

# H.10.117 Release Notes

## Abstract

This document contains supplemental information for the H.10.117 release.



© Copyright 2015 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP 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.

The information contained herein is subject to change without notice. The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.

#### **Acknowledgments**

Microsoft®, Windows®, and Windows Server® are trademarks of the Microsoft group of companies.

---

# Contents

1 H.10.117 Release Notes.....	6
Description.....	6
Important information.....	6
Products supported.....	6
Compatibility/interoperability.....	6
Enhancements.....	7
Fixes.....	7
Version H.10.117.....	7
SFTP.....	7
Web Management.....	7
Version H.10.115.....	7
Stacking.....	7
Web Management.....	7
Version H.10.114.....	7
Command Authorization.....	7
Config.....	7
Version H.10.113.....	8
Crash.....	8
Version H.10.112.....	8
Crash.....	8
DHCP Snooping.....	8
Version H.10.111.....	8
802.1X.....	8
MAC Tables.....	8
Web Management.....	8
Version H.10.110.....	8
Config.....	8
RADIUS.....	8
Version H.10.109.....	9
Loop Protection.....	9
Multicast.....	9
SNMP.....	9
Version H.10.108.....	9
802.1X.....	9
CLI.....	9
Crash.....	9
File Transfer.....	9
Multiple Symptoms.....	9
SNMP.....	9
Version H.10.107.....	10
CLI.....	10
IGMP.....	10
QoS.....	10
SNMP.....	10
Syslog.....	10
Version H.10.104.....	10
Authentication.....	10
Secure Copy.....	10
Version H.10.103.....	10
CLI.....	10
QoS.....	10

Version H.10.102.....	10
MAC Authentication.....	10
Web Management.....	10
Version H.10.101.....	11
CLI.....	11
Crash.....	11
Version H.10.100.....	11
SSL.....	11
Version H.10.99.....	11
802.1X.....	11
Version H.10.98.....	11
FFI/Config.....	11
SSL.....	11
Version H.10.97.....	11
Authentication.....	11
SSH.....	11
Version H.10.96.....	12
CLI.....	12
Web Management.....	12
Version H.10.95.....	12
Management.....	12
Version H.10.94.....	12
DHCP.....	12
Routing.....	12
STP.....	12
Version H.10.93.....	12
LLDP-MED.....	12
Version H.10.92.....	12
CLI.....	12
DHCP Snooping.....	12
Spanning Tree.....	12
Version H.10.91.....	13
Console.....	13
Crash.....	13
LLDP-MED.....	13
SNMP/Config.....	13
STP.....	13
UDLD.....	13
Version H.10.90.....	13
GVRP.....	13
LLDP.....	13
Stacking.....	13
Version H.10.89.....	14
Authentication.....	14
Config.....	14
Unauthenticated VLAN.....	14
Version H.10.88.....	14
SNMP/Config.....	14
Switch Tables.....	14
Version H.10.87.....	14
CDP.....	14
CPU Utilization.....	14
Crash.....	14
Version H.10.86.....	14
802.1X.....	14

Authentication.....	15
CDP.....	15
Config.....	15
DHCP Snooping.....	15
Management.....	15
SSH.....	15
UDLD.....	15
Version H.10.85.....	15
Authentication.....	15
GVRP.....	15
RADIUS Accounting.....	15
UDLD.....	15
Version H.10.84.....	16
802.1X.....	16
Command Authorization.....	16
DHCP Snooping.....	16
Web Management.....	16
Upgrade information.....	16
Upgrading restrictions and guidelines.....	16
Contacting HP.....	16
HP security policy.....	16
Related information.....	17
Documents.....	17
Websites.....	17
Documentation feedback.....	17

# 1 H.10.117 Release Notes

## Description

This release note covers software versions beginning with H.10.84. For information about earlier software versions, please see the H.10.83 release notes.

Product series supported by this software:

- HP 2600 Switch Series

## Important information

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

## Products supported

This release applies to the following product models:

Product number	Description
J4900A/B/C	HP 2626 Switch
J4899A/B/C	HP 2650 Switch
J8164A	HP 2626-PWR Switch
J8165A	HP 2650-PWR Switch
J8762A	HP 2600-8-PWR Switch with Gigabit Uplink

## Compatibility/interoperability

The switch web agent supports the following operating system and web browser combinations:

Operating System	Supported Web Browsers
Windows XP SP3	Internet Explorer 7, 8 Firefox 12
Windows 7	Internet Explorer 9, 10 Firefox 24 Chrome 30
Windows 8	Internet Explorer 9, 10 Firefox 24 Chrome 30
Windows Server 2008 SP2	Internet Explorer 8, 9 Firefox 24
Windows Server 2012	Internet Explorer 9, 10 Firefox 24
Macintosh OS	Firefox 24

## Enhancements

This section lists released builds that include enhancements. Software enhancements are listed in reverse-chronological order, with the newest at the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier editions.

---

**NOTE:** The number preceding the enhancement description is used for tracking purposes.

---

No enhancements have been introduced since H.10.83.

## Fixes

Software fixes are listed in reverse-chronological order, from newest to oldest software version. Unless otherwise noted, each software version listed includes all the software fixes and enhancements added in previous versions listed below.

---

**NOTE:** The number preceding the fix description is used for tracking purposes.

---

## Version H.10.117

### SFTP

**CR\_0000154313** With SSH enabled, attempting SFTP transfers might cause the switch to reboot unexpectedly with a message similar to `TLB Miss: Virtual Addr=0x0000001c IP=0x8008b24c Task='tSftp0', Task ID=0x85717f10 fp:0x85d83a38 sp:0x85717d58 ra:0x8008b1c8 sr:0x1000fc01`.

### Web Management

**CR\_0000162905** When a user connects to an IP address on the switch using a browser with Java version 7U51 or later, the web interface will be blocked because the Java applets were not code-signed. This issue was already fixed in a previous version, but required a re-implementation.

## Version H.10.115

### Stacking

**CR\_0000146549** If the switches are configured to disable HTTP (**no web-management**) and instead use HTTPS (**web-management ssl**), some stack members might not be accessible from the commander.

### Web Management

**CR\_0000145618** The Web user interface is inaccessible to clients using Java version 7, update 51 (Java 7u51).

## Version H.10.114

### Command Authorization

**CR\_0000137774** When issuing a command such as `show tech` (which invokes many sub-commands), if any of the sub-commands are on the HP-Command-Exception "DenyList", the command fails and the user is removed from enable mode.

### Config

**CR\_0000135481** After boot, a config file that has a trap destination community name with an open parenthesis "(" or a close parenthesis ")" cannot be downloaded to the switch.

## Version H.10.113

### Crash

**CR\_0000139768** When the switch receives multiple requests to download the config file via SFTP, the switch might reboot unexpectedly with a message similar to Software exception at exception.c:373 -- in 'tSsh0', task ID = 0x145d168 -> Memory system error at 0x15a5d58 - memPartFree.

## Version H.10.112

### Crash

**CR\_0000131197** With MSTP enabled, a large number of MAC address moves and/or learns might cause the switch to reboot unexpectedly with a message similar to Software exception at svc\_misc.c:514 -- in 'mMstpCtrl', task ID = 0x1637388, -> No memory available.

### DHCP Snooping

**CR\_0000126311** The CLI entry **dhcp-snooping option 82 untrusted-policy keep** is not included in the config file if **no dhcp-snooping option 82** is also configured. If the config file is saved to a TFTP server, it will not function properly when subsequently loaded on a switch.

## Version H.10.111

### 802.1X

**CR\_0000108818** CPU utilization becomes very high when 802.1X is enabled on a port, and the switch also has ports blocked by Spanning Tree.

### MAC Tables

**CR\_0000120855** MAC address entries in the hardware and software tabled might become out of sync. This has been observed to cause problems with DHCP snooping. For example, a client does not receive a DHCP Offer because the switch does not have the client's MAC address in its table and therefore DHCP snooping does not allow the switch to forward the DHCP Offer.

### Web Management

**CR\_0000123053** The Web interface allows the password to be viewed.

## Version H.10.110

### Config

**CR\_0000116462** If an untagged port member of a port-based VLAN is changed to tagged member of the same VLAN, all inbound tagged traffic is dropped.

### RADIUS

**CR\_0000116468** When only one VLAN has an IP address configured, and it is not the primary VLAN, the RADIUS Request does not include the NSA-IP-ADDRESS attribute.

**CR\_0000117215** If the encryption keys are not configured the same for primary and secondary RADIUS servers on the switch, the RADIUS server may reject clients with wrong username-password.

## Version H.10.109

### Loop Protection

**CR\_0000110201** If you disable a port already disabled by loop-protect, it may still show as enabled after timer expiry.

### Multicast

**CR\_0000107597** The switch floods GMRP (GARP Multicast Registration Protocol) packets that are received on Spanning Tree backup and alternate ports, instead of dropping the packets.

**CR\_0000110677** GMRP Frames should flood to the VLAN just as multicast traffic does but are not flooding as expected.

### SNMP

**CR\_0000113034** "SNMPget" of object dot3adAggPortListPorts returns extraneous comma and space characters, which can affect scripts based on the "SNMPget" output.

## Version H.10.108

### 802.1X

**PR\_0000073291** Some devices are not set to the configured unauthorized VLAN when **authenticator client-limit** is set to a value of 1. Seen mainly on devices which are HP printers or when using JetDirect cards.

### CLI

**PR\_0000105415** The config may display incorrectly with regard to how it displays which ports are in a particular VLAN. For example: **untagged 3–Trk1** instead of **untagged 3–50,Trk1**.

### Crash

**PR\_0000073576** Switch can hang or reboot if transferring a config file > ~4300 bytes using SCP in SFTP mode. Smaller configuration files do not exhibit a problem.

### File Transfer

**PR\_0000073633** Error sometimes seen during SSH file transfer error while reading: received a short buffer from FXP\_READ, but not at EOF.

### Multiple Symptoms

**PR\_0000073630** Several Issues Resolved: 1) SFTP sessions do not close properly, 2) Error message Error while reading: received a short buffer from FXP\_READ, but not EOF, 3) Crash message Software Exception at xception.c:373 -- in 'tSsh0', -> Memory system error.

### SNMP

**PR\_0000107406** The following command, if run against ports 1–24, may result in a trap message reporting the wrong VLAN, if routing is enabled: **'port-security x learn-mode configured action send-alarm mac-address xx:xx:xx:xx:xx:xx'**. Running this command against ports 25–48 never exhibits the problem.

## Version H.10.107

### CLI

**PR\_0000103448** Enabling and Disabling loop-protect on a range of ports may result in ports 4 and higher to be disabled and left in an error state. For example **loop-protect 1–24** then **no loop-protect 1–24** may result in ports 4–24 to be disabled.

### IGMP

**PR\_0000105407** When an IGMPv2 host leaves a group, the switch may send a malformed GSG message.

### QoS

**PR\_0000105258** Switch may change the priority of routed packets. This PR\_0000105258 improves the QoS fix in PR\_0000070680 in H.10.103.

### SNMP

**PR\_0000105142** LLDP information from some devices causes an `snmpwalk` of the switch to truncate after the `lldpRemManAddrIfld` OID (iso.0.8802.1.1.2.1.4.2.1.4).

### Syslog

**PR\_0000065540** There is a long delay before the switch event log messages are sent to the syslog server.

## Version H.10.104

### Authentication

**PR\_0000070500** When the 802.1X authenticator times out waiting for a supplicant response, instead of transitioning to the connecting state and restarting the attempt to acquire a supplicant by transmitting Identity-Requests, it falls silent.

### Secure Copy

**PR\_0000072803** After disabling SCP (Secure Copy Protocol) and enabling TFTP, the switch's config file retains the **no tftp client** that was automatically added when SCP was enabled.

## Version H.10.103

### CLI

**PR\_0000071004** The output of the command `show port-access authenticator config` displays the direction as `both`, even if the direction was configured to be **in** or **out**.

### QoS

**PR\_0000070680** Switch may change the priority of routed packets.

## Version H.10.102

### MAC Authentication

**PR\_0000071595** MAC authentication on Cisco IP phones may fail.

### Web Management

**PR\_0000070015** A VLAN QoS priority that is set in the Web user interface is not saved to the switch startup-config. **Workaround:** Go to **Configuration** → **System Info** and click **Apply Changes** to manually save the configuration.

## Version H.10.101

### CLI

**PR\_0000041836** The switch asks users if they want to save the configuration even though no changes were made. Note that configuration changes made via SNMP will still trigger this behavior even after this fix.

### Crash

**PR\_0000067243** Switch may reboot unexpectedly with a message similar to the following:  
`Software exception with task mAcctCtrl?.`

## Version H.10.100

### SSL

**PR\_0000070330** After copying the CA certificate to the switch, this error message is received:  
`Error setting CA Signed Request Configuration – No certificate is installed.` This improves the original SSL fix (PR\_0000064686) in H.10.98.

## Version H.10.99

### 802.1X

**PR\_0000067682** When using 802.1X in client mode, the command `aaa port-access authenticator 1 client-limit 2` should allow two clients to authenticate on that port. After one client is removed and the timeout period has passed, the switch does not allow a new second client to authenticate.

## Version H.10.98

### FFI/Config

**PR\_0000039989**

**FFI** — If an FFI event is triggered, and then the link is brought down and back again, the same FFI event will be triggered again in about 20 seconds even if the trigger condition isn't met.

**Config** — This fix makes the downgrade of the port to auto-10/100 visible in the running configuration.

Note that this may trigger the switch to ask `Do you want to save current configuration? upon logout or switch reload.`

### SSL

**PR\_0000064686** After copying the CA certificate to the switch, this error message is received:  
`Error setting CA Signed Request Configuration – No certificate is installed.`

## Version H.10.97

### Authentication

**PR\_0000058441** User authentication fails if the user's RADIUS configuration includes a non-HP VSA before any HP VSAs. **Workaround:** Configure the user in RADIUS with at least one HP VSA before any non-HP VSAs.

### SSH

**PR\_0000062389** After connecting to the switch with operator privileges, a subsequent SSH connection will only receive operator privileges instead of manager privileges.

## Version H.10.96

### CLI

**PR\_0000058067** When the switch is configured with a default gateway, the output of `show ip route` gives incorrect values for Metric and Distance. However, communication with the default gateway works properly.

### Web Management

**PR\_0000060662** The Web user interface displays the word **Status** at top of screen even though there is no status information provided.

## Version H.10.95

### Management

**PR\_0000053533** The ProCurve Manager (PCM) **Test communication parameters** test might fail on the second attempt.

## Version H.10.94

### DHCP

**PR\_0000055868** DHCP can fail if uplinked to a non-DHCP Snooping device.

### Routing

**PR\_0000057394** Switch not routing properly until after ARP cache cleared.

### STP

**PR\_0000062186** In certain circumstances, the switch reports chronic STP Root changes.

## Version H.10.93

### LLDP-MED

**PR\_0000057609** LLDP-MED packets are sent from authenticated clients connected.

## Version H.10.92

### CLI

**PR\_0000041272** CLI output from the commands `show port-access web clients` or `show port-access web clients detailed` only displays the client information from the first port that is active (i.e. has authenticated or unauthenticated clients). All other ports will not show any clients, even if the port has several authenticated or unauthenticated clients.

**PR\_0000051188** If the switch uses DHCP to obtain an IP address, the output of `show ip` does not display the correct default gateway. This is a display issue only; the correct gateway address is used by the switch.

### DHCP Snooping

**PR\_0000046276** With DHCP snooping enabled, a MAC-Authentication client whose session times out cannot reauthenticate.

### Spanning Tree

**PR\_0000057003** The switch might experience Spanning Tree instability upon changing the system time via CLI, TimeP, or SNTP, if the time change occurs while the switch is receiving high volumes

of broadcast traffic (on the order of 1 Mbps) on its Spanning Tree root port. This issue might also affect switch management traffic, causing unresponsive SNMP, TELNET, and SSH sessions.

## Version H.10.91

### Console

**PR\_0000001136** Rarely, the switch console may hang after a software image transfer to the switch.  
**Workaround:** <Ctrl-C> will restore the command prompt.

### Crash

**PR\_0000050061** Switch may sometimes reboot unexpectedly during a topology change with an error similar to the following: Software exception at exception.c:373 -- in mRadius005', task ID = 0x2594760 -> Memory system error at 0x243fb68 - memPartFree.

### LLDP-MED

**PR\_0000050798** In some cases the LLDP-MED inventory for an attached IP phone is not properly received or stored by the switch.

### SNMP/Config

**PR\_0000039221** The switch can misinterpret the community name as if it were a trap level, in the snmp-server host command. This fix modifies the command with keywords **community** and **trap-level**. The new command syntax is as follows. snmp-server host <ip addr> [community <community string>] [trap-level <none | all | not-info | critical | debug>] [informs].

### STP

**PR\_0000037812** When using force-version RSTP, the switch sends the root bridge ID in Spanning Tree BPDUs instead of its own bridge ID.

### UDLD

**PR\_0000047414** When UDLD is enabled, communication with the switch might be inconsistent, affecting the switch response to ping, TELNET, 802.1X requests, SNMP requests, and SNTP packets.

## Version H.10.90

### GVRP

**PR\_0000046133** Switches do not use multiple GARP Information Propagation (GIP) contexts when the switch has been configured for MSTP operation; the same GIP context is used for all ports participating in GVRP. There should be multiple GIP contexts - one for each 'spanning-tree' (the IST and each of the MSTIs). This fix improves the GVRP fix in H.10.85 (PR\_0000040758).

### LLDP

**PR\_0000051224** In some cases LLDP packets are transmitted from a switch port before the client is authenticated.

### Stacking

**PR\_0000052110** When a commander accesses a member switch and the user issues the show tech all command, in some situations the session from commander to member can become unresponsive. **Workaround:** From the commander switch, **kill** the unresponsive session.

## Version H.10.89

### Authentication

**PR\_0000052226** When port authentication methods are in use on a switch, if all of the clients are disconnected, the switch may change the Class of Service (CoS) settings. This PR\_0000052226 improves the Authentication fix in H.10.85 software (PR\_0000044893).

**PR\_0000053003** After a client is authenticated by 802.1X, if the switch receives a subsequent successful Web or MAC Authentication for that same client, the switch overwrites the 802.1X client RADIUS attributes.

### Config

**PR\_0000037570** After using the CLI to assign a port in a VLAN number higher than 32, the configuration cannot be saved via the Menu interface.

### Unauthenticated VLAN

**PR\_0000045072** An unauthenticated VLAN cannot be configured for 802.1X authentication, when another authentication method is also in use on a port. This fix also adds the unauth-period parameter for MAC authentication.

## Version H.10.88

### SNMP/Config

**PR\_0000043775** The switch allows invalid configuration parameters to be set via SNMP.

### Switch Tables

**PR\_0000050024** The switch's VLAN MAC address is not removed when the VLAN is removed.

## Version H.10.87

### CDP

**PR\_0000051209** Switch is forwarding CDP packets to other ports even when CDP is globally enabled.

### CPU Utilization

**PR\_0000044632** Data transfer in one VLAN with DIPLD and IP Routing enabled elevates CPU to 99%.

### Crash

**PR\_0000049246** The command `aaa accounting commands stop-only radius - causes` switch to crash with Software exception 'mRadius005'.

## Version H.10.86

### 802.1X

**PR\_0000047025** After the switch reboots and before IP communication is initialized, the switch accepts authentication requests from 802.1X clients. Because the switch cannot communicate with the RADIUS server yet, it sends EAP-Failure notifications to the client, which causes client authentication to fail.

**PR\_0000048284** 802.1X showing in an open state and receiving packets, under certain conditions causes the port to be in a down state with no traffic being passed.

## Authentication

**PR\_0000045069** In some situations the switch authenticates an EAP 802.1X client but does not allow communication from the client.

## CDP

**PR\_0000047116** CDP packets are not dropped, even when the switch is configured with the command `no cdp run`.

## Config

**PR\_0000048466** J4900C does not boot (goes into fault mode during startup) if using config file saved from J4900B.

## DHCP Snooping

**PR\_0000040580** Configuration of trust status for DHCP snooping on ports participating in a dynamic trunk yields undesirable results when the ports of the trunk are removed. This configuration should not be allowed on dynamic trunks (e.g. **dhcp-snooping trust Dyn1**), and this fix enforces that limitation at the CLI with an error message.

## Management

**PR\_0000044146** Ping and telnet to the switch fail at exactly 1243 days of uptime.

## SSH

**PR\_0000014531** Rarely, after some period of time with normal SSH connectivity, the switch may become unresponsive to further SSH management.

## UDLD

**PR\_0000043071** UDLD transmits a burst of packets when any port on the switch goes down (one packet is sent for each port that goes down), falsely triggering a failure state.

## Version H.10.85

### Authentication

**PR\_0000038263** Some frames are allowed on the switch port despite the default `aaa parameter controlled-directions both`.

**PR\_0000044893** When port authentication methods are in use on a switch, if all of the clients are disconnected, the switch may change the Class of Service (CoS) settings.

### GVRP

**PR\_0000040758** Switches do not use multiple GARP Information Propagation (GIP) contexts when the switch has been configured for MSTP operation; the same GIP context is used for all ports participating in GVRP. There should be multiple GIP contexts - one for each 'spanning-tree' (the IST and each of the MSTIs).

### RADIUS Accounting

**PR\_0000042522** The 'class' attribute is not included in the accounting-request to the RADIUS server; RFC 2865 states that this should occur.

## UDLD

**PR\_0000009505** UDLD misconfiguration (where UDLD is enabled on one side and disabled on the other) could lead to a unicast packet storm which results in MSTP running with multiple roots.

## Version H.10.84

### 802.1X

**PR\_0000039909** 802.1X authentication appears to work, but the client cannot communicate on the network for approximately 30 seconds.

### Command Authorization

**PR\_0000043525** HP-Command-String authorization does not work as expected.

### DHCP Snooping

**PR\_0000044797** When a PXE protocol DHCP-offer packet is sent from a boot server through a trusted port, the switch drops the packet.

### Web Management

**PR\_0000043510** The Web GUI does not display the lightning bolt for ports that are delivering power via PoE. This only affects the J8762A 2600-8-PoE Switch.

## Upgrade information

### Upgrading restrictions and guidelines

H.10.117 uses BootROM H.08.02. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

## Contacting HP

For additional information or assistance, contact HP Networking Support:

[www.hp.com/networking/support](http://www.hp.com/networking/support)

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

## HP 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.

To find security bulletins:

1. Go to the HP Support Center website at [www.hp.com/go/hpsc](http://www.hp.com/go/hpsc).
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.

To initiate a subscription to receive future HP Security Bulletin alerts via email, sign up at:  
[www4.hp.com/signup\\_alerts](http://www4.hp.com/signup_alerts)

## Related information

### Documents

To find related documents, see the HP Support Center website:

[www.hp.com/support/manuals](http://www.hp.com/support/manuals)

- Enter your product name or number and click **Go**. If necessary, select your product from the resulting list.
- For a complete list of acronyms and their definitions, see *HP FlexNetwork Technology Acronyms*.

### Websites

- Official HP Home page: [www.hp.com](http://www.hp.com)
- HP Networking: [www.hp.com/go/networking](http://www.hp.com/go/networking)
- HP product manuals: [www.hp.com/support/manuals](http://www.hp.com/support/manuals)
- HP download drivers and software: [www.hp.com/networking/software](http://www.hp.com/networking/software)
- HP software depot: [www.software.hp.com](http://www.software.hp.com)
- HP education services: [www.hp.com/learn](http://www.hp.com/learn)

## Documentation feedback

HP 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@hp.com](mailto:docsfeedback@hp.com)). Include the document title and part number, version number, or the URL when submitting your feedback.