AOS-S
WB 16.10
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
Campus Access Points + Controllers	Master-Slave	Conductor-Member
Instant Access Points	Master-Slave	Conductor-Member
Switch Stack	Master-Slave	Conductor-Member
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types 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	Release Date	Remarks
16.10.0013	2021-05-10	Released, fully supported, and posted on the web.
16.10.0012	2021-04-01	Released, fully supported, and posted on the web.
16.10.0011	2021-01-29	Released, fully supported, and posted on the web.
16.10.0010	2020-08-24	Released, fully supported, and posted on the web.
16.10.0009	2020-06-30	Released, fully supported, and posted on the web.
16.10.0008	n/a	Never released.
16.10.0007	2020-04-21	Released, fully supported, and posted on the web.
16.10.0006	n/a	Never released.
16.10.0005	2020-02-17	Released, fully supported, and posted on the web.
16.10.0004	n/a	Never released.
16.10.0003	2020-01-21	Released, fully supported, and posted on the web.
16.10.0002	2019-11-04	Released, fully supported, and posted on the web.
16.10.0001	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 WB.16.10 branch of the software.

Version WB.16.10.0001 is the initial build of Major version WB.16.10 software. WB.16.10.0001 includes all enhancements and fixes in the WB.16.09.0001 software, plus the additional enhancements and fixes in the WB.16.10.0001 enhancements and fixes sections of this release note.

This release applies to the following Aruba 2920 Switch Series:

Table 2: *Products Supported*

Product number	Description
J9726A	Aruba 2920 24G Switch
J9728A	Aruba 2920 48G Switch
J9727A	Aruba 2920 24G PoE+ Switch
J9729A	Aruba 2920 48G PoE+ Switch
J9836A	Aruba 2920 48G PoE+ 740W 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 3: *Enhancements*

Version	Software	Description	Category
16.10.0013	WB	No enhancements were included in version 16.10.0013.	NA
16.10.0012	WB	No enhancements were included in version 16.10.0012.	NA
16.10.0011	WB	No enhancements were included in version 16.10.0011.	NA
16.10.0010	WB	No enhancements were included in version 16.10.0010.	NA
16.10.0009	WB	Added support to configure probe delay for the IP Client Tracker: `ip client-tracker probe-delay <INTERVAL>`	Probe Delay for Client Tracker

Version	Software	Description	Category
		Refer to the *Access Security Guide* for more information.	
16.10.0009	WB	Added support for the following RADIUS enhancements: ■ Support to configure RadSec server as FQDN. ■ Support to configure per-port RADIUS server group for MAC authentication. ■ Support for automatic download of the certificate required to establish secur connection (HTTPS) with ClearPass Policy Manager server. Refer to the *Access Security Guide* for more information.	RADIUS Enhancement
16.10.0008	WB	Version 16.10.0008 was never released.	NA
16.10.0007	WB	■ Added additional support for pipe "|" option to grep for pattern match the output of CLI commands, such as: ◦ Case-insensitive option to allow a case insensitive pattern match ◦ Up to four consecutive pattern matches in one CLI command ■ 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	WB	Added the following REST enhancements: ■ Support for ARP table data. ■ Support for primary VLAN. ■ Support for reserved-vlan and clearpass options to configure dynamic segmentation. ■ REST API schema moved under device-rest-api/services/server.html. Refer to the *REST API Guide* for more information.	REST
16.10.0007	WB	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: ■ It works on the standard TLS handshake mechanism and uses mutual authentication. ■ It uses certificates issued by HP CA for establishing TLS connections. 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

Version	Software	Description	Category
16.10.0006	WB	Version 16.10.0006 was never released.	NA
16.10.0005	WB	No enhancements were included in version 16.10.0005.	NA
16.10.0004	WB	Version 16.10.0004 was never released.	NA
16.10.0003	WB	No enhancements were included in version 16.10.0003.	NA
16.10.0002	WB	No enhancements were included in version 16.10.0002.	NA
16.10.0001	WB	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 4: *Fixed Issues*

Version	Bug ID	Software	Description	Category
16.10.0013	255376	WB	**Symptom/Scenario**: Traffic loss is observed in Port-Based Tunneling (PBT) and controller Virtual Router Redundancy Protocol (VRRP) topology. **Workaround**: Disable and enable PBT on the switch.	Tunneled Node
16.10.0013	255058	WB	**Symptom**: After a new template is applied to the switch, the switch is unable to connect to Aruba Central. **Scenario**: This issue occurred because the primary VLAN on the switch was changed when the new template was applied. **Workaround**: Reboot the switch.	Central
16.10.0012	253965	WB	**Symptom**: The switch closes the REST connection when the request is made from a Windows client. **Scenario**: This issue occurred when a REST request was sent from PowerShell on a Windows client.	REST
16.10.0012	254255	WB	**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. **Workaround**: Do not access the switch using local-authentication when `cfg-restore` operation is in progress.	
16.10.0012	254333, 254339	WB	**Symptom**: Switch crashes with a message similar to the following: `Software exception at trlock.c -- in 'InetServer'.` **Scenario**: This issue occurred when the `show tech all` command was executed from Aruba Central. **Workaround**: Execute the `show tech all` command through the switch CLI.	Central
16.10.0012	254311	WB	**Symptom**: Gradual memory depletion on a switch is observed. **Scenario**: This issue occurred when the telnet sessions were closed abruptly. **Workaround**: Disable the telnet server on the switch.	Telnet
16.10.0012	254360	WB	**Symptom**: A configuration push using the `cfg-restore` command from Aruba Central fails. **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. **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
16.10.0011	253853	WB	**Symptom**: Continuous RADIUS access request packets are sent from the switch to the RADIUS server. **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	254278	WB	**Symptom**: The switch crashes when the `show crypto client-public-key` command is issued. **Scenario**:This issue occurred when the `show crypto client-public-key` was issued when the `\t:` symbol was present in the client public key file. **Workaround**: Remove `\t:` symbol from the client public key file content.	SSH

Version	Bug ID	Software	Description	Category
16.10.0010	253807	WB	**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	WB	**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	WB	**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	WB	**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
16.10.0010	253507	WB	**Symptom**: Devices connected to the switch are unable to send or receive packets. **Scenario**: This issue occurred when a multicast listener query was received with an unspecified source IP address. **Workaround**: Stop sending malformed multicast listener query packets to the switch.	Multicast
16.10.0010	253557	WB	**Symptom**: Using REST to retrieve the resource identifier `/lldp/remote-device` fails to display the IPv4 address of the neighbor. **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	WB	**Symptom**: Some RADIUS accounting packets sent to the RADIUS server have a very large size. **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

Version	Bug ID	Software	Description	Category
16.10.0010	253736	WB	**Symptom**: Disconnect Change of Authorization (CoA) request is not honored. **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. **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	253342	WB	**Symptom**: SSH/Telnet/Console connections to the switch fail with an error message: `Maximum session limit is reached`. **Scenario**: This issue occurred when multiple users logged in and out and RADIUS was configured as the primary authentication method. **Workaround**: Reboot the switch.	Switch Access
16.10.0010	253407	WB	**Symptom**: Unable to log in to the switch using TACACS credentials. **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	WB	**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. **Scenario**: This issue occurred when the link-to-monitor port used a transceiver connected by fibre and flapped continuously at a high rate. **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	WB	**Symptom**: Switch crashes when it is accessed through the web interface. **Scenario**: This issue occurred when the switch was accessed using the web interface and RADIUS authentication was configured for web access. **Workaround**: Disable RADIUS authentication for web access.	Web UI
16.10.0010	253877	WB	**Symptom**: The **WebUI Security > Clients** page displays incorrect MAC addresses, which results in the user role, IP address, and status columns to be empty. **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	WB	**Symptom**: Switch appears down in Aruba Central.	Activate

Version	Bug ID	Software	Description	Category
			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. **Workaround**: Configure an NTP server in the switch.	
16.10.0009	252226	WB	**Symptom**: Switch does not respond during the ZTP process. **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	WB	**Symptom**: Pushing a switch configuration template from Aruba Central fails and a 500 error code is returned. **Scenario**: This issue occurred when a configuration template that had no untagged ports in VLAN 1 was pushed from Aruba Central. **Workaround**: In the configuration template, add at least one untagged port in VLAN 1.	Central
16.10.0009	253174	WB	**Symptom/Scenario**: The switch experienced an NMI crash with the following message: `Task='ewsCloudRcv'.`	Central
16.10.0009	253276	WB	**Symptom**: Unable to copy crash-files, core-dump, and the `show tech all` command output from the switch. **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. **Workaround**: ■ Copy the core file from the web interface. ■ Copy the `show tech all` command output from the console interface.	CLI
16.10.0009	252430	WB	**Symptom**: Invalid MAC address entries are seen in the DHCP snooping binding table. **Scenario**: This issue occurred when switch received malformed DHCP or BOOTP packets. **Workaround**: Configure a DHCP authorized server so that requests only from authorized servers are processed.	DHCP Snooping
16.10.0009	252265	WB	**Symptom**: The switch does not forward DHCP packets. **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	WB	**Symptom**: MSTP does not work as expected and does not block ports when it should. **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. **Workaround**: Disable port-security.	Spanning Tree

Version	Bug ID	Software	Description	Category
16.10.0009	252338	WB	**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. **Scenario**: This issue occurred when establishing an SSH connection to the standby OOBM IP address.	SSH
16.10.0009	252613	WB	**Symptom**: Unable to connect to the switch using SSH. **Scenario**: This issue occurred when the switch is configured to use TACACS and a malformed TACACS packet is received by the switch. **Workaround**: Reboot the switch.	SSH
16.10.0009	251966	WB	**Symptom**: The switch sends logging events with a "Z" at the end of the timestamp when the it is not configured to use UTC. **Scenario**: This issue occurred when the switch sent syslog messages over TLS.	Syslog
16.10.0009	252443	WB	**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	-	WB	Version 16.10.0008 was never released.	-
16.10.0007	252007	WB	**Symptom**: The switch sends an incorrect CLASS attribute value in the RADIUS accounting packet. **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. **Workaround**: Force a new client authentication session by disabling/enabling the port after the CLASS attribute value changes.	Accounting
16.10.0007	251765	WB	**Symptom**: The show runnig-config output does not display some access list entries (ACEs). **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. **Workaround**: Use the `show access-list config` command to get the complete extended ACL configuration.	ACLs
16.10.0007	251273	WB	**Symptom**: The switch incorrectly places clients in the configured authorized VLAN (auth-vid). **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. **Workaround**: Reauthenticate the affected clients.	Authentication
16.10.0007	251659	WB	**Symptom**: Switch fails to move the client MAC address from one port to another.	Authentication

Version	Bug ID	Software	Description	Category
			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. **Workaround**: Disable and re-enable the switch interface where the affected client moved to.	
16.10.0007	251927	WB	**Symptom**: The switch fails to remove CDP configuration for a port. **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>). **Workaround**: Remove the non-default CDP configuration from the individual port before adding it to trunk interface.	CDP
16.10.0007	252053	WB	**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	WB	**Symptom**: The switch experiences high CPU utilization. **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. **Workaround**: Use only one NMS application to manage the switch if network bandwidth capacity or congestion cannot be improved.	Central
16.10.0007	251876	WB	**Symptom**: The switch may fail to apply the correct VLAN to dynamic trunks. **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. **Workaround**: Disable and enable device-profile.	Dynamic Trunks
16.10.0007	251972	WB	**Symptom**: Some clients using the PEAP authentication mechanism are not successfully authenticated. **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	WB	**Symptom**: REST API calls may experience some slight delay in execution response. **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	250797	WB	**Symptom**: The switch sends an incorrect checksum when forwarding certain UDP frames. **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	WB	**Symptom**: The switch experiences high CPU utilization and possible console connectivity issues. **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	WB	**Symptom**: The WebUI contains an XSS vulnerability. **Scenario**: Configure the editable parameters in the WebUI with values that can cause an XSS attack.	Web UI
16.10.0007	251524	WB	**Symptom**: The switch fails to display some ports on the Ports page of the WebUI. **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. **Workaround**: To get the information for all ports use one of the following options: ■ Disable LLDP on the port where the device with `invalidSysName` is connected. ■ Use the traditional web UI to get the information for the affected/missing ports. ■ Use switch CLI commands to get the information for the affected/missing ports.	Web UI
16.10.0006	-	WB	Version 16.10.0006 was never released.	-
16.10.0005	251473	WB	**Symptom**: End devices periodically lose access to the network. **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	-	WB	Version 16.10.0004 was never released.	-
16.10.0003	251317	WB	**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.	802.1X

Version	Bug ID	Software	Description	Category
			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.	
16.10.0003	251464	WB	**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!.` **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	WB	**Symptom**: A client is unable to pass traffic. **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	WB	**Symptom**: Deploying a switch template through Airwave/Aruba Central fails. **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>". **Workaround**: Do not remove the IP address from VLAN 1 in the new template.	Central
16.10.0003	251393	WB	**Symptom**: A switch crashes with the following message "`Software exception in ISR at pvDmaV1Rx.c -> ASSERT: No resources available`". **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	WB	**Symptom**: Authenticated users are disconnected from the switch. **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. **Workaround**: Disable ip-source lockdown.	DIPLD
16.10.0003	251662	WB	**Symptom**: Unable to configure a /31 subnet address as source/destination address for tunnel interfaces. **Scenario**: This issue is observed when users attempt to configure a /31 subnet address as source/ destination address for a tunnel interface. **Workaround**: Configure a /30 subnet address.	L3 Addressing

Version	Bug ID	Software	Description	Category
16.10.0003	249465	WB	**Symptom**: A switch crashes and displays the following message: `Software exception at ospf2.c -- in 'eRouteCtrl' -> Routing Stack: Assert Failed.` **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		**Symptom**: An attacker is able to obtain sensitive data without providing valid login credentials after a successful REST query. **Scenario**: This issue is observed when web management is enabled on the switch.	REST
16.10.0003	251340		**Symptom**: Tunneled clients lose network connectivity. **Scenario**: This issue is observed when user tunnels are configured in addition to ip client-tracker trusted and ip client-tracker probe-delay. **Workaround**: 1. Remove ip client-tracker probe-delay from the configuration. 2. Disable the port. 3. Clear ARP. 4. Re-enable the port.	Tunneled Node
16.10.0003	251893	WB	**Symptom**: A switch port is in the Disabled state. **Scenario**: This issue is observed when spanning tree is enabled and Per-Port Tunneled Node (PPTN) is configured on two ports that are connected. **Workaround**: Do not connect two PPTN ports.	Tunneled Node
16.10.0003	251506	WB	**Symptom**: The switch manager password is altered to an attack-controlled value. **Scenario**: This issue is observed when the user clicks a malicious hyperlink.	Web UI
16.10.0003	251314	WB	**Symptom**: Switches appear offline in Aruba Central. **Scenario**: This issue is observed after the switch software is upgraded from 16.04 to 16.08. **Workaround**: Reboot the switch.	ZTP
16.10.0002	250366	WB	**Symptom**: An Apple MacOS device (desktop or laptop) is unable to maintain authentication with APs. **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. **Workaround**: Configure a MAC-based ACL to block the EAP request identity to multicast MAC address.	802.1X
16.10.0002	250681	WB	**Symptom/Scenario**: The Topology section of Airwave shows spanning tree details for a switch that does not have spanning tree enabled.	AirWave

Version	Bug ID	Software	Description	Category
16.10.0002	251313	WB	**Symptom**: The switch experiences a high CPU utilization and loses connection with Central. **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. **Workaround**: Remove tls application cloud lowest-version tls1.2 and cwmp from the switch template.	Central
16.10.0002	250600	WB	**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	WB	**Symptom**: Host packets are denied with a message similar to `dlpld: AM1: Access denied`. **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. **Workaround**: Disable Dynamic IP Lockdown on the switch using the `no ip source-lockdown` command.	DIPLD
16.10.0002	250550	WB	**Symptom**: Primary and secondary VLANs do not have MAC address entries. **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. **Workaround**: Reconfigure the port security configuration of the port.	MAC address
16.10.0002	250392	WB	**Symptom**: The switch crashes with a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access`. **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`. **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	WB	**Symptom**: The switch fails to list the switch ports in the Ports web management page. **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. **Workaround**: Remove the special characters from the peer device sysName or use CLI commands to get specific port information.	Next Gen GUI

Version	Bug ID	Software	Description	Category
16.10.0002	250833	WB	**Symptom**: After a switch reboot, OSPF is stuck in the INIT state. **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. **Workaround**: Configure the router ID manually.	OSPF
16.10.0002	250896	WB	**Symptom**: Switch ports are not listed in the web interface. **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	WB	**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	WB	**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	WB	**Symptom**: Host packets are denied with a message similar to `dlpld: AM1: Access denied`. **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. **Workaround**: Disable Dynamic IP Lockdown on the switch using the `no ip source-lockdown` command.	DIPLD
16.10.0001	250550	WB	**Symptom**: Primary and secondary VLANs do not have MAC address entries. **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. **Workaround**: Reconfigure the port security configuration of the port.	MAC address
16.10.0001	250392	WB	**Symptom**: The switch crashes with a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access`. **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`. **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	WB	**Symptom**: After a switch reboot, OSPF is stuck in the INIT state.	OSPF

Version	Bug ID	Software	Description	Category
			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. **Workaround**: Configure the router ID manually.	
16.10.0001	245830	WB	**Symptom**: The switch fails to list the switch ports in the Ports web management page. **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. **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	WB	**Symptom**: Switch ports are not listed in the web interface. **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

WB.16.10.0009 uses BootROM WB.16.03. 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 the max-vlans value is greater than 2048.

Unconfigure the max-vlans before attempting to downgrade from WB.16.02.0008 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/.