Hewlett Packard Enterprise

S.15.09.0029 Release Notes

Abstract

This document contains supplemental information for the S.15.09.0029 release.

Part Number: 5200-3850
Published: April 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

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

Contents

S.15.09.0029 Release Notes

Description

This release note covers software versions beginning with S.15.09.0003.

Product series supported by this software:

- HPE 2520 Switch Series

Important information

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

Products supported

This release applies to the following product models:

Product number	Description
J9137A	HPE 2520 8 PoE Switch
J9138A	HPE 2520 24 PoE 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

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 S.15.09.0029

No enhancements were included in version S.15.09.0029.

Version S.15.09.0003

CDPv2 Transmit Capability

CR_0000107011

When a Cisco VoIP phone boots up (or sometimes periodically), it queries the switch and advertises information about itself using CDPv2. The switch receives the VoIP VLAN Query TLV (type 0x0f) from the phone and then immediately sends the voice VLAN ID in a reply packet to the phone using the VLAN Reply TLV (type 0x0e). The phone then begins tagging all packets with the advertised voice VLAN ID.

MAC Limit Notify

PR_0000073085, CR_0000077875

The MAC Address Count feature provides a way to notify the switch management system when the number of MAC addresses learned on a switch port exceeds the permitted configurable number.

Reporting Config Changes

PR_0000069196, CR_0000074531

This feature provides the ability to track and report information about switch management processes on a per-user, per-session basis. Syslog or RADIUS will be used for logging the information.

Terminal Line Width and Length

CR_0000074537

For console/serial link and inbound telnet sessions, the switch output:

- Uses whatever width is set by the terminal program. If width is not specified, 80 characters is the default.
- Automatically wraps on word boundaries (such as spaces) for non-columnar output
- Automatically wraps on column boundaries for columnar output

Hewlett Packard Enterprise recommends that you do not set your terminal width (**terminal width <y>**) above 150 columns.

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 S.15.09.0029

Port Authentication

CR_0000229021

Symptom: 'Authentication and security' process reports 60-70% CPU utilization. "Debug security" logging shows a continually repeating loop of 802.1x authentications, followed by age-outs and deletions of the client-mac.

Scenario: When both MAC authentication (mac-auth) and 802.1x (authenticator) are configured on the same switch port and the same client MAC address first does a successful mac-auth authentication followed by a successful 802.1x authentication, the authentication process may enter in a continuous re-authentication process that also triggers high CPU utilization. The issue does not occur when the 802.1x/ authenticator logoff-period is different than the global mac-age-time.

Workaround: Configure a switch global mac-age-time which differs from the 802.1x logoff period for each port configured with both mac-auth and 802.1x authentication. Both values are 300 seconds by default.

Example:

```
mac-age-time <60-999960>
```

```
aaa port-access authenticator <PORT-LIST> logoff-period <1-999999999>
```

Version S.15.09.0028

File Transfer

CR_0000211619

Symptom: The switch is administratively rebooted/reloaded before finalizing writing OS image files to the flash file system.

Scenario: When OS image files are put into the switch via SCP/SFTP, the switch allows execution of the CLI command `boot system flash [primary|secondary]` before finalizing writing OS image files to the flash file system. This can lead to a corrupted OS image on the flash and the inability of the switch to boot from that OS. The switch will failback to the uncorrupted primary/secondary OS image, if available.

Workaround: Reboot/reload the switch after confirming the OS image files are completely written to the flash file system. Verify the switch event log system for a message similar to `Update: Primary Image updated` or `Update: Secondary Image updated.`

Online Help

CR_0000201063

Symptom: Web management help file is not accessible.

Scenario: The web management interface online help file URL changed to accommodate domain change for host files.

Spanning Tree

CR_0000202511

Symptom: Incorrect spanning tree hello time is reported as a MIB value.

Scenario: In a spanning tree topology, the switch reports the value of OID dot1dStpHelloTime on a root switch in seconds instead of centiseconds as reported in non-root switches.

Workaround: There is no impact on spanning tree functionality as this is merely a value conversion from seconds to centiseconds.

Version S.15.09.0027

TFTP

CR_0000180230

Symptom: TFTP transfer does not work with packet sizes other than 1416 bytes.

Workaround: Configure TFTP client to use a packet size of 1416 bytes.

Version S.15.09.0026

Config

CR_0000175001

When the value of any event's `eventtype` is set to a non-default value, after the switch is rebooted, the new value that has been set does not take effect. The issue lies with reading of the value from the file after reload.

Version S.15.09.0025

Crash

CR_0000158589

When GVRP is configured and active, entering the command `no gvrp` might cause the switch to reboot unexpectedly with a message similar to `Health Monitor: Restr Mem Access, HW Addr=0x7c7342ae IP=0x3cd640 Task='mGarpCtrl' Task ID=0x5dbf400sp:0x1dc2618 lr:0x3c4bd8 msr: 0x00009032 xer: 0x20000000 cr: 0x48000400.`

Version S.15.09.0024

Crash

CR_0000146306

The switch uses TCP connections internally for inter-process communication. In a situation where an internal loopback TCP socket pair receives stimulus after an extended period of idle time, the switch might reboot unexpectedly with a message similar to `NMI event SW:IP=0x00e20c1c MSR: 0x02029200 LR:0x00e077d0 cr: 0x44000400 sp:0x02b03c58 xer:0x00000000 Task='InetServer' Task ID=0xab31000.`

File Transfer

CR_0000148584

A configuration file with a blank community name in the **snmp-server host** entry cannot be downloaded to the switch. Although the switch does not allow the **snmp-server host** entry to be configured with a blank community name, earlier software bugs might cause this condition.

TFTP

CR_0000132721

Certain lines in the configuration file are sometimes incorrectly changed when imported via TFTP. For example, the configuration entry **snmp-server community public unrestricted** might have the unrestricted parameter removed when the configuration file is downloaded via TFTP.

Web Management

CR_0000151179

After clicking "Save" without making changes, the Web user interface incorrectly changes VLAN members to be untagged. This happens after selecting "VLAN Mgmt", clicking "Change", and then clicking "Save" without making any changes. Also, the VLAN port membership is not correctly displayed in the Web user interface, which is a display issue; the correct VLAN port membership can be seen with the command line interface (CLI).

Version S.15.09.0023

ARP

CR_0000145065

ARP packets sent to a broadcast destination address are forwarded twice by the switch.

Config

CR_0000138447

After a switch software update, SNMP community access privileges are incorrectly changed by the switch. The output of `show snmp-server` and the output of a `walkmib` command give different results, and neither output represents how the switch actually behaves for Manager or Operator access. This issue was introduced with CR_0000122623; if the access settings were configured on a switch without the CR_0000122623 fix, after updating to software with the CR_0000122623 fix the settings are changed.

Version S.15.09.0022

File Transfer

CR_0000113260

Attempts to upgrade software via PCM (ProCurve Manager) fail. Also, actions taken via the Web user interface might experience delayed responses or timeouts.

SSH

CR_0000114000

After rebooting the switch many times, the Operator public key might erroneously be removed from the config file.

CR_0000137266b

This removes the CR_0000137266 fix: After rebooting the switch many times, the Operator public key might erroneously be removed from the config file. Instead, this issue is fixed with CR_0000114000.

Version S.15.09.0021

Crash

CR_0000115372

The switch might reboot unexpectedly with a message similar to `NMI event SW:IP=0x00000000 MSR:0x00000000 LR:0x00000000 cr: 0x00000000 sp:0x00000000 xer:0x00000000 Task='InetServer' Task ID=0xaad3000.`

CR_0000135900

In some situations it is possible for the switch to reboot unexpectedly with a message similar to `Software exception at alloc_free.c:646 -- in 'eDrvPoll', task ID = 0xa9a7a80 -> buf already freed by 0x0A9A7D40, op=0x0006003E`.

SSH

CR_0000137266

After rebooting the switch many times, the Operator public key might erroneously be removed from the config file.

Stacking

CR_0000121075

When stacking is enabled, the switch is accessible via the Web even after disabling the Web server, and via TELNET even after disabling TELNET.

Transceivers

CR_0000140560

The port shows link, but no traffic passes through a J4858C Gigabit-SX transceiver when the port is configured for **1000-full** operation.

Version S.15.09.0020

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.

Event Log

CR_0000127436

After the switch uptime reaches 497 days, the timestamp entries in the event log become erratic with gaps of several hours or days. In some cases, the timestamps revert to previous months and years, even though SNTP updates with those wrong timestamps report the correct date and time.

IGMP

CR_0000132149

Although the RFC requires that the switch with the lowest IP address becomes querier, a switch that is acting as querier stops being querier when it receives a query from a switch with a higher IP address.

CR_0000135527

A non-querier switch that receives a Join from the querier fails to send further Joins to the querier, resulting in loss of multicast traffic.

MAC Authentication

CR_0000129991

MAC Authentication fails when the **peap-mschapv2** parameter is included in the `aaa authentication` CLI command.

SNMP

CR_0000129191

When an SNMP trap destination is set for "no destinations", the log reports an entry of `unknown var type` when the event happens. Also, when the SNMP trap destination is set for "trap receivers only", traps are not sent.

CR_0000134672

The entStateOper OID from the Entity State MIB gives an incorrect value of 1 (unknown) instead of 3 (enabled), for some switches.

Version S.15.09.0018

Management

CR_0000134091

Disabling write access to an SNMP community via the Web user interface might cause the switch to become unresponsive to command input. The switch must be rebooted to regain management access.

Passwords

CR_0000134675

The switch does not automatically create a default username of **manager** or **operator** when a password is configured for those levels of access.

Version S.15.09.0017

LLDP

CR_0000132891

When an IP phone is connected directly to the switch, the output of the command `show lldp info remote-device` gives an incorrect value for the phone's IP address.

Loop Protection

CR_0000127150

Loop protection fails to detect a loop on a port configured for 802.1X authentication, if 802.1X is not enabled globally.

Passwords

CR_0000130921

If the switch is configured with a username and password, changing the password causes the username to also change. The username is changed to the default **manager** or **operator**, depending on which password is changed.

Trunking

CR_0000132453

When the switch has a total of four ports configured as LACP trunks, some trunk members always have LACP status of **blocked**. For example, with a single 4-port trunk, three members are blocked. With two 2-port trunks, one trunk has one member blocked and the other trunk functions properly.

Version S.15.09.0015

Authentication

CR_0000114480

In some situations a client cannot be authenticated.

CLI

CR_0000130897

Existing trap receiver entries might be overwritten by later entries.

GVRP

CR_0000129917

When the switch receives its own GVRP frames, it learns from them instead of dropping the frames.

CR_0000130090

After rebooting the switch, the configuration **unknown-vlans disable** does not work on trunks.

Management

CR_0000132070

Tagged packets sent to the switch agent with total Ethernet frame length = 64 bytes are not processed by the switch.

Multicast

CR_0000130559

Multicast packets with destination addresses in the reserved ranges are sent twice from the switch. This affects IGMP and/or IPv6 packets.

Version S.15.09.0014

Crash

CR_0000122568

With SSL enabled, an attempt to download software via the Web interface might cause the switch to reboot unexpectedly with a message similar to: `NMI event SW:IP=0x006d1538 MSR:0x02029200 LR:0x006d19e4, cr: 0x28000800 sp:0x05197088 xer:0x20000000, Task=tHttpd Task ID=0xa955000.`

CR_0000127335

In some situations, issuing the `show tech all` command might cause the switch to reboot unexpectedly with a message similar to `Length Corruption`.

DHCP

CR_0000128754

If the switch is a DHCP client and the DHCP reply contains option 43 with sub-option codes that conflict with RFC 2132 options, the switch might use incorrect settings such as an incorrect subnet mask.

IGMP

CR_0000127628

In a topology where the host connects to a querier, the querier connects to a non-querier switch, the non-querier switch connects to a router, and the multicast source is beyond the router, the host might not receive the multicast stream. This happens because a **join** from the host that is received by the querier is not forwarded by the non-querier switch.

CR_0000127974

If a switch receives a PIM packet while it is in the querier election state, the switch gives up the querier role and does not forward multicast traffic.

Link

CR_0000127550

When two 2520-24 powered-on switches are connected via a 1 Gigabit copper link (using ports 25-28) and the ports are configured for Auto-MDIX, the link comes up, goes down, and stays down. If the switches are rebooted with the cable already connected, the problem does not occur.

Multicast

CR_0000125558

Multicast streams sometimes stop after a few minutes. Disabling IGMP restores the multicast stream. Other qualifiers: IP Multicast Route table may still “see” the stream, and VLAN ingress port may show the stream exists while the same VLAN egress port might not.

PIM

CR_0000128681

After a large number of multicast streams are added and old streams time out, the switch might get into a state where it is unable to add new multicast streams, responding with a message similar to `IpAddrMgr: Failed to allocate new SW IP multicast group, table full FIB entry.`

Version S.15.09.0013

Crash

CR_0000126799

Under unusual stress conditions, the switch might reboot unexpectedly with a message similar to `Software exception at fileTransfer.c:1144 -- in 'tHttpd', task ID = 0xa9389c0 -> Could not open file.`

CR_0000127541

While providing output for some `show` commands, the switch experiences a gradual loss of free memory. When memory is depleted, the switch might reboot unexpectedly with a message similar to `Software exception at svc_misc.c:831 -- in 'mSess3', task ID = 0x5d9ff40 -> Failed to malloc 16472 bytes.`

Include Credentials

CR_0000127700

With include credentials enabled, a config file that is saved to a TFTP server does not contain the SNMPv3 credentials.

Management

CR_0000127197

The 2520-8-PoE Switch (J9137A) might become inaccessible to in-band management until the switch is rebooted. Note that the switch's console port is unaffected and works properly during the problem time. This improves the original Management fix (CR_0000115882) in S.15.09.0012.

Web Management

CR_0000125239

After logging into the switch Web user interface, closing the tab on some Web browsers does not log the user out of the Web session.

Version S.15.09.0012

Authentication

CR_0000124607

Disconnecting an authenticated PC from an authenticated VoIP phone might cause the phone to lose its authentication. The phone must be disconnected from and then reconnected to the switch to recover.

Management

CR_0000115882

The 2520-8-PoE Switch (J9137A) might become inaccessible to in-band management until the switch is rebooted. Note that the switch's console port is unaffected and works properly during the problem time.

SNMP

CR_0000122623

After rebooting a switch configured for SNMP with the parameters **operator unrestricted**, the switch does not allow the user to set any read/write MIB objects.

Version S.15.09.0011

802.1X

CR_0000122837

Clients have issues with authentication when 802.1X and MAC Authentication are both configured on a port.

IGMP

CR_0000105902

IGMPv2 LEAVE processing functionality no longer works for a multicast group after receipt of IGMPv1 group specific membership query (GSMQ) packet when operating in IGMPv2 mode, even when **ip igmp forcedfastleave 1-24** is enabled.

SSH

CR_0000122795

SSH session disconnects when the SSH key re-exchange takes place.

Version S.15.09.0010

CPU

CR_0000123333

After the switch has been booted or upgraded to an S.15.xx version, the device may become unresponsive due to high CPU utilization.

Display Issue

CR_0000121028

Some MAC addresses are displayed incorrectly in the output of CLI commands `show lldp info remote-device` and `display lldp neighbor-information list`.

Multicast

CR_0000110677

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

Spanning Tree

CR_0000110052

In a topology with multiple MSTP regions and multiple same-cost links connecting the regions, the CST root port might change to a CST alternate port, and MSTP instances might be blocked on region boundary ports.

System

CR_0000123647

At times, the switch is unable to process packets that require CPU processing, taking from a few seconds up to minutes to complete the process. Symptoms include recurring BDPU starvation, and `Out of pkt buffers; miss count: 0` error messages.

Version S.15.09.0007

Authentication

CR_0000109782

In some situations the switch stops sending RADIUS requests and client authentication fails.

SNMP

CR_0000119914

Adds the ability to configure port security via SNMP. This was not available in earlier S.15.09 software versions.

TFTP

CR_0000119184

The switch experiences a loss of free memory each time command output is copied to a TFTP server. When memory is no longer available, the TFTP will fail with a message similar to the following.

```
TFTP download in progress.
Failed to allocate a new TFTP client.
00000K Request failed.
```

Version S.15.09.0005

Crash Messaging

CR_0000114843

The output of an `NMI event` crash wrongly shows pointer values to be all zeros.

Display Issue

CR_0000118422

A MAC address that begins with a non-zero value is displayed incorrectly in CLI and Web interface output.

MSTP

CR_0000117421

A trunk has the default MSTP port priority = 4. If the trunk is configured with a port priority = 8 (which is the default for non-trunk gigabit ports), after saving the configuration and rebooting the switch, that port priority is wrongly changed to 4.

CR_0000117473

With MSTP enabled and multiple instances configured, LACP is incorrectly blocked on ports connected to MSTP-blocked ports.

Port Security

CR_0000114545

With port security enabled, the first packet received on the port is not forwarded by the switch. This can cause DHCP failures for clients that send only one DHCP Discover packet.

Version S.15.09.0004

Authentication

CR_0000114832

On a port configured for authentication with a **logoff-period** longer than the MAC age time, authenticated clients that send no traffic might be de-authenticated at the MAC age time instead of the configured **logoff-period**.

CLI

CR_0000115515

The switch does not allow configuration changes via the CLI, responding with the error message `inconsistent value`. This has been observed when the configuration includes **snmpv3 targetaddress TARGETADDRESS** with a **TARGETADDRESS** string longer than 24 characters.

Config

CR_0000117518

A switch configured with a username and password and with **include-credentials** cannot be accessed after updating software, because the username is wrongly removed from the config file during the software update.

Crash

CR_0000115929

With very large key sizes, the command `show crypto host-cert` might cause the switch to reboot unexpectedly with a message similar to the following.

```
Invalid Instr HW Addr=0x00000000 IP=0x0 Task='mSess2' Task ID=0xa97ad40 sp:
0x4acecc8 lr: 0x57e468 msr: 0x02029200 xer: 0x20000000 cr: 0x28000400
```

CR_0000116647

It is possible for the switch to reboot unexpectedly with a message similar to the following.

```
Software exception in kernel context at ghsException.c:1101 -> Internal
system error
```

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.

SSL

CR_0000115933

Under certain conditions, the **VLAN** > **VLAN Mgmt** page on the switch cannot be accessed via an SSL connection to the web user interface.

Web Management

CR_0000108339

The switch's web user interface cannot be accessed via the fully-qualified domain name in some situations.

Workaround: Use the IP address to access the switch's web user interface.

Upgrade information

Upgrading restrictions and guidelines

S.15.09.0029 uses BootROM S.14.03. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

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**.
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** to initiate a subscription to receive future Hewlett Packard Enterprise Security Bulletin alerts via email.

Websites

Networking Websites

Hewlett Packard Enterprise Networking Information Library

www.hpe.com/networking/resourcefinder

Hewlett Packard Enterprise Networking Software

www.hpe.com/networking/software

Hewlett Packard Enterprise Networking website

www.hpe.com/info/networking

Hewlett Packard Enterprise My Networking website

www.hpe.com/networking/support

Hewlett Packard Enterprise My Networking Portal

www.hpe.com/networking/mynetworking

Hewlett Packard Enterprise Networking Warranty

www.hpe.com/networking/warranty

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

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

  Hewlett Packard Enterprise Support Center: Software downloads

  www.hpe.com/support/downloads

  Software Depot

  www.hpe.com/support/softwaredepot
- To subscribe to eNewsletters and alerts:

  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

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

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

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

Additional warranty information

HPE ProLiant and x86 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

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

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

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

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

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**). 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.