# AOS-S Switch 16.10.0020 Release Notes

a Hewlett Packard Enterprise company

### Copyright Information



### 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 |
|---|---|---|---|
| 16.10.0020 | KB, WC, YC, and YA/YB | 2022-03-16 | Released, fully supported, and posted on the web. |
| 16.10.0019 | KB, WC, YC, and YA/YB | 2022-01-14 | Released, fully supported, and posted on the web. |
| 16.10.0018 | KB, WC, YC, and YA/YB | 2021-12-13 | Released, fully supported, and posted on the web. |
| 16.10.0017 | KB, WC, YC, and YA/YB | 2021-09-30 | Released, fully supported, and posted on the web. |
| 16.10.0016 | KB, WC, YC, and YA/YB | 2021-08-06 | Released, fully supported, and posted on the web. |
| 16.10.0015 | KB, WC, YC, and YA/YB | 2021-06-09 | Released, fully supported, and posted on the web. |
| 16.10.0014 | KB and WC | 2021-05-10 | Released, fully supported, and posted on the web. |
| 16.10.0013 | KB, WC, YC, and YA/YB | 2021-04-09 | Released, fully supported, and posted on the web. |
| 16.10.0012 | KB, WC, YC, and YA/YB | 2021-01-25 | Released, fully supported, and posted on the web. |
| 16.10.0011 | KB, WC, YC, and YA/YB | 2020-10-28 | Released, fully supported, and posted on the web. |
| 16.10.0010 | All | 2020-08-24 | Released, fully supported, and posted on the web. |
| 16.10.0009 | All | 2020-06-30 | Released, fully supported, and posted on the web. |
| 16.10.0008 | All | n/a | Never released. |
| 16.10.0007 | All | 2020-04-21 | Released, fully supported, and posted on the web. |
| 16.10.0006 | All | n/a | Never released. |
| 16.10.0005 | All | 2020-02-17 | Released, fully supported, and posted on the web. |
| 16.10.0004 | All | n/a | Never released. |
| 16.10.0003 | All | 2020-01-21 | Released, fully supported, and posted on the web. |
| 16.10.0002 | All | 2019-11-04 | Released, fully supported, and posted on the web. |
| 16.10.0001 | All | 2019-10-07 | Initial release of the 16.10 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.16.10 branch of the software.
Version KB.16.10.0001 is the initial build of Major version KB.16.10 software. KB.16.10.0020 includes all enhancements and fixes in the KB.16.10.0019 software, plus the additional enhancements and fixes in the KB.16.10.0020 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+ (No PSU) v3 zl2 Switch | KB.15.17.0003 |
| 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 |

| Product number | Product name | Minimum software version |
|---|---|---|
| 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 |
|---|---|---|---|
| 16.10.0020 | KB | OSPF Route Filtering feature provides an option to filter the intra-area routes from installing into local FIB table.<br>By using this, operator can create `distribute-list` with one or more network addresses which will be used to filter the intra area routes in OSPFv2/OSPFv3.<br>**Syntax:**<br>OSPFv2: `distribute-list <IP-ADDR>/<Prefix-Len>`<br>OSPFv3: `distribute-list <IPV6-ADDR>/<Prefix-Len>` | OSPF/OSPFv3 |

| Version | Software | Description | Category |
|---|---|---|---|
| | | Refer to the *Aruba 3810/5400R Multicasting and Routing Guide for AOS-S Switch 16.11* and *Aruba 3810/5400R IPv6 Configuration Guide for AOS-S Switch 16.11* for more information. | |
| 16.10.0020 | KB | Added support in Device fingerprinting (DFP) module to send protocol data to Aruba Central for telemetry.<br>Added `options-list` parameter to device-fingerprinting CLI. Switch software is enhanced to collect DHCP options list and up to three instances of HTTP user agent headers.<br>**Syntax:** `device-fingerprinting [policy]<PROFILE_NAME> dhcp [option-num <NUM> \| options-list].`<br>Refer to the *Aruba 3810/5400R Access Security Guide for AOS-S Switch 16.11* for more information. | Device Finger Printing |
| 16.10.0019 | KB | No enhancements were included in version 16.10.0019. | NA |
| 16.10.0018 | KB | The Enrollment over Secured Transport (EST) client feature is updated to download and renew the CA certificates from an EST server independent of application certificate enrollment.<br>A new command `est-server <profile-name> cacerts-download` is added to enable independent CA certificate download from the EST server. This enhancement initiates automatic CA certificate download and renewal when the existing TA profile is about to expire. The switch will use the existing `est-server <profile-name> re-enrollment-prior-expiry` command to determine how many days in advance the renewal is to be done. A MIB has also been added to enable automatic download and renew of the CA certificates from the EST server.<br>Refer to the *Aruba 3810/5400R Access Security Guide for AOS-S Switch 16.10* and *Aruba MIB and Trap Support Matrix for AOS-S Switch 16.10* for more information. | EST |
| 16.10.0017 | 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.<br>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.<br>A MIB has also been added to enable or disable the randomization of TCP timestamp offsets.<br>Refer to the *Aruba 3810/5400R Management and Configuration Guide for AOS-S Switch 16.10* and *Aruba MIB and Trap Support Matrix for AOS-S Switch 16.10* for more information. | Security |

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0017 | 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.<br>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.<br>A MIB has also been added to enable User-Based Tunneling Wake-on-LAN (WoL) on the specified VLANs.<br>Refer to the *Aruba 3810/5400R Management and Configuration Guide for AOS-S Switch 16.10* and *Aruba MIB and Trap Support Matrix for AOS-S Switch 16.10* for more information. | Support for Silent Device |
| 16.10.0016 | KB | Added support for the new SSH data integrity algorithm hmac-sha2-256, which is defined in RFC 6668.<br>Refer to the *Aruba 3810/5400R Access Security Guide for AOS-S Switch 16.10* and *Aruba 3810/5400R IPv6 Configuration Guide for AOS-S Switch 16.10* for more information. | SSH |
| 16.10.0016 | KB | Added support to configure the size of the EAP-TLS fragments sent from the switch to the RADIUS server. Configuring EAP-TLS fragment size based on the MTU of the network avoids IP fragmentation in the network, and thus, the fragmented packets will not be dropped by the firewall or gateways.<br>Added a MIB to indicate the maximum size of the EAP-TLS fragment sent to the RADIUS server.<br>Refer to the *Aruba 3810/5400R Access Security Guide for AOS-S Switch 16.10* and *Aruba MIB and Trap Support Matrix for AOS-S Switch 16.10* for more information. | EAP-TLS Fragmentation |
| 16.10.0015 | KB | No enhancements were included in version 16.10.0015. | NA |
| 16.10.0014 | KB | No enhancements were included in version 16.10.0014. | NA |
| 16.10.0013 | KB | Added support to user roles to establish user-based tunneling to tunnel voice and data traffic selectively and authenticate critical-role user in the event of RADIUS server unavailability.<br>Refer to the *Aruba 3810/5400R Access Security Guide for AOS-S Switch 16.10* and the *Aruba 3810/5400R Management and Configuration Guide for AOS-S Switch 16.10* for more information. | Enhancement in traffic tunneling and critical-role authentication |

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0013 | KB | Added MIBs to display the count of total and operational members in a VSF and BPS stack. Refer to the *Aruba MIB and Trap Support Matrix for AOS-S Switch 16.10* for more information. | Back Plane Stacking (BPS) and Virtual Switch Framework (VSF) |
| 16.10.0012 | KB | Added `concise` parameter to display port-access and spanning-tree attributes in a consolidated format, when executing `show config` and `show running-config` commands. | Enhancement for `show config` and `show running-config` commands |
| 16.10.0012 | KB | Added support to enable SNMP traps for a specified event. This helps to filter out particular traps from all SNMP trap messages.<br>**Syntax:** `snmp-server enable traps event-list <EVENT-LIST-STR>` | Customization for SNMP Traps |
| 16.10.0012 | KB | Added `recv-disable` parameter to configure loop-protect from blocking the receiving port when a loop is detected.<br>**Syntax:** `no loop-protect <PORT-LIST> receiver-action [recv-disable]` | Configuration for loop-protect receiver-action |
| 16.10.0012 | KB | Added support to maintain the current role of the User Based Tunneling client in the switch instead of de-authenticating the client during controller maintenance. The client traffic flow is resumed at the switch ingress port when the controller is reachable.<br>**NOTE:** The client is de-authenticated when the controller is not available even after the configured maintenance period. | Enhancement for `tunneled-node-server` command |
| 16.10.0011 | KB | Improved performance when executing `show config` command. | Performance improvements for `show config` command |
| 16.10.0011 | KB | Added support to format MAC address in upper case for the Called and Calling Station IDs.<br>Refer to the *Access Security Guide* for more information. | Port Access Enhancement |
| 16.10.0011 | KB | Added support to include the Port VLAN information in RADIUS access request for all authentication types.<br>Refer to the *Access Security Guide* for more information. | Port Access Enhancement |
| 16.10.0011 | KB | Added support to enable AES 256-bit encryption for SNMP. Refer to the *Management and Configuration Guide* for more information. | AES 256-bit encryption for SNMP |

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0011 | KB | Added support to configure a prefix string along with the switch IP address or hostname in the logs sent to the Syslog servers. This helps to classify and group log entries based on the string value.<br>**Syntax:** `logging prefix <ASCII-STR>`<br>Refer to the *Management and Configuration Guide* for more information. | Syslog Enhancement |
| 16.10.0011 | KB | Added support to schedule a stack or chassis reboot.<br>**Syntax:** `reload <after\|at> [system]`<br>Refer to the *Management and Configuration Guide* for more information. | Stacking Enhancement |
| 16.10.0010 | KB | Added support to provide the option to specify the source interface or VLAN for Central connectivity. The existing IP source-interface command is enhanced to override current configuration check for provisioning using Aruba Activate.<br>Refer to the *Management and Configuration Guide* for more information. | Source interface option for Central connectivity |
| 16.10.0010 | KB | Added support to allow more PoE devices to be connected to the switch by using `poe-alloc-by-usage`, when using Device Profiles. This can be based on either **Usage** or **Class**. Default allocation will be based on **Class**.<br>Refer to the *Management and Configuration Guide* for more information. | Device Profile Enhancement |
| 16.10.0010 | KB | Added support for FQDN (only IPv4) while configuring TACACS server along with the existing support of IP address.<br>Refer to the *Access Security Guide* for more information. | TACACS Option |
| 16.10.0010 | KB | Added support to work with the default setting in OpenSSH 8.2 by choosing an inherently more secure algorithm as the default on the switch for SSH communication. Refer to the *Access Security Guide* for more information.<br>The list of new Host-Key algorithms are as follows:<br>■ rsa-sha2-512<br>■ rsa-sha2-256<br>The list of new SSH KEX algorithms are as follows:<br>■ ecdh-sha2-nistp521<br>■ ecdh-sha2-nistp381<br>■ ecdh-sha2-nistp256<br>■ diffie-hellman-group-exchange-sha256 | Support for OpenSSH 8.2 |
| 16.10.0010 | KB | Improved performance when displaying large configurations. | Performance improvements for `show running-config` command |

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0010 | KB | Added RMON logging for the failure events in SSH, Web UI, Syslog over TLS sessions, and x509 certificate processing. Refer to the *Event Log Message Reference Guide* for more information. | RMON logging |
| 16.10.0009 | KB | Added support for the manager password enforcement to ensure that the switch prompts the user to configure the manager password on the switch before configuring any other features. If the manager password is not configured, then the user will have read-only access to the switch. This is applicable only to switches with factory default configuration. Refer to the *Access Security Guide* for more information. | Manager Password Enforcement |
| 16.10.0009 | KB | Added support to enhance the payload size for the REST API interfaces. The increased payload size for 3810M and 54xxR platforms is 1024K.<br>Refer to the *REST API Guide* for more information. | REST API Payload Enhancement |
| 16.10.0009 | KB | Added support for Server Name Indication (SNI), which is a TLS extension defined in RFC 6066. This feature is enabled by default to include the SNI extension in the Client Hello sent from the switch to all the TLS client applications.<br>Refer to the *Access Security Guide* for more information. | Server Name Indication for TLS |
| 16.10.0008 | KB | Version 16.10.0008 was never released. | NA |
| 16.10.0007 | KB | ■ Added additional support for pipe "\|" option to grep for pattern match the output of CLI commands, such as:<br>◦ Case-insensitive option to allow a case insensitive pattern match<br>◦ Up to four consecutive pattern matches in one CLI command<br>■ Added support for a per-session based command to wrap column display in the CLI output using session wrap-text option when its length is exceeding the column width. Refer to the Management and Configuration Guide for more information. | CLI |
| 16.10.0007 | KB | Added the following REST enhancements:<br>■ Support for ARP table data.<br>■ Support for downloadable user-roles configuration.<br>■ Support for primary VLAN.<br>■ Support for reserved-vlan and clearpass options to configure dynamic segmentation.<br>■ REST API schema moved under device-rest-api/services/server.html. Refer to the *REST API Guide* for more information. | REST |
| 16.10.0007 | KB | Added support for the following 1G and 10G TAA transceivers: | Transceivers |

| Version | Software | Description | Category |
|---|---|---|---|
| | | ■ JL745A - Aruba 1G SFP LC SX 500m MMF TAA XCVR<br>■ JL746A - Aruba 1G SFP LC LX 10km SMF TAA XCVR<br>■ JL747A - Aruba 1G SFP RJ45 T 100m Cat5e TAA XCVR<br>■ JL748A - Aruba 10G SFP+ LC SR 300m MMF TAA XCVR<br>■ JL749A - Aruba 10G SFP+ LC LR 10km SMF TAA XCVR | |
| 16.10.0007 | KB | Added support for the new activate endpoint devices-v2.arubanetworks.com which has the following two major differences compared to the old endpoint device.arubanetworks.com:<br>■ It works on the standard TLS handshake mechanism and uses mutual authentication.<br>■ It uses certificates issued by HP CA for establishing TLS connections.<br>Zero Touch Provisioning (ZTP) improvements were made to deal with situations such as unresponsive DNS servers. Refer to the *Management and Configuration Guide* for more information. | Zero Touch Provisioning |
| 16.10.0006 | KB | Version 16.10.0006 was never released. | NA |
| 16.10.0005 | KB | No enhancements were included in version 16.10.0005. | NA |
| 16.10.0004 | KB | Version 16.10.0004 was never released. | NA |
| 16.10.0003 | KB | New command `aaa accounting session-id include-switch-identity` was added. When this command is invoked, an accounting session ID is generated with Switch Base MAC, Client MAC, and Timestamp for network accounting type. The other accounting types (exec, system, commands) do not include Client MAC and hence the session ID is generated with Switch Base MAC, Track ID, and Timestamp.<br>If the same client is accessing the network from multiple switches, then the accounting session ID can be duplicated. This caused issues in Clearpass where client insertion in the database failed with an error similar to Integrity Error: acct_id, calling_station_id violates check constraint. This new command alleviates that problem. | AAA |
| 16.10.0003 | KB | Extended the device identify capability by just matching based on the attribute MAC OUI to the Sys name and Sys description attributes. | Device profile |

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0003 | KB | This enhancement will only be in effect if the CoA/Disconnect request has a message authenticator attribute in request packet. The message authenticator attribute is used to verify the integrity (HMAC-MD5) of the RADIUS packet. This is an optional attribute in the Access/CoA/Disconnect packet. If the received packet has this attribute in the RADIUS packet, the receiver will validate the integrity value and discard it if the value is incorrect. | RADIUS |
| 16.10.0002 | KB | No enhancements were included in version 16.10.0002. | NA |
| 16.10.0001 | KB | No enhancements were included in version 16.10.0001. | NA |

# 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 |
|---|---|---|---|---|
| 16.10.0020 | 256274 | KB | **Symptom/Scenario**: VSF Stack Member crashed with a message similar to the following: `Software exception at lava_chassis_slot_sm.c:3626 - in 'eChassMgr', task ID = 0x37b07bc0.` | VSF |
| 16.10.0020 | 256257 | KB | **Symptom/Scenario**: Certain transceivers had link issues in unsupported transceiver mode. | Transceivers |
| 16.10.0020 | 256234 | KB | **Symptom**: The `show rmon statistics <port no>` command returns the wrong counter values. **Scenario**:This issue occurred when the `clear statistics global` or `clear statistics <port no>` was executed first and then `show rmon statistics <port no>`. | CLI |
| 16.10.0020 | 256233 | KB | **Symptom**: Client ports may encounter packet drops when multicast sources stream video over 500 Mbps. | IGMP-NG |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue can occur when multiple clients from different ports subscribed to the same group, which streams using HD channels requiring high bandwidth. TX drops can occur when several clients change channels simultaneously.<br>**Workaround**: Lower the bandwidth of the video streams to below 500 Mbps in order to avoid over-subscription of ports. | |
| 16.10.0020 | 256220 | KB | **Symptom**: Missing OSPF routes.<br>**Scenario**: This issue occurred when both userbased tunneling and OSPF are configured and either of the uplinks to the controller is down.<br><br>**NOTE:** `source-interface` to be configured for tunneled node when the switch has more than one vlan to the reach the controller. | OSPFv2 |
| 16.10.0020 | 256205 | KB | **Symptom**: A configuration template push from Aruba Central fails.<br>**Scenario**: This issue occurred when the end devices are connected to ports that are configured with `port-security learn-mode static`. | Central Integration |
| 16.10.0020 | 256140 | KB | **Symptom**: The switch crashes with an error message: `NMI event`.<br>**Scenario**: This issue occurred when the HP MSM 775 wireless controller was connected to the switch and `snmpwalk` was executed. | SNMPV2 |
| 16.10.0020 | 256167 | KB | **Symptom**: Ports with per-port tunneled node (PPTN) configured might be disabled after a switch reboot.<br>**Scenario**: This issue occurred when a device profile was configured with tunneled-node.<br>**Workaround**: Disable and enable the problematic PPTN enabled port manually. | Tunneled Node |
| 16.10.0020 | 255916 | KB | **Symptom/Scenario**: Slot crashes with signatures `OMFP LPTR Err Status = 0x00000310 (DEC_ERR_CNT)` and `FR Error = 0x18000020 (ALLOC_CHIP_ PORT_UNDERFLOW).` | Basic Layer2 |
| 16.10.0019 | 256115 | KB | **Symptom**: Although the switch does not react to pings or SSH commands, it continues to transit traffic. The event log contains a crash message.<br>**Scenario**: This issue occurred when device fingerprinting was configured with DHCP protocol. | CPPM |
| 16.10.0019 | 256200 | KB | **Symptom**: Per-port tunneled node (PPTN) disables the port for one second as part of tunnel deletion. | Tunneled Node |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue occurred when the device-profile application with tunneled-node was disabled on a PPTN enabled port.<br>**Workaround**: Disable and enable the problematic PPTN enabled port manually. | |
| 16.10.0019 | 256121 | KB | **Symptom**: Web authentication fails when the switch is managed by Aruba Central (`aruba-central support-mode disable`).<br>**Scenario**: This issue occurred when the switch was connected to Aruba Central and `aruba-central support-mode` was disabled.<br>**Workaround**: Execute `aruba-central support-mode enable` command so the switch is longer managed by Aruba Central. | Web Authentication |
| 16.10.0019 | 256144 | KB | **Symptom**: Switch is unable to connect to Activate.<br>**Scenario**: This issue occurred during the initial onboarding of the switch, however it can also occur after the switch is visible on Aruba Central. | Activate |
| 16.10.0018 | 256037 | KB | **Symptom**: Clients are not authenticated on a switch port.<br>**Scenario**: This issue occurred when multiple clients were connected to a single port (for example, a Personal Computer (PC) was connected to a phone), both MAC authentication and 802.1X authentication methods were attempted at the same time on the PC, and both the authentication methods used the same user role attribute.<br>**Workaround**: Configure the `auth-order` parameter first with `authenticator`, and then with `mac-based`. | 802.1X |
| 16.10.0018 | 255928 | KB | **Symptom/Scenario**: A switch is unable to connect to Aruba Central. | Aruba Central |
| 16.10.0018 | 255940 | KB | **Symptom**: A switch crashes with a message similar to the following:<br>`Software exception at svc_misc.c:1088 - in 'mDHCPClint'`<br>`-> Failed to malloc 9202 bytes.`<br>**Scenario**: This issue occurred when the switch attempted to reconnect to Aruba Central. | Aruba Central |
| 16.10.0018 | 255978 | KB | **Symptom**: A switch crashes with a message similar to the following:<br>`Software exception in ISR at pvDmaV1Rx.c`<br>`-> ASSERT: No resources available!.` | Authentication |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue occurred when 802.1X and MAC authentication were enabled on the same port with auth-order, and the client was initially authenticated through MAC authentication with a user role having the `port mode` attribute. | |
| 16.10.0018 | 255995 | KB | **Symptom**: A switch crashes when the `show port-access clients` command is issued or when an `SNMP GET` operation is performed to get the MIB object `hpicfUsrAuthMacAuthSessionStatsEntry`.<br>**Scenario**: The switch crashed when a MAC-authenticated client had a username of more than 40 characters. | Authentication |
| 16.10.0018 | 255896 | KB | **Symptom**: A stack member loses connection to the stack and gets stuck in a boot loop.<br>**Scenario**: This issue occurred when the stacking links were configured as a full mesh, and two links went down leaving the stacking links in a chain configuration. | Back Plan Stacking |
| 16.10.0018 | 254566 | KB | **Symptom**: Traffic fails to pass through an IEEE 802.1ad tunnel.<br>**Scenario**: This issue occurred because of the following reasons:<br>1. A Small Form-factor Pluggable+ (SFP+) port was configured as an uplink.<br>2. IEEE 802.1ad was configured on the same port.<br>3. The switch was rebooted without a transceiver in the slot.<br>4. A 1G SFP transceiver was inserted during the runtime.<br>**Workaround**: Insert the 1G SFP transceiver, and then reboot the switch. | IEEE 802.1ad |
| 16.10.0018 | 256123 | KB | **Symptom**: Received packet drops are observed on a port.<br>**Scenario**: This issue occurred when the TCP traffic, with the push flag set, consumed 100% bandwidth on a 1G port of a V3 module. | Interfaces |
| 16.10.0018 | 256016 | KB | **Symptom**: When a private VLAN is configured on a switch, the traffic from the secondary VLAN does not reach the primary VLAN.<br>**Scenario**: This issue occurred when the switch was rebooted, and the secondary VLAN contained a tagged trunk or Link Aggregation Control Protocol (LACP) port. | Private VLAN |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Workaround**: Remove and add the tagged trunk or LACP configuration to the secondary VLAN. | |
| 16.10.0018 | 256034 | KB | **Symptom**: SNMP MIB files are not reachable, and the MIB file returns some errors.<br>**Scenario**: This issue occurred when the customer used an SNMP monitoring tool to read or parse the MIB files. | SNMP |
| 16.10.0018 | 256050 | KB | **Symptom**: A switch crashes when the **WebUI Security > Clientspage** is accessed.<br>**Scenario**: The switch crashed when a MAC-authenticated client had a username of more than 40 characters. | Web UI |
| 16.10.0017 | 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 |
| 16.10.0017 | 255762 | KB | **Symptom/Scenario**: A switch crashes with the following message:<br>`OMFP LPTR Err Status = 0x00000310 (DEC_ERR_CNT) .` | Chassis |
| 16.10.0017 | 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.<br>`Invalid input: grep usage error`<br>**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.<br>**Workaround**: Do not use the pipe character (\|) in the command input for the configuration commands. | Configuration |
| 16.10.0017 | 255908 | KB | **Symptom/Scenario**: A new multicast stream is initially broadcast on a VLAN even when no IGMP join is sent. | IGMP |
| 16.10.0017 | 255195 | KB | **Symptom**: The switch memory utilization spikes and might reach to 100%.<br>**Scenario**: This issue occurred when many ports were monitored and mirrored to one port.<br>**Workaround**: Disable mirroring on the ports. | Mirroring |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0017 | 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 |
| 16.10.0017 | 255827 | KB | **Symptom/Scenario**: A switch crashes with the following message:<br>`Health Monitor: Invalid Instr Misaligned Mem Access .......Task='InetServer'.` | System |
| 16.10.0017 | 255760 | KB | **Symptom/Scenario**: A switch crashes with the following message:<br>`Software exception at bsp_interrupts.c:90 - in 'fault_handler'.` | Tunneled Node |
| 16.10.0016 | 255682 | KB | **Symptom**: The RADIUS accounting packets sent from the switch to the RADIUS server do not contain the correct client IP address.<br>**Scenario**: This issue occurred when both user authentication and MAC authentication were configured. | 802.1X |
| 16.10.0016 | 255400 | KB | **Symptom**: The switch is unable to connect to Activate or Aruba Central.<br>**Scenario**: This issue occurred when the `show crypto pki ta-profile` command displayed `Pending Root Certificate In...` for the `GEOTRUST_CA` profile, and the following event was recorded in the event log:<br>`05222 activate: ST1-CMDR: Error connecting to the Activate server: Activate TLS connection error.` | Activate |
| 16.10.0016 | 255653 | KB | **Symptom**: The switch crashes with a Non-Maskable Interrupt (NMI) event.<br>**Scenario**: The switch crashed because of the following reasons:<br>1. The switch was configured to receive a DHCP address.<br>2. The `activate provision force` command was configured on the switch.<br>3. The `no activate software-update` | Activate |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | `check` command was executed. | |
| 16.10.0016 | 255554 | KB | **Symptom/Scenario**: When the switch is powered on for the first time and ZTP is initiated, the switch does not come online in Aruba Central.<br>**Workaround**: Reboot the switch or execute the `reset saved-configuration` command. | Central |
| 16.10.0016 | 255672 | KB | **Symptom/Scenario**: A configuration push from Aruba Central fails when the configuration contains the `crypto pki enroll-est-certificate` command.<br>**Workaround**: Add a valid value for `Enter Country (C)` field in the `subject fields` of the `crypto pki enroll-est-certificate` command. | Central |
| 16.10.0016 | 255697 | KB | **Symptom**: The switch crashes with the following message:<br>`Software exception in ISR at btmDmaApi.c:650 -> ASSERT: No resources available!.`<br>**Scenario**: This issue occurred when there was a repeated hardware fault in one of the power supplies. | Chassis Manager |
| 16.10.0016 | 255570 | KB | **Symptom/Scenario**: The `Rx Errors` counter in the `show interfaces` command output is not cleared when the `clear statistics global` command is executed. | CLI |
| 16.10.0016 | 255719 | KB | **Symptom**: The IP address of the next server is not present in the DHCP response packet.<br>**Scenario**: This issue occurred when the DHCP server with option 66 and option 150 was configured in the server pool. | DHCP Server |
| 16.10.0016 | 255417 | KB | **Symptom**: The switch crashes with an NMI event.<br>**Scenario**: This issue occurred when the DHCP snooping traffic was sent continuously to the switch with DHCP option 82, and the DHCP clients rebooted frequently. | DHCP Snooping |
| 16.10.0016 | 255552 | KB | **Symptom/Scenario**: Mirrored egress packets are tagged even though the `no-tag-added` option is configured.<br>**Workaround**: Reapply the existing monitor configuration after removing the configuration using the `no monitor all both mirror 1` command. | Port Mirroring |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0016 | 255593 | KB | **Symptom**: The switch crashes when the `qos trust dscp` configuration is applied.<br>**Scenario**: This issue occurred when the `qos trust dscp` command was configured on an admin disabled port of a v2 module.<br>**Workaround**: Enable the port before configuring the `qos trust dscp` command. | QoS |
| 16.10.0016 | 255638 | KB | **Symptom**: Some PBT clients experience traffic loss.<br>**Scenario**: This issue occurred when both VRRP and PBT were configured on the switch, and a VRRP failover event was recorded.<br>**Workaround**: Disable and enable PBT on the switch. | Tunneled Node |
| 16.10.0016 | 255586 | KB | **Symptom**: Running configuration does not display the local user roles.<br>**Scenario**: The issue occurred when the switch was configured to use both downloadable and local user roles.<br>**Workaround**: Reboot the switch. | User Roles |
| 16.10.0016 | 255619 | KB | **Symptom**: The Ports table on the Web UI does not display all the interfaces of the switch.<br>**Scenario**: This issue occurred when the Name and Id sent through LLDP contained a trailing backslash (\), and the same was configured on the port.<br>**Workaround**: Disable LLDP on the switch using the `no lldp run` command. | Web UI |
| 16.10.0015 | 255511 | KB | **Symptom**: Border Gateway Protocol (BGP) route updates do not contain the community value.<br>**Scenario**: This issue occurred when an unused route map was deleted. | BGP |
| 16.10.0015 | 255500 | KB | **Symptom**: BGP route updates are not sent with the community value.<br>**Scenario**: This issue occurred when a new route map was applied to a neighbor with the matching community rule. | BGP |
| 16.10.0015 | 255124 | KB | **Symptom**: Captive portal redirection does not work.<br>**Scenario**: This issue occurred when the `ip client-tracker` command was enabled, and the VLAN where the client onboarded had the `disable layer3` command configured.<br>**Workaround**: Remove `ip client-tracker` or `disable layer3` configuration from the client VLAN. | Captive Portal |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0015 | 255259 | KB | **Symptom/Scenario**: Executing the `show tech all` command resets the port counters in all sessions. | CLI |
| 16.10.0015 | 255134 | KB | **Symptom**: Switch crashes regularly with the following message:<br>`Active/Commander system went down: eSoftware exception at msgSys.c:641 -- in 'mNSR',`<br>`-> Can't get message buffer for msgSys_recv.`<br>The event log indicates continuous removal and application of the device-profile.<br>**Scenario**: This issue occurred with a device profile for an AP enabled, with both interfaces of the AP connected to the switch through a trunk, and when the switch was rebooted.<br>**Workaround**: Disable and enable the device profile. | Device Profile |
| 16.10.0015 | 255158 | KB | **Symptom**: Multicast traffic with the source IP address 0.0.0.0 floods to all ports, even with IGMP snooping enabled.<br>**Scenario**: This issue occurred when the multicast traffic was sent with a NULL IP source from a device connected to a non-querier device. | IGMP |
| 16.10.0015 | 255408 | KB | **Symptom**: Unauthorized clients can connect and access the switch using the loopback address.<br>**Scenario**: This issue occurred when the `ip authorized-managers` command was configured and an unauthorized client attempted to connect to the loopback address. | IP Authorized Manager |
| 16.10.0015 | 255105 | KB | **Symptom**: Module reboots with the following message:<br>`Ports A subsystem went down Software exception at mrtm_shadow.c:500 -- in 'mAsicUpd'`<br>`-> MRT parity error.`<br>Module crashes when the multicast traffic hits Port-Based Forwarding (PBF) rule.<br>**Scenario**: This issue occurred when the PBF rule is configured with the destination IP of `any`, a trunk interface is the next hop, and multicast traffic hits the PDF rule. | PBF |
| 16.10.0015 | 255464 | KB | **Symptom/Scenario**: A Quality of Service (QoS) policy, which has a space character in the name, cannot be removed from an interface or VLAN. | Policy Map |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0015 | 255430 | KB | **Symptom**: When the `show radius` command is executed, the output shows the RadSec server as a Dead server.<br>**Scenario**: This issue occurred because of the following reason:<br>1. When the `radius-server dead-time`, `aaa authentication` and `aaa accounting` commands were configured.<br>2. Accounting was disabled on the RADIUS server and a RadSec connection was established.<br>3. When an SSH session was established and commands were executed from that session. | RADIUS |
| 16.10.0015 | 255342 | KB | **Symptom**: When an initial role is applied, clients do not attempt to reauthenticate.<br>**Scenario**: This issue occurred when the server-timeout value was less than the RADIUS request timeout.<br>**Workaround**: Configure a greater server-timeout value than the RADIUS request timeout. | RADIUS |
| 16.10.0015 | 255171 | KB | **Symptom**: The switch CPU spikes and the ClearPass RADIUS server shuts down.<br>**Scenario**: This issue occurred when MAC authentication used the peap-mschapv2 authentication method. As a result, Access-Request and Access-challenge messages were exchanged in a loop. | RADIUS |
| 16.10.0015 | 255067 | KB | **Symptom**: Switch does not respond to Simple Network Management Protocol version 3 (SNMPv3) queries.<br>**Scenario**: This issue occurred when there was a wrong value in the boot counter. | SNMPv3 |
| 16.10.0015 | 255072 | KB | **Symptom/Scenario**: The following issues may be seen with a switch module:<br>■ When the `no module` command is executed for a module that is present in a VSF standby switch, the module reboots instead of staying in a powered down state.<br>■ When the `no module` command is executed for a module that is in a failed state in a VSF standby switch, the switch returns the following error:<br>`Module unconfiguration is in progress.`<br>**Workaround**: Remove the module physically, and execute the `no module` command. | VSF |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0014 | 255376 | KB | **Symptom/Scenario**: Traffic loss is observed in Port-Based Tunneling (PBT) and controller Virtual Router Redundancy Protocol (VRRP) topology.<br>**Workaround**: Disable and enable PBT on the switch. | Tunneled Node |
| 16.10.0013 | 255031 | KB | **Symptom**: Switch loses connectivity to Aruba Central after a template is pushed.<br>**Scenario**: This issue occurred when a template with netdestination commands were pushed to the switch.<br>**Workaround**: Add `aruba-central url` to the template that is applied. | Central |
| 16.10.0013 | 254985 | KB | **Symptom**: End devices (example, printer) become unreachable when they do not send or receive much traffic.<br>**Scenario**: This issue occurred when the switch stack was not rebooted after a new member was added to the stack.<br>**Workaround**:<br>■ Reboot the stack after adding a new member.<br>■ Bounce the port connecting to the end device.<br>■ Configure the MAC age time to match the ARP ageout time of the router. | ARP |
| 16.10.0013 | 254974 | KB | **Symptom/Scenario**: When the OOBM port is a DHCP client, The DHCP server receives an incorrect MAC address from the switch. | OOBM |
| 16.10.0013 | 254868 | KB | **Symptom**: When connection to the neighbor is lost, an incorrect OSPF route is removed from the routing table.<br>**Scenario**: This issue occurred when more than one point-to-point OSPF interface was configured with the same router.<br>**Workaround**: Configure broadcast OSPF interface instead of point-to-point OSPF interface. | OSPFv2 |
| 16.10.0013 | 255135 | KB | **Symptom**: A MACsec connection is not established on the last fixed or last flex port of the switch.<br>**Scenario**: This issue occurred because of the following reasons:<br>■ MACsec was enabled on the last fixed or last flex port of the switch.<br>■ There was an intermediate device that filtered packets with null MAC address.<br>**Workaround**: Connect the MACsec peer switches without any devices in between. | MACsec |
| 16.10.0013 | 255125 | KB | **Symptom**: Clients authenticated by Aruba Central are not placed in the proper VLAN.<br>**Scenario**: This issue occurred because of the following reasons: | Central |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | ■ Both MAC authentication and 802.1X are configured on the same port.<br>■ There are two clients on the port, which had a tagged membership for a VLAN, and the user role for a client had an untagged membership for the same VLAN. | |
| 16.10.0013 | 255123 | KB | **Symptom**: The following event did not identify the affected module correctly: `00907 IpAddrMgr: ST3-CMDR: Module p BMP TCAM parity recovery.`<br>**Scenario**: The following event was recorded in the event log when there was a hardware issue: `00907 IpAddrMgr: ST3-CMDR: Module p BMP TCAM parity recovery.` | RMON Logging |
| 16.10.0013 | 255115 | KB | **Symptom**: Some VoIP phones did not receive an IP address from the Dynamic Host Configuration Protocol (DHCP) server.<br>**Scenario**: This issue occurred when user-based tunneling was configured on the port and DHCP snooping was enabled.<br>**Workaround**: Disable DHCP snooping. | DHCP Snooping |
| 16.10.0013 | 255062 | KB | **Symptom**: User-based tunnel (802.1X) is not established when MAC authentication is also configured on the port with a different VLAN assignment.<br>**Scenario**: This issue occurred when both MAC authentication and 802.1X were configured on a port, and the 802.1X authentication contained a VLAN change. | MAC Authentication |
| 16.10.0013 | 255058 | KB | **Symptom**: After a new template is applied to the switch, the switch is unable to connect to Aruba Central.<br>**Scenario**: This issue occurred because the primary VLAN on the switch was changed when the new template was applied.<br>**Workaround**: Reboot the switch. | Central |
| 16.10.0013 | 254976 | KB | **Symptom/Scenario**: The SSH, telnet, and console connections cannot be established with the switch, and the following event is recorded in the event log: `maximum user session limit reached.` | Switch Access |
| 16.10.0013 | 254966 | KB | **Symptom**: Applying a template from Aruba Central to a switch fails with the following reasons:<br>■ `Failure Reason: Add and Remove commands have been failed`<br>■ `Reason: Invalid netdestination` | Central |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | `entry`.<br>**Scenario**: This issue occurred when the template contained changes to the host configurations of the netdestination entries, which are used in an ACL. | |
| 16.10.0013 | 254958 | KB | **Symptom**: After the transition of 802.1X machine authentication to user authentication with User-Based Tunnel, the client username in the show command in the controller is not updated.<br>**Scenario**: This issue occurred when 802.1X with User-Based Tunneling was established and then the transition of machine authentication to user authentication was done. | Tunneled Node |
| 16.10.0013 | 254893 | KB | **Symptom/Scenario**: The switch crashes due to an MSTP NMI event. | Spanning Tree |
| 16.10.0013 | 254797 | KB | **Symptom**: The following event is recorded in the event file: `Lease table is full, DHCP lease was not added`.<br>**Scenario**: This issue occurred when DHCP snooping was configured. | DHCP Snooping |
| 16.10.0013 | 254786 | KB | **Symptom**: SSH fails to connect to the switch.<br>**Scenario**: This issue occurred because of the following reasons:<br>■ More than one RADIUS server was configured.<br>■ `aaa authentication ssh enable` was configured to use the other RADIUS server, instead of using the first one in the configuration. | AAA Authentication |
| 16.10.0013 | 254780 | KB | **Symptom**: When more number of MAC authentication clients (auth method: peap-mschapv2) get authenticated or reauthenticated, the following event is recorded multiple times in the event log: `PEAP SSL socket connection limit reached`.<br>**Scenario**: This issue occurred when more than 20 clients were authenticated or reauthenticated at the same time.<br>**Workaround**: Authenticate or reauthenticate less than 20 clients at the same time. | MAC Authentication |
| 16.10.0013 | 254481 | KB | **Symptom**: The switch CPU utilization increases to 80% or more, and CDP packet looping is observed across VLANs.<br>**Scenario**: This issue occurred when CDP pass-through was configured on two switches, which had more than one connection between them.<br>**Workaround**: Use `no cdp run` command to disable CDP globally, instead of configuring CDP mode pass-through. | CDP |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0012 | 254360 | KB | **Symptom**: A configuration push using the `cfg-restore` command from Aruba Central fails.<br>**Scenario**: This issue occurred when a switch configuration, containing `radius server host` commands, was pushed to Aruba Central or when the `cfg-restore` command was executed with the same `radius server host` configuration.<br>**Workaround**: Use the `copy tftp config` command to copy a configuration to the switch from Aruba Central, instead of the `cfg-restore` command for pushing a configuration. | Central |
| 16.10.0012 | 254519 | KB | **Symptom**: Aruba Central captures traffic only for one direction when a packet captured is performed.<br>**Scenario**: This issue occurred when traffic from a client in one subnet was sent to a client in another subnet, where the switch was acting as the gateway. | Central |
| 16.10.0012 | 254198 | KB | **Symptom**: A switch or management module crashes with the following message:<br>`Active/Commander system went down:`<br>`...`<br>`Health Monitor: Invalid Instr Misaligned Mem Access.`<br>**Scenario**: This issue occurred when the `copy command-output show tech all tftp <ip-address> <filename>` command was executed.<br>**Workaround**: Do not execute the `copy command-output show tech all tftp <ip-address> <filename>` command. | Chassis |
| 16.10.0012 | 254508 | KB | **Symptom**: Line card crashes due to `LOST_COMM_HEARTBEAT`.<br>**Scenario**: This issue occurred when there was a failover following a non-hitless failover. | Chassis |
| 16.10.0012 | 254096 | KB | **Symptom**: The `Rx Drop Bytes` parameter in the command output for `show interface queues <port>` displays very high values for the last few ports, even though these ports were down.<br>**Scenario**: This issue occurred when the `show interface queues <port>` command was issued. | CLI |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0012 | 254278 | KB | **Symptom**: The switch crashes when the `show crypto client-public-key` command is issued.<br>**Scenario**:This issue was observed when the `show crypto client-public-key` was issued when the `\t:` symbol was present in the client pub key file.<br>**Workaround**: Remove `\t:` symbol from the client public key file content. | Crypto |
| 16.10.0012 | 254380 | KB | **Symptom**: The switch crashes with the following message: `Health Monitor: Read Error Restr Mem Access .... Task='mdevMntr'.`<br>**Scenario**: This issue occurred when device-fingerprinting (DFP) was configured and DFP clients moved between ports. | Device Finger Printing |
| 16.10.0012 | 254354 | KB | **Symptom**: Although the packet is received before the MAC-age timeout interval expires, the MAC address of a peer is not available in the MAC table.<br>**Scenario**: This issue occurred when a packet of same source MAC address was sent on both the distributed trunk links alternatively at an interval close to the MAC-age timeout interval.<br>**Workaround**:<br>■ Increase the MAC-age timeout interval to a higher value.<br>■ Configure the MAC address statically. | Distribute Trunking |
| 16.10.0012 | 254768 | KB | **Symptom**: The switch crashes due to message buffer exhaustion.<br>**Scenario**: This issue occurred when the switch was configured with distributed trunking and VRRP. | Distribute Trunking |
| 16.10.0012 | 254760 | KB | **Symptom**: Removal of OSPF routes from the link-state database is delayed.<br>**Scenario**: This issue occurred when the switch received a Link-State Advertisement (LSA) that advertised routes with max age configured to remove the routes from the database. | OSPFv2 |
| 16.10.0012 | 254395 | KB | **Symptom**: The switch does not send the configured NAS-ID while sending a request to the RADIUS server.<br>**Scenario**: This issue occurred for both login and enable when the switch was configured with a non-default `server-group nas-id` and `ssh` was configured with peap-mschapv2. | Radius |
| 16.10.0012 | 254403 | KB | **Symptom**: The HTTP GET for /system/status/power/supply returns an internal server error. | REST |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue occurred when GET of /system/status/power/supply was executed when a stack member was down. | |
| 16.10.0012 | 254665 | KB | **Symptom**: REST connection fails when a Windows client makes an HTTP request.<br>**Scenario**: This issue occurred when a Windows client sent a REST HTTP request using PowerShell. | REST |
| 16.10.0012 | 254525 | KB | **Symptom**: The smartlink port stops forwarding VLAN traffic.<br>**Scenario**: This issue occurred when the:<br>■ The VLAN membership of a port was changed by removing it or adding it to any of the protected VLANs of the smartlink group.<br>■ STP was enabled and a non-default MSTP instance was created.<br>**Workaround**: Disable/enable the port. | Smartlinks |
| 16.10.0012 | 253623 | KB | **Symptom/Scenario**: When there is a change in backplane stacking, VSF topology, or removal of a power supply, no SNMP trap is sent. | SNMP |
| 16.10.0012 | 254722 | KB | **Symptom/Scenario**: When a user fails to login to the switch using SSH, no SNMP trap is sent. | SNMPv2 |
| 16.10.0012 | 254580 | KB | **Symptom/Scenario**: A switch no longer accepts SSH connections.<br>**Workaround**: Reboot the switch. | SSH |
| 16.10.0012 | 254393 | KB | **Symptom**: Event messages are sent to a Syslog server.<br>**Scenario**: This issue occurred when a syslog server was configured with the TCP option, `logging <IP-ADDR> tcp` and `ip source-interface syslog` was configured.<br>**Workaround**: Remove `ip source-interface syslog ...` from the config or reboot the switch after configuring syslog over TCP. | Syslog |
| 16.10.0012 | 254311 | KB | **Symptom**: Gradual memory depletion on a switch is observed.<br>**Scenario**: This issue occurred when the telnet sessions were closed abruptly.<br>**Workaround**: Disable the telnet server on the switch. | Telnet |
| 16.10.0011 | 253563 | KB | **Symptom**: The switch crashes with the following message: `Health Monitor: Misaligned Mem Access.` | 802.1X |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue occurred when any of the 802.1X clients' MAC address had a NULL value due to corruption, and the authenticator configuration on a switch port was disabled. | |
| 16.10.0011 | 254333, 254339 | KB | **Symptom**: Switch crashes with a message similar to the following: `Software exception at trlock.c -- in 'InetServer'.`<br>**Scenario**: This issue occurred when the `show tech all` command was executed from Aruba Central.<br>**Workaround**: Execute the `show tech all` command through the switch CLI. | Central |
| 16.10.0011 | 254255 | KB | **Symptom**: Switch crashes with a message similar to the following: `Software exception at multMgmtUtil.c -- in 'mOobmCtrl'.`<br>**Scenario**: This issue occurred when continuous or frequent `cfg-restore` operations (with password or aaa authentication related configurations) were executed, and in parallel, the switch was accessed through local-authentication.<br>**Workaround**: Do not access the switch using local-authentication when `cfg-restore` operation is in progress. | Chassis |
| 16.10.0011 | 253472 | KB | **Symptom/Scenario**: The following event is recorded in the event log multiple times where `xx%` is an increasing value: `03008 system: Ports A,B packet buffer allocation has reached xx%.`<br>**Workaround**: Reboot the switch. | Chassis |
| 16.10.0011 | 253803 | KB | **Symptom**: SSH connection (Remote Console) cannot be established from Aruba Central to the switch.<br>**Scenario**: This issue occurred when `ip authorized-managers` was configured on the switch and a Remote Console connection was attempted from Aruba Central.<br>**Workaround**: Add the following configuration to the switch:<br>`ip authorized-managers 127.0.0.1 255.255.255.254 access manager` | Console |
| 16.10.0011 | 254196 | KB | **Symptom**: Multicast traffic stops after a redundancy switchover. | IGMP |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue occurred when the IGMP `query-max-response-time` was configured to be `128` seconds and a redundancy switchover was performed.<br>**Workaround**: Remove IGMP from the VLAN and reconfigure the `query-max-response-time` to the default value of `10` seconds. | |
| 16.10.0011 | 253853 | KB | **Symptom**: Continuous RADIUS access request packets are sent from the switch to the RADIUS server.<br>**Scenario**: This issue occurred when a MAC address limit was configured and a device was attempted to be authenticated beyond the configured limit. | MAC Authentication |
| 16.10.0011 | 253844 | KB | **Symptom**: Removal of OSPF link state prefix from the link state database is delayed.<br>**Scenario**: This issue occurred when the switch received an OSPF Link-State Advertisement (LSA) with `MaxAge` configured to `3600` from a neighbor, and there were multiple OSPF sessions to the same router. | OSPFv2 |
| 16.10.0011 | 253965 | KB | **Symptom**: The switch closes the REST connection when the request is made from a Windows client.<br>**Scenario**: This issue occurred when a REST request was sent from PowerShell on a Windows client. | REST |
| 16.10.0011 | 253921 | KB | **Symptom**: MAC addresses are not learned on some ports and spanning tree shows the port in a `BLOCKED LISTEN` state.<br>**Scenario**: This issue occurred when the switch was configured to use RPVST.<br>**Workaround**: Reboot the switch. | Spanning Tree Protocol |
| 16.10.0011 | 252721 | KB | **Symptom**: Attempts to SSH or telnet to the switch fail and the following message is displayed: `Sorry, the maximum number of telnet sessions are active. Try again later.`<br>**Scenario**: This issue occurred when a vulnerability scan was run against the switch multiple times.<br>**Workaround**: Disable Telnet server. | Switch Access |
| 16.10.0011 | 254174 | KB | **Symptom**: The CPU utilization is elevated and the switch crashes with a `No msg buffer` message.<br>**Scenario**: This issue occurred when the switch was configured to use user-based tunnels (tunneled-node server). | Tunneling |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0011 | 253970 | KB | **Symptom**: Ports can be added to a trunk using the web interface even if those ports are configured with IGMP fastlearn.<br>**Scenario**: This issue occurred when IGMP fastlearn was configured on a few ports of the switch, and the switch was accessed through the web interface to add the IGMP fastlearn enabled ports to the trunk.<br>**Workaround**: Use the CLI to add ports to a trunk. | Web Interface |
| 16.10.0010 | 253775 | KB | **Symptom/Scenario**: Switch does not get provisioned to Activate. | Activate |
| 16.10.0010 | 253807 | KB | **Symptom**: Unsupported values are accepted as ACL numbers for both standard and extended ACLs when configuring ACLs from the REST interface (for example, Aruba Central). Once configured, these ACLs cannot be deleted using REST or the CLI.<br>**Scenario**: This issue occurred when the REST interface was used to configure an ACL with an unsupported value. | ACLs |
| 16.10.0010 | 253425 | KB | **Symptom**: The username sent for a successful MAC-authenticated client is the MAC address, rather than the username.<br>**Scenario**: This issue occurred when a client was authenticated using MAC authentication. | Authentication |
| 16.10.0010 | 250901 | KB | **Symptom**: Switch randomly loses connectivity to Activate and Aruba Central.<br>**Scenario**: This issue occurred when configuring the switch to connect to Aruba Central. | Central |
| 16.10.0010 | 253659<br>253925 | KB | **Symptom**: Switch fails to connect to Aruba Central.<br>**Scenario**: This issue occurred when the switch was configured to connect to Aruba Central. | Central |
| 16.10.0010 | 252143 | KB | **Symptom**: One of the following symptoms are seen:<br>■ When the command `show system power-supply` is executed, the output displays one or more power supplies with a state of **Not Powered** even though all modules are powered and PoE is functioning normally.<br>■ One or more port modules is stuck in a booting or failed state.<br>**Scenario**: This issue occurred when all power supplies in the switch lost and regained power at the same time. This scenario was most commonly experienced with very brief power loss or brownout events.<br>**Workaround**:<br>■ Distribute PSU power sources to different power circuits to prevent simultaneous power | Chassis |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | down/power up.<br>■ Reboot switch, remove and insert power cords, or remove and insert power supplies that are in a **Not powered** state.<br>■ Modules may recover after an undetermined period of time. Otherwise, resetting the affected slots, resetting the affected modules, or rebooting the switch may be required to recover. | |
| 16.10.0010 | 253422 | KB | **Symptom**: The following error message is displayed: `Invalid Input : grep usage error` when executing `show` command.<br>**Scenario**: This issue occurred when a `show` command was executed with `include <anyword> <anyword>`.<br>**Workaround**: Execute the `show` command without `include <anyword> <anyword>`. | CLI |
| 16.10.0010 | 253485 | KB | **Symptom**: When more than 3000 VLANs are configured, executing the `show run` command takes one or two minutes to begin displaying output.<br>**Scenario**: This issue occurred when `show run` command was executed after configuring a minimum of 3000 VLANs. | CLI |
| 16.10.0010 | 252317 | KB | **Symptom**: Connectivity to end devices may be lost due to MAC learn inconsistencies between the InterSwitch-Connect (ISC) link and a trunk member link.<br>**Scenario**: This issue occurred when the distributed trunking was configured and one of the DT member switches was upgraded.<br>**Workaround**: Clear the incorrect MAC entries in both of the DT switches using the `clear mac-address` command. | Distributed Trunking |
| 16.10.0010 | 253303 | KB | **Symptom**: Peer device does not get an IP address when the port it is connected to is configured using a device-profile.<br>**Scenario**: This issue occurred when a port is configured using device profile and a peer device is connected to it.<br>**Workaround**: Disable device-profile and manually configure the port. | Device Profile |
| 16.10.0010 | 253507 | KB | **Symptom**: Devices connected to the switch are unable to send or receive packets.<br>**Scenario**: This issue occurred when a multicast listener query was received with an unspecified source IP address. | Multicast |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Workaround**: Stop sending malformed multicast listener query packets to the switch. | |
| 16.10.0010 | 252993 | KB | **Symptom**: Some RADIUS accounting packets sent to the RADIUS server have a very large size.<br>**Scenario**: This issue occurred when a downloadable user role was configured with a user policy, network accounting was enabled, and a client was authenticated. | RADIUS |
| 16.10.0010 | 253736 | KB | **Symptom**: Disconnect Change of Authorization (CoA) request is not honored.<br>**Scenario**: This issue occurred when the radius-server group was configured, a client was authenticated, and a disconnect CoA request with the default nas-id was sent.<br>**Workaround**: Configure `aaa server-group radius <Group name> nas-id <NAS-ID>` where the NAS-ID matches the NAS Identifier value shown in the output of the `show radius authentication` command. | RADIUS |
| 16.10.0010 | 253557 | KB | **Symptom**: Using REST to retrieve the resource identifier `/lldp/remote-device` fails to display the IPv4 address of the neighbor.<br>**Scenario**: This issue occurred when the REST resource operation GET was used to retrieve the data associated with `/lldp/remote-device`. | REST |
| 16.10.0010 | 253789 | KB | **Symptom**: Switch serial number contains an extra space at the end when it is read using SNMP.<br>**Scenario**: This issue occurred when the switch serial number was read using SNMP.<br>Example:<br>MIB OID: 1.3.6.1.2.1.47.1.1.1.1.11.1<br>MIB File: ENTITY-MIB | SNMP |
| 16.10.0010 | 253342 | KB | **Symptom**: SSH/Telnet/Console connections to the switch fail with an error message: `Maximum session limit is reached`.<br>**Scenario**: This issue occurred when multiple users logged in and out and RADIUS was configured as the primary authentication method.<br>**Workaround**: Reboot the switch. | Switch Access |
| 16.10.0010 | 253407 | KB | **Symptom**: Unable to log in to the switch using TACACS credentials.<br>**Scenario**: This issue occurred when a source interface for TACACS was configured using the `ip source-interface tacacs` command and the switch was upgraded to 16.10.0009. | TACACS |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0010 | 253001 | KB | **Symptom**: When there are continuous link flaps on the link-to-monitor ports within a fraction of a second, some link-to-disable ports may not come up once the link-to-monitor port stabilizes.<br>**Scenario**: This issue occurred when the link-to-monitor port used a transceiver connected by fibre and flapped continuously at a high rate.<br>**Workaround**: Use Fault-Finder to disable the link-to-monitor if it is flapping too often. The link-to-disable port can be disabled and re-enabled to bring it back up. | UFD |
| 16.10.0010 | 253290 | KB | **Symptom**: Switch crashes when it is accessed through the web interface.<br>**Scenario**: This issue occurred when the switch was accessed using the web interface and RADIUS authentication was configured for web access.<br>**Workaround**: Disable RADIUS authentication for web access. | Web UI |
| 16.10.0010 | 253577 | KB | **Symptom**: When the VLAN edit option is clicked in the web interface, the screen is greyed out, and no pop-up menu is displayed.<br>**Scenario**: This issue occurred when the switch is configured to use meshing and the web interface is accessed to select the **Edit** option on the **Interface > VLAN** page.<br>**Workaround**: Configure VLANs using the CLI or the traditional web interface. | Web UI |
| 16.10.0010 | 253877 | KB | **Symptom**: The **WebUI Security > Clients** page displays incorrect MAC addresses, which results in the user role, IP address, and status columns to be empty.<br>**Scenario**: This issue occurred when a few workstations with higher value MAC addresses (for example, 9c:dc:71:fb:77:fe) are connected to the last ports of a 2930 stack or the last module of a 5400R. | Web UI |
| 16.10.0009 | 252885 | KB | **Symptom**: Switch appears down in Aruba Central.<br>**Scenario**: This issue occurred because the system time was set to the year 2036, though NTP sync was successful, and the switch was connected to Aruba Central.<br>**Workaround**: Configure an NTP server in the switch. | Activate |
| 16.10.0009 | 252226 | KB | **Symptom**: Switch does not respond during the ZTP process.<br>**Scenario**: This issue occurred when connecting to the switch using SSH, while Airwave was transferring the configuration to the switch. | AirWave |
| 16.10.0009 | 252825 | KB | **Symptom**: A switch crashes and displays the following message: | BGP |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | `Software exception at bgp_med.c: 629 -- in 'eRouteCtrl' …. Routing Stack: Assert Failed.`<br>**Scenario**: This issue occurred when the maximum prefix for BGP was configured to limit the number of routes BGP learns, in an environment with many route flaps.<br>**Workaround**: Eliminate the frequent BGP route flaps. | |
| 16.10.0009 | 253081 | KB | **Symptom**: Switch reports self test failure or unsupported module in the event log.<br>**Scenario**: This issue occurred when the module is booted with a `JL308A xcvr`. | Boot |
| 16.10.0009 | 251418 | KB | **Symptom**: Pushing a switch configuration template from Aruba Central fails and a 500 error code is returned.<br>**Scenario**: This issue occurred when a configuration template that had no untagged ports in VLAN 1 was pushed from Aruba Central.<br>**Workaround**: In the configuration template, add at least one untagged port in VLAN 1. | Central |
| 16.10.0009 | 253174 | KB | **Symptom/Scenario**: The switch experienced an NMI crash with the following message:<br>`Task='ewsCloudRcv'.` | Central |
| 16.10.0009 | 250966 | KB | **Symptom**: The switch fails to display the power supply details.<br>**Scenario**: In a stack or VSF configuration, the switch failed to display the power supply details for all stack member switches when using the show system power-supply detailed command. | CLI |
| 16.10.0009 | 253276 | KB | **Symptom**: Unable to copy crash-files, core-dump, and the show tech all command output from the switch.<br>**Scenario**: This issue occurred when executing the copy command with an invalid IP address, file name, hostname, or when parallelly executing the copy command in other sessions.<br>**Workaround**:<br>■ Copy the core file from the web interface.<br>■ Copy the show tech all command output from the console interface. | CLI |
| 16.10.0009 | 252430 | KB | **Symptom**: Invalid MAC address entries are seen in the DHCP snooping binding table.<br>**Scenario**: This issue occurred when switch received malformed DHCP or BOOTP packets.<br>**Workaround**: Configure a DHCP authorized server so that requests only from authorized servers are processed. | DHCP Snooping |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0009 | 252265 | KB | **Symptom**: The switch does not forward DHCP packets.<br>**Scenario**: This issue occurred when both DHCP snooping and IP client tracker trusted were configured, and the client was authenticated. | IP Client Tracker |
| 16.10.0009 | 252701 | KB | **Symptom/Scenario**: User tunnel is lost when a controller fail-over is performed in a two node controller cluster.<br>**Workaround**: Re-establish the tunnel with a port flap and re-authentication. | Jumbo Frames |
| 16.10.0009 | 252833 | KB | **Symptom**: MSTP does not work as expected and does not block ports when it should.<br>**Scenario**: This issue occurred when two ports in a loop were in a forwarding state with MSTP and port-security non-default learn mode enabled.<br>**Workaround**: Disable port-security. | Spanning Tree |
| 16.10.0009 | 252338 | KB | **Symptom**: Incorrect message Rejected because maximum session limit is reached is printed when attempting to establish an SSH connection to the VSF standby OOBM IP address.<br>**Scenario**: This issue occurred when establishing an SSH connection to the standby OOBM IP address. | SSH |
| 16.10.0009 | 252613 | KB | **Symptom**: Unable to connect to the switch using SSH.<br>**Scenario**: This issue occurred when the switch is configured to use TACACS and a malformed TACACS packet is received by the switch.<br>**Workaround**: Reboot the switch. | SSH |
| 16.10.0009 | 251966 | KB | **Symptom**: The switch sends logging events with a "Z" at the end of the timestamp when the it is not configured to use UTC.<br>**Scenario**: This issue occurred when the switch sent syslog messages over TLS. | Syslog |
| 16.10.0009 | 252410 | KB | **Symptom**: The switch either reboots or fails over from the active to standby management module and records a Watchdog Reset entry in the event log.<br>**Scenario**: This issue occurred when IP directed-broadcast was configured in the switch and Wake On LAN traffic was sent to a directly connected subnet.<br>**Workaround**: Disable IP directed-broadcast. | VSF |
| 16.10.0009 | 252762 | KB | **Symptom**: Although the VXLAN tunnel name was configured, it was not displayed.<br>**Scenario**: This issue occurred when the VXLAN tunnel name was configured before configuring the source and destination IP addresses for the tunnel. | VXLAN |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0009 | 252443 | KB | **Symptom/Scenario**: The Reboot button is displayed for a few seconds in the Web UI. Clicking it allowed an operator to reboot the switch. | Web UI |
| 16.10.0008 | - | KB | Version 16.10.0008 was never released. | - |
| 16.10.0007 | 252007 | KB | **Symptom**: The switch sends an incorrect CLASS attribute value in the RADIUS accounting packet.<br>**Scenario**: When the CLASS attribute is updated during re-authentication of a MAC-authenticated client session, the switch fails to send the new CLASS attribute value in the RADIUS accounting packet.<br>**Workaround**: Force a new client authentication session by disabling/enabling the port after the CLASS attribute value changes. | Accounting |
| 16.10.0007 | 251765 | KB | **Symptom**: The `show runnig-config` output does not display some access list entries (ACEs).<br>**Scenario**: When the switch is configured with extended ACLs and connect-rate-filter, some ACEs are not displayed in the output of the show runnig-config command.<br>**Workaround**: Use the show access-list config command to get the complete extended ACL configuration. | ACLs |
| 16.10.0007 | 251273 | KB | **Symptom**: The switch incorrectly places clients in the configured authorized VLAN (auth-vid).<br>**Scenario**: When using chap-radius authorized option, if the route to the RADIUS server is not resolved during the switch boot up, clients are incorrectly placed in the configured authorized VLAN (auth-vid) rather than the guest VLAN (unauth-vid) or initial-role.<br>**Workaround**: Reauthenticate the affected clients. | Authentication |
| 16.10.0007 | 251659 | KB | **Symptom**: Switch fails to move the client MAC address from one port to another.<br>**Scenario**: When addr-move is configured to enable roaming for authenticated clients from one port to another, with Private VLAN enabled, the switch fails to move the client MAC address.<br>**Workaround**: Disable and re-enable the switch interface where the affected client moved to. | Authentication |
| 16.10.0007 | 252183 | KB | **Symptom**: The switch experiences traffic loss after an indirect nexthop peer failure.<br>**Scenario**: If an older ECMP route is removed due to an indirect nexthop peer failure, the switch fails to correctly update the IP route description table with the newer nexthop route. | BGP |
| 16.10.0007 | 251927 | KB | **Symptom**: The switch fails to remove CDP configuration for a port. | CDP |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: When a port is added to a trunk interface, the switch fails to remove the previous non-default CDP configuration for that port (example: no cdp enable <PORT-NUM>).<br>**Workaround**: Remove the non-default CDP configuration from the individual port before adding it to trunk interface. | |
| 16.10.0007 | 252053 | KB | **Symptom/Scenario**: The switch crashes with an error message similar to: `Software exception in ISR at pvDmaV1Rx.c <...> ASSERT: No resources available!` | Central |
| 16.10.0007 | 252267 | KB | **Symptom**: The switch experiences high CPU utilization.<br>**Scenario**: In conditions of low network bandwidth or network congestion that cause frequent disconnections from the Aruba Central Portal, the switch experiences high CPU utilization while attempting to reconnect to Aruba Central and while being managed by other NMS applications such as Solarwinds at the same time.<br>**Workaround**: Use only one NMS application to manage the switch if network bandwidth capacity or congestion cannot be improved. | Central |
| 16.10.0007 | 252066 | KB | **Symptom/Scenario**: The switch crashes with a message similar to: `Health Monitor: Restr Mem Access ... Task='mdevMntr'.` | Device finger printing |
| 16.10.0007 | 251876 | KB | **Symptom**: The switch may fail to apply the correct VLAN to dynamic trunks.<br>**Scenario**: After a reboot of a switch configured for dynamic trunks with device profile enabled on ports, the switch may fail to apply the correct VLAN configured in the device-profile, after the port is joined to the dynamic trunk.<br>**Workaround**: Disable and enable device-profile. | Dynamic Trunks |
| 16.10.0007 | 251579 | KB | **Symptom**: The switch port LEDs light amber (self-test failure).<br>**Scenario**: In rare conditions, random ports may fail self-test after a switch reboot causing the port LED to be lit amber and triggering a warning event message similar to: `00371 chassis: Port <PORT-NAME> self test failure ERR: 10191800`<br>**Workaround**: Reboot the switch. | Interfaces |
| 16.10.0007 | 252187 | KB | **Symptom**: PoE LED is incorrectly lit green on the management module. | LEDs |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: In a VSF stack, when the respective switch member does not have any PoE capable line modules installed. | |
| 16.10.0007 | 251972 | KB | **Symptom**: Some clients using the PEAP authentication mechanism are not successfully authenticated.<br>**Scenario**: When concurrent authentication requests are sent to the switch using peap-mschapv2, some clients may not be successfully authenticated, even though ACCESS ACCEPT is sent from the RADIUS server. | MAC Authentication |
| 16.10.0007 | 252170 | KB | **Symptom**: Some multicast traffic is incorrectly flooded on all ports belonging to a VLAN.<br>**Scenario**: Multicast packets received with aTTL <= 1 are indefinitely flooded to all ports of a PIM enabled VLAN. | Multicast |
| 16.10.0007 | 249716 | KB | **Symptom**: The switch fails to pass traffic through a promiscuous port.<br>**Scenario**: After a reboot event, the switch fails to pass traffic trough a promiscuous port in the primary VLAN.<br>**Workaround**: Remove and re-add the affected promiscuous port from/to the primary VLAN. | Private VLAN |
| 16.10.0007 | 251339 | KB | **Symptom**: The switch or the switch module may crash with an error message similar to: `Read Error Restr Mem Access <...> Task='mAdMUpCtrl'.`<br>**Scenario**: When qos trust dscp on a 40G port is enabled, the switch or switch module may crash with an error message similar to: `Read Error Restr Mem Access <...> Task='mAdMUpCtrl.` | QoS |
| 16.10.0007 | 252090 | KB | **Symptom**: Switch fails to flag the unreachable RADIUS servers.<br>**Scenario**: When RADIUS server tracking is enabled, the switch fails to flag those RADIUS servers configured using the fully qualified domain name (FQDN) when they are unreachable with an asterisk (*) in the output of the show radius command.<br>**Workaround**: Use IP address for RADIUS server configuration when RADIUS server tracking is enabled. | RADIUS |
| 16.10.0007 | 252131 | KB | **Symptom**: REST API calls may experience some slight delay in execution response.<br>**Scenario**: When multiple REST API commands are executed over the same HTTPS session, they may experience a slight delay in execution response. | REST |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Workaround**: Use a new HTTPS session for each REST API call. | |
| 16.10.0007 | 251899 | KB | **Symptom**: Switch fails to return the serial number of the power supply.<br>**Scenario**: When configured in a stack, the switch does not return the serial number of power supplies for the stack member switches when polling the entPhysicalSerialNum SNMP object.<br>**Workaround**: The power supply serial number can be found in the show system power-supply output. | SNMP |
| 16.10.0007 | 252377 | KB | **Symptom**: The switch fails to send traffic over some switch interfaces.<br>**Scenario**: After a redundancy switchover to the standby VSF switch while spanning tree is enabled in PVST mode, the switch fails to forward traffic over the switch ports transitioned from Blocking to Forwarding state.<br>**Workaround**: Disable and re-enable the affected switch ports. | Spanning Tree |
| 16.10.0007 | 250797 | KB | **Symptom**: The switch sends an incorrect checksum when forwarding certain UDP frames.<br>**Scenario**: If a received UDP frame has no checksum or the checksum value of zero (0), the switch incorrectly calculates the checksum when forwarding it. | UDP |
| 16.10.0007 | 252409 | KB | **Symptom**: The switch fails to override the initial-role.<br>**Scenario**: When an existing per-port initial-role is modified, the switch fails to re-apply the new initial-role to ports with clients already authenticated in the previous initial-role.<br>**Workaround**: Remove the existing per-port initial-role config and configure the new initial-role on the port. | User Roles |
| 16.10.0007 | 251475 | KB | **Symptom**: The switch experiences high CPU utilization and possible console connectivity issues.<br>**Scenario**: When configuring or modifying aggregated interfaces (trunks) with more than 3 member ports on a switch where there is a very high number of configured VLANs, the switch experiences high CPU utilization and possible console connectivity issues while applying the configuration. | VLAN |
| 16.10.0007 | 251505 | KB | **Symptom**: The WebUI contains an XSS vulnerability.<br>**Scenario**: Configure the editable parameters in the WebUI with values that can cause an XSS attack. | Web UI |
| 16.10.0007 | 251524 | KB | **Symptom**: The switch fails to display some ports on the Ports page of the WebUI. | Web UI |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: When aSysName with trailing zeroes is received in the LLDP packet from a neighboring device, the switch fails to list some ports in the Ports page when using the WebUI.<br>**Workaround**: To get the information for all ports use one of the following options:<br>■ Disable LLDP on the port where the device with `invalidSysName` is connected.<br>■ Use the traditional web UI to get the information for the affected/missing ports.<br>■ Use switch CLI commands to get the information for the affected/missing ports. | |
| 16.10.0006 | - | KB | Version 16.10.0006 was never released. | - |
| 16.10.0005 | 251473 | KB | **Symptom**: End devices periodically lose access to the network.<br>**Scenario**: When ports are configured with user-based tunneling in addition to 802.1X and MAC authentication, end devices connected to those parts periodically lose access to the network. | Tunneling |
| 16.10.0004 | - | KB | Version 16.10.0004 was never released. | - |
| 16.10.0003 | 251317 | | **Symptom**: A Windows client that joins a domain other than the one defined in Cisco ISE fails to authenticate. The client will also wait more than 5 minutes before attempting MAC address authentication.<br>**Scenario**: This issue is observed when MAC and 802.1X authentication are enabled on the port and the configured auth-order is 802.1X-MAC and an initial role. | 802.1X |
| 16.10.0003 | 251464 | KB | **Symptom**: VSF stack members crash intermittently during 802.1X client reauthentication and the following message is displayed: `Software exception in ISR at pvDmaV1Rx.c: -> ASSERT: No resources available!.`<br>**Scenario**: This issue is observed when ports with LLDP traffic are configured with 802.1X and MAC authentication, and the RADIUS VSA HP-Port-Client-Limit-MA value is zero. | 802.1X |
| 16.10.0003 | 251498 | KB | **Symptom**: A client is unable to pass traffic.<br>**Scenario**: This issue is observed when the clear mac-address vlan 1 mac command is issued to clear the switch's base MAC address from VLAN 1. | Basic Layer 2 |
| 16.10.0003 | 251280 | KB | **Symptom**: Deploying a switch template through Airwave/Aruba Central fails. | Central |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue is observed when the IP address from VLAN1 is removed from a new configuration template and is pushed to the switch with the "ntpserver-name <server name>".<br>**Workaround**: Do not remove the IP address from VLAN 1 in the new template. | |
| 16.10.0003 | 249172 | KB | **Symptom**: The Event log lists fan failure events and the amber LED is displayed on the front panel of the switch.<br>**Scenario**: The switch operates normally with no change in the environmental temperature. | Chassis Manager |
| 16.10.0003 | 251393 | KB | **Symptom**: A switch crashes with the following message `Software exception in ISR at pvDmaV1Rx.c -> ASSERT: No resources available.`<br>**Scenario**: This issue is observed when a switch is configured with an initial role with a captive-portal-profile and a client is placed in this initial role because the RADIUS server is unreachable. | Classifier |
| 16.10.0003 | 250816 | KB | **Symptom**: Authenticated users are disconnected from the switch.<br>**Scenario**: This issue is observed when users disable and enable the interface which connects to the dhcp- relay switch, after configuring the DHCP server, DHCP relay, and DHCP snooping with ip-source lockdown.<br>**Workaround**: Disable ip-source lockdown. | DIPLD |
| 16.10.0003 | 251662 | KB | **Symptom**: Unable to configure a /31 subnet address as source/destination address for tunnel interfaces.<br>**Scenario**: This issue is observed when users attempt to configure a /31 subnet address as source/ destination address for a tunnel interface.<br>**Workaround**: Configure a /30 subnet address. | L3 Addressing |
| 16.10.0003 | 249465 | KB | **Symptom**: A switch crashes and displays the following message: `Software exception at ospf2.c -- in 'eRouteCtrl' -> Routing Stack: Assert Failed.`<br>**Scenario**: This issue is observed when a switch is configured with OSPF and one of the OSPF neighbors is disconnected. | OSPF |
| 16.10.0003 | 251615 | KB | **Symptom**: An attacker is able to obtain sensitive data without providing valid login credentials after a successful REST query.<br>**Scenario**: This issue is observed when web management is enabled on the switch. | REST |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0003 | 251340 | KB | **Symptom**: Tunneled clients lose network connectivity.<br>**Scenario**: This issue is observed when user tunnels are configured in addition to ip client-tracker trusted and ip client-tracker probe-delay.<br>**Workaround**:<br>1. Remove ip client-tracker probe-delay from the configuration.<br>2. Disable the port.<br>3. Clear ARP.<br>4. Re-enable the port. | Tunneled Node |
| 16.10.0003 | 251893 | KB | **Symptom**: A switch port is in the Disabled state.<br>**Scenario**: This issue is observed when spanning tree is enabled and Per-Port Tunneled Node (PPTN) is configured on two ports that are connected.<br>**Workaround**: Do not connect two PPTN ports. | Tunneled Node |
| 16.10.0003 | 251325 | KB | **Symptom**: Users are unable to modify the vlan-id-tagged list of a user role.<br>**Scenario**: This issue is observed when the user applies a template that adds VLANs to the vlan-id-tagged list of a user role.<br>**Workaround**: Use a template that does not extend the list of VLANs in vlan-id-tagged. | User Roles |
| 16.10.0003 | 251030 | KB | **Symptom**: The output of the show interface command differs for a VSF and a non-VSF interface.<br>**Scenario**: This issue is observed when a switch is configured for VSF.<br>**Workaround**: Execute the clear statistics global command and output of show interface command will be the same for both VSF and non-VSF interfaces. | VSF |
| 16.10.0003 | 251506 | KB | **Symptom**: The switch manager password is altered to an attack-controlled value.<br>**Scenario**: This issue is observed when the user clicks a malicious hyperlink. | Web UI |
| 16.10.0003 | 251314 | KB | **Symptom**: Switches appear offline in Aruba Central.<br>**Scenario**: This issue is observed after the switch software is upgraded from 16.04 to 16.08.<br>**Workaround**: Reboot the switch. | ZTP |
| 16.10.0002 | 250366 | KB | **Symptom**: An Apple MacOS device (desktop or laptop) is unable to maintain authentication with APs. | 802.1X |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: When an AP is connected to a switch port that has been configured with device-identity bypass, an Apple MacOS device (desktop or laptop) receives EAP request ID packets after 802.1X authentication and is unable to maintain authentication with the AP.<br>**Workaround**: Configure a MAC-based ACL to block the EAP request identity to multicast MAC address. | |
| 16.10.0002 | 250681 | KB | **Symptom/Scenario**: The Topology section of Airwave shows spanning tree details for a switch that does not have spanning tree enabled. | AirWave |
| 16.10.0002 | 250934 | KB | **Symptom**: The switch does not respond to commands from a console or SSH session.<br>**Scenario**: After updating the switch configuration using Aruba Central while clients are authenticated, the switch may not respond to commands from a console or SSH session.<br>**Workaround**:<br>1. Apply a template disabling MAC authentication on all ports.<br>2. Apply a template with AAA config changes.<br>3. Apply a template enabling MAC authentication on all ports. | Central |
| 16.10.0002 | 251313 | KB | **Symptom**: The switch experiences a high CPU utilization and loses connection with Central.<br>**Scenario**: when the switch is upgraded to 16.08.0001 and a template with tls and cwmp commands is pushed from Central, the switch experiences high CPE utilization and loses the connection to Aruba Central.<br>**Workaround**: Remove tls application cloud lowest-version tls1.2 and cwmp from the switch template. | Central |
| 16.10.0002 | 250247 | KB | **Symptom/Scenario**: The switch crashes with a message similar to: `Software exception in ISR at interrupts_om.c-> Excessive OM FP interrupts.` | Chassis |
| 16.10.0002 | 250514 | KB | **Symptom**: The show running config and show modules commands report false information.<br>**Scenario**: When a VSF configuration has been loaded to the switch without MAC addresses specified and the switch is rebooted, the `show running config` command returns incorrect data and the show modules command reports a module as failed.<br>**Workaround**: Download a VSF configuration that includes member MAC addresses. | Config |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0002 | 250542 | KB | **Symptom**: The switch is unable to classify Aruba APs.<br>**Scenario**: After configuring device fingerprinting, the switch is unable to classify Aruba APs. | Device finger printing |
| 16.10.0002 | 250600 | KB | **Symptom/Scenario**: The help text for the `device-identity lldp oui` command indicates that the required input is a MAC-OUI. | Device finger printing |
| 16.10.0002 | 251075 | KB | **Symptom**: The switch crashes with a message similar to `Task='mdevMntr'`.<br>**Scenario**: When the switch has been configured with a device finger printing policy on a port with clients, if the port is bounced multiple times, the switch may crash with a message similar to `Task='mdevMntr'`. | Device finger printing |
| 16.10.0002 | 250957 | KB | **Symptom**: Host packets are denied with a message similar to `dlpld: AM1: Access denied`.<br>**Scenario**: When the switch has been configured using the aaa port-access and ip source-lockdown commands and clients authenticate to the switch, if more than one client is placed in a VLAN provided by the RADIUS server, host packets are denied.<br>**Workaround**: Disable Dynamic IP Lockdown on the switch using the no ip source-lockdown command. | DIPLD |
| 16.10.0002 | 250550 | KB | **Symptom**: Primary and secondary VLANs do not have MAC address entries.<br>**Scenario**: When a port has been configured with PVLAN and port security and the port is subsequently disabled and re-enabled, MAC address entries are not present in the primary and secondary VLANs.<br>**Workaround**: Reconfigure the port security configuration of the port. | MAC address |
| 16.10.0002 | 250392 | KB | **Symptom**: The switch crashes with a message similar to: `Health Monitor: Invalid Instr Misaligned Mem Access.`<br>**Scenario**: After an IP address has been reassigned from one VLAN to another VLAN using the menu interface, the switch may crash with a message similar to: `Health Monitor: Invalid Instr Misaligned Mem Access.`<br>**Workaround**: Disable the first VLAN and save the configuration from the menu interface. Then, configure the deleted IP address on the second VLAN. | Menu |
| 16.10.0002 | 245830 | KB | **Symptom**: The switch fails to list the switch ports in the Ports web management page. | Next Gen GUI |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: When a peer device that advertises information in LLDP has a sysName string with special characters, the switch fails to display the port list table on the Ports web management page.<br>**Workaround**: Remove the special characters from the peer device sysName or use CLI commands to get specific port information. | |
| 16.10.0002 | 250833 | KB | **Symptom**: After a switch reboot, OSPF is stuck in the INIT state.<br>**Scenario**: When a switch that is configured with OSPF, but ip router-id has not been configured, is rebooted OSPF remains in the INIT state.<br>**Workaround**: Configure the router ID manually. | OSPF |
| 16.10.0002 | 250958 | KB | **Symptom**: The hit counters in the output of the show statistics policy command shows all zeros.<br>**Scenario**: If a QoS policy with several class entries across all ports on multiple modules has been applied, the output of the show statistics policy command shows all zeros in the hit counters. | QoS |
| 16.10.0002 | 251017 | KB | **Symptom**: The event log displays `lpAddrMgr: Failed to add FIB entry - neighbor matches existing route (vrf:0 A.B.C.D/32).`<br>**Scenario**: When the switch has been configured with a VRRP master and the connected routes are redistributed using routing protocols, the event log will display a lpAddrMgr message. | VRRP |
| 16.10.0002 | 251203 | KB | **Symptom**: Pings to the VRRP virtual IP address fail.<br>**Scenario**: If a switch module is reloaded, added, or hot-swapped, if a VSF stack member joins the stack after a stack split event or after a switch reboot with expansion module present, the switch fails to respond to ping packets to the VRRP virtual IP address. | VRRP |
| 16.10.0002 | 250489 | KB | **Symptom**: High utilization of a VSF link is reported by the switch.<br>**Scenario**: When VSF is configured with one link having multiple ports and then a VSF link port toggle is performed by disabling then re-enabling the VSF interface, the switch reports a high link utilization. | VSF |
| 16.10.0002 | 250754 | KB | **Symptom**: The switch cannot be found in Aruba Central even though the CLI reports the switch as being connected.<br>**Scenario**: When a VSF stack is already checked into Aruba Central with the same stack ID as another VSF stack, switches in the stack cannot be found in Aruba Central. | VSF |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Workaround**: Ensure all switches are running 16.06 or later and then form the VSF stack. | |
| 16.10.0002 | 250896 | KB | **Symptom**: Switch ports are not listed in the web interface.<br>**Scenario**: If a peer device advertises an LLDP port ID containing special characters, switch ports are not listed in the web interface. | Web UI |
| 16.10.0001 | 250366 | KB | **Symptom**: An Apple MacOS device (desktop or laptop) is unable to maintain authentication with APs.<br>**Scenario**: When an AP is connected to a switch port that has been configured with device-identity bypass, an Apple MacOS device (desktop or laptop) receives EAP request ID packets after 802.1X authentication and is unable to maintain authentication with the AP.<br>**Workaround**: Configure a MAC-based ACL to block the EAP request identity to multicast MAC address. | 802.1X |
| 16.10.0001 | 250681 | KB | **Symptom/Scenario**: The Topology section of Airwave shows spanning tree details for a switch that does not have spanning tree enabled. | AirWave |
| 16.10.0001 | 250934 | KB | **Symptom**: The switch does not respond to commands from a console or SSH session.<br>**Scenario**: After updating the switch configuration using Aruba Central while clients are authenticated, the switch may not respond to commands from a console or SSH session.<br>**Workaround**:<br>1. Apply a template disabling MAC authentication on all ports.<br>2. Apply a template with AAA config changes.<br>3. Apply a template enabling MAC authentication on all ports. | Central |
| 16.10.0001 | 250247 | KB | **Symptom/Scenario**: The switch crashes with a message similar to: `Software exception in ISR at interrupts_om.c-> Excessive OM FP interrupts.` | Chassis |
| 16.10.0001 | 250154 | KB | **Symptom**: The global status LED on all members of a VSF stack turns amber.<br>**Scenario**: When one member of a VSF stack experiences an over temperature, the global status LED on all members of the stack turns amber. | Chassis Manager |
| 16.10.0001 | 250514 | KB | **Symptom**: The show running config and show modules commands report false information. | Config |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: When a VSF configuration has been loaded to the switch without MAC addresses specified and the switch is rebooted, the show running config command returns incorrect data and the show modules command reports a module as failed.<br>**Workaround**: Download a VSF configuration that includes member MAC addresses. | |
| 16.10.0001 | 250542 | KB | **Symptom**: The switch is unable to classify Aruba APs.<br>**Scenario**: After configuring device fingerprinting, the switch is unable to classify Aruba APs. | Device finger printing |
| 16.10.0001 | 251075 | KB | **Symptom**: The switch crashes with a message similar to `Task='mdevMntr'`.<br>**Scenario**: When the switch has been configured with a device finger printing policy on a port with clients, if the port is bounced multiple times, the switch may crash with a message similar to `Task='mdevMntr'`. | Device finger printing |
| 16.10.0001 | 250600 | KB | **Symptom/Scenario**: The help text for the device-identity lldp oui command indicates that the required input is a MAC-OUI. | Device identity |
| 16.10.0001 | 250957 | KB | **Symptom**: Host packets are denied with a message similar to `dlpld: AM1: Access denied`.<br>**Scenario**: When the switch has been configured using the aaa port-access and ip source-lockdown commands and clients authenticate to the switch, if more than one client is placed in a VLAN provided by the RADIUS server, host packets are denied.<br>**Workaround**: Disable Dynamic IP Lockdown on the switch using the no ip source-lockdown command. | DIPLD |
| 16.10.0001 | 250550 | KB | **Symptom**: Primary and secondary VLANs do not have MAC address entries.<br>**Scenario**: When a port has been configured with PVLAN and port security and the port is subsequently disabled and re-enabled, MAC address entries are not present in the primary and secondary VLANs.<br>**Workaround**: Reconfigure the port security configuration of the port. | MAC address |
| 16.10.0001 | 250392 | KB | **Symptom**: The switch crashes with a message similar to: `Health Monitor: Invalid Instr Misaligned Mem Access`.<br>**Scenario**: After an IP address has been reassigned from one VLAN to another VLAN using the menu interface, the switch may crash with a message similar to: `Health Monitor: Invalid Instr Misaligned Mem Access`. | Menu |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Workaround**: Disable the first VLAN and save the configuration from the menu interface. Then, configure the deleted IP address on the second VLAN. | |
| 16.10.0001 | 250833 | KB | **Symptom**: After a switch reboot, OSPF is stuck in the INIT state.<br>**Scenario**: When a switch that is configured with OSPF, but ip router-id has not been configured, is rebooted OSPF remains in the INIT state.<br>**Workaround**: Configure the router ID manually. | OSPF |
| 16.10.0001 | 250958 | KB | **Symptom**: The hit counters in the output of the show statistics policy command shows all zeros.<br>**Scenario**: If a QoS policy with several class entries across all ports on multiple modules has been applied, the output of the show statistics policy command shows all zeros in the hit counters. | QoS |
| 16.10.0001 | 251017 | KB | **Symptom**: The event log displays `lpAddrMgr: Failed to add FIB entry - neighbor matches existing route (vrf:0 A.B.C.D/32)..`<br>**Scenario**: When the switch has been configured with a VRRP master and the connected routes are redistributed using routing protocols, the event log will display a lpAddrMgr message. | VRRP |
| 16.10.0001 | 251203 | KB | **Symptom**: Pings to the VRRP virtual IP address fail.<br>**Scenario**: If a switch module is reloaded, added, or hot-swapped, if a VSF stack member joins the stack after a stack split event or after a switch reboot with expansion module present, the switch fails to respond to ping packets to the VRRP virtual IP address. | VRRP |
| 16.10.0001 | 250489 | KB | **Symptom**: High utilization of a VSF link is reported by the switch.<br>**Scenario**: When VSF is configured with one link having multiple ports and then a VSF link port toggle is performed by disabling then re-enabling the VSF interface, the switch reports a high link utilization. | VSF |
| 16.10.0001 | 250754 | KB | **Symptom**: The switch cannot be found in Aruba Central even though the CLI reports the switch as being connected.<br>**Scenario**: When a VSF stack is already checked into Aruba Central with the same stack ID as another VSF stack, switches in the stack cannot be found in Aruba Central.<br>**Workaround**: Ensure all switches are running 16.06 or later and then form the VSF stack. | VSF |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0001 | 245830 | KB | **Symptom**: The switch fails to list the switch ports in the Ports web management page.<br>**Scenario**: When a peer device that advertises information in LLDP has a sysName string with special characters, the switch fails to display the port list table on the Ports web management page.<br>**Workaround**: Remove the special characters from the peer device sysName or use CLI commands to get specific port information. | Web UI |

# Issues and Workarounds

The following are known open issues with this branch of the software.

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.

**Table 6:** *Known Issues*

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0016 | 255646 | KB | **Symptom**: The `show statistics aclv4 <ACL-NAME-STR> vlan <VLAN-ID> out` command displays lesser `HitCounts for ACL` for deny rule.<br>**Scenario**: The routed traffic is denied even before the egress Access control list (ACL) when the ACL contains a deny rule, and it is applied in the VLAN egress direction. | ACL |
| 16.08.009 | 247648 | KB | **Symptom**: The switch fails to bypass authentication for random devices.<br>**Scenario**: When the CDP/LLDP bypass is enabled on a switch configured in VSF, the switch fails to bypass authentication for random devices after a redundancy switchover event.<br>**Workaround**: Disable and re-enable the affected port to re-enforce CDP/LLDP bypass on the port. | CDP/LLDP Bypass |

# Upgrade Information

## Upgrading Restrictions and Guidelines

KB.16.10.0009 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.16.10 branch of the software.
Version WC.16.10.0001 is the initial build of Major version WC.16.10 software. WC.16.10.0020 includes all enhancements and fixes in the WC.16.10.0019 software, plus the additional enhancements and fixes in the WC.16.10.0020 enhancements and fixes sections of this release note.

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

**Table 7:** *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 |
| JL557A | Aruba 2930F 48G PoE+ 4SFP 740W Switch |
| JL558A | Aruba 2930F 48G PoE+ 4SFP+ 740W Switch |

| Product number | Description |
|---|---|
| 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 8:** *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 |
| 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 |

| Product number | Product name | Minimum software version |
|---|---|---|
| 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 9:** *Enhancements*

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0020 | WC | OSPF Route Filtering feature provides an option to filter the intra-area routes from installing into local FIB table.<br>By using this, operator can create `distribute-list` with one or more network addresses which will be used to filter the intra area routes in OSPFv2/OSPFv3.<br>**Syntax:**<br>OSPFv2: `distribute-list <IP-ADDR>/<Prefix-Len>`<br>OSPFv3: `distribute-list <IPV6-ADDR>/<Prefix-Len>`<br>Refer to the *Aruba 3810/5400R Multicasting and Routing Guide for AOS-S Switch 16.11* and *Aruba 3810/5400R IPv6 Configuration Guide for AOS-S Switch 16.11* for more information. | OSPF/OSPFv3 |
| 16.10.0020 | WC | Added support in Device fingerprinting (DFP) module to send protocol data to Aruba Central for telemetry.<br>Added `options-list` parameter to device-fingerprinting CLI. Switch software is enhanced to collect DHCP options list and up to three instances of HTTP user agent headers.<br>**Syntax:** `device-fingerprinting [policy]<PROFILE_NAME> dhcp [option-num <NUM> \| options-list].`<br>Refer to the *Aruba 3810/5400R Access Security Guide for AOS-S Switch 16.11* for more information. | Device Finger Printing |
| 16.10.0019 | WC | No enhancements were included in version 16.10.0019. | NA |

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0018 | WC | The Enrollment over Secured Transport (EST) client feature is updated to download and renew the CA certificates from an EST server independent of application certificate enrollment. A new command `est-server <profile-name> cacerts-download` is added to enable independent CA certificate download from the EST server. This enhancement initiates automatic CA certificate download and renewal when the existing TA profile is about to expire. The switch will use the existing `est-server <profile-name> re-enrollment-prior-expiry` command to determine how many days in advance the renewal is to be done. A MIB has also been added to enable automatic download and renew of the CA certificates from the EST server.<br>Refer to the *Aruba 2930M/2930F Access Security Guide for AOS-S Switch 16.10* and *Aruba MIB and Trap Support Matrix for AOS-S Switch 16.10* for more information. | EST |
| 16.10.0017 | 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.<br>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.<br>A MIB has also been added to enable or disable the randomization of TCP timestamp offsets.<br>Refer to the *Aruba 2930F/2930M Management and Configuration Guide for AOS-S Switch 16.10* and *Aruba MIB and Trap Support Matrix for AOS-S Switch 16.10* for more information. | Security |
| 16.10.0017 | 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.<br>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.<br>A MIB has also been added to enable User-Based Tunneling Wake-on-LAN (WoL) on the specified VLANs. | Support for Silent Device |

| Version | Software | Description | Category |
|---|---|---|---|
| | | Refer to the *Aruba 2930F/2930M Management and Configuration Guide for AOS-S Switch 16.10* and *Aruba MIB and Trap Support Matrix for AOS-S Switch 16.10* for more information. | |
| 16.10.0016 | WC | Added support for the new SSH data integrity algorithm hmac-sha2-256, which is defined in RFC 6668.<br>Refer to the *Aruba 2930M/2930F Access Security Guide for AOS-S Switch 16.10* and *Aruba 2930M/2930F IPv6 Configuration Guide for AOS-S Switch 16.10* for more information. | SSH |
| 16.10.0016 | WC | Added support to configure the size of the EAP-TLS fragments sent from the switch to the RADIUS server. Configuring EAP-TLS fragment size based on the MTU of the network avoids IP fragmentation in the network, and thus, the fragmented packets will not be dropped by the firewall or gateways.<br>Added a MIB to indicate the maximum size of the EAP-TLS fragment sent to the RADIUS server.<br>Refer to the *Aruba 2930M/2930F Access Security Guide for AOS-S Switch 16.10* and *Aruba MIB and Trap Support Matrix for AOS-S Switch 16.10* for more information. | EAP-TLS Fragmentation |
| 16.10.0015 | WC | No enhancements were included in version 16.10.0015. | NA |
| 16.10.0014 | WC | No enhancements were included in version 16.10.0014. | NA |
| 16.10.0013 | WC | Added support to enable force-2-pair mode. This feature protects the Powered Devices (PD) from hardware failure by delivering power over 2-pairs of a 4-pair Ethernet cable.<br>Added RMON to indicate the force-2-pair mode is configured and enabled on a port.<br>**Syntax:** `power-over-ethernet force-2pair-mode ports <port-list>`<br>Refer to the *Aruba 2930M/2930F Management and Configuration Guide for AOS-S Switch 16.10* and *Aruba Event Log Message Reference Guide for AOS-S Switch 16.10* for more information. | Enhancement for power delivery and RMON Logging |
| 16.10.0013 | WC | Added support to user roles to establish user-based tunneling to tunnel voice and data traffic selectively and authenticate critical role user in the event of RADIUS server unavailability.<br>Refer to the *Aruba 2930M/2930F Access Security Guide for AOS-S Switch 16.10* and the *Aruba 2930M/2930F Management and Configuration Guide for AOS-S Switch 16.10* for more information. | Enhancement in traffic tunneling and critical-role authentication |
| 16.10.0013 | WC | Added MIBs to display the count of total and operational members in a VSF and BPS stack. Refer to the *Aruba MIB and Trap Support Matrix for AOS-S Switch 16.10* for more information. | Back Plane Stacking (BPS) and Virtual Switch Framework (VSF) |

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0012 | WC | Added `concise` parameter to display port-access and spanning-tree attributes in a consolidated format, when executing `show config` and `show running-config` commands. | Enhancement for `show config` and `show running-config` commands |
| 16.10.0012 | WC | Added support to enable SNMP traps for a specified event. This helps to filter out particular traps from all SNMP trap messages.<br>**Syntax:** `snmp-server enable traps event-list <EVENT-LIST-STR>` | Customization for SNMP Traps |
| 16.10.0012 | WC | Added support to maintain the current role of the User-Based Tunneling client in the switch instead of de-authenticating the client during controller maintenance. The client traffic flow is resumed at the switch ingress port when the controller is reachable.<br>**NOTE:** The client is de-authenticated when the controller is not available even after the configured maintenance period. | Enhancement for `tunneled-node-server` command |
| 16.10.0012 | WC | Added `recv-disable` parameter to configure loop-protect from blocking the receiving port when a loop is detected.<br>**Syntax:** `no loop-protect <PORT-LIST> receiver-action [recv-disable]` | Configuration for loop-protect receiver-action |
| 16.10.0011 | WC | Improved performance when executing `show config` command. | Performance improvements for `show config` command |
| 16.10.0011 | WC | Added support to format MAC address in upper case for the Called and Calling Station IDs.<br>Refer to the *Access Security Guide* for more information. | Port Access Enhancement |
| 16.10.0011 | WC | Added support to include the Port VLAN information in RADIUS access request for all authentication types.<br>Refer to the *Access Security Guide* for more information. | Port Access Enhancement |
| 16.10.0011 | WC | Added support to enable AES 256-bit encryption for SNMP.<br>Refer to the *Management and Configuration Guide* for more information. | AES 256-bit encryption for SNMP |
| 16.10.0011 | WC | Added support to configure a prefix string along with the switch IP address or hostname in the logs sent to the Syslog servers. This helps to classify and group log entries based on the string value.<br>**Syntax:** `logging prefix <ASCII-STR>`<br>Refer to the *Management and Configuration Guide* for more information. | Syslog Enhancement |

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0011 | WC | Added support to schedule a stack or chassis reboot.<br>**Syntax:** `reload <after\|at> [system]`<br>Refer to the *Management and Configuration Guide* for more information. | Stacking Enhancement |
| 16.10.0010 | WC | Added support to provide the option to specify the source interface or VLAN for Central connectivity. The existing IP source-interface command is enhanced to override current configuration check for provisioning using Aruba Activate.<br>Refer to the *Management and Configuration Guide* for more information. | Source interface option for Central connectivity |
| 16.10.0010 | WC | Added support to allow more PoE devices to be connected to the switch by using `poe-alloc-by-usage` when using Device Profiles. This can be based on either **Usage** or **Class**. Default allocation will be based on **Class**.<br>Refer to the *Management and Configuration Guide* for more information. | Device Profile Enhancement |
| 16.10.0010 | WC | Added support for FQDN (only IPv4) while configuring TACACS server along with the existing support of IP address.<br>Refer to the *Access Security Guide* for more information. | TACACS Option |
| 16.10.0010 | WC | Added support to work with the default setting in OpenSSH 8.2 by choosing an inherently more secure algorithm as the default on the switch for SSH communication. Refer to the *Access Security Guide* for more information.<br>The list of new Host-Key algorithms are as follows:<br>■ rsa-sha2-512<br>■ rsa-sha2-256<br>The list of new SSH KEX algorithms are as follows:<br>■ ecdh-sha2-nistp521<br>■ ecdh-sha2-nistp381<br>■ ecdh-sha2-nistp256<br>■ diffie-hellman-group-exchange-sha256 | Support for OpenSSH 8.2 |
| 16.10.0010 | WC | Improved performance when displaying large configurations. | Performance improvements for `show running-config` command |
| 16.10.0010 | WC | Added RMON logging for the failure events in SSH, Web UI, Syslog over TLS sessions, and x509 certificate processing.<br>Refer to the *Event Log Message Reference Guide* for more information. | RMON Logging |

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0009 | WC | Added support for the manager password enforcement to ensure that the switch prompts the user to configure the manager password on the switch before configuring any other features. If the manager password is not configured, then the user will have read-only access to the switch. This is applicable only to switches with factory default configuration.<br>Refer to the *Access Security Guide* for more information. | Manager Password Enforcement |
| 16.10.0009 | WC | Added support to enhance the payload size for the REST API interfaces. The increased payload size for 2930F\M platforms is 1024K.<br>Refer to the *REST API Guide* for more information. | REST API Payload Enhancement |
| 16.10.0009 | WC | Added support for Server Name Indication (SNI), which is a TLS extension defined in RFC 6066. This feature is enabled by default to include the SNI extension in the Client Hello sent from the switch to all the TLS client applications.<br>Refer to the *Access Security Guide* for more information. | Server Name Indication for TLS |
| 16.10.0008 | WC | Version 16.10.0008 was never released. | NA |
| 16.10.0007 | WC | ■ Added additional support for pipe "\|" option to grep for pattern match the output of CLI commands, such as:<br>◦ Case-insensitive option to allow a case insensitive pattern match<br>◦ Up to four consecutive pattern matches in one CLI command<br>■ Added support for a per-session based command to wrap column display in the CLI output using session wrap-text option when its length is exceeding the column width.<br>Refer to the *Management and Configuration Guide* for more information. | CLI |
| 16.10.0007 | WC | Added the following REST enhancements:<br>■ Support for ARP table data.<br>■ Support for downloadable user-roles configuration.<br>■ Support for primary VLAN.<br>■ Support for reserved-vlan and clearpass options to configure dynamic segmentation.<br>■ REST API schema moved under device-rest-api/services/server.html.<br>Refer to the *REST API Guide* for more information. | REST |
| 16.10.0007 | WC | Added support for the following 1G and 10G TAA transceivers:<br>■ JL745A - Aruba 1G SFP LC SX 500m MMF TAA XCVR<br>■ JL746A - Aruba 1G SFP LC LX 10km SMF TAA XCVR<br>■ JL747A - Aruba 1G SFP RJ45 T 100m Cat5e TAA XCVR<br>■ JL748A - Aruba 10G SFP+ LC SR 300m MMF TAA XCVR | Transceivers |

| Version | Software | Description | Category |
|---|---|---|---|
| | | ■ JL749A - Aruba 10G SFP+ LC LR 10km SMF TAA XCVR | |
| 16.10.0007 | WC | Added support for the new activate endpoint devices-v2.arubanetworks.com which has the following two major differences compared to the old endpoint device.arubanetworks.com:<br>■ It works on the standard TLS handshake mechanism and uses mutual authentication.<br>■ It uses certificates issued by HP CA for establishing TLS connections.<br>Zero Touch Provisioning (ZTP) improvements were made to deal with situations such as unresponsive DNS servers. Refer to the *Management and Configuration Guide* for more information. | Zero Touch Provisioning |
| 16.10.0006 | WC | Version 16.10.0006 was never released. | NA |
| 16.10.0005 | WC | No enhancements were included in version 16.10.0005. | NA |
| 16.10.0004 | WC | Version 16.10.0004 was never released. | NA |
| 16.10.0003 | WC | New command aaa accounting session-id include-switch-identity was added. When this command is invoked, an accounting session ID is generated with Switch Base MAC, Client MAC, and Timestamp for network accounting type. The other accounting types (exec, system, commands) do not include Client MAC and hence the session ID is generated with Switch Base MAC, Track ID, and Timestamp.<br>If the same client is accessing the network from multiple switches, then the accounting session ID can be duplicated. This caused issues in Clearpass where client insertion in the database failed with an error similar to Integrity Error: acct_id, calling_station_id violates check constraint. This new command alleviates that problem. | AAA |
| 16.10.0003 | WC | Extended the device identify capability by just matching based on the attribute MAC OUI to the Sys name and Sys description attributes. | Device profile |
| 16.10.0003 | WC | This enhancement will only be in effect if the CoA/Disconnect request has a message authenticator attribute in request packet. The message authenticator attribute is used to verify the integrity (HMAC-MD5) of the RADIUS packet. This is an optional attribute in the Access/CoA/Disconnect packet. If the received packet has this attribute in the RADIUS packet, the receiver will validate the integrity value and discard it if the value is incorrect. | RADIUS |
| 16.10.0002 | WC | An event is added to the log when the switch experiences an over temperature condition. | Event Log |
| 16.10.0001 | WC | Added support for JL693A, Aruba 2930F 12G PoE+ 2G/2SFP+ Switch. | Hardware |

# 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 10:** *Fixed Issues*

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0020 | 256274 | WC | **Symptom/Scenario**: VSF Stack Member crashed with a message similar to the following: `Software exception at lava_chassis_slot_sm.c:3626 - in 'eChassMgr', task ID = 0x37b07bc0.` | VSF |
| 16.10.0020 | 256257 | WC | **Symptom/Scenario**: Certain transceivers had link issues in unsupported transceiver mode. | Transceivers |
| 16.10.0020 | 256234 | WC | **Symptom**: The `show rmon statistics <port no>` command returns the wrong counter values. **Scenario**: This issue occurred when the command `clear statistics global` or `clear statistics <port no>` was first executed and then `show rmon statistics <port no>`. | CLI |
| 16.10.0020 | 256233 | WC | **Symptom**: Client ports may encounter packet drops when multicast sources stream video over 500 Mbps. **Scenario**: This issue can occur when multiple clients from different ports subscribed to the same group, which streams using HD channels requiring high bandwidth. TX drops can occur when several clients change channels simultaneously. **Workaround**: Lower the bandwidth of the video streams to below 500 Mbps in order to avoid over-subscription of ports. | IGMP-NG |
| 16.10.0020 | 256220 | WC | **Symptom**: Missing OSPF routes. **Scenario**: This issue occurred when both userbased tunneling and OSPF are configured and either of the uplinks to the controller is down.<br><br>**NOTE:** `source-interface` to be configured for tunneled node when the switch has more than one vlan to the reach the controller. | OSPFv2 |
| 16.10.0020 | 256205 | WC | **Symptom**: A configuration template push from Aruba Central fails. | Central Integration |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue occurred when the end devices are connected to ports that are configured with `port-security learn-mode static`. | |
| 16.10.0020 | 256167 | WC | **Symptom**: Ports with per-port tunneled node (PPTN) configured might be disabled after a switch reboot.<br>**Scenario**: This issue occurred when a device profile was configured with tunneled-node.<br>**Workaround**: Disable and enable the problematic PPTN enabled port manually. | Tunneled Node |
| 16.10.0019 | 256115 | WC | **Symptom**: Although the switch does not react to pings or SSH commands, it continues to transit traffic. The event log contains a crash message.<br>**Scenario**: This issue occurred when device fingerprinting was configured with DHCP protocol. | CPPM |
| 16.10.0019 | 256200 | WC | **Symptom**: Per-port tunneled node (PPTN) disables the port for one second as part of tunnel deletion.<br>**Scenario**: This issue occurred when the device-profile application with tunneled-node was disabled on a PPTN enabled port.<br>**Workaround**: Disable and enable the problematic PPTN enabled port manually. | Tunneled Node |
| 16.10.0019 | 256121 | WC | **Symptom**: Web authentication fails when the switch is managed by Aruba Central (`aruba-central support-mode disable`).<br>**Scenario**: This issue occurred when the switch was connected to Aruba Central and `aruba-central support-mode` was disabled.<br>**Workaround**: Execute `aruba-central support-mode enable` command so the switch is longer managed by Aruba Central. | Web Authentication |
| 16.10.0018 | 256037 | WC | **Symptom/Scenario**: Clients are not authenticated on a switch port.<br>**Scenario**: This issue occurred when multiple clients were connected to a single port (for example, a Personal Computer (PC) was connected to a phone), both MAC authentication and 802.1X authentication methods were attempted at the same time on the PC, and both the authentication methods used the same user role attribute.<br>**Workaround**: Configure the `auth-order` parameter first with `authenticator`, and then with `mac-based`. | 802.1X |
| 16.10.0018 | 255928 | WC | **Symptom/Scenario**: A switch is unable to connect to Aruba Central. | Aruba Central |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0018 | 255940 | WC | **Symptom**: A switch crashes with a message similar to the following:<br>`Software exception at svc_misc.c:1088 - in 'mDHCPClint'`<br>`-> Failed to malloc 9202 bytes.`<br>**Scenario**: This issue occurred when the switch attempted to reconnect to Aruba Central. | Aruba Central |
| 16.10.0018 | 255978 | WC | **Symptom**: A switch crashes with a message similar to the following:<br>`Software exception in ISR at pvDmaV1Rx.c`<br>`-> ASSERT: No resources available!.`<br>**Scenario**: This issue occurred when 802.1X and MAC authentication were enabled on the same port with auth-order, and the client was initially authenticated through MAC authentication with a user role having the `port mode` attribute. | Authentication |
| 16.10.0018 | 255995 | WC | **Symptom**: A switch crashes when the `show port-access clients` command is issued or when an `SNMP GET` operation is performed to get the MIB object `hpicfUsrAuthMacAuthSessionStatsEntry`.<br>**Scenario**: The switch crashed when a MAC-authenticated client had a username of more than 40 characters. | Authentication |
| 16.10.0018 | 254566 | WC | **Symptom**: Traffic fails to pass through an IEEE 802.1ad tunnel.<br>**Scenario**: This issue occurred because of the following reasons:<br>1. A Small Form-factor Pluggable+ (SFP+) port was configured as an uplink.<br>2. IEEE 802.1ad was configured on the same port.<br>3. The switch was rebooted without a transceiver in the slot.<br>4. A 1G SFP transceiver was inserted during the runtime.<br>**Workaround**: Insert the 1G SFP transceiver, and then reboot the switch. | IEEE 802.1ad |
| 16.10.0018 | 256016 | WC | **Symptom**: When a private VLAN is configured on a switch, the traffic from the secondary VLAN does not reach the primary VLAN. | Private VLAN |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue occurred when the switch was rebooted, and the secondary VLAN contained a tagged trunk or Link Aggregation Control Protocol (LACP) port.<br>**Workaround**: Remove and add the tagged trunk or LACP configuration to the secondary VLAN. | |
| 16.10.0018 | 256034 | WC | **Symptom**: SNMP MIB files are not reachable, and the MIB file returns some errors.<br>**Scenario**: This issue occurred when the customer used an SNMP monitoring tool to read or parse the MIB files. | SNMP |
| 16.10.0018 | 256050 | WC | **Symptom**: A switch crashes when the **WebUI Security > Clientspage** is accessed.<br>**Scenario**: The switch crashed when a MAC-authenticated client had a username of more than 40 characters. | Web UI |
| 16.10.0017 | 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 |
| 16.10.0017 | 255882 | WC | **Symptom**: When a switch fails to connect to Aruba Central, the switch configuration rolls back.<br>**Scenario**: This issue occurred when the connection between the switch and Aruba Central was lost. | Aruba Central |
| 16.10.0017 | 255762 | WC | **Symptom/Scenario**: A switch crashes with the following message:<br>`OMFP LPTR Err Status = 0x00000310 (DEC_ERR_CNT).` | Chassis |
| 16.10.0017 | 255713 | WC | **Symptom**: Some devices that are connected to a switch become unreachable.<br>**Scenario**: This issue occurred because of the following reasons:<br>1. The switch was running Multiple Spanning Tree Protocol (MSTP).<br>2. A large number of ports were MAC-authenticated.<br>3. Topology Change Notification (TCN) events occurred, which caused the authentication to block or unblock the port without the port flap.<br>**Workaround**: Disable and enable the ports. | Chassis Manager |
| 16.10.0017 | 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.<br>`Invalid input: grep usage error` | Configuration |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **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.<br>**Workaround**: Do not use the pipe character (\|) in the command input for the configuration commands. | |
| 16.10.0017 | 255908 | WC | **Symptom/Scenario**: A new multicast stream is initially broadcast on a VLAN even when no IGMP join is sent. | IGMP |
| 16.10.0017 | 255195 | WC | **Symptom**: The switch memory utilization spikes and might reach to 100%.<br>**Scenario**: This issue occurred when many ports were monitored and mirrored to one port.<br>**Workaround**: Disable mirroring on the ports. | Mirroring |
| 16.10.0017 | 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 |
| 16.10.0017 | 255827 | WC | **Symptom/Scenario**: A switch crashes with the following message:<br>`Health Monitor: Invalid Instr Misaligned Mem Access .... Task='InetServer'.` | System |
| 16.10.0017 | 254817 | WC | **Symptom**: When the Virtual Switch Framework (VSF) stack is pinged and the commander switch is rebooted, a temporary ping loss of 20 to 30 seconds is observed in Aruba 2930F switch series.<br>**Scenario**: This issue occurred when J9054C transceivers were used, and the commander switch of a 2 member VSF stack was rebooted. | Transceivers |
| 16.10.0017 | 255760 | WC | **Symptom/Scenario**: A switch crashes with the following message:<br>`Software exception at bsp_interrupts.c:90 - in 'fault_handler'` | Tunneled Node |
| 16.10.0016 | 255682 | WC | **Symptom**: The RADIUS accounting packets sent from the switch to the RADIUS server do not contain the correct client IP address.<br>**Scenario**: This issue occurred when both user authentication and MAC authentication were configured. | 802.1X |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0016 | 255400 | WC | **Symptom**: The switch is unable to connect to Activate or Aruba Central.<br>**Scenario**: This issue occurred when the `show crypto pki ta-profile` command displayed `Pending Root Certificate In...` for the `GEOTRUST_CA` profile, and the following event was recorded in the event log:<br>`05222 activate: ST1-CMDR: Error connecting to the Activate server: Activate TLS connection error.` | Activate |
| 16.10.0016 | 255653 | WC | **Symptom**: The switch crashes with a Non-Maskable Interrupt (NMI) event.<br>**Scenario**: The switch crashed because of the following reasons:<br>1. The switch was configured to receive a DHCP address.<br>2. The `activate provision force` command was configured on the switch.<br>3. The `no activate software-update check` command was executed. | Activate |
| 16.10.0016 | 255554 | WC | **Symptom/Scenario**: When the switch is powered on for the first time and ZTP is initiated, the switch does not come online in Aruba Central.<br>**Workaround**: Reboot the switch or execute the `reset saved-configuration` command. | Central |
| 16.10.0016 | 255672 | WC | **Symptom/Scenario**: A configuration push from Aruba Central fails when the configuration contains the `crypto pki enroll-est-certificate` command.<br>**Workaround**: Add a valid value for `Enter Country (C)` field in the `subject fields` of the `crypto pki enroll-est-certificate` command. | Central |
| 16.10.0016 | 255697 | WC | **Symptom**: The switch crashes with the following message:<br>`Software exception in ISR at btmDmaApi.c:650 -> ASSERT: No resources available!.`<br>**Scenario**: This issue occurred when there was a repeated hardware fault in one of the power supplies. | Chassis Manager |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0016 | 255570 | WC | **Symptom/Scenario**: The `Rx Errors` counter in the `show interfaces` command output is not cleared when the `clear statistics global` command is executed. | CLI |
| 16.10.0016 | 255719 | WC | **Symptom**: The IP address of the next server is not present in the DHCP response packet.<br>**Scenario**: This issue occurred when the DHCP server with option 66 and option 150 was configured in the server pool. | DHCP Server |
| 16.10.0016 | 255417 | WC | **Symptom**: The switch crashes with an NMI event.<br>**Scenario**: This issue occurred when the DHCP snooping traffic was sent continuously to the switch with DHCP option 82, and the DHCP clients rebooted frequently. | DHCP Snooping |
| 16.10.0016 | 255552 | WC | **Symptom/Scenario**: Mirrored egress packets are tagged even though the `no-tag-added` option is configured.<br>**Workaround**: Reapply the existing monitor configuration after removing the configuration using the `no monitor all both mirror 1` command. | Port Mirroring |
| 16.10.0016 | 255638 | WC | **Symptom**: Some PBT clients experience traffic loss.<br>**Scenario**: This issue occurred when both VRRP and PBT were configured on the switch, and a VRRP failover event was recorded.<br>**Workaround**: Disable and enable PBT on the switch. | Tunneled Node |
| 16.10.0016 | 255586 | WC | **Symptom**: Running configuration does not display the local user roles.<br>**Scenario**: The issue occurred when the switch was configured to use both downloadable and local user roles.<br>**Workaround**: Reboot the switch. | User Roles |
| 16.10.0016 | 255619 | WC | **Symptom**: The Ports table on the Web UI does not display all the interfaces of the switch.<br>**Scenario**: This issue occurred when the Name and Id sent through LLDP contained a trailing backslash (\), and the same was configured on the port.<br>**Workaround**: Disable LLDP on the switch using the `no lldp run` command. | Web UI |
| 16.10.0015 | 255124 | WC | **Symptom**: Captive portal redirection does not work.<br>**Scenario**: This issue occurred when the `ip client-tracker` command was enabled, and the VLAN where the client onboarded had the `disable layer3` command configured. | Captive Portal |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Workaround**: Remove `ip client-tracker` or `disable layer3` configuration from the client VLAN. | |
| 16.10.0015 | 255259 | WC | **Symptom/Scenario**: Executing the `show tech all` command resets the port counters in all sessions. | CLI |
| 16.10.0015 | 255134 | WC | **Symptom**: Switch crashes regularly with the following message:<br>`Active/Commander system went down:eSoftware exception at msgSys.c:641 -- in 'mNSR',`<br>`-> Can't get message buffer for msgSys_recv.`<br>The event log indicates continuous removal and application of the device-profile.<br>**Scenario**: This issue occurred with a device profile for an AP enabled, with both interfaces of the AP connected to the switch through a trunk, and when the switch was rebooted.<br>**Workaround**: Disable and enable the device profile. | Device Profile |
| 16.10.0015 | 255158 | WC | **Symptom**: Multicast traffic with the source IP address 0.0.0.0 floods to all ports, even with IGMP snooping enabled.<br>**Scenario**: This issue occurred when the multicast traffic was sent with a NULL IP source from a device connected to a non-querier device. | IGMP |
| 16.10.0015 | 255408 | WC | **Symptom**: Unauthorized clients can connect and access the switch using the loopback address.<br>**Scenario**: This issue occurred when the `ip authorized-managers` command was configured and an unauthorized client attempted to connect to the loopback address. | IP Authorized Managers |
| 16.10.0015 | 255464 | WC | **Symptom/Scenario**: A Quality of Service (QoS) policy, which has a space character in the name, cannot be removed from an interface or VLAN. | Policy Map |
| 16.10.0015 | 255430 | WC | **Symptom**: When the `show radius` command is executed, the output shows the RadSec server as a Dead server.<br>**Scenario**: This issue occurred because of the following reason:<br>1. When the `radius-server dead-time`, `aaa authentication` and `aaa accounting` commands were configured. | RADIUS |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | 2. Accounting was disabled on the RADIUS server and a RadSec connection was established.<br>3. When an SSH session was established and commands were executed from that session. | |
| 16.10.0015 | 255342 | WC | **Symptom**: When an initial role is applied, clients do not attempt to reauthenticate.<br>**Scenario**: This issue occurred when the server-timeout value was less than the RADIUS request timeout.<br>**Workaround**: Configure a greater server-timeout value than the RADIUS request timeout. | RADIUS |
| 16.10.0015 | 255171 | WC | **Symptom**: The switch CPU spikes and the ClearPass RADIUS server shuts down.<br>**Scenario**: This issue occurred when MAC authentication used the peap-mschapv2 authentication method. As a result, Access-Request and Access-challenge messages were exchanged in a loop. | RADIUS |
| 16.10.0015 | 255067 | WC | **Symptom**: Switch does not respond to Simple Network Management Protocol version 3 (SNMPv3) queries.<br>**Scenario**: This issue occurred when there was a wrong value in the boot counter. | SNMPv3 |
| 16.10.0014 | 255376 | WC | **Symptom/Scenario**: Traffic loss is observed in Port-Based Tunneling (PBT) and controller Virtual Router Redundancy Protocol (VRRP) topology.<br>**Workaround**: Disable and enable PBT on the switch. | Tunneled Node |
| 16.10.0013 | 255031 | WC | **Symptom**: Switch loses connectivity to Aruba Central after a template is pushed.<br>**Scenario**: This issue occurred when a template with netdestination commands were pushed to the switch.<br>**Workaround**: Add `aruba-central url` to the template that is applied. | Central |
| 16.10.0013 | 254985 | WC | **Symptom**: End devices (example, printer) become unreachable when they do not send or receive much traffic.<br>**Scenario**: This issue occurred when the switch stack was not rebooted after a new member was added to the stack.<br>**Workaround**:<br>■ Reboot the switch stack after adding a new member.<br>■ Bounce the port connecting to the end device.<br>■ Configure the MAC age time to match the ARP | ARP |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | ageout time of the router. | |
| 16.10.0013 | 254974 | WC | **Symptom/Scenario**: When the OOBM port is a DHCP client, the DHCP server receives an incorrect MAC address from the switch. | OOBM |
| 16.10.0013 | 254922 | WC | **Symptom**: When the switch attempts to connect to Aruba Central, the switch stack reboots.<br>**Scenario**: This issue occurred when switch stack member 1 was in the `Missing` state and the switch stack attempted to connect to Aruba Central. | Central |
| 16.10.0013 | 254868 | WC | **Symptom**: When connection to the neighbor is lost, an incorrect OSPF route is removed from the routing table.<br>**Scenario**: This issue occurred when more than one point-to-point OSPF interface was configured with the same router.<br>**Workaround**: Configure broadcast OSPF interface instead of point-to-point OSPF interface. | OSPFv2 |
| 16.10.0013 | 255135 | WC | **Symptom**: A MACsec connection is not established on the last fixed or last flex port of the switch.<br>**Scenario**: This issue occurred because of the following reasons:<br>■ MACsec was enabled on the last fixed or last flex port of the switch.<br>■ There was an intermediate device that filtered packets with null MAC address.<br>**Workaround**: Connect the MACsec peer switches without any devices in between. | MACsec |
| 16.10.0013 | 255125 | WC | **Symptom**: Clients authenticated by Aruba Central are not placed in the proper VLAN.<br>**Scenario**: This issue occurred because of the following reasons:<br>■ Both MAC authentication and 802.1X are configured on the same port.<br>■ There are two clients on the port, which had a tagged membership for a VLAN, and the user role for a client had an untagged membership for the same VLAN. | Central |
| 16.10.0013 | 255123 | WC | **Symptom**: The following event did not identify the affected module correctly: `00907 IpAddrMgr: ST3-CMDR: Module p BMP TCAM parity recovery`.<br>**Scenario**: The following event was recorded in the event log when there was a hardware issue: `00907 IpAddrMgr: ST3-CMDR: Module p BMP TCAM parity recovery`. | RMON Logging |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0013 | 255115 | WC | **Symptom**: Some VoIP phones did not receive an IP address from the DHCP server.<br>**Scenario**: This issue occurred when user-based tunneling was configured on the port and DHCP snooping was enabled.<br>**Workaround**: Disable DHCP snooping. | DHCP Snooping |
| 16.10.0013 | 255062 | WC | **Symptom**: User-based tunnel (802.1X) is not established when MAC authentication is also configured on the port with a different VLAN assignment.<br>**Scenario**: This issue occurred when both MAC authentication and 802.1X were configured on a port, and the 802.1X authentication contained a VLAN change. | MAC Authentication |
| 16.10.0013 | 255058 | WC | **Symptom**: After a new template is applied to the switch, the switch is unable to connect to Aruba Central.<br>**Scenario**: This issue occurred because the primary VLAN on the switch was changed when the new template was applied.<br>**Workaround**: Reboot the switch. | Central |
| 16.10.0013 | 254976 | WC | **Symptom/Scenario**: The SSH, telnet, and console connections cannot be established with the switch, and the following event is recorded in the event log: `maximum user session limit reached.` | Switch Access |
| 16.10.0013 | 254966 | WC | **Symptom**: Applying a template from Aruba Central to a switch fails with the following reasons:<br>▪ `Failure Reason: Add and Remove commands have been failed`<br>▪ `Reason: Invalid netdestination entry.`<br>**Scenario**: This issue occurred when the template contained changes to the host configurations of the netdestination entries, which are used in an ACL. | Central |
| 16.10.0013 | 254958 | WC | **Symptom**: After the transition of 802.1X machine authentication to user authentication with User-Based Tunnel, the client username in the show command in the controller is not updated.<br>**Scenario**: This issue occurred when 802.1X with User-Based Tunneling was established and then the transition of machine authentication to user authentication was done. | Tunneled Node |
| 16.10.0013 | 254893 | WC | **Symptom/Scenario**: The switch crashes due to an MSTP NMI event. | Spanning Tree |
| 16.10.0013 | 254797 | WC | **Symptom**: The following event is recorded in the event file: `Lease table is full, DHCP lease was not added.` | DHCP Snooping |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue occurred when DHCP snooping was configured. | |
| 16.10.0013 | 254786 | WC | **Symptom**: SSH fails to connect to the switch.<br>**Scenario**: This issue occurred because of the following reasons:<br>■ More than one RADIUS server was configured.<br>■ `aaa authentication ssh enable` was configured to use the other RADIUS server, instead of using the first one in the configuration. | AAA Authentication |
| 16.10.0013 | 254780 | WC | **Symptom**: When more number of MAC authentication clients (auth method: peap-mschapv2) get authenticated or reauthenticated, the following event is recorded multiple times in the event log: `PEAP SSL socket connection limit reached`.<br>**Scenario**: This issue occurred when more than 20 clients were authenticated or reauthenticated at the same time.<br>**Workaround**: Authenticate or reauthenticate less than 20 clients at the same time. | MAC Authentication |
| 16.10.0013 | 254481 | WC | **Symptom**: The switch CPU utilization increases to 80% or more, and CDP packet looping is observed across VLANs.<br>**Scenario**: This issue occurred when CDP pass-through was configured on two switches, which had more than one connection between them.<br>**Workaround**: Use `no cdp run` command to disable CDP globally, instead of configuring CDP mode pass-through. | CDP |
| 16.10.0012 | 254360 | WC | **Symptom**: A configuration push using the `cfg-restore` command from Aruba Central fails.<br>**Scenario**: This issue occurred when a switch configuration, containing `radius server host` commands, was pushed to Aruba Central or when the `cfg-restore` command was executed with the same `radius server host` configuration.<br>**Workaround**: Use the `copy tftp config` command to copy a configuration to the switch from Aruba Central, instead of the `cfg-restore` command for pushing a configuration. | Central |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0012 | 254198 | WC | **Symptom**: A switch or management module crashes with the following message: `Active/Commander system went down: ... Health Monitor: Invalid Instr Misaligned Mem Access.` **Scenario**: This issue occurred when the `copy command-output show tech all tftp <ip-address> <filename>` command was executed. **Workaround**: Do not execute the `copy command-output show tech all tftp <ip-address> <filename>` command. | Chassis |
| 16.10.0012 | 254096 | WC | **Symptom**: The `Rx Drop Bytes` parameter in the command output for `show interface queues <port>` displays very high values for the last few ports, even though these ports were down. **Scenario**: This issue occurred when the `show interface queues <port>` command was issued. | CLI |
| 16.10.0012 | 254278 | WC | **Symptom**: The switch crashes when the `show crypto client-public-key` command is issued. **Scenario**:This issue was observed when the `show crypto client-public-key` was issued when the `\t:` symbol was present in the client pub key file. **Workaround**: Remove `\t:` symbol from the client public key file content. | Crypto |
| 16.10.0012 | 254380 | WC | **Symptom**: The switch crashes with the following message: `Health Monitor: Read Error Restr Mem Access .... Task='mdevMntr'.` **Scenario**: This issue occurred when device-fingerprinting (DFP) was configured and DFP clients moved between ports. | Device Finger Printing |
| 16.10.0012 | 254760 | WC | **Symptom**: Removal of OSPF routes from the link-state database is delayed. **Scenario**: This issue occurred when the switch received a Link-State Advertisement (LSA) that advertised routes with max age configured to remove the routes from the database. | OSPFv2 |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0012 | 254395 | WC | **Symptom**: The switch does not send the configured NAS-ID while sending a request to the RADIUS server.<br>**Scenario**: This issue occurred for both login and enable when the switch was configured with a non-default `server-group nas-id` and `ssh` was configured with peap-mschapv2. | Radius |
| 16.10.0012 | 254403 | WC | **Symptom**: The HTTP GET for /system/status/power/supply returns an internal server error.<br>**Scenario**: This issue occurred when GET of /system/status/power/supply was executed when a stack member was down. | REST |
| 16.10.0012 | 254665 | WC | **Symptom**: REST connection fails when a Windows client makes an HTTP request.<br>**Scenario**: This issue occurred when a Windows client sent a REST HTTP request using PowerShell. | REST |
| 16.10.0012 | 254553 | WC | **Symptom**: The switch crashes with the following message: `Health Monitor: Read Error Restr Mem Access ... Task='eNtpTask'.`<br>**Scenario**: This issue occurred when NTP was configured including the `ntp unicast` command and once NTP was functioning, the `no ntp` command was executed. | NTP |
| 16.10.0012 | 254525 | WC | **Symptom**: The smartlink port stops forwarding VLAN traffic.<br>**Scenario**: This issue occurred when the:<br>■ The VLAN membership of a port was changed by removing it or adding it to any of the protected VLANs of the smartlink group.<br>■ STP was enabled and a non-default MSTP instance was created.<br>**Workaround**: Disable/enable the port. | Smartlinks |
| 16.10.0012 | 253623 | WC | **Symptom/Scenario**: When there is a change in backplane stacking, VSF topology, or removal of a power supply, no SNMP trap is sent. | SNMP |
| 16.10.0012 | 254722 | WC | **Symptom/Scenario**: When a user fails to login to the switch using SSH, no SNMP trap is sent. | SNMPv2 |
| 16.10.0012 | 254580 | WC | **Symptom/Scenario**: A switch no longer accepts SSH connections.<br>**Workaround**: Reboot the switch. | SSH |
| 16.10.0012 | 254393 | WC | **Symptom**: Event messages are not printed on the Syslog server. | Syslog |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue occurred when a syslog server was configured with the TCP option, `logging <IP-ADDR> tcp` and `ip source-interface syslog` was configured.<br>**Workaround**: Remove `ip source-interface syslog ...` from the config or reboot the switch after configuring syslog over TCP. | |
| 16.10.0012 | 254311 | WC | **Symptom**: Gradual memory depletion on a switch is observed.<br>**Scenario**: This issue occurred when the telnet sessions were closed abruptly.<br>**Workaround**: Disable the telnet server on the switch. | Telnet |
| 16.10.0011 | 253563 | WC | **Symptom**: The switch crashes with the following message: `Health Monitor: Misaligned Mem Access.`<br>**Scenario**: This issue occurred when any of the 802.1X clients' MAC address had a NULL value due to corruption, and the authenticator configuration on a switch port was disabled. | 802.1X |
| 16.10.0011 | 254333, 254339 | WC | **Symptom**: Switch crashes with a message similar to the following: `Software exception at trlock.c -- in 'InetServer'.`<br>**Scenario**: This issue occurred when the `show tech all` command was executed from Aruba Central.<br>**Workaround**: Execute the `show tech all` command through the switch CLI. | Central |
| 16.10.0011 | 254255 | WC | **Symptom**: Switch crashes with a message similar to the following: `Software exception at multMgmtUtil.c -- in 'mOobmCtrl'.`<br>**Scenario**: This issue occurred when continuous or frequent `cfg-restore` operations (with password or aaa authentication related configurations) were executed, and in parallel, the switch was accessed through local-authentication.<br>**Workaround**: Do not access the switch using local-authentication when `cfg-restore` operation is in progress. | Chassis |
| 16.10.0011 | 253472 | WC | **Symptom/Scenario**: The following event is recorded in the event log multiple times where `xx%` is an increasing value: `03008 system: Ports A,B packet buffer allocation has reached xx%.` | Chassis |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Workaround**: Reboot the switch. | |
| 16.10.0011 | 253803 | WC | **Symptom**: SSH connection (Remote Console) cannot be established from Aruba Central to the switch.<br>**Scenario**: This issue occurred when `ip authorized-managers` was configured on the switch and a Remote Console connection was attempted from Aruba Central.<br>**Workaround**: Add the following configuration to the switch:<br>`ip authorized-managers 127.0.0.1 255.255.255.254 access manager` | Console |
| 16.10.0011 | 254196 | WC | **Symptom**: Multicast traffic stops after a redundancy switchover.<br>**Scenario**: This issue occurred when the IGMP `query-max-response-time` was configured to be `128` seconds and a redundancy switchover was performed.<br>**Workaround**: Remove IGMP from the VLAN and reconfigure the `query-max-response-time` to the default value of `10` seconds. | IGMP |
| 16.10.0011 | 253853 | WC | **Symptom**: Continuous RADIUS access request packets are sent from the switch to the RADIUS server.<br>**Scenario**: This issue occurred when a MAC address limit was configured and a device was attempted to be authenticated beyond the configured limit. | MAC Authentication |
| 16.10.0011 | 253844 | WC | **Symptom**: Removal of OSPF link state prefix from the link state database is delayed.<br>**Scenario**: This issue occurred when the switch received an OSPF Link-State Advertisement (LSA) with `MaxAge` configured to `3600` from a neighbor, and there were multiple OSPF sessions to the same router. | OSPFv2 |
| 16.10.0011 | 254095 | WC | **Symptom/Scenario**: Some IP phones are not powered on when connected to the switch. | Power Over Ethernet |
| 16.10.0011 | 253965 | WC | **Symptom**: The switch closes the REST connection when the request is made from a Windows client.<br>**Scenario**: This issue occurred when a REST request was sent from PowerShell on a Windows client. | REST |
| 16.10.0011 | 253921 | WC | **Symptom**: MAC addresses are not learned on some ports and spanning tree shows the port in a `BLOCKED LISTEN` state. | Spanning Tree Protocol |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue occurred when the switch was configured to use RPVST.<br>**Workaround**: Reboot the switch. | |
| 16.10.0011 | 252721 | WC | **Symptom**: Attempts to SSH or telnet to the switch fail and the following message is displayed:<br>`Sorry, the maximum number of telnet sessions are active. Try again later.`<br>**Scenario**: This issue occurred when a vulnerability scan was run against the switch multiple times.<br>**Workaround**: Disable Telnet server. | Switch Access |
| 16.10.0011 | 254174 | WC | **Symptom**: The CPU utilization is elevated and the switch crashes with a `No msg buffer` message.<br>**Scenario**: This issue occurred when the switch was configured to use user-based tunnels (tunneled-node server). | Tunneling |
| 16.10.0011 | 253970 | WC | **Symptom**: Ports can be added to a trunk using the web interface even if those ports are configured with IGMP fastlearn.<br>**Scenario**: This issue occurred when IGMP fastlearn was configured on a few ports of the switch, and the switch was accessed through the web interface to add the IGMP fastlearn enabled ports to the trunk.<br>**Workaround**: Use the CLI to add ports to a trunk. | Web Interface |
| 16.10.0010 | 253775 | WC | **Symptom/Scenario**: Switch does not get provisioned to Activate. | Activate |
| 16.10.0010 | 253807 | WC | **Symptom**: Unsupported values are accepted as ACL numbers for both standard and extended ACLs when configuring ACLs from the REST interface (for example, Aruba Central). Once configured, these ACLs cannot be deleted using REST or the CLI.<br>**Scenario**: This issue occurred when the REST interface was used to configure an ACL with an unsupported value. | ACLs |
| 16.10.0010 | 253425 | WC | **Symptom**: The username sent for a successful MAC-authenticated client is the MAC address, rather than the username.<br>**Scenario**: This issue occurred when a client was authenticated using MAC authentication. | Authentication |
| 16.10.0010 | 250901 | WC | **Symptom**: Switch randomly loses connectivity to Activate and Aruba Central.<br>**Scenario**: This issue occurred when configuring the switch to connect to Aruba Central. | Central |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0010 | 253422 | WC | **Symptom**: When a `show` command is executed using `\| include <anyword> <anyword>` the following error message is displayed: `Invalid Input : grep usage error.`<br>**Scenario**: This issue occurred when a `show` command was executed using `\| include <anyword> <anyword>`.<br>**Workaround**: Execute the `show` command without `\| include <anyword> <anyword>`. | CLI |
| 16.10.0010 | 253485 | WC | **Symptom**: When more than 3000 VLANs are configured, executing the `show run` command takes one or two minutes to begin displaying output.<br>**Scenario**: This issue occurred when `show run` command was executed after configuring a minimum of 3000 VLANs. | CLI |
| 16.10.0010 | 253303 | WC | **Symptom**: Peer device does not get an IP address when the port it is connected to is configured using a device-profile.<br>**Scenario**: This issue occurred when a port is configured using device profile and a peer device is connected to it.<br>**Workaround**:Disable device-profile and manually configure the port. | Device Profile |
| 16.10.0010 | 253507 | WC | **Symptom**: Devices connected to the switch are unable to send or receive packets.<br>**Scenario**: This issue occurred when a multicast listener query was received with an unspecified source IP address.<br>**Workaround**: Stop sending malformed multicast listener query packets to the switch. | Multicast |
| 16.10.0010 | 253557 | WC | **Symptom**: Using REST to retrieve the resource identifier `/lldp/remote-device` fails to display the IPv4 address of the neighbor.<br>**Scenario**: This issue occurred when the REST resource operation GET was used to retrieve the data associated with `/lldp/remote-device`. | REST |
| 16.10.0010 | 252993 | WC | **Symptom**: Some RADIUS accounting packets sent to the RADIUS server have a very large size.<br>**Scenario**: This issue occurred when a downloadable user role was configured with a user policy, network accounting was enabled, and a client was authenticated. | RADIUS |
| 16.10.0010 | 253736 | WC | **Symptom**: Disconnect Change of Authorization (CoA) request is not honored. | RADIUS |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue occurred when the radius-server group was configured, a client was authenticated, and a disconnect CoA request with the default nas-id was sent.<br>**Workaround**: Configure `aaa server-group radius <Group name> nas-id <NAS-ID>` where the NAS-ID matches the NAS Identifier value shown in the output of the `show radius authentication` command. | |
| 16.10.0010 | 253789 | WC | **Symptom**: Switch serial number contains an extra space at the end when it is read using SNMP.<br>**Scenario**: This issue occurred when the switch serial number was read using SNMP.<br>Example:<br>MIB OID: 1.3.6.1.2.1.47.1.1.1.1.11.1<br>MIB File: ENTITY-MIB | SNMP |
| 16.10.0010 | 253342 | WC | **Symptom**: SSH/Telnet/Console connections to the switch fail with an error message: `Maximum session limit is reached`.<br>**Scenario**: This issue occurred when multiple users logged in and out and RADIUS was configured as the primary authentication method.<br>**Workaround**: Reboot the switch. | Switch Access |
| 16.10.0010 | 253407 | WC | **Symptom**: Unable to log in to the switch using TACACS credentials.<br>**Scenario**: This issue occurred when a source interface for TACACS was configured using the `ip source-interface tacacs` command and the switch was upgraded to 16.10.0009. | TACACS |
| 16.10.0010 | 253001 | WC | **Symptom**: When there are continuous link flaps on the link-to-monitor ports within a fraction of a second, some link-to-disable ports may not come up once the link-to-monitor port stabilizes.<br>**Scenario**: This issue occurred when the link-to-monitor port used a transceiver connected by fibre and flapped continuously at a high rate.<br>**Workaround**: Use Fault-Finder to disable the link-to-monitor if it is flapping too often. The link-to-disable port can be disabled and re-enabled to bring it back up. | UFD |
| 16.10.0010 | 253290 | WC | **Symptom**: Switch crashes when it is accessed through the web interface.<br>**Scenario**: This issue occurred when the switch was accessed using the web interface and RADIUS authentication was configured for web access.<br>**Workaround**: Disable RADIUS authentication for web access. | Web UI |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0010 | 253877 | WC | **Symptom**: The **WebUI Security > Clients** page displays incorrect MAC addresses, which results in the user role, IP address, and status columns to be empty.<br>**Scenario**: This issue occurred when a few workstations with higher value MAC addresses (for example, 9c:dc:71:fb:77:fe) are connected to the last ports of a 2930 stack or the last module of a 5400R. | Web UI |
| 16.10.0009 | 252885 | WC | **Symptom**: Switch appears down in Aruba Central.<br>**Scenario**: This issue occurred because the system time was set to the year 2036, though NTP sync was successful, and the switch was connected to Aruba Central.<br>**Workaround**: Configure an NTP server in the switch. | Activate |
| 16.10.0009 | 252226 | WC | **Symptom**: Switch does not respond during the ZTP process.<br>**Scenario**: This issue occurred when connecting to the switch using SSH, while Airwave was transferring the configuration to the switch. | AirWave |
| 16.10.0009 | 253081 | WC | **Symptom**: Switch reports self test failure or unsupported module in the event log.<br>**Scenario**: This issue occurred when the module is booted with a `JL308A xcvr`. | Boot |
| 16.10.0009 | 251418 | WC | **Symptom**: Pushing a switch configuration template from Aruba Central fails and a 500 error code is returned.<br>**Scenario**: This issue occurred when a configuration template that had no untagged ports in VLAN 1 was pushed from Aruba Central.<br>**Workaround**: In the configuration template, add at least one untagged port in VLAN 1. | Central |
| 16.10.0009 | 253174 | WC | **Symptom/Scenario**: The switch experienced an NMI crash with the following message: `Task='ewsCloudRcv'`. | Central |
| 16.10.0009 | 250966 | WC | **Symptom**: The switch fails to display the power supply details.<br>**Scenario**: In a stack or VSF configuration, the switch failed to display the power supply details for all stack member switches when using the show system power-supply detailed command. | CLI |
| 16.10.0009 | 253276 | WC | **Symptom**: Unable to copy crash-files, core-dump, and the show tech all command output from the switch.<br>**Scenario**: This issue occurred when executing the copy command with an invalid IP address, file name, hostname, or when parallelly executing the copy command in other sessions. | CLI |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Workaround**:<br>■ Copy the core file from the web interface.<br>■ Copy the show tech all command output from the console interface. | |
| 16.10.0009 | 252430 | WC | **Symptom**: Invalid MAC address entries are seen in the DHCP snooping binding table.<br>**Scenario**: This issue occurred when switch received malformed DHCP or BOOTP packets.<br>**Workaround**: Configure a DHCP authorized server so that requests only from authorized servers are processed. | DHCP Snooping |
| 16.10.0009 | 252265 | WC | **Symptom**: The switch does not forward DHCP packets.<br>**Scenario**: This issue occurred when both DHCP snooping and IP client tracker trusted were configured, and the client was authenticated. | IP Client Tracker |
| 16.10.0009 | 252701 | WC | **Symptom/Scenario**: User tunnel is lost when a controller fail-over is performed in a two node controller cluster.<br>**Workaround**: Re-establish the tunnel with a port flap and re-authentication. | Jumbo Frames |
| 16.10.0009 | 252833 | WC | **Symptom**: MSTP does not work as expected and does not block ports when it should.<br>**Scenario**: This issue occurred when two ports in a loop were in a forwarding state with MSTP and port-security non-default learn mode enabled.<br>**Workaround**: Disable port-security. | Spanning Tree |
| 16.10.0009 | 252338 | WC | **Symptom**: Incorrect message Rejected because maximum session limit is reached is printed when attempting to establish an SSH connection to the VSF standby OOBM IP address.<br>**Scenario**: This issue occurred when establishing an SSH connection to the standby OOBM IP address. | SSH |
| 16.10.0009 | 252613 | WC | **Symptom**: Unable to connect to the switch using SSH.<br>**Scenario**: This issue occurred when the switch is configured to use TACACS and a malformed TACACS packet is received by the switch.<br>**Workaround**: Reboot the switch. | SSH |
| 16.10.0009 | 251966 | WC | **Symptom**: The switch sends logging events with a "Z" at the end of the timestamp when the it is not configured to use UTC.<br>**Scenario**: This issue occurred when the switch sent syslog messages over TLS. | Syslog |
| 16.10.0009 | 252410 | WC | **Symptom**: The switch either reboots or fails over from the active to standby management module and records a Watchdog Reset entry in the event log. | VSF |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue occurred when IP directed-broadcast was configured in the switch and Wake On LAN traffic was sent to a directly connected subnet.<br>**Workaround**: Disable IP directed-broadcast. | |
| 16.10.0009 | 252762 | WC | **Symptom**: Although the VXLAN tunnel name was configured, it was not displayed.<br>**Scenario**: This issue occurred when the VXLAN tunnel name was configured before configuring the source and destination IP addresses for the tunnel. | VXLAN |
| 16.10.0009 | 252443 | WC | **Symptom/Scenario**: The Reboot button is displayed for a few seconds in the Web UI. Clicking it allowed an operator to reboot the switch. | Web UI |
| 16.10.0008 | - | WC | Version 16.10.0008 was never released. | - |
| 16.10.0007 | 252007 | WC | **Symptom**: The switch sends an incorrect CLASS attribute value in the RADIUS accounting packet.<br>**Scenario**: When the CLASS attribute is updated during re-authentication of a MAC-authenticated client session, the switch fails to send the new CLASS attribute value in the RADIUS accounting packet.<br>**Workaround**: Force a new client authentication session by disabling/enabling the port after the CLASS attribute value changes. | Accounting |
| 16.10.0007 | 251765 | WC | **Symptom**: The show runnig-config output does not display some access list entries (ACEs).<br>**Scenario**: When the switch is configured with extended ACLs and connect-rate-filter, some ACEs are not displayed in the output of the show runnig-config command.<br>**Workaround**: Use the show access-list config command to get the complete extended ACL configuration. | ACLs |
| 16.10.0007 | 251273 | WC | **Symptom**: The switch incorrectly places clients in the configured authorized VLAN (auth-vid).<br>**Scenario**: When using chap-radius authorized option, if the route to the RADIUS server is not resolved during the switch boot up, clients are incorrectly placed in the configured authorized VLAN (auth-vid) rather than the guest VLAN (unauth-vid) or initial-role.<br>**Workaround**: Reauthenticate the affected clients. | Authentication |
| 16.10.0007 | 251659 | WC | **Symptom**: Switch fails to move the client MAC address from one port to another.<br>**Scenario**: When addr-move is configured to enable roaming for authenticated clients from one port to another, with Private VLAN enabled, the switch fails to move the client MAC address.<br>**Workaround**: Disable and re-enable the switch interface where the affected client moved to. | Authentication |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0007 | 251927 | WC | **Symptom**: The switch fails to remove CDP configuration for a port.<br>**Scenario**: When a port is added to a trunk interface, the switch fails to remove the previous non-default CDP configuration for that port (example: no cdp enable <PORT-NUM>).<br>**Workaround**: Remove the non-default CDP configuration from the individual port before adding it to trunk interface. | CDP |
| 16.10.0007 | 252053 | WC | **Symptom/Scenario**: The switch crashes with an error message similar to: `Software exception in ISR at pvDmaV1Rx.c <...> ASSERT: No resources available!.` | Central |
| 16.10.0007 | 252267 | WC | **Symptom**: The switch experiences high CPU utilization.<br>**Scenario**: In conditions of low network bandwidth or network congestion that cause frequent disconnections from the Aruba Central Portal, the switch experiences high CPU utilization while attempting to reconnect to Aruba Central and while being managed by other NMS applications such as Solarwinds at the same time.<br>**Workaround**: Use only one NMS application to manage the switch if network bandwidth capacity or congestion cannot be improved. | Central |
| 16.10.0007 | 252066 | WC | **Symptom/Scenario**: The switch crashes with a message similar to: `Health Monitor: Restr Mem Access ... Task='mdevMntr'.` | Device finger printing |
| 16.10.0007 | 251876 | WC | **Symptom**: The switch may fail to apply the correct VLAN to dynamic trunks.<br>**Scenario**: After a reboot of a switch configured for dynamic trunks with device profile enabled on ports, the switch may fail to apply the correct VLAN configured in the device-profile, after the port is joined to the dynamic trunk.<br>**Workaround**: Disable and enable device-profile. | Dynamic Trunks |
| 16.10.0007 | 251972 | WC | **Symptom**: Some clients using the PEAP authentication mechanism are not successfully authenticated.<br>**Scenario**: When concurrent authentication requests are sent to the switch using peap-mschapv2, some clients may not be successfully authenticated, even though ACCESS ACCEPT is sent from the RADIUS server. | MAC Authentication |
| 16.10.0007 | 252170 | WC | **Symptom**: Some multicast traffic is incorrectly flooded on all ports belonging to a VLAN. | Multicast |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: Multicast packets received with aTTL <= 1 are indefinitely flooded to all ports of a PIM enabled VLAN. | |
| 16.10.0007 | 249716 | WC | **Symptom**: The switch fails to pass traffic through a promiscuous port.<br>**Scenario**: After a reboot event, the switch fails to pass traffic trough a promiscuous port in the primary VLAN.<br>**Workaround**: Remove and re-add the affected promiscuous port from/to the primary VLAN. | Private VLAN |
| 16.10.0007 | 251339 | WC | **Symptom**: The switch or the switch module may crash with an error message similar to: `Read Error Restr Mem Access <...> Task='mAdMUpCtrl'.`<br>**Scenario**: When qos trust dscp on a 40G port is enabled, the switch or switch module may crash with an error message similar to: `Read Error Restr Mem Access <...> Task='mAdMUpCtrl.` | QoS |
| 16.10.0007 | 252090 | WC | **Symptom**: Switch fails to flag the unreachable RADIUS servers.<br>**Scenario**: When RADIUS server tracking is enabled, the switch fails to flag those RADIUS servers configured using the fully qualified domain name (FQDN) when they are unreachable with an asterisk (*) in the output of the show radius command.<br>**Workaround**: Use IP address for RADIUS server configuration when RADIUS server tracking is enabled. | RADIUS |
| 16.10.0007 | 252131 | WC | **Symptom**: REST API calls may experience some slight delay in execution response.<br>**Scenario**: When multiple REST API commands are executed over the same HTTPS session, they may experience a slight delay in execution response.<br>**Workaround**: Use a new HTTPS session for each REST API call. | REST |
| 16.10.0007 | 251899 | WC | **Symptom**: Switch fails to return the serial number of the power supply.<br>**Scenario**: When configured in a stack, the switch does not return the serial number of power supplies for the stack member switches when polling the entPhysicalSerialNum SNMP object.<br>**Workaround**: The power supply serial number can be found in the show system power-supply output. | SNMP |
| 16.10.0007 | 252377 | WC | **Symptom**: The switch fails to send traffic over some switch interfaces. | Spanning Tree |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: After a redundancy switchover to the standby VSF switch while spanning tree is enabled in PVST mode, the switch fails to forward traffic over the switch ports transitioned from Blocking to Forwarding state.<br>**Workaround**: Disable and re-enable the affected switch ports. | |
| 16.10.0007 | 250797 | WC | **Symptom**: The switch sends an incorrect checksum when forwarding certain UDP frames.<br>**Scenario**: If a received UDP frame has no checksum or the checksum value of zero (0), the switch incorrectly calculates the checksum when forwarding it. | UDP |
| 16.10.0007 | 252409 | WC | **Symptom**: The switch fails to override the initial-role.<br>**Scenario**: When an existing per-port initial-role is modified, the switch fails to re-apply the new initial-role to ports with clients already authenticated in the previous initial-role.<br>**Workaround**: Remove the existing per-port initial-role config and configure the new initial-role on the port. | User Roles |
| 16.10.0007 | 251475 | WC | **Symptom**: The switch experiences high CPU utilization and possible console connectivity issues.<br>**Scenario**: When configuring or modifying aggregated interfaces (trunks) with more than 3 member ports on a switch where there is a very high number of configured VLANs, the switch experiences high CPU utilization and possible console connectivity issues while applying the configuration. | VLAN |
| 16.10.0007 | 251505 | WC | **Symptom**: The WebUI contains an XSS vulnerability.<br>**Scenario**: Configure the editable parameters in the WebUI with values that can cause an XSS attack. | Web UI |
| 16.10.0007 | 251524 | WC | **Symptom**: The switch fails to display some ports on the Ports page of the WebUI.<br>**Scenario**: When aSysName with trailing zeroes is received in the LLDP packet from a neighboring device, the switch fails to list some ports in the Ports page when using the WebUI.<br>**Workaround**: To get the information for all ports use one of the following options:<br>■ Disable LLDP on the port where the device with `invalidSysName` is connected.<br>■ Use the traditional web UI to get the information for the affected/missing ports.<br>■ Use switch CLI commands to get the information for the affected/missing ports. | Web UI |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0006 | - | WC | Version 16.10.0006 was never released. | - |
| 16.10.0005 | 251473 | WC | **Symptom**: End devices periodically lose access to the network.<br>**Scenario**: When ports are configured with user-based tunneling in addition to 802.1X and MAC authentication, end devices connected to those parts periodically lose access to the network. | Tunneling |
| 16.10.0004 | - | WC | Version 16.10.0004 was never released. | - |
| 16.10.0003 | 251317 | WC | **Symptom**: A Windows client that joins a domain other than the one defined in Cisco ISE fails to authenticate. The client will also wait more than 5 minutes before attempting MAC address authentication.<br>**Scenario**: This issue is observed when MAC and 802.1X authentication are enabled on the port and the configured auth-order is 802.1X-MAC and an initial role. | 802.1X |
| 16.10.0003 | 251464 | WC | **Symptom**: VSF stack members crash intermittently during 802.1X client reauthentication and the following message is displayed: `Software exception in ISR at pvDmaV1Rx.c: -> ASSERT: No resources available!.`<br>**Scenario**: This issue is observed when ports with LLDP traffic are configured with 802.1X and MAC authentication, and the RADIUS VSA `HP-Port-Client-Limit-MA` value is zero. | 802.1X |
| 16.10.0003 | 251498 | WC | **Symptom**: A client is unable to pass traffic.<br>**Scenario**: This issue is observed when the clear mac-address vlan 1 mac command is issued to clear the switch's base MAC address from VLAN 1. | Basic Layer 2 |
| 16.10.0003 | 251280 | WC | **Symptom**: Deploying a switch template through Airwave/Aruba Central fails.<br>**Scenario**: This issue is observed when the IP address from VLAN1 is removed from a new configuration template and is pushed to the switch with the "ntpserver-name <server name>".<br>**Workaround**: Do not remove the IP address from VLAN 1 in the new template. | Central |
| 16.10.0003 | 249172 | WC | **Symptom**: The Event log lists fan failure events and the amber LED is displayed on the front panel of the switch.<br>**Scenario**: The switch operates normally with no change in the environmental temperature. | Chassis Manager |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0003 | 251393 | WC | **Symptom**: A switch crashes with the following message `Software exception in ISR at pvDmaV1Rx.c -> ASSERT: No resources available.`<br>**Scenario**: This issue is observed when a switch is configured with an initial role with a captive-portal-profile and a client is placed in this initial role because the RADIUS server is unreachable. | Classifier |
| 16.10.0003 | 250816 | WC | **Symptom**: Authenticated users are disconnected from the switch.<br>**Scenario**: This issue is observed when users disable and enable the interface which connects to the dhcp- relay switch, after configuring the DHCP server, DHCP relay, and DHCP snooping with ip-source lockdown.<br>**Workaround**: Disable ip-source lockdown. | DIPLD |
| 16.10.0003 | 251662 | WC | **Symptom**: Unable to configure a /31 subnet address as source/destination address for tunnel interfaces.<br>**Scenario**: This issue is observed when users attempt to configure a /31 subnet address as source/ destination address for a tunnel interface.<br>**Workaround**: Configure a /30 subnet address. | L3 Addressing |
| 16.10.0003 | 249465 | WC | **Symptom**: A switch crashes and displays the following message: `Software exception at ospf2.c -- in 'eRouteCtrl' -> Routing Stack: Assert Failed.`<br>**Scenario**: This issue is observed when a switch is configured with OSPF and one of the OSPF neighbors is disconnected. | OSPF |
| 16.10.0003 | 251615 | WC | **Symptom**: An attacker is able to obtain sensitive data without providing valid login credentials after a successful REST query.<br>**Scenario**: This issue is observed when web management is enabled on the switch. | REST |
| 16.10.0003 | 251340 | WC | **Symptom**: Tunneled clients lose network connectivity.<br>**Scenario**: This issue is observed when user tunnels are configured in addition to ip client-tracker trusted and ip client-tracker probe-delay.<br>**Workaround**:<br>1. Remove ip client-tracker probe-delay from the configuration.<br>2. Disable the port.<br>3. Clear ARP.<br>4. Re-enable the port. | Tunneled Node |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0003 | 251893 | WC | **Symptom**: A switch port is in the Disabled state.<br>**Scenario**: This issue is observed when spanning tree is enabled and Per-Port Tunneled Node (PPTN) is configured on two ports that are connected.<br>**Workaround**: Do not connect two PPTN ports. | Tunneled Node |
| 16.10.0003 | 251325 | WC | **Symptom**: Users are unable to modify the vlan-id-tagged list of a user role.<br>**Scenario**: This issue is observed when the user applies a template that adds VLANs to the vlan-id-tagged list of a user role.<br>**Workaround**: Use a template that does not extend the list of VLANs in vlan-id-tagged. | User Roles |
| 16.10.0003 | 251030 | WC | **Symptom**: The output of the show interface command differs for a VSF and a non-VSF interface.<br>**Scenario**: This issue is observed when a switch is configured for VSF.<br>**Workaround**: Execute the clear statistics global command and output of show interface command will be the same for both VSF and non-VSF interfaces. | VSF |
| 16.10.0003 | 251506 | WC | **Symptom**: The switch manager password is altered to an attack-controlled value.<br>**Scenario**: This issue is observed when the user clicks a malicious hyperlink. | Web UI |
| 16.10.0003 | 251314 | WC | **Symptom**: Switches appear offline in Aruba Central.<br>**Scenario**: This issue is observed after the switch software is upgraded from 16.04 to 16.08.<br>**Workaround**: Reboot the switch. | ZTP |
| 16.10.0002 | CR_ 251119 | WC | **Symptom**: Switch is unable to connect to a remote server.<br>**Scenario**: Switch attempts to connect to a remote server such as Activate when attempting Zero Touch Provisioning (ZTP).<br>**Workaround**: Ensure that an MSS Option value is returned in the TCP SYN-ACK from the server. | Activate |
| 16.10.0002 | 250681 | WC | **Symptom/Scenario**: The Topology section of Airwave shows spanning tree details for a switch that does not have spanning tree enabled. | AirWave |
| 16.10.0002 | 250934 | WC | **Symptom**: The switch does not respond to commands from a console or SSH session.<br>**Scenario**: After updating the switch configuration using Aruba Central while clients are authenticated, the switch may not respond to commands from a console or SSH session.<br>**Workaround**: | Central |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | 1. Apply a template disabling MAC authentication on all ports.<br>2. Apply a template with AAA config changes.<br>3. Apply a template enabling MAC authentication on all ports. | |
| 16.10.0002 | 251313 | WC | **Symptom**: The switch experiences a high CPU utilization and loses connection with Central.<br>**Scenario**: when the switch is upgraded to 16.08.0001 and a template with tls and cwmp commands is pushed from Central, the switch experiences high CPE utilization and loses the connection to Aruba Central.<br>**Workaround**: Remove tls application cloud lowest-version tls1.2 and cwmp from the switch template. | Central |
| 16.10.0002 | 250251 | WC | **Symptom/Scenario**: The switch crashes with a message similar to: `Software exception in ISR at interrupts_om.c-> Excessive OM FP interrupts.` | Chassis |
| 16.10.0002 | 250542 | WC | **Symptom**: The switch is unable to classify Aruba APs.<br>**Scenario**: After configuring device fingerprinting, the switch is unable to classify Aruba APs. | Device finger printing |
| 16.10.0002 | 250600 | WC | **Symptom/Scenario**: The help text for the device-identity lldp oui command indicates that the required input is a MAC-OUI. | Device finger printing |
| 16.10.0002 | 250957 | WC | **Symptom**: Host packets are denied with a message similar to `dlpld: AM1: Access denied.`<br>**Scenario**: When the switch has been configured using the aaa port-access and ip source-lockdown commands and clients authenticate to the switch, if more than one client is placed in a VLAN provided by the RADIUS server, host packets are denied.<br>**Workaround**: Disable Dynamic IP Lockdown on the switch using the no ip source-lockdown command. | DIPLD |
| 16.10.0002 | 250550 | WC | **Symptom**: Primary and secondary VLANs do not have MAC address entries.<br>**Scenario**: When a port has been configured with PVLAN and port security and the port is subsequently disabled and re-enabled, MAC address entries are not present in the primary and secondary VLANs.<br>**Workaround**: Reconfigure the port security configuration of the port. | MAC address |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0002 | 250392 | WC | **Symptom**: The switch crashes with a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access.`<br>**Scenario**: After an IP address has been reassigned from one VLAN to another VLAN using the menu interface, the switch may crash with a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access.`<br>**Workaround**: Disable the first VLAN and save the configuration from the menu interface. Then, configure the deleted IP address on the second VLAN. | Menu |
| 16.10.0002 | 245830 | WC | **Symptom**: The switch fails to list the switch ports in the Ports web management page.<br>**Scenario**: When a peer device that advertises information in LLDP has a sysName string with special characters, the switch fails to display the port list table on the Ports web management page.<br>**Workaround**: Remove the special characters from the peer device sysName or use CLI commands to get specific port information. | Next Gen GUI |
| 16.10.0002 | 250833 | WC | **Symptom**: After a switch reboot, OSPF is stuck in the INIT state.<br>**Scenario**: When a switch that is configured with OSPF, but ip router-id has not been configured, is rebooted OSPF remains in the INIT state.<br>**Workaround**: Configure the router ID manually. | OSPF |
| 16.10.0002 | 250958 | WC | **Symptom**: The hit counters in the output of the show statistics policy command shows all zeros.<br>**Scenario**: If a QoS policy with several class entries across all ports on multiple modules has been applied, the output of the show statistics policy command shows all zeros in the hit counters. | QoS |
| 16.10.0002 | 250691 | WC | **Symptom**: The Aruba 1G SFP LC SX 500m MMF transceiver ( J4858D) takes a long time to link up.<br>**Scenario**: After hot swapping an Aruba 1G SFP LC SX 500m MMF transceiver ( J4858D), the transceiver takes a longer time than usual to link up. | Transceivers |
| 16.10.0002 | 251102 | WC | **Symptom**: The switch crashes with a message similar to `Software exception at ppmgr_globals.c ... in 'mPpmgrCtrl' -> Port record out of bounds!!!.`<br>**Scenario**: After inserting an Aruba Gigabit 1000Base-T Mini-GBIC transceiver ( J8177B), the switch crashes. | Transceivers |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0002 | 251017 | WC | **Symptom**: The event log displays `lpAddrMgr: Failed to add FIB entry - neighbor matches existing route (vrf:0 A.B.C.D/32).`<br>**Scenario**: When the switch has been configured with a VRRP master and the connected routes are redistributed using routing protocols, the event log will display a lpAddrMgr message. | VRRP |
| 16.10.0002 | 251203 | WC | **Symptom**: Pings to the VRRP virtual IP address fail.<br>**Scenario**: If a switch module is reloaded, added, or hot-swapped, if a VSF stack member joins the stack after a stack split event or after a switch reboot with expansion module present, the switch fails to respond to ping packets to the VRRP virtual IP address. | VRRP |
| 16.10.0002 | 250489 | WC | **Symptom**: High utilization of a VSF link is reported by the switch.<br>**Scenario**: When VSF is configured with one link having multiple ports and then a VSF link port toggle is performed by disabling then re-enabling the VSF interface, the switch reports a high link utilization. | VSF |
| 16.10.0002 | 250754 | WC | **Symptom**: The switch cannot be found in Aruba Central even though the CLI reports the switch as being connected.<br>**Scenario**: When a VSF stack is already checked into Aruba Central with the same stack ID as another VSF stack, switches in the stack cannot be found in Aruba Central.<br>**Workaround**: Ensure all switches are running 16.06 or later and then form the VSF stack. | VSF |
| 16.10.0002 | 250896 | WC | **Symptom**: Switch ports are not listed in the web interface.<br>**Scenario**: If a peer device advertises an LLDP port ID containing special characters, switch ports are not listed in the web interface. | Web UI |
| 16.10.0001 | 250366 | WC | **Symptom**: An Apple MacOS device (desktop or laptop) is unable to maintain authentication with APs.<br>**Scenario**: When an AP is connected to a switch port that has been configured with device-identity bypass, an Apple MacOS device (desktop or laptop) receives EAP request ID packets after 802.1X authentication and is unable to maintain authentication with the AP.<br>**Workaround**: Configure a MAC-based ACL to block the EAP request identity to multicast MAC address. | 802.1X |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0001 | 250681 | WC | **Symptom/Scenario**: The Topology section of Airwave shows spanning tree details for a switch that does not have spanning tree enabled. | AirWave |
| 16.10.0001 | 250934 | WC | **Symptom**: The switch does not respond to commands from a console or SSH session.<br>**Scenario**: After updating the switch configuration using Aruba Central while clients are authenticated, the switch may not respond to commands from a console or SSH session.<br>**Workaround**:<br>1. Apply a template disabling MAC authentication on all ports.<br>2. Apply a template with AAA config changes.<br>3. Apply a template enabling MAC authentication on all ports. | Central |
| 16.10.0001 | 250251 | WC | **Symptom/Scenario**: The switch crashes with a message similar to: `Software exception in ISR at interrupts_om.c-> Excessive OM FP interrupts.` | Chassis |
| 16.10.0001 | 250154 | WC | **Symptom**: The global status LED on all members of a VSF stack turns amber.<br>**Scenario**: When one member of a VSF stack experiences an over temperature, the global status LED on all members of the stack turns amber. | Chassis Manager |
| 16.10.0001 | 250542 | WC | **Symptom**: The switch is unable to classify Aruba APs.<br>**Scenario**: After configuring device fingerprinting, the switch is unable to classify Aruba APs. | Device finger printing |
| 16.10.0001 | 250600 | WC | **Symptom/Scenario**: The help text for the device-identity lldp oui command indicates that the required input is a MAC-OUI. | Device identity |
| 16.10.0001 | 250957 | WC | **Symptom**: Host packets are denied with a message similar to `dlpld: AM1: Access denied.`<br>**Scenario**: When the switch has been configured using the aaa port-access and ip source-lockdown commands and clients authenticate to the switch, if more than one client is placed in a VLAN provided by the RADIUS server, host packets are denied.<br>**Workaround**: Disable Dynamic IP Lockdown on the switch using the no ip source-lockdown command. | DIPLD |
| 16.10.0001 | 250550 | WC | **Symptom**: Primary and secondary VLANs do not have MAC address entries. | MAC address |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: When a port has been configured with PVLAN and port security and the port is subsequently disabled and re-enabled, MAC address entries are not present in the primary and secondary VLANs.<br>**Workaround**: Reconfigure the port security configuration of the port. | |
| 16.10.0001 | 250392 | WC | **Symptom**: The switch crashes with a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access.`<br>**Scenario**: After an IP address has been reassigned from one VLAN to another VLAN using the menu interface, the switch may crash with a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access.`<br>**Workaround**: Disable the first VLAN and save the configuration from the menu interface. Then, configure the deleted IP address on the second VLAN. | Menu |
| 16.10.0001 | 250833 | WC | **Symptom**: After a switch reboot, OSPF is stuck in the INIT state.<br>**Scenario**: When a switch that is configured with OSPF, but ip router-id has not been configured, is rebooted OSPF remains in the INIT state.<br>**Workaround**: Configure the router ID manually. | OSPF |
| 16.10.0001 | 251092 | WC | **Symptom**: PoE power is not provided to certain Cisco IP phones.<br>**Scenario**: When certain Cisco IP phones are connected to an Aruba 2930M (R0M67A) switch using a Y-cable or DAC, the phone does not receive PoE power from the switch. | PoE |
| 16.10.0001 | 250958 | WC | **Symptom**: The hit counters in the output of the show statistics policy command shows all zeros.<br>**Scenario**: If a QoS policy with several class entries across all ports on multiple modules has been applied, the output of the show statistics policy command shows all zeros in the hit counters. | QoS |
| 16.10.0002 | 250691 | WC | **Symptom**: The Aruba 1G SFP LC SX 500m MMF transceiver ( J4858D) takes a long time to link up.<br>**Scenario**: After hot swapping an Aruba 1G SFP LC SX 500m MMF transceiver ( J4858D), the transceiver takes a longer time than usual to link up. | Transceivers |
| 16.10.0002 | 251102 | WC | **Symptom**: The switch crashes with a message similar to `Software exception at ppmgr_globals.c ... in 'mPpmgrCtrl' -> Port record out of bounds!!!.` | Transceivers |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: After inserting an Aruba Gigabit 1000Base-T Mini-GBIC transceiver ( J8177B), the switch crashes. | |
| 16.10.0001 | 251017 | WC | **Symptom**: The event log displays `lpAddrMgr: Failed to add FIB entry - neighbor matches existing route (vrf:0 A.B.C.D/32).`<br>**Scenario**: When the switch has been configured with a VRRP master and the connected routes are redistributed using routing protocols, the event log will display a lpAddrMgr message. | VRRP |
| 16.10.0001 | 251203 | WC | **Symptom**: Pings to the VRRP virtual IP address fail.<br>**Scenario**: If a switch module is reloaded, added, or hot-swapped, if a VSF stack member joins the stack after a stack split event or after a switch reboot with expansion module present, the switch fails to respond to ping packets to the VRRP virtual IP address. | VRRP |
| 16.10.0001 | 250489 | WC | **Symptom**: High utilization of a VSF link is reported by the switch.<br>**Scenario**: When VSF is configured with one link having multiple ports and then a VSF link port toggle is performed by disabling then re-enabling the VSF interface, the switch reports a high link utilization. | VSF |
| 16.10.0001 | 250754 | WC | **Symptom**: The switch cannot be found in Aruba Central even though the CLI reports the switch as being connected.<br>**Scenario**: When a VSF stack is already checked into Aruba Central with the same stack ID as another VSF stack, switches in the stack cannot be found in Aruba Central.<br>**Workaround**: Ensure all switches are running 16.06 or later and then form the VSF stack. | VSF |
| 16.10.0001 | 245830 | WC | **Symptom**: The switch fails to list the switch ports in the Ports web management page.<br>**Scenario**: When a peer device that advertises information in LLDP has a sysName string with special characters, the switch fails to display the port list table on the Ports web management page.<br>**Workaround**: Remove the special characters from the peer device sysName or use CLI commands to get specific port information. | Web UI |
| 16.10.0001 | 250896 | WC | **Symptom**: Switch ports are not listed in the web interface.<br>**Scenario**: If a peer device advertises an LLDP port ID containing special characters, switch ports are not listed in the web interface. | Web UI |

# Issues and Workarounds

The following are known open issues with this branch of the software.

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.

**Table 11:** *Known Issues*

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0016 | 255646 | WC | **Symptom**: The `show statistics aclv4 <ACL-NAME-STR> vlan <VLAN-ID> out` command displays lesser `HitCounts for ACL` for deny rule.<br>**Scenario**: The routed traffic is denied even before the egress Access control list (ACL) when the ACL contains a deny rule, and it is applied in the VLAN egress direction. | ACL |
| 16.10.0015 | 255554 | WC | **Symptom**: Aruba 2930F switches fail to connect to Aruba Central during the ZTP process.<br>**Scenario**: This issue occurs when the Simple Network Time Protocol (SNTP) or any other time protocol is not configured on the network.<br>**Workaround**: Use one of the following workarounds to fix this issue:<br>■ Manually configure the system time.<br>◦ Set the current date and time using the `time [HH:MM:SS] [MM/DD/YYYY]` command.<br>◦ Force connection to Aruba Central using the `aruba-central disable` and `aruba-central enable` commands.<br>■ Execute any reboot command that gracefully reboot the switch. The following are some of the commands that gracefully reboot the switch:<br>◦ `boot system flash {<primary \| secondary>}`<br>◦ `reboot`<br>◦ `reset saved-configuration`<br>■ Enable SNTP on the network.<br>◦ By default, SNTP updates the system time. This issue does not occur when the SNTP server is enabled on the network. | Central |
| 16.08.0009 | 247648 | WC | **Symptom**: The switch fails to bypass authentication for random devices. | CDP/LLDP Bypass |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: When the CDP/LLDP bypass is enabled on a switch configured in VSF, the switch fails to bypass authentication for random devices after a redundancy switchover event.<br>**Workaround**: Disable and re-enable the affected port to re-enforce CDP/LLDP bypass on the port. | |

# Upgrade Information

## Upgrading Restrictions and Guidelines

WC.16.10.0009 uses BootROM WC.16.01.0006 or WC.16.01.0007 ( JL692A only) when running on 2930F switches and BootROM WC.17.02.0006 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.16.10 branch of the software.
Version YA/YB.16.10.0001 is the initial build of Major version YA/YB.16.10 software. YA/YB.16.10.0020 includes all enhancements and fixes in the YA/YB.16.10.0019 software, plus the additional enhancements and fixes in the YA/YB.16.10.0020 enhancements and fixes sections of this release note.

This release applies to the following Aruba 2530 Switch Series:

**Table 12:** *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


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

**Table 13:** *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 |

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 14:** *Enhancements*

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0020 | YA/YB | No enhancements were included in version 16.10.0020. | NA |
| 16.10.0019 | YA/YB | No enhancements were included in version 16.10.0019. | NA |

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0018 | YA/YB | No enhancements were included in version 16.10.0018. | NA |
| 16.10.0017 | 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.<br>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.<br>A MIB has also been added to enable or disable the randomization of TCP timestamp offsets.<br>Refer to the *Aruba 2530 Management and Configuration Guide for AOS-S Switch 16.10* and *Aruba MIB and Trap Support Matrix for AOS-S Switch 16.10* for more information. | Security |
| 16.10.0016 | YA/YB | Added support for the new SSH data integrity algorithm hmac-sha2-256, which is defined in RFC 6668.<br>Refer to the *Aruba 2530 Access Security Guide for AOS-S Switch 16.10* and *Aruba 2530 IPv6 Configuration Guide for AOS-S Switch 16.10* for more information. | SSH |
| 16.10.0016 | YA/YB | Added support to configure the size of the EAP-TLS fragments sent from the switch to the RADIUS server. Configuring EAP-TLS fragment size based on the MTU of the network avoids IP fragmentation in the network, and thus, the fragmented packets will not be dropped by the firewall or gateways.<br>Added a MIB to indicate the maximum size of the EAP-TLS fragment sent to the RADIUS server.<br>Refer to the *Aruba 2530 Access Security Guide for AOS-S Switch 16.10* and *Aruba MIB and Trap Support Matrix for AOS-S Switch 16.10* for more information. | EAP-TLS Fragmentation |
| 16.10.0015 | YA/YB | This release brings the ability for REST clients to use RADIUS/TACACS+ for authorization instead of using per-switch passwords. This ability for REST clients has the following limitation:<br>When RADIUS is used for the REST authorization, the VSAs HP-URI-String, HP-URI-Access, HP-URI-Exception, and HP-URI-Json-String should be configured in the correct order, for each URIs to be authorized. Also the RADIUS server should send the VSA in RADIUS ACCESS ACCEPT in the same order as it is configured. If the order of VSAs are not maintained by RADIUS server while sending out RADIUS ACCESS ACCEPT, the switch can not use the authorization data. As a result, the authentication/authorization of REST user fails.<br>Refer to the *Aruba REST API for AOS-S Switch 16.10* for more information. | AAA for REST Interface |
| 16.10.0014 | YA/YB | No enhancements were included in version 16.10.0014. | NA |
| 16.10.0013 | YA/YB | No enhancements were included in version 16.10.0013. | NA |

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0012 | YA/YB | Added `concise` parameter to display port-access and spanning-tree attributes in a consolidated format, when executing `show config` and `show running-config` commands. | Enhancement for `show config` and `show running-config` commands |
| 16.10.0012 | YA/YB | Added support to enable SNMP traps for a specified event. This helps to filter out particular traps from all SNMP trap messages.<br>**Syntax:** `snmp-server enable traps event-list <EVENT-LIST-STR>` | Customization for SNMP Traps |
| 16.10.0012 | YA/YB | Added `recv-disable` parameter to configure loop-protect from blocking the receiving port when a loop is detected.<br>**Syntax:** `no loop-protect <PORT-LIST> receiver-action [recv-disable]` | Configuration for loop-protect receiver-action |
| 16.10.0011 | YA/YB | Added support to format MAC address in upper case for the Called and Calling Station IDs.<br>Refer to the *Access Security Guide* for more information. | Port Access Enhancement |
| 16.10.0011 | YA/YB | Added support to include the Port VLAN information in RADIUS access request for all authentication types.<br>Refer to the *Access Security Guide* for more information. | Port Access Enhancement |
| 16.10.0011 | YA/YB | Added support to enable AES 256-bit encryption for SNMP.<br>Refer to the *Management and Configuration Guide* for more information. | AES 256-bit encryption for SNMP |
| 16.10.0011 | YA/YB | Added support to configure a prefix string along with the switch IP address or hostname in the logs sent to the Syslog servers. This helps to classify and group log entries based on the string value.<br>**Syntax:** `logging prefix <ASCII-STR>`<br>Refer to the *Management and Configuration Guide* for more information. | Syslog Enhancement |
| 16.10.0010 | YA/YB | Added support to provide the option to specify the source interface or VLAN for Central connectivity. The existing IP source-interface command is enhanced to override current configuration check for provisioning using Aruba Activate.<br>Refer to the *Management and Configuration Guide* for more information. | Source interface option for Central connectivity |
| 16.10.0010 | YA/YB | Added support to allow more PoE devices to be connected to the switch by using `poe-alloc-by-usage` when using Device Profiles. This can be based on either **Usage** or **Class**. Default allocation will be based on **Class**.<br>Refer to the *Management and Configuration Guide* for more information. | Device Profile Enhancement |

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0010 | YA/YB | Added support to work with the default setting in OpenSSH 8.2 by choosing an inherently more secure algorithm as the default on the switch for SSH communication. Refer to the *Access Security Guide* for more information.<br>The list of new Host-Key algorithms are as follows:<br>■ rsa-sha2-512<br>■ rsa-sha2-256<br>The list of new SSH KEX algorithms are as follows:<br>■ ecdh-sha2-nistp521<br>■ ecdh-sha2-nistp381<br>■ ecdh-sha2-nistp256<br>■ diffie-hellman-group-exchange-sha256 | Support for OpenSSH 8.2 |
| 16.10.0009 | YA/YB | Added support for the manager password enforcement to ensure that the switch prompts the user to configure the manager password on the switch before configuring any other features. If the manager password is not configured, then the user will have read-only access to the switch. This is applicable only to switches with factory default configuration. Refer to the *Access Security Guide* for more information. | Manager Password Enforcement |
| 16.10.0009 | YA/YB | Added support to enhance the payload size for the REST API interfaces. The increased payload size for 2530 YA/YB platforms is 64K. Refer to the *REST API Guide* for more information. | REST API Payload Enhancement |
| 16.10.0009 | YA/YB | Added support for Server Name Indication (SNI), which is a TLS extension defined in RFC 6066. This feature is enabled by default to include the SNI extension in the Client Hello sent from the switch to all the TLS client applications. Refer to the *Access Security Guide* for more information. | Server Name Indication for TLS |
| 16.10.0008 | YA/YB | Version 16.10.0008 was never released. | NA |
| 16.10.0007 | YA/YB | ■ Added additional support for pipe "\|" option to grep for pattern match the output of CLI commands, such as:<br>◦ Case-insensitive option to allow a case insensitive pattern match<br>◦ Up to four consecutive pattern matches in one CLI command<br>■ Added support for a per-session based command to wrap column display in the CLI output using session wrap-text option when its length is exceeding the column width.<br>Refer to the *Management and Configuration Guide* for more information. | CLI |
| 16.10.0007 | YA/YB | Added support for monitoring authenticated devices with static IP address using the following CLI command:<br>`ip client-tracker <trusted>`<br>Refer to the *Access Security Guide* for more information. | Client Visibility |

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.007 | YA/YB | Added the following REST enhancements:<br>■ Support for ARP table data.<br>■ Support for primary VLAN.<br>■ Support for reserved-vlan and clearpass options to configure dynamic segmentation.<br>■ REST API schema moved under `device-rest-api/services/server.html`.<br>Refer to the *REST API Guide* for more information. | REST |
| 16.10.0007 | YA/YB | Added support for the new activate endpoint `devices-v2.arubanetworks.com` which has the following two major differences compared to the old endpoint device.arubanetworks.com:<br>■ It works on the standard TLS handshake mechanism and uses mutual authentication.<br>■ It uses certificates issued by HP CA for establishing TLS connections.<br>Zero Touch Provisioning (ZTP) improvements were made to deal with situations such as unresponsive DNS servers. Refer to the *Management and Configuration Guide* for more information. | Zero Touch Provisioning |
| 16.10.0006 | YA/YB | Version 16.10.0006 was never released. | NA |
| 16.10.0005 | YA/YB | Version 16.10.0005 was never released. | NA |
| 16.10.0004 | YA/YB | Version 16.10.0004 was never released. | NA |
| 16.10.0003 | YA/YB | New command `aaa accounting session-id include-switch-identity` was added. When this command is invoked, an accounting session ID is generated with Switch Base MAC, Client MAC, and Timestamp for network accounting type. The other accounting types (exec, system, commands) do not include Client MAC and hence the session ID is generated with Switch Base MAC, Track ID, and Timestamp.<br>If the same client is accessing the network from multiple switches, then the accounting session ID can be duplicated. This caused issues in ClearPass Policy Manager where client insertion in the database failed with an error similar to Integrity Error: `acct_id, calling_station_id` violates check constraint. This new command alleviates that problem. | AAA |
| 16.10.0003 | YA/YB | This enhancement will only be in effect if the CoA/Disconnect request has a message authenticator attribute in request packet. The message authenticator attribute is used to verify the integrity (HMAC-MD5) of the RADIUS packet. This is an optional attribute in the Access/CoA/Disconnect packet. If the received packet has this attribute in the RADIUS packet, the receiver will validate the integrity value and discard it if the value is incorrect. | RADIUS |

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0002 | YA/YB | No enhancements were included in version 16.10.0002. | NA |
| 16.10.0001 | YA/YB | No enhancements were included in version 16.10.0001. | NA |

# 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 15:** *Fixed Issues*

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0020 | 256257 | YA/YB | **Symptom/Scenario**: Certain transceivers had link issues in unsupported transceiver mode. | Transceivers |
| 16.10.0020 | 256234 | YA/YB | **Symptom**: The `show rmon statistics <port no>` command returns the wrong counter values.<br>**Scenario**: This issue occurred when the `clear statistics global` or `clear statistics <port no>` was executed first and then `show rmon statistics <port no>`. | CLI |
| 16.10.0020 | 256233 | YA/YB | **Symptom**: Client ports may encounter packet drops when multicast sources stream video over 500 Mbps.<br>**Scenario**: This issue can occur when multiple clients from different ports subscribed to the same group, which streams using HD channels requiring high bandwidth. TX drops can occur when several clients change channels simultaneously.<br>**Workaround**: Lower the bandwidth of the video streams to below 500 Mbps in order to avoid over-subscription of ports. | IGMP-NG |
| 16.10.0020 | 256310 | YA/YB | **Symptom**: The switch fails to update the IDEVID_CERT certificate when it is about to expire.<br>**Scenario**: This issue occurred when a switch with an expiring IDEVID CERT certificate that is provisioned in Aruba Central is rebooted.<br>**Workaround**: Execute the command `activate provision force` to update the certificate manually. | Central Integration |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0020 | 256205 | YA/YB | **Symptom**: A configuration template push from Aruba Central fails.<br>**Scenario**: This issue occurred when the end devices are connected to ports that are configured with `port-security learn-mode static`. | Central Integration |
| 16.10.0019 | 256121 | YA/YB | **Symptom**: Web authentication fails when the switch is managed by Aruba Central (`aruba-central support-mode disable`).<br>**Scenario**: This issue occurred when the switch was connected to Aruba Central and `aruba-central support-mode` was disabled.<br>**Workaround**: Execute `aruba-central support-mode enable` command so the switch is longer managed by Aruba Central. | Web Authentication |
| 16.10.0018 | 255819 | YA/YB | **Symptom**: A switch crashes with a message similar to the following:<br>`SubSystem 100 went down: Health Monitor: Read Error Restr Mem Access`<br>**Scenario**: This issue occurred because of the following actions:<br>1. An AP was authenticated with 802.1X `port mode`.<br>2. The AP was rebooted, and the 802.1X authentication configuration was removed from the port. | 802.1X |
| 16.10.0018 | 255940 | YA/YB | **Symptom**: A switch crashes with a message similar to the following:<br>`Software exception at svc_misc.c:1088 - in 'mDHCPClint' -> Failed to malloc 9202 bytes.`<br>**Scenario**: This issue occurred when the switch attempted to reconnect to Aruba Central. | Aruba Central |
| 16.10.0018 | 255995 | YA/YB | **Symptom**: A switch crashes when the `show port-access clients` command is issued or when an `SNMP GET` operation is performed to get the MIB object `hpicfUsrAuthMacAuthSessionStatsEntry`.<br>**Scenario**: The switch crashed when a MAC-authenticated client had a username of more than 40 characters. | Authentication |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0018 | 255120 | YA/YB | **Symptom/Scenario**: The Key Expansion Module of a Cisco 8851 phone does not power up.<br>**Workaround**: Configure `poe-allocate-by` command with `class` parameter on the ports, and reduce the number of powered devices connected to the switch. | PoE |
| 16.10.0018 | 256034 | YA/YB | **Symptom**: SNMP MIB files are not reachable, and the MIB file returns some errors.<br>**Scenario**: This issue occurred when the customer used an SNMP monitoring tool to read or parse the MIB files. | SNMP |
| 16.10.0018 | 256050 | YA/YB | **Symptom**: A switch crashes when the **WebUI Security > Clientspage** is accessed.<br>**Scenario**: The switch crashed when a MAC-authenticated client had a username of more than 40 characters. | Web UI |
| 16.10.0017 | 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 |
| 16.10.0017 | 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.<br>`Invalid input: grep usage error.`<br>**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.<br>**Workaround**: Do not use the pipe character (\|) in the command input for the configuration commands. | Configuration |
| 16.10.0017 | 255195 | YA/YB | **Symptom**: The switch memory utilization spikes and might reach to 100%.<br>**Scenario**: This issue occurred when many ports were monitored and mirrored to one port.<br>**Workaround**: Disable mirroring on the ports. | Mirroring |
| 16.10.0017 | 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 |
| 16.10.0017 | 255760 | YA/YB | **Symptom/Scenario**: A switch crashes with the following message:<br>`Software exception at bsp_` | Tunneled Node |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | `interrupts.c:90 - in 'fault_handler'.` | |
| 16.10.0016 | 255682 | YA/YB | **Symptom**: The RADIUS accounting packets sent from the switch to the RADIUS server do not contain the correct client IP address.<br>**Scenario**: This issue occurred when both user authentication and MAC authentication were configured. | 802.1X |
| 16.10.0016 | 255400 | YA/YB | **Symptom**: The switch is unable to connect to Activate or Aruba Central.<br>**Scenario**: This issue occurred when the `show crypto pki ta-profile` command displayed `Pending Root Certificate In...` for the `GEOTRUST_CA` profile, and the following event was recorded in the event log: `05222 activate: ST1-CMDR: Error connecting to the Activate server: Activate TLS connection error.` | Activate |
| 16.10.0016 | 255653 | YA/YB | **Symptom**: The switch crashes with a Non-Maskable Interrupt (NMI) event.<br>**Scenario**: The switch crashed because of the following reasons:<br>1. The switch was configured to receive a DHCP address.<br>2. The `activate provision force` command was configured on the switch.<br>3. The `no activate software-update check` command was executed. | Activate |
| 16.10.0016 | 255770 | YA/YB | **Symptom**: The switch fails to connect to Aruba Central, and the `show aruba-central` command output displays an Enrollment over Secured Transport (EST) enrollment error.<br>**Scenario**: This issue occurred when the switch software version is upgraded to version 16.10.0015.<br>**Workaround**: Downgrade to an older switch software version once the EST provisions IDEVID-CERT, you can upgrade the switch to the latest switch software version. | Central |
| 16.10.0016 | 255417 | YA/YB | **Symptom**: The switch crashes with an NMI event.<br>**Scenario**: This issue occurred when the DHCP snooping traffic was sent continuously to the switch with DHCP option 82, and the DHCP clients rebooted frequently. | DHCP Snooping |
| 16.10.0016 | 255619 | YA/YB | **Symptom**: The Ports table on the Web UI does not display all the interfaces of the switch. | Web UI |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue occurred when the Name and Id sent through LLDP contained a trailing backslash (\), and the same was configured on the port.<br>**Workaround**: Disable LLDP on the switch using the `no lldp run` command. | |
| 16.10.0015 | 255124 | YA/YB | **Symptom**: Captive portal redirection does not work.<br>**Scenario**: This issue occurred when the `ip client-tracker` command was enabled, and the VLAN where the client onboarded had the `disable layer3` command configured.<br>**Workaround**: Remove `ip client-tracker` or `disable layer3` configuration from the client VLAN. | Captive Portal |
| 16.10.0015 | 255259 | YA/YB | **Symptom/Scenario**: Executing the `show tech all` command resets the port counters in all sessions. | CLI |
| 16.10.0015 | 255134 | YA/YB | **Symptom**: Switch crashes regularly with the following message:<br>`Active/Commander system went down: eSoftware exception at msgSys.c:641 -- in 'mNSR',`<br>`-> Can't get message buffer for msgSys_recv.`<br>The event log indicates continuous removal and application of the device-profile.<br>**Scenario**: This issue occurred with a device profile for an AP enabled, with both interfaces of the AP connected to the switch through a trunk, and when the switch was rebooted.<br>**Workaround**: Disable and enable the device profile. | Device Profile |
| 16.10.0015 | 255158 | YA/YB | **Symptom**: Multicast traffic with the source IP address 0.0.0.0 floods to all ports, even with IGMP snooping enabled.<br>**Scenario**: This issue occurred when the multicast traffic was sent with a NULL IP source from a device connected to a non-querier device. | IGMP |
| 16.10.0015 | 255408 | YA/YB | **Symptom**: Unauthorized clients can connect and access the switch using the loopback address.<br>**Scenario**: This issue occurred when the `ip authorized-managers` command was configured and an unauthorized client attempted to connect to the loopback address. | IP Authorized Managers |
| 16.10.0015 | 255342 | YA/YB | **Symptom**: When an initial role is applied, clients do not attempt to reauthenticate. | RADIUS |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue occurred when the server-timeout value was less than the RADIUS request timeout.<br>**Workaround**: Configure a greater server-timeout value than the RADIUS request timeout. | |
| 16.10.0015 | 255171 | YA/YB | **Symptom**: The switch CPU spikes and the ClearPass RADIUS server shuts down.<br>**Scenario**: This issue occurred when MAC authentication used the peap-mschapv2 authentication method. As a result, Access-Request and Access-challenge messages were exchanged in a loop. | RADIUS |
| 16.10.0015 | 255067 | YA/YB | **Symptom**: Switch does not respond to Simple Network Management Protocol version 3 (SNMPv3) queries.<br>**Scenario**: This issue occurred when there was a wrong value in the boot counter. | SNMPv3 |
| 16.10.0014 | - | YA/YB | No fixes were included in version 16.10.0014. | NA |
| 16.10.0013 | 255125 | YA/YB | **Symptom**: Clients authenticated by Aruba Central are not placed in the proper VLAN.<br>**Scenario**: This issue occurred because of the following reasons:<br>■ Both MAC authentication and 802.1X are configured on the same port.<br>■ There are two clients on the port, which had a tagged membership for a VLAN, and the user role for a client had an untagged membership for the same VLAN. | Central |
| 16.10.0013 | 255062 | YA/YB | **Symptom**: User-based tunnel (802.1X) is not established when MAC authentication is also configured on the port with a different VLAN assignment.<br>**Scenario**: This issue occurred when both MAC authentication and 802.1X were configured on a port, and the 802.1X authentication contained a VLAN change. | MAC Authentication |
| 16.10.0013 | 254976 | YA/YB | **Symptom/Scenario**: The SSH, telnet, and console connections cannot be established with the switch, and the following event is recorded in the event log: `maximum user session limit reached.` | Switch Access |
| 16.10.0013 | 254780 | YA/YB | **Symptom**: When more number of MAC authentication clients (auth method: peap-mschapv2) get authenticated or reauthenticated, the following event is recorded multiple times in the event log: `PEAP SSL socket connection limit reached.` | MAC Authentication |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue occurred when more than 20 clients were authenticated or reauthenticated at the same time.<br>**Workaround**: Authenticate or reauthenticate less than 20 clients at the same time. | |
| 16.10.0013 | 254481 | YA/YB | **Symptom**: The switch CPU utilization increases to 80% or more, and CDP packet looping is observed across VLANs.<br>**Scenario**: This issue occurred when CDP pass-through was configured on two switches, which had more than one connection between them.<br>**Workaround**: Use `no cdp run` command to disable CDP globally, instead of configuring CDP mode pass-through. | CDP |
| 16.10.0012 | 254678 | YA/YB | **Symptom**: An Aruba Central connection is not established and the Error Reason returned is `TLS generic error (code: -1007).`<br>**Scenario**: This issue occurred when the switch attempted to contact Aruba Central.<br>**Workaround**: Zerorize the local certificates using `crypto pki zeroize` and activate the connection to Central again (aruba-central enable). | Central |
| 16.10.0012 | 254198 | YA/YB | **Symptom**: A switch or management module crashes with the following message:<br>`Active/Commander system went down:`<br>`...`<br>`Health Monitor: Invalid Instr Misaligned Mem Access.`<br>**Scenario**: This issue occurred when the `copy command-output show tech all tftp <ip-address> <filename>` command was executed.<br>**Workaround**: Do not execute the `copy command-output show tech all tftp <ip-address> <filename>` command. | Chassis |
| 16.10.0012 | 254096 | YA/YB | **Symptom**: The `Rx Drop Bytes` parameter in the command output for `show interface queues <port>` displays very high values for the last few ports, even though these ports were down.<br>**Scenario**: This issue occurred when the `show interface queues <port>` command was issued. | CLI |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0012 | 254278 | YA/YB | **Symptom**: The switch crashes when the `show crypto client-public-key` command is issued.<br>**Scenario**:This issue was observed when the `show crypto client-public-key` was issued when the `\t:` symbol was present in the client pub key file.<br>**Workaround**: Remove `\t:` symbol from the client public key file content. | Crypto |
| 16.10.0012 | 254395 | YA/YB | **Symptom**: The switch does not send the configured NAS-ID while sending a request to the RADIUS server.<br>**Scenario**: This issue occurred for both login and enable when the switch was configured with a non-default `server-group nas-id` and `ssh` was configured with peap-mschapv2. | Radius |
| 16.10.0012 | 254665 | YA/YB | **Symptom**: REST connection fails when a Windows client makes an HTTP request.<br>**Scenario**: This issue occurred when a Windows client sent a REST HTTP request using PowerShell. | REST |
| 16.10.0012 | 254722 | YA/YB | **Symptom/Scenario**: When a user fails to login to the switch using SSH, no SNMP trap is sent. | SNMPv2 |
| 16.10.0012 | 254393 | YA/YB | **Symptom**: Event messages are not printed on the Syslog server.<br>**Scenario**: This issue occurred when a syslog server was configured with the TCP option, `logging <IP-ADDR> tcp` and `ip source-interface syslog` was configured.<br>**Workaround**: Remove `ip source-interface syslog ...` from the config or reboot the switch after configuring syslog over TCP. | Syslog |
| 16.10.0012 | 254311 | YA/YB | **Symptom**: Gradual memory depletion on a switch is observed.<br>**Scenario**: This issue occurred when the telnet sessions were closed abruptly.<br>**Workaround**: Disable the telnet server on the switch. | Telnet |
| 16.10.0012 | 254572 | YA/YB | **Symptom**: The switch crashes with the following message: `Health Monitor: Misaligned Mem Access.`<br>**Scenario**: This issue occurred when a MAC address moved between aaa authenticated ports. | Telnet |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0011 | 253563 | YA/YB | **Symptom**: The switch crashes with the following message: `Health Monitor: Misaligned Mem Access.....Task='mWebAuth'.`<br>**Scenario**: This issue occurred when any of the 802.1X clients' MAC address had a NULL value due to corruption when authenticator configuration on a switch port was disabled. | 802.1X |
| 16.10.0011 | 254333, 254339 | YA/YB | **Symptom**: Switch crashes with a message similar to the following: `Software exception at trlock.c -- in 'InetServer'.`<br>**Scenario**: This issue occurred when the `show tech all` command was executed from Aruba Central.<br>**Workaround**: Execute the `show tech all` command through the switch CLI. | Central |
| 16.10.0011 | 254255 | YA/YB | **Symptom**: Switch crashes with a message similar to the following: `Software exception at multMgmtUtil.c -- in 'mOobmCtrl'.`<br>**Scenario**: This issue occurred when continuous or frequent `cfg-restore` operations (with password or aaa authentication related configurations) were executed, and in parallel, the switch was accessed through local-authentication.<br>**Workaround**: Do not access the switch using local-authentication when `cfg-restore` operation is in progress. | Chassis |
| 16.10.0011 | 253803 | YA/YB | **Symptom**: SSH connection (Remote Console) cannot be established from Aruba Central to the switch.<br>**Scenario**: This issue occurred when `ip authorized-managers` was configured on the switch and a Remote Console connection was attempted from Aruba Central.<br>**Workaround**: Add the following configuration to the switch:<br>`ip authorized-managers 127.0.0.1 255.255.255.254 access manager` | Console |
| 16.10.0011 | 254196 | YA/YB | **Symptom**: Multicast traffic stops after a redundancy switchover.<br>**Scenario**: This issue occurred when the IGMP `query-max-response-time` was configured to be `128` seconds and a redundancy switchover was performed. | IGMP |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Workaround**: Remove IGMP from the VLAN and reconfigure the `query-max-response-time` to the default value of `10` seconds. | |
| 16.10.0011 | 253853 | YA/YB | **Symptom**: Continuous RADIUS access request packets are sent from the switch to the RADIUS server.<br>**Scenario**: This issue occurred when a MAC address limit was configured and a device was attempted to be authenticated beyond the configured limit. | MAC Authentication |
| 16.10.0011 | 253965 | YA/YB | **Symptom**: The switch closes the REST connection when the request is made from a Windows client.<br>**Scenario**: This issue occurred when a REST request was sent from PowerShell on a Windows client. | REST |
| 16.10.0011 | 252721 | YA/YB | **Symptom**: Attempts to SSH or telnet to the switch fail and the following message is displayed: `Sorry, the maximum number of telnet sessions are active. Try again later.`<br>**Scenario**: This issue occurred when a vulnerability scan was run against the switch multiple times.<br>**Workaround**: Disable Telnet server. | Switch Access |
| 16.10.0011 | 253970 | YA/YB | **Symptom**: Ports can be added to a trunk using the web interface even if those ports are configured with IGMP fastlearn.<br>**Scenario**: This issue occurred when IGMP fastlearn was configured on a few ports of the switch, and the switch was accessed through the web interface to add the IGMP fastlearn enabled ports to the trunk.<br>**Workaround**: Use the CLI to add ports to a trunk. | Web Interface |
| 16.10.0010 | 253641 | YA/YB | **Symptom**: Clients that do not match an allowed entry in an ACL are not implicitly denied and are able to access the network.<br>**Scenario**: This issue occurred when a user-role was configured containing a policy that allowed network access to only select IP addresses.<br>**Workaround**: Create an ACL that specifically denies access to particular IP addresses. | ACLs |
| 16.10.0010 | 253807 | YA/YB | **Symptom**: Unsupported values are accepted as ACL numbers for both standard and extended ACLs when configuring ACLs from the REST interface (for example, Aruba Central). Once configured, these ACLs cannot be deleted using REST or the CLI.<br>**Scenario**: This issue occurred when the REST interface was used to configure an ACL with an unsupported value. | ACLs |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0010 | 253425 | YA/YB | **Symptom**: The username sent for a successful MAC-authenticated client is the MAC address, rather than the username.<br>**Scenario**: This issue occurred when a client was authenticated using MAC authentication. | Authentication |
| 16.10.0010 | 253422 | YA/YB | **Symptom**: When a `show` command is executed using `\| include <anyword> <anyword>` the following error message is displayed: `Invalid Input : grep usage error.`<br>**Scenario**: This issue occurred when a `show` command was executed using `\| include <anyword> <anyword>`.<br>**Workaround**: Execute the `show` command without `\| include <anyword> <anyword>`. | CLI |
| 16.10.0010 | 253303 | YA/YB | **Symptom**: Peer device does not get an IP address when the port it is connected to is configured using a device-profile.<br>**Scenario**: This issue occurred when a port is configured using device profile and a peer device is connected to it.<br>**Workaround**:Disable device-profile and manually configure the port. | Device Profile |
| 16.10.0010 | 253557 | YA/YB | **Symptom**: Using REST to retrieve the resource identifier `/lldp/remote-device` fails to display the IPv4 address of the neighbor.<br>**Scenario**: This issue occurred when the REST resource operation GET was used to retrieve the data associated with `/lldp/remote-device`. | REST |
| 16.10.0010 | 252993 | YA/YB | **Symptom**: Some RADIUS accounting packets sent to the RADIUS server have a very large size.<br>**Scenario**: This issue occurred when a downloadable user role was configured with a user policy, network accounting was enabled, and a client was authenticated. | RADIUS |
| 16.10.0010 | 253736 | YA/YB | **Symptom**: Disconnect Change of Authorization (CoA) request is not honored.<br>**Scenario**: This issue occurred when the radius-server group was configured, a client was authenticated, and a disconnect CoA request with the default nas-id was sent.<br>**Workaround**: Configure `aaa server-group radius <Group name> nas-id <NAS-ID>` where the NAS-ID matches the NAS Identifier value shown in the output of the `show radius authentication` command. | RADIUS |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0010 | 253789 | YA/YB | **Symptom**: Switch serial number contains an extra space at the end when it is read using SNMP.<br>**Scenario**: This issue occurred when the switch serial number was read using SNMP.<br>Example:<br>MIB OID: 1.3.6.1.2.1.47.1.1.1.1.11.1<br>MIB File: ENTITY-MIB | SNMP |
| 16.10.0010 | 253342 | YA/YB | **Symptom**: SSH/Telnet/Console connections to the switch fail with an error message: `Maximum session limit is reached.`<br>**Scenario**: This issue occurred when multiple users logged in and out and RADIUS was configured as the primary authentication method.<br>**Workaround**: Reboot the switch. | Switch Access |
| 16.10.0010 | 253407 | YA/YB | **Symptom**: Unable to log in to the switch using TACACS credentials.<br>**Scenario**: This issue occurred when a source interface for TACACS was configured using the `ip source-interface tacacs` command and the switch was upgraded to 16.10.0009. | TACACS |
| 16.10.0010 | 253290 | YA/YB | **Symptom**: Switch crashes when it is accessed through the web interface.<br>**Scenario**: This issue occurred when the switch was accessed using the web interface and RADIUS authentication was configured for web access.<br>**Workaround**: Disable RADIUS authentication for web access. | Web UI |
| 16.10.0010 | 253877 | YA/YB | **Symptom**: The **WebUI Security > Clients** page displays incorrect MAC addresses, which results in the user role, IP address, and status columns to be empty.<br>**Scenario**: This issue occurred when a few workstations with higher value MAC addresses (for example, 9c:dc:71:fb:77:fe) are connected to the last ports of a 2930 stack or the last module of a 5400R. | Web UI |
| 16.10.0009 | 252885 | YA/YB | **Symptom**: Switch appears down in Aruba Central.<br>**Scenario**: This issue occurred because the system time was set to the year 2036, though NTP sync was successful, and the switch was connected to Aruba Central.<br>**Workaround**: Configure an NTP server in the switch. | Activate |
| 16.10.0009 | 252226 | YA/YB | **Symptom**: Switch does not respond during the ZTP process.<br>**Scenario**: This issue occurred when connecting to the switch using SSH, while Airwave was transferring the configuration to the switch. | AirWave |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0009 | 251418 | YA/YB | **Symptom**: Pushing a switch configuration template from Aruba Central fails and a 500 error code is returned.<br>**Scenario**: This issue occurred when a configuration template that had no untagged ports in VLAN 1 was pushed from Aruba Central.<br>**Workaround**: In the configuration template, add at least one untagged port in VLAN 1. | Central |
| 16.10.0009 | 253174 | YA/YB | Symptom/Scenario: The switch experienced an NMI crash with the following message: `Task='ewsCloudRcv'.` | Central |
| 16.10.0009 | 253276 | YA/YB | **Symptom**: Unable to copy crash-files, core-dump, and the `show tech all` command output from the switch.<br>**Scenario**: This issue occurred when executing the `copy` command with an invalid IP address, file name, hostname, or when parallelly executing the `copy` command in other sessions.<br>**Workaround**:<br>■ Copy the core file from the web interface.<br>■ Copy the `show tech all` command output from the console interface. | CLI |
| 16.10.0009 | 252833 | YA/YB | **Symptom**: MSTP does not work as expected and does not block ports when it should.<br>**Scenario**: This issue occurred when two ports in a loop were in a forwarding state with MSTP and port-security non-default learn mode enabled.<br>**Workaround**: Disable port-security. | Spanning Tree |
| 16.10.0009 | 252613 | YA/YB | **Symptom**: Unable to connect to the switch using SSH.<br>**Scenario**: This issue occurred when the switch is configured to use TACACS and a malformed TACACS packet is received by the switch.<br>**Workaround**: Reboot the switch. | SSH |
| 16.10.0009 | 251966 | YA/YB | **Symptom**: The switch sends logging events with a "Z" at the end of the timestamp when the it is not configured to use UTC.<br>**Scenario**: This issue occurred when the switch sent syslog messages over TLS. | Syslog |
| 16.10.0009 | 252443 | YA/YB | **Symptom/Scenario**: The Reboot button is displayed for a few seconds in the Web UI. Clicking it allowed an operator to reboot the switch. | Web UI |
| 16.10.0008 | - | YA/YB | Version 16.10.0008 was never released. | - |
| 16.10.0007 | 252007 | YA/YB | **Symptom**: The switch sends an incorrect CLASS attribute value in the RADIUS accounting packet. | Accounting |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: When the CLASS attribute is updated during re-authentication of a MAC-authenticated client session, the switch fails to send the new CLASS attribute value in the RADIUS accounting packet.<br>**Workaround**: Force a new client authentication session by disabling/enabling the port after the CLASS attribute value changes. | |
| 16.10.0007 | 251273 | YA/YB | **Symptom**: The switch incorrectly places clients in the configured authorized VLAN (auth-vid).<br>**Scenario**: When using chap-radius authorized option, if the route to the RADIUS server is not resolved during the switch boot up, clients are incorrectly placed in the configured authorized VLAN (auth-vid) rather than the guest VLAN (unauth-vid) or initial-role.<br>**Workaround**: Reauthenticate the affected clients. | Authentication |
| 16.10.0007 | 251927 | YA/YB | **Symptom**: The switch fails to remove CDP configuration for a port.<br>**Scenario**: When a port is added to a trunk interface, the switch fails to remove the previous non-default CDP configuration for that port (example: no cdp enable <PORT-NUM>).<br>**Workaround**: Remove the non-default CDP configuration from the individual port before adding it to trunk interface. | CDP |
| 16.10.0007 | 252053 | YA/YB | **Symptom/Scenario**: The switch crashes with an error message similar to:<br>`Software exception in ISR at pvDmaV1Rx.c <...> ASSERT: No resources available!.` | Central |
| 16.10.0007 | 252267 | YA/YB | **Symptom**: The switch experiences high CPU utilization.<br>**Scenario**: In conditions of low network bandwidth or network congestion that cause frequent disconnections from the Aruba Central Portal, the switch experiences high CPU utilization while attempting to reconnect to Aruba Central and while being managed by other NMS applications such as Solarwinds at the same time.<br>**Workaround**: Use only one NMS application to manage the switch if network bandwidth capacity or congestion cannot be improved. | Central |
| 16.10.0007 | 251876 | YA/YB | **Symptom**: The switch may fail to apply the correct VLAN to dynamic trunks.<br>**Scenario**: After a reboot of a switch configured for dynamic trunks with device profile enabled on ports, the switch may fail to apply the correct VLAN configured in the device-profile, after the port is joined to the dynamic trunk. | Dynamic Trunks |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Workaround**: Disable and enable device-profile. | |
| 16.10.0007 | 251972 | YA/YB | **Symptom**: Some clients using the PEAP authentication mechanism are not successfully authenticated.<br>**Scenario**: When concurrent authentication requests are sent to the switch using peap-mschapv2, some clients may not be successfully authenticated, even though ACCESS ACCEPT is sent from the RADIUS server. | MAC Authentication |
| 16.10.0007 | 252131 | YA/YB | **Symptom**: REST API calls may experience some slight delay in execution response.<br>**Scenario**: When multiple REST API commands are executed over the same HTTPS session, they may experience a slight delay in execution response.<br>**Workaround**: Use a new HTTPS session for each REST API call. | REST |
| 16.10.0007 | 251475 | YA/YB | **Symptom**: The switch experiences high CPU utilization and possible console connectivity issues.<br>**Scenario**: When configuring or modifying aggregated interfaces (trunks) with more than 3 member ports on a switch where there is a very high number of configured VLANs, the switch experiences high CPU utilization and possible console connectivity issues while applying the configuration. | VLAN |
| 16.10.0007 | 251505 | YA/YB | **Symptom**: The WebUI contains an XSS vulnerability.<br>**Scenario**: Configure the editable parameters in the WebUI with values that can cause an XSS attack. | Web UI |
| 16.10.0007 | 251524 | YA/YB | **Symptom**: The switch fails to display some ports on the Ports page of the WebUI.<br>**Scenario**: When aSysName with trailing zeroes is received in the LLDP packet from a neighboring device, the switch fails to list some ports in the Ports page when using the WebUI.<br>**Workaround**: To get the information for all ports use one of the following options:<br>■ Disable LLDP on the port where the device with `invalidSysName` is connected.<br>■ Use the traditional web UI to get the information for the affected/missing ports.<br>■ Use switch CLI commands to get the information for the affected/missing ports. | Web UI |
| 16.10.0006 | - | YA/YB | Version 16.10.0006 was never released. | - |
| 16.10.0005 | - | YA/YB | Version 16.10.0005 was never released. | - |
| 16.10.0004 | - | YA/YB | Version 16.10.0004 was never released. | - |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0003 | 251317 | | **Symptom**: A Windows client that joins a domain other than the one defined in Cisco ISE fails to authenticate. The client will also wait more than 5 minutes before attempting MAC address authentication.<br>**Scenario**: This issue is observed when MAC and 802.1X authentication are enabled on the port and the configured auth-order is 802.1X-MAC and an initial role. | 802.1X |
| 16.10.0003 | 251280 | YA/YB | **Symptom**: Deploying a switch template through Airwave/Aruba Central fails.<br>**Scenario**: This issue is observed when the IP address from VLAN1 is removed from a new configuration template and is pushed to the switch with the "ntpserver-name <server name>".<br>**Workaround**: Do not remove the IP address from VLAN 1 in the new template. | Central |
| 16.10.0003 | 250816 | YA/YB | **Symptom**: Authenticated users are disconnected from the switch.<br>**Scenario**: This issue is observed when users disable and enable the interface which connects to the dhcp- relay switch, after configuring the DHCP server, DHCP relay, and DHCP snooping with ip-source lockdown.<br>**Workaround**: Disable ip-source lockdown. | DIPLD |
| 16.10.0003 | 251615 | YA/YB | **Symptom**: An attacker is able to obtain sensitive data without providing valid login credentials after a successful REST query.<br>**Scenario**: This issue is observed when web management is enabled on the switch. | REST |
| 16.10.0003 | 251506 | YA/YB | **Symptom**: The switch manager password is altered to an attack-controlled value.<br>**Scenario**: This issue is observed when the user clicks a malicious hyperlink. | Web UI |
| 16.10.0003 | 251314 | YA/YB | **Symptom**: Switches appear offline in Aruba Central.<br>**Scenario**: This issue is observed after the switch software is upgraded from 16.04 to 16.08.<br>**Workaround**: Reboot the switch. | ZTP |
| 16.10.0002 | 250681 | YA/YB | **Symptom/Scenario**: The Topology section of Airwave shows spanning tree details for a switch that does not have spanning tree enabled. | AirWave |
| 16.10.0002 | 251313 | YA/YB | **Symptom**: The switch experiences a high CPU utilization and loses connection with Central.<br>**Scenario**: when the switch is upgraded to 16.08.0001 and a template with `tls` and `cwmp` commands is pushed from Central, the switch experiences high CPE utilization and loses the connection to Aruba Central. | Central |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Workaround**: Remove tls application cloud lowest-version tls1.2 and cwmp from the switch template. | |
| 16.10.0002 | 250600 | YA/YB | **Symptom/Scenario**: The help text for the `device-identity lldp oui` command indicates that the required input is a MAC-OUI. | Device finger printing |
| 16.10.0002 | 250392 | YA/YB | **Symptom**: The switch crashes with a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access.`<br>**Scenario**: After an IP address has been reassigned from one VLAN to another VLAN using the menu interface, the switch may crash with a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access.`<br>**Workaround**: Disable the first VLAN and save the configuration from the menu interface. Then, configure the deleted IP address on the second VLAN. | Menu |
| 16.10.0002 | 245830 | YA/YB | **Symptom**: The switch fails to list the switch ports in the Ports web management page.<br>**Scenario**: When a peer device that advertises information in LLDP has a sysName string with special characters, the switch fails to display the port list table on the Ports web management page.<br>**Workaround**: Remove the special characters from the peer device sysName or use CLI commands to get specific port information. | Next Gen GUI |
| 16.10.0002 | 250995 | YA/YB | **Symptom**: Speed-duplex configuration on the port is lost.<br>**Scenario**: After configuring an HPE X121 1G SFP LC SX Transceiver ( J4858C) to 1000-full and rebooting the switch, the speed-duplex configuration on the port is lost. | Transceivers |
| 16.10.0002 | 250896 | YA/YB | **Symptom**: Switch ports are not listed in the web interface.<br>**Scenario**: If a peer device advertises an LLDP port ID containing special characters, switch ports are not listed in the web interface. | Web UI |
| 16.10.0001 | 250681 | YA/YB | **Symptom/Scenario**: The Topology section of Airwave shows spanning tree details for a switch that does not have spanning tree enabled. | AirWave |
| 16.10.0001 | 250600 | YA/YB | **Symptom/Scenario**: The help text for the `device-identity lldp oui` command indicates that the required input is a MAC-OUI. | Device identity |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0001 | 250392 | YA/YB | **Symptom**: The switch crashes with a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access.`<br>**Scenario**: After an IP address has been reassigned from one VLAN to another VLAN using the menu interface, the switch may crash with a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access.`<br>**Workaround**: Disable the first VLAN and save the configuration from the menu interface. Then, configure the deleted IP address on the second VLAN. | Menu |
| 16.10.0002 | 250995 | YA/YB | **Symptom**: Speed-duplex configuration on the port is lost.<br>**Scenario**: After configuring an HPE X121 1G SFP LC SX Transceiver ( J4858C) to 1000-full and rebooting the switch, the speed-duplex configuration on the port is lost. | Transceivers |
| 16.10.0001 | 245830 | YA/YB | **Symptom**: The switch fails to list the switch ports in the `Ports` web management page.<br>**Scenario**: When a peer device that advertises information in LLDP has a sysName string with special characters, the switch fails to display the port list table on the Ports web management page.<br>**Workaround**: Remove the special characters from the peer device sysName or use CLI commands to get specific port information. | Web UI |
| 16.10.0001 | 250896 | YA/YB | **Symptom**: Switch ports are not listed in the web interface.<br>**Scenario**: If a peer device advertises an LLDP port ID containing special characters, switch ports are not listed in the web interface. | Web UI |

# Upgrade Information

## Upgrading Restrictions and Guidelines

YA/YB.16.10.0009 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.16.10 branch of the software.
Version YC.16.10.0001 is the initial build of Major version YC.16.10 software. YC.16.10.0020 includes all enhancements and fixes in the YC.16.10.0019 software, plus the additional enhancements and fixes in the YC.16.10.0020 enhancements and fixes sections of this release note.

This release applies to the following Aruba 2540 Switch Series:

**Table 16:** *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 17:** *Enhancements*

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0020 | YC | No enhancements were included in version 16.10.0020. | NA |
| 16.10.0019 | YC | No enhancements were included in version 16.10.0019. | NA |
| 16.10.0018 | YC | No enhancements were included in version 16.10.0018. | NA |
| 16.10.0017 | 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.<br>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. | Security |

| Version | Software | Description | Category |
|---|---|---|---|
| | | A MIB has also been added to enable or disable the randomization of TCP timestamp offsets.<br>Refer to the *Aruba 2540 Management and Configuration Guide for AOS-S Switch 16.10* and *Aruba MIB and Trap Support Matrix for AOS-S Switch 16.10* for more information. | |
| 16.10.0016 | YC | Added support for the new SSH data integrity algorithm hmac-sha2-256, which is defined in RFC 6668.<br>Refer to the *Aruba 2540 Access Security Guide for AOS-S Switch 16.10* and *Aruba 2540 IPv6 Configuration Guide for AOS-S Switch 16.10* for more information. | SSH |
| 16.10.0016 | YC | Added support to configure the size of the EAP-TLS fragments sent from the switch to the RADIUS server. Configuring EAP-TLS fragment size based on the MTU of the network avoids IP fragmentation in the network, and thus, the fragmented packets will not be dropped by the firewall or gateways.<br>Added a MIB to indicate the maximum size of the EAP-TLS fragment sent to the RADIUS server.<br>Refer to the *Aruba 2540 Access Security Guide for AOS-S Switch 16.10* and *Aruba MIB and Trap Support Matrix for AOS-S Switch 16.10* for more information. | EAP-TLS Fragmentation |
| 16.10.0015 | YC | No enhancements were included in version 16.10.0015. | NA |
| 16.10.0014 | YC | No enhancements were included in version 16.10.0014. | NA |
| 16.10.0013 | YC | No enhancements were included in version 16.10.0013. | NA |
| 16.10.0012 | YC | Added `concise` parameter to display port-access and spanning-tree attributes in a consolidated format, when executing `show config` and `show running-config` commands. | Enhancement for `show config` and `show running-config` commands |
| 16.10.0012 | YC | Added support to enable SNMP traps for a specified event. This helps to filter out particular traps from all SNMP trap messages.<br>**Syntax:** `snmp-server enable traps event-list <EVENT-LIST-STR>` | Customization for SNMP Traps |
| 16.10.0012 | YC | Added `recv-disable`parameter to configure loop-protect from blocking the receiving port when a loop is detected.<br>**Syntax:** `no loop-protect <PORT-LIST> receiver-action [recv-disable]` | Configuration for loop-protect receiver-action |
| 16.10.0011 | YC | Added support to format MAC address in upper case for the Called and Calling Station IDs.<br>Refer to the *Access Security Guide* for more information. | Port Access Enhancement |
| 16.10.0011 | YC | Added support to include the Port VLAN information in RADIUS access request for all authentication types.<br>Refer to the *Access Security Guide* for more information. | Port Access Enhancement |

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0011 | YC | Added support to enable AES 256-bit encryption for SNMP. Refer to the *Management and Configuration Guide* for more information. | AES 256-bit encryption for SNMP |
| 16.10.0011 | YC | Added support to configure a prefix string along with the switch IP address or hostname in the logs sent to the Syslog servers. This helps to classify and group log entries based on the string value.<br>**Syntax:** `logging prefix <ASCII-STR>`<br>Refer to the *Management and Configuration Guide* for more information. | Syslog Enhancement |
| 16.10.0010 | YC | Added support to provide the option to specify the source interface or VLAN for Central connectivity. The existing IP source-interface command is enhanced to override current configuration check for provisioning using Aruba Activate. Refer to the *Management and Configuration Guide* for more information. | Source interface option for Central connectivity |
| 16.10.0010 | YC | Added support to allow more PoE devices to be connected to the switch by using `poe-alloc-by-usage` when using Device Profiles. This can be based on either **Usage** or **Class**. Default allocation will be based on **Class**.<br>Refer to the *Management and Configuration Guide* for more information. | Device Profile Enhancement |
| 16.10.0010 | YC | Added support to work with the default setting in OpenSSH 8.2 by choosing an inherently more secure algorithm as the default on the switch for SSH communication. Refer to the *Access Security Guide* for more information.<br>The list of new Host-Key algorithms are as follows:<br>■ rsa-sha2-512<br>■ rsa-sha2-256<br>The list of new SSH KEX algorithms are as follows:<br>■ ecdh-sha2-nistp521<br>■ ecdh-sha2-nistp381<br>■ ecdh-sha2-nistp256<br>■ diffie-hellman-group-exchange-sha256 | Support for OpenSSH 8.2 |
| 16.10.0009 | YC | Added support for the manager password enforcement to ensure that the switch prompts the user to configure the manager password on the switch before configuring any other features. If the manager password is not configured, then the user will have read-only access to the switch. This is applicable only to switches with factory default configuration. Refer to the *Access Security Guide* for more information. | Manager Password Enforcement |
| 16.10.0009 | YC | Added support to enable MAC pinning. This feature allows administrators to let clients stay authenticated to the switch by disabling the log-off period associated with the client.<br>Refer to the *Access Security Guide* for more information. | MAC Pinning |

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0009 | YC | Added support to enhance the payload size for the REST API interfaces. The increased payload size for 3810M and 54xxR platforms is 1024K.<br>Refer to the *REST API Guide* for more information. | REST API Payload Enhancement |
| 16.10.0009 | YC | Added support for Server Name Indication (SNI), which is a TLS extension defined in RFC 6066. This feature is enabled by default to include the SNI extension in the Client Hello sent from the switch to all the TLS client applications. Refer to the *Access Security Guide* for more information. | Server Name Indication for TLS |
| 16.10.0008 | YC | Version 16.10.0008 was never released. | NA |
| 16.10.0007 | YC | ■ Added additional support for pipe "\|" option to grep for pattern match the output of CLI commands, such as:<br>◦ Case-insensitive option to allow a case insensitive pattern match<br>◦ Up to four consecutive pattern matches in one CLI command<br>■ Added support for a per-session based command to wrap column display in the CLI output using session wrap-text option when its length is exceeding the column width.<br>Refer to the *Management and Configuration Guide* for more information. | CLI |
| 16.10.0007 | YC | Added the following REST enhancements:<br>■ Support for ARP table data.<br>■ Support for primary VLAN.<br>■ Support for reserved-vlan and clearpass options to configure dynamic segmentation.<br>■ REST API schema moved under `device-rest-api/services/server.html`.<br>Refer to the *REST API Guide* for more information. | REST |
| 16.10.0007 | YC | Added support for the new activate endpoint `devices-v2.arubanetworks.com` which has the following two major differences compared to the old end point device.arubanetworks.com:<br>■ It works on the standard TLS handshake mechanism and uses mutual authentication.<br>■ It uses certificates issued by HP CA for establishing TLS connections.<br>Zero Touch Provisioning (ZTP) improvements were made to deal with situations such as unresponsive DNS servers. Refer to the *Management and Configuration Guide* for more information. | Zero Touch Provisioning |
| 16.10.0006 | YC | Version 16.10.0006 was never released. | NA |
| 16.10.0005 | YC | Version 16.10.0005 was never released. | NA |

| Version | Software | Description | Category |
|---|---|---|---|
| 16.10.0004 | YC | Version 16.10.0004 was never released. | NA |
| 16.10.0003 | YC | New command `aaa accounting session-id include-switch-identity` was added. When this command is invoked, an accounting session ID is generated with Switch Base MAC, Client MAC, and Timestamp for network accounting type. The other accounting types (exec, system, commands) do not include Client MAC and hence the session ID is generated with Switch Base MAC, Track ID, and Timestamp.<br>If the same client is accessing the network from multiple switches, then the accounting session ID can be duplicated. This caused issues in ClearPass Policy Manager where client insertion in the database failed with an error similar to Integrity Error: `acct_id, calling_station_id` violates check constraint. This new command alleviates that problem. | AAA |
| 16.10.0003 | YC | This enhancement will only be in effect if the CoA/Disconnect request has a message authenticator attribute in request packet. The message authenticator attribute is used to verify the integrity (HMAC-MD5) of the RADIUS packet. This is an optional attribute in the Access/CoA/Disconnect packet. If the received packet has this attribute in the RADIUS packet, the receiver will validate the integrity value and discard it if the value is incorrect. | RADIUS |
| 16.10.0002 | YC | An event is added to the log when the switch experiences an over temperature condition. | Event Log |
| 16.10.0001 | YC | No enhancements were included in version 16.10.0001. | NA |

# 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 18:** *Fixed Issues*

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0020 | 256274 | YC | **Symptom/Scenario**: VSF Stack Member crashed with a message similar to the following: `Software exception at lava_chassis_slot_sm.c:3626 - in 'eChassMgr', task ID = 0x37b07bc0.` | VSF |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0020 | 256257 | YC | **Symptom/Scenario**: Certain transceivers had link issues in unsupported transceiver mode. | Transceivers |
| 16.10.0020 | 256234 | YC | **Symptom**: The `show rmon statistics <port no>` command returns the wrong counter values.<br>**Scenario**:This issue occurred when the command `clear statistics global` or `clear statistics <port no>`was first executed and then `show rmon statistics <port no>`. | CLI |
| 16.10.0020 | 256233 | YC | **Symptom**: Client ports may encounter packet drops when multicast sources stream video over 500 Mbps.<br>**Scenario**: This issue can occur when multiple clients from different ports subscribed to the same group, which streams using HD channels requiring high bandwidth. TX drops can occur when several clients change channels simultaneously.<br>**Workaround**: Lower the bandwidth of the video streams to below 500 Mbps in order to avoid over-subscription of ports. | IGMP-NG |
| 16.10.0020 | 256205 | YC | **Symptom**: A configuration template push from Aruba Central fails.<br>**Scenario**: This issue occurred when the end devices are connected to ports that are configured with `port-security learn-mode static`. | Central Integration |
| 16.10.0019 | 256121 | YC | **Symptom**: Web authentication fails when the switch is managed by Aruba Central (`aruba-central support-mode disable`).<br>**Scenario**: This issue occurred when the switch was connected to Aruba Central and `aruba-central support-mode` was disabled.<br>**Workaround**: Execute `aruba-central support-mode enable` command so the switch is longer managed by Aruba Central. | Web Authentication |
| 16.10.0018 | 256037 | YC | **Symptom**: Clients are not authenticated on a switch port.<br>**Scenario**: This issue occurred when multiple clients were connected to a single port (for example, a Personal Computer (PC) was connected to a phone), both MAC authentication and 802.1X authentication methods were attempted at the same time on the PC, and both the authentication methods used the same user role attribute.<br>**Workaround**: Configure the `auth-order` parameter first with `authenticator`, and then with `mac-based`. | 802.1X |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0018 | 255928 | YC | **Symptom/Scenario**: A switch is unable to connect to Aruba Central. | Aruba Central |
| 16.10.0018 | 255940 | YC | **Symptom**: A switch crashes with a message similar to the following:<br>`Software exception at svc_misc.c:1088 - in 'mDHCPClint'`<br>`-> Failed to malloc 9202 bytes.`<br>**Scenario**: This issue occurred when the switch attempted to reconnect to Aruba Central. | Aruba Central |
| 16.10.0018 | 255995 | YC | **Symptom**: A switch crashes when the `show port-access clients` command is issued or when an `SNMP GET` operation is performed to get the MIB object `hpicfUsrAuthMacAuthSessionStatsEntry`.<br>**Scenario**: The switch crashed when a MAC-authenticated client had a username of more than 40 characters. | Authentication |
| 16.10.0018 | 256016 | YC | **Symptom**: When a private VLAN is configured on a switch, the traffic from the secondary VLAN does not reach the primary VLAN.<br>**Scenario**: This issue occurred when the switch was rebooted, and the secondary VLAN contained a tagged trunk or Link Aggregation Control Protocol (LACP) port.<br>**Workaround**: Remove and add the tagged trunk or LACP configuration to the secondary VLAN. | Private VLAN |
| 16.10.0018 | 256034 | YC | **Symptom**: SNMP MIB files are not reachable, and the MIB file returns some errors.<br>**Scenario**: This issue occurred when the customer used an SNMP monitoring tool to read or parse the MIB files. | SNMP |
| 16.10.0018 | 256050 | YC | **Symptom**: A switch crashes when the **WebUI Security > Clientspage** is accessed.<br>**Scenario**: The switch crashed when a MAC-authenticated client had a username of more than 40 characters. | Web UI |
| 16.10.0017 | 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 |
| 16.10.0017 | 255882 | YC | **Symptom**: When a switch fails to connect to Aruba Central, the switch configuration rolls back.<br>**Scenario**: This issue occurred when the connection between the switch and Aruba Central was lost. | Aruba Central |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0017 | 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.<br>`Invalid input: grep usage error`<br>**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.<br>**Workaround**: Do not use the pipe character (\|) in the command input for the configuration commands. | Configuration |
| 16.10.0017 | 255195 | YC | **Symptom**: The switch memory utilization spikes and might reach to 100%.<br>**Scenario**: This issue occurred when many ports were monitored and mirrored to one port.<br>**Workaround**: Disable mirroring on the ports. | Mirroring |
| 16.10.0017 | 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 |
| 16.10.0017 | 255760 | YC | **Symptom/Scenario**: A switch crashes with the following message:<br>`Software exception at bsp_interrupts.c:90 - in 'fault_handler'.` | Tunneled Node |
| 16.10.0016 | 255682 | YC | **Symptom**: The RADIUS accounting packets sent from the switch to the RADIUS server do not contain the correct client IP address.<br>**Scenario**: This issue occurred when both user authentication and MAC authentication were configured. | 802.1X |
| 16.10.0016 | 255400 | YC | **Symptom**: The switch is unable to connect to Activate or Aruba Central.<br>**Scenario**: This issue occurred when the `show crypto pki ta-profile` command displayed `Pending Root Certificate In...` for the `GEOTRUST_CA` profile, and the following event was recorded in the event log:<br>`05222 activate: ST1-CMDR: Error connecting to the Activate server: Activate TLS connection error` | Activate |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0016 | 255653 | YC | **Symptom**: The switch crashes with a Non-Maskable Interrupt (NMI) event.<br>**Scenario**: The switch crashed because of the following reasons:<br>1. The switch was configured to receive a DHCP address.<br>2. The `activate provision force` command was configured on the switch.<br>3. The `no activate software-update check` command was executed. | Activate |
| 16.10.0016 | 255719 | YC | **Symptom**: The IP address of the next server is not present in the DHCP response packet.<br>**Scenario**: This issue occurred when the DHCP server with option 66 and option 150 was configured in the server pool. | DHCP Server |
| 16.10.0016 | 255417 | YC | **Symptom**: The switch crashes with an NMI event.<br>**Scenario**: This issue occurred when the DHCP snooping traffic was sent continuously to the switch with DHCP option 82, and the DHCP clients rebooted frequently. | DHCP Snooping |
| 16.10.0016 | 255586 | YC | **Symptom**: Running configuration does not display the local user roles.<br>**Scenario**: The issue occurred when the switch was configured to use both downloadable and local user roles.<br>**Workaround**: Reboot the switch. | User Roles |
| 16.10.0016 | 255619 | YC | **Symptom**: The Ports table on the Web UI does not display all the interfaces of the switch.<br>**Scenario**: This issue occurred when the Name and Id sent through LLDP contained a trailing backslash (\), and the same was configured on the port.<br>**Workaround**: Disable LLDP on the switch using the `no lldp run` command. | Web UI |
| 16.10.0015 | 255124 | YC | **Symptom**: Captive portal redirection does not work.<br>**Scenario**: This issue occurred when the `ip client-tracker` command was enabled, and the VLAN where the client onboarded had the `disable layer3` command configured.<br>**Workaround**: Remove `ip client-tracker` or `disable layer3` configuration from the client VLAN. | Captive Portal |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0015 | 255259 | YC | **Symptom/Scenario**: Executing the `show tech all` command resets the port counters in all sessions. | CLI |
| 16.10.0015 | 255134 | YC | **Symptom**: Switch crashes regularly with the following message:<br>`Active/Commander system went down: eSoftware exception at msgSys.c:641 -- in 'mNSR',`<br>`-> Can't get message buffer for msgSys_recv.`<br>The event log indicates continuous removal and application of the device-profile.<br>**Scenario**: This issue occurred with a device profile for an AP enabled, with both interfaces of the AP connected to the switch through a trunk, and when the switch was rebooted.<br>**Workaround**: Disable and enable the device profile. | Device Profile |
| 16.10.0015 | 255158 | YC | **Symptom**: Multicast traffic with the source IP address 0.0.0.0 floods to all ports, even with IGMP snooping enabled.<br>**Scenario**: This issue occurred when the multicast traffic was sent with a NULL IP source from a device connected to a non-querier device. | IGMP |
| 16.10.0015 | 255408 | YC | **Symptom**: Unauthorized clients can connect and access the switch using the loopback address.<br>**Scenario**: This issue occurred when the `ip authorized-managers` command was configured and an unauthorized client attempted to connect to the loopback address. | IP Authorized Managers |
| 16.10.0015 | 255342 | YC | **Symptom**: When an initial role is applied, clients do not attempt to reauthenticate.<br>**Scenario**: This issue occurred when the server-timeout value was less than the RADIUS request timeout.<br>**Workaround**: Configure a greater server-timeout value than the RADIUS request timeout. | RADIUS |
| 16.10.0015 | 255171 | YC | **Symptom**: The switch CPU spikes and the ClearPass RADIUS server shuts down.<br>**Scenario**: This issue occurred when MAC authentication used the peap-mschapv2 authentication method. As a result, Access-Request and Access-challenge messages were exchanged in a loop. | RADIUS |
| 16.10.0015 | 255067 | YC | **Symptom**: Switch does not respond to Simple Network Management Protocol version 3 (SNMPv3) queries. | SNMPv3 |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue occurred when there was a wrong value in the boot counter. | |
| 16.10.0014 | - | YC | No fixes were included in version 16.10.0014. | NA |
| 16.10.0013 | 255031 | YC | **Symptom**: Switch loses connectivity to Aruba Central after a template is pushed.<br>**Scenario**: This issue occurred when a template with netdestination commands were pushed to the switch.<br>**Workaround**: Add `aruba-central url` to the template that is applied. | Central |
| 16.10.0013 | 255125 | YC | **Symptom**: Clients authenticated by Aruba Central are not placed in the proper VLAN.<br>**Scenario**: This issue occurred because of the following reasons:<br>■ Both MAC authentication and 802.1X are configured on the same port.<br>■ There are two clients on the port, which had a tagged membership for a VLAN, and the user role for a client had an untagged membership for the same VLAN. | Central |
| 16.10.0013 | 255123 | YC | **Symptom**: The following event did not identify the affected module correctly: `00907 IpAddrMgr: ST3-CMDR: Module p BMP TCAM parity recovery.`<br>**Scenario**: The following event was recorded in the event log when there was a hardware issue: `00907 IpAddrMgr: ST3-CMDR: Module p BMP TCAM parity recovery.` | RMON Logging |
| 16.10.0013 | 255058 | YC | **Symptom**: After a new template is applied to the switch, the switch is unable to connect to Aruba Central.<br>**Scenario**: This issue occurred because the primary VLAN on the switch was changed when the new template was applied. | Central |
| 16.10.0013 | 254976 | YC | **Symptom/Scenario**: The SSH, telnet, and console connections cannot be established with the switch, and the following event is recorded in the event log: `maximum user session limit reached.` | Switch Access |
| 16.10.0013 | 254966 | YC | **Symptom**: Applying a template from Aruba Central to a switch fails with the following reasons:<br>■ `Failure Reason: Add and Remove commands have been failed`<br>■ `Reason: Invalid netdestination` | Central |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | `entry`.<br>**Scenario**: This issue occurred when the template contained changes to the host configurations of the netdestination entries, which are used in an ACL. | |
| 16.10.0013 | 254893 | YC | **Symptom/Scenario**: The switch crashes due to an MSTP NMI event. | Spanning Tree |
| 16.10.0013 | 254797 | YC | **Symptom**: The following event is recorded in the event file: `Lease table is full, DHCP lease was not added`.<br>**Scenario**: This issue occurred when DHCP snooping was configured. | DHCP Snooping |
| 16.10.0013 | 254786 | YC | **Symptom**: SSH fails to connect to the switch.<br>**Scenario**: This issue occurred because of the following reasons:<br>■ More than one RADIUS server was configured.<br>■ `aaa authentication ssh enable` was configured to use the other RADIUS server, instead of using the first one in the configuration. | AAA Authentication |
| 16.10.0013 | 254780 | YC | **Symptom**: When more number of MAC authentication clients (auth method: peap-mschapv2) get authenticated or reauthenticated, the following event is recorded multiple times in the event log: `PEAP SSL socket connection limit reached`.<br>**Scenario**: This issue occurred when more than 20 clients were authenticated or reauthenticated at the same time.<br>**Workaround**: Authenticate or reauthenticate less than 20 clients at the same time. | MAC Authentication |
| 16.10.0013 | 254481 | YC | **Symptom**: The switch CPU utilization increases to 80% or more, and CDP packet looping is observed across VLANs.<br>**Scenario**: This issue occurred when CDP pass-through was configured on two switches, which had more than one connection between them.<br>**Workaround**: Use `no cdp run` command to disable CDP globally, instead of configuring CDP mode pass-through. | CDP |
| 16.10.0012 | 254360 | YC | **Symptom**: A configuration push using the `cfg-restore` command from Aruba Central fails.<br>**Scenario**: This issue occurred when a switch configuration, containing `radius server host` commands, was pushed to Aruba Central or when the `cfg-restore` command was executed with the same `radius server host` configuration. | Central |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Workaround**: Use the `copy tftp config` command to copy a configuration to the switch from Aruba Central, instead of the `cfg-restore` command for pushing a configuration. | |
| 16.10.0012 | 254096 | YC | **Symptom**: The `Rx Drop Bytes` parameter in the command output for `show interface queues <port>` displays very high values for the last few ports, even though these ports were down.<br>**Scenario**: This issue occurred when the `show interface queues <port>` command was issued. | CLI |
| 16.10.0012 | 254278 | YC | **Symptom**: The switch crashes when the `show crypto client-public-key` command is issued.<br>**Scenario**:This issue was observed when the `show crypto client-public-key` was issued when the `\t:` symbol was present in the client pub key file.<br>**Workaround**: Remove `\t:` symbol from the client public key file content. | Crypto |
| 16.10.0012 | 254760 | YC | **Symptom**: Removal of OSPF routes from the link-state database is delayed.<br>**Scenario**: This issue occurred when the switch received a Link-State Advertisement (LSA) that advertised routes with max age configured to remove the routes from the database. | OSPFv2 |
| 16.10.0012 | 254395 | YC | **Symptom**: The switch does not send the configured NAS-ID while sending a request to the RADIUS server.<br>**Scenario**: This issue occurred for both login and enable when the switch was configured with a non-default `server-group nas-id` and `ssh` was configured with peap-mschapv2. | Radius |
| 16.10.0012 | 254665 | YC | **Symptom**: REST connection fails when a Windows client makes an HTTP request.<br>**Scenario**: This issue occurred when a Windows client sent a REST HTTP request using PowerShell. | REST |
| 16.10.0012 | 254525 | YC | **Symptom**: The smartlink port stops forwarding VLAN traffic.<br>**Scenario**: This issue occurred when the:<br>■ The VLAN membership of a port was changed by removing it or adding it to any of the protected VLANs of the smartlink group. | Smartlinks |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | ■ STP was enabled and a non-default MSTP instance was created.<br>**Workaround**: Disable/enable the port. | |
| 16.10.0012 | 254722 | YC | **Symptom/Scenario**: When a user fails to login to the switch using SSH, no SNMP trap is sent. | SNMPv2 |
| 16.10.0012 | 254580 | YC | **Symptom**: A switch no longer accepts SSH connections.<br>**Scenario**: A switch no longer accepts SSH connections.<br>**Workaround**: Reboot the switch. | SSH |
| 16.10.0012 | 254393 | YC | **Symptom**: Event messages are not printed on the Syslog server.<br>**Scenario**: This issue occurred when a syslog server was configured with the TCP option, `logging <IP-ADDR> tcp` and `ip source-interface syslog` was configured.<br>**Workaround**: Remove `ip source-interface syslog ...` from the config or reboot the switch after configuring syslog over TCP. | Syslog |
| 16.10.0012 | 254311 | YC | **Symptom**: Gradual memory depletion on a switch is observed.<br>**Scenario**: This issue occurred when the telnet sessions were closed abruptly.<br>**Workaround**: Disable the telnet server on the switch. | Telnet |
| 16.10.0011 | 253563 | YC | **Symptom**: The switch crashes with the following message: `Health Monitor: Misaligned Mem Access.`<br>**Scenario**: This issue occurred when any of the 802.1X clients' MAC address had a NULL value due to corruption when authenticator configuration on a switch port was disabled. | 802.1X |
| 16.10.0011 | 254333, 254339 | YC | **Symptom**: Switch crashes with a message similar to the following: `Software exception at trlock.c -- in 'InetServer'.`<br>**Scenario**: This issue occurred when the `show tech all` command was executed from Aruba Central.<br>**Workaround**: Execute the `show tech all` command through the switch CLI. | Central |
| 16.10.0011 | 254255 | YC | **Symptom**: Switch crashes with a message similar to the following: `Software exception at multMgmtUtil.c -- in 'mOobmCtrl'.` | Chassis |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue occurred when continuous or frequent `cfg-restore` operations (with password or aaa authentication related configurations) were executed, and in parallel, the switch was accessed through local-authentication.<br>**Workaround**: Do not access the switch using local-authentication when `cfg-restore` operation is in progress. | |
| 16.10.0011 | 253472 | YC | **Symptom/Scenario**: The following event is recorded in the event log multiple times where `xx%` is an increasing value: `03008 system: Ports A,B packet buffer allocation has reached xx%`.<br>**Workaround**: Reboot the switch. | Chassis |
| 16.10.0011 | 253803 | YC | **Symptom**: SSH connection (Remote Console) cannot be established from Aruba Central to the switch.<br>**Scenario**: This issue occurred when `ip authorized-managers` was configured on the switch and a Remote Console connection was attempted from Aruba Central.<br>**Workaround**: Add the following configuration to the switch:<br>`ip authorized-managers 127.0.0.1 255.255.255.254 access manager` | Console |
| 16.10.0011 | 254196 | YC | **Symptom**: Multicast traffic stops after a redundancy switchover.<br>**Scenario**: This issue occurred when the IGMP `query-max-response-time` was configured to be `128` seconds and a redundancy switchover was performed.<br>**Workaround**: Remove IGMP from the VLAN and reconfigure the `query-max-response-time` to the default value of `10` seconds. | IGMP |
| 16.10.0011 | 253853 | YC | **Symptom**: Continuous RADIUS access request packets are sent from the switch to the RADIUS server.<br>**Scenario**: This issue occurred when a MAC address limit was configured and a device was attempted to be authenticated beyond the configured limit. | MAC Authentication |
| 16.10.0011 | 253965 | YC | **Symptom**: The switch closes the REST connection when the request is made from a Windows client.<br>**Scenario**: This issue occurred when a REST request was sent from PowerShell on a Windows client. | REST |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0011 | 252721 | YC | **Symptom**: Attempts to SSH or telnet to the switch fail and the following message is displayed: `Sorry, the maximum number of telnet sessions are active. Try again later.` **Scenario**: This issue occurred when a vulnerability scan was run against the switch multiple times. **Workaround**: Disable Telnet server. | Switch Access |
| 16.10.0011 | 253970 | YC | **Symptom**: Ports can be added to a trunk using the web interface even if those ports are configured with IGMP fastlearn. **Scenario**: This issue occurred when IGMP fastlearn was configured on a few ports of the switch, and the switch was accessed through the web interface to add the IGMP fastlearn enabled ports to the trunk. **Workaround**: Use the CLI to add ports to a trunk. | Web Interface |
| 16.10.0010 | 253807 | YC | **Symptom**: Unsupported values are accepted as ACL numbers for both standard and extended ACLs when configuring ACLs from the REST interface (for example, Aruba Central). Once configured, these ACLs cannot be deleted using REST or the CLI. **Scenario**: This issue occurred when the REST interface was used to configure an ACL with an unsupported value. | ACLs |
| 16.10.0010 | 253425 | YC | **Symptom**: The username sent for a successful MAC-authenticated client is the MAC address, rather than the username. **Scenario**: This issue occurred when a client was authenticated using MAC authentication. | Authentication |
| 16.10.0010 | 253422 | YC | **Symptom**: When a `show` command is executed using `\| include <anyword> <anyword>` the following error message is displayed: `Invalid Input : grep usage error.` **Scenario**: This issue occurred when a `show` command was executed using `\| include <anyword> <anyword>`. **Workaround**: Execute the `show` command without `\| include <anyword> <anyword>`. | CLI |
| 16.10.0010 | 253303 | YC | **Symptom**: Peer device does not get an IP address when the port it is connected to is configured using a device-profile. **Scenario**: This issue occurred when a port is configured using device profile and a peer device is connected to it. **Workaround**:Disable device-profile and manually configure the port. | Device Profile |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0010 | 253507 | YC | **Symptom**: Devices connected to the switch are unable to send or receive packets.<br>**Scenario**: This issue occurred when a multicast listener query was received with an unspecified source IP address.<br>**Workaround**: Stop sending malformed multicast listener query packets to the switch. | Multicast |
| 16.10.0010 | 253557 | YC | **Symptom**: Using REST to retrieve the resource identifier `/lldp/remote-device` fails to display the IPv4 address of the neighbor.<br>**Scenario**: This issue occurred when the REST resource operation GET was used to retrieve the data associated with `/lldp/remote-device`. | REST |
| 16.10.0010 | 252993 | YC | **Symptom**: Some RADIUS accounting packets sent to the RADIUS server have a very large size.<br>**Scenario**: This issue occurred when a downloadable user role was configured with a user policy, network accounting was enabled, and a client was authenticated. | RADIUS |
| 16.10.0010 | 253736 | YC | **Symptom**: Disconnect Change of Authorization (CoA) request is not honored.<br>**Scenario**: This issue occurred when the radius-server group was configured, a client was authenticated, and a disconnect CoA request with the default nas-id was sent.<br>**Workaround**: Configure `aaa server-group radius <Group name> nas-id <NAS-ID>` where the NAS-ID matches the NAS Identifier value shown in the output of the `show radius authentication` command. | RADIUS |
| 16.10.0010 | 253789 | YC | **Symptom**: Switch serial number contains an extra space at the end when it is read using SNMP.<br>**Scenario**: This issue occurred when the switch serial number was read using SNMP.<br>Example:<br>MIB OID: 1.3.6.1.2.1.47.1.1.1.1.11.1<br>MIB File: ENTITY-MIB | SNMP |
| 16.10.0010 | 253342 | YC | **Symptom**: SSH/Telnet/Console connections to the switch fail with an error message: `Maximum session limit is reached.`<br>**Scenario**: This issue occurred when multiple users logged in and out and RADIUS was configured as the primary authentication method.<br>**Workaround**: Reboot the switch. | Switch Access |
| 16.10.0010 | 253407 | YC | **Symptom**: Unable to log in to the switch using TACACS credentials. | TACACS |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: This issue occurred when a source interface for TACACS was configured using the `ip source-interface tacacs` command and the switch was upgraded to 16.10.0009. | |
| 16.10.0010 | 253001 | YC | **Symptom**: When there are continuous link flaps on the link-to-monitor ports within a fraction of a second, some link-to-disable ports may not come up once the link-to-monitor port stabilizes.<br>**Scenario**: This issue occurred when the link-to-monitor port used a transceiver connected by fibre and flapped continuously at a high rate.<br>**Workaround**: Use Fault-Finder to disable the link-to-monitor if it is flapping too often. The link-to-disable port can be disabled and re-enabled to bring it back up. | UFD |
| 16.10.0010 | 253290 | YC | **Symptom**: Switch crashes when it is accessed through the web interface.<br>**Scenario**: This issue occurred when the switch was accessed using the web interface and RADIUS authentication was configured for web access.<br>**Workaround**: Disable RADIUS authentication for web access. | Web UI |
| 16.10.0010 | 253877 | YC | **Symptom**: The **WebUI Security > Clients** page displays incorrect MAC addresses, which results in the user role, IP address, and status columns to be empty.<br>**Scenario**: This issue occurred when a few workstations with higher value MAC addresses (for example, 9c:dc:71:fb:77:fe) are connected to the last ports of a 2930 stack or the last module of a 5400R. | Web UI |
| 16.10.0009 | 252885 | YC | **Symptom**: Switch appears down in Aruba Central.<br>**Scenario**: This issue occurred because the system time was set to the year 2036, though NTP sync was successful, and the switch was connected to Aruba Central.<br>**Workaround**: Configure an NTP server in the switch. | Activate |
| 16.10.0009 | 252226 | YC | **Symptom**: Switch does not respond during the ZTP process.<br>**Scenario**: This issue occurred when connecting to the switch using SSH, while Airwave was transferring the configuration to the switch. | AirWave |
| 16.10.0009 | 251418 | YC | **Symptom**: Pushing a switch configuration template from Aruba Central fails and a 500 error code is returned.<br>**Scenario**: This issue occurred when a configuration template that had no untagged ports in VLAN 1 was pushed from Aruba Central. | Central |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Workaround**: In the configuration template, add at least one untagged port in VLAN 1. | |
| 16.10.0009 | 253174 | YC | **Symptom/Scenario**: The switch experienced an NMI crash with the following message: `Task='ewsCloudRcv'.` | Central |
| 16.10.0009 | 253276 | YC | **Symptom**: Unable to copy crash-files, core-dump, and the `show tech all` command output from the switch.<br>**Scenario**: This issue occurred when executing the `copy` command with an invalid IP address, file name, hostname, or when parallelly executing the `copy` command in other sessions.<br>**Workaround**:<br>■ Copy the core file from the web interface.<br>■ Copy the `show tech all` command output from the console interface. | CLI |
| 16.10.0009 | 252265 | YC | **Symptom**: The switch does not forward DHCP packets.<br>**Scenario**: This issue occurred when both DHCP snooping and IP client tracker trusted were configured, and the client was authenticated. | IP Client Tracker |
| 16.10.0009 | 252833 | YC | **Symptom**: MSTP does not work as expected and does not block ports when it should.<br>**Scenario**: This issue occurred when two ports in a loop were in a forwarding state with MSTP and port-security non-default learn mode enabled.<br>**Workaround**: Disable port-security. | Spanning Tree |
| 16.10.0009 | 252613 | YC | **Symptom**: Unable to connect to the switch using SSH.<br>**Scenario**: This issue occurred when the switch is configured to use TACACS and a malformed TACACS packet is received by the switch.<br>**Workaround**: Reboot the switch. | SSH |
| 16.10.0009 | 251966 | YC | **Symptom**: The switch sends logging events with a "Z" at the end of the timestamp when the it is not configured to use UTC.<br>**Scenario**: This issue occurred when the switch sent syslog messages over TLS. | Syslog |
| 16.10.0009 | 252410 | YC | **Symptom**: The switch either reboots or fails over from the active to standby management module and records a Watchdog Reset entry in the event log.<br>**Scenario**: This issue occurred when IP directed-broadcast was configured in the switch and Wake On LAN traffic was sent to a directly connected subnet.<br>**Workaround**: Disable IP directed-broadcast. | VSF |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0009 | 252443 | YC | **Symptom/Scenario**: The Reboot button is displayed for a few seconds in the Web UI. Clicking it allowed an operator to reboot the switch. | Web UI |
| 16.10.0008 | - | YC | Version 16.10.0008 was never released. | - |
| 16.10.0007 | 252007 | YC | **Symptom**: The switch sends an incorrect CLASS attribute value in the RADIUS accounting packet.<br>**Scenario**: When the CLASS attribute is updated during re-authentication of a MAC-authenticated client session, the switch fails to send the new CLASS attribute value in the RADIUS accounting packet.<br>**Workaround**: Force a new client authentication session by disabling/enabling the port after the CLASS attribute value changes. | Accounting |
| 16.10.0007 | 251765 | YC | **Symptom**: The show runnig-config output does not display some access list entries (ACEs).<br>**Scenario**: When the switch is configured with extended ACLs and connect-rate-filter, some ACEs are not displayed in the output of the `show runnig-config` command.<br>**Workaround**: Use the `show access-list config` command to get the complete extended ACL configuration. | ACLs |
| 16.10.0007 | 251273 | YC | **Symptom**: The switch incorrectly places clients in the configured authorized VLAN (auth-vid).<br>**Scenario**: When using `chap-radius authorized` option, if the route to the RADIUS server is not resolved during the switch boot up, clients are incorrectly placed in the configured authorized VLAN (auth-vid) rather than the guest VLAN (unauth-vid) or initial-role.<br>**Workaround**: Reauthenticate the affected clients. | Authentication |
| 16.10.0007 | 251927 | YC | **Symptom**: The switch fails to remove CDP configuration for a port.<br>**Scenario**: When a port is added to a trunk interface, the switch fails to remove the previous non-default CDP configuration for that port (example: no cdp enable <PORT-NUM>).<br>**Workaround**: Remove the non-default CDP configuration from the individual port before adding it to trunk interface. | CDP |
| 16.10.0007 | 252053 | YC | **Symptom/Scenario**: The switch crashes with an error message similar to: `Software exception in ISR at pvDmaV1Rx.c <...>`<br>`ASSERT:  No resources available!.` | Central |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0007 | 252267 | YC | **Symptom**: The switch experiences high CPU utilization.<br>**Scenario**: In conditions of low network bandwidth or network congestion that cause frequent disconnections from the Aruba Central Portal, the switch experiences high CPU utilization while attempting to reconnect to Aruba Central and while being managed by other NMS applications such as Solarwinds at the same time.<br>**Workaround**: Use only one NMS application to manage the switch if network bandwidth capacity or congestion cannot be improved. | Central |
| 16.10.0007 | 251876 | YC | **Symptom**: The switch may fail to apply the correct VLAN to dynamic trunks.<br>**Scenario**: After a reboot of a switch configured for dynamic trunks with device profile enabled on ports, the switch may fail to apply the correct VLAN configured in the device-profile, after the port is joined to the dynamic trunk.<br>**Workaround**: Disable and enable device-profile. | Dynamic Trunks |
| 16.10.0007 | 251972 | YC | **Symptom**: Some clients using the PEAP authentication mechanism are not successfully authenticated.<br>**Scenario**: When concurrent authentication requests are sent to the switch using peap-mschapv2, some clients may not be successfully authenticated, even though ACCESS ACCEPT is sent from the RADIUS server. | MAC Authentication |
| 16.10.0007 | 252131 | YC | **Symptom**: REST API calls may experience some slight delay in execution response.<br>**Scenario**: When multiple REST API commands are executed over the same HTTPS session, they may experience a slight delay in execution response.<br>**Workaround**: Use a new HTTPS session for each REST API call. | REST |
| 16.10.0007 | 250797 | YC | **Symptom**: The switch sends an incorrect checksum when forwarding certain UDP frames.<br>**Scenario**: If a received UDP frame has no checksum or the checksum value of zero (0), the switch incorrectly calculates the checksum when forwarding it. | UDP |
| 16.10.0007 | 251475 | YC | **Symptom**: The switch experiences high CPU utilization and possible console connectivity issues.<br>**Scenario**: When configuring or modifying aggregated interfaces (trunks) with more than 3 member ports on a switch where there is a very high number of configured VLANs, the switch experiences high CPU utilization and possible console connectivity issues while applying the configuration. | VLAN |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0007 | 251505 | YC | **Symptom**: The WebUI contains an XSS vulnerability.<br>**Scenario**: Configure the editable parameters in the WebUI with values that can cause an XSS attack. | Web UI |
| 16.10.0007 | 251524 | YC | **Symptom**: The switch fails to display some ports on the Ports page of the WebUI.<br>**Scenario**: When aSysName with trailing zeroes is received in the LLDP packet from a neighboring device, the switch fails to list some ports in the Ports page when using the WebUI.<br>**Workaround**: To get the information for all ports use one of the following options:<br>■ Disable LLDP on the port where the device with `invalidSysName` is connected.<br>■ Use the traditional web UI to get the information for the affected/missing ports.<br>■ Use switch CLI commands to get the information for the affected/missing ports. | Web UI |
| 16.10.0006 | - | YC | Version 16.10.0006 was never released. | - |
| 16.10.0005 | - | YC | Version 16.10.0005 was never released. | - |
| 16.10.0004 | - | YC | Version 16.10.0004 was never released. | - |
| 16.10.0003 | 251317 | YC | **Symptom**: A Windows client that joins a domain other than the one defined in Cisco ISE fails to authenticate. The client will also wait more than 5 minutes before attempting MAC address authentication.<br>**Scenario**: This issue is observed when MAC and 802.1X authentication are enabled on the port and the configured auth-order is 802.1X-MAC and an initial role. | 802.1X |
| 16.10.0003 | 251464 | YC | **Symptom**: VSF stack members crash intermittently during 802.1X client reauthentication and the following message is displayed: `Software exception in ISR at pvDmaV1Rx.c: -> ASSERT: No resources available!.`<br>**Scenario**: This issue is observed when ports with LLDP traffic are configured with 802.1X and MAC authentication, and the RADIUS VSA `HP-Port-Client-Limit-MA` value is zero. | 802.1X |
| 16.10.0003 | 251498 | YC | **Symptom**: A client is unable to pass traffic.<br>**Scenario**: This issue is observed when the clear `mac-address vlan 1 mac` command is issued to clear the switch's base MAC address from VLAN 1. | Basic Layer 2 |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0003 | 251280 | YC | **Symptom**: Deploying a switch template through Airwave/Aruba Central fails.<br>**Scenario**: This issue is observed when the IP address from VLAN1 is removed from a new configuration template and is pushed to the switch with the "ntpserver-name <server name>".<br>**Workaround**: Do not remove the IP address from VLAN 1 in the new template. | Central |
| 16.10.0003 | 251393 | YC | **Symptom**: A switch crashes with the following message "`Software exception in ISR at pvDmaV1Rx.c -> ASSERT: No resources available`".<br>**Scenario**: This issue is observed when a switch is configured with an initial role with a captive-portal-profile and a client is placed in this initial role because the RADIUS server is unreachable. | Classifier |
| 16.10.0003 | 250816 | YC | **Symptom**: Authenticated users are disconnected from the switch.<br>**Scenario**: This issue is observed when users disable and enable the interface which connects to the dhcp- relay switch, after configuring the DHCP server, DHCP relay, and DHCP snooping with ip-source lockdown.<br>**Workaround**: Disable ip-source lockdown. | DIPLD |
| 16.10.0003 | 249465 | YC | **Symptom**: A switch crashes and displays the following message: `Software exception at ospf2.c -- in 'eRouteCtrl' -> Routing Stack: Assert Failed.`<br>**Scenario**: This issue is observed when a switch is configured with OSPF and one of the OSPF neighbors is disconnected. | OSPF |
| 16.10.0003 | 251615 | YC | **Symptom**: An attacker is able to obtain sensitive data without providing valid login credentials after a successful REST query.<br>**Scenario**: This issue is observed when web management is enabled on the switch. | REST |
| 16.10.0003 | 251340 | YC | **Symptom**: Tunneled clients lose network connectivity.<br>**Scenario**: This issue is observed when user tunnels are configured in addition to ip client-tracker trusted and ip client-tracker probe-delay.<br>**Workaround**:<br>1. Remove ip client-tracker probe-delay from the configuration.<br>2. Disable the port.<br>3. Clear ARP. | Tunneled Node |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | 4. Re-enable the port. | |
| 16.10.0003 | 251325 | YC | **Symptom**: Users are unable to modify the vlan-id-tagged list of a user role.<br>**Scenario**: This issue is observed when the user applies a template that adds VLANs to the vlan-id-tagged list of a user role.<br>**Workaround**: Use a template that does not extend the list of VLANs in vlan-id-tagged. | User Roles |
| 16.10.0003 | 251506 | YC | **Symptom**: The switch manager password is altered to an attack-controlled value.<br>**Scenario**: This issue is observed when the user clicks a malicious hyperlink. | Web UI |
| 16.10.0003 | 251314 | YC | **Symptom**: Switches appear offline in Aruba Central.<br>**Scenario**: This issue is observed after the switch software is upgraded from 16.04 to 16.08.<br>**Workaround**: Reboot the switch. | ZTP |
| 16.10.0002 | 250681 | YC | **Symptom/Scenario**: The Topology section of Airwave shows spanning tree details for a switch that does not have spanning tree enabled. | AirWave |
| 16.10.0002 | 251313 | YC | **Symptom**: The switch experiences a high CPU utilization and loses connection with Central.<br>**Scenario**: When the switch is upgraded to 16.08.0001 and a template with `tls` and `cwmp` commands is pushed from Central, the switch experiences high CPE utilization and loses the connection to Aruba Central.<br>**Workaround**: Remove `tls application cloud lowest-version tls1.2` and `cwmp` from the switch template. | Central |
| 16.10.0002 | 250251 | YC | **Symptom/Scenario**: The switch crashes with a message similar to: `Software exception in ISR at interrupts_om.c-> Excessive OM FP interrupts.` | Chassis |
| 16.10.0002 | 250600 | YC | **Symptom/Scenario**: The help text for the `device-identity lldp oui` command indicates that the required input is a MAC-OUI. | Device finger printing |
| 16.10.0002 | 250957 | YC | **Symptom**: Host packets are denied with a message similar to `dlpld: AM1: Access denied.` | DIPLD |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: When the switch has been configured using the `aaa port-access` and `ip source-lockdown` commands and clients authenticate to the switch, if more than one client is placed in a VLAN provided by the RADIUS server, host packets are denied.<br>**Workaround**: Disable Dynamic IP Lockdown on the switch using the `no ip source-lockdown` command. | |
| 16.10.0002 | 250550 | YC | **Symptom**: Primary and secondary VLANs do not have MAC address entries.<br>**Scenario**: When a port has been configured with PVLAN and port security and the port is subsequently disabled and re-enabled, MAC address entries are not present in the primary and secondary VLANs.<br>**Workaround**: Reconfigure the port security configuration of the port. | MAC address |
| 16.10.0002 | 250392 | YC | **Symptom**: The switch crashes with a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access.`<br>**Scenario**: After an IP address has been reassigned from one VLAN to another VLAN using the menu interface, the switch may crash with a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access.`<br>**Workaround**: Disable the first VLAN and save the configuration from the menu interface. Then, configure the deleted IP address on the second VLAN. | Menu |
| 16.10.0002 | 245830 | YC | **Symptom**: The switch fails to list the switch ports in the Ports web management page.<br>**Scenario**: When a peer device that advertises information in LLDP has a sysName string with special characters, the switch fails to display the port list table on the Ports web management page.<br>**Workaround**: Remove the special characters from the peer device sysName or use CLI commands to get specific port information. | Next Gen GUI |
| 16.10.0002 | 250896 | YC | **Symptom**: Switch ports are not listed in the web interface.<br>**Scenario**: If a peer device advertises an LLDP port ID containing special characters, switch ports are not listed in the web interface. | Web UI |
| 16.10.0001 | 250366 | YC | **Symptom**: An Apple MacOS device (desktop or laptop) is unable to maintain authentication with APs. | 802.1X |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Scenario**: When an AP is connected to a switch port that has been configured with device-identity bypass, an Apple MacOS device (desktop or laptop) receives EAP request ID packets after 802.1X authentication and is unable to maintain authentication with the AP.<br>**Workaround**: Configure a MAC-based ACL to block the EAP request identity to multicast MAC address. | |
| 16.10.0001 | 250681 | YC | **Symptom/Scenario**: The Topology section of Airwave shows spanning tree details for a switch that does not have spanning tree enabled. | AirWave |
| 16.10.0001 | 250251 | YC | **Symptom/Scenario**: The switch crashes with a message similar to: `Software exception in ISR at interrupts_om.c-> Excessive OM FP interrupts.` | Chassis |
| 16.10.0001 | 250600 | YC | **Symptom/Scenario**: The help text for the `device-identity lldp oui` command indicates that the required input is a MAC-OUI. | Device identity |
| 16.10.0001 | 250957 | YC | **Symptom**: Host packets are denied with a message similar to `dlpld: AM1: Access denied.`<br>**Scenario**: When the switch has been configured using the `aaa port-access` and `ip source-lockdown` commands and clients authenticate to the switch, if more than one client is placed in a VLAN provided by the RADIUS server, host packets are denied.<br>**Workaround**: Disable Dynamic IP Lockdown on the switch using the `no ip source-lockdown` command. | DIPLD |
| 16.10.0001 | 250550 | YC | **Symptom**: Primary and secondary VLANs do not have MAC address entries.<br>**Scenario**: When a port has been configured with PVLAN and port security and the port is subsequently disabled and re-enabled, MAC address entries are not present in the primary and secondary VLANs.<br>**Workaround**: Reconfigure the port security configuration of the port. | MAC address |
| 16.10.0001 | 250392 | YC | **Symptom**: The switch crashes with a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access.`<br>**Scenario**: After an IP address has been reassigned from one VLAN to another VLAN using the menu interface, the switch may crash with a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access.` | Menu |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | **Workaround**: Disable the first VLAN and save the configuration from the menu interface. Then, configure the deleted IP address on the second VLAN. | |
| 16.10.0001 | 245830 | YC | **Symptom**: The switch fails to list the switch ports in the Ports web management page.<br>**Scenario**: When a peer device that advertises information in LLDP has a sysName string with special characters, the switch fails to display the port list table on the Ports web management page.<br>**Workaround**: Remove the special characters from the peer device sysName or use CLI commands to get specific port information. | Web UI |
| 16.10.0001 | 250896 | YC | **Symptom**: Switch ports are not listed in the web interface.<br>**Scenario**: If a peer device advertises an LLDP port ID containing special characters, switch ports are not listed in the web interface. | Web UI |

# Issues and Workarounds

The following are known open issues with this branch of the software.

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.

**Table 19:** *Known Issues*

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| 16.10.0016 | 255646 | YC | **Symptom**: The `show statistics aclv4 <ACL-NAME-STR> vlan <VLAN-ID> out` command displays lesser `HitCounts for ACL` for deny rule.<br>**Scenario**: The routed traffic is denied even before the egress Access control list (ACL) when the ACL contains a deny rule, and it is applied in the VLAN egress direction. | ACL |
| 16.10.0015 | 255554 | YC | **Symptom**: Aruba 2540 switches fail to connect to Aruba Central during the ZTP process.<br>**Scenario**: This issue occurs when the Simple Network Time Protocol (SNTP) or any other time protocol is not configured on the network.<br>**Workaround**: Use one of the following workarounds to fix this issue:<br>■ Manually configure the system time.<br>◦ Set the current date and time using the `time [HH:MM:SS] [MM/DD/YYYY]` command.<br>◦ Force connection to Aruba Central using the | Central |

| Version | Bug ID | Software | Description | Category |
|---|---|---|---|---|
| | | | `aruba-central disable` and `aruba-central enable` commands.<br>■ Execute any reboot command that gracefully reboot the switch. The following are some of the commands that gracefully reboot the switch:<br>◦ `boot system flash {<primary \| secondary>}`<br>◦ `reboot`<br>◦ `reset saved-configuration`<br>■ Enable SNTP on the network.<br>◦ By default, SNTP updates the system time. This issue does not occur when the SNTP server is enabled on the network. | |

# Upgrade Information

## Upgrading Restrictions and Guidelines

YC.16.10.0009 uses BootROM YC.16.01.0002. 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/.