Abstract
This document contains supplemental information for the W.15.14.0015 release.
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.


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.

Description .......................................................................................................................... 6
Important information ......................................................................................................... 6
Version history ..................................................................................................................... 6
Products supported ............................................................................................................. 8
Compatibility/interoperability ............................................................................................ 8
Minimum supported software versions .............................................................................. 8
Enhancements ..................................................................................................................... 9
  Version W.15.14.0015 ........................................................................................................ 9
  Version W.15.14.0013 ........................................................................................................ 9
  Version W.15.14.0012 ........................................................................................................ 9
  Version W.15.14.0009 ........................................................................................................ 9
  Version W.15.14.0008 ........................................................................................................ 9
  Version W.15.14.0007 ........................................................................................................ 9
  Additional Debug Capability ............................................................................................ 9
  Version W.15.14.0006 ........................................................................................................ 9
  Version W.15.14.0005 ........................................................................................................ 10
      Hostname ...................................................................................................................... 10
  Version W.15.14.0004 ........................................................................................................ 10
  Version W.15.14.0003 ........................................................................................................ 10
  Version W.15.14.0002 ........................................................................................................ 10
      Certificate Manager ..................................................................................................... 10
      Chassis Locate LED ...................................................................................................... 10
      DHCPv4 Snooping ......................................................................................................... 10
      Filtering PVID Messages .............................................................................................. 10
      Local MAC Authentication ........................................................................................... 10
      SNMP Trap ................................................................................................................... 11
Fixes .................................................................................................................................... 11
  Version W.15.14.0015 ........................................................................................................ 11
      IP Stacking .................................................................................................................... 11
      LLDP ............................................................................................................................. 11
      Online Help ................................................................................................................... 12
      Spanning Tree ............................................................................................................... 12
      Web UI .......................................................................................................................... 12
  Version W.15.14.0013 ........................................................................................................ 12
      Config ............................................................................................................................ 12
      Crash ............................................................................................................................. 12
      PoE ................................................................................................................................. 12
      Routing .......................................................................................................................... 13
      SFTP ............................................................................................................................... 13
  Version W.15.14.0012 ........................................................................................................ 13
      802.1X ........................................................................................................................... 13
      Certificate Manager ..................................................................................................... 13
      CLI ................................................................................................................................. 13
      Crash ............................................................................................................................. 14
      Routing .......................................................................................................................... 14
<table>
<thead>
<tr>
<th>Version W.15.14.0011</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Manager</td>
<td>14</td>
</tr>
<tr>
<td>CLI</td>
<td>14</td>
</tr>
<tr>
<td>Crash</td>
<td>15</td>
</tr>
<tr>
<td>SSH</td>
<td>15</td>
</tr>
<tr>
<td>TFTP</td>
<td>15</td>
</tr>
<tr>
<td>Stacking</td>
<td>14</td>
</tr>
<tr>
<td>SSL</td>
<td>14</td>
</tr>
<tr>
<td>SSH</td>
<td>14</td>
</tr>
<tr>
<td>Certificate Manager</td>
<td>14</td>
</tr>
<tr>
<td>CLI</td>
<td>14</td>
</tr>
<tr>
<td>Crash</td>
<td>15</td>
</tr>
<tr>
<td>SSH</td>
<td>15</td>
</tr>
<tr>
<td>TFTP</td>
<td>15</td>
</tr>
<tr>
<td>Stacking</td>
<td>14</td>
</tr>
<tr>
<td>Multicast</td>
<td>24</td>
</tr>
<tr>
<td>MSTP</td>
<td>24</td>
</tr>
<tr>
<td>IP Phones</td>
<td>23</td>
</tr>
<tr>
<td>Flow Control</td>
<td>23</td>
</tr>
<tr>
<td>Fastboot</td>
<td>23</td>
</tr>
<tr>
<td>Display Issue</td>
<td>23</td>
</tr>
<tr>
<td>Crash</td>
<td>16</td>
</tr>
<tr>
<td>Counters</td>
<td>22</td>
</tr>
</tbody>
</table>

- **Version W.15.14.0010**
  - ARP...........................................16
  - CLI..........................................16
  - Config.................................16
  - Crash...................................16
  - ICMP.....................................17
  - IP Phones..............................17
  - Memory....................................18
  - Redundant Memory...................18
  - Smart Link.............................18
  - Stacking..............................18
  - Switch Hang..........................18
  - TACACS......18

- **Version W.15.14.0009**
  - 802.1X........................................18
  - CLI..........................................19
  - PoE.........................................19
  - Switch Hang............................19

- **Version W.15.14.0008**
  - Crash.....................................19

- **Version W.15.14.0007**
  - Authentication......................19
  - BPDU Protection....................19
  - CLI..........................................20
  - IPv6......................................20
  - Logging..................................20
  - Management..........................20
  - PoE.........................................21
  - sFlow......................................21
  - SNMP.......................................21
  - Switch Hang..........................21
  - TELNET..................................21

- **Version W.15.14.0006**
  - CLI..........................................22
  - Counters..............................22
  - Crash....................................22
  - Display Issue.......................23
  - Fastboot..............................23
  - Flow Control.......................23
  - IGMP......................................23
  - IP Phones............................23
  - MAC Table............................23
  - MSTP......................................24
  - Multicast................................24
  - Stacking..............................24
  - Transceivers.......................24

- **Version W.15.14.0005**
  - CLI..........................................24
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS</td>
<td>24</td>
</tr>
<tr>
<td>Version W.15.14.0004</td>
<td>24</td>
</tr>
<tr>
<td>Version W.15.14.0002</td>
<td>25</td>
</tr>
<tr>
<td>802.1X</td>
<td>25</td>
</tr>
<tr>
<td>Accounting</td>
<td>25</td>
</tr>
<tr>
<td>Authentication</td>
<td>25</td>
</tr>
<tr>
<td>CLI</td>
<td>25</td>
</tr>
<tr>
<td>Config</td>
<td>25</td>
</tr>
<tr>
<td>Crash</td>
<td>26</td>
</tr>
<tr>
<td>DHCP</td>
<td>26</td>
</tr>
<tr>
<td>Event Log</td>
<td>27</td>
</tr>
<tr>
<td>GVRP</td>
<td>27</td>
</tr>
<tr>
<td>ICMP</td>
<td>27</td>
</tr>
<tr>
<td>IGMP</td>
<td>27</td>
</tr>
<tr>
<td>Jumbo Frames</td>
<td>27</td>
</tr>
<tr>
<td>Link</td>
<td>27</td>
</tr>
<tr>
<td>Loop Protection</td>
<td>28</td>
</tr>
<tr>
<td>MAC Authentication</td>
<td>28</td>
</tr>
<tr>
<td>OpenFlow</td>
<td>28</td>
</tr>
<tr>
<td>Passwords</td>
<td>28</td>
</tr>
<tr>
<td>RADIUS Accounting</td>
<td>28</td>
</tr>
<tr>
<td>Routing</td>
<td>28</td>
</tr>
<tr>
<td>sFlow</td>
<td>28</td>
</tr>
<tr>
<td>SNMP</td>
<td>29</td>
</tr>
<tr>
<td>SSH</td>
<td>29</td>
</tr>
<tr>
<td>SSL</td>
<td>29</td>
</tr>
<tr>
<td>Stacking</td>
<td>29</td>
</tr>
<tr>
<td>TFTP</td>
<td>29</td>
</tr>
<tr>
<td>Transceivers</td>
<td>29</td>
</tr>
<tr>
<td>Trunking</td>
<td>30</td>
</tr>
<tr>
<td>Web Management</td>
<td>30</td>
</tr>
<tr>
<td>Upgrade information</td>
<td>30</td>
</tr>
</tbody>
</table>

**Hewlett Packard Enterprise security policy** ........................................ 31

Finding Security Bulletins................................................................. 31

Security Bulletin subscription service.................................................. 31

**Websites** .......................................................................................... 32

**Support and other resources** ............................................................ 33

Accessing Hewlett Packard Enterprise Support........................................ 33
Accessing updates.................................................................................. 33
Customer self repair............................................................................. 33
Remote support...................................................................................... 34
Warranty information............................................................................ 34
Regulatory information......................................................................... 34
Documentation feedback........................................................................ 35

Description

This release note covers software versions for the W.15.14 branch of the software.


Product series supported by this software:
- HPE 2910al 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.

<table>
<thead>
<tr>
<th>Version number</th>
<th>Release date</th>
<th>Based on</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>W.15.14.0004</td>
<td>n/a</td>
<td></td>
<td>Never built.</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Version number</th>
<th>Release date</th>
<th>Based on</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>W.15.14.0003</td>
<td>n/a</td>
<td></td>
<td>Never built.</td>
</tr>
<tr>
<td>W.15.13.0010</td>
<td>n/a</td>
<td>W.15.13.0009</td>
<td>Never released.</td>
</tr>
<tr>
<td>W.15.13.0009</td>
<td>n/a</td>
<td>W.15.13.0008</td>
<td>Never released.</td>
</tr>
<tr>
<td>W.15.13.0007</td>
<td>n/a</td>
<td></td>
<td>Never built.</td>
</tr>
<tr>
<td>W.15.12.0013</td>
<td>n/a</td>
<td></td>
<td>Never built.</td>
</tr>
<tr>
<td>W.15.12.0009</td>
<td>n/a</td>
<td></td>
<td>Never built.</td>
</tr>
<tr>
<td>Version number</td>
<td>Release date</td>
<td>Based on</td>
<td>Remarks</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>W.15.12.0007</td>
<td>2013-03-26</td>
<td>W.15.12.0006</td>
<td>Released, fully supported, but not posted on the web.</td>
</tr>
<tr>
<td>W.15.12.0006</td>
<td>2013-02-28</td>
<td>First release</td>
<td>Initial release of W.15.12, fully supported, but not posted on the web.</td>
</tr>
</tbody>
</table>

**Products supported**

This release applies to the following product models:

<table>
<thead>
<tr>
<th>Product number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>J9145A</td>
<td>HPE 2910al 24G Switch</td>
</tr>
<tr>
<td>J9147A</td>
<td>HPE 2910al 48G Switch</td>
</tr>
<tr>
<td>J9146A</td>
<td>HPE 2910al 24G PoE+ Switch</td>
</tr>
<tr>
<td>J9148A</td>
<td>HPE 2910al 48G PoE+ Switch</td>
</tr>
</tbody>
</table>

**Compatibility/interoperability**

The switch web agent supports the following web browsers:

<table>
<thead>
<tr>
<th>Browser</th>
<th>Supported versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer</td>
<td>• Edge &lt;br&gt;• 11</td>
</tr>
<tr>
<td>Chrome</td>
<td>• 53 &lt;br&gt;• 52</td>
</tr>
<tr>
<td>Firefox</td>
<td>• 49 &lt;br&gt;• 48</td>
</tr>
<tr>
<td>Safari (MacOS only)</td>
<td>• 10 &lt;br&gt;• 9</td>
</tr>
</tbody>
</table>

**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.

Table sorted by minimum supported software version (reverse chronological order)

<table>
<thead>
<tr>
<th>Product number</th>
<th>Product name</th>
<th>Minimum software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>J9805A</td>
<td>HPE 640 Redundant/External PS Shelf</td>
<td>WB.15.13.0003</td>
</tr>
</tbody>
</table>
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 W.15.14.0015
No enhancements were included in version W.15.14.0015.

Version W.15.14.0014
No enhancements were included in version W.15.14.0014.

Version W.15.14.0013
No enhancements were included in version W.15.14.0013.

Version W.15.14.0012
No enhancements were included in version W.15.14.0012.

Version W.15.14.0011
No enhancements were included in version W.15.14.0011.

Version W.15.14.0010
No enhancements were included in version W.15.14.0010.

Version W.15.14.0009
No enhancements were included in version W.15.14.0009.

Version W.15.14.0008
No enhancements were included in version W.15.14.0008.

Version W.15.14.0007
Additional Debug Capability

CR_0000132845
This enhancement adds tracking to identify possible switch hang situations during switch boot.

Version W.15.14.0006
No enhancements were included in version W.15.14.0006.
Version W.15.14.0005

Hostname

CR_0000141040

Hostname in Syslog Messages. The switch can be configured to include its hostname as the source or "origin" for messages sent to a syslog server. For more information, see "Troubleshooting" in the Management and Configuration Guide for your switch.

Version W.15.14.0004

Version W.15.14.0004 was never built.

Version W.15.14.0003

Version W.15.14.0003 was never built.

Version W.15.14.0002

Certificate Manager

CR_0000115812


Chassis Locate LED

CR_0000134999

Chassis Locate LED at Boot. The chassislocate command has an optional parameter that configures it to run in the future instead of immediately. See "Troubleshooting" in the HP Switch Software Management and Configuration Guide for your switch.

DHCPv4 Snooping

CR_0000129524

DHCPv4 Snooping Max Binding. DHCP snooping max-binding prevents binding entries from getting exhausted. This feature is on a per-port basis and restricts the maximum number of bindings allowed on a port/interface. The maximum bindings for a particular port includes both statically configured and dynamically learned. The number of bindings on a per port basis is incremented upon a lease offer and decremented upon a lease expiry or release. See "Port Security" in the HP Switch Software Access Security Guide for your switch.

Filtering PVID Messages

CR_0000127014

Filtering PVID Mismatch Log Messages. This enhancement filters out PVID mismatch log messages on a per-port basis. PVID mismatches are logged when there is a difference in the PVID advertised by a neighboring switch and the PVID of the switch port which receives the LLDP advertisement. However, if these events are logged too frequently, they can overwhelm the log buffer and push relevant logging data out of log memory, making it difficult to troubleshoot another issue. See "Troubleshooting" in the HP Switch Software Management and Configuration Guide for your switch.
Local MAC Authentication

**CR_0000128955**

Local MAC Authentication (LMA). LMA is a software feature that simplifies deployment for devices such as IP phones and security cameras. In general, it provides dynamic attribute assignment (e.g., VLAN and QoS) through the use of a locally configured authentication repository. The most common use model for LMA is to automatically assign a VLAN to IP phones. In some cases, it can also provide rudimentary access security for the network. See "Web and MAC Authentication" in the *HP Switch Software Access Security Guide* for your switch.

SNMP Trap

**CR_0000135708**

SNMP Trap When MAC Address Table Changes. This enhancement causes an SNMP trap to be generated once a laptop/PC is removed from the back of an IP phone and the laptop/PC MAC address ages out of the MAC table. See "Configuring for Network Management Applications" in the *HP Switch Software Management and Configuration Guide* for your switch.

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 W.15.14.0015

**IP Stacking**

**CR_0000225769**

**Symptom:** IP communication between members of an IP stack may fail.

**Scenario:** When 2 or more switches are configured with IP stacking and the IP address configuration on the Primary VLAN is disabled (no ip address) on a stack member switch, the IP communication between commander switch and a stack member, such as ping <switch-number> or telnet <switch-number>, fails after the stack member reboot.

**Workaround:** Do not disable the IP address (no ip address) on the stack member switch.

**LLDP**

**CR_0000227582**

**Symptom:** Chassis ID field is not displayed in the output of CLI command show lldp info <local-device | remote device>.

**Scenario:** The switch does not display the local Chassis ID information in the output of the CLI command show lldp info local-device. The Chassis ID for remote devices is empty in the output of CLI command show lldp info remote device.
**Version W.15.14.0014**

**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.

**Web UI**

CR_0000210499

**Symptom:** Switch may crash during authentication to access Web UI management interface.

**Scenario:** When using a Windows Network Policy Server as RADIUS server for the switch authentication mechanism to control web access to the switch management, the switch may crash with an error message similar to `Health Monitor: Read Error Restr Mem Access <...> Task='tHttpd' <...>`.

**Version W.15.14.0013**

**Config**

CR_0000170324

When a change is made from the CLI in the 'Switch Configuration – Port/Trunk Settings' Menu, the change is not saved, resulting in an `Unable to save field` error.

**Crash**

CR_0000168083

The switch may reboot unexpectedly at the point when an IGMP static group is created in the configuration if an IGMP join occurs to the same group address.

**PoE**

CR_0000172947

**Symptom:** The switch crashes when the CLI commands `show tech` or `show tech all` are executed.

**Scenario:** When there is a faulty module, running the CLI commands `show tech` or `show tech all` might cause the switch to crash with an error message similar to `Software exception at samba_chassis_slot_sm <...> Co-Processor Crash detected <...>`.
Workaround: Replace the faulty PoE module or do not run the CLI commands `show tech` or `show tech all` when the switch indicates a PoE module failure on the front panel LED status.

Routing

CR_0000162176
Under stress conditions, the switch sometimes enters a state where it does not send an ARP to a particular destination and it becomes unreachable on the customer network.

Workaround: Initiate a ping from the switch to the unreachable destination to restore connectivity to that destination through this switch.

SFTP

CR_0000162987
Management modules go out of synchronization and fail to recover when large SFTP copies or a large number of SFTP copies are performed.

Version W.15.14.0012

802.1X

CR_0000164489
802.1x re-authentication period works if the client connects after the switch is booted. If, however, the switch reboots while clients are connected, it authenticates initially, but no re-authentication occurs.

Certificate Manager

CR_0000164093
When an IDEVID certificate is being used to establish TLS connections with a CNM server, the existing signature algorithm has been updated from SHA-1 to DER, with new root certificate for the RA server.

CLI

CR_0000163218
The output of the CLI command `show interface ethernet <interface>` becomes misaligned when the value of `Total Rx (bps)` reaches 100,000,000. When the 9th digit is added to the value of `Total Rx`, the adjacent line in the output (`Total Tx (bps)`) is shifted one column farther.

CR_0000163219
After issuing the CLI command `clear statistics global`, two problems might appear in the output of `show interface ethernet <port ID>`:

1. The values of `Bytes Rx` and `Bytes Tx` are no longer displayed as comma-separated values. This applies to counter values from 2,147,483,647 through 4,294,967,295. Other counters than the number of bytes sent and received also appear to be affected by the same display issue (for example, Unicast counters and Deferred Tx).

2. After entering `clear stat global`, the format of the output of `show interface ethernet <port>` shifts two places. The missing space might appear at Giant Rx – Late Collisions, but where the space is added seems can differ.
Crash

**CR_0000154769**

The switch may reboot unexpectedly when the management interface is accessed via SSH and the `show tech all` CLI command is executed, or when the SSH session is idle following execution of the CLI command `show run` a few minutes earlier.

Routing

**CR_0000162833**

The IP RIP Route Change counter might increment every 30 seconds, even though there is no actual change taking place.

**CR_0000164381**

When multiple ECMP routes are used with BGP, MSTP, and VRRP issues resulted due to message queues becoming full.

SSH

**CR_0000165393**

When the SSH client has a keepalive mechanism configured that requires a response from the SSH server on the switch, the SSH client will terminate the session after the first keepalive packet is transmitted. This happens because the switch drops the client's keepalive packet due to an incorrect packet length calculation.

This issue has been observed using an openSSH client with the `ServerAliveInterval` configured and the parameter 'want_reply' enabled.

SSL

**CR_0000162587**

SSL Security vulnerability due to 56 bit DES-CBC-SHA. Due to security vulnerability the cipher DES-CBC-SHA is now unavailable.

Stacking

**CR_0000164406**

If IP stacking is configured, and a user connects via browser to the stack commander via its (http) web management address and selects the drop down box to connect to a stack member, the user is not connected to the stack member and is returned back to the stack commander view instead.

Version W.15.14.0011

Certificate Manager

**CR_0000159204**

When a self-signed certificate is generated in the CLI, the certificate does not contain a valid start and end-date. This causes the certificate to be invalid, which causes problems establishing HTTPS sessions or using syslog over TLS. When the self-signed certificate is generated in the web interface, this problem does not occur.
When a user enables Spanning Tree in the CLI and configured a protocol version other than the default MSTP, the CLI Menu does not allow the user to modify Spanning Tree parameters. The menu indicates that the switch requires a reboot. When the switch is actually rebooted, the same problem is present after the reboot.

After a user changes the Spanning Tree Protocol Version to RPVST in the CLI Menu, the switch prompts the user to save the configuration and reboot the system to activate the changes. However, after saving and rebooting, those messages continue to be displayed.

When an exceptionally large amount of IP Address Manager (IPAM) output is generated by the `show tech all` command and captured using the `copy command-output` CLI command, the system might crash with the following message: NMI event SW:IP=0x00147168 MSR:0x02029200 LR: 0x00120f7c cr: 0x44000400 sp:0x04d60f30 xer:0x00000000 Task='mSess3' Task ID=0x4d59728.

The switch might reboot unexpectedly with a Software Exception message similar to: `Software exception at stackingFile.c:2224 -- in 'mStackDatWriter', task ID = 0x3c953b00 -> Internal Error ID: 6382d706)` when a lot of TFTP file transfers to an external TFTP server occur.

When the switch continuously attempts to transfer a file to a destination that returns an error; for example, because it ran out of space to store the file, the switch might eventually crash with the message: `Software exception at hwBp.c:218 -- in 'fault_handler', task ID = 0x3c403380 -> MemWatch Trigger: Offending task 'mftTask'.`

When a user copies a large file from the switch to a server using the SFTP client on the switch, the file transfer might be prematurely interrupted because the session disconnects before the file transfer has been completed. When this occurs, the following message is recorded in the system's Event Log: `03311 sftp: AM1: User: SFTP connection failure while connecting from <ip address>`.

When the switch is used as a TFTP server and configuration files are transferred from the switch to an external TFTP client, the software creates a temporary file in memory that is removed after the transfer has completed. However, the temporary file is not deleted when an error occurs during the file transfer. When repeated file transfers of configuration files fail, the temporary files accumulate and might deplete the available memory space. Once depleted, further file transfers fail and the switch might reboot.
unexpectedly (crash). Note that when the switch is rebooted, all temporary files are removed from memory.

Version W.15.14.0010

**ARP**

**CR_0000152907**

Changing the `ip arp-age` value should apply to existing ARP cache entries, but it does not.

**CLI**

**CR_0000145136**

When the switch is configured with the `console event critical` setting, the event log output of `show tech all` lists only the critical events. With this fix, `show tech all` lists all event log entries.

**CR_0000152440**

The output of `show tech all` halts while displaying `ImaDbUtil traverseLmaProfTbl`, with the message `=== The command has completed with errors. ===`.

**CR_0000155063**

The output of `show run` lists modules that are not installed in the switch. The nonexistent modules are also in the config file. This fix improves the original CLI fix (CR_0000147898).

**Config**

**CR_0000145221**

The switch prompts users to save the configuration when no changes have been made. This has been observed after configuring meshing, saving the config, and rebooting the switch.

**CR_0000152418**

Routing must be enabled before the Local Proxy-ARP feature can be configured, but when routing is removed from the configuration, the Local Proxy-ARP configuration is not removed.

**Crash**

**CR_0000151102**

In a rare situation, after a failover to the Standby Management Module (SMM) or the stack's Standby switch, the switch might reboot unexpectedly with a message similar to `Software exception at asicMgrSlaveFilters.c:185 -- in 'mNSA', task ID = 0x1blfeaa80 -> Internal Name Server Error`.

**CR_0000152930**

After deleting the last of any configured Smart Link groups, the switch might reboot unexpectedly.

**CR_0000153035**

With MAC-based authentication and mixed-mode enabled on a port that has both authenticated and unauthenticated clients, a redundancy failover might cause the switch to reboot unexpectedly with a message similar to `Software exception at bttfHwSrcBasedVlan.c:263 -- in 'mAdMUpCtrl', task ID = 0x1fecc6c0 -> ASSERT: failed.`
When a large number of 802.1X clients are being authenticated, reconfiguring port security modes such as learn-mode might cause the switch to reboot unexpectedly with a message similar to Software exception at multMgmtUtil.c:88 -- in 'mPpmgrCtrl', task ID = 0x13b1f940 -> Internal error.

The switch experiences a loss of free memory for failed PEAP-MSCHAPv2 MAC-based authentication requests. When memory is no longer available, the switch reboots unexpectedly with a message similar to Software exception at wma_peap.c:713 -- in 'mWebAuth', task ID = 0x1de85340 -> ASSERT: failed.

Enabling the arp-protect command on 4094 VLANs causes CPU utilization to increase to 100%.

Disabling and re-enabling a port configured for Web or MAC-authentication during client authentication might cause the switch to reboot unexpectedly with a message similar to Health Monitor: Restr Mem Access HW Addr=0xb1ba0c1a IP=0x108682b8 Task='mWebAuth' Task ID=0x1de8c680 sp:0x12f98530 lr:0x10868664 msr: 0x0000b032 xer: 0x00000000 cr: 0x88000400.

When a CLI command is entered with a backslash as the last character and then the repeat command is issued, the switch might reboot unexpectedly with a message similar to Task mSess1 encountered an exception.

Sending an ICMPv6 echo request packet with multiple fragment headers to the switch causes an NMI crash.

When using MAC Authentication on 2620, the following software exception may occur: wma_client_sm.c:1646 -- in 'mWebAuth', task ID = 0x1de85380.

The switch sends a ping request to a random IP address every 20 minutes.

If an IP phone sends the switch an invalid power value of zero watts in an LLDP-MED TLV, the switch log shows PD Over Current indication and the phone might continuously reboot. This has been observed with the Avaya 9641G IP phone.
Memory

CR_0000152126

Issuing the terminal length or terminal width command causes a small loss of free memory.

Redundant Memory

CR_0000156759

After redundancy switchover with boot command when modules have not finished booting an internal buffer may become corrupted. This could possibly lead to a crash.

Smart Link

CR_0000152346

Upstream switches do not flush the MAC and ARP entries after a Smart Link switchover.

CR_0000152422

After deleting the active Master port from a Smart Link group, the Slave port takes over but does not send flush packets.

CR_0000152432

When Spanning Tree is enabled after Smart Link is configured, the Smart Link ports incorrectly take part in Spanning Tree.

Stacking

CR_0000152647

When configured for IP Stacking, the commander or stack member does not respond to packets that are 1461 bytes or greater.

Switch Hang

CR_0000154477

Attempting to apply a 32-character local-mac profile name to a 32-character local-mac mac-group name causes the switch to become unresponsive, requiring a reboot to recover.

TACACS

CR_0000155541

TACACS authentication is not working with encrypt credentials in FIPS devices.

Version W.15.14.0009

802.1X

CR_0000149780

Already-authenticated clients that send an EAPOL-Start message are de-authenticated by the switch. This situation happens if the client runs Windows Vista and later operating systems that are set to "include learning".
The output of `show tech all` halts while displaying `hw aqread 0 8191 pbf cm`, with the message `=== The command has completed with errors. ===`

PoE

CR_0000155619

Some Unify IP phones exhibit a PoE incompatibility with some HPE switches, which might result in a hard failure of the phone. For more information, see the customer advisory at http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=c04438506&lang=en-us&cc=us.

Switch Hang

CR_0000154152

If the switch is sending output to the console at the time the switch is rebooted, the switch might hang and not boot properly.

Version W.15.14.0008

Crash

CR_0000152222

With multiple authentication protocols active in a high-stress environment, the switch might reboot unexpectedly with a message similar to `NMI event HW:IP=0x0103191c MSR:0x02029200 LR: 0x00121208 cr: 0x20000800 sp:0x02d56220 xer:0x20000000 Task='tDevPollRx' Task ID=0x2d3fc78`.

Version W.15.14.0007

Authentication

CR_0000148832

A switch configured with RADIUS authentication for primary login, and local authentication for secondary login fails to use local authentication when RADIUS servers do not respond. In that situation, the switch console is not accessible to valid users. This fix was inadvertently omitted from the original W.15.14.0007 fix list.

BPDU Protection

CR_0000144148

If VLAN 1 is not enabled on the link between a switch running rapid PVST and a switch running any Spanning Tree version, a rapid PVST switch configured for BPDU protection does not shut down the port when it receives a BPDU from the neighboring switch. However, the BPDUs are correctly dropped. This fix was inadvertently omitted from the original W.15.14.0007 fix list.
The output of show tech halts after displaying show debug buffer, with the message === The command has completed with errors. ===.

A new command tcp-push-preserve is added. This command is enabled by default, and causes TCP packets with the "push" flag to be sent before other packets in the queue. Note that high concentrations of TCP packets with push flags under certain conditions can destabilize your network. Use the no form of this command to disable the feature.

On a 2910al switch with no modules inserted, the output of show modules incorrectly lists two modules.

When the output of show power-over-ethernet brief displays a Detection Status of either Searching or Delivering for a port, the show tech all "poe_status_port all" section displays Other Fault as the Detect Stat.

IPv6 Router Advertisements that indicate an off-link prefix are not set as "preferred" in the switch, which causes incorrect information in the output of show ipv6, and can affect connectivity to hosts that use IPv6 Stateless Address Autoconfiguration. This issue also causes the sFlow "Agent Address" to be listed as 0.0.0.0.

In an IPv4 plus IPv6 environment, upon switch bootup the event log displays the set of source IP policy ("srcip") messages twice. With this fix, IPv6 policy messages are distinguished from IPv4 policy messages.

Some RMON events are not correctly defined for fault-finder (FFI), SSL, and virus throttling, which causes the switch to report an error such as system: Unknown Event ID 776 when those events occur.

In some situations with multiple TELNET and/or SSH sessions established, the switch does not accept additional management sessions even if some of the existing ones are killed, responding with the message Sorry, the maximum number of sessions are active. Try again later.
PoE

CR_0000148808

After disabling PoE on one or more ports, the output of `show cpu slot <slot-number>` shows an increase in CPU utilization of 15% or more.

sFlow

CR_0000147660

In an IPv6-only environment with Stateless Address Autoconfiguration, sFlow incorrectly uses the link-local address as the agent ID.

SNMP

CR_0000147370

After using SNMP to configure a RADIUS server on the switch, the switch does not allow a login until the switch is rebooted.

CR_0000149657

When using the "createAndWait" mode to set parameters via SNMP, multiple RADIUS servers cannot be configured.

CR_0000151035

The switch incorrectly reports that MIB object entPhysicalIsFRU = False for removable fantrays and transceivers.

Switch Hang

CR_0000146247

With both authentication and accounting enabled, the switch might become unresponsive to management, requiring a reboot to recover.

TELNET

CR_0000142571

While a user is being authenticated by a RADIUS server, issuing the `show access-list radius all` command from a TELNET session might cause the TELNET session to hang.

Web Management

CR_0000149099

When Spanning Tree Protocol (STP) is enabled via the Web user interface, "mstp" is shown as the default STP mode, and "mstp" is displayed as the operational mode after the user enables STP and saves the change. However, the command line interface shows that the switch operates in "rpvst" mode.

**Workaround:** From the Web user interface, use the dropdown menu to explicitly select "mstp" from the dropdown options, then save the change.
The switch does not allow the `lockout-mac` command to be configured for a MAC address that is all zeros (000000-000000).

The output of `show ip counters` is incorrect when routing is enabled for IP, IPv6, or multicasts.

When a trunk configured for sFlow polling is simultaneously queried via SNMP, all counter values for the trunk are zero.

On a switch configured with rapid PVST and BPDU protection, the output of the command `show spanning-tree bpdu-protection` shows zero errant BPDUs received, even when the switch has disabled a port due to receiving a BPDU. This is a display issue only, both rapid PVST and BPDU protection function properly.

The switch might reboot unexpectedly in these situations:

1. The switch is running 15.08 or earlier software, is configured to drop frames that have a destination address of 01:00:0c:cc:cc:cd, and has PVST filtering or PVST protection enabled. Then the switch is updated to 15.09 or later software.
2. The switch is running 15.09 or later software, is configured to drop frames that have a destination address of 01:00:0c:cc:cc:cd, and then PVST filtering or PVST protection is enabled.

The switch reboots unexpectedly with a message similar to `Software exception at bttfLearn.c:2616 -- in 'mLpmgrCtrl', task ID = 0xa98a9c0 -> Mac Table Error`.

With local MAC authentication enabled, issuing the `show run` command causes a small decrease in the switch's available memory. Over time if memory becomes depleted, the switch might reboot unexpectedly with a message similar to `Software exception at cli_show_config.c:667 -- in 'mSess6', task ID = 0xa965540`.

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=0x00b31000.`
Display Issue

**CR_0000140830**

When terminal length is changed from the default of 24, the config file display is truncated, and the outputs of `show logging` and `show interfaces` might be interleaved in the output of `show tech all`.

Fastboot

**CR_0000141043**

If the fastboot setting is changed by the user, and the switch experiences a power interruption or reboot while the new setting is being written to flash, upon bootup the MAC address on a switch or stack member might be erased. Note that this fix has a side effect: If the fastboot setting is changed by the user and the switch software is downgraded (changed to an earlier version), upon bootup the fastboot setting might revert to what it was before the user-initiated change, even though the switch reports that it has been changed.

**Workaround:** Change the fastboot setting twice - first change it back to what it was before the user-initiated change, then change fastboot to the desired setting.

Flow Control

**CR_0000140706**

With flow control enabled, the switch might not always forward high priority frames (such as Spanning Tree BPDUs) if it has received PAUSE frames from the connected device.

IGMP

**CR_0000138408**

Joins sent by clients in response to a Group Specific Query are not forwarded by the Querier, causing the clients to lose the stream.

**CR_0000140514**

After disabling IGMP forwarding on a port, multicast traffic incorrectly continues to flow from that port.

IP Phones

**CR_0000147849**

Alcatel phones might reboot unexpectedly when connected to a switch configured for IP phones to use MAC authentication and for PCs to use 802.1X authentication.

MAC Table

**CR_0000143371**

A MAC table entry does not age out while there is traffic destined to the MAC address, even if no traffic is received from that MAC address.
MSTP

CR_0000134194
With Spanning Tree enabled, configuring a live port as an admin-edge-port causes the output of show run to display a fixed path-cost for that port in the IST (for example, spanning-tree instance ist 5 path-cost 20000). Note that this is a display issue only, the switch uses the automatic path-cost based on the link speed.

Multicast

CR_0000138817
When a multicast stream is sent to a reserved multicast address, a General Query might not be forwarded by the switch, causing clients to be dropped from the multicast stream.

Stacking

CR_0000135643
With the default terminal size of 80x24, connecting to the stack commander via TELNET or SSH results in the list of stack member switches displayed below the command prompt, with each additional member overwriting the previous one, leaving only the last stack member visible to the user.

Transceivers

CR_0000143444
Software does not allow the dual-speed J8177C Gigabit-copper transceiver to be configured for 100 Mbps operation, responding with a message such as Value auto-100 is not applicable to port A21. This is the same fix as CR_0000132781 in 15.13.0003, which was inadvertently removed by CR_0000126473 in 15.13.0004 software.

Version W.15.14.0005

RADIUS

CR_0000138258
In some situations, the switch response to "Change of Authorization" and "Disconnect Messages" from the RADIUS server is sent from an incorrect source IP address, which the RADIUS server therefore ignores.

Version W.15.14.0004
Version W.15.14.0004 was never built.

Version W.15.14.0003
Version W.15.14.0003 was never built.
802.1X

CR_0000134257

After 802.1X frame counters reach a maximum value of 2,147,483,647, the counters are displayed as negative values that become smaller until they reach zero. When the counters reach zero, they begin incrementing again.

Accounting

CR_0000133762

If a Windows system is configured for both computer authentication and user authentication, accounting might not function properly.

Authentication

CR_0000134114

With both 802.1X and MAC Authentication configured on a port, it is possible for an already-authenticated client to be erroneously moved to the unauthenticated VLAN.

CLI

CR_0000136428

CLI output for show ip igmp vlan x conf displays a plus sign under the Interconnect Trunk column heading, and nothing (blank) under the Port column heading.

CR_0000138493

The error message is not clear when the user attempts to create an overlapping network on a switch. This fix was inadvertently omitted from the original W.15.14.0002 fix list.

Config

CR_0000124808

A switch that is upgraded from K.14 to K.15 software or from W.14 to W.15 software has a tilde erroneously added to the community name specified in the snmp-server host command.

CR_0000131054

Setting an operator or manager password on the switch causes four features to be disabled: auto run, DHCP-based config file download from an external tftp server, DHCP-based software image download from an external tftp server, and tftp server functionality within the switch. With this fix, more accurate messages are sent regarding the specific features that are disabled by setting the operator or manager password.

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.
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.

When a configuration file is downloaded to the switch, a default SNMPv3 user named "initial" is created on the switch even though it is not in the config file.

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.

In a rare situation the switch might reboot unexpectedly with a message similar to Software exception at rt_table.c:4453 -- in 'eRouteCtrl', task ID = 0xa9c4c00 -> Routing Stack: Assert Failed. This improves the original Crash fix (CR_0000120116).

With SNTP configured, in a rare situation after a time update the switch might reboot unexpectedly with a message similar to Health Monitor: Invalid Instr Misaligned Mem Access HW Addr=0x31352e30 IP=0x31352e30 Task='mDebugCtrl' Task ID=0x3c9558c0 sp: 0x11f92cd0 lr:0x31352e31 msr: 0x02029200 xer: 0x00000000 cr: 0x28000400.

After boot, a switch that has a syslog server and an IPv6 address configured might become unresponsive to management, and after a period of time the switch might reboot repeatedly with a message similar to NMI event SW:IP=0x001517d4 MSR:0x02029200 LR:0x0015178c cr: 0x28000400 sp: 0x03aae0e0 xer:0x00000000 Task='mDebugCtrl' Task ID=0xa9f8000.

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.

A switch acting as a DHCP relay agent sends two DHCP packets, one of which incorrectly has the source MAC address of the client instead of 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.

GVRP

CR_0000130090
After rebooting the switch, the configuration unknown-vlans disable does not work on trunks.

ICMP

CR_0000134682
The switch does not log an unsolicited ICMP reply unless it has first pinged some (any) IP address. Also, unsolicited ICMP reply log messages are sometimes associated with the DEFAULT_VLAN instead of the VLAN of the incoming unsolicited ICMP reply.

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.

IGMP

CR_0000134412
The switch sends an IGMP General Query with an incorrect layer 2 destination 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.

Jumbo Frames

CR_0000137961
When jumbo frames are enabled on any VLAN, OSPF fails to establish an adjacency after a switch reboot, and RIP updates might not be accepted by the router.

Link

CR_0000137549
Gigabit fiber transceivers operate in auto-negotiation mode even if the port is configured for 1000 Mbps full-duplex operation (speed-duplex 1000-full). If both sides of the link were configured as 1000-full, the link will go down after the switch at one side of the link is updated with affected software. This issue was introduced in software version 15.12.0006.
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.

MAC Authentication

CR_0000129991
MAC Authentication fails when the peap-mschapv2 parameter is included in the aaa authentication CLI command.

OpenFlow

CR_0000134471
OpenFlow flows are not programmed correctly when RPVST+ is disabled on the OpenFlow member VLAN.

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 which password is changed.

RADIUS Accounting

CR_0000137793
An interim-update status request generates incorrect accounting information in the RADIUS server. This issue was introduced with CR_0000123330.

Routing

CR_0000123230
The switch does not forward traffic to a host that has a static route configured with a 32-bit subnet mask. Traces show that the switch never sends an ARP request for that host.

sFlow

CR_0000128439
When an sFlow-sampled inbound packet is to be routed, the sFlow data gives the wrong output port on the switch.

CR_0000134427
sFlow sampling of multicast packets sometimes results in duplicate packets that can cause pixelation of video or other degradation of the multicast stream.
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.

CR_0000135477
A trap from an undocumented OID can be triggered under certain conditions. With this fix, OID 1.3.6.1.4.1.11.2.3.7.11.107.0.2 has been added to the MIB.

SSH

CR_0000130312
The output of `show ip ssh` lists incorrect port numbers for the clients.

SSL

CR_0000127972
A self-signed certificate cannot use a common name (CNAME) longer than 40 characters. With this fix, the limit is 90 characters.

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.

TFTP

CR_0000123187
TFTP file transfers initiated via TELNET or SSH fail, if the console inactivity-timer setting causes the TELNET or SSH session to end during the transfer. This issue does not affect file transfers initiated via the console or via SFTP.

Transceivers

CR_0000132781
Software does not allow the dual-speed J8177C Gigabit-copper transceiver to be configured for 100 Mbps operation, responding with a message such as `Value auto-100 is not applicable to port A21`.

CR_0000133023
100-Megabit transceivers might have one or more of these symptoms:
1. Link LED is lit but link is down
2. No Link after the transceiver is hot-swapped
3. Transceiver fails self test
Trunking

CR_0000126473
The switch does not allow a static LACP trunk to be configured as active or passive. This fix adds a new interface command: `lacp static [active | passive].`

Web Management

CR_0000135883
The "Rx Errors" column is missing from the Web user interface.

CR_0000137792
A self-signed SSL certificate generated via the Web interface cannot use a common name (CNAME) longer than 40 characters. With this fix, the limit is 90 characters.

Upgrade information

Upgrading restrictions and guidelines
W.15.14.0015 uses BootROM W.14.06. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

For more information about BootROM, see the Management and Configuration Guide for your switch.

**IMPORTANT:**
During the software update, the switch will automatically boot twice. The switch will update the primary BootROM, then reboot, and then update the secondary BootROM. After the switch flash memory is updated and the final boot is initiated, no additional user intervention is needed. Do not interrupt power to the switch during this important update.
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

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: Software downloads
  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](http://www.hpe.com/services/getconnected)
- **HPE Proactive Care services**: [www.hpe.com/services/proactivecare](http://www.hpe.com/services/proactivecare)
- **HPE Proactive Care service**: [www.hpe.com/services/proactivecaresupportedproducts](http://www.hpe.com/services/proactivecaresupportedproducts)
- **HPE Proactive Care advanced service**: [www.hpe.com/services/proactivecareadvancedsupportedproducts](http://www.hpe.com/services/proactivecareadvancedsupportedproducts)

Proactive Care customer information

- **Proactive Care central**: [www.hpe.com/services/proactivecarecentral](http://www.hpe.com/services/proactivecarecentral)
- **Proactive Care service activation**: [www.hpe.com/services/proactivecarecentralgetstarted](http://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:


Additional warranty information

- **HPE ProLiant and x86 Servers and Options**: [www.hpe.com/support/ProLiantServers-Warranties](http://www.hpe.com/support/ProLiantServers-Warranties)
- **HPE Enterprise Servers**: [www.hpe.com/support/EnterpriseServers-Warranties](http://www.hpe.com/support/EnterpriseServers-Warranties)
- **HPE Storage Products**: [www.hpe.com/support/Storage-Warranties](http://www.hpe.com/support/Storage-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:

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.