



SonicWall Wireless Network Manager

Release Notes

Wireless Network Manager is a cloud-based management system used to configure, manage, and monitor a wireless network. These release notes provide information about the SonicWall Wireless Network Manager release.

Versions:

- [Version 4.4.0](#)
- [Version 4.3.2](#)
- [Version 4.3.1](#)
- [SonicWave Firmware Upgrade](#)
- [Version 4.3.0-10](#)
- [SonicWaveFirmware Upgrade](#)
- [Version 4.2.0-9](#)
- [Version 4.2.0](#)
- [Version 4.1](#)
- [Version 4.0.25](#)
- [Version 4.0](#)

For additional information, refer to the [Wireless Network Manager document set](#).

Version 4.4.0

March 2024

Important

- SonicWall Wireless Network Manager components must be registered on [MySonicWall](#) to enable full functionality and the benefits of Wireless Network Manager services, updates, and technical support. Log in or register for a MySonicWall account at <https://mysonicwall.com>.
- Standard SonicWave access points include Secure WiFi wireless cloud and support services. Additional advanced wireless cloud and security subscription services, including Capture ATP, Content Filtering Service, Cloud Gateway Anti-Virus, and Geo-IP and Botnet Security Services are available for purchase separately at [MySonicWall](#). After logging in, navigate to **Product Management > My Products**.

Compatibility and Installation Notes

The following compatibility and installation notes apply to this release of Wireless Network Manager.

Browser Requirements

For Wireless Network Manager use the latest browser with HTML5 support.

Supported SonicWave Access Points

Wireless Network Manager 4.4 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
<ul style="list-style-type: none">• 224w• 231c• 231o	<ul style="list-style-type: none">• 432e• 432i• 432o	<ul style="list-style-type: none">• 621• 641• 681

① | **NOTE:** The SonicWave access points require the following minimum SonicWave firmware build levels:

- For SonicWave 200 Series, the minimum build level is 9.2.4.7-7.
- For SonicWave 400 Series, the minimum build level is 9.1.4.7-7.
- For SonicWave 600 Series, the minimum build level is 9.6.4.7-7.

Supported SonicWall Switches

Wireless Network Manager 4.4 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
<ul style="list-style-type: none">• SWS12-8• SWS12-8FPOE• SWS12-10FPOE	<ul style="list-style-type: none">• SWS14-24• SWS14-24FPOE• SWS14-48• SWS14-48FPOE

① | **NOTE:** Switch management support requires SonicWall Switch firmware version 1.2.0.2-6 or later.

What's New

- **Syslog Server Support** - Ability to redirect all events and alerts for either an individual AP or all APs to a local syslog server.
- **Packet Capture** - Ability to capture packets in PCAP format on wired and wireless interfaces.
- **Client Load Balancing** - Client load balancing feature uses IEEE 802.11v to steer the client to the best available AP to improve download and upload performance while reducing loss and latency for mission-critical applications.
- WPA3 Enhanced Open (OWE) transition mode support

- **BSS Coloring on SonicWaveAX** - Support for BSS coloring method as defined in 802.11ax standard, to reduce co-channel interference
- **Walled Garden Support in Captive Portal** - A walled garden feature enables administrator to create an allowed list of URLs and IP addresses that users of a captive portal is allowed to access prior to authentication.
- **WNM User Console Session Timeout** - Enhanced user experience, as Admins can now set the maximum and minimum timeout clock.
- **Search for MAC address and Port/Switch/Location** - Users can search for a client by their MAC address and discover the switch, port, and location it is associated with.
- **Time Management options for PoE switch ports** - Administrator can define a periodic or static time schedule in Schedule Objects.

Resolved Issues

Issue ID	Issue Description
WSC-5141	The radio band and radio channel can't be displayed on the Device page, when country Morocco-MA is selected.
WSC-5123	The RF spectrum heatmap is not displayed for the APs with the country codes AZ, EG, IR, JO, MY, OM, AE, and GB.
WSC-5097	The 802.1X doesn't work after rebooting.
WSC-5069	Enhancing the usability of filters.
WSC-4955	WNM LOG does not display the AP policy name after the AP policy parameter is edited.
WSC-4945	The Switch reboot button on dashboard is not working.
WSC-4885	Switch policy - Admin/Password creates confusion for the users as getting error messages after adding a new user and password in the right format.
WSC-4864	The Native VLAN in a port doesnot change automatically when adding or removing the port to or from untagged ports, by the graphical tool.
WSC-4763	Behavior modification not to auto-expand the Default grouping of Zones, Policies, etc.
WSC-4759	Allow multiple selections in notifications.
WSC-4710	The radio channel is not displayed on the Device page when using wide 160MHz channel.

Known Issues

There are no Known Issues in this release.

Additional References

WSC-5134, WSC-4916

Version 4.3.2

December 2023

Important

- WiFi Cloud Manager (WCM) has been renamed to Wireless Network Manager.
- SonicWall Wireless Network Manager components must be registered on [MySonicWall](https://mysonicwall.com) to enable full functionality and the benefits of Wireless Network Manager services, updates, and technical support. Log in or register for a MySonicWall account at <https://mysonicwall.com>.
- Standard SonicWave access points include Secure WiFi wireless cloud and support services. Additional advanced wireless cloud and security subscription services, including Capture ATP, Content Filtering Service, Cloud Gateway Anti-Virus, and Geo-IP and Botnet Security Services are available for purchase separately at [MySonicWall](https://mysonicwall.com). After logging in, navigate to **Product Management > My Products**.

Compatibility and Installation Notes

The following compatibility and installation notes apply to this release of Wireless Network Manager.

Browser Requirements

For Wireless Network Manager use the latest browser with HTML5 support.

Supported SonicWave Access Points

Wireless Network Manager 4.4 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
<ul style="list-style-type: none">• 224w• 231c• 231o	<ul style="list-style-type: none">• 432e• 432i• 432o	<ul style="list-style-type: none">• 621• 641• 681

NOTE: The SonicWave access points require the following minimum SonicWave firmware build levels:

- For SonicWave 200 Series, the minimum build level is 9.2.4.7-7.
- For SonicWave 400 Series, the minimum build level is 9.1.4.7-7.
- For SonicWave 600 Series, the minimum build level is 9.6.4.7-7.

Supported SonicWall Switches

Wireless Network Manager 4.4 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
<ul style="list-style-type: none">• SWS12-8• SWS12-8POE• SWS12-10FPOE	<ul style="list-style-type: none">• SWS14-24• SWS14-24FPOE• SWS14-48• SWS14-48FPOE

① | **NOTE:** Switch management support requires SonicWall Switch firmware version 1.2.0.2-6 or later.

What's New

- A pop-up window has been added to notify users to change their account passwords. This pop-up is a reminder of the New Password criteria introduced in 4.3.1 WNM release.

The New Password Criteria (introduced in 4.3.1):

- Password must be at least 10 characters long.
- Password must be at least including a capital letter.
- Password must be at least including a number.
- Allowed characters are %-._~:/#[]@*

① | **NOTE:** Switch will continue to communicate with Wireless Network Manager using existing passwords

① | **NOTE:** Wireless Network Manager will prompt user to change password to meet new password criteria before pushing configuration update on switches.

Users can update passwords after logging in to Wireless Network Manager from **Network > Devices > Switches > Configure > Switch Config > General** Tab, or by updating the policy assigned to switch from the **Policies > Switch Policies > Edit Switch Policy > Switch Config > General > User Management** option.

Resolved Issues

Issue ID	Issue Description
WSC-4715	A switch port is accepting multiple VLAN memberships as untagged.

Known Issues

Issue ID	Issue Description
WSC-4885	Switch policy - Admin/Password creates confusion for the users as getting error messages after adding a new user and password in the right format.

Issue ID	Issue Description
WSC-4864	The Native VLAN in a port doesnot change automatically when adding or removing the port to or from untagged ports, by the graphical tool.

Additional References

WSC-4871

Version 4.3.1

November 2023

Important

- WiFi Cloud Manager (WCM) has been renamed to Wireless Network Manager.
- SonicWall Wireless Network Manager components must be registered on [MySonicWall](https://mysonicwall.com) to enable full functionality and the benefits of Wireless Network Manager services, updates, and technical support. Log in or register for a MySonicWall account at <https://mysonicwall.com>.
- Standard SonicWave access points include Secure WiFi wireless cloud and support services. Additional advanced wireless cloud and security subscription services, including Capture ATP, Content Filtering Service, Cloud Gateway Anti-Virus, and Geo-IP and Botnet Security Services are available for purchase separately at [MySonicWall](https://mysonicwall.com). After logging in, navigate to **Product Management > My Products**.

Compatibility and Installation Notes

The following compatibility and installation notes apply to this release of Wireless Network Manager.

Browser Requirements

For Wireless Network Manager use the latest browser with HTML5 support.

Supported SonicWave Access Points

Wireless Network Manager 4.4 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
<ul style="list-style-type: none"> • 224w • 231c • 231o 	<ul style="list-style-type: none"> • 432e • 432i • 432o 	<ul style="list-style-type: none"> • 621 • 641 • 681

① | **NOTE:** The SonicWave access points require the following minimum SonicWave firmware build levels:

- For SonicWave 200 Series, the minimum build level is 9.2.4.7-7.
- For SonicWave 400 Series, the minimum build level is 9.1.4.7-7.
- For SonicWave 600 Series, the minimum build level is 9.6.4.7-7.

Supported SonicWall Switches

Wireless Network Manager 4.4 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
<ul style="list-style-type: none">• SWS12-8• SWS12-8POE• SWS12-10FPOE	<ul style="list-style-type: none">• SWS14-24• SWS14-24FPOE• SWS14-48• SWS14-48FPOE

① | **NOTE:** Switch management support requires SonicWall Switch firmware version 1.2.0.2-6 or later.

What's New

- **New Password Criteria for Switch** - This release introduces a new password criteria for switches managed from Wireless Network Manager. All the existing switches managed from Wireless Network Manager should meet new password criteria for all users configured in a switch. The new password criteria requires updating passwords for all users configured in switch if the existing password does not meet the new password criteria. If switch is already configured with a password that meets the new password criteria, users can continue using existing passwords.

The New Password Criteria:

- Password must be at least 10 characters long
- Password must be at least including a capital letter.
- Password must be at least including a number.
- Allowed characters are %-._~:/#[]@*

① | **NOTE:** Switch will continue to communicate with Wireless Network Manager using existing passwords.

① | **NOTE:** Wireless Network Manager will prompt user to change password to meet new password criteria before pushing configuration update on switches.

Users can update passwords after logging in to Wireless Network Manager from **Network > Devices > Switches > Configure > Switch Config > General** Tab, or by updating the policy assigned to switch from the **Policies > Switch Policies > Edit Switch Policy > Switch Config > General > User Management** option.

- **MAC Authentication Bypass (MAB)** - Allows a device without an 802.1x supplicant running on it to authenticate against RADIUS via MAC address.

- **Import mac addresses** - Helps the users to import multiple mac addresses on Wireless Network Manager using spreadsheets.
- **Scheduled Reboot (AP)** - Allows the users with a new SonicWave auto reboot function by schedule in Wireless Network Manager.

Resolved Issues

Issue ID	Issue Description
WSC-4685	Issue with a social account: Guest portal > social account users are unable to connect to SSID with a social account using Gmail authentication.
WSC-4649	The reset notification settings of Threat fails.
WSC-4648	Switch doesn't sync settings from WNM if VLAN 1 name contains + symbol particularly with latest firmware 1.2.0.1-6.
WSC-4610	The social login always fails when SSID contains space.
WSC-4605	Creating a schedule object in Tenant fails.
WSC-4602	Not able to Tag/Untag LAG Ports properly on WNM profile.
WSC-4558	The switch Notify API doesn't accept special characters.
WSC-4557	The switch Group API doesn't accept special characters.
WSC-4538	On the Edit SNMP Policy page, the UDP Port , Timeout , and Retry fail when the user enters the symbol ".".
WSC-4537	Tag Identifier doesn't accept special characters for Target Params .
WSC-4522	Enhancement to display the client vendor as <i>local mac</i> instead of <i>unknown</i> for local mac address.
WSC-4513	NTP sync time takes too long, and fails the switch auto upgrade function when the auto upgrade is set after three minutes.
WSC-4504	Clients displayed as 160MHZ (4x4) 802.11.ax even when their channel bandwidth are not configured as 160MHZ.
WSC-4491	IGMP Snooping Mrouter and blocked-router ports information could not be applied to local switch.
WSC-4486	The set PoE USER DEFINED value fails to display on the Switch Policy > Ports page. It shows wrong graphical user interface.
WSC-4477	An item with the same group name but different security mode can't be added to the Access List.
WSC-4448	On the Switch Device page > VLAN tab, Remark CoS/802.1p shows empty, when Voice VLAN Enable is selected.
WSC-4443	The Switch Device > VLAN configurations can't be saved.
WSC-4440	Enable maximum entries for each item in the Switch SNMP Policy .
WSC-4387	Unexpected graphics show up on the Switch SNMP Policy page.
WSC-3657	On the Add Matched Objects page, user is able to create invalid IPv4 Subnet Mask.

Issue ID	Issue Description
WSC-3603	Adding a new user is success even when the Password and Confirm Password fields are empty, on the Switch Config > General page.
WSC-3496	User can create illogical Matched Group Names using symbols in Wireless Network Manager.
WSC-3495	User can create illogical Matched Group Names using symbols in Wireless Network Manager
WSC-3488	Filter is not working as expected for Network >Topology .
WSC-3470	The Description field on the Voice VLAN >Add OU Address should not take more than 32 characters.
WSC-3456	The IPV4 Route Destination IP cannot be configured as 0.0.0.0, the local GUI can configure destination IP as 0.0.0.0.
WSC-3372	Clicking on the VLAN tab on the Network > Devices page should navigate to Ports > VLAN tab in the Switch Config window.
WSC-3187	The USER DEFINED column should not be editable when the PoE type is Auto .
WSC-3155	Input reboot in console, there should be a System Restart alert in the Alerts page after the switch restarted
WSC-3135	For Add New Security Policy , there should not be a Matched Group displayed when Matched Group exists.
WSC-3130	Invalid network informaion getting applied to local switch on Switch Policy > VLAN page.
WSC-3075	On the Logs page, the switch sub type is different from Notification Center Logs Switch Sub Type ; the LBD Subtype is missing.
WSC-1822	Remove the Scan Radio page on the standalone GUI and the related CLI command for 224w.

Known Issues

Issue ID	Issue Description
WSC-4704	The data of CPU is not accurate on the Device page
WSC-4667	On the Switch Config > System tab, the Static Route Destination IP does not respond as required.
WSC-4565	The connected client is not displayed on the report Topology part.

Additional References

WSC-4546

SonicWave Firmware Upgrade

 **CAUTION:** This is a specialty version, use only if directed by Support.

June 2023

Compatibility and Installation Notes

The following compatibility and installation notes apply to this release of SonicWave 200, 400, and 600 Series firmware 9.2.4.6_10/9.1.4.6_10/9.6.4.6_10.

What's New

- Fixed MAC-IP anti spoofing issue and other vulnerability fixes.

Resolved Issues

Issue ID	Issue Description
ACP-293	Updated the Nginx version on the APIs to the latest version.
WSC-4543	MAC-IP Anti spoof showing clients IP address with SonicWave 432i MAC address in spoof detected list.

Version 4.3.0-10

April 2023

Important

- WiFi Cloud Manager (WCM) has been renamed to Wireless Network Manager.
- SonicWall Wireless Network Manager components must be registered on **MySonicWall** to enable full functionality and the benefits of Wireless Network Manager services, updates, and technical support. Log in or register for a MySonicWall account at <https://mysonicwall.com>.
- Standard SonicWave access points include Secure WiFi wireless cloud and support services. Additional advanced wireless cloud and security subscription services, including Capture ATP, Content Filtering Service, Cloud Gateway Anti-Virus, and Geo-IP and Botnet Security Services are available for purchase separately at **MySonicWall**. After logging in, navigate to **Product Management > My Products**.

Compatibility and Installation Notes

The following compatibility and installation notes apply to this release of Wireless Network Manager.

Browser Requirements

For Wireless Network Manager use the latest browser with HTML5 support.

Supported SonicWave Access Points

Wireless Network Manager 4.4 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
<ul style="list-style-type: none">• 224w• 231c• 231o	<ul style="list-style-type: none">• 432e• 432i• 432o	<ul style="list-style-type: none">• 621• 641• 681

① | **NOTE:** The SonicWave access points require the following minimum SonicWave firmware build levels:

- For SonicWave 200 Series, the minimum build level is 9.2.4.6-8.
- For SonicWave 400 Series, the minimum build level is 9.1.4.6-8.
- For SonicWave 600 Series, the minimum build level is 9.6.4.6-8.

Supported SonicWall Switches

Wireless Network Manager 4.4 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
<ul style="list-style-type: none">• SWS12-8• SWS12-8POE• SWS12-10FPOE	<ul style="list-style-type: none">• SWS14-24• SWS14-24FPOE• SWS14-48• SWS14-48FPOE

① | **NOTE:** Switch management support requires SonicWall Switch firmware version 1.2.0.0-5 or later.

What's New

- **TOTP Authentication** - Time-based one-time password (TOTP) authentication for enhanced security and better user experience.
- **Switch SNMP** - Added SNMP feature within the user interface to manage switches.
- **Daylight Savings Time** - Automatic adjusts time schedule for the beginning and end of Day light savings time.
- **Customize security blockpage** - Custom CFS block page or redirect URL to display company logo or customized message.
- **Pagination for Devices and Clients page** - An improved user interface for Devices and Clients by paginating for easy access.

Resolved Issues

Issue ID	Issue Description
WSC-3466	Router static and forbidden ports information in VLAN > IGMP/MLD tab now changes when the model is switched.
WSC-4116	Added CLI command for multiple PSK.
WSC-4261	Topology page is blank when clicked on Unmanaged Switch button.
WSC-4301	Incorrect port color is displayed on the Device page when the Port's Speed is changed to 100M_F.
WSC-4334	USB0 interface does not appear when plugged to 4G USB.
WSC-4346	iOS devices cannot connect to SonicWave.
WSC-4353	SonicWaves 432i becomes unresponsive after auto-upgrading WNM.
WSC-4403	Disabled VLAN VAP HTTPS/HTTP/SSH port and replaced HTTPS for Client diagnostic page to enforce security.
WSC-4458	QoS policy doesn't synchronize to standalone GUI (Graphical User Interface)

Known Issues

Issue ID	Issue Description
WSC-4489	The radius server related configuration is not removed after clearing the configuration on cloud.
WSC-4491	Router and blocked-router ports information does not apply to local switch.
WSC-4513	Due to longer NTP sync time, switch auto upgrade function doesn't work after setting to 3 minutes.

Additional References

WSC-4328

SonicWaveFirmware Upgrade

March 2023

Compatibility and Installation Notes

The following compatibility and installation notes apply to this release of SonicWave 200, 400, and 600 Series firmware 9.2.4.2_6/9.1.4.2_6/9.6.4.5_6.

What's New

- OpenSSL vulnerability fix

Resolved Issues

Issue ID	Issue Description
WSC-4353	Fixed an issue with Sonicwave 432i that becomes unresponsive after autoupgrade of WNM.
WSC-4334	USB0 interface does not appear when plugged to 4G USB.
WSC-4262	iOS devices cannot connect to SonicWave.
ACP-272	A timing-based side channel exists in the Open SSL RSA Decryption implementation.

Version 4.2.0-9

February 2023

Important

- WiFi Cloud Manager (WCM) has been renamed to Wireless Network Manager.
- SonicWall Wireless Network Manager components must be registered on [MySonicWall](https://mysonicwall.com) to enable full functionality and the benefits of Wireless Network Manager services, updates, and technical support. Log in or register for a MySonicWall account at <https://mysonicwall.com>.
- Standard SonicWave access points include Secure WiFi wireless cloud and support services. Additional advanced wireless cloud and security subscription services, including Capture ATP, Content Filtering Service, Cloud Gateway Anti-Virus, and Geo-IP and Botnet Security Services are available for purchase separately at [MySonicWall](https://mysonicwall.com). After logging in, navigate to **Product Management > My Products**.

Compatibility and Installation Notes

The following compatibility and installation notes apply to this release of Wireless Network Manager.

Browser Requirements

For Wireless Network Manager use the latest browser with HTML5 support.

Supported SonicWave Access Points

Wireless Network Manager 4.4 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
<ul style="list-style-type: none"> • 224w • 231c • 231o 	<ul style="list-style-type: none"> • 432e • 432i • 432o 	<ul style="list-style-type: none"> • 621 • 641 • 681

① | **NOTE:** The SonicWave access points require the following minimum SonicWave firmware build levels:

- For SonicWave 200 Series, the minimum build level is 9.2.4.2-5.
- For SonicWave 400 Series, the minimum build level is 9.1.4.2-5.
- For SonicWave 600 Series, the minimum build level is 9.6.4.5-5.

Supported SonicWall Switches

Wireless Network Manager 4.4 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
<ul style="list-style-type: none"> • SWS12-8 • SWS12-8POE • SWS12-10FPOE 	<ul style="list-style-type: none"> • SWS14-24 • SWS14-24FPOE • SWS14-48 • SWS14-48FPOE

① | **NOTE:** Switch management support requires SonicWall Switch firmware version 1.2.0.0-5 or later.

What's New

This maintenance release provides fixes for previously reported issues.

Resolved Issues

Issue ID	Issue Description
WSC-4348	Unable to add device even with a valid license.

Version 4.2.0

January 2023

Important

- WiFi Cloud Manager (WCM) has been renamed to Wireless Network Manager.
- SonicWall Wireless Network Manager components must be registered on [MySonicWall](https://mysonicwall.com) to enable full functionality and the benefits of Wireless Network Manager services, updates, and technical support. Log in or register for a MySonicWall account at <https://mysonicwall.com>.
- Standard SonicWave access points include Secure WiFi wireless cloud and support services. Additional advanced wireless cloud and security subscription services, including Capture ATP, Content Filtering Service, Cloud Gateway Anti-Virus, and Geo-IP and Botnet Security Services are available for purchase separately at [MySonicWall](https://mysonicwall.com). After logging in, navigate to **Product Management > My Products**.

Compatibility and Installation Notes

The following compatibility and installation notes apply to this release of Wireless Network Manager.

Browser Requirements

For Wireless Network Manager use the latest browser with HTML5 support.

Supported SonicWave Access Points

Wireless Network Manager 4.4 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
<ul style="list-style-type: none">• 224w• 231c• 231o	<ul style="list-style-type: none">• 432e• 432i• 432o	<ul style="list-style-type: none">• 621• 641• 681

① | **NOTE:** The SonicWave access points require the following minimum SonicWave firmware build levels:

- For SonicWave 200 Series, the minimum build level is 9.2.4.2-5.
- For SonicWave 400 Series, the minimum build level is 9.1.4.2-5.
- For SonicWave 600 Series, the minimum build level is 9.6.4.5-5.

Supported SonicWall Switches

Wireless Network Manager 4.4 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
<ul style="list-style-type: none">• SWS12-8• SWS12-8POE• SWS12-10FPOE	<ul style="list-style-type: none">• SWS14-24• SWS14-24FPOE• SWS14-48• SWS14-48FPOE

① | **NOTE:** Switch management support requires SonicWall Switch firmware version 1.2.0.0-5 or later.

What's New

- **Wireless Security Policy schedule support** - Schedule the corresponding security policy at a specified time or periodically.
- **Clients** - Edit client friendly name, Kickoff client, and add client to special address group.
- **User Quota control** - Allows you to control the usage based on the user's account.

Resolved Issues

Issue ID	Issue Description
WSC-4256	Fixed an issue with WPA3 MuIPSK H2E for STA fails to connect into Sonicwave200.
WSC-4262	Low signal strength randomly on 2.4Ghz and 5Ghz.
WSC-4270	Unable to connect to LDAP server through TLS from the Guest SSID.
WSC-4281	RF monitor page remains empty when there is related info on Access Points.

Known Issues

Issue ID	Issue Description
WSC-4301	The port's color is incorrect on device page when the speed is changed.
WSC-4319	Switch does not appear in the device list when transferring the tenants.
WSC-4334	USB0 interface does not appear when plugged to 4G USB.

Additional References

WSC-4264

Version 4.1

September 2022

Important

- WiFi Cloud Manager (WCM) has been renamed to Wireless Network Manager.
- SonicWall Wireless Network Manager components must be registered on [MySonicWall](https://mysonicwall.com) to enable full functionality and the benefits of Wireless Network Manager services, updates, and technical support. Log in or register for a MySonicWall account at <https://mysonicwall.com>.
- Standard SonicWave access points include Secure WiFi wireless cloud and support services. Additional advanced wireless cloud and security subscription services, including Capture ATP, Content Filtering Service, Cloud Gateway Anti-Virus, and Geo-IP and Botnet Security Services are available for purchase separately at [MySonicWall](https://mysonicwall.com). After logging in, navigate to **Product Management > My Products**.

Compatibility and Installation Notes

The following compatibility and installation notes apply to this release of Wireless Network Manager.

Browser Requirements

For Wireless Network Manager use the latest browser with HTML5 support.

Supported SonicWave Access Points

Wireless Network Manager 4.4 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
<ul style="list-style-type: none">• 224w• 231c• 231o	<ul style="list-style-type: none">• 432e• 432i• 432o	<ul style="list-style-type: none">• 621• 641• 681

① | **NOTE:** The SonicWave access points require the following minimum SonicWave firmware build levels:

- For SonicWave 200 Series, the minimum build level is 9.2.4.1-8.
- For SonicWave 400 Series, the minimum build level is 9.1.4.1-8.
- For SonicWave 600 Series, the minimum build level is 9.6.4.4-9.

Supported SonicWall Switches

Wireless Network Manager 4.4 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
<ul style="list-style-type: none">• SWS12-8• SWS12-8POE• SWS12-10FPOE	<ul style="list-style-type: none">• SWS14-24• SWS14-24FPOE• SWS14-48• SWS14-48FPOE

① | **NOTE:** Switch management support requires SonicWall Switch firmware version 1.1.1.0-2 or later.

What's New

- **New PoE Switch** - New PoE Switch Model is now supported in dashboard and device page.
- **WPA3 and WiFi Alliance** - Support for WPA3 and WiFi Alliance certificate; 802.11r protocols for WPA3 PSK and WPA3 enterprise authentication type.

Resolved Issues

Issue ID	Issue Description
WSC-3618	Guest Vlan works when Global Guest Vlan is disabled and every guest port Vlan is enabled.
WSC-3828	Client label still exists even after selecting " Hide All labels " option.
WSC-4094	The operating system type of the same Android phone sometimes displays Linux and sometimes Android.
WSC-4154	The traffic data for the access point can't be displayed when a location containing more than one child location is selected.
WSC-4161	WPA3 client sometimes has a reconnect failure due to wrong VLAN ID when access point is enabled with multi PSK with dynamic VLAN.
WSC-4191	Accessing WNM GUI and options gives error: " Response error message:Internal server error " or " Response error message:Endpoint request timed ".
WSC-4260	Out of memory issue occurs to 5GHz's when reconnected continuously.

Known Issues

Issue ID	Issue Description
WSC-4256	WPA3 Multiple PSK for STA fails to connect to Sonicwave200.
WSC-4261	Blank page appears in Network > Devices when clicked on show topology button.

Additional References

WSC-4178, WSC-4167

Version 4.0.25

June 2022

Important

- SonicWall Wireless Network Manager components must be registered on [MySonicWall](#) to enable full functionality and the benefits of Wireless Network Manager services, updates, and technical support. Log in or register for a MySonicWall account at <https://mysonicwall.com>.
- Standard SonicWave access points include Secure WiFi wireless cloud and support services. Additional advanced wireless cloud and security subscription services, including Capture ATP, Content Filtering Service, Cloud Gateway Anti-Virus, and Geo-IP and Botnet Security Services are available for purchase separately at [MySonicWall](#). After logging in, navigate to **Product Management > My Products**.

Compatibility and Installation Notes

The following compatibility and installation notes apply to this release of Wireless Network Manager.

Browser Requirements

For Wireless Network Manager use the latest browser with HTML5 support.

Supported SonicWave Access Points

Wireless Network Manager 4.4 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
<ul style="list-style-type: none">• 224w• 231c• 231o	<ul style="list-style-type: none">• 432e• 432i• 432o	<ul style="list-style-type: none">• 621• 641• 681

① | **NOTE:** The SonicWave access points require the following minimum SonicWave firmware build levels:

- For SonicWave 200 Series, the minimum build level is 9.2.4.0-9.
- For SonicWave 400 Series, the minimum build level is 9.1.4.0-9.
- For SonicWave 600 Series, the minimum build level is 9.6.4.3-9.

Supported SonicWall Switches

Wireless Network Manager 4.4 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
<ul style="list-style-type: none">• SWS12-8• SWS12-8POE• SWS12-10FPOE	<ul style="list-style-type: none">• SWS14-24• SWS14-24FPOE• SWS14-48• SWS14-48FPOE

① | **NOTE:** Switch management support requires SonicWall Switch firmware version 1.1.1.0-2 or later.

What's New

This maintenance release provides fixes for previously reported issues.

Resolved Issues

Issue ID	Issue Description
WSC-4191	Accessing the WNM portal incurs the following errors Response error message:Internal server error or Response error message:Endpoint request timed .

Known Issues

No additional known issues.

Version 4.0

June 2022

Important

- WiFi Cloud Manager (WCM) has been renamed to Wireless Network Manager.
- SonicWall Wireless Network Manager components must be registered on [MySonicWall](https://mysonicwall.com) to enable full functionality and the benefits of Wireless Network Manager services, updates, and technical support. Log in or register for a MySonicWall account at <https://mysonicwall.com>.
- Standard SonicWave access points include Secure WiFi wireless cloud and support services. Additional advanced wireless cloud and security subscription services, including Capture ATP, Content Filtering Service, Cloud Gateway Anti-Virus, and Geo-IP and Botnet Security Services are available for purchase separately at [MySonicWall](https://mysonicwall.com). After logging in, navigate to **Product Management > My Products**.

Compatibility and Installation Notes

The following compatibility and installation notes apply to this release of Wireless Network Manager.

Browser Requirements

For Wireless Network Manager use the latest browser with HTML5 support.

Supported SonicWave Access Points

Wireless Network Manager 4.4 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
<ul style="list-style-type: none">• 224w• 231c• 231o	<ul style="list-style-type: none">• 432e• 432i• 432o	<ul style="list-style-type: none">• 621• 641• 681

NOTE: The SonicWave access points require the following minimum SonicWave firmware build levels:

- For SonicWave 200 Series, the minimum build level is 9.2.4.0-9.
- For SonicWave 400 Series, the minimum build level is 9.1.4.0-9.
- For SonicWave 600 Series, the minimum build level is 9.6.4.3-9.

Supported SonicWall Switches

Wireless Network Manager 4.4 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
<ul style="list-style-type: none">• SWS12-8• SWS12-8POE• SWS12-10FPOE	<ul style="list-style-type: none">• SWS14-24• SWS14-24FPOE• SWS14-48• SWS14-48FPOE

① | **NOTE:** Switch management support requires SonicWall Switch firmware version 1.1.1.0-2 or later.

What's New

- **Content Filtering Service (CFS) Support** - Intercepts TCP connections to pick up URL of HTTP or domain name in SSL SNI field of HTTPS for rating purpose and controls these connections for replay, drop and reject as needed after rating result matches policy.
- **Cloud Backend Updates**- Improves cloud system scalability and stability and improves performance.
- **Pre-Shared Key** - Supports private pre-shared keys (PPSK), or per user pre-shared keys, which allows easier use and management, compatibility for legacy clients, support for different VLANs, and increased security.
- **Wireless Setup Guide** - Provides a setup tool or wizard that can help walk you through the process of adding or configuring a new access point.
- **SAML Authentication** - Can be used to validate the identify of users accessing the wireless network.
- **DHCP Fingerprinting** - Allows the detection of an end operating system based on the DHCP exchange packets. Knowing the OS allows you to categorize the devices and decide what level of access they should have.
- **SonicWave 621** - Allows Wireless Network Manager to manage the new SonicWave 621 access point.

Resolved Issues

Issue ID	Issue Description
WSC-4003	EAP authentication takes a long time when Radius Server 1 is unreachable.
WSC-3978	When only AP or Switch view is selected on the Dashboard and the user clicks Alert/Threat center data to redirect to Alerts/Threat page, both AP and Switch are selected for View filter/Model field.
WSC-3891	SSID for 5G can't be disabled when a country with only 2.4G is selected.
WSC-3765	The Guest settings can't be saved when wrong format is used for radius server settings first and then changed to correct LDAP server settings.
WSC-3400	Tagged and untagged ports information in the VLAN tab should change per the switch model.

Known Issues

Issue ID	Issue Description
WSC-4161	WPA3 client sometimes has a reconnect failure due to wrong VLAN ID when access point is enabled with multi PSK with dynamic VLAN.
WSC-4154	The traffic data for the access point can't be displayed when a location containing more than one child location is selected.
WSC-4094	The operating system type of the same Android phone sometimes displays Linux and sometimes Android.

Additional References

WCS-2914

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The [Support Portal](#) provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year.

The [Support Portal](#) enables you to:

- View [Knowledge Base articles](#) and [Technical Documentation](#)
- View and participate in the [Community Forum](#) discussions
- View [Video Tutorials](#)
- Access [MySonicWall](#)
- Learn about [SonicWall Professional Services](#)
- Review [SonicWall Support services and warranty information](#)
- Register to [SonicWall University](#) for training and certification

About This Document

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

⚠ | **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.

Wireless Network Manager Release Notes

Updated - March 2024

232-005842-00 Rev M

Copyright © 2024 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' 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 products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME 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 SONICWALL AND/OR ITS AFFILIATES 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 SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make 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. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.