SonicWall Switch 1.3.0

Release Notes

These release notes provide information about the SonicWall Switch 1.3.0 releases.

NOTE: The versioning convention for the Switch has been updated from a 4-digit format to a 3-digit format. Version 1.3.0 is a minor feature release.

Versions:

Version 1.3.0

December 2024

Compatibility and Installation Notes

The SonicWall Switch 1.3.0 release is supported on all SonicWall Switch platforms:

- SWS12-8
- SWS12-8POE
- SWS12-10FPOE
- SWS14-24
- SWS14-24FPOE

- SWS14-48
- SWS14-48FPOE

For information about obtaining the latest Switch firmware and upgrading the firmware image on your SonicWall Switch, see the *Switch Getting Started Guide* available on the Support portal at Switch Getting Started Guide.

What's New

SonicWall Switch 1.3.0 addresses inconsistencies in previous releases and offers enhancements, such as:

- The **Cable Diagnostics** feature is available, which helps identify any connectivity problems with cabling and provides information about where errors may have occurred.

  ⓘ | **NOTE:** There are cable length limitations in the Switch as per below table.

Series	Link down	Link up
SWS14	• ±15m when the cable length is less than 30m or between 110m and 130m • ± 7m when the cable length is between 30m and 110m	• ± 25m when the cable length is less than 40m • ± 20m when the cable length is between 40m and 110m
SWS12	• ± 6m deviation	• ±10m deviation

- **DHCP Snooping** status is available under **System Management > VLAN > 802.1Q**.
- **Trunk Port** settings allow the creation of a trunk by aggregating multiple links and configuring port trunking for increased bandwidth, available under **Switching > Link Aggregation > Trunk Port Settings**.
- More detailed Link Layer Discovery Protocol transmission information is available under **Switching > Link Layer Discovery Protocol > Global Settings**.

Attention

For Firewall Managed Switch:

Due to the introduction of the new secure password policy, the existing switch password may not be compatible with the new password policy and may result in Firewall-Switch connectivity issues.

Firmware version 1.2.0.2-6 introduced a new password policy. When upgrading from versions older than 1.2.0.2-6 to 1.3.0, existing passwords lead to Firewall-Switch connectivity and authorization problems.

Recommended steps for firewall-managed switch:

1. Upgrade the switch from the older build to the latest 1.3.0 through the firewall-managed user interface.
2. Change the switch password (Based on the new policy) in the firewall-managed user interface under **Device**>**Switch Network**>**Overview**> **Edit Switch** section.

Resolved Issues

Issue ID	Issue Description
SWO-1474	Under **System Management > VLAN > 802.1Q** the port tooltip shows incorrect configuration.
SWO-1564	In the standalone Switch user interface, the user cannot define **Radius Server** as a "Primary" or "Secondary" server.
SWO-2141	The ports diagram or picture shown for the POE ports is improper in the standalone GUI.
SWO-2178	Display **Authentication code** or **Device code** information in both the user interface and CLI.
SWO-2232	When Daylight Savings Time (DST) ends, the **Daylight Savings Time** option is disabled.
SWO-2374	The MAC forwarding table does not update when a device changes ports, so the MAC address cache entry remains until it expires.

Known Issues

Issue ID	Issue Description
SWO-2289	Block test cable diagnostics in CLI if port is disabled for switch.
SWO-2310	There is no banner displayed in the standalone Switch user interface when the Switch is managed by a Firewall.

Additional References

SWO-2208

Version 1.2.1.1

July 2024

Compatibility and Installation Notes

The SonicWall Switch 1.2.1.1 release is supported on all SonicWall Switch platforms:

- SWS12-8
- SWS12-8POE

- SWS12-10FPOE
- SWS14-24
- SWS14-24FPOE
- SWS14-48
- SWS14-48FPOE

For information about obtaining the latest Switch firmware and upgrading the firmware image on your SonicWall Switch, see the *Switch Getting Started Guide* available on the Support portal at Switch Getting Started Guide.

What's New

SonicWall Switch 1.3.0 fixes many issues found in previous releases and some significant enhancements like:

- After creating an MST instance under **Switching > Spanning Tree Protocol > Instance > Add Instance**, you can modify the Spanning Tree Protocol (STP) states for individual ports in **Switching > Port Settings**.
- Cloud management status is shown in the dashboard using green and red icons for easy understanding.
- In Switch CLI, untagged and member ports are displayed, making it challenging to locate tagged ports. Tagged ports are now listed separately in the Switch CLI.

Attention

For Firewall Managed Switch:

Due to the introduction of the new secure password policy, the existing switch password that might not be compatible with the new password policy may result in Firewall-Switch connectivity issues.

Firmware version 1.2.0.2-6 introduced a new password policy. When upgrading from versions older than 1.2.0.2-6 to 1.2.1.1, existing passwords lead to Firewall-Switch connectivity and authorization problems.

Recommended steps for firewall-managed switch:

1. Upgrade the switch from the older build to the latest 1.2.1.1 through the firewall-managed user interface.
2. Change the switch password (Based on the new policy) in the firewall-managed user interface under **Device**>**Switch Network**>**Overview**> **Edit Switch** section.

Resolved Issues

Issue ID	Issue Description
SWO-2020	DST end time is not working as expected in Pacific Time (US & Canada) (GMT-8:00).
SWO-2040	Remote logging configurations are not saved in the Switch UI.

Issue ID	Issue Description
SWO-2078	Configuring VLAN with LAG group ID and Other ports also throws an error.
SWO-2147	DST end time is not working as expected in the United Kingdom (GMT).
SWO-2174	Switch CLI and UI which are showing deleted entries after reboot.
SWO-2200	The deleted VLAN entry is showing after rebooting in CLI and UI.

Known Issues

Issue ID	Issue Description
SWO-2232	After daylight saving time ends, the **Daylight Savings Time** option is disabled.

Additional References

No additional issues.

Version 1.2.1.0

March 2024

Compatibility and Installation Notes

The SonicWall Switch 1.2.1.0 release is supported on all SonicWall Switch platforms:

- SWS12-8
- SWS12-8POE
- SWS12-10FPOE
- SWS14-24
- SWS14-24FPOE
- SWS14-48
- SWS14-48FPOE

For information about obtaining the latest Switch firmware and upgrading the firmware image on your SonicWall Switch, see the *Switch Getting Started Guide* available on the Support portal at Switch Getting Started Guide.

What's New

- Time Management options for PoE: Now, you can set a static or periodic schedule on the ports, ensuring that connected PoE devices are active only during business hours. This new feature saves energy, reduces electricity consumption, and lowers associated costs.
- Enhancements in the **Settings** section (**Import** and **Export**: For a consistent user experience across our products, Switch settings can now be imported or exported under the **System > Settings > Firmware and Settings** section.
- Friendly name or Hostname Update: You can enter the name you wish to use to identify the Switch. You can use up to 255 alphanumeric characters. This setting is available under **System Information**.

Attention

For Firewall Managed Switch:

Due to the introduction of the new secure password policy, the existing switch password that might not be compatible with the new password policy may result in Firewall-Switch connectivity issues.

Firmware version 1.2.0.2-6 introduced a new password policy. When upgrading from versions older than 1.2.0.2-6 to 1.2.1.0, existing passwords lead to Firewall-Switch connectivity and authorization problems.

Recommended steps for firewall-managed switch:

1. Upgrade the switch from the older build to the latest 1.2.1.0 through the firewall-managed user interface.
2. Change the switch password (Based on the new policy) in the firewall-managed user interface under **Device**>**Switch Network**>**Overview**> **Edit Switch** section.

Resolved Issues

Issue ID	Issue Description
SWO-1619	No options are available to add static MAC address to the LAG Group
SWO-1669	Unable to change the VLAN priority from **802.1p to match** to **Any** in class policy of the SonicWall standalone switch.
SWO-1670	Unable to change the **Type** of service from **DSCP to match** to **Any** in class policy of the SonicWall standalone switch.
SWO-1853	Unable to create Rmon Event List when the event type is SNMP Trap.
SWO-1854	Unable to create Rmon Event List when the event type is Log and Trap.
SWO-2036	IP address and UDP ports details displays blank in the **SNMP Target** address section.
SWO-2079	The CPU data on the Device page is not accurate.

Known Issues

Issue ID	Issue Description
SWO-2020	DST end time is not working as expected in Pacific Time (US & Canada) (GMT-8:00)
SWO-2147	DST end time is not working as expected in United Kingdom (GMT)

Additional References

SWO-2082, SWO-1755.

Version 1.2.0.2

November 2023

Compatibility and Installation Notes

The SonicWall Switch 1.2.0.2 release is supported on all SonicWall Switch platforms:

- SWS12-8
- SWS12-8POE
- SWS12-10FPOE
- SWS14-24
- SWS14-24FPOE
- SWS14-48
- SWS14-48FPOE

For information about obtaining the latest Switch firmware and upgrading the firmware image on your SonicWall Switch, see the *Switch Getting Started Guide* available on the Support portal at Switch Getting Started Guide.

What's New

- Secure password policy introduction.
- UI feature introduced to set daylight saving enable settings in SNTP system time tab.
- A tooltip is displayed to support special characters for passwords.

- 802.1x MAC Authentication Bypass allows a device without an 802.1x supplicant running on it to authenticate against RADIUS via MAC address.

Attention

New password policy:

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

For Firewall Managed Switch:

Due to the introduction of the new secure password policy, the existing switch password that might not be compatible with the new password policy may result in Firewall-Switch connectivity issues.

Recommended steps for firewall-managed switch:

1. Upgrade the switch from the older build to the latest 1.2.0.2-6 build through firewall-managed UI.
2. Change the switch password(Based on the new policy) in the firewall-managed UI under **Device**>**Switch Network**>**Overview**>Select **Edit Switch** section.

Resolved Issues

Issue ID	Issue Description
SWO-1935	Dynamic Voice VLAN works only on ports 1-28 and does not work beyond port 28.
SWO-1915	802.1x Network Access Control with TLS certificate were not working with SWS.
SWO-1884	LLDP version can be changed only through CLI, but there is no option to change through switching GUI.
SWO-1865	SonicWall Switch stops responding when the threshold set by Storm Control exceeds.
SWO-1859	Adding multiple VLANs to a switch interface throws a general error.
SWO-1841	The new OUI voice VLAN is not working when available.
SWO-1834	Unable to log in to SWS12-10FPOE switch through GUI.
SWO-1828	Unable to port shield firewall VLANs with switch port .
SWO-1823	Due to high latency while pinging, the SonicWall switches are causing VOIP and RDP traffic to drop.
SWO-1703	There is no option to edit users under SNMP.
SWO-1553	The error is displayed when any configuration change is done on a switch port with 802.1X enabled.

Issue ID	Issue Description
SWO-1497	Switch fails to complete 802.1x authentication when using the EAP-TLS protocol.

Known Issues

Issue ID	Issue Description
SWO-2036	IP address and UDP port details shows blank in the SNMP Target address section in the UI.
SWO-2030	Switch API Bearer authentication token should expire based on an Inactive session or traffic.
SWO-1974	Auto-Authorize is not coming up for GEN 6 and Gen7 firewall.
SWO-1651	Unable to access switch UI from a different VLAN when switching VLAN interface is used as a gateway for the client.

Version 1.2.0.1

May 2023

Compatibility and Installation Notes

The SonicWall Switch 1.2.0.1 release is supported on all SonicWall Switch platforms:

- SWS12-8
- SWS12-8POE
- SWS12-10FPOE
- SWS14-24
- SWS14-24FPOE
- SWS14-48
- SWS14-48FPOE

For information about obtaining the latest Switch firmware and upgrading the firmware image on your SonicWall Switch, see the *Switch Getting Started Guide* available on the Support portal at Switch Getting Started Guide.

What's New

- Tool tips were added to the LLDP timers and for MSTP since it is a supported STP protocol.
- The TCP Flag name was added in the IPv4 ACE header row for easy identification.

Resolved Issues

Issue ID	Issue Description
SWO-1855	SonicWall Switch stops working sporadically with SNMP V3 enabled or SNMP disabled, and switches are working fine
SWO-1754	Not able to edit or delete the **SNMP Group**
SWO-1744	VoIP phones are not getting DHCP IP from the **Voice VLAN** subnet
SWO-1713	The **Apply** button is not grayed out if the limit exceeds for RMON configuration and there is no pop-up message on the screen.
SWO-1712	User should not be allowed to enter out of range Source and Destination port values.
SWO-1708	The new PoE switch model switches like SWS12-8PoE, SWS12-10FPoE,SWS14-24FPoE, and SWS14-48FPOE running Switch image 1.2.0.0 by default and above cannot be downgraded to 1.1.1.0 and below versions.
SWO-1705	Issue adding Target Address under **SNMP**.
SWO-1702	Unable to delete **Group List** under **SNMP** tab.
SWO-1697	High Latency & Ping drop after firmware upgrade on 48 Port Switch-1.1.0.2-17s
SWO-1694	The active firmware display page does not show the firmware version clearly in **Firmware Images** tab
SWO-1661	Ping to an IP in local subnet fails when tried from UI
SWO-1649	SFP ports with transceivers are not active when using Auto-Negotiate
SWO-1618	Add Mac Entries text showing two times in MAC Adress Table section
SWO-1605	Switch IPv4 ACE list - Header row contents are not fully shown
SWO-1599	Reaching maximum number of ipv4 acl should display proper error message
SWO-1590	Under **QOS** > **Class mapping** table does not show complete information
SWO-1589	Under **QOS** name of **Class map** should not accept negative numbers and special characters.
SWO-1582	Under **QOS** > **Advanced policy**, creating new class policy with invalid mac address fails to throw error
SWO-1558	Binding ACL to ports should throw success prompt
SWO-1551	Adding duplicate entry for ipv4 ACL throws wrong error message
SWO-1544	Class map name should support only characters and positive numbers

Issue ID	Issue Description
SWO-1543	The character limit shown in the tooltip is incorrect for the name of the class map under QOS
SWO-1533	Unable to create a static route with subnet mask as 255.255.255.255
SWO-1439	The issue in adding the target address under **SNMP**
SWO-1046	Subnet Mask always saving as 255.255.255.255. When the user tried to save in CIDR subnet mask notation
SWO-1044	The user can save Switch Network IP with invalid IPs (like Loopback IP and Multicast IP).
SWO-764	Unable to download or export switch logs from standalone switch UI

Known Issues

No additional known issues.

Version 1.2.0.0-7

March 2023

Compatibility and Installation Notes

The SonicWall Switch 1.2.0.0 release is supported on all SonicWall Switch platforms:

- SWS12-8
- SWS12-8POE
- SWS12-10FPOE
- SWS14-24
- SWS14-24FPOE
- SWS14-48
- SWS14-48FPOE

For information about obtaining the latest Switch firmware and upgrading the firmware image on your SonicWall Switch, see the *Switch Getting Started Guide* available on the Support portal at Switch Getting Started Guide.

Resolved Issues

Issue ID	Issue Description
SWO-1882	OpenSSL Vulnerabilities 2023-02-07
SWO-1756	Cloud management is enabled automatically after the switch reboot

Known Issues

No additional known issues.

Version 1.2.0.0

July 2022

Compatibility and Installation Notes

The SonicWall Switch 1.2.0.0 release is supported on all SonicWall Switch platforms:

- SWS12-8
- SWS12-8POE
- SWS12-10FPOE
- SWS14-24
- SWS14-24FPOE
- SWS14-48
- SWS14-48FPOE

For information about obtaining the latest Switch firmware and upgrading the firmware image on your SonicWall Switch, see the *Switch Getting Started Guide* available on the Support portal at Switch Getting Started Guide.

Resolved Issues

Issue ID	Issue Description
SWO-1709	OpenSSL upgraded to 1.1.1o
SWO-1707	OpenSSL upgraded to remediate CVE-2022-0778
SWO-1706	SonicWall Switch Post-Authenticated remote code execution CVE-2022-2323

Known Issues

Issue ID	Issue Description
SWO-1739	The **Dynamic Mac Address** page does not show any entries on the Firewall Managed SwitchUI, but we can see all entries in the switch console and standalone switch UI.
SWO-1713	There is no pop-up message, and the apply button is not greyed out if the limit exceeds the RMON configuration.
SWO-1712	While creating the IPV4 ACE rule for TCP, entering negative and out-of-range values (Range: 0 - 65535) for the Source and Destination Port fields is possible but should not be allowed.
SWO-1708	The new PoE switch model switches like SWS12-8PoE, SWS12-10FPoE, SWS14-24FPoE, and SWS14-48FPOE running Switch image 1.2.0.0 by default and above cannot be downgraded to 1.1.1.0 and below versions.
SWO-1553	The error is displayed when any configuration change is done on a switch port with 802.1X enabled.
SWO-1497	Switch fails to complete 802.1x authentication when using the EAP-TLS protocol.

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.

Switch Release Notes
Updated - December 2024
Software Version - 1.3.0
232-005890-00 Rev J