PT.02.19 Release Notes

a Hewlett Packard
Enterprise company

Published: February 2024
Edition: 1

Release Notes

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 beginning with PT.02.01.

Version PT.02.01 is the initial release of major version PT.02 software. PT.02.01 includes all enhancements and fixes in the PT.01.18 software, plus the additional enhancements and fixes in the PT.02.01 enhancements and fixes sections of this release note.

Product series supported by this software:

- HPE OfficeConnect 1820 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	Release date	Remarks
PT.02.19	2024-02-13	Released, fully supported, and posted on the web.
PT.02.18	2023-04-11	Released, fully supported, and posted on the web.
PT.02.17	2022-12-20	Released, fully supported, and posted on the web.
PT.02.16	2022-10-27	Released, fully supported, and posted on the web.
PT.02.15	2022-09-12	Released, fully supported, and posted on the web.
PT.02.14	2022-02-28	Released, fully supported, and posted on the web.
PT.02.13	2021-01-24	Released, fully supported, and posted on the web.
PT.02.12	2021-05-07	Released, fully supported, and posted on the web.

Version	Release date	Remarks
PT.02.11	2021-01-14	Released, fully supported, and posted on the web.
PT.02.10	2020-10-12	Released, fully supported, and posted on the web.
PT.02.09	2020-06-22	Released, fully supported, and posted on the web.
PT.02.08	2019-12-18	Released, fully supported, and posted on the web.
PT.02.07	2019-05-15	Released, fully supported, and posted on the web.
PT.02.06	2018-09-20	Released, fully supported, and posted on the web.
PT.02.05	2018-04-02	Released, fully supported, and posted on the web.
PT.02.04	2017-12-19	Released, fully supported, and posted on the web.
PT.02.03	2017-06-30	Released, fully supported, and posted on the web.
PT.02.02	2017-04-10	Released, fully supported, and posted on the web.
PT.02.01	2017-01-06	Initial release of PT.02. Released, fully supported, and posted on the web.
PT.01.14	2016-06-06	Please see the PT.01.14 release note for information on the PT.01 branch. Released, fully supported, and posted on the web.
PT.01.13	2016-01-06	Released, fully supported, and posted on the web.
PT.01.12	n/a	Never released.
PT.01.11	2015-10-27	Released, fully supported, and posted on the web.
PT.01.10	2015-08-21	Released, fully supported, and posted on the web.
PT.01.09	n/a	Never released.
PT.01.08	n/a	Never released.
PT.01.07	n/a	Never released.
PT.01.06	2015-03-30	Released, fully supported, and posted on the web.

Version	Release date	Remarks
PT.01.05	n/a	Never built.
PT.01.04	2015-03-30	Initial release of PT.01, fully supported, and posted on the web.

Products Supported

This release applies to the following product models:

Product number	Description
J9979A	HPE OfficeConnect 1820 8G Switch
J9980A	HPE OfficeConnect 1820 24G Switch
J9981A	HPE OfficeConnect 1820 48G Switch
J9982A	HPE OfficeConnect 1820 8G PoE+ (65W) Switch
J9983A	HPE OfficeConnect 1820 24G PoE+ (185W) Switch
J9984A	HPE OfficeConnect 1820 48G PoE+ (370W) Switch

Compatibility/Interoperability

The switch web agent supports the following web browsers:

Browser	Supported versions
Internet Explorer	▪ Edge (105) ▪ 11
Chrome	▪ 105 ▪ 104
Firefox	▪ 104 ▪ 103
Safari (MacOS only)	▪ 15 ▪ 14

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

Minimum Supported Software Versions

Product number	Product name	Minimum supported software version
J9979A	HPE OfficeConnect 1820 8G Switch	PT.01.04
J9980A	HPE OfficeConnect 1820 24G Switch	PT.01.04
J9981A	HPE OfficeConnect 1820 48G Switch	PT.01.04
J9982A	HPE OfficeConnect 1820 8G PoE+ (65W) Switch	PT.01.04
J9983A	HPE OfficeConnect 1820 24G PoE+ (185W) Switch	PT.01.04
J9984A	HPE OfficeConnect 1820 48G PoE+ (370W) Switch	PT.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 02.19

Added security improvements for web management.

Version 02.18

No enhancements were added in version 02.18.

Version 02.17

Security

Added security improvements for web-management.

Version 02.16

No enhancements were included in version 02.16.

Version 02.15

Security

Added security improvements for web access to the switch.

Version 02.14

No enhancements were included in version 02.14.

Version 02.13

No enhancements were included in version 02.13.

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

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 02.07

No enhancements were included in version 02.07.

Version 02.06

No enhancements were included in version 02.06.

Version 02.05

No enhancements were included in version 02.05.

Version 02.04

No enhancements were included in version 02.04.

Version 02.03

Web UI

Added support to display user-defined port descriptions on the **Port Configuration > Status** page and the **Device Image** displayed at the top of each web page.

Version 02.02

No enhancements were included in version 02.02.

Version 02.01

Branding

The web management interface has been changed to reflect the product branding of HPE OfficeConnect.

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 02.19

No fixes were included in version 02.19.

Version 02.18

Configuration

PT0218-01

Symptom/Scenario: Users were unable to upload the configuration file using HTTP following a firmware upgrade to PT.02.17. This issue is now resolved.

Version 02.17

Security

PT0217-01

Symptom/Scenario: Resolved a security related defect when using the Support File feature.

Version 02.16

Security

PT0216-01

Symptom/Scenario: Resolved an issue where HTTPS became disabled following firmware upgrade to PT.02.15 from previous releases.

PT0216-02

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

Version 02.15

Security

PT0214-01

Symptom/Scenario: Web access to the switch failed on newer web browsers. Security improvements for web access to the switch resolved this issue.

Version 02.14

IGMP Snooping

PT0214-01

Symptom/Scenario: Multicast traffic might be dropped from the switch, when multiple multicast streams are received on multiple ports.

Version 02.13

VLANS

PT0213-01

Symptom/Scenario: Saving ports untagged membership to VLANs to which they already belong causes random ports to end up in an **Excluded** state following a reboot.

Web UI

PT0213-02

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

PT0213-03

Symptom/Scenario: The device image graphic displayed in the web-interface is missing port #32.

Workaround: Mouse over the device image ports to display the port number in a tool tip.

Version 02.10

Syslog

CR_0000254031

Symptom/Scenario: The switch forwards the syslog events to both the current and previously configured server address.

Version 02.09

PT0209-01

Symptom/Scenario: An error is generated when a colon (:) symbol is used in the port description field.

Workaround: Do not use a colon (:) symbol in the port description field.

Version 02.08

CR_0000251069

Symptom/Scenario: Use of an apostrophe (') in the Port Description field causes web page corruption.

Workaround: Use special characters other than the apostrophe symbol.

Version 02.07

System

CR_0000248051

Symptom/Scenario: The switch periodically fails to properly initialize communications between ports 1-24 and 25-48.

Workaround: Rebooting the switch will re-initialization communications across all ports.

Version 02.06

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.

Web Management

CR_0000244869

Symptom/Scenario: A trunk group set with priority 0 causes a page loading fault on the spanning-tree page.

Workaround: Set trunk group priority to a non-zero value.

Version 02.05

Version 02.04

Spanning Tree

CR_0000236906

Symptom: The spanning tree switch priority is not displayed correctly in the Support File.

Scenario: After enabling and modifying the spanning tree switch priority is not update properly on the Diagnostics > Support File page.

Workaround: The correct spanning tree switch priority is displayed on the Spanning Tree > Configuration page.

VLAN

CR_0000227723

Symptom: On rare occasion, ports may become orphaned when switching port memberships between VLANS.

Scenario: If VLAN ports or port memberships are switched between VLANS, they may become orphaned and no longer visible in the web interface.

Workaround: Delete the VLAN where ports have been assigned but are no longer visible, then recreate the VLAN and reassign the ports.

Web UI

PC0106-01

Symptom: Action buttons are missing from the web interface when using a Chrome web browser.

Scenario: The web UI will load in a read-only state and not allow configuration modifications due to missing Action buttons when using Chrome version 61.0.3163.100.

Workaround: The web UI will load and display the Action buttons properly when using supported versions of Internet Explorer and Firefox.

Version 02.03

VLAN

CR_0000232483

Symptom/Scenario: The web UI will not allow the Management VLAN configuration to contain only a trunk group.

Workaround: In addition to the trunk group, add a physical port to the Management VLAN configuration.

Version 02.02

PoE

CR_0000228055

Symptom/Scenario: PoE schedule isn't properly applied to the second periodic entry.

SNMP

CR_0000226390

Symptom/Scenario: SNMP returns an invalid value for VLAN untagged port membership.

Syslog

PT2201

Symptom/Scenario: Modified the factory default setting for syslog to enabled.

Workaround: Syslog may be manually enabled from the Log Configuration webpage.

Web UI

CR_0000228334

Symptom/Scenario: The Clear Unexpected Restart button and Crash Log window are missing from the web management interface.

Version 02.01

LLDP Remote Devices Page Parsing Error

Fixes an issue in which using the single quote (') character in port description or system name fields will result in a formatting error in the LLDP remote devices page.

Unexpected Restart

Fixes an issue in which the message "An unexpected restart has occurred. Switch was reset due to power disruption" is displayed when booting the box for the first time.

Upgrade Information

To upgrade the software:

1. Navigate to the **Maintenance > Backup and Update Manager** page.
2. Select either **HTTP** 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 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 HP 1820 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/en-au/support-services/sirt/. Security bulletins can be found at https://www.arubanetworks.com/en-au/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.