PD.02.10 Release Notes

a Hewlett Packard
Enterprise company

Part Number: 5200-6606
Published: August 2019
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

Intel®, Itanium®, Pentium®, Xeon®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the U.S. and other countries.

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

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

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 Hewlett Packard Enterprise, unless noted in the table.

Version number	Release date	Based on	Remarks
PD.02.10	2019-08-27	PD.02.09	Released, fully supported, and posted on the web.
PD.02.09	2019-05-15	PD.02.08	Released, fully supported, and posted on the web.
PD.02.08	2018-12-17	PD.02.07	Released, fully supported, and posted on the web.
PD.02.07	n/a	PD.02.06	Never released.
PD.02.06	2018-09-20	PD.02.05	Released, fully supported, and posted on the web.
PD.02.05	2018-06-27	PD.02.04	Released, fully supported, and posted on the web.
PD.02.04	2018-06-01	PD.01.08	Initial release of the PD.02 branch of software. Released, but reverted and pulled from the web.
PD.01.08	2018-04-02	PD.01.07	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	PD.01.06	Released, fully supported, and posted on the web.
PD.01.06	2017-06-30	PD.01.05	Released, fully supported, and posted on the web.

Table Continued

Version number	Release date	Based on	Remarks
PD.01.05	2017-02-28	PD.01.04	Released, fully supported, and posted on the web.
PD.01.04	2017-01-03	PD.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
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	• Edge • 11
Chrome	• 53 • 52
Firefox	• 49 • 48
Safari (MacOS only)	• 10 • 9

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

Minimum supported software versions

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

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 02.10

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.

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

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

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.

NOTE: 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.

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.