Dell SonicWALL™ SonicOS 6.2.2.0

Release Notes

January, 2015

These release notes provide information about the Dell SonicWALL SonicOS 6.2.2.0 release.

About SonicOS 6.2.2.0

SonicOS 6.2.2.0 introduces support for the Dell SonicPoint ACe, ACi, and N2 wireless access points on Dell SonicWALL network security appliances capable of running SonicOS 6.2 firmware. This release includes a number of related SonicPoint and wireless features. See the New features section for more information.

This release provides all the features and contains all the resolved issues that were included in the SonicOS 6.2.0.0 and 6.2.0.1 releases. For more information, see the previous release notes:

SonicOS 6.2.0.1 Release Notes	https://support.software.dell.com/download/downloads?id=5744093
SonicOS 6.2.0.0 Release Notes	https://support.software.dell.com/download/downloads?id=5601864

IMPORTANT: SonicOS 6.2.2.0 includes a *design change* added in recent releases for the treatment of traffic over VPN Tunnel Interfaces. By default, NAT policies are now applied to this traffic. In SonicOS 6.2.0.0, and in SonicOS 6.1.1.9 and earlier 6.1.1.x, traffic over VPN Tunnel Interfaces was exempt from NAT policies. Upgrading from one of these earlier releases to 6.2.2.0 may require configuration changes.

Supported platforms

The SonicOS 6.2.2.0 release is supported on the following Dell SonicWALL network security appliances:

• SuperMassive 9600	• NSA 6600
• SuperMassive 9400	• NSA 5600
• SuperMassive 9200	• NSA 4600
	• NSA 3600
	• NSA 2600

New features

The following are the new features in the SonicOS 6.2.2.0 release:

SonicPoint AC and N2 support

SonicOS 6.2.2.0 provides support for the new Dell SonicPoint wireless access points:

- Dell SonicPoint ACe — 802.11ac compliant with external antennas
- Dell SonicPoint ACi — 802.11ac compliant with internal antennas
- Dell SonicPoint N2 — 802.11n compliant with external antennas

Dell SonicPoint ACe and ACi support the 802.11ac standard for Wi-Fi. This includes higher throughput in the 5-GHz band, wider channels, more spatial streams, and other features that boost throughput and reliability. The Dell SonicPoint ACe/ACi provide the following key technical components:

- Wider Channels—80 MHz channel bandwidths
- New Modulation and Coding—64-QAM, rates 3/4 and 5/6 added as option modes
- Up to 4 Spatial Streams—Adding spatial streams increases throughput proportionally. Two streams double the throughput of a single stream. Four streams increase the throughput four times.

Dell SonicPoint ACe, ACi, and N2 provide dual radios for wireless access on both the 5-GHz and 2.4-GHz radio bands.

Dell SonicPoint ACi and N2 are powered by 802.3at compliant Power Over Ethernet (PoE).

Dell SonicPoint ACe can be powered by 802.3at compliant PoE or with the included power adaptor (input 120V-240V AC to output 12V DC).

SonicPoint and wireless enhancements

The following SonicPoint and wireless enhancements are included in SonicOS 6.2.2.0:

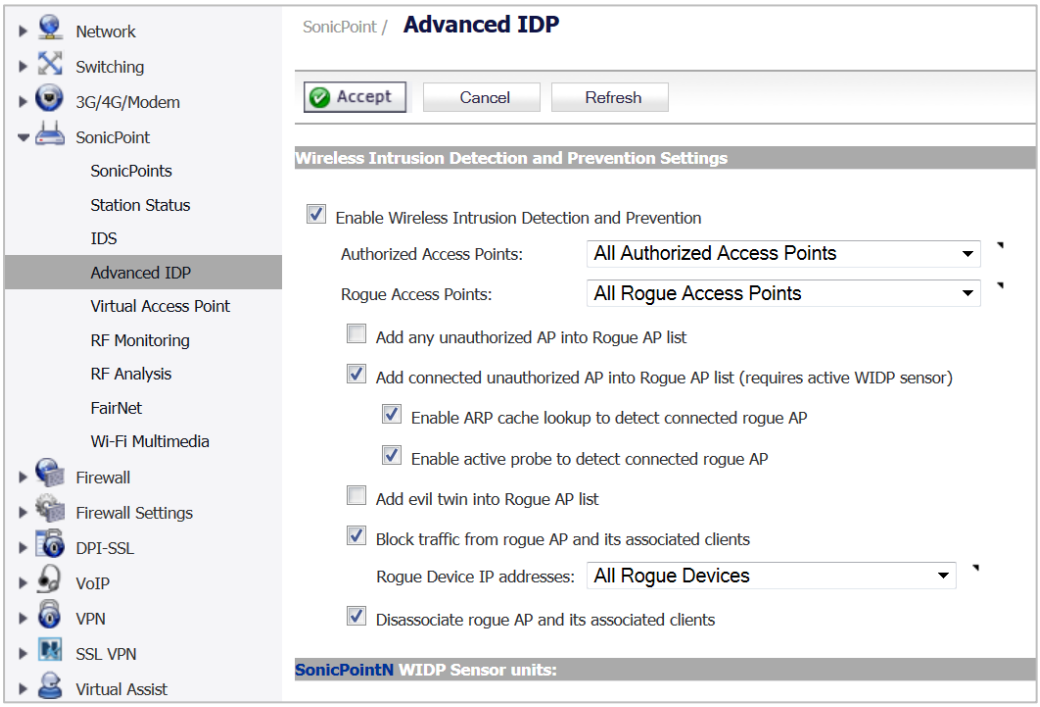
Internal radio IDS scan scheduling

Advanced IDP or Wireless Intrusion Detection and Prevention (WIDP) monitors the radio spectrum for the presence of unauthorized access points (intrusion detection) and automatically takes counter measures (intrusion prevention). Previously, only a wireless scan was done. SonicOS 6.2.2.0 provides a solution that detects rogue access points and takes action according to the administrator settings.

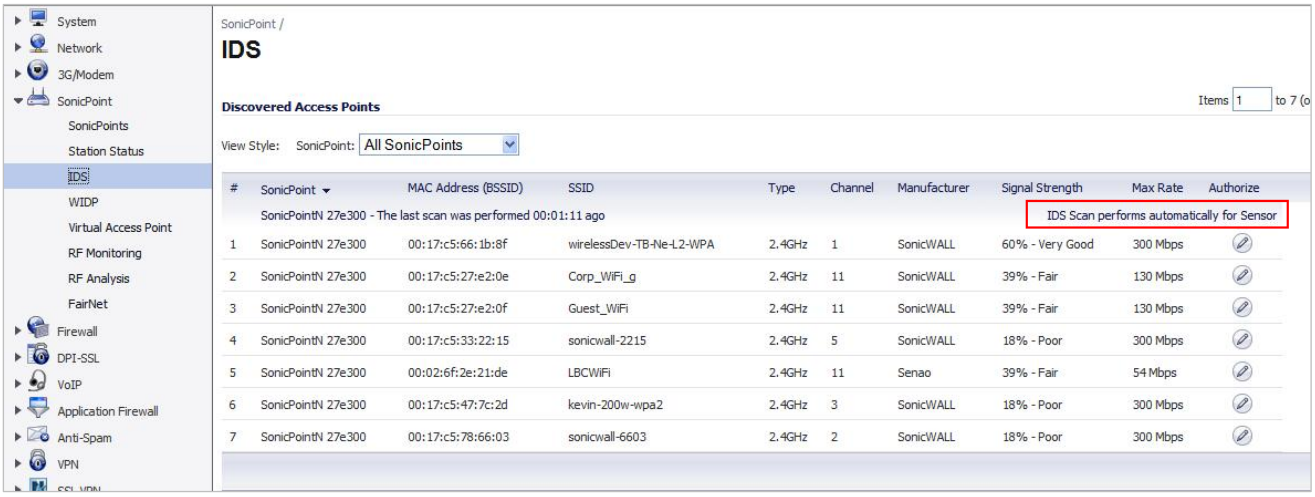
SonicOS Wireless Intrusion Detection and Prevention is based on SonicPoint N and cooperates with a Dell SonicWALL NSA gateway. This feature turns SonicPoint Ns into dedicated WIDP sensors that detect unauthorized access points connected to a Dell SonicWALL network.

This feature is available for single radio SonicPoint N, including SonicPoint Ne and SonicPoint Ni.

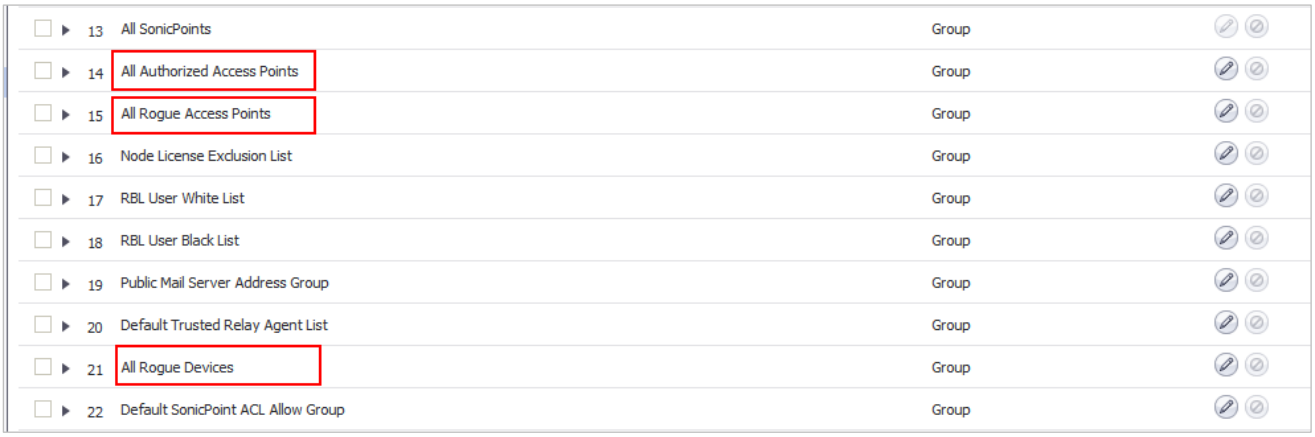
Under **SonicPoint**, a new GUI page is added with **Advanced IDP** options.



When a SonicPoint N is configured as a WIDP sensor, it can no longer function as an access point. IDS scans are done automatically.



When an access point is identified as a rogue access point, its MAC address is added to the **All Rogue Access Points** group, and its source IP address is added to **All Rogue Devices** group.



For SonicPoint Ns, no access point mode Virtual Access Point (VAP) is created. One station mode VAP is created, which is used to do IDS scans, and to connect to and send probes to unsecured access points.

SonicPoint 802.11e (WMM) QoS

SonicPoint access points now support Wi-Fi Multimedia (WMM) to provide a better Quality of Service experience on miscellaneous applications, including VoIP on Wi-Fi phones, and multimedia traffic on IEEE 802.11 networks. WMM is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard. It prioritizes traffic according to four access categories: voice, video, best effort, and background. Note that WMM does not provide guaranteed throughput.

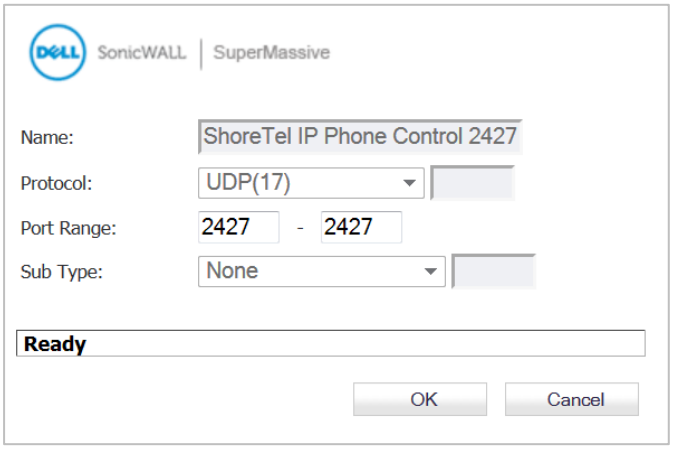
The following table shows the User Priority to Access Category mapping for the four access categories:

Priority	UP (Same as 802.1D user priority)	802.1D designation	AC	Designation (informative)
Lowest	1	BK	AC_BK	Background
	2	—	AC_BK	Background
	0	BE	AC_BE	Best Effort
	3	EE	AC_BE	Best Effort
	4	CL	AC_VI	Video
Highest	5	VI	AC_VI	Video
	6	VO	AC_VO	Voice
	7	NC	AC_VO	Voice

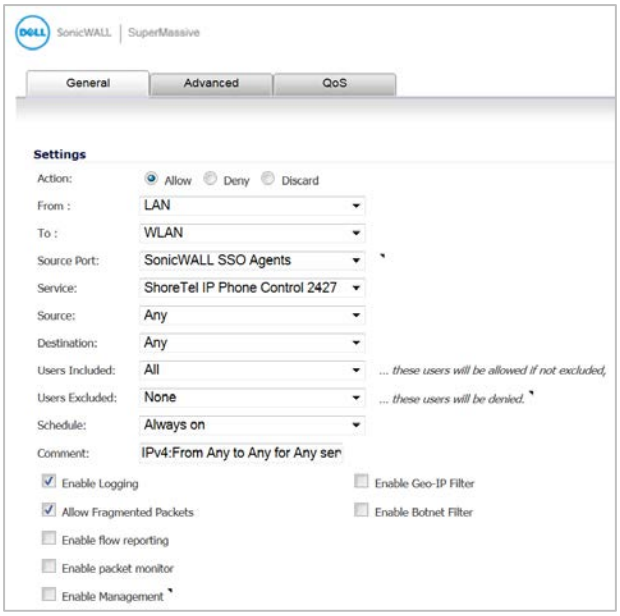
Each Access Category has its own transmit queue. WMM requires the SonicPoint N to implement multiple queues for multiple priority access categories. The SonicPoint N relies on either the application or the firewall to provide type of service (TOS) information in the IP data in order to differentiate traffic types. One way to provide TOS is through firewall services and access rules; another way is through VLAN tagging.

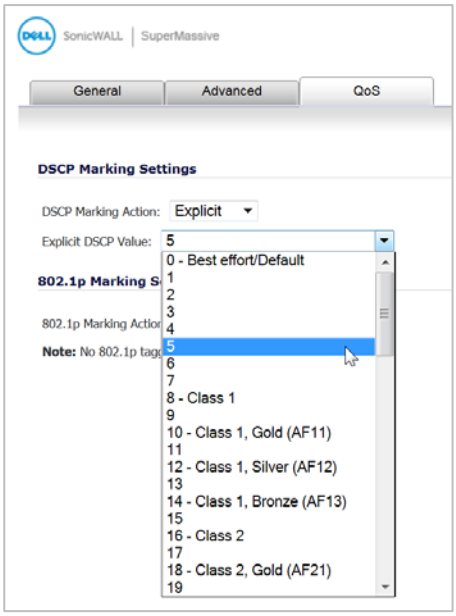
Firewall services and access rules:

Services using a certain port can be prioritized and put into a proper transmit queue. For example, UDP traffic sending to port 2427 can be regarded as a video stream. The SonicOS administrator can add a custom service on the **Firewall > Service Objects** page, similar to the following:



At least one access rule should be added on the **Firewall > Access Rules** page for the new service. For example, when such a service happens from a station on the LAN zone to a wireless client on the WLAN zone, an access rule can be inserted. In the QoS setting tab, an explicit DSCP value is defined. Later, when packets are sent to the SonicPoint N through the firewall using UDP protocol with destination port 2427, their TOS fields are set according to the QoS setting in the access rule. The General and QoS tabs of an example access rule are shown below:

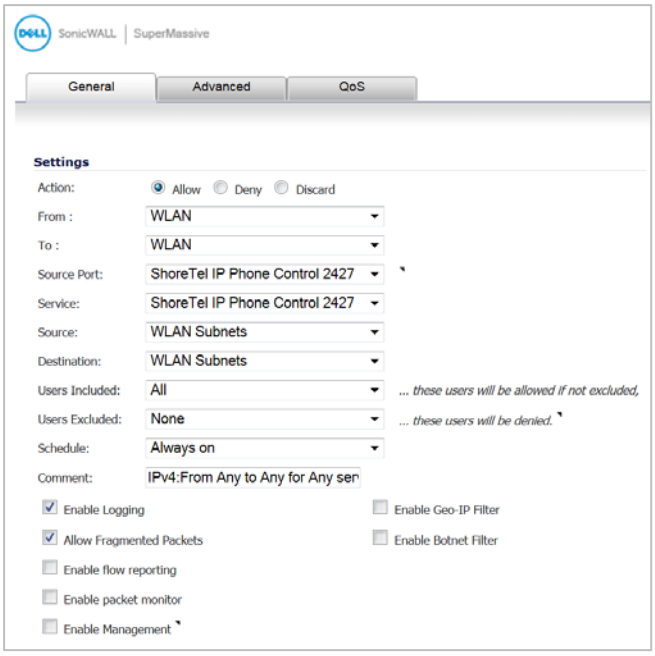




VLAN tagging:

Prioritization is possible in VLAN over Virtual Access Point (VAP), because the SonicPoint N and ACs allow a VAP to be configured to connect with a VLAN by using same VLAN ID. You can set priority for VLAN traffic through a firewall access rule.

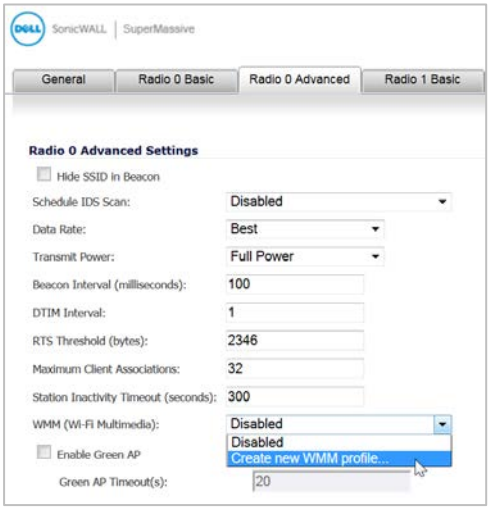
The firewall access rule is similar to that shown above to set priority for a UDP service destined to a port such as 2427, but is configured with a VLAN (VLAN over VAP) interface, such as WLAN Subnets, as the **Source** and **Destination**, and is a WLAN to WLAN rule.

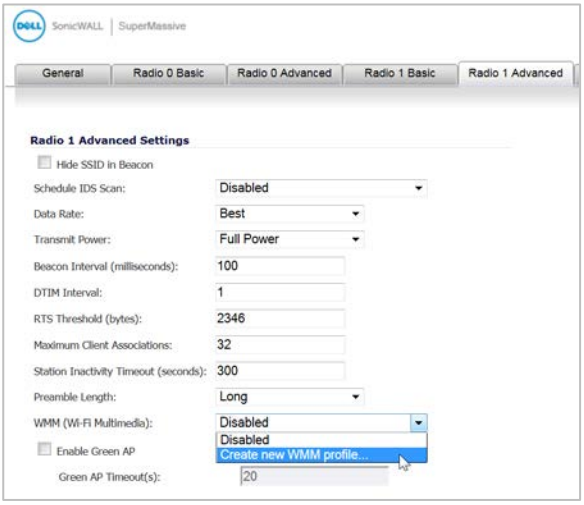


SonicPoint WMM configuration

The **SonicPoint > Wi-Fi Multimedia** page provides a way to configure WMM profiles, including parameters and priority mappings.

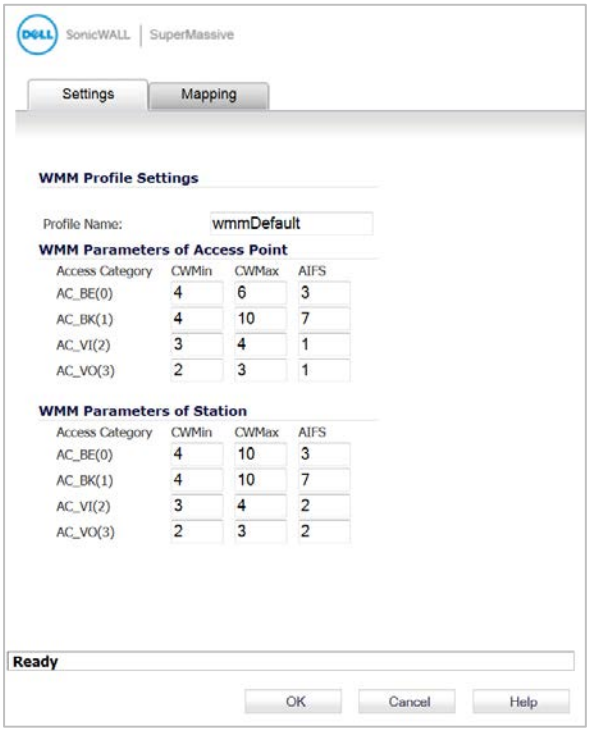
You can also create a WMM profile or select an existing WMM profile when configuring a SonicPoint N or a SonicPoint AC Profile from the **SonicPoint > SonicPoints** page. The **Configuration** window provides a WMM **(Wi-Fi Multimedia)** drop-down list on the **Radio Advanced** tabs with these options.

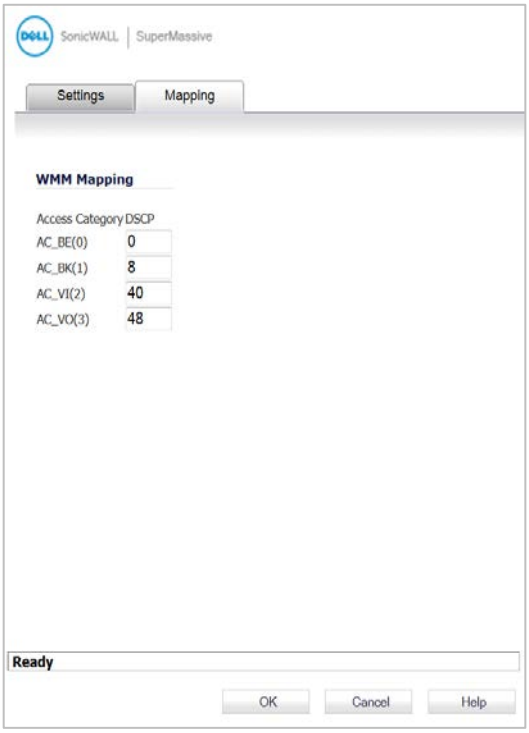




When configuring the WMM profile, on the **Settings** tab, the administrator can configure the size of the contention window (CWMin/CWMax) and the arbitration interframe space (AIFS) number when creating a WMM profile. These values can be configured individually for each priority, AC_BK, AC_BE, AC_VI, and AC_VO on the Access Point (SonicPoint N, AC) and for the Station (firewall).

The **Mapping** tab allows you to map priority levels to DSCP values. The default DSCP values are as same as the ones in **SonicPoint > Wi-Fi Multimedia > Add Wlan WMM Profile**.

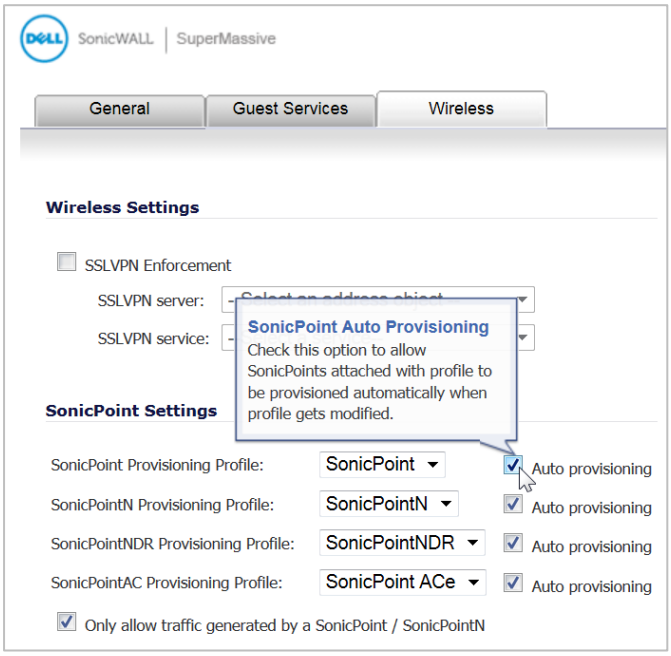




SonicPoint auto provisioning

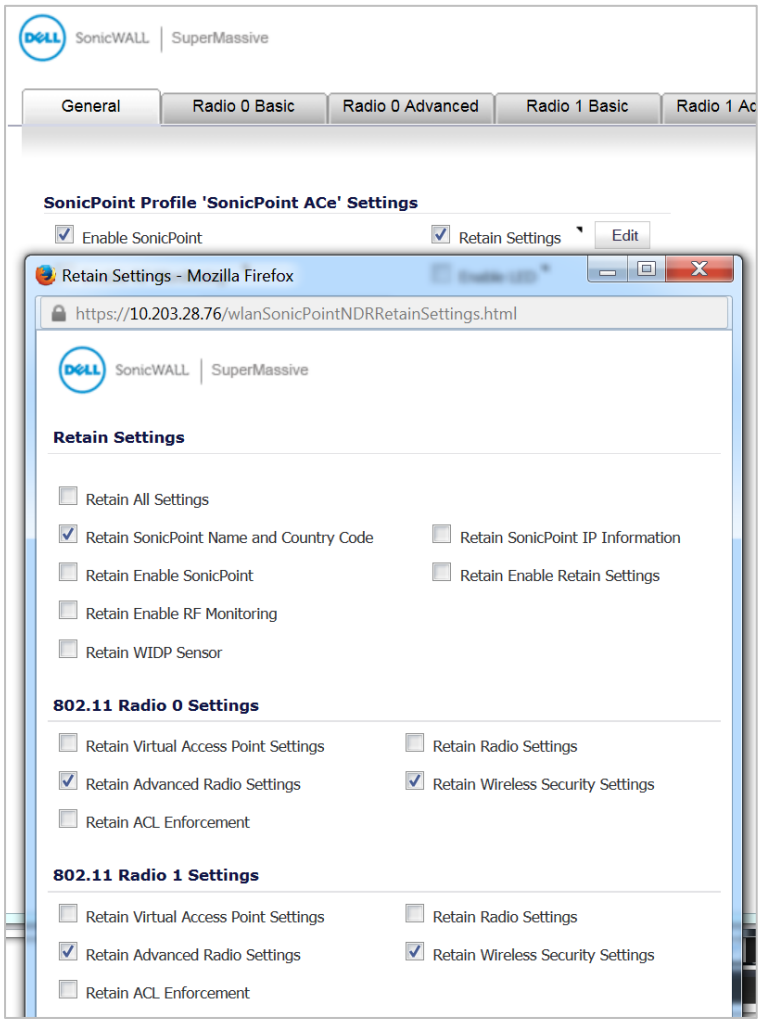
A SonicPoint can be re-provisioned automatically according to a wireless zone profile. This increases management efficiency and ease of use, as previously a SonicPoint had to be deleted and re-added in order to be re-provisioned with a modified profile.

To enable automatic provisioning, navigate to the **Network > Zones** page and click the **Configure** icon for the WLAN zone. In the Edit Zone window on the **Wireless** tab, select **Auto provisioning** for each type of **SonicPoint Provisioning Profile** listed there, and then click **OK**.



SonicPoint customized configuration preservation

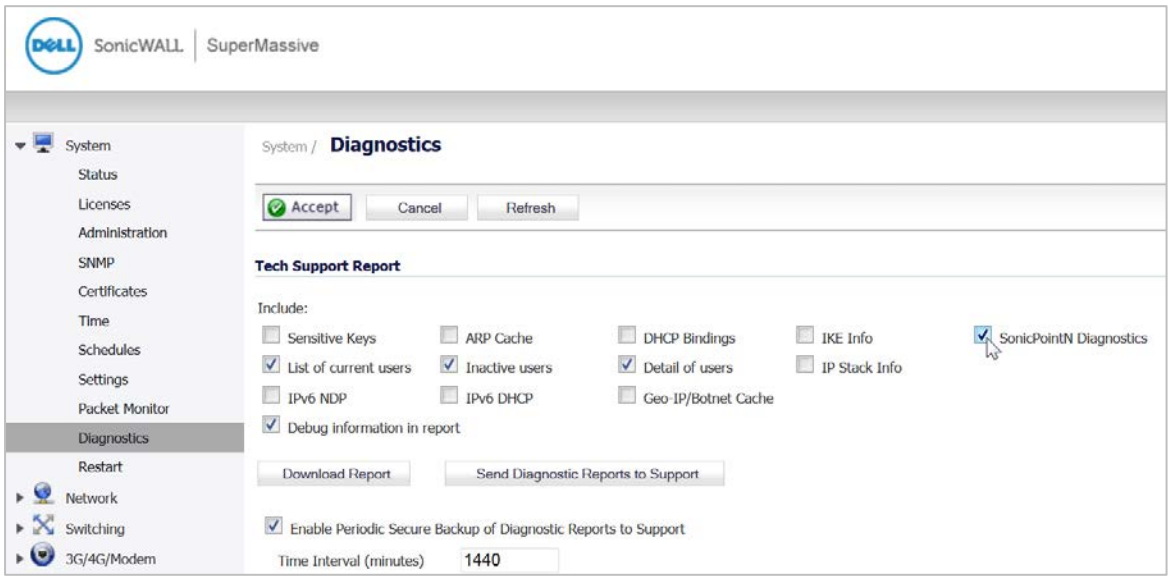
SonicOS includes the ability to configure SonicPoint profiles so that the SonicPoints retain portions of their configuration after they are deleted and resynchronized. To configure this feature, navigate to the **SonicPoint > SonicPoints** page and click the **Configure** icon for the appropriate SonicPoint profile. Enable the **Retain Settings** checkbox and click **Edit** to configure which settings to retain.



SonicPoint diagnostics enhancement

A SonicPoint can collect critical runtime data and save it into persistent storage. If the SonicPoint has a failure, the Dell SonicWALL managing appliance retrieves that data when the SonicPoint reboots, and incorporates it into the Tech Support Report (TSR). A subsequent SonicPoint failure overwrites the data.

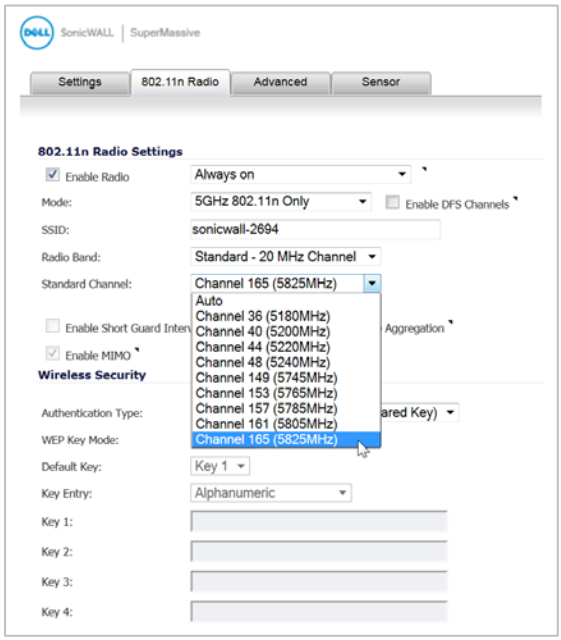
To enable this feature, navigate to the **System > Diagnostics** page and select the **SonicPointN Diagnostics** checkbox in the **Tech Support Report** section, then click **Accept**.

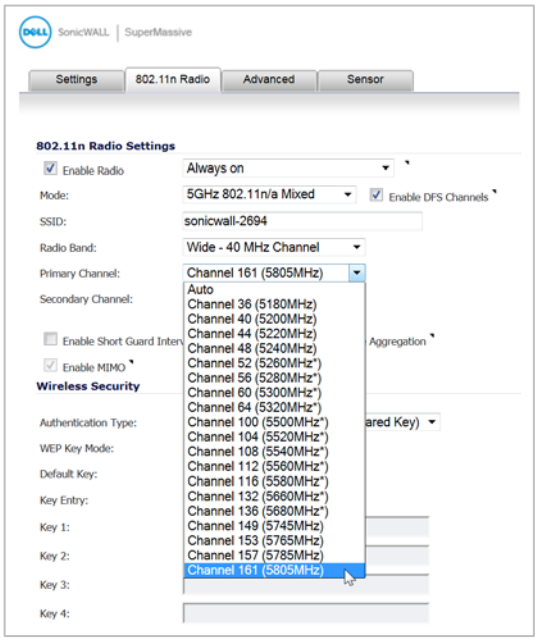


SonicPoint DFS support

After a Dynamic Frequency Selection (DFS) certificate is issued, the SonicPoint N can support dynamic frequency selection to allow a SonicPoint N to be deployed in sensitive channels of the 5GHz frequency band.

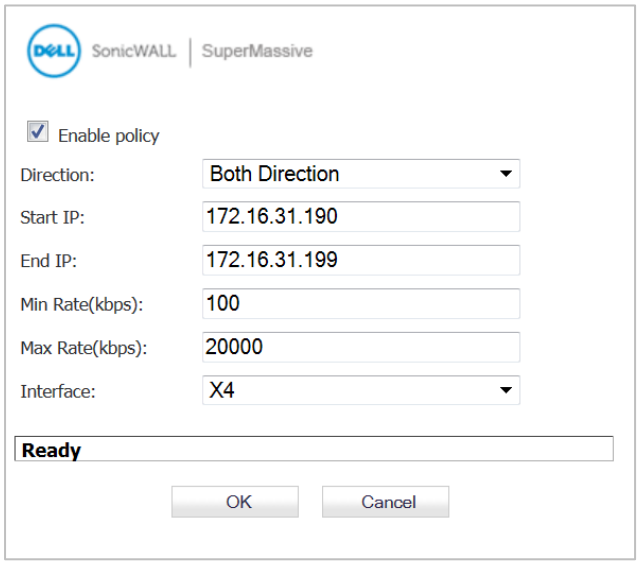
To view and select from these 5GHz channels, navigate to **SonicPoint > SonicPoints** and configure a SonicPoint N Profile or an individual SonicPoint N. On the **802.11n Radio** tab, select any 5GHz setting in the **Mode** field and then select either Standard or Wide as the **Radio Band**. The **Standard Channel** or **Primary Channel** drop-down lists display a choice of sensitive channels.





SonicPoint FairNet support

After optimizing the system resources, FairNet is now supported on the SonicPoints to provide bandwidth fairness control in the WLAN. To configure a FairNet policy, navigate to the **SonicPoint > FairNet** page and click **Add**.

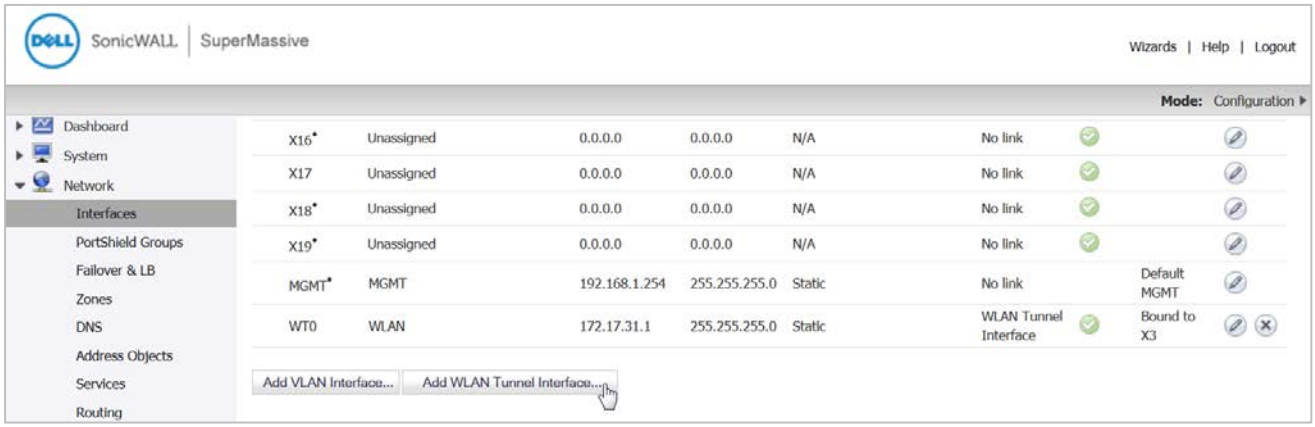


Use the **Start IP** and **End IP** fields to specify a subset of the SonicPoint DHCP range. The rates are per client; the minimum is 100Kbps and the maximum is 300Mbps (300,000 Kbps), although 20Mbps might be a more typical **Max Rate** setting.

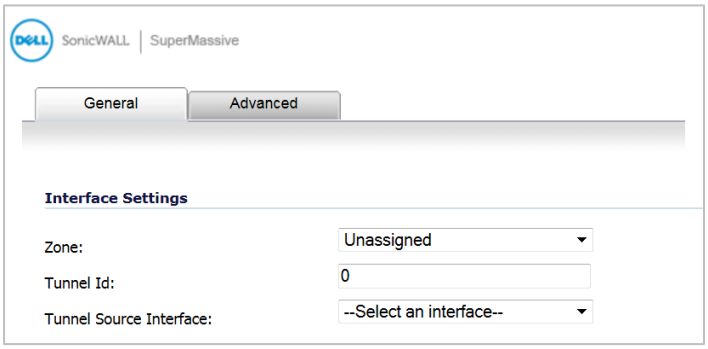
SonicPoint Layer 3 management phase 1

This enhancement provides the DHCP and tunneling solution to support SonicPoint deployment in a Layer 3 network. SonicOS DHCP-based Discovery Protocol (SDDP) is based on the well-known DHCP protocol and allows the Dell SonicWALL gateway and SonicPoint to discover each other automatically across Layer 3 local networks. The remote network management protocol, SonicOS SSLVPN-based Management Protocol (SSMP), is based on SonicOS SSLVPN infrastructure to allow SonicPoints to be managed by a Dell SonicWALL network security appliance with the SSL-VPN option enabled. This feature is supported on the SonicPoint wireless access points.

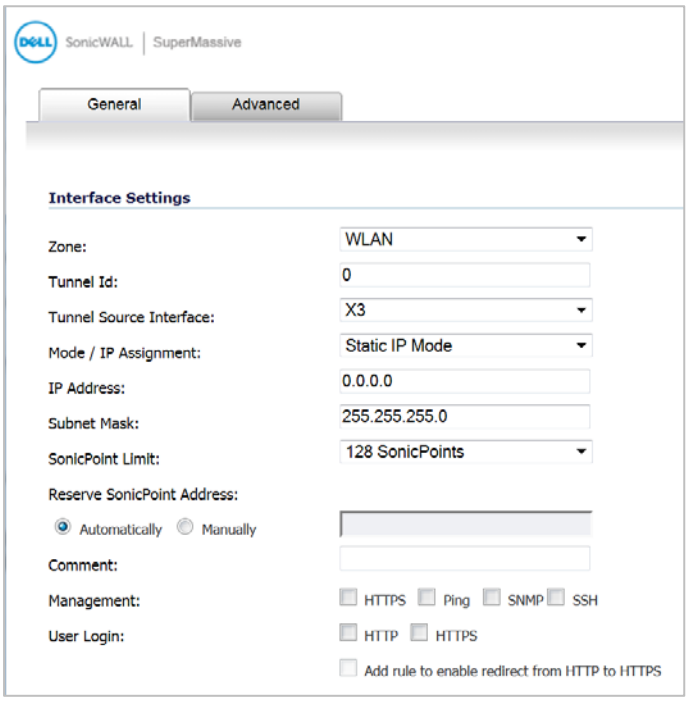
To configure the Layer 3 settings, navigate to the **Network > Interfaces** page and click **Add WLAN Tunnel Interface** below the **Interface Settings** table.



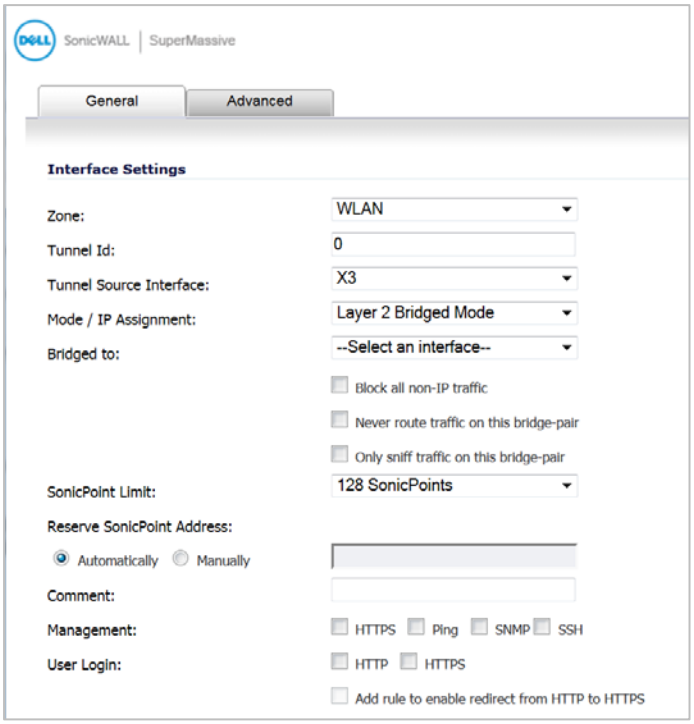
When first displayed, the configuration page displays only three fields.



Select **WLAN** for the **Zone**. More fields are displayed. Select an interface that is connected to the SonicPoint from the **Tunnel Source Interface** drop-down list.



You can choose a **Mode / IP Assignment** of either **Static IP Mode** (shown above) or **Layer 2 Bridged Mode** (shown below). Fill in the **IP Address** or **Bridged to** interface and select the management options, then click **OK**.



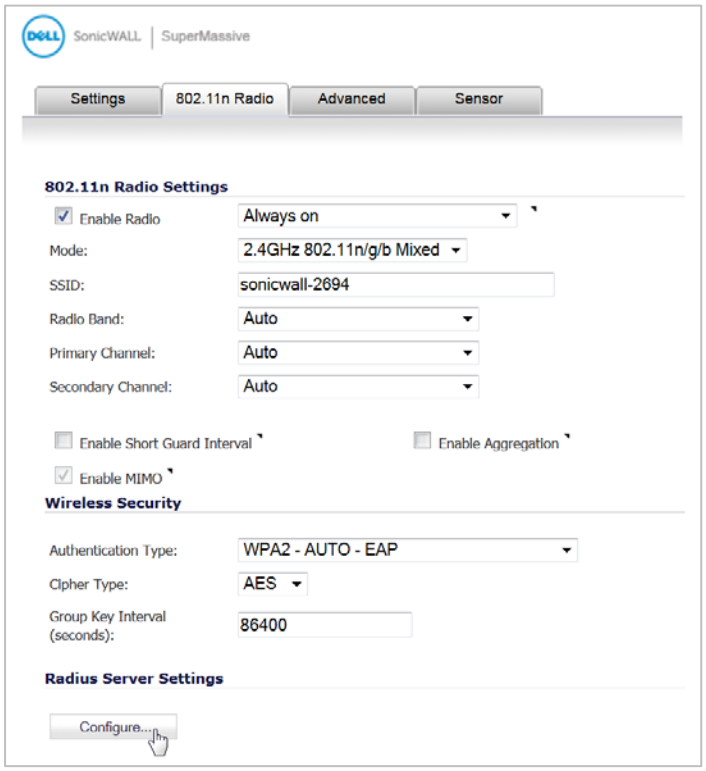
After completing the configuration, the **SonicPointNs** table on the **SonicPoint > SonicPoints** page shows **MGMT: Layer 3** in the **Network Settings** column.

SonicPoint RADIUS server failover

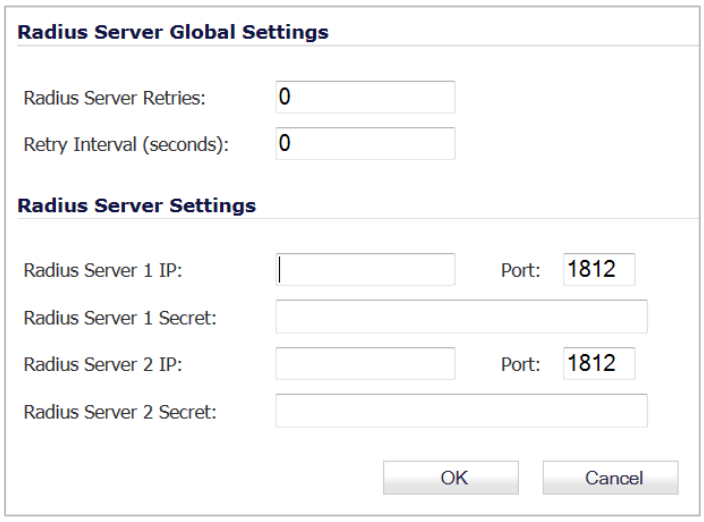
Provides round-robin algorithm and more flexibility to manage the primary and secondary RADIUS servers. To configure the RADIUS servers, navigate to the **SonicPoint > SonicPoints** page. **Add** or **Edit** a SonicPoint or a SonicPoint Profile. On the **802.11n Radio** tab under **Wireless Security**, select one of the following for **Authentication Type**:

- WPA – EAP
- WPA2 – EAP
- WPA2 – Auto – EAP

The **Radius Server Settings** section appears in the window.



Click the **Configure** button to configure the RADIUS server settings.



You can set the **Radius Server Retries** to a value between **1** and **10**. This is the number of times the firewall will attempt to connect before it fails over to the other RADIUS server. The **Retry Interval** can be set to a value between **0** and **60** seconds, with a default of 0 meaning no wait between retries.

Under **Radius Server Settings**, enter the **IP** address, **Port**, and **Secret** for each RADIUS server.

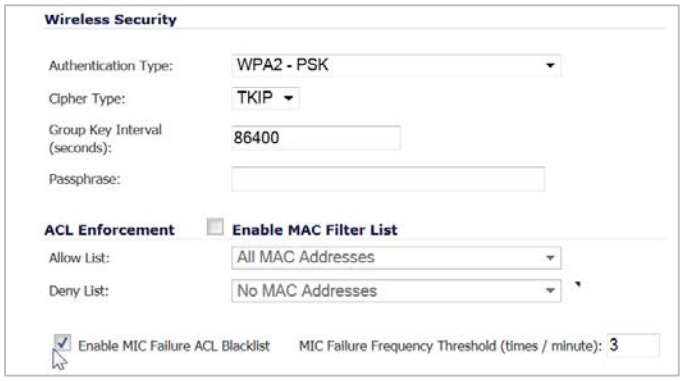
SonicPoint WPA TKIP countermeasures and MIC failure flooding detection and protection

Wi-Fi Protected Access (WPA) TKIP countermeasures will lock down the entire Wireless LAN network in situations where an intruder launches a WPA passphrase dictionary attack to generate a Message Integrity Check (MIC) failure flood in an attempt to impact the WLAN functionality and performance. This SonicOS solution can detect a TKIP MIC failure flood and take action with TKIP countermeasures against the source to automatically block them by adding them to the runtime blacklist, protecting the overall system.

To configure this feature, navigate to the **SonicPoint > SonicPoints** page. **Add** or **Edit** a SonicPoint Profile. On the **802.11n Radio** tab under **Wireless Security**, select one of the following for **Authentication Type**:

- WPA – PSK
- WPA2 – PSK
- WPA2 – Auto – PSK

For the **Cipher Type**, select **TKIP**. Under **ACL Enforcement**, select the **Enable MIC Failure ACL Blacklist** checkbox. You can adjust the **MIC Failure Frequency Threshold** setting. The default is three times per minute. After the threshold is reached, the source is blacklisted.

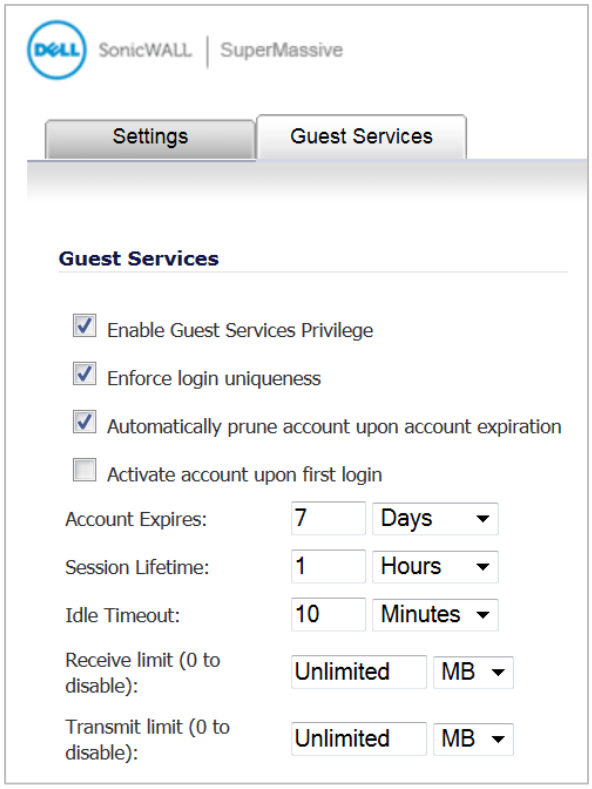


When a source is blacklisted, it is added to the dynamically created **Default SonicPoint ACL Deny Group**. You can view this on the **Network > Address Objects** page.

Traffic quota based guest server policy

Guest sessions can be controlled based on traffic quota policy for better usability. This allows you to configure different transmit/receive limits for different guest clients, possibly based on payment.

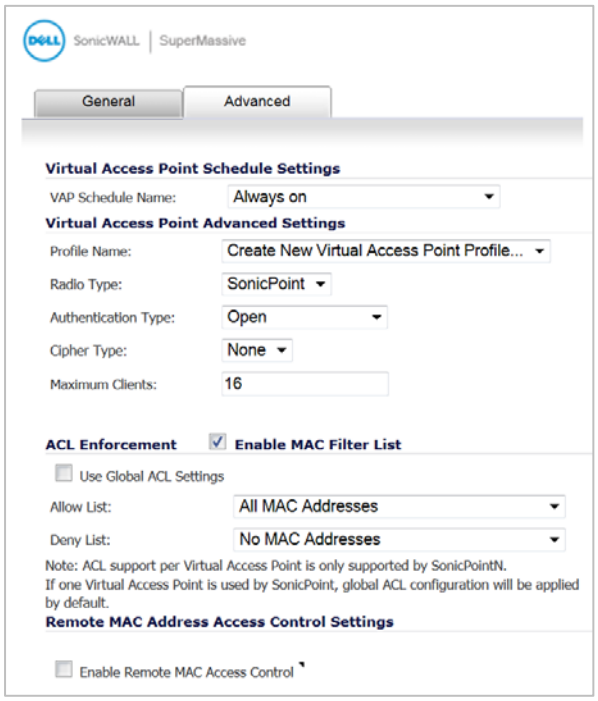
To configure a traffic quota based policy, navigate to the **Users > Guest Accounts** page and click **Add Guest**. In the Add Guest window on the **Guest Services** tab, set the desired number of megabytes in the **Receive limit** and **Transmit limit** fields. Set the fields to **0** to disable limits. Click **OK**.



Virtual Access Point ACL support

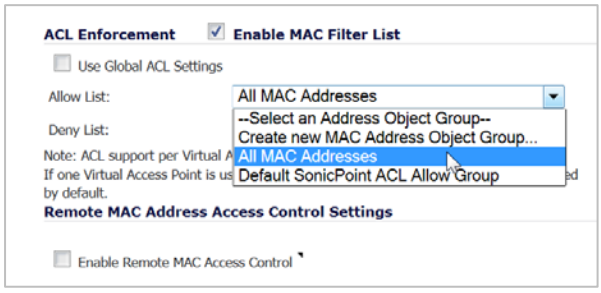
Each Virtual Access Point (VAP) can support an individual Access Control List (ACL) to provide more effective authentication control. Unified ACL support is provided for both SonicPoints and built-in wireless radio.

To enable this feature, navigate to the **SonicPoint > Virtual Access Point** page. **Add** or **Edit** a Virtual Access Point and click the **Advanced** tab. In the **ACL Enforcement** section, select **Enable MAC Filter List**.

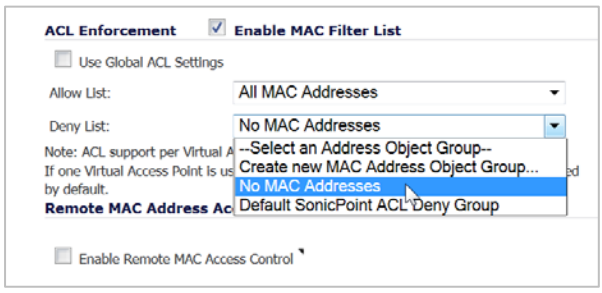


You can select the **Use Global ACL Settings** checkbox, or select an Address Group for both the **Allow List** and **Deny List**. You can also create a new, custom MAC Address Object Group.

Allow List options:



Deny List options:

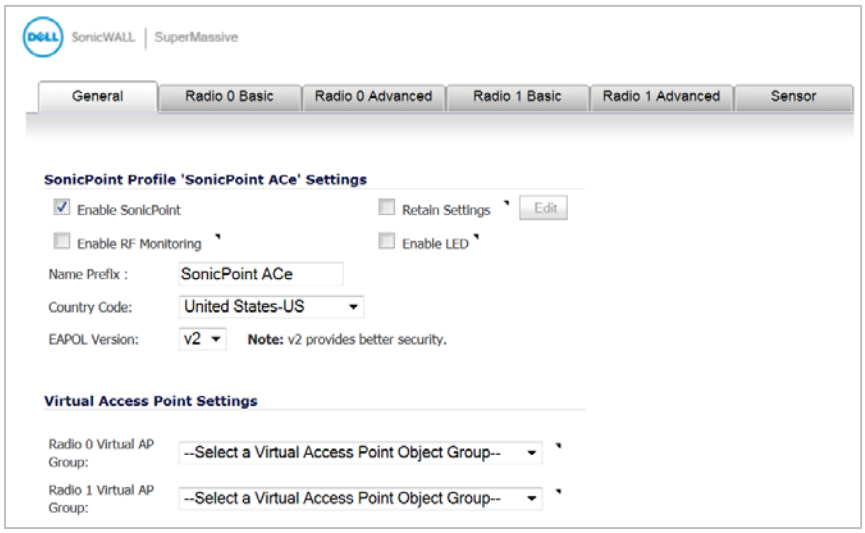


See the **Network > Address Objects** page to view the ACL Allow and Deny groups.

VAP Group sharing on dual radio SonicPoints

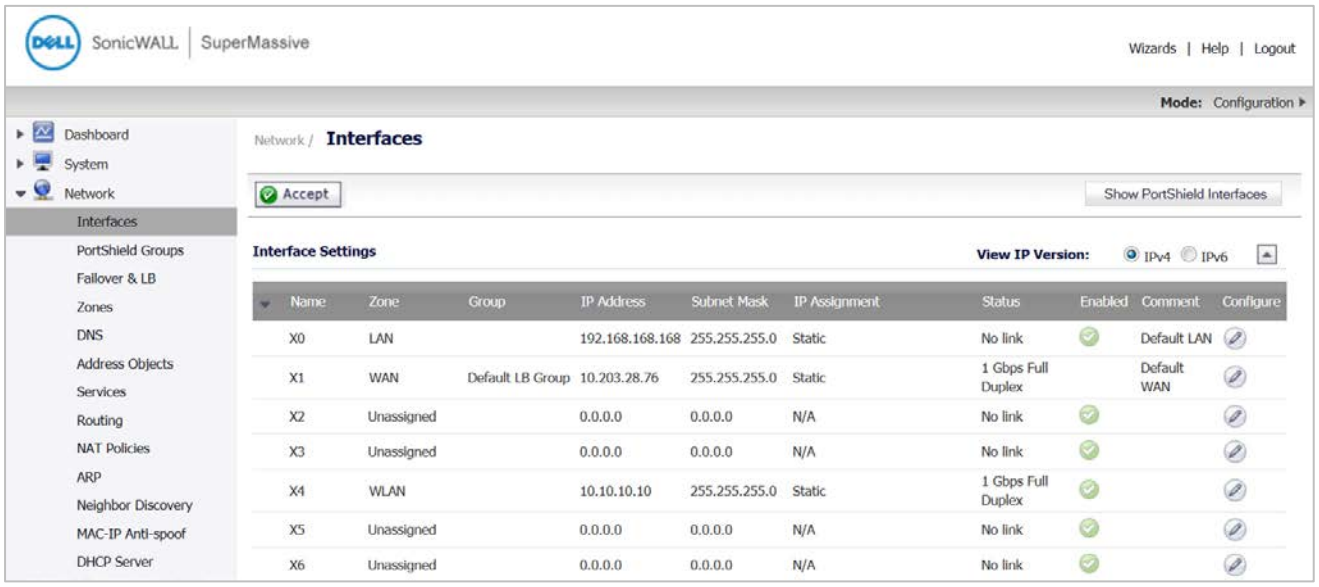
The same Virtual Access Point / VLAN settings can be applied to dual radios. This allows you to use a unified policy for both radios, and to share a VLAN trunk in the network switch. Supported on the dual radio SonicPoint NDR and ACe/ACi/N2 access points.

To apply the settings to both radios, navigate to the **SonicPoint > SonicPoints** page and edit a SonicPoint dual radio profile. In the configuration window on the **General** tab, in the **Virtual Access Point Settings** section, select the same Virtual Access Point Group for both **Radio 0** and **Radio 1**. The drop-down list also provides the option to create the VAP Object Group.

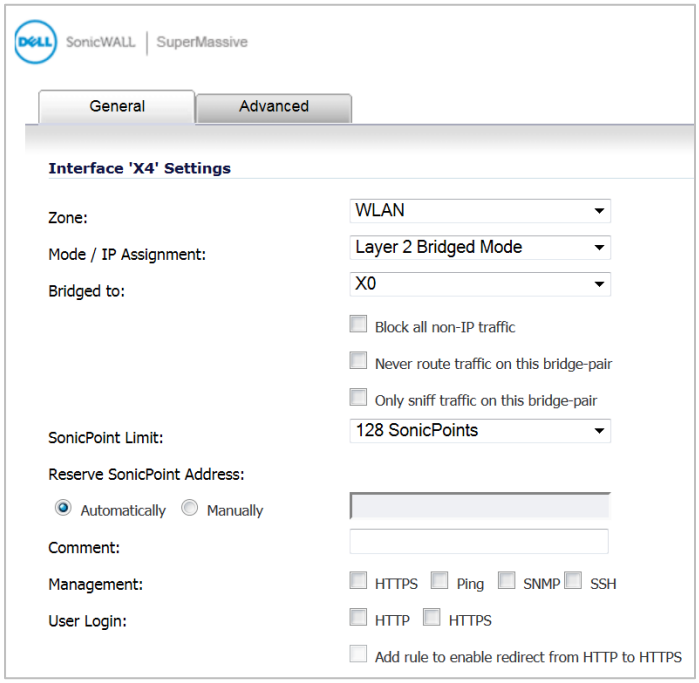


Virtual Access Point Layer 2 bridging

Each Virtual Access Point can be bridged to a corresponding VLAN interface on the LAN zone, providing better flexibility. To configure a Virtual Access Point Layer 2 bridge, navigate to the **Network > Interfaces** page. If you have a Virtual Access Point configured, then you already have a VLAN interface under an interface, such as X4, in the WLAN zone, and your Virtual Access Point is configured to use that VLAN ID. Create a corresponding VLAN interface under the desired "bridge to" interface, such as **X0**.

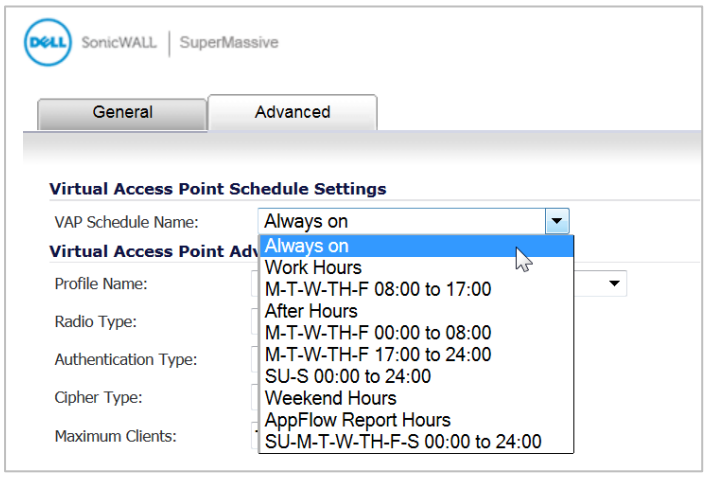


Next, edit the VLAN interface that is used by the VAP. For **IP Assignment**, select **Layer 2 Bridged Mode**, and for the **Bridged to** field, select the corresponding VLAN that you created under X0. Click **OK**.



Virtual Access Point schedule support

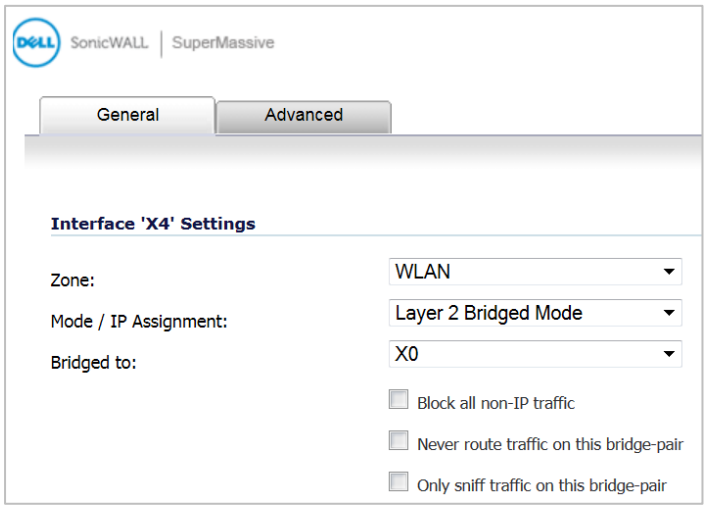
Each Virtual Access Point schedule can be individually enabled or disabled, for ease of use. To select a VAP schedule, navigate to the **SonicPoint > Virtual Access Point** page. **Add** or **Edit** a Virtual Access Point. In the configuration window, click the **Advanced** tab. Select the desired schedule from the **VAP Schedule Name** drop-down list.



Wireless client bridge support

A wireless bridge is supported in WLAN Layer 2 Bridge Mode to provide more flexibility. This feature allows you to bridge wired traffic wirelessly to another LAN.

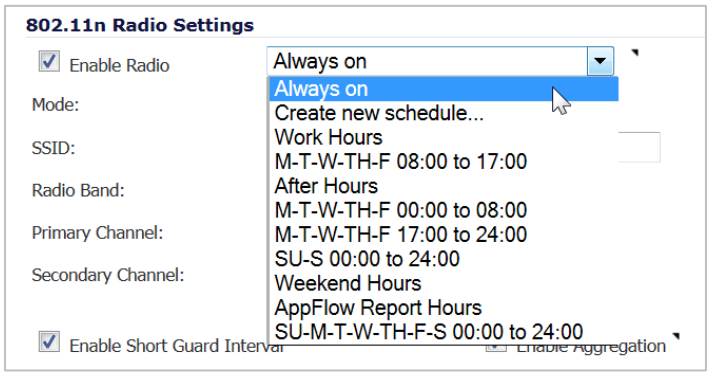
To configure the bridge, edit the WLAN interface in **Network > Interfaces**. Set the **IP Assignment** field to **Layer 2 Bridged Mode**, and set the **Bridged to** interface to a LAN interface, such as **X0**.



Wireless radio built-in scan schedule

In **SonicPoint > SonicPoints**, **Add** or **Edit** a SonicPoint profile. The internal built-in radio on Dell SonicWALL TZ and NSA Wireless appliances can now be scheduled to perform Intrusion Detection/Prevention scanning with granular scheduling options to cover up to 24 hours a day, 7 days a week. The same scheduling options already exist on the **802.11n Radio** tab (or comparable tab) when editing SonicPoint profiles for all SonicPoint models.

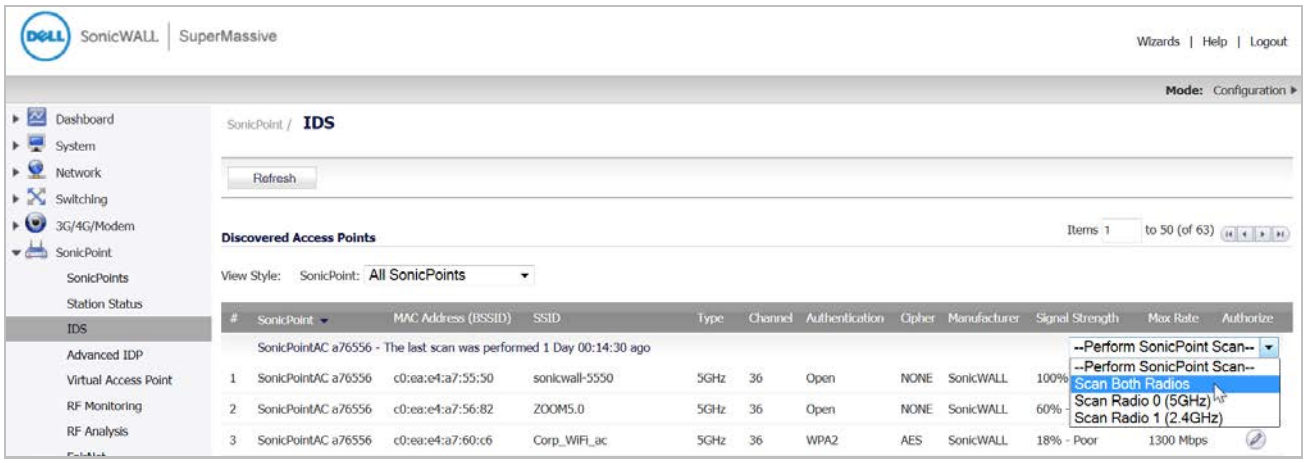
The scheduling options are shown in the image below:



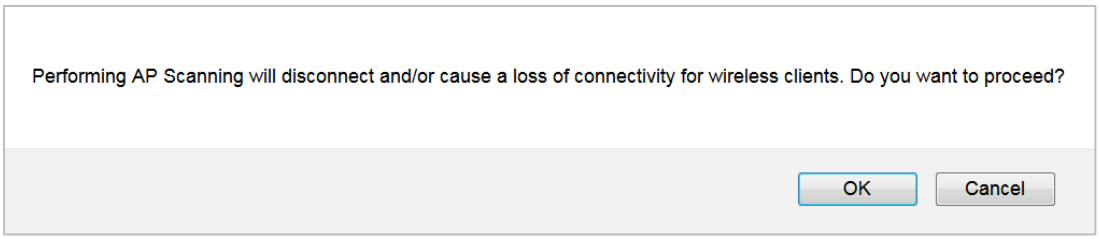
Wireless rogue device detection and prevention

The SonicPoints can be configured in dedicated sensor mode to focus on rogue device detection and prevention, either passively or proactively on both the 2.4GHz and 5GHz bands. Both bands can be scanned even if only one is in use. The rogue device can be analyzed to report whether it is connected to the network and if it is blocked by a wired or wireless mechanism.

To scan rogue devices, navigate to the **SonicPoint > IDS** page. Select the type of scan to perform from the **Perform SonicPoint Scan** drop-down list.



A pop-up message will warn you that performing the scan will cause all current wireless clients to be disconnected. Click **OK** to proceed with the scan.



Remote MAC access control

The **Enable Remote MAC Access Control** option has been added for SonicPoints.

In **SonicPoint > SonicPoints**, when a VAP is selected in the **802.11n Radio Virtual AP Group** drop-down menu on the **Settings** tab, this section is not available.

Select **Enable Remote MAC Access Control** to enforce 802.11n wireless access control based on a MAC-based authentication policy in a remote Radius server.

CAUTION: You cannot enable the **Remote MAC address access control** option at the same time that the **IEEE 802.11i EAP** is enabled. If you try to enable the **Remote MAC address access control** option at the same time that the **IEEE 802.11i EAP** is enabled, you receive the following error message:

NOTE: Remote MAC address access control cannot be set when IEEE 802.11i EAP is enabled.

Resolved issues

The following issues are resolved in this release.

AppFlow

Resolved issue	Issue ID
The IPFIX netflow data sent from the firewall to the external netflow collector randomly shows -ve or a large, incorrect duration for the flows and sometimes has the wrong timestamp of Jan 1, 1970. Occurs when there is a flow message for opening a connection. The finish time is incorrect due to a negative number being sent.	152294

Content Filtering

Resolved issue	Issue ID
Users may experience slow web browsing and slowness in the local network. Some web sites take a long time to load and might not display at all. Occurs when a WebSense server is located upstream of the firewall, connected via a switch and the X1 interface of the firewall.	154107
HTTP traffic is very slow. Occurs when WebSense is enabled.	139990

Firewall

Resolved issue	Issue ID
Access rules are not created for LAN > WAN, DMZ > WAN, and WLAN > WAN. Occurs when an interface is set to the DMZ zone and another interface is set to the WLAN zone and then the Firewall > Access Rules page is viewed.	153047

Log

Resolved issue	Issue ID
The Log Monitor page stops responding and displays “Processing Please wait...”. Occurs when VPN names include the pipe character "|", which is also used for the table format in the Log Monitor page.	153449
Log events are not filtered according to the string entered in the Filter field. Occurs when characters are entered in the Filter field on the Log Monitor page.	145567

Networking

Resolved issue	Issue ID
An IP Helper policy for user defined protocols cannot be deleted. Occurs when the policy is deleted and then created again, followed by attempting to delete the protocols and the policy.	154543
The DHCP server in SonicOS cannot allocate IP address leases for a period of time. Occurs when the number of DHCP clients has reached the limit and certain settings require adjustment so that expired leases can be recycled more aggressively.	137700

SSL VPN

Resolved issue	Issue ID
SSLVPN Enforcement does not work on the WLAN zone. The user is redirected to the SSLVPN portal logon page, but it does not open. Occurs when browsing to any HTTP website from a client on the WLAN zone.	154065
Cannot associate an SSLVPN client to X1 when it is in the primary L2B mode. Occurs when the LAN SSLVPN access for this topology has not yet been enabled.	153576
An error occurs when the SSLVPN Enforcement for WLAN zone is disabled. Occurs when editing or disabling the SSLVPN Enforcement of a WLAN zone object.	153482
Users cannot launch the NetExtender client. Occurs when a user has installed NetExtender from the SSL VPN portal using Internet Explorer 11.	152827

Switching

Resolved issue	Issue ID
No reply is received when pinging a static IP address for a trunk port and its VLAN sub-interface, such as X5:V100. Occurs when a client receives a DHCP address from X5:V100 and then attempts to ping the interface at its static IP address.	153099

Users

Resolved issue	Issue ID
Local or LDAP users or local administrators are logged out of the firewall after less than a minute. Local users must manually log in again. Occurs when running SonicOS 6.2.0.0 and Show User Login Status Window is not enabled.	154227

Wireless

Resolved issue	Issue ID
Guest Authentication and WLAN to WAN traffic can fail and logs the message “Guest login denied. Guest <name> is already logged in. Please try again later.” Occurs when Guest Services is enabled on the WLAN zone and a wireless client connects, receives a DHCP lease and successfully authenticates as a guest user, and then the client machine is changed to a static IP address. When the client attempts to access an external website, the page redirects to the SSLVPN user logon page, but the guest user cannot authenticate.	154303
A wireless client cannot connect to a SonicPoint AC if WPA2-EAP is selected for authentication. The WLAN > WAN RADIUS authentication packet source is NAT’d into the WLAN interface instead of the WAN interface. Occurs when the firewall is rebooted after it was working fine for wireless clients using the SonicPoint with WPA2-EAP and a RADIUS server for authentication.	153039
Throughput is always higher with lowest indexed Virtual Access Point object. Occurs when more than one Virtual Access Point is configured for a SonicPoint.	147509
No Virtual Access Point Groups can be added. Occurs when clicking the Add Group button on the SonicPoint > Virtual Access Point page and there are currently no VAP Groups displayed in the page.	143797

Known issues

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

High Availability

Known issue	Issue ID
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.	152565

Log

Known issue	Issue ID
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.	149458

Networking

Known issue	Issue ID
The WAN to WAN HTTPS/HTTP management access rule is not automatically added for the X1 WAN interface. Occurs when X1 WAN Mode is initially configured as Static IP with Management over HTTPS enabled and a static IP address is assigned, and then the WAN Mode is changed to PPTP or L2TP.	155245
Oversize packets cannot pass from one interface to another on the firewall. Occurs when using IPv6 and Jumbo Frames is enabled, with the MTU set to 9000 on both interfaces.	155083
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.	153350
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.	153267
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.	153096

SSL VPN

Known issue	Issue ID
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.	154958

System compatibility

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

Dell SonicWALL WXA support

The Dell SonicWALL WXA 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 6.2.2.0. The recommended firmware version for the WXA 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.

After your Dell SonicPoint ACi, ACi, or N2 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.

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:

https://support.software.dell.com/download/downloads?id=5601743

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/.

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

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

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: 1/6/2015

232-002762-00 Rev A