P.2.24 Release Notes

a Hewlett Packard
Enterprise company

Part Number: 5200-7097
Published: April 2020
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

Description

This release note covers software versions for the P.2 branch of the software.

Version P.2.1 was the initial release of Major version P.2 software. P.2.1 software was built from the same source as P.1.6. P.2.1 includes all enhancements and fixes in P.1.6 software, plus the additional enhancements and fixes in the P.2.1 enhancements and fixes section of this release note.

Product series supported by this software:

- HPE 1810 8G Switch Series
- HPE 1810 24G Switch Series

Version history

All released versions are fully supported by Hewlett Packard Enterprise, unless noted in the table.

Version	Release date	Remarks
P.2.24	2020-03-30	Released, fully supported, and posted on the web.
P.2.23	2018-04-02	Released, fully supported, and posted on the web.
P.2.22	2017-04-10	Released, fully supported, and posted on the web.
P.2.21	2016-06-06	Released, fully supported, and posted on the web.
P.2.20	n/a	Never released.
P.2.19	n/a	Never released.
P.2.18	2016-01-06	Released, fully supported, and posted on the web.
P.2.17	n/a	Never released.
P.2.16	2015-02-19	Released, fully supported, and posted on the web.
P.2.15	2014-09-26	Released, fully supported, but not posted on the web.
P.2.14	2014-09-10	Released, fully supported, but not posted on the web.
P.2.13	2014-01-07	Released, fully supported, but not posted on the web.
P.2.12	2013-08-05	Released, fully supported, and posted on the web.
P.2.11	2013-04-03	Released, fully supported, but not posted on the web.
P.2.10	2012-12-07	Released, fully supported, and posted on the web.
P.2.9	2012-09-18	Released, fully supported, but not posted on the web.
P.2.8	2012-04-03	Released, fully supported, but not posted on the web.

Table Continued

Version	Release date	Remarks
P.2.7	2012-01-23	Released, fully supported, but not posted on the web.
P.2.6	2011-12-02	Released, fully supported, but not posted on the web.
P.2.5	2011-07-26	Released, fully supported, but not posted on the web.
P.2.4	2011-07-15	Released, fully supported, but not posted on the web.
P.2.3	2011-02-18	Released, fully supported, but not posted on the web.
P.2.2	2010-11-24	Released, fully supported, and posted on the web.

Products supported

This release applies to the following product models:

Product number	Description
J9449A	HPE 1810 8G Switch
J9450A	HPE 1810 24G 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

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

Enhancements

This section lists enhancements found in the P.2.18 branch of the software. Software enhancements are listed in reverse-chronological order, with the newest at the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions.

NOTE:

The number that precedes the enhancement description is used for tracking purposes.

Version P.2.24

No enhancements were included in version P.2.24.

Version P.2.23

No enhancements were included in version P.2.23.

Version P.2.22

No enhancements were included in version P.2.22.

Version P.2.21

No enhancements were included in version P.2.21.

Version P.2.20

Version P.2.20 was never released.

Version P.2.19

Version P.2.19 was never released.

Version P.2.18

No enhancements were included in version P.2.18.

Version P.2.17

Version P.2.17 was never released.

Version P.2.16

No enhancements were included in version P.2.16.

Version P.2.15

No enhancements were included in version P.2.15.

Version P.2.14

No enhancements were included in version P.2.14.

Version P.2.13

No enhancements were included in version P.2.13.

Version P.2.12

No enhancements were included in version P.2.12.

Version P.2.11

No enhancements were included in version P.2.11.

Version P.2.10

No enhancements were included in version P.2.10.

Version P.2.9

No enhancements were included in version P.2.9.

Version P.2.8

No enhancements were included in version P.2.8.

Version P.2.7

No enhancements were included in version P.2.7.

Version P.2.6

No enhancements were included in version P.2.6.

Version P.2.5

No enhancements were included in version P.2.5.

Version P.2.4

No enhancements were included in version P.2.4.

Version P.2.3

No enhancements were included in version P.2.3.

Version P.2.2

No enhancements were included in version P.2.2.

Version P.2.1

No enhancements were included in version P.2.1.

Fixes

Software fixes are listed in reverse-chronological order, from newest to oldest software version. Unless otherwise noted, each software version listed below includes all the software fixes and enhancements added in previous versions listed below. P.1.6 was the first software version for HPE 1810G switches.

NOTE:

The number that precedes the fix description is used for tracking purposes.

Version P.2.24

HTTPS
CR_0000250442

Symptom/Scenario: Firefox 66 and newer browser versions check for unique serial numbers within the self-signed certificate.

Version P.2.23

Trunking
CR_0000241136

Symptom/Scenario: If a multicast packet is received on the highest port number of a trunk, the packet is incorrectly forwarded back to the sender.

Version P.2.22

Trunking
CR_0000223122

Symptom/Scenario: Unable to permanently delete a Trunk group as the configuration will not be preserved following a reboot.

Workaround: Trunk groups may be manually removed from the Trunk configuration webpage.

Version P.2.21

Support Links

CR_0000200768 Support links were updated to the hpe.com domain.

Version P.2.20

Version P.2.20 was never released.

Version P.2.19

Version P.2.19 was never released.

Version P.2.18

SSL

CR_0000167323 The remote service accepts connections using SSL 2.0 or 3.0, which may suffer from several cryptographic flaws. NIST has determined that SSL v3.0 is no longer acceptable for secure communications between the affected service and clients. As per date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Workaround: Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.0 or higher instead.

Version P.2.17

Version P.2.17 was never released.

Version P.2.16

No fixes were included in version P.2.16.

Version P.2.15

Subnet Mask

CR_0000158242 The error message when entering an incorrect subnet mask has been fixed. Previously, an error such as `Error! Failed to Set 'Community Name' with <subnet mask IP>` was being displayed instead.

Trunking

CR_0000154885 When saving the configuration, even if the configuration has not changed, a trunk goes down for several seconds.

Version P.2.14

Crash

CR_0000152728 The switch unexpectedly reboots when being discovered by certain network management software, such as Observium. It occurs when the switch incorrectly processes the SNMP Get of lldpRemSysDesc from the network management software.

Web Authentication

CR_0000153455 A blank default gateway is not allowed (0.0.0.0), resulting in various error messages when saving as either blank or 0.0.0.0.

Version P.2.13

Jumbo Frames

CR_0000145820 When Jumbo Frames are transmitted over a trunked port, the software increments both the counters `Transmitted Packets without Errors` and `Transmitted Packets with Errors`.

LLDP

CR_0000142692 The switch transmits incorrect LLDP MED TLVs that contain an incorrect VLAN ID, thus causing devices to be assigned to an incorrect or non-existing VLAN. The proper behavior for the switch is not to transmit LLDP MED packets.

Port Access

CR_0000128904 Randomly, a port on the switch might hang. No MAC addresses are registered on the port and both inbound and outbound traffic is no longer forwarded on an affected port. The only recovery method is to reset the switch.

SNMP

CR_0000140101 The software does not create an instance for a trunk for the object ifInDiscards (. 1.3.6.1.2.1.2.2.1.13). When the object is queried, the log might return the following message:

```
UNKN Failed to get counter value.
```

When requesting the trunk's instance of the object directly, the software returns the error:

```
No Such Instance currently exists at this OID.
```

SNTP

CR_0000142367 The switch might stop requesting SNTP updates after it receives a Kiss-of-Death (KoD) packet with an INIT or STEP code. After it receives such a packet, the switch should retransmit using an exponential backoff algorithm if no other NTP server is available, but instead, it stops requesting SNTP updates altogether.

Version P.2.12

Event Log

CR_0000131240 After each reboot, the switch log includes a message similar to `Migrating config file log.cfg from version 1 to 2. A configuration file version mismatch was detected so a configuration file migration has started.` With this fix, the message appears only after the first reboot with new software.

IP Communication

CR_0000131152 Some clients connected directly to the switch become unable to communicate on the network. When this happens, the switch log shows `Unable to delete FDB entry messages`.

Web Management

CR_0000135147 When the switch handles broadcast traffic at rates of 500 packets/second or more, the switch's Web user interface responds very slowly. This issue affects only switch management; network traffic, including broadcast traffic, is switched properly.

Version P.2.11

Counters

CR_0000126495 Jumbo frames received by the switch are not included in the interface counters.

Version P.2.10

No fixes were included in version P.2.10.

Version P.2.9

Counters

CR_0000118897 The `SysUptime` shows zero after 49.7 days, although the switch does not reboot at 49.7 days.

MAC Table

CR_0000116501 Addresses in the MAC table are displayed with the VLAN prepended in HEX as the first two leading bytes, which is confusing for administrators. For example, `00:01:00:00:85:4E:59:4A`.

Version P.2.8

ARP

CR_0000110978 The switch does not update its ARP cache with information from a gratuitous ARP packet.

DHCP

CR_0000110554 The switch does not get an IP address from the DHCP server when there are two IPs configured in Router options.

Web Management

CR_0000109304 Port configuration for 1000Base-SX SFP on dual-personality ports 23/24 are changed automatically from 1000FDX to AUTO after reboot or power cycle.

CR_0000110351 The switch does not save changes to the originally-configured SysLog Host IP address.

Version P.2.7

Event Log

CR_0000105018 Excessive error messages appear in the log file regarding `avl mac delete` errors similar to the following:

```
200 06 03:33:03 9 is Link Down201 06 03:33:03 avl mac delete error.202 06 03:33:05
9 is Link Up
```

Switch Hang

CR_0000105424 The switch cannot be accessed by the web user interface, and end-user traffic is not forwarded after 2-3 days of system uptime.

Version P.2.6

Event Log

CR_0000105930 Using the wrong log-level for SNTP messages results in filling up the log with successful NTP sync messages.

SNMP

PR_0000072943, CR_0000077752 The switch uses incorrect OIDs for `lldpRemChassisIdSubtype`.

Version P.2.5

Web Management

PR_0000072872 When logging into the switch via the web user interface at the login dialog box, using the **Enter** key does not work; you must click the **login** button.

Version P.2.4

SNMP

PR_0000070032 SNMP walk on `SNMPv2-SMI::mib-2.17.4.3.1.1` (MAC table) times out at around 380-400 addresses.

PR_0000070455 The MIB object `ifStackStatus` (1.3.6.1.2.1.31.1.2.1.3) does not hold the correct value.

Web Management

PR_0000072156 Underscore characters were not allowed in community names.

PR_0000072776 It was possible to set the subnet mask to an illegal value of 0.0.0.0.

PR_0000072786 Password change did not provide a confirmation.

Version P.2.3

DHCP

PR_0000065677 Sometimes the switch does not renew a DHCP lease after it expires.

PR_0000067398 If the switch is configured for DHCP but cannot reach a DHCP server, the switch reverts to its default IP address of 192.168.2.10/24, and becomes inaccessible on the network. After 60 seconds this configuration is automatically saved, replacing the desired DHCP configuration.

SNMP

PR_0000060097 The switch does allow LLDP information to be accessed via SNMP.

Version P.2.2

Loop Protection

PR_0000064159 A port that is configured for loop protection and is administratively disabled is wrongly enabled when a device is connected to that port.

Version P.2.1

LLDP

PR_0000061756 The switch provides incorrect LLDP values to neighbor switches.

SNMP

PR_0000061888 The switch stores incorrect information in the Bridge MIB table.

Upgrade information

NOTE:

To update from P.1.x (where x <= 19) to P.2.x, you must update to P.1.20 first. Therefore, this is a two-step update:

1. Update P.1.x to P.1.20.
2. Update P.1.20 to P.2.x.

Both these update paths and the path to downgrade from P.2.x to P.1.x are described in this section.

Use Update Manager to Update/Downgrade Switch Software

Update Manager enables a new image or configuration file to be downloaded from a local or network system to the switch. To access this page, click **Maintenance** > **Update Manager** in the navigation pane.

NOTE: Downloading new software does not change the current switch configuration. The switch configuration is contained in a separate file that can also be uploaded or downloaded (for example, as backup, or for use in another switch of the same model).

Update Manager displays different options depending on the transfer protocol, file, or image type selected for an update. In the example in **Figure 1: Update Manager page**, the inactive (or Backup) image on the switch is being updated with the file named `switchdrvr.stk` from a TFTP server. For example, if the `image1` file is being used as the currently-active image running on the switch, then `image2` is the backup image file to be updated. To check the software version in each image, and to determine which image is currently active, use the **Status** > **Dual Image** screen.

Figure 1: *Update Manager page*

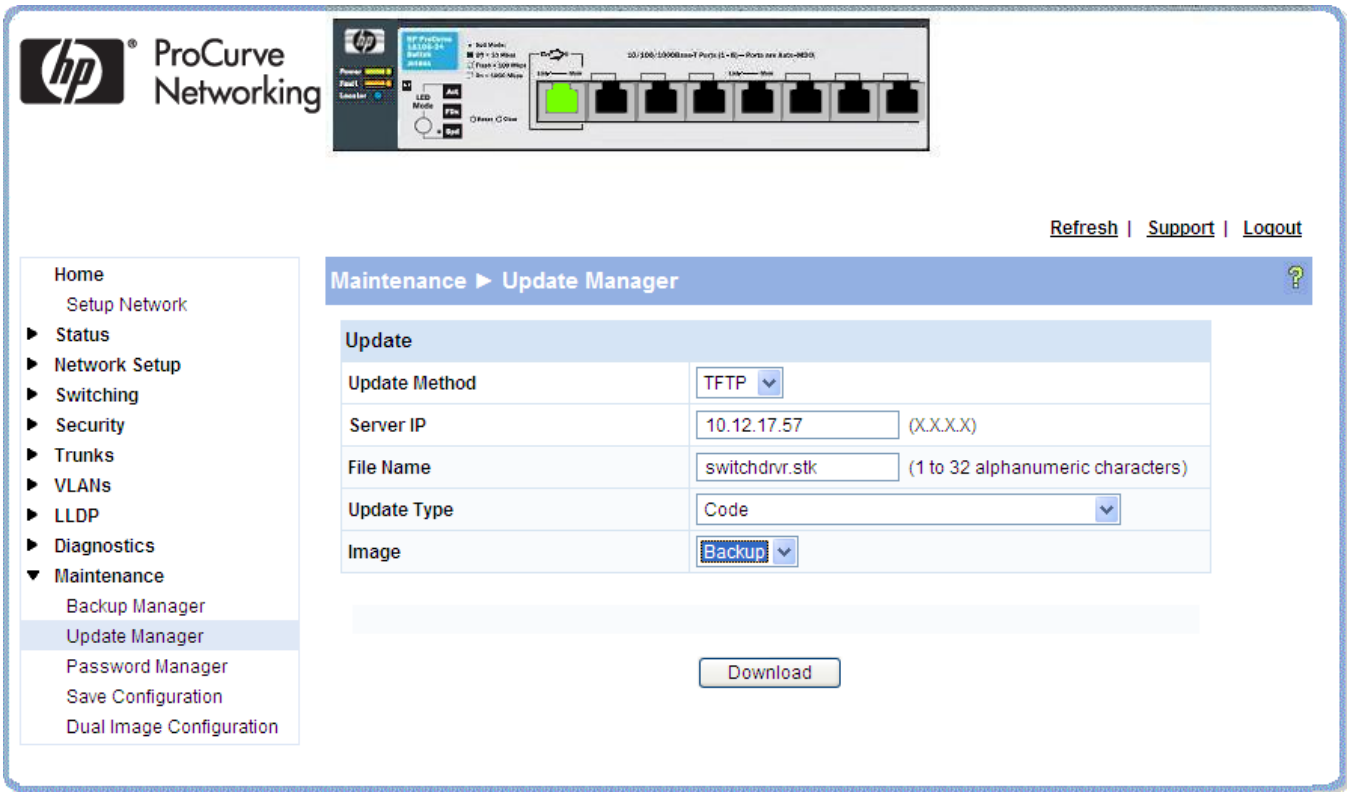


Table 1: *Update Manager Fields*

Field	Description
Update Method	Select the protocol to use: • **HTTP** - The file is downloaded using HTTP from a local or remote drive. • **TFTP** - The file is downloaded using TFTP from a TFTP server operating on the system/network.
Browse for file (HTTP download)	If HTTP is used for the software download, click **Browse** to select the designated file. **NOTE:** If the file name differs from the default name on the switch, the file will be renamed to the default name when downloaded.

Table Continued

Field	Description
Server IP (TFTP download)	If a TFTP download is performed, enter the IP address of the TFTP server.
File Name (TFTP download)	If a TFTP download is performed, enter the name of the software file on the TFTP server.
Update type	Select the file type to be updated: • **Code** - Update the software image file. • **Configuration** - Update the configuration file. • To update an SSL certificate or key encryption file, select the certificate type (for a description of these files, see the *Management and Configuration Guide* for your switch). • **SSL Trusted Root Certificate PEM File** - SSL Trusted Root Certificate File, which is encoded using the Privacy Enhanced Mail (PEM) protocol. • **SSL Server Certificate PEM File** - SSL Server Certificate File (PEM-encoded). • **SSL DH Weak Encryption Parameter PEM File** - SSL Diffie-Hellman Weak Encryption Parameter File (PEM encoded). • **SSL DH Strong Encryption Parameter PEM File** - SSL Diffie-Hellman Strong Encryption Parameter File (PEM encoded).
Image (for Code updates)	If **Code** is selected as the update type, select which of the two images stored on the switch is to be updated: • **Active** - The downloaded image will replace the currently active image. • **Backup** - The downloaded image will replace the backup image.

Updating the Switch Software to P.1.x

CAUTION: HPE recommends that you back up the image file before updating it. For information on Backup Manager, see the *Management and Configuration Guide* for your switch.

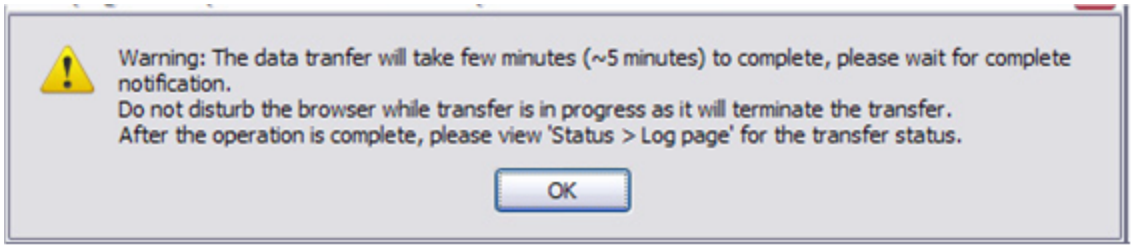
Follow these instructions to update the switch software (firmware code image):

Procedure

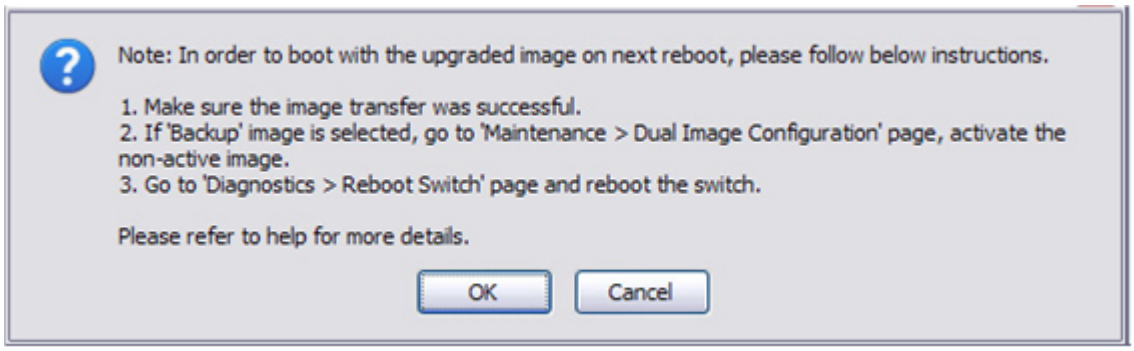
1. In the **Update Method** field, select the protocol to use to upload the file to the system. If the file is located on a local or network drive, select **HTTP**. If the file is located on a TFTP server, select **TFTP**.
2. If **TFTP** is selected, specify the IP address of the TFTP server and the name of the file as it appears on the server. If **HTTP** is selected, browse to locate the file on your network or local drive.
3. In the Update Type field, select **Code**.
4. In the **Image** field, choose **Backup** or **Active**.
5. If you choose **Backup**, the inactive (backup) image file will be updated. In the example in **Figure 1: Update Manager page**, the Backup image file is selected for update.
6. If you choose **Active**, the active image file is updated. To check the software version in each image, and to determine which image is currently active, use the **Status** > **Dual Image** screen.

NOTE: When updating to P.1.20, the new switch software should always be downloaded to Image1. Any other P.1.x may be loaded on Image1 or Image2.

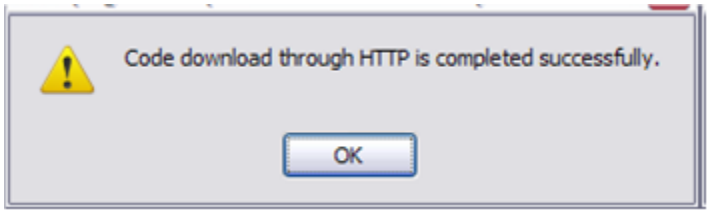
7. Click **Download**.
8. A warning page like the following displays (the text may differ depending on the protocol selected):



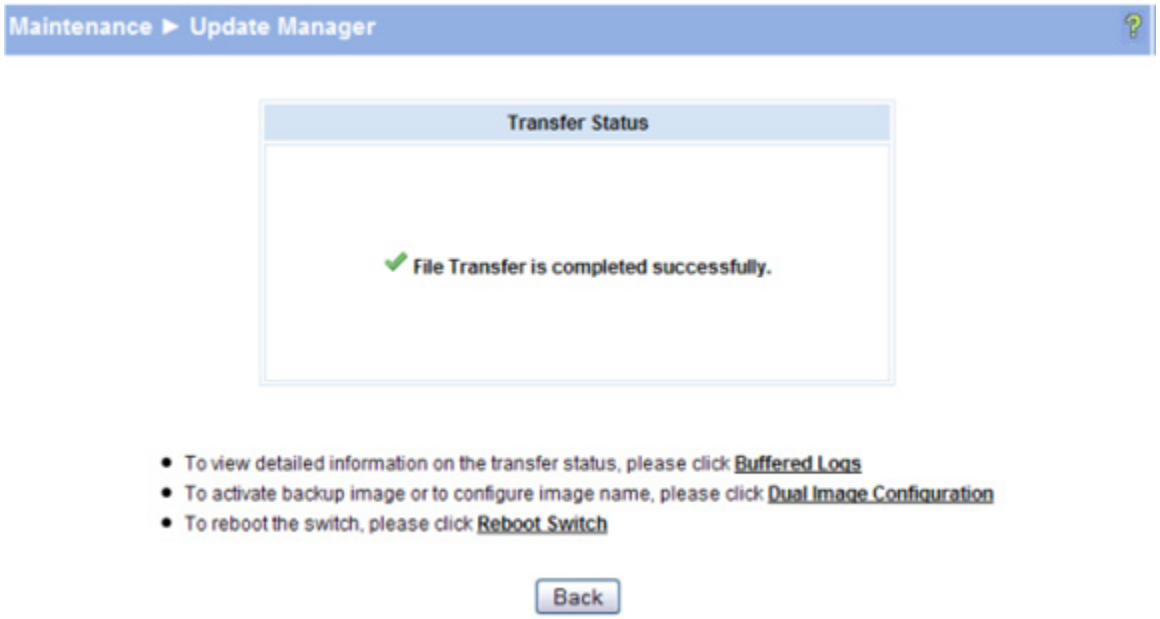
9. Click **OK**.
10. The following page displays.



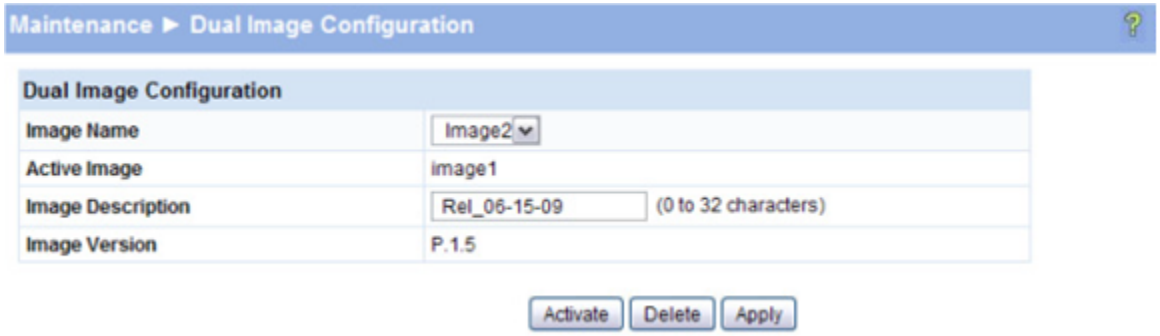
11. Click **OK**.
12. A download in progress page displays. When the transfer is complete, a window like the following displays:



13. Click **OK**.
14. Update Manager displays the following status message:

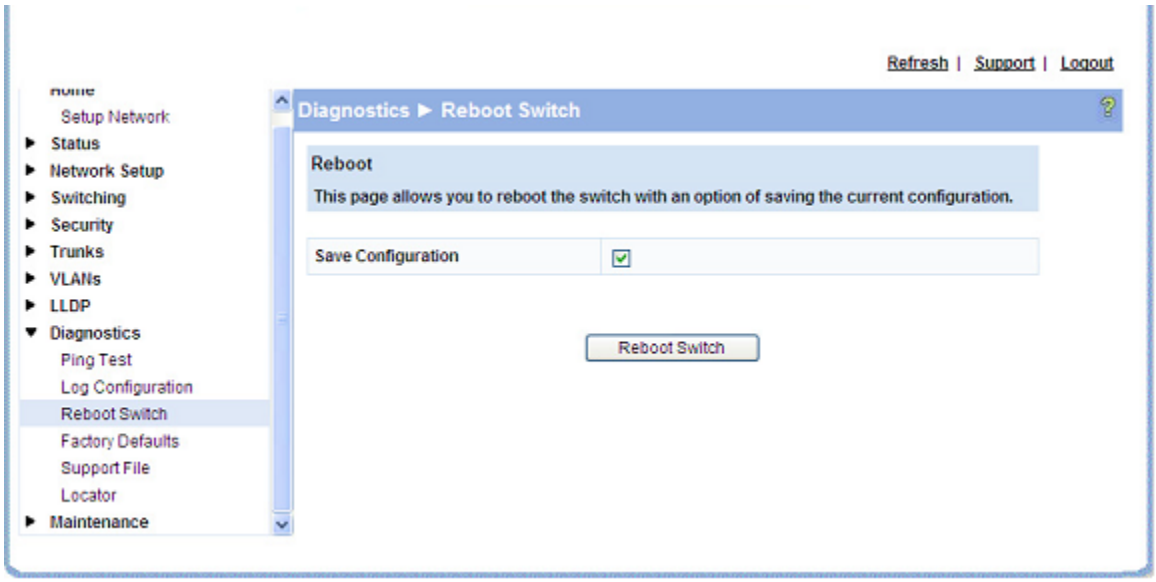


15. Click **Back** to redisplay the **Update Manager** page.
16. In this example, the image was downloaded as the inactive (backup) image. To complete the update process and to activate the backup image as the operating software, use the **Dual Image Configuration** page.
17. In the next figure, Image1 is the active image and is the newly updated backup image. Image2 is to be activated on the next reboot (and Image1 will become the inactive backup image).



18. (Optional) Add a description for the selected image (Image2) and click **Apply**.
19. Click **Activate** to activate the selected image on the next reboot.
20. You can verify the next active image prior to rebooting the switch by viewing the **Status** > **Dual Image** screen.

21. Click **Diagnostics** > **Reboot Switch**, and then click **Reboot Switch** to complete the update.



22. Wait about a minute, then refresh your browser to redisplay the Web interface.
23. Upon reboot, the previously-active image (Image1, in this example) becomes the inactive (backup) image.

Updating the Switch Software P.1.x to P.2.x

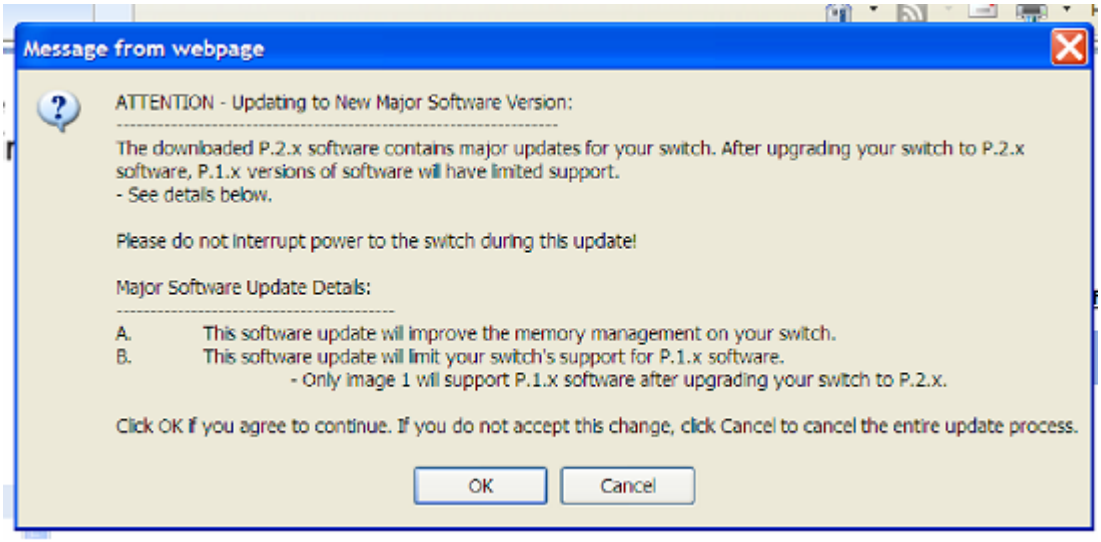
NOTE:

Before updating to P.2.x, you must first update to P.1.20 (on Image1) following the procedure described above.

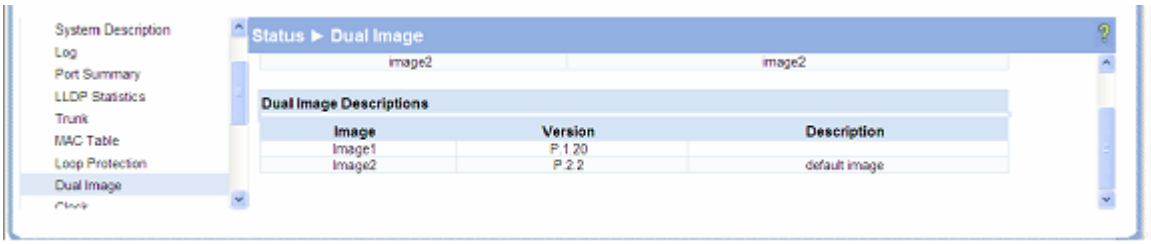
In addition, the initial update to P.2.x is allowed on the Image2 location only. After the switch is booted with P.2.x in Image2, P.2.x software versions can be loaded onto either Image1 or Image2.

Procedure

1. Update to P.2.x (on Image2) following the procedure described above. Once P.2.x has been downloaded, the message in the next figure is displayed.



2. After the download, activate P.2.x and reboot the switch. At this point you can verify the switch software versions by viewing the **Status** > **Dual Image** screen (next figure).

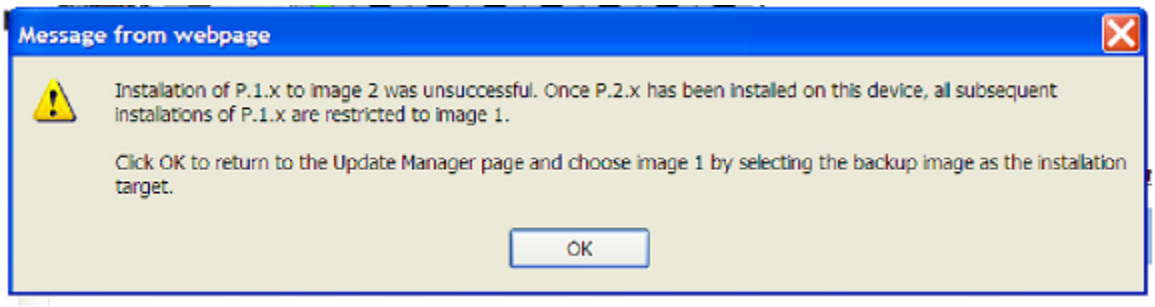


Downgrading the Switch Software P.2.x to P.1.x

Once the switch has been updated to P.2.x, only Image1 will support P.1.x software. Therefore, to downgrade to P.1.x, the software must be loaded to Image1. If you attempt to downgrade by loading P.1.x on Image2, switch behavior differs depending on the software installed on Image1. The differing behaviors are described below.

Downgrading the Switch Software with P.1.20 Installed on Image1

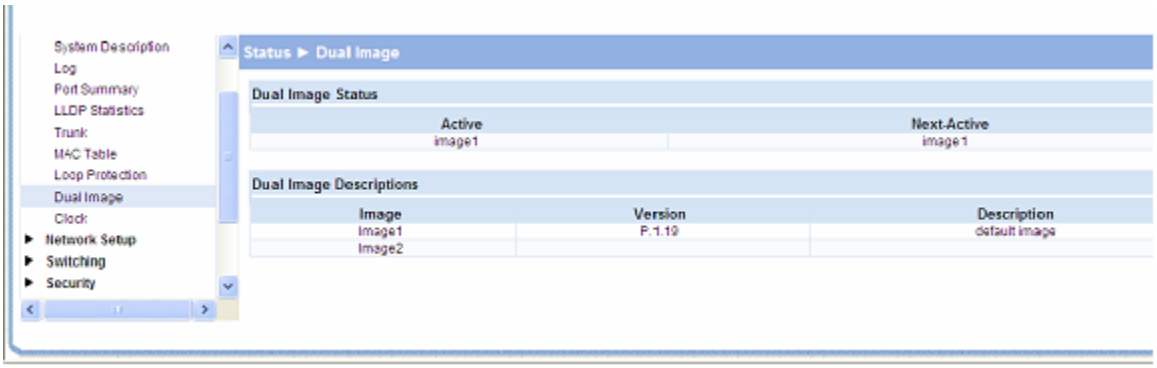
As long as Image1 has P.1.20 installed, any attempt to load P.1.x to Image2 will fail with the following message displayed:



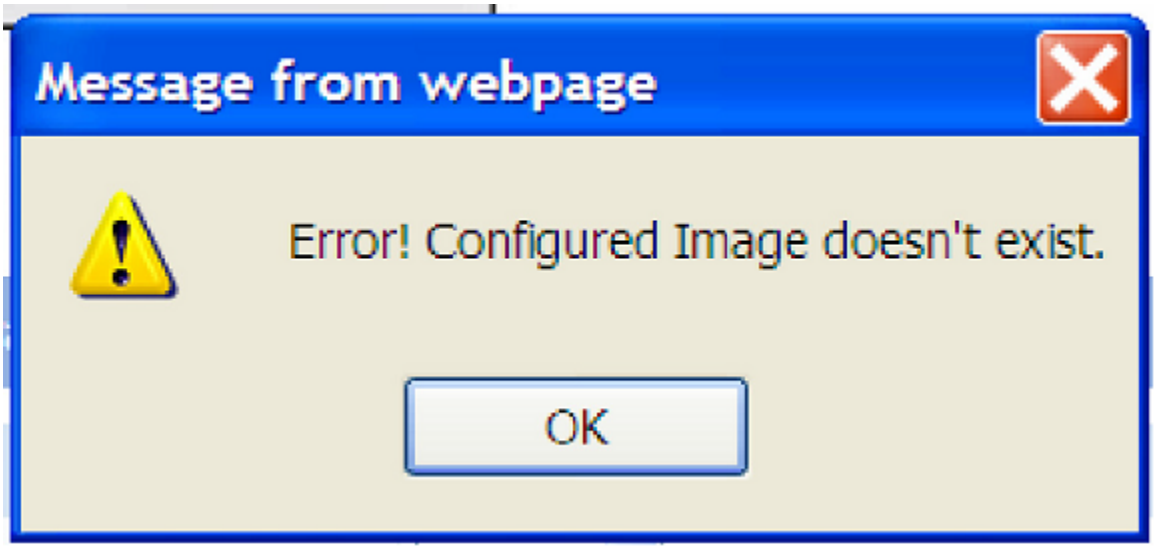
Downgrading the Switch Software with P.1.x (where x <=19) Installed on Image1

Once you have successfully downgraded switch software by downloading P.1.x (where x <=19) to Image1, activating Image1, and booting into P.1.x on Image1, the switch can no longer recognize the P.2.x software

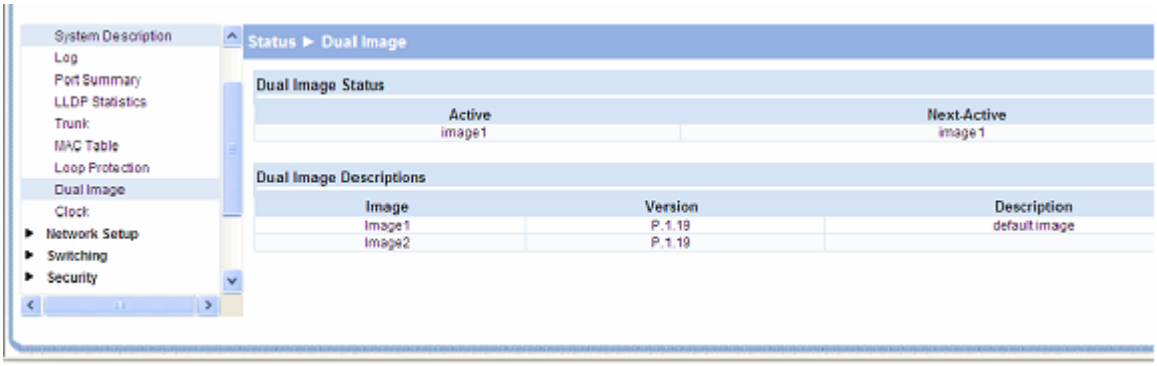
loaded on Image2. The **Status** > **Dual Image** screen shows the following even though P.2.x is still installed on Image2.



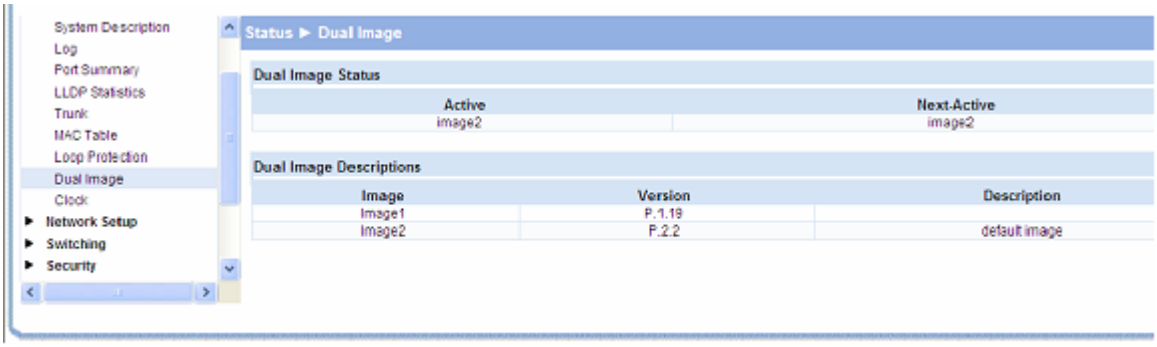
In this situation, Image2 cannot be updated, activated, or deleted. If you try to activate Image2 from the **Maintenance** > **Dual Image Configuration** screen, the following message is displayed:



If you now attempt to load P.1.x to Image2, the download appears to work. For example, if you download P.1.19 on Image2, with P.1.19 already on Image1, the **Status** > **Dual Image** screen shows the following before Image2 is activated and the switch is rebooted.



Next activate Image2 and reboot the switch. The **Status** > **Dual Image** screen now shows the following, and illustrates that in reality, P.2.2 never does get uninstalled from Image2.


System Description
Log
Port Summary
LLDP Statistics
Trunk
MAC Table
Loop Protection
Dual Image
Clock
Network Setup
Switching
Security
Status ▶ Dual Image
Dual Image Status
Active
image2
Next-Active
image2
Dual Image Descriptions
Image
Version
Description
Image1
P.1.19
Image2
P.2.2
default image

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 **http://www.hpe.com/support/Subscriber_Choice** to initiate a subscription to receive future Hewlett Packard Enterprise Security Bulletin alerts via email.