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 4.5.2
- Version 4.5.1
- Version 4.5.0
- Version 4.4.1
- 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 4.5.2

December 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 4.5.2 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
• 224w • 231c • 231o	• 432e • 432i • 432o	• 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 9.2.5.0-9.
- For SonicWave 400 Series, the minimum build level is 9.1.5.0-9.
- For SonicWave 600 Series, the minimum build level is 9.6.5.0-9.

Supported SonicWall Switches

Wireless Network Manager 4.5.2 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
• SWS12-8 • SWS12-8POE • SWS12-10FPOE	• SWS14-24 • SWS14-24FPOE • SWS14-48 • SWS14-48FPOE

ⓘ | **NOTE:** Switch management support requires SonicWall Switch firmware versions 1.3.0-3 for SWS12 versions, and 1.3.0-4 for SWS14 versions.

What's New

- This maintenance release provides the bug fixes for the previously reported issues.

Resolved Issues

Issue ID	Issue Description
WSC-5836	The Wireless Network Manager **Report Task** is not complete when there are many locations.
WSC-5812	Unable to change the SonicWave IP address to static in Wireless Network Manager.
WSC-5785	Incomplete chart in the Dashboard for Top Client by Traffic.
WSC-5774	Validate the phone number of unsupported characters.
WSC-5770	Validate session life time for a social account in the guest portal.

Known Issues

There are no Known Issues in this release.

Additional References

There are no Additional References in this release.

Version 4.5.1

October 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 4.5.1 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
• 224w • 231c • 231o	• 432e • 432i • 432o	• 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 9.2.5.0-9.
- For SonicWave 400 Series, the minimum build level is 9.1.5.0-9.
- For SonicWave 600 Series, the minimum build level is 9.6.5.0-9.

Supported SonicWall Switches

Wireless Network Manager 4.5.1 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
• SWS12-8 • SWS12-8POE • SWS12-10FPOE	• SWS14-24 • SWS14-24FPOE • SWS14-48 • SWS14-48FPOE

ⓘ | **NOTE:** Switch management support requires SonicWall Switch firmware version 1.3.0-3 or later.

What's New

- This maintenance release provides the bug fixes for the previously reported issues.

Resolved Issues

Issue ID	Issue Description
WSC-5753	Some of the SonicWave APs shows the blue firmware upgrade icon but the upgrading does not work as required.
WSC-5737	The position of the **Inherited from Default Policy** button in the **Switch Policy > Port tab** is incorrect.
WSC-5709	Include wireless client IP address and summary in the WNM reports.
WSC-5705	The **Inheritance Off** information is not accurate for the Switch Devices.

Issue ID	Issue Description
WSC-5704	The WNM Log does not display the VLAN Object edits done.
WSC-5703	The WNM Log does not display the Switch Port Policy edits done.
WSC-5696	The AP/Switch status does not get updated unless the user update it manually on the Wireless Network Manager dashboard.

Known Issues

Issue ID	Issue Description
WSC-5757	On the **Device** page, the **SSLVPN Inherit DNS domain** is not working, after the SSLVPN and DNS proxy with Bridge Mode are enabled for the AP.

Additional References

WSC-5754, WSC-5751, WSC-5743, WSC-5734, WSC-5683

Version 4.5.0

September 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 4.4.1 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
• 224w • 231c • 231o	• 432e • 432i • 432o	• 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 9.2.5.0-8.
- For SonicWave 400 Series, the minimum build level is 9.1.5.0-8.
- For SonicWave 600 Series, the minimum build level is 9.6.5.0-8.

Supported SonicWall Switches

Wireless Network Manager 4.4.1 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
• SWS12-8 • SWS12-8POE • SWS12-10FPOE	• SWS14-24 • SWS14-24FPOE • SWS14-48 • SWS14-48FPOE

ⓘ | **NOTE:** Switch management support requires SonicWall Switch firmware version 1.3.0-3 or later.

What's New

- **Switch Daylight (DST) configuration:** Wireless Network Manager now supports DST configuration in switch which will enable switches to automatically adjust switch time as per DST settings.
- **Simplified device on-boarding:** New work-flow to on-board device in Wireless Network Manager from the **Devices** page by moving device to the desired zone.
- **Audit log enhancements:** Wireless Network Manager now stores audit logs for 365 days. We have also fixed several bugs in the audit log area to ensure that all user activity is captured in WNM audit logs.
- **New WNM workflow for VLAN creation and Port Assignments:** Wireless Network Manager has a new workflow for VLAN creation and port assignments. We are introducing a VLAN object and switch port policy, simplifying creating and assignment of the same VLAN to multiple switches.

- **MSSP Monthly program for AP and Switches:** Wireless Network Manager supports service provider monthly program. WNM will be able to understand monthly licenses provisioned in MSW and enable the capability for AP and Switches as per the provisioned licenses.
- **UX improvements:** Wireless Network Manager provides options to keep the UX consistent. **Security Policy** is moved under **Policies** and all WNM objects are grouped under new menu option **Object**.
- **Alert enhancements:** Ability to configure instant or near real-time email alerts for conditions that requires immediate attention. Users can customize the list of email addresses to send notifications.

Resolved Issues

Issue ID	Issue Description
WSC-5542	The WNM Audit Log does not display the edits done on the **General/Notifcation/QOS** policies page.
WSC-5519	The WNM Audit Log does not display the Location edits done.
WSC-5498	The SAML guest access is not working on the SonicWave 600 series.
WSC-5380	The custom logo is not getting displayed on the report.
WSC-5330	The Group for link aggregation can't be configured to switch, if 802.1x for same port is Auto configured.
WSC-5281	The WNM Log does not display the SNMP policy edits done.
WSC-5047	The TCP Flags and ToS related configurations are not getting applied to the local switch.
WSC-5027	The WNM SNTP Log does not display the SNTP information edits done.
WSC-4667	When you provide letters in the **Destination IP** for the **Static Route (IPV4)**, there is no response.
WSC-4565	Connected client does not display the Topology on the Report.

Known Issues

Issue ID	Issue Description
WSC-5704	The WNM Log does not display the VLAN Object edits done.
WSC-5703	The WNM Log does not display the Switch Port Policy edits done.
WSC-5696	The AP/Switch status does not get updated unless the user update it manually on the Wireless Network Manager dashboard.

Additional References

WSC-5427, WSC-5301

Version 4.4.1

May 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 4.4.1 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
• 224w • 231c • 231o	• 432e • 432i • 432o	• 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 9.2.4.9-6.
- For SonicWave 400 Series, the minimum build level is 9.1.4.9-6.
- For SonicWave 600 Series, the minimum build level is 9.6.4.9-6.

Supported SonicWall Switches

Wireless Network Manager 4.4.1 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
• SWS12-8 • SWS12-8POE • SWS12-10FPOE	• SWS14-24 • SWS14-24FPOE • SWS14-48 • SWS14-48FPOE

ⓘ | **NOTE:** Switch management support requires SonicWall Switch firmware version 1.2.1.0-5 or later.

What's New

- **Monthly Scheduled Report -** Ability to generate report every month, selecting the specific day of the month and timezone to generate a report.
- **Wireless Session Count in the Reports -** Ability to count the use of each wireless access, regardless of the amount of time spent online.
- **Audit Log Default Priority Range -** The visibility of default audit logs to the customer is changed from two to three.

Resolved Issues

Issue ID	Issue Description
WSC-5335	Wireless Network Managerhas Sync issue with MySonicWall, and throwing the error 500.
WSC-5295	Wireless Network Manager does not update the email address for non-login logs.
WSC-5211	The VLAN configuration updates are not shown in the logs.
WSC-5191	The users with SAML have issues connecting with the Guest Portal.
WSC-5165	The Wireless Network Manager and mysonicwave certificates on the **Guest Portal Customized Splash** page displays that *the connection is not private with gstatic.com*.
WSC-5089	Audit log is not generated after **Switch Policy->Ports Configurations** are edited.
WSC-5041	Log messages are not generated for **Switch CLI**.
WSC-5017	The **View List** configuration is lost after adding a view with *SUBTREE MASK LEVEL is not 1*.
WSC-4963	Audit log displays all the port configurations, even after some port POE options are edited.
WSC-4789	Changes for the switch security policy L2 ACL Allow/Deny Mode is not synced to switch.
WSC-4783	Device name shows *none* on the **Logs** page.

Known Issues

Issue ID	Issue Description
WSC-5330	The Group for link aggregation can't be configured to switch, if 802.1x for same port is Auto configured.
WSC-5281	The WNM Log does not display the SNMP policy edits done.

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 4.5 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
• 224w • 231c • 231o	• 432e • 432i • 432o	• 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 4.5 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
• SWS12-8 • SWS12-8POE • SWS12-10FPOE	• SWS14-24 • SWS14-24FPOE • SWS14-48 • SWS14-48FPOE

ⓘ | **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 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 4.5 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
• 224w • 231c • 231o	• 432e • 432i • 432o	• 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 4.5 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
• SWS12-8 • SWS12-8POE • SWS12-10FPOE	• SWS14-24 • SWS14-24FPOE • SWS14-48 • SWS14-48FPOE

ⓘ | **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 %-._~:/#[]@*

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

  ⓘ **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.
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 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 4.5 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
• 224w • 231c • 231o	• 432e • 432i • 432o	• 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 4.5 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
• SWS12-8 • SWS12-8POE • SWS12-10FPOE	• SWS14-24 • SWS14-24FPOE • SWS14-48 • SWS14-48FPOE

ⓘ | **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 %-._~:/#[]@*

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

  ⓘ | **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 *local mac* instead of *unknown* 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 **Swtich SNMP Policy** page.
WSC-3657	On the **Add Matched Objects** page, user is able to create invalid IPv4 Subnet Mask.
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.

Issue ID	Issue Description
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 shoud 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 Mathced 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 4.5 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
• 224w • 231c • 231o	• 432e • 432i • 432o	• 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 9.2.4.6-8.
- 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 4.5 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
• SWS12-8 • SWS12-8POE • SWS12-10FPOE	• SWS14-24 • SWS14-24FPOE • SWS14-48 • SWS14-48FPOE

ⓘ | **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 does'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 doesnt 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 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 4.5 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
• 224w • 231c • 231o	• 432e • 432i • 432o	• 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 9.2.4.2-5.
- 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 4.5 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
• SWS12-8 • SWS12-8POE • SWS12-10FPOE	• SWS14-24 • SWS14-24FPOE • SWS14-48 • SWS14-48FPOE

ⓘ | **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 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 4.5 is supported for the following SonicWall SonicWave wireless access points:

SonicWave 200 Series	SonicWave 400 Series	SonicWave 600 Series
• 224w • 231c • 231o	• 432e • 432i • 432o	• 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 9.2.4.2-5.
- 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 4.5 is supported for the following SonicWall Switches:

Switch SWS12 Series	Switch SWS14 Series
• SWS12-8 • SWS12-8POE • SWS12-10FPOE	• SWS14-24 • SWS14-24FPOE • SWS14-48 • SWS14-48FPOE

ⓘ | **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 MulPSK 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

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
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University for training and certification

About This Document

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

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

ⓘ | **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 - December 2024
232-005842-00 Rev S

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.