

WB.16.07.0003 Release Notes

aruba

a Hewlett Packard
Enterprise company

Part Number: 5200-5534
Published: November 2018
Edition: 1

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Chapter 1 16.07.0003 Release Notes	5
Description.....	5
Important information.....	5
Version history.....	5
Products supported.....	6
Compatibility/interoperability.....	6
Enhancements.....	7
Version 16.07.0003.....	7
Version 16.07.0002.....	7
Fixes.....	7
Version 16.07.0003.....	7
Authentication.....	7
Central.....	7
IPsec.....	7
IPv4.....	8
IPv6 RA.....	8
Logging.....	8
PoE.....	8
RADIUS Accounting.....	8
SNMP.....	8
Spanning Tree.....	9
User Roles.....	9
VLAN.....	9
Web UI.....	9
Version 16.07.0002.....	10
ACLs.....	10
Central.....	10
Certificates.....	10
mDNS.....	10
RMON.....	10
SNMP.....	11
Spanning Tree.....	11
Syslog.....	11
Telnet/SSH.....	11
Transceivers.....	12
VLAN.....	12
Upgrade information.....	12
 Chapter 2 Hewlett Packard Enterprise security policy	 13
Finding Security Bulletins.....	13
Security Bulletin subscription service.....	13
 Chapter 3 Websites	 14
 Chapter 4 Support and other resources	 15
Accessing Hewlett Packard Enterprise Support.....	15
Accessing updates.....	15

Customer self repair 16
Remote support 16
Warranty information 16
Regulatory information 17
Documentation feedback 17

Description

This release note covers software versions for the WB.16.07 branch of the software.

Version WB.16.07.0002 is the initial build of Major version WB.16.07 software. WB.16.07.0002 includes all enhancements and fixes in the WB.16.06.0006 software, plus the additional enhancements and fixes in the WB.16.07.0002 enhancements and fixes sections of this release note.

Product series supported by this software:

Aruba 2920 Switch Series

Important information

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

Version history

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

Version number	Release date	Based on	Remarks
WB.16.07.0003	2018-11-21	WB.16.07.0002	Released, fully supported, and posted on the web.
WB.16.07.0002	2018-09-13	WB.16.06.0006	Initial release of the WB.16.07 branch. Released, fully supported, and posted on the web.
WB.16.06.0008	2018-09-05	WB.16.06.0007	Released, fully supported, and posted on the web.
WB.16.06.0007	n/a	WB.16.05.0006	Never released.
WB.16.06.0006	2018-06-26	WB.16.05.0003	Initial release of the WB.16.06 branch. Released, fully supported, and posted on the web.
WB.16.05.0009	2018-06-08	WB.16.05.0008	Released, fully supported, and posted on the web.
WB.16.05.0008	n/a	WB.16.05.0007	Never released.
WB.16.05.0007	2018-03-28	WB.16.05.0006	Released, fully supported, and posted on the web.
WB.16.05.0006	n/a	WB.16.05.0005	Never released.
WB.16.05.0005	n/a	WB.16.05.0004	Never released.
WB.16.05.0004	2017-12-22	WB.16.05.0003	Released, fully supported, and posted on the web.

Table Continued

Version number	Release date	Based on	Remarks
WB.16.05.0003	2017-12-12	WB.16.04.0008	Initial release of the WB.16.05 branch. Released, fully supported, and posted on the web.
WB.16.04.0010	2017-10-16	WB.16.04.0008	Released, fully supported, and posted on the web.
WB.16.04.0008	2017-07-27	WB.16.03.0003	Initial release of the WB.16.04 branch. Released, fully supported, and posted on the web.

Products supported

This release applies to the following product models:

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

Compatibility/interoperability

The switch web agent supports the following web browsers:

Browser	Supported versions
Internet Explorer	<ul style="list-style-type: none"> Edge 11
Chrome	<ul style="list-style-type: none"> 53 52
Firefox	<ul style="list-style-type: none"> 49 48
Safari (MacOS only)	<ul style="list-style-type: none"> 10 9



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

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.

Version 16.07.0003

No enhancements were included in version 16.07.0003.

Version 16.07.0002

No enhancements were included in version 16.07.0002.

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.



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

Version 16.07.0003

Authentication CR_0000245450

Symptom: The switch fails to display the correct expected username in the Endpoint Username attribute.

Scenario: When the username attribute of the mac-based authenticated client is changed in the authenticating server before the next reauth-period, the switch fails to update the username of the authenticated client in the output of the CLI command `show port-access client`.

Workaround: Disable and re-enable the interface to force all the new authentication attributes to be reapplied.

Central CR_0000246091

Symptom/Scenario: The switch fails to close TCP port 8900 (jmb-cds1) after completing the connection to the Aruba Central application.

IPsec CR_0000244975

Symptom: A VPN tunnel to Airwave fails and does not recover.

Scenario: A VPN tunnel to Airwave is established but is brought down and the switch is not able to re-establish the tunnel to Airwave.

Workaround: Reboot the switch or set the IP address to none and then back to DHCP (no ip address, ip address dhcp) for VLAN 1.

IPv4

CR_0000244916

Symptom: The switch is unable to communicate with any device outside of the VLANs configured on the switch.

Scenario: When a default gateway is configured and the switch loses power or undergoes a cold/warm reboot, it cannot communicate with any device outside of the VLANs configured when it powers back up.

Workaround: Delete and re-add the default gateway.

IPv6 RA

CR_0000246423

Symptom: The switch fails to forward IPv6 RA packets.

Scenario: When both IGMP and MLD are enabled on an un-authenticated VLAN (unauth-vid), the switch may randomly fail to forward IPv6 RA packets destined to authenticated users on the authenticated VLAN (auth-vid).

Workaround: Disable MLD on the un-authenticated VLAN (unauth-vid).

Logging

CR_0000246621

Symptom: In certain conditions, the switch fails with an error message similar to `NMI event <...>`
`Task='eDevIdle'`.

Scenario: When issuing the CLI command `show logging`, if the switch event log is over 80% full and the switch CPU is under high utilization, the switch may randomly fail with an error message similar to `NMI event <...>`
`Task='eDevIdle'`.

PoE

CR_0000244889

Symptom: Unable to configure the PoE allocate by value on dual personality ports.

Scenario: While provisioning a new member to the 2-member stack the poe-allocate-by value on the dual personality ports cannot be configured.

Workaround: After connecting the physical switch, configure the poe-allocate-by value.

RADIUS Accounting

CR_0000244813

Symptom: The switch delays the accounting request packet by 50-60 seconds after the client authentication is accepted.

Scenario: When the port access is configured for MAC address and 802.1x authentication and the switch is enabled for DHCP snooping, if the authenticated port is concurrently untagged and tagged in different VLAN IDs, the accounting request packet may be delayed by 50-60 seconds.

SNMP

CR_0000246595

Symptom: The switch fails to report some stacking ports' details.

Scenario: In a stacking configuration, after a switch reboot or redundancy switchover, the switch may fail to report the port status for the standby switch in the SNMP MIB 1.3.6.1.2.1.47.1.1.1.7.

Workaround: Use the CLI command `show stacking stack-ports` to get the stacking ports' details.

Spanning Tree

CR_0000245603

Symptom: The switch CPU utilization increases leading to a switch failure with an error message similar to NMI event <...> Task='mMstpCtrl' <...>.

Scenario: When root-guard is enabled on multiple switch interfaces, if there are frequent root-guard inconsistencies due to spanning tree instance priority changes, the switch CPU utilization may get high and lead to a switch failure with an error message similar to NMI event <...> Task='mMstpCtrl' <...>.

Workaround: Adjust the switch spanning tree priority to eliminate the root-guard inconsistencies.

CR_0000246715

Symptom: The switch fails to properly send traffic over the forwarding switch interfaces.

Scenario: In a stacking configuration running spanning tree in PVST mode, after a redundancy switchover to the standby switch, the switch fails to forward traffic after the switch ports transition from Blocking to Forwarding.

Workaround: Disable and re-enable the affected switch ports.

User Roles

CR_0000245072

Symptom: The switch fails to place authenticated users in the critical authentication role.

Scenario: When RADIUS server tracking is enabled and the RADIUS server is unresponsive, the switch fails to place the authenticated clients in the critical authentication role.

Workaround: Disable RADIUS tracking or configure the initial role with the same privileges as the critical authentication role.

VLAN

CR_0000245933

Symptom: Unable to enter the VLAN context using the name of the VLAN.

Scenario: When using the `vlan <vlan-name>` CLI command to enter the VLAN context, an `Invalid input: <vlan-name>` error is displayed.

Workaround: Use the `vlan <vlan-id>` CLI command to enter the VLAN context.

Web UI

CR_0000243495

Symptom: On the Web UI, the switch fails to display the port list under the Ports status web page.

Scenario: When the LLDP information is updated for a neighbor device, if the SysName contains a colon (":") character, the switch fails to display the port list under the Ports status web page.

Workaround: Avoid using the colon (":") character in SysName on peer devices.

CR_0000245750

Symptom/Scenario: After switch upgrade, when the self-signed certificate is generated, the connection to the switch cannot be established via web server using HTTPS.

Workaround: Downgrade to the lower version, generate the self-signed certificate from that build and use this generated certificate in the upgraded build.

Version 16.07.0002

ACLs

CR_0000245015

Symptom: When an IP access-list is configured with a name containing a dot character, the access-list cannot be modified or deleted.

Scenario: In the VLAN context, when an IP access-group is configured with a name containing a dot character, the access-list cannot be modified or deleted.

Workaround: Configure access-groups with names that do not contain dot characters.

Central

CR_0000237778

Symptom: Login to switch from Central Remote Console System (RCS) may fail.

Scenario: When the switch is configured with local authentication as well as RADIUS/TACACS authentication and the local user credentials are not provisioned in RADIUS/TACACS, Central RCS authentication fails.

Workaround: Add local user credentials to RADIUS/TACACS server.

Certificates

CR_0000245750

Symptom/Scenario: After switch upgrade, when the self-signed certificate is generated, the connection to the switch cannot be established via web server using HTTPS.

Workaround: Downgrade to the lower version, generate the self-signed certificate from that build and use this generated certificate in the upgraded build.

mDNS

CR_0000244624

Symptom: mDNS rule to permit/deny "any" traffic does not work as expected, instead the global default rule to deny all traffic is applied.

Scenario: When the following mDNS rules are created, the "any" keyword will be treated as any other service name and the rule will not allow "any" mDNS traffic through the specified VLANs. Instead, the default rule to deny all traffic is applied.

```
mdns profile "mDNS_Profile1"
  rule 1 service "any" action permit
  vlan 10,20
  exit
mdns profile "mDNS_Profile2"
  rule 1 service "any" action deny
  vlan 30,40
  exit
```

Workaround: Apply permit/deny rule by specifying the exact service name.

RMON

CR_0000244685

Symptom: The switch fails to record some user logout RMON events in the switch event log.

Scenario: When the operator user is configured using the `password operator` command without configuring any manager users, if the user connects to the switching using SSH and logs in as the operator user then moves

to manager mode using the `enable` command and logs out from the SSH session, the RMON log-out event of SSH is not displayed in the event logs.

Workaround: Configure both operator and manager usernames and passwords on the switch.

SNMP

CR_0000245461

Symptom/Scenario: When IPv4 addresses and subnet masks are configured in both ACEs and class entries using SNMP, if the GPPCv2 SNMP code does not contain proper byte-order conversions (NTOHL) for the source and destination IPv4 addresses and their subnet masks, the IP address and subnet mask values are displayed in reverse.

Spanning Tree

CR_0000211478

Symptom: The switch displays the port ID as a + symbol in the output of the `show spanning-tree topo-change-history <...>` command.

Scenario: When the switch is configured with aggregated ports using a trunk ID greater than 4 characters (for example, `trk11`, `trk111`), the switch displays the Port ID as a + symbol in the output of the `show spanning-tree topo-change-history <...>` for those trunk IDs. For example:

Port	Mac Address	Date	Time
+	40a8f0-0e75db	08/18/2016	16:08:18

CR_0000244858

Symptom/Scenario: When the `show spanning-tree detail` command is executed, the output does not list the counters of the 802.1w and 802.1s topology change packets.

Workaround: Execute the `show spanning-tree debug-counters` command to display the counters of the 802.1w and 802.1s topology change packets.

Syslog

CR_0000244622

Symptom: When `logging origin-id hostname` is configured and the hostname length is more than 16 characters, the hostname in the syslog message is truncated.

Scenario: When the hostname is configured with a length of more than 16 characters and the syslog server is configured over UDP, if the origin-id is set to hostname, the hostname in the syslog message is truncated.

Workaround: Configure a shorter hostname where the length is less than or equal to 16 or configure using `logging origin-id ip-address`.

Telnet/SSH

CR_0000244606

Symptom: Telnet/SSH session cannot be established after a period of time.

Scenario: When connecting via telnet/SSH, the switches may report all sessions are in-use (TELNET from <...> is rejected because maximum session limit is reached), even though the `show session-list` command shows connected session under maximum supported.

Transceivers

CR_0000245596

Symptom/Scenario: When `allow-unsupported-transceiver` is enabled on a switch, the supported transceiver is shown as unsupported or excluded. However, when the `allow-unsupported-transceiver` is disabled, the same transceiver works.

Workaround: Disable unsupported transceiver mode config.

VLAN

CR_0000245933

Symptom: Unable to enter the VLAN context using the name of the VLAN.

Scenario: When using the `vlan <vlan-name>` CLI command to enter the VLAN context, an `Invalid input: <vlan-name>` error is displayed.

Workaround: Use the `vlan <vlan-id>` CLI command to enter the VLAN context.

Upgrade information

Upgrading restrictions and guidelines

WB.16.07.0003 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 *ArubaOS-Switch Basic Operations Guide*.

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.

Finding Security Bulletins

Procedure

1. Go to the HPE Support Center - Hewlett Packard Enterprise at www.hpe.com/support/hpesc.
2. Enter your product name or number and click **Go**.
3. Select your product from the list of results.
4. Click the **Top issues & solutions** tab.
5. Click the **Advisories, bulletins & notices** link.

Security Bulletin subscription service

You can sign up at http://www.hpe.com/support/Subscriber_Choice to initiate a subscription to receive future Hewlett Packard Enterprise Security Bulletin alerts via email.

Networking Websites

Hewlett Packard Enterprise Networking Information Library

www.hpe.com/networking/resourcefinder

Hewlett Packard Enterprise Networking Software

www.hpe.com/networking/software

Hewlett Packard Enterprise Networking website

www.hpe.com/info/networking

Hewlett Packard Enterprise My Networking website

www.hpe.com/networking/support

Hewlett Packard Enterprise My Networking Portal

www.hpe.com/networking/mynetworking

Hewlett Packard Enterprise Networking Warranty

www.hpe.com/networking/warranty

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

For additional websites, see [Support and other resources](#).

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
<http://www.hpe.com/assistance>
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
<http://www.hpe.com/support/hpesc>

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:
Hewlett Packard Enterprise Support Center
www.hpe.com/support/hpesc
Hewlett Packard Enterprise Support Center: Software downloads
www.hpe.com/support/downloads
Software Depot
www.hpe.com/support/softwaredepot
- To subscribe to eNewsletters and alerts:
www.hpe.com/support/e-updates
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:
www.hpe.com/support/AccessToSupportMaterials



IMPORTANT: Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

<http://www.hpe.com/support/selfrepair>

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.