

PD.02.22 Release Notes



Copyright Information

© Copyright 2022 Hewlett Packard Enterprise Development LP.

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

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.

Description

This release note covers software versions for the PD.02 branch of the software.

Version PD.02.04 is the initial release of major version PD.02.

Product series supported by this software:

- HPE OfficeConnect 1920S 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 Aruba, unless noted in the table.

Version Number	Release Date	Remarks
PD.02.22	2022-10-27	Released, fully supported, and posted on the web.
PD.02.21	2022-09-12	Released, fully supported, and posted on the web.
PD.02.20	N/A	Not Released.
PD.02.19	2022-01-24	Released, fully supported, and posted on the web.
PD.02.18	2021-09-13	Released, fully supported, and posted on the web.
PD.02.17	2021-05-07	Released, fully supported, and posted on the web.
PD.02.16	2021-01-14	Released, fully supported, and posted on the web.
PD.02.15	2020-10-12	Released, fully supported, and posted on the web.
PD.02.14	2020-06-22	Released, fully supported, and posted on the web.
PD.02.13	2020-03-30	Released, fully supported, and posted on the web.

Version Number	Release Date	Remarks
PD.02.12	2019-12-18	Released, fully supported, and posted on the web.
PD.02.11	2019-10-07	Released, fully supported, and posted on the web.
PD.02.10	2019-08-27	Released, fully supported, and posted on the web.
PD.02.09	2019-05-15	Released, fully supported, and posted on the web.
PD.02.08	2018-12-17	Released, fully supported, and posted on the web.
PD.02.07	n/a	Never released.
PD.02.06	2018-09-20	Released, fully supported, and posted on the web.
PD.02.05	2018-06-27	Released, fully supported, and posted on the web.
PD.02.04	2018-06-01	Initial release of the PD.02 branch of software. Released, but reverted and pulled from the web.
PD.01.08	2018-04-02	Please see the PD.01.08 release notes for detailed information on the PD.01 branch. Released, fully supported, and posted on the web.
PD.01.07	2017-12-14	Released, fully supported, and posted on the web.
PD.01.06	2017-06-30	Released, fully supported, and posted on the web.
PD.01.05	2017-02-28	Released, fully supported, and posted on the web.
PD.01.04	2017-01-03	Released, fully supported, and posted on the web.
PD.01.03	2016-12-08	Initial release of the PD software. Released, fully supported, but not posted to the web.

Products Supported

This release applies to the following product models:

Product number	Description
JL380A	HPE OfficeConnect 1920S 8G Switch

Product number	Description
JL381A	HPE OfficeConnect 1920S 24G 2SFP Switch
JL382A	HPE OfficeConnect 1920S 48G 4SFP Switch
JL383A	HPE OfficeConnect 1920S 8G PPOE+ 65W Switch
JL384A	HPE OfficeConnect 1920S 24G 2SFP PPOE+ 185W Switch
JL385A	HPE OfficeConnect 1920S 24G 2SFP PoE+ 370W Switch
JL386A	HPE OfficeConnect 1920S 48G 4SFP PPOE+ 370W Switch

Compatibility/Interoperability

The switch web agent supports the following web browsers:

Browser	Supported Versions
Internet Explorer	<ul style="list-style-type: none"> ▪ Edge (105) ▪ 11
Chrome	<ul style="list-style-type: none"> ▪ 105 ▪ 104
Firefox	<ul style="list-style-type: none"> ▪ 104 ▪ 103
Safari (MacOS only)	<ul style="list-style-type: none"> ▪ 15 ▪ 14



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

Minimum supported software versions



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

Product Number	Product Name	Minimum Software Version
JL385A	HPE OfficeConnect 1920S 24G 2SFP PoE+ 370W Switch	PD.01.04

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 02.22

No enhancements were included in version 02.22.

Version 02.21

Security

Added security improvements for web access to the switch.

Version 02.20

This software version was not released.

Version 02.19

No enhancements were included in version 02.19.

Version 02.18

No enhancements were included in version 02.18.

Version 02.17

No enhancements were included in version 02.17.

Version 02.16

No enhancements were included in version 02.16.

Version 02.15

No enhancements were included in version 02.15.

Version 02.14

Usability improvements.

Version 02.13

No enhancements were included in version 02.13.

Version 02.12

Password Security

A requirement to modify the switch default password has been added to enhance security of the switch. Upon initial boot-up or following a factory reset, a change to the default password will be required.

Version 02.11

No enhancements were included in version 02.11.

Version 02.10

No enhancements were included in version 02.10.

Version 02.09

No enhancements were included in version 02.09.

Version 02.08

No enhancements were included in version 02.08.

Version 02.07

Version 02.07 was never released.

Version 02.06

MAC Authentication

Added ability to use PAP authentication which sends the MAC address of the client as the password in the User-Password (RADIUS attribute 2) to the authentication server.

Password Manager

Enhanced the help text description of the Encrypted Password checkbox in the "Edit existing user" window to include "If this box is checked, the provided password must be in encrypted format."

Version 02.05

No enhancements were included in version 02.05.

Version 02.04

IGMP Snooping

Added support for per-VLAN IGMP snooping and static mrouter port configuration.

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.

Version 02.22

Security

PD0222-01

Symptom/Scenario: Resolved a security related defect when using the forced password update feature.

Version 02.21

No fixes were included in version 02.21.

Version 02.20

This version was not released.

Version 02.19

Web UI

PD0219-01

Symptom/Scenario: The current copyright statement is not up to date.

Version 02.18

Patches applied to various open source components.

Version 02.17

ARP

CR_254987

Symptom/Scenario: In networks with a high amount of ARP traffic (for example, APR flooding), the ARP table exceeds its maximum limit, causing the switch to reset.

Workaround: Identify and resolve the source of excessive ARP traffic on the network.

Version 02.16

IGMP Snooping

PD0216-03

Symptom/Scenario: When IGMP snooping is enabled for VLANs, IPv6 router advertisements are blocked.

Workaround: Enabled IGMP snooping on individual ports rather than per VLAN.

Web UI

CR_254616

Symptom/Scenario: When using the Chrome browser, the browser reports the SSL certificate is invalid.

Workaround: Use the Internet Explorer or Firefox web browsers.

PD0216-01

Symptom/Scenario: The Web UI allows SFP ports to be set at a 100MB link speed.

PD0216-02

Symptom/Scenario: Non-default HTTP/HTTPS session timeout values are not preserved following a reboot.

Version 02.15

SNMPv3

CR_0000248798

RADIUS

Symptom/Scenario: The switch fails to perform dynamic VLAN assignment after MAC authentication.

Web Management

CR_0000253436

Symptom/Scenario: Non-default HTTPS port configuration is not taking effect after performing configuration backup and restore.

Workaround: Utilize default HTTPS port setting 443.

Version 02.14

No fixes were included in version 02.14.

Version 02.13

ARP

CR_0000252400

Symptom/Scenario: Proxy-ARP settings revert to factory defaults after a switch reboot.

MAC Authentication

CR_0000248798

RADIUS

Symptom/Scenario: The switch fails to perform dynamic VLAN assignment after MAC authentication.

RADIUS

CR_0000251834

Symptom: RADIUS accounting is not active, even though it has been enabled on the switch.

Scenario: When RADIUS authentication and accounting have been configured on the switch, the **calling_station_id** and **called_station_id** fields display invalid MAC addresses, causing RADIUS accounting to fail.

Version 02.12

LLDP

CR_0000251449

Symptom/Scenario: Unsupported discovery protocol frames are transmitted by the switch with destination address: 01:00:0c:cc:cc:cc.

Management

CR_0000250690

Symptom/Scenario: The web-interface accepts an invalid SNMP view name of 'default'.

Version 02.11

System

CR_0000250982

Symptom/Scenario: When MAC addresses age out, the switch may spontaneously reset.

Workaround: Increasing MAC address aging time to the maximum value will reduce the frequency of occurrence.

Version 02.10

System

PD0210-01

Symptom/Scenario: Occasionally, the switch improperly removes individual MAC addresses from the system and may result in an unexpected reset.

Workaround: Increasing the MAC address aging time to the maximum value will reduce the frequency of occurrence.

Version 02.09

RADIUS

CR_0000248798

RADIUS

Symptom/Scenario: The switch fails to perform dynamic VLAN assignment after MAC authentication.

System

CR_0000248755/CR_0000249838

Symptom/Scenario: The switch randomly resets during periods of high sustained traffic volume directed at the CPU.

Version 02.08

Management VLAN

CR_0000247836

Symptom/Scenario: If a second VLAN (non-management VLAN) is created, the clients connected to that non-management VLAN can establish an HTTP connection to the management interface of the switch when such a connection should only be allowed from the management VLAN.

SNMP

PD0208-01

Symptom/Scenario: The switch permits SNMP community name configurations but they are not applied until after the switch is rebooted.

System

CR_0000247865

Symptom/Scenario: The switch randomly resets during periods of sustained high traffic volumes directed at the CPU.

Web UI

CR0000247549

Symptom/Scenario: When using software version PD.02.06, disabling both HTTP & HTTPS results in loss of access to the web interface.

CR0000247995

Symptom/Scenario: When using software version PD.02.06, the attempts to save files from the switch with HTTP or HTTPS timeout.

Workaround: Use TFTP to save files.

Version 02.07

Version 02.07 was never released.

Version 02.06

MAC Authentication

CR_0000243416

Symptom/Scenario: Utilizing PAP authentication with MAC auth results in an error due to being an unsupported setting.

Workaround: Use MD5 authentication method.

Password Manager

PD0206-02

Symptom/Scenario: With encryption enabled, attempting to enter a non-encrypted password displays an invalid error message.

Workaround: Disable encryption and reenter the password or enter an encrypted password.

Web Management

PD0206-01

Symptom/Scenario: An Ajax scripting error message appears when attempting firmware update over HTTP.

Workaround: Use TFTP for firmware upgrades or reattempt the firmware upgrade over HTTP.

Version 02.05

Port Connectivity

PD0205-01

Symptom: SFP ports on the HPE OfficeConnect 1920S 48G 4SFP Ppoe+ 370W Switch (JL386A) do not establish a link or convey switch traffic.

Scenario: After installing PD.02.04 on the HPE OfficeConnect 1920S 48G 4SFP PPoE+ 370W Switch (JL386A), SFP ports do not establish a link or convey switch traffic. SFP port LEDs may flash continually, indicating a fault condition.

Version 02.04

Certificates

PD0204-01

Symptom/Scenario: Updating self-signed certificate generation from SHA1 to SHA256 and public key length from 1024 to 2048 bits.

Workaround: Utilize a CA signed certificate that can be manually uploaded to the 1920S.

LLDP

CR_0000244109

Symptom/Scenario: If a connected device sends an LLDP TLV in "string" format to the 1920 switch, a software crash occurs requiring a reboot to clear.

Workaround: Configure connected devices to send LLDP TLV's in "normal" format.

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.

Trunking

PD0107-02

Symptom/Scenario: The Protected Ports configuration modal does not allow selection of ports belonging to trunk groups.

Upgrade Information

Use Update Manager to update/downgrade switch software

1. Navigate to the Maintenance > Backup and Update Manager page.
2. Select either HTTP, SFTP, or TFTP from the Update – Transfer a file to the switch column.
3. The modal window appears.
4. Select Backup Code from the menu.



The selection is named "Backup Code" because the firmware update occurs on the backup image – not the active/primary image. This prevents the active image from being corrupted during the firmware update, for example, a power failure occurring during the update process.

5. When using the Update Manager for the firmware update, the Digital Signature Verification option should be selected.

6. Provide the firmware image name, IP address and path appropriate for the file transfer method – either HTTP, SFTP, or TFTP.
7. Select Begin Transfer.
Firmware update runs to completion.
8. Once the firmware update is done, you are presented with an option to reboot the switch and activate the backup image.
9. If you select OK, the software reboots the switch and activates the newly installed image. The previous active/primary image becomes the backup image.
10. If you select Cancel, the software closes the window without activating the newly installed image.
11. To activate the newly installed image later:
 - a. Navigate to Maintenance > Dual Image Configuration.
 - b. Select Next Active > Backup. Then, click Apply.
12. See the HPE OfficeConnect 1920S Switches Management and Configuration Guide for additional information.

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/support-services/sirt/>. Security advisories can be found at <https://www.arubanetworks.com/support-services/security-bulletins/>.

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.