



**Hewlett Packard**  
Enterprise

## **PD.01.04 Release Notes**

### **Abstract**

This document contains supplemental information for the PD.01.04 release.

Part Number: 5200-3426  
Published: March 2017  
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<sup>®</sup>, Itanium<sup>®</sup>, Pentium<sup>®</sup>, Intel Inside<sup>®</sup>, and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

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

Adobe<sup>®</sup> and Acrobat<sup>®</sup> are trademarks of Adobe Systems Incorporated.

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

UNIX<sup>®</sup> is a registered trademark of The Open Group.

# Contents

<b>PD.01.04 Release Notes.....</b>	<b>5</b>
Description.....	5
Important information.....	5
Version history.....	5
Products supported.....	5
Compatibility/interoperability.....	5
Minimum supported software versions.....	6
Enhancements.....	6
Version PD.01.04.....	6
Support for JL385A.....	6
Fixes.....	6
Version PD.01.04.....	7
ACLs.....	7
AutoDoS.....	7
HTTPS.....	7
LEDs.....	7
Port Configuration.....	7
SNMP.....	7
Spanning Tree.....	8
Traceroute.....	8
Issues and workarounds.....	8
Password Manager.....	8
PD0104-I02.....	8
PD0104-I05.....	8
Port Configuration.....	8
PD0104-I03.....	9
Spanning Tree.....	9
PD0104-I04.....	9
Storm control.....	9
PD0104-I01.....	9
Web UI.....	9
PD0104-I06.....	9
Upgrade information.....	9
<b>Hewlett Packard Enterprise security policy.....</b>	<b>11</b>
Finding Security Bulletins.....	11
Security Bulletin subscription service.....	11
<b>Websites.....</b>	<b>12</b>
<b>Support and other resources.....</b>	<b>13</b>
Accessing Hewlett Packard Enterprise Support.....	13
Accessing updates.....	13
Customer self repair.....	13
Remote support.....	14
Warranty information.....	14

Regulatory information.....	14
Documentation feedback.....	15

# PD.01.04 Release Notes

## Description

This release note covers software versions for the PD.01 branch of the software.

Version PD.01.03 was the initial build of major version PD.01.

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.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	<ul style="list-style-type: none"> <li>• Edge</li> <li>• 11</li> </ul>
Chrome	<ul style="list-style-type: none"> <li>• 53</li> <li>• 52</li> </ul>
Firefox	<ul style="list-style-type: none"> <li>• 49</li> <li>• 48</li> </ul>
Safari (MacOS only)	<ul style="list-style-type: none"> <li>• 10</li> <li>• 9</li> </ul>

## 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 PD.01.04

#### Support for JL385A

Support for JL385A, HPE 1920S 24G 2SFP PoE+ 370W Switch, has been added.

## 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 PD.01.04

### ACLs

#### PD0104-08

**Symptom/Scenario:** When editing ACL rules, configuration settings are cleared when selecting any of the tool tip icons marked with a ? symbol.

**Workaround:** ACL rule settings may be restored by manually reentering them.

#### PD0104-10

**Symptom:** The ICMP code value for an IPv4 Extended ACL is misconfigured to 256 if left blank.

**Scenario:** When configuring an IPv4 Extended ACL, if the ICMP code value is left blank the software will misconfigure the setting to 256.

**Scenario:** Configure the ICMP code setting to the desired value.

### AutoDoS

#### PD0104-11

**Symptom:** The **Advance Security Configuration Help** page does not correctly call out scenarios for packet drop when "Prevent Invalid TCP Flags Attack" is set.

**Scenario:** Help page indicates that the switch drops packets when TCP Flags **SYN** and **FIN** are set. In addition, the switch drops packets when the TCP flag SYN is set and the Source Port is less than 1024.

### HTTPS

#### PD0104-07

**Symptom/Scenario:** HTTPS can be enabled when the required self-signed certificate is absent.

**Workaround:** From the HTTPS page, select **Download certificate**.

### LEDs

#### PD0104-06

**Symptom:** Incorrect Fault/Locator LED behavior when pressing reset button.

**Scenario:** When pressing the reset button on the switch, the Fault/Locator LED will repeat the solid orange - turn off - blink 3 times - turn off sequence multiple times instead of just once.

### Port Configuration

#### PD0104-02

**Symptom:** The port mirroring Direction field displays N/A when mirroring traffic from a VLAN.

**Scenario:** When mirroring traffic from a VLAN, the Direction field should display the configured value R<sub>x</sub> but incorrectly displays the value N/A.

#### PD0104-03

**Symptom/Scenario:** The port mirroring source, with type **VLAN**, can be overwritten by type **Interface** for the same session ID. Port mirroring may have only one source type per session ID: **Interface** or **VLAN**.

**Workaround:** Manually remove port mirroring source type **VLAN** prior to configuring type **Interface**.

### SNMP

#### PD0104-17

**Symptom:** Unable to configure SNMPv3 permit/deny access to specified OID branch views.

**Scenario:** Configuration settings to customize OID branch views and access privileges are missing from the web interface, preventing configuration of SNMPv3 permit/deny access to specified OID branch views.

## Spanning Tree

### PD0104-01

**Symptom:** Spanning-tree configuration status is not updated on the port status table.

**Scenario:** The port configuration status page does not update properly when spanning-tree admin mode is enabled or disabled.

**Workaround:** Navigate to the Spanning-tree page to view the correct spanning tree status.

### PD0104-15

**Symptom/Scenario:** The port path cost is incorrectly displayed in the web interface as 0.

## Traceroute

### PD0104-09

**Symptom:** Unable to configure a VLAN ID as a source for Traceroute.

**Scenario:** **VLAN interface** is missing from the Traceroute **Source Interface** dropdown, preventing configuration of a VLAN ID as a source for Traceroute.

### PD0104-14

**Symptom:** The web interface displays invalid settings for the Traceroute IPv6 source IP address / Interface field.

**Scenario:** On the Traceroute IPv6 web page, when Source is set to **IP Address** or **Interface**, traceroute fails since IPv6 routing is unsupported.

**Workaround:** Select "None" for Source and Traceroute IPv6 will work

## 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.

## Password Manager

### PD0104-I02

**Symptom:** An incorrect error description is displayed when attempts are made to reuse a password that exceeds the password history value.

**Scenario:** When attempting to reuse a password that exceeds the password history value the error message `user does not exist` is displayed.

**Workaround:** Click **OK** and configure a new password or increase the password history value.

### PD0104-I05

**Symptom/Scenario:** Password expiration time isn't synchronized with the system clock.

## Port Configuration



## PD0104-I03

**Symptom/Scenario:** Switch will generate an invalid warning message when attempting to configure a port that isn't part of the management VLAN.

**Workaround:** Click **OK** and continue with port configuration.

## Spanning Tree

### PD0104-I04

**Symptom/Scenario:** Topology change notification values in the Support file don't match the MSTP web page.

**Workaround:** Utilize the MSTP web page to view the topology change notification value.

## Storm control

### PD0104-I01

**Symptom:** Auto-recovery timer is reverting to the default setting following a reboot.

**Scenario:** If the switch is rebooted when a port is in a disabled state for exceeding the storm control threshold, the auto-recovery timer is reset to the default value of 300 seconds instead of adhering to the user defined setting.

**Workaround:** Reconfigure the auto-recovery timer following a reboot.

## Web UI

### PD0104-I06

**Symptom/Scenario:** Description fields that use special characters are not retained.

**Symptom/Scenario:** When the following special characters are used in Dual Image configuration, Spanning Tree Switch configuration, SNMP Community configuration, SNMP Trap Receivers v1 or v2, Protected ports, or VLAN names the settings are not retained: !, ", #, \$, %, &, ', (, ), \*, or +

## 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.

# Hewlett Packard Enterprise 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.

## Finding Security Bulletins

### Procedure

1. Go to the HPE Support Center - Hewlett Packard Enterprise at [www.hpe.com/support/hpesc](http://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 [www4.hpe.com/signup\\_alerts](http://www4.hpe.com/signup_alerts) to initiate a subscription to receive future Hewlett Packard Enterprise Security Bulletin alerts via email.

# Websites

## Networking Websites

<b>Hewlett Packard Enterprise Networking Information Library</b>	<a href="http://www.hpe.com/networking/resourcefinder"><u>www.hpe.com/networking/resourcefinder</u></a>
<b>Hewlett Packard Enterprise Networking Software</b>	<a href="http://www.hpe.com/networking/software"><u>www.hpe.com/networking/software</u></a>
<b>Hewlett Packard Enterprise Networking website</b>	<a href="http://www.hpe.com/info/networking"><u>www.hpe.com/info/networking</u></a>
<b>Hewlett Packard Enterprise My Networking website</b>	<a href="http://www.hpe.com/networking/support"><u>www.hpe.com/networking/support</u></a>
<b>Hewlett Packard Enterprise My Networking Portal</b>	<a href="http://www.hpe.com/networking/mynetworking"><u>www.hpe.com/networking/mynetworking</u></a>
<b>Hewlett Packard Enterprise Networking Warranty</b>	<a href="http://www.hpe.com/networking/warranty"><u>www.hpe.com/networking/warranty</u></a>

## General websites

<b>Hewlett Packard Enterprise Information Library</b>	<a href="http://www.hpe.com/info/EIL"><u>www.hpe.com/info/EIL</u></a>
---	---

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

# 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](http://www.hpe.com/support/hpesc)

**Hewlett Packard Enterprise Support Center: Software downloads**

[www.hpe.com/support/downloads](http://www.hpe.com/support/downloads)

**Software Depot**

[www.hpe.com/support/softwaredepot](http://www.hpe.com/support/softwaredepot)

- To subscribe to eNewsletters and alerts:

[www.hpe.com/support/e-updates](http://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](http://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

<b>HPE Get Connected</b>	<a href="http://www.hpe.com/services/getconnected">www.hpe.com/services/getconnected</a>
<b>HPE Proactive Care services</b>	<a href="http://www.hpe.com/services/proactivecare">www.hpe.com/services/proactivecare</a>
<b>HPE Proactive Care service: Supported products list</b>	<a href="http://www.hpe.com/services/proactivecaresupportedproducts">www.hpe.com/services/proactivecaresupportedproducts</a>
<b>HPE Proactive Care advanced service: Supported products list</b>	<a href="http://www.hpe.com/services/proactivecareadvancedsupportedproducts">www.hpe.com/services/proactivecareadvancedsupportedproducts</a>

### Proactive Care customer information

<b>Proactive Care central</b>	<a href="http://www.hpe.com/services/proactivecarecentral">www.hpe.com/services/proactivecarecentral</a>
<b>Proactive Care service activation</b>	<a href="http://www.hpe.com/services/proactivecarecentralgetstarted">www.hpe.com/services/proactivecarecentralgetstarted</a>

## Warranty information

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

[www.hpe.com/support/Safety-Compliance-EnterpriseProducts](http://www.hpe.com/support/Safety-Compliance-EnterpriseProducts)

### Additional warranty information

<b>HPE ProLiant and x86 Servers and Options</b>	<a href="http://www.hpe.com/support/ProLiantServers-Warranties">www.hpe.com/support/ProLiantServers-Warranties</a>
<b>HPE Enterprise Servers</b>	<a href="http://www.hpe.com/support/EnterpriseServers-Warranties">www.hpe.com/support/EnterpriseServers-Warranties</a>
<b>HPE Storage Products</b>	<a href="http://www.hpe.com/support/Storage-Warranties">www.hpe.com/support/Storage-Warranties</a>
<b>HPE Networking Products</b>	<a href="http://www.hpe.com/support/Networking-Warranties">www.hpe.com/support/Networking-Warranties</a>

## 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](http://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](http://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](http://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](http://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](mailto: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.