AOS-S 16.11.0002
Release Notes

a Hewlett Packard
Enterprise company

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

These release notes include the following topics:

Important Information

To avoid damage to your equipment, do not interrupt power to the switch during a software update.

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, Aruba will replace racially insensitive terms and instead use the following new language:

Usage	Old Language	New Language
Switch Security	Master	Main
Switch Routing	Master	Main Router
Smart Link	Master-Slave	Primary-Secondary
Chassis Events, IPv6 Configuration, and Troubleshooting	Master-Slave	Management-Slot
Switch Stack	Master-Slave	Conductor-Member
Switch Security, Configuration and Routing	Blacklist, Whitelist	Denylist, Allowlist
Route Type	Blackhole Route	Null Route
Type of Hackers	Black Hat, White Hat	Unethical, Ethical

Version History

All released versions are fully supported by Hewlett Packard Enterprise, unless noted in the table.

Table 1: *Version History*

Version number	Software	Release Date	Remarks
16.11.0002	KB, WC, YC, and YA/YB	2021-10-04	Initial release of the 16.11 branch. Released, fully supported, and posted on the web.
16.11.0001	KB, WC, YC, and YA/YB	2021-09-13	Initial release of the 16.11 branch. Released, fully supported, and posted on the web.

Security Bulletin Subscription Service

You can sign up at https://sirt.arubanetworks.com/mailman/listinfo/security-alerts_sirt.arubanetworks.com to initiate a subscription to receive future Aruba Security Bulletin alerts via email.

Compatibility/Interoperability

The switch web agent supports the following web browsers:

- Internet Explorer- Edge, 11
- Chrome- 53, 52
- Firefox- 49, 48
- Safari (MacOS only)- 10, 9

HPE recommends using the most recent version of each browser as of the date of this release note.

This release note covers software versions for the KB.16.11 branch of the software.

Version KB.16.11.0001 is the initial build of Major version KB.16.11 software. KB.16.11.0002 includes all enhancements and fixes in the KB.16.11.0001 software, plus the additional enhancements and fixes in the KB.16.11.0002 enhancements and fixes sections of this release note.

This release applies to the following Aruba 5400R Switch Series and Aruba 3810M Switch Series:

Table 2: *Products Supported*

Product number	Description
J9821A	Aruba 5406R zl2 Switch
J9823A	Aruba 5406R 44G PoE+/2SFP+ (No PSU) v2 zl2 Switch
J9824A	Aruba 5406R 44G PoE+/4SFP (No PSU) v2 zl2 Switch
J9822A	Aruba 5412R zl2 Switch
J9825A	Aruba 5412R 92G PoE+/2SFP+ (No PSU) v2 zl2 Switch
J9826A	Aruba 5412R 92G PoE+/4SFP (No PSU) v2 zl2 Switch
J9868A	Aruba 5406R 8XGT/8SFP+ (No PSU) v2 zl2 Switch
JL001A	Aruba 5412R 92GT PoE+ / 4SFP+ (No PSU) v3 zl2 Switch
JL002A	Aruba 5406R 8 port 1/2.5/5/10GBASE T PoE+ / 8 port SFP+ (No PSU) v3 zl2 Switch
JL095A	Aruba 5406R 16 port SFP+ (No PSU) v3 zl2 Switch
JL003A	Aruba 5406R 44GT PoE+ / 4SFP+ (No PSU) v3 zl2 Switch
JL071A	Aruba 3810M 24G 1 slot Switch
JL072A	Aruba 3810M 48G 1 slot Switch
JL073A	Aruba 3810M 24G PoE+ 1 slot Switch
JL074A	Aruba 3810M 48G PoE+ 1 slot Switch
JL075A	Aruba 3810M 16SFP+ 2 slot Switch
JL076A	Aruba 3810M 40G 8 HPE Smart Rate PoE+ 1 slot Switch

Minimum Supported Software Versions

If your switch or module is not listed in the below table, it runs on all versions of the software.

Table 3: *Minimum Supported Software Versions*

Product number	Product name	Minimum software version
J9986A	HPE 24-port 10/100/1000BASE-T PoE+ MACsec v3 zl2 Module	KB.15.17.0003
J9987A	HPE 24-port 10/100/1000BASE-T MACsec v3 zl2 Module	KB.15.17.0003
J9988A	HPE 24-port 1GbE SFP MACsec v3 zl2 Module	KB.15.17.0003
J9989A	HPE 12-port 10/100/1000BASE-T PoE+ / 12-port 1GbE SFP MACsec v3 zl2 Module	KB.15.17.0003
J9990A	HPE 20-port 10/100/1000BASE-T PoE+ / 4-port 1G/10GbE SFP+ MACsec v3 zl2 Module	KB.15.17.0003
J9991A	HPE 20-port 10/100/1000BASE-T PoE+ / 4p 1/2.5/5/10GBASE-T PoE+ MACsec v3 zl2 Module	KB.15.17.0003
J9992A	HPE 20-port 10/100/1000BASE-T PoE+ MACsec / 1-port 40GbE QSFP+ v3 zl2 Module	KB.15.17.0003
J9993A	HPE 8-port 1G/10GbE SFP+ MACsec v3 zl2 Module	KB.15.17.0003
J9995A	HPE 8-port 1/2.5/5/10GBASE-T PoE+ MACsec v3 zl2 Module	KB.15.17.0003
J9996A	HPE 2-port 40GbE QSFP+ v3 zl2 Module	KB.15.17.0003
JH231A	HPE X142 40G QSFP+ MPO SR4 Transceiver	KB.15.17.0003
JH232A	HPE X142 40G QSFP+ LC LR4 SM Transceiver	KB.15.17.0003
JH233A	HPE X142 40G QSFP+ MPO eSR4 300M XCVR	KB.15.17.0003
JH234A	HPE X242 40G QSFP+ to QSFP+ 1m DAC Cable	KB.15.17.0003
JH235A	HPE X242 40G QSFP+ to QSFP+ 3m DAC Cable	KB.15.17.0003
JH236A	HPE X242 40G QSFP+ to QSFP+ 5m DAC Cable	KB.15.17.0003
JL001A	Aruba 5412R 92GT PoE+ / 4SFP+ (No PSU) v3 zl2 Switch	KB.15.17.0003
JL002A	Aruba 5406R 8-port 1/2.5/5/10GBASE-T PoE+ / 8-port SFP+	KB.15.17.0003

Product number	Product name	Minimum software version
	(No PSU) v3 zl2 Switch	
JL003A	Aruba 5406R 44GT PoE+ / 4SFP+ (No PSU) v3 zl2 Switch	KB.15.17.0003
JL095A	Aruba 5406R 16-port SFP+ (No PSU) v3 zl2 Switch	KB.15.17.0003
JL075A	Aruba 3810M 16SFP+ 2-slot Switch	KB.16.01.0004
JL071A	Aruba 3810M 24G 1-slot Switch	KB.16.01.0004
JL073A	Aruba 3810M 24G PoE+ 1-slot Switch	KB.16.01.0004
JL076A	Aruba 3810M 40G 8 HPE Smart Rate PoE+ 1-slot Switch	KB.16.01.0004
JL072A	Aruba 3810M 48G 1-slot Switch	KB.16.01.0004
JL074A	Aruba 3810M 48G PoE+ 1-slot Switch	KB.16.01.0004
JL081A	Aruba 3810M/2930M 4 1/2.5/5/10 GbE HPE Smart Rate Module	KB.16.04.0008
JL308A	Aruba 40G QSFP+ LC Bidirectional 150m MMF 2-strand Transceiver	KB.16.04.0008
JL745A	Aruba 1G SFP LC SX 500m MMF TAA XCVR	KB.16.10.0007
JL746A	Aruba 1G SFP LC LX 10km SMF TAA XCVR	KB.16.10.0007
JL747A	Aruba 1G SFP RJ45 T 100m Cat5e TAA XCVR	KB.16.10.0007
JL748A	Aruba 10G SFP+ LC SR 300m MMF TAA XCVR	KB.16.10.0007
JL749A	Aruba 10G SFP+ LC LR 10km SMF TAA XCVR	KB.16.10.0007

For information on networking application compatibility, see the Software Feature Support Matrix.

Enhancements

This section lists enhancements added to this branch of the software.

Software enhancements are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions.

Table 4: *Enhancements*

Version	Software	Description	Category
16.11.0002	KB	TCP timestamps are an extension to the original TCP stack, that was introduced to identify and reject old duplicate packets (PAWS) and to improve round-trip-time measurement. Using a scanner or other tool, an attacker can observe the TCP timestamp and determine the system uptime to gain information about the operational state of the system. To avoid such risks, a new command `ip tcp randomize-timestamp` has been introduced to randomize the TCP timestamp offsets per connection. Once the command is issued, all the newly established TCP sessions will a use random offset along with the timestamp. A MIB has also been added to enable or disable the randomization of TCP timestamp offsets. Refer to the *Aruba 3810/5400R Management and Configuration Guide for AOS-S 16.11* and *Aruba MIB and Trap Support Matrix for AOS-S 16.11* for more information.	Security
16.11.0002	KB	This is an enhancement to an existing User-Based Tunneling `vlan-extend-enable` (VLAN-aware) mode. Silent devices like Programmable Logic Controller (PLC) devices do not initiate any traffic until they receive a message from the uplink server. Thus, such devices cannot leverage the benefits of colorless ports, which include being authenticated through a RADIUS server and being dynamically placed in a VLAN or being tunneled to a controller. To support such silent devices, a new command `tunneled-node-server ubt-wol-enable vlan <VLAN-ID-LIST>` has been introduced. This command configures the silent client so that the controller allows the first packet from the silent server to reach the silent client without a user tunnel. This will initiate user authentication and tunnel formation. A MIB has also been added to enable User-Based Tunneling Wake-on-LAN (WoL) on the specified VLANs. Refer to the *Aruba 3810/5400R Management and Configuration Guide for AOS-S 16.11* and *Aruba MIB and Trap Support Matrix for AOS-S 16.11* for more information.	Support for Silent Device
16.11.0001	KB	Updated all non-inclusive terminologies. Refer to Terminology Change for more information.	-

Fixes

This section lists released builds that include fixes found in this branch of the software. Software fixes are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

The Symptom statement describes what a user might experience if this is seen on the network. The Scenario statement provides additional environment details and trigger summaries. When available, the Workaround statement provides a workaround to the issue for customers who decide not to update to this version of software.

The number that precedes the fix description is used for tracking purposes.

Table 5: *Fixed Issues*

Version	Bug ID	Software	Description	Category
16.11.0002	255888	KB	**Symptom/Scenario**: When a proxy server is configured on the switch, the switch does not onboard into Aruba Central or Activate.	Aruba Central
16.11.0002	255799	KB	**Symptom**: The user is unable to copy a configuration file to the switch using Secure File Transfer Protocol (SFTP) and the following error message is displayed. `Invalid input: grep usage error` **Scenario**: This issue occurred when the pipe character (|) was used as a part of the command input for some configuration commands, such as the `banner motd` and `snmpv3 user` commands. **Workaround**: Do not use the pipe character (|) in the command input for the configuration commands.	Configuration
16.11.0002	255825	KB	**Symptom/Scenario**: When a switch is rebooted through an SSH session, the `show boot-history`, `show logging`, and `boot` command outputs include the `Operator cold reboot from TELNET session` message instead of the `Operator cold reboot from SSH session` message.	SSH
16.11.0001	-	KB	No fixes were included in version 16.11.0001.	-

Upgrade Information

Upgrading Restrictions and Guidelines

KB.16.10.0002 uses BootROM KB.16.01.0006 when running on 5400R switches and BootROM KB.16.01.0008 when running on 3810M switches. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

IMPORTANT: During the software update, the switch will automatically boot twice. The switch will update the primary BootROM, then reboot, and then update the secondary BootROM. After the switch flash memory is updated and the final boot is initiated, no additional user intervention is needed. Do not interrupt power to the switch during this important update.

Firmware downgrade to a version earlier than 16.01 is not allowed if MSTP instances configured are greater than 16; or the max-vlans value is greater than 2048, or this system is part of a VSF stack.

Unconfigure these features before attempting to downgrade from KB.16.01.0004 or later to a version earlier than 16.01 of the firmware.

Firmware downgrade to a version earlier than 16.04 will generate new SSH keys upon switch boot-up. These keys will be different than the ones previously stored in SSH peer's known hosts file and may result in SSH connectivity

issues after the OS downgrade completes. You will need to erase the pre-existing switch keys from SSH peer's known hosts file to restore SSH connectivity.

This issue will not be encountered when the option "StrictHostKeyChecking" is disabled in the SSH peer.

For more information regarding clearing SSH keys and changing strict host key checking settings, see the documentation provided with your SSH client.

For information on best practices when updating software or rolling back to previous versions of software, see the "Best practices for software updates" section of the Basic Operation Guide.

Aruba Security Policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

The Aruba security policy can be found at https://www.arubanetworks.com/en-au/support-services/ sirt/. Security bulletins can be found at https://www.arubanetworks.com/en-au/support-services/ security-bulletins/.

This release note covers software versions for the WC.16.11 branch of the software.

Version WC.16.11.0001 is the initial build of Major version WC.16.11 software. WC.16.11.0002 includes all enhancements and fixes in the WC.16.11.0001 software, plus the additional enhancements and fixes in the WC.16.11.0002 enhancements and fixes sections of this release note.

This release applies to the following Aruba 2930F Switch Series and Aruba 2930M Switch Series:

Table 6: *Products Supported*

Product number	Description
JL253A	Aruba 2930F 24G 4SFP+ Switch
JL254A	Aruba 2930F 48G 4SFP+ Switch
JL255A	Aruba 2930F 24G PoE+ 4SFP+ Switch
JL256A	Aruba 2930F 48G PoE+ 4SFP+ Switch
JL258A	Aruba 2930F 8G PoE+ 2SFP+ Switch
JL259A	Aruba 2930F 24G 4SFP Switch
JL260A	Aruba 2930F 48G 4SFP Switch
JL261A	Aruba 2930F 24G PoE+ 4SFP Switch
JL262A	Aruba 2930F 48G PoE+ 4SFP Switch
JL263A	Aruba 2930F 24G PoE+ 4SFP+ TAA-compliant Switch
JL264A	Aruba 2930F 48G PoE+ 4SFP+ TAA-compliant Switch
JL319A	Aruba 2930M 24G 1-slot Switch
JL320A	Aruba 2930M 24G PoE+ 1-slot Switch
JL321A	Aruba 2930M 48G 1-slot Switch
JL322A	Aruba 2930M 48G PoE+ 1-slot Switch
JL323A	Aruba 2930M 40G 8SR PoE+ 1-slot Switch
JL324A	Aruba 2930M 24SR PoE+ 1-slot Switch

Product number	Description
JL557A	Aruba 2930F 48G PoE+ 4SFP 740W Switch
JL558A	Aruba 2930F 48G PoE+ 4SFP+ 740W Switch
JL559A	Aruba 2930F 48G PoE+ 4SFP+ 740W TAA-compliant Switch
JL692A	Aruba 2930F 8G PoE+ 2SFP+ TAA Switch
JL693A	Aruba 2930F 12G PoE+ 2G/2SFP+ Switch
R0M67A	Aruba 2930M 40G 8 HPE Smart Rate PoE Class 6 1-slot Switch
R0M68A	Aruba 2930M 24 HPE Smart Rate PoE Class 6 1-slot Switch

Minimum Supported Software Versions

If your switch or module is not listed in the below table, it runs on all versions of the software.

Table 7: *Minimum Supported Software Versions*

Product number	Product name	Minimum software version
JL078A	Aruba 3810M/2930M 1-port QSFP+ 40GbE Module	WC.16.04.0004
JL083A	Aruba 3810M/2930M 4-port 100M/1G/10G SFP+ MACsec Module	WC.16.04.0004
JL308A	Aruba 40G QSFP+ LC Bidirectional 150m MMF 2-strand Transceiver	WC.16.04.0008
JL323A	Aruba 2930M 40G 8SR PoE+ 1-slot Switch	WC.16.04.0008
JL324A	Aruba 2930M 24SR PoE+ 1-slot Switch	WC.16.04.0008
JL557A	Aruba 2930F 48G PoE+ 4SFP 740W Switch	WC.16.05.0003
JL558A	Aruba 2930F 48G PoE+ 4SFP+ 740W Switch	WC.16.05.0003
JL559A	Aruba 2930F 48G PoE+ 4SFP+ 740W TAA-compliant Switch	WC.16.05.0003
R0M67A	Aruba 2930M 40G 8 HPE Smart Rate PoE Class 6 1-slot Switch	WC.16.07.0002
R0M68A	Aruba 2930M 24 HPE Smart Rate PoE Class 6 1-slot Switch	WC.16.07.0002

Product number	Product name	Minimum software version
J9142B	HPE X122 1G SFP LC BX-D Transceiver	WC.16.07.0003
J9143B	HPE X122 1G SFP LC BX-U Transceiver	WC.16.07.0003
JL692A	Aruba 2930F 8G PoE+ 2SFP+ TAA Switch	WC.16.08.0005
JL693A	Aruba 2930F 12G PoE+ 2G/2SFP+ Switch	WC.16.10.0001
JL745A	Aruba 1G SFP LC SX 500m MMF TAA XCVR	WC.16.10.0007
JL746A	Aruba 1G SFP LC LX 10km SMF TAA XCVR	WC.16.10.0007
JL747A	Aruba 1G SFP RJ45 T 100m Cat5e TAA XCVR	WC.16.10.0007
JL748A	Aruba 10G SFP+ LC SR 300m MMF TAA XCVR	WC.16.10.0007
JL749A	Aruba 10G SFP+ LC LR 10km SMF TAA XCVR	WC.16.10.0007

For information on networking application compatibility, see the Software Feature Support Matrix.

Enhancements

This section lists enhancements added to this branch of the software.

Software enhancements are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions

Table 8: *Enhancements*

Version	Software	Description	Category
16.11.0002	WC	TCP timestamps are an extension to the original TCP stack, that was introduced to identify and reject old duplicate packets (PAWS) and to improve round-trip-time measurement. Using a scanner or other tool, an attacker can observe the TCP timestamp and determine the system uptime to gain information about the operational state of the system. To avoid such risks, a new command `ip tcp randomize-timestamp` has been introduced to randomize the TCP timestamp offsets per connection. Once the command is issued, all the newly established TCP sessions will a use random offset along with the timestamp. A MIB has also been added to enable or disable the randomization of TCP timestamp offsets. Refer to the *Aruba 2930F/2930M Management and Configuration Guide for AOS-S 16.11* and *Aruba MIB and Trap Support Matrix for AOS-S 16.11* for more information.	Security

Version	Software	Description	Category
16.11.0002	WC	This is an enhancement to an existing User-Based Tunneling `vlan-extend-enable` (VLAN-aware) mode. Silent devices like Programmable Logic Controller (PLC) devices do not initiate any traffic until they receive a message from the uplink server. Thus, such devices cannot leverage the benefits of colorless ports, which include being authenticated through a RADIUS server and being dynamically placed in a VLAN or being tunneled to a controller. To support such silent devices, a new command `tunneled-node-server ubt-wol-enable vlan <VLAN-ID-LIST>` has been introduced. This command configures the silent client so that the controller allows the first packet from the silent server to reach the silent client without a user tunnel. This will initiate user authentication and tunnel formation. A MIB has also been added to enable User-Based Tunneling Wake-on-LAN (WoL) on the specified VLANs. Refer to the *Aruba 2930F/2930M Management and Configuration Guide for AOS-S 16.11* and *Aruba MIB and Trap Support Matrix for AOS-S 16.11* for more information.	Support for Silent Device
16.11.0001	WC	Updated all non-inclusive terminologies. Refer to Terminology Change for more information.	-

Fixes

This section lists released builds that include fixes found in this branch of the software. Software fixes are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

The Symptom statement describes what a user might experience if this is seen on the network. The Scenario statement provides additional environment details and trigger summaries. When available, the Workaround statement provides a workaround to the issue for customers who decide not to update to this version of software.

The number that precedes the fix description is used for tracking purposes.

Table 9: *Fixed Issues*

Version	Bug ID	Software	Description	Category
16.11.0002	255888	WC	**Symptom/Scenario**: When a proxy server is configured on the switch, the switch does not onboard into Aruba Central or Activate.	Aruba Central
16.11.0002	255799	WC	**Symptom**: The user is unable to copy a configuration file to the switch using Secure File Transfer Protocol (SFTP) and the following error message is displayed. `Invalid input: grep usage error` **Scenario**: This issue occurred when the pipe character (|) was used as a part of the command input for some configuration commands, such as the `banner motd` and `snmpv3 user` commands.	Configuration

Version	Bug ID	Software	Description	Category
			Workaround: Do not use the pipe character (|) in the command input for the configuration commands.	
16.11.0002	255825	WC	**Symptom/Scenario**: When a switch is rebooted through an SSH session, the `show boot-history`, `show logging`, and `boot` command outputs include the `Operator cold reboot from TELNET session` message instead of the `Operator cold reboot from SSH session` message.	SSH
16.11.0001	-	WC	No fixes were included in version 16.11.0001.	-

Upgrade Information

Upgrading Restrictions and Guidelines

WC.16.10.0002 uses BootROM WC.16.01.0010 when running on 2930F switches and BootROM WC.17.02.0007 when running on 2930M switches. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.
IMPORTANT: During the software update, the switch will automatically boot twice. The switch will update the primary BootROM, then reboot, and then update the secondary BootROM. After the switch flash memory is updated and the final boot is initiated, no additional user intervention is needed. Do not interrupt power to the switch during this important update.

Firmware downgrade to a version earlier than 16.04 will generate new SSH keys upon switch boot-up. These keys will be different than the ones previously stored in SSH peer's known hosts file and may result in SSH connectivity issues after the OS downgrade completes. You will need to erase the pre-existing switch keys from SSH peer's known hosts file to restore SSH connectivity.

This issue will not be encountered when the option "StrictHostKeyChecking" is disabled in the SSH peer.

For more information regarding clearing SSH keys and changing strict host key checking settings, see the documentation provided with your SSH client.

For information on best practices when updating software or rolling back to previous versions of software, see the "Best practices for software updates" section of theBasic Operation Guide.

Aruba Security Policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

The Aruba security policy can be found at https://www.arubanetworks.com/en-au/support-services/ sirt/. Security bulletins can be found at https://www.arubanetworks.com/en-au/support-services/ security-bulletins/.

This release note covers software versions for the YA/YB.16.11 branch of the software.

Version YA/YB.16.11.0001 is the initial build of Major version YA/YB.16.11 software. YA/YB.16.11.0002 includes all enhancements and fixes in the YA/YB.16.11.0001 software, plus the additional enhancements and fixes in the YA/YB.16.11.0002 enhancements and fixes sections of this release note.

This release applies to the following Aruba 2530 Switch Series:

Table 10: *Products Supported*

Product number	Description
J9783A	Aruba 2530 8 Switch
J9782A	Aruba 2530 24 Switch
J9781A	Aruba 2530 48 Switch
J9777A	Aruba 2530 8G Switch
J9776A	Aruba 2530 24G Switch
J9775A	Aruba 2530 48G Switch
J9780A	Aruba 2530 8 PoE+ Switch
J9779A	Aruba 2530 24 PoE+ Switch
J9778A	Aruba 2530 48 PoE+ Switch
J9774A	Aruba 2530 8G PoE+ Switch
J9773A	Aruba 2530 24G PoE+ Switch
J9772A	Aruba 2530 48G PoE+ Switch
JL070A	Aruba 2530 8 PoE+ Internal Power Supply Switch
J9856A	Aruba 2530 24G 2SFP+ Switch
J9855A	2530 48G 2SFP+ Switch
J9854A	2530 24G PoE+ 2SFP+ Switch
J9853A	2530 48G PoE+ 2SFP+ Switch

Minimum Supported Software Versions

NOTE

If your switch or module is not listed in the below table, it runs on all versions of the software.

Table 11: *Minimum Supported Software Versions*

Product number	Product name	Minimum software version
J9856A	Aruba 2530 24G 2SFP+ Switch	YA.15.15.0006
J9855A	Aruba 2530 48G 2SFP+ Switch	YA.15.15.0006
J9854A	Aruba 2530 24G PoE+ 2SFP+ Switch	YA.15.15.0006
J9853A	Aruba 2530 48G PoE+ 2SFP+ Switch	YA.15.15.0006
J9783A	Aruba 2530 8 Switch	YB.15.12.0006
J9782A	Aruba 2530 24 Switch	YB.15.12.0006
J9780A	Aruba 2530 8 PoE+ Switch	YB.15.12.0006
J9779A	Aruba 2530 24 PoE+ Switch	YB.15.12.0006
J9781A	Aruba 2530 48 Switch	YA.15.12.0006
J9778A	Aruba 2530 48 PoE+ Switch	YA.15.12.0006
J9777A	Aruba 2530 8G Switch	YA.15.12.0006
J9774A	Aruba 2530 8G PoE+ Switch	YA.15.12.0006
J9776A	Aruba 2530 24G Switch	YA.15.10.0003
J9775A	Aruba 2530 48G Switch	YA.15.10.0003
J9773A	Aruba 2530 24G PoE+ Switch	YA.15.10.0003
J9772A	Aruba 2530 48G PoE+ Switch	YA.15.10.0003

NOTE

For information on networking application compatibility, see the Software Feature Support Matrix.

Enhancements

This section lists enhancements added to this branch of the software.

Software enhancements are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions.

Table 12: *Enhancements*

Version	Software	Description	Category
16.11.0002	YA/YB	TCP timestamps are an extension to the original TCP stack, that was introduced to identify and reject old duplicate packets (PAWS) and to improve round-trip-time measurement. Using a scanner or other tool, an attacker can observe the TCP timestamp and determine the system uptime to gain information about the operational state of the system. To avoid such risks, a new command `ip tcp randomize-timestamp` has been introduced to randomize the TCP timestamp offsets per connection. Once the command is issued, all the newly established TCP sessions will a use random offset along with the timestamp. A MIB has also been added to enable or disable the randomization of TCP timestamp offsets. Refer to the *Aruba 2530 Management and Configuration Guide for AOS-S 16.11* and *Aruba MIB and Trap Support Matrix for AOS-S 16.11* for more information.	Security
16.11.0001	YA/YB	Updated all non-inclusive terminologies. Refer to Terminology Change for more information.	-

Fixes

This section lists released builds that include fixes found in this branch of the software. Software fixes are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

The Symptom statement describes what a user might experience if this is seen on the network. The Scenario statement provides additional environment details and trigger summaries. When available, the Workaround statement provides a workaround to the issue for customers who decide not to update to this version of software.

The number that precedes the fix description is used for tracking purposes.

Table 13: *Fixed Issues*

Version	Bug ID	Software	Description	Category
16.11.0002	255888	YA/YB	**Symptom/Scenario**: When a proxy server is configured on the switch, the switch does not onboard into Aruba Central or Activate.	Aruba Central
16.11.0002	255799	YA/YB	**Symptom**: The user is unable to copy a configuration file to the switch using Secure File Transfer Protocol (SFTP) and the following error message is displayed. `Invalid input: grep usage error` **Scenario**: This issue occurred when the pipe character (|) was used as a part of the command input for some configuration commands, such as the `banner motd` and `snmpv3 user` commands. **Workaround**: Do not use the pipe character (|) in the command input for the configuration commands.	Configuration

Version	Bug ID	Software	Description	Category
16.11.0002	255825	YA/YB	**Symptom/Scenario**: When a switch is rebooted through an SSH session, the `show boot-history`, `show logging`, and `boot` command outputs include the `Operator cold reboot from TELNET session` message instead of the `Operator cold reboot from SSH session` message.	SSH
16.11.0001	-	YA/YB	No fixes were included in version 16.11.0001.	-

Upgrade Information

Upgrading Restrictions and Guidelines

YA/YB.16.10.0002 uses BootROM YA.15.20 or YB.15.10. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

IMPORTANT: During the software update, the switch will automatically boot twice. The switch will update the primary BootROM, then reboot, and then update the secondary BootROM. After the switch flash memory is updated and the final boot is initiated, no additional user intervention is needed. Do not interrupt power to the switch during this important update.

Firmware downgrade to a version earlier than 16.04 will generate new SSH keys upon switch boot-up. These keys will be different than the ones previously stored in SSH peer's known hosts file and may result in SSH connectivity issues after the OS downgrade completes. You will need to erase the pre-existing switch keys from SSH peer's known hosts file to restore SSH connectivity.

This issue will not be encountered when the option "StrictHostKeyChecking" is disabled in the SSH peer.

For more information regarding clearing SSH keys and changing strict host key checking settings, see the documentation provided with your SSH client.

For information on best practices when updating software or rolling back to previous versions of software, see the "Best practices for software updates" section of the **Basic Operation Guide**.

Aruba Security Policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

The Aruba security policy can be found at https://www.arubanetworks.com/en-au/support-services/ sirt/. Security bulletins can be found at https://www.arubanetworks.com/en-au/support-services/ security-bulletins/.

This release note covers software versions for the YC.16.11 branch of the software.

Version YC.16.11.0001 is the initial build of Major version YC.16.11 software. YC.16.11.0002 includes all enhancements and fixes in the YC.16.11.0001 software, plus the additional enhancements and fixes in the YC.16.11.0002 enhancements and fixes sections of this release note.

This release applies to the following Aruba 2540 Switch Series:

Table 14: *Products Supported*

Product number	Description
JL354A	Aruba 2540 24G 4SFP+ Switch
JL356A	Aruba 2540 24G PoE+ 4SFP+ Switch
JL355A	Aruba 2540 48G 4SFP+ Switch
JL357A	Aruba 2540 48G PoE+ 4SFP+ Switch

Enhancements

This section lists enhancements added to this branch of the software.

Software enhancements are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions.

Table 15: *Enhancements*

Version	Software	Description	Category
16.11.0002	YC	TCP timestamps are an extension to the original TCP stack, that was introduced to identify and reject old duplicate packets (PAWS) and to improve round-trip-time measurement. Using a scanner or other tool, an attacker can observe the TCP timestamp and determine the system uptime to gain information about the operational state of the system. To avoid such risks, a new command `ip tcp randomize-timestamp` has been introduced to randomize the TCP timestamp offsets per connection. Once the command is issued, all the newly established TCP sessions will a use random offset along with the timestamp. A MIB has also been added to enable or disable the randomization of TCP timestamp offsets. Refer to the *Aruba 2540 Management and Configuration Guide for AOS-S 16.11* and *Aruba MIB and Trap Support Matrix for AOS-S 16.11* for more information.	Security
16.11.0001	YC	Updated all non-inclusive terminologies. Refer to Terminology Change for more information.	-

Fixes

This section lists released builds that include fixes found in this branch of the software. Software fixes are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

The Symptom statement describes what a user might experience if this is seen on the network. The Scenario statement provides additional environment details and trigger summaries. When available, the Workaround statement provides a workaround to the issue for customers who decide not to update to this version of software.

The number that precedes the fix description is used for tracking purposes.

Table 16: *Fixed Issues*

Version	Bug ID	Software	Description	Category
16.11.0002	255888	YC	**Symptom/Scenario**: When a proxy server is configured on the switch, the switch does not onboard into Aruba Central or Activate.	Aruba Central
16.11.0002	255799	YC	**Symptom**: The user is unable to copy a configuration file to the switch using Secure File Transfer Protocol (SFTP) and the following error message is displayed. `Invalid input: grep usage error` **Scenario**: This issue occurred when the pipe character (|) was used as a part of the command input for some configuration commands, such as the `banner motd` and `snmpv3 user` commands. **Workaround**: Do not use the pipe character (|) in the command input for the configuration commands.	Configuration
16.11.0002	255825	YC	**Symptom/Scenario**: When a switch is rebooted through an SSH session, the `show boot-history`, `show logging`, and `boot` command outputs include the `Operator cold reboot from TELNET session` message instead of the `Operator cold reboot from SSH session` message.	SSH
16.11.0001	-	YC	No fixes were included in version 16.11.0001.	-

Upgrade Information

Upgrading Restrictions and Guidelines

YC.16.10.0002 uses BootROM YC.16.01.0003. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

IMPORTANT: During the software update, the switch will automatically boot twice. The switch will update the primary BootROM, then reboot, and then update the secondary BootROM. After the switch flash memory is updated and the final boot is initiated, no additional user intervention is needed. Do not interrupt power to the switch during this important update.

Firmware downgrade to a version earlier than 16.04 will generate new SSH keys upon switch boot-up. These keys will be different than the ones previously stored in SSH peer's known hosts file and may result in SSH connectivity issues after the OS downgrade completes. You will need to erase the pre-existing switch keys from SSH peer's known hosts file to restore SSH connectivity.

This issue will not be encountered when the option "StrictHostKeyChecking" is disabled in the SSH peer.

For more information regarding clearing SSH keys and changing strict host key checking settings, see the documentation provided with your SSH client.

For information on best practices when updating software or rolling back to previous versions of software, see the "Best practices for software updates" section of the Basic Operation Guide.

Aruba Security Policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

The Aruba security policy can be found at https://www.arubanetworks.com/en-au/support-services/ sirt/. Security bulletins can be found at https://www.arubanetworks.com/en-au/support-services/ security-bulletins/.