dell logo, and SonicWALL are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.

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

Last updated: 6/9/2015
232-002904-00 Rev A