



Hewlett Packard
Enterprise

MSM7xx Controllers and MSM Access Points Version 6.6.9.1 Release Notes

Abstract

These release notes provide important release-related information for MSM software Version 6.6.9.1.

Part Number: 5200-4227d
Published: May 2019
Edition: 5

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

Intel[®], Itanium[®], Pentium[®], Xeon[®], Intel Inside[®], and the Intel Inside logo are trademarks of Intel Corporation in the U.S. and other countries.

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

Adobe[®] and Acrobat[®] are trademarks of Adobe Systems Incorporated.

Java[®] and Oracle[®] are registered trademarks of Oracle and/or its affiliates.

UNIX[®] is a registered trademark of The Open Group.

Contents

- MSM software V6.6.9.1.....4**
 - Description..... 4
 - Products supported..... 4
 - Certificate replacement information..... 5
 - Upgrade information..... 5
 - Prerequisites..... 6
 - Software Updates and Licensing portal..... 6
 - Upgrading restrictions and guidelines..... 6
 - Transitioning APs from Unified controllers to use MSM software..... 6
 - HP 560 autonomous mode..... 7
 - Downgrading software..... 7
 - Compatibility/interoperability..... 7
 - Internet connection required..... 7
 - SSLv3 support..... 7
 - RF Manager software and MSM software version compatibility..... 7
 - Local mesh..... 8
 - GMS (Guest Management Software) for controllers..... 9
 - Changes..... 9
 - Fixes..... 10
 - Version 6.6.9.1..... 10
 - Version 6.6.9.0..... 10
 - Version 6.6.8.2..... 11
 - Version 6.6.8.1..... 11
 - Version 6.6.8.0..... 12
 - Version 6.6.7.1..... 13
 - Version 6.6.7.0..... 13
 - Version 6.6.5.0..... 15
 - Version 6.6.4.0..... 16
 - Version 6.6.3.0..... 17
 - Version 6.6.2.0..... 18
 - Version 6.6.0.0..... 22
 - Issues and workarounds..... 25
 - Version 6.6.9.1..... 25
 - SOAP function limitations for controller teaming environment..... 27
 - Documentation updates and corrections..... 28
 - Hewlett Packard Enterprise security policy..... 28

- Support and other resources.....29**
 - Accessing Hewlett Packard Enterprise Support..... 29
 - Accessing updates..... 29
 - Customer self repair..... 30
 - Remote support..... 30
 - Warranty information..... 30
 - Regulatory information..... 31
 - Documentation feedback..... 31

MSM software V6.6.9.1

Description

This document provides important V6.6.9.1 release information.

Products supported

This document applies to these Hewlett Packard Enterprise products:

Product number	Model
J9693A	MSM720 Access Controller
J9694A	MSM720 Premium Mobility Controller
J9695A	MSM720 Access Controller (TAA)
J9696A	MSM720 Premium Mobility Controller (TAA)
J9421A	MSM760 Access Controller
J9420A	MSM760 Premium Mobility Controller
J9370A	MSM765 zl Premium Mobility Controller
J9840A	MSM775 zl Premium Controller

Product number					
WW ¹	Americas	TAA	Japan	Israel	Model
J9846A	J9845A	—	J9847A	J9848A	HP 560 802.11ac Dual Radio AP
J9842A	J9841A	—	J9843A	J9844A	HP 517 802.11ac Unified Walljack
JG654A	JG653A	—	JG655A	JG656A	HP 425 802.11n Dual Radio AP
J9651A	J9650A	J9654A	J9652A	J9653A	MSM430 802.11n Dual Radio AP
J9591A	J9590A	J9655A	J9589A	J9618A	MSM460 802.11n Dual Radio AP
J9622A	J9621A	J9656A	J9620A	J9619A	MSM466 802.11n Dual Radio AP
J9716A	J9715A	—	J9717A	J9718A	MSM466-R 802.11n Dual Radio Outdoor AP

¹ Identifies worldwide regions not otherwise explicitly named.

Product number				
WW ¹	USA	Japan	Israel	Model
J9427A/B/C	J9426A/B	J9529A/B	J9616A	MSM410 802.11n AP
J9359A/B	J9358A/B	J9530A/B	J9617A	MSM422 802.11n AP
J9379A/B	J9374A/B	J9524A/B	—	MSM310 AP
J9383A/B	J9380A/B	—	—	MSM310-R AP
J9423A	J9422A	—	—	MSM317 Access Device
J9364A/B	J9360A/B	J9527A/B	—	MSM320 AP
J9368A/B	J9365A/B	J9528A/B	—	MSM320-R AP
J9373A/B	J9369A/B	—	—	MSM325 AP

¹ Identifies worldwide regions not otherwise explicitly named.

NOTE: As of Version 6.4.0.0 software release, the MSM310, MSM320, and MSM325 APs work in controlled mode only. Autonomous mode is no longer supported.

Support for the discontinued MSM335 AP is available in software versions prior to V6.4.0.0.

Certificate replacement information

A certificate included with the MSM7xx software will expire in May 2019 and needs to be replaced to avoid warnings in the web interface.

As of release 6.6.9.1, the new certificate "Entrust Root Certification Authority - G2" was added to the certificate store. This new certificate can be used to replace the expiring certificate "Entrust.net Secure Server Certification Authority."

For those with software versions prior to 6.6.9.1, you must first download the updated certificate and then install it on your controller. For those with software versions 6.6.9.1 and later, you can install the new certificate that is available in the controller certificate store.

For information on downloading the replacement certificate (for those with software versions prior to 6.6.9.1) and for information on replacing/deleting the certificate (for all software versions), consult document **HPE MSM Controller Series - "Entrust.net Secure Server Certification Authority" Certificate Included with the MSM7xx Software is Expiring and Needs to be Replaced** at: https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00072523en_us

For details on managing certificates on MSM controllers, refer to the **MSM Controllers Configuration Guide**.

Upgrade information

Prerequisites

- ❗ **IMPORTANT:** If your controller is not already running Version 5.7.5.0 or 6.0.3.0 or later, a two-step upgrade must be performed. First upgrade your controller to Version 5.7.5.0 or 6.2.1.1, and then as a second step, upgrade the controller to V6.6.9.1.
-

Mandatory channel change required prior to software upgrade; discontinue use of channel 132

Applies to these Americas/USA models: MSM410 (J9426A/B), MSM422 (J9358A/B), MSM430 (J9650A), MSM460 (J9590A), MSM466 (J9621A), MSM466-R (J9715A), MSM310 (J9374A/B), MSM310-R (J9380A/B), MSM320 (J9360A/B), MSM320-R (J9365A/B), and MSM325 (J9369A/B).

- ❗ **IMPORTANT:** Prior to upgrading to MSM software Version 6.6.9.1, all applicable APs (autonomous or controlled) that are manually configured to use channel 132 must be either reconfigured to use a different channel or be reconfigured to use auto channel. This is required because channel 132 is no longer available for use.
-

NOTE: Due to a problem with AP channel use validation, a banner similar to this may appear at the top of the Home screen: AP CNxxxxxxxx, Radio 1 channel configuration has been set to autochannel because the previously configured channel is not supported by this version of software. The same message is added to the system log. These messages can be safely ignored.

Software configuration change might be required prior to upgrade

If the MSM7xx Controller is configured with the NAT feature enabled (default setting) and with the **Extend VSC egress subnet to VSC ingress subnet** feature enabled (disabled by default), the MSM software V6.2.x and higher will disable the NAT feature. Hewlett Packard Enterprise recommends that you review your existing settings and disable one of these features before upgrading to V6.2.x or higher.

Software Updates and Licensing portal

The Software Updates and Licensing portal provides access to the latest software updates to customers with a support contract. An Hewlett Packard Enterprise Passport is required to access the Software Updates and Licensing portal at www.hpe.com/support/e-updates and it is available to customers who have purchased a maintenance and support agreement.

Upgrading restrictions and guidelines

(Not applicable to HP 425, HP 517, and MSM317.) For autonomous APs, update the software as described in the “Software updates” section of the *MSM APs Configuration Guide*.

Otherwise, update the controller software as described in the “Software updates” section of the *MSM7xx Controllers Configuration Guide*. After the controller update is complete, it automatically updates all of its controlled devices to the same software version.

Transitioning APs from Unified controllers to use MSM software

Applies to these APs that have been used with any Unified controller (HP 10500/7500, HP 830, HP 850, HP 870, or HP WX5002/WX5004 Controller):

- HP 425
- HP 560
- MSM430
- MSM460
- MSM466
- MSM466-R

❗ **IMPORTANT:** If any of these APs have ever been adopted by a Unified controller, it is mandatory to follow the procedures in the separate document *Instructions for Converting an Access Point from Unified-Controlled to Using MSM Software* before you can use these APs with MSM software (controlled or autonomous).

HP 560 autonomous mode

❗ **IMPORTANT:** The *HP 560 802.11ac Access Point Quickstart* instructs you to select the **Switch to Autonomous Mode** button. This however, may not be possible. If you do not see the **Switch to Autonomous Mode** button, it is mandatory to follow the procedures relevant to autonomous mode in the separate document *Instructions for Converting an Access Point from Unified-Controlled to Using MSM Software*.

Downgrading software

If you upgrade to Version 6.6.9.1 and then want to return to the version (older than V6.6.0.0) that you had been running prior to upgrading, the configuration that you used originally with that version will still be available.

If you have made configuration changes while using Version 6.6.9.1, those changes will not be present when you downgrade to the previous version.

If you factory reset your device after upgrading to Version 6.6.9.1, your previous configuration will be lost, and when you downgrade to any previous version you will be in a factory reset state.

Compatibility/interoperability

Internet connection required

The computer running the MSM7xx Controller web-based user interface must have an Internet connection to complete product registration or display the new Simplified UI web-based online help.

SSLv3 support

Support for the SSLv3 cryptographic protocol has been removed as of Version 6.2.1.2.

RF Manager software and MSM software version compatibility

RF Manager Versions 6.0.x, and 6.7.x work with MSM software Version 5.7.x or later. However, to use the WLAN Integration feature in RF Manager 6.0.x or 6.7.x, the RF Manager and MSM software versions must be matched as follows:

MSM7xx software version	Compatible RF Manager versions	Sensor devices version	
		Sensor-only devices (MSM415)	AP/Sensor combo devices (MSM320 ¹ , MSM325, HP 425 ²)
6.6.9.1, 6.6.9.0, 6.6.8.2, 6.6.8.1, 6.6.8.0, 6.6.7.1, 6.6.7.0, 6.6.5.0, 6.6.4.0, 6.6.3.0, 6.6.2.0, 6.6.0.0, 6.5.2.0, 6.5.1.0, 6.5.0.x, 6.4.1.0, 6.4.0.0, 6.3.0.0, 6.0.3.0, 5.7.5.0	6.7.769 or later	Upgraded automatically by RF Manager.	Upgraded automatically by MSM7xx Controller.
6.2.0.0	6.0.185, 6.7.769 or later		
5.7.4.0	6.0.185 or later		
5.7.1.x, 5.7.2.0, 6.0.0.1, 6.0.1.x	6.0.177 or later		
5.7.0.2, 5.7.0.3, 5.7.0.4	6.0.162 or later		

¹ MSM320 APs that have been upgraded to MSM325 RF sensor via HP MSM320 RF Sensor License J9384A.

² HP 425 requires RF Manager V6.7.769.42 or later.

NOTE: Software Versions 6.2.0.0 and later are compatible with RF Manager versions listed above, but the MSM320 and MSM325 sensors may appear orange and indicate that there is a version mismatch. This is expected and the sensors will function normally. Note also, that with RF Manager 6.7.769, these sensors will function at an RF Manager 6.0.x feature level.

NOTE: If you choose to use mismatched software versions with RF Manager 6.0.177 or later, you should first turn off the WLAN Integration in RF Manager.

NOTE: Upgrading an MSM7xx Controller to V6.6.5.0 also automatically upgrades any MSM320 and MSM325 Sensors it manages to MSM software V6.6.5.0.

NOTE: The MSM415 Sensor has no MSM software dependency. It is managed and upgraded directly by RF Manager.

Local mesh

Hewlett Packard Enterprise strongly recommends that the same AP model be used for nodes of the mesh. If for local mesh, recent APs (MSM430, MSM46x, HP 425, HP 560) are mixed with older APs (MSM3xx, MSM422), the local mesh connectivity might be unstable.

GMS (Guest Management Software) for controllers

⚠ CAUTION: The Simplified UI and GMS: If you will be using the Guest Management Software (GMS) Microsoft Windows application, and the MSM7xx Controllers Simplified UI, you must NOT import user accounts when prompted to do so when navigating to the Users page in the Simplified UI. Instead, when GMS will be used, manage all subscription plans and account profiles from the Advanced UI only. Failure to heed this caution will result in the user accounts being migrated to the user account model used in the Simplified UI, and such "new model" user accounts cannot be seen in GMS.

❗ IMPORTANT: As of October 2015, GMS version numbering has changed. GMS version 2.0 is the version to use with MSM software version 6.6.5.0 and higher.

GMS simplifies centralized guest-account creation from any Microsoft Windows-based computer. It provides centralized, real-time management of visitor accounts and sessions with a configurable visitor session duration per account. Working with MSM7xx Controllers, secure login prevents unauthorized account creation, and the reporting feature records all account management activity.

For details and download instructions, consult the *Guest Management Software Release Notes*. Search for "Guest Management Software" at www.hpe.com/support/hpesc.

Changes

NOTE: The numbers that precede some change descriptions are used for tracking purposes.

Version 6.6.9.1 includes the following change:

[**248866**] The new certificate "Entrust Root Certification Authority - G2" has been added to the certificate store. It can be used in place of the current certificate "Entrust.net Secure Server Certification Authority" which expires in May 2019. See also [Certificate replacement information](#) on page 5.

Versions 6.6.9.0 and higher include the following change:

While upgrading to V6.6.9.0 or higher from any earlier 6.x version or downgrading from V6.6.9.0 or higher, the current 24-hour data visible on Dashboard will be cleared and data collection for dashboard updates will start again.

Versions 6.6.5.0 and higher include the following changes:

- [**211468**] (Applies to HPE 425.) Added country support for Kenya and Rwanda.
- [**210396**] (Applies to MSM430, MSM460, MSM466, MSM466-R, and HPE 560.) A new private certificate, **wireless.hpe.internal.sha256**, has been added to the certificate store. It is signed using the sha256 algorithm which provides enhanced security. It can be used as an alternative to the current certificate **wireless.hp.internal**.
- [**180132**] A new private certificate, **Dummy RADIUS Server Certificate**, and trusted certificate authority, **Dummy RADIUS Authority**, have been added to the certificate store. They can be used in place of the current certificates, **Dummy Server Certificate** and **Dummy Authority**, which expire in 2017.

Versions 6.6.4.0 and higher include the following change:

[**192798**] Software for radio 1 on the HPE 560 (FCCID: RTP-MRLBB1303) has been enhanced to comply with new FCC requirements that go into effect in the United States on June 1, 2016.

Versions 6.5.0.0 and higher include the following change:

[**153332, 155783**] The MSM software has been updated to support the new ETSI (European Telecommunications Standards Institute) EN 300 328 V1.8.1 and EN 301 893 V1.7.1 requirements.

Fixes

NOTE: The number that precedes the issue description is used for tracking purposes.

Version 6.6.9.1

The following fixes are included in release 6.6.9.1:

[**249136**] (Applies to HP 560 radio 1 having channel width configured as 20 MHz.) Fixed an issue in which wireless clients were sometimes not able to get network access. (Apple MacBook clients were particularly sensitive to this issue.)

[**249098, 249601**] (Applies to a wireless client trying to connect with different access-controlled VSCs (configured for 802.1X authentication) using different usernames.) Fixed an issue in which the controller would sometimes stop providing network access to the wireless client.

[**246219, 248530**] (Applies only to the MSM317 on a heavily-loaded network from which it receives traffic from more than 500 devices.) Fixed an issue in which AP CPU utilization was unnecessarily high, resulting in loss of connection with controller.

Version 6.6.9.0

The following fixes were included in release 6.6.9.0:

[**246831, 247814**] (Applies only to HPE 517.) Fixed an issue in which an HPE 517 could reboot occasionally while handling client data traffic.

[**246084, 247480**] (Applies to the MSM410, HPE 425, HPE 560, MSM430, MSM460, MSM466, MSM466-R.) Fixed an issue in which an AP configured as Local Mesh master with LLDP agent enabled, could sometimes reboot if there were more than 6 Local Mesh links established with other APs.

[**246042**] (Applies only to the MSM720 with a nondefault access network configured.) Fixed an issue in which the AP discovery port information was incorrectly displayed on the AP Overview page.

[**245679, 247068, 245781**] (Applies to all controllers and access points.) Fixed an issue in which outdated information was displayed in the Web UI when the controller was up for 248 days or more.

[**245648, 247735**] (Applies to HPE 425, HPE 560, MSM410, MSM430, MSM460, MSM466, MSM466-R.) Fixed an issue in which under heavy traffic load, an AP would sometimes stop providing network connectivity to the associated wireless clients. An access point restart was required to recover.

[**245520, 247656**] (Applies to all controllers.) Fixed an issue in which a controller could occasionally reboot due to mishandled IP fragments.

[**244915, 245640**] (Applies to all teamed controllers.) Fixed an issue related to when a wireless client roamed from an AP connected to a team manager to an AP connected to the team member, the client did not receive an IP address.

[**244255, 245137**] (Applies to all controllers.) Fixed an issue in which a controller could occasionally reboot due to critical resource exhaustion caused by improper handling of a faulty process.

[**241688, 244141**] (Applies to all controllers.) Improved CPU utilization on MSM controllers related to collecting data for dashboard updates.

[**240712, 245151**] (Applies to all controllers.) Fixed an issue in which an SNMP walk operation on COLUBRIS-DEVICE-EVENT-MIB resulted in high CPU utilization on the controller, possibly impacting its performance.

[**155676**] (Applies only to the HPE 560.) Fixed an issue in which sFlow was supported on only radio 2.

[**150193, 243350**] (Applies to both Simplified and Advanced UI.) Fixed an issue in which the wireless throughput data displayed on the Access Point Utilization page inappropriately included traffic from access point radios operating in monitor or sensor mode.

Version 6.6.8.2

The following fixes were included in release 6.6.8.2:

Miscellaneous

[**240711, 243371**] (Applies to HP 517, HP 560, MSM410, MSM425, MSM430, MSM460, MSM466, MSM466R, and MSM 7xx Controllers.) Fixed an issue that was preventing video streaming between devices using IP fragmentation.

[**240665, 243351**] (Applies to all controllers.) Fixed an issue in which, after upgrading from version 6.6.0.0 or above, a team of MSM controllers failed to form due to an invalid egress vlan mapping which was retained after modifying an access controlled VSC to become non-access controlled.

Performance

[**241688, 244392**] (Applies to all controllers.) Improved CPU utilization on MSM controllers related to collecting data for dashboard updates.

Wireless connectivity

[**244143**] (Applies to HP 425, HP 560, MSM410, MSM430, MSM460, MSM466, MSM466-R.) Fixed an issue in which an access point would stop providing services for 30 minutes after detecting radar twice within one minute.

[**241627, 243391**] (Applies to HP 425, MSM410, MSM430, MSM460, MSM466, MSM466-R.) Fixed an issue in which the access point would sometimes stop providing network connectivity to the associated wireless clients. An access point restart was required to recover.

[**236516, 243352**] (Applies to HP 560 radio 1 with multiple VSC bindings.) Fixed an issue in which radio 1 would sometimes stop servicing wireless clients if a new VSC binding was added under an AP group which already had at least one other active VSC binding on the same radio. An access point restart was required to recover.

Version 6.6.8.1

The following fixes were included in release 6.6.8.1:

Wireless connectivity

[**237060**] (Applies only to HP 560 radio 1.) Fixed an issue in which radio 1 on the HP 560 was sometimes unable to provide wireless services until the AP was restarted.

[**233814**] (Applies to HP 425, MSM410, MSM430, MSM460, MSM466, MSM466-R.) Fixed an issue in which an AP would sometimes switch to a new channel, indicating in the logs that it was caused by radar detection in spite of no radar being detected.

Version 6.6.8.0

The following fixes were included in release 6.6.8.0:

Access points

[**232789, 235608**] (Applies to MSM430, MSM460, MSM466, MSM466-R and HP 560 in controlled mode) Fixed an issue in which an access point provisioned with a default gateway lost external network access when wireless clients sent a high volume of traffic.

[**228503**] (Applies only to access points) Fixed an issue in which some wireless clients were not able to associate with an access point, while coming out of power save mode, until the access point was restarted.

Authentication

[**138791**] (Applies to MSM317 and HP 517) Fixed an issue in which, for a VSC with both MAC and 802.1X authentication enabled, a successfully MAC-authenticated wired client was forcibly disassociated every 4 minutes, causing re-association and re-authentication each time.

Controller teaming

[**234571**] (Applies to all controllers) Fixed an issue in which a team of MSM controllers would fail to form when none of LAN port, Internet port, or VPN were selected under **Active Interfaces** on the page **Management > Management tool**. (On the MSM720 controller, these three interfaces are named: Access network, Internet Network, and VPN.)

[**227229, 229232**] (Applies only to MSM760, MSM765 and MSM775) Fixed an issue in which the system information file was incompletely saved from a team manager for a team of more than three controllers having large number of wireless access points and associated wireless clients.

Miscellaneous

[**234677**] (Applies to all controllers) Made additional fixes to issue 214044 from 6.6.5.0 to cover errors found with events, alarms, and status/statistics for synchronized access points upon reaching an uptime of 248 days.

[**233084**] (Applies to all controllers) Fixed an issue in which a CLI session was terminated when executing the command **show wireless clients**.

Performance

[**230031**] (Applies to all controllers) Fixed an issue in which, on a controller with many APs and wireless clients, CPU utilization was unnecessarily high (possibly impacting performance).

SNMP

[**234533, 235555**] (Applies to all controllers) Fixed an issue in which an SNMP walk command returned MIB object information for an access point even if the access point had been previously deleted.

User accounts

[**228258**] (Applies to all controllers) Fixed an issue in which, after restarting the controller, some user accounts were deleted before the end of their validity period. This issue also occurred for user accounts created with the Guest Management Software.

Web interface

[**232513**] (Applies to the Simplified UI) Fixed an issue in which the controller was always using the HPE default SSL certificate (**wireless.hp.internal**) instead of using the one configured for **Web Management Tool** service under **Views > Software Settings > Certificates > Usage**.

Version 6.6.7.1

The following fix was included in release 6.6.7.1:

Radio features and configuration

[**230960**] (Applies only to access points with RRM disabled.) Fixed an issue in which access points had a high probability of selecting the first available channel upon radar detection (DFS) instead of randomly selecting a channel from the available channel list. As a result, multiple access points ended up operating on the same channel, impacting the performance of that channel.

Version 6.6.7.0

The following fixes were included in release 6.6.7.0:

Authentication

[**224506**] Fixed an issue in which, for a VSC with both MAC and 802.1x authentication enabled, a successfully MAC authenticated wireless client was forcibly disassociated every few minutes, causing re-association and re-authentication each time.

[**209144**] Fixed an issue in which unnecessary authentication requests were generated by a switch to which MSM APs were connected when a wireless client was roaming to a new AP. This authentication was triggered by LLC packets sent outside the client data tunnel when MTM was enabled, even if no local network was defined under **Configuration > Local networks**.

CLI

[**228768**] (Applies to MSM760, MSM765, and MSM775.) Fixed an issue in which, upon disabling SSH access to the CLI, serial access would also get disabled and serial port speed changed to 115200.

Controller teaming

[**227531**] Fixed an apparent issue with team members losing communication, by updating the help to clarify the only valid teaming configuration with which data rate limiting can be enabled.

[**148260**] Fixed an issue in which a timeout could occur while attempting to save system information from a team manager that had joined an Active Directory Domain Server.

Local mesh

[**216014**] Fixed an issue in which, in a local mesh topology, remote access points were not visible in the LLDP status page on the master and the LLDP PDUs received count was no longer incremented.

Miscellaneous

[**227779**] Fixed an issue in which MIB object information for a few of the synchronized access points was missing in the SNMP walk command output.

[**222097**] Fixed the user tracking feature to support clients connected to a VSC with an egress VLAN mapped to the LAN port.

Performance

[**201534**] (Applies to MSM310, MSM317, MSM320 and MSM422.) Fixed an issue in which, in environments with very high station movement (association and disassociation), AP performance would gradually decrease over time and the AP would eventually reboot.

Radio features and configuration

[**223273**] Fixed an issue in which an RRM baseline could not be applied due to invalid radio quality metrics found in that baseline.

[**222199**] (Applies to MSM410.) Enabled the 5 GHz band (wireless modes 802.11a and 802.11n/a) for United Arab Emirates.

RADIUS

[**146640**] Added missing RADIUS attribute "Acct-Terminate-Cause" in accounting STOP requests for clients connected to a non-access controlled VSC with 802.1x authentication.

SNMP

[**229072**] (Applies only to access points.) Fixed an issue in which an SNMP GET query for MIB object **dot1dBaseBridgeAddress** defined in **BRIDGE-MIB** was wrongly returning the MAC address of the root bridge instead of the MAC address of the AP itself.

[**216828**] Fixed an issue in which a repetitive SNMP walk on a team of MSM controllers could eventually fail, when retrieving data for an AP connected to a team member (other than the team manager)

[**214321**] Fixed an issue in which a controller could sometimes return `no such instance` for some SNMP OIDs such as **ifOperStatus**, when receiving a large number of requests from an SNMP client. Messages similar to this were logged:

```
debug monitor: Stopping [939,8]: 'snmpd -Lsd -f -c /ram/snmpd.conf -x /var/net-snmpp/agentx/master 161' [pid 4286, up for 400 sec(s)]
```

```
debug monitor: Starting [940,3]: 'snmpd -Lsd -f -c /ram/snmpd.conf -x /var/net-snmpp/agentx/master 161' (pid='6439')
```

Synchronization and discovery

[**227967**] Fixed an issue in which, after a controller had been running for a period ranging from days to weeks, all APs synchronized with this controller would disconnect and then reconnect to the same controller or to another controller in the team. This may have caused temporary connectivity problems for the wireless clients and could also have exposed misconfiguration of AP provisioning.

Upgrades

[**225501**] Fixed an issue in which the controller could reboot every 30 minutes after an upgrade from an older version where RIP was configurable and had been enabled. Messages similar to this were logged:

```
debug monitor: Stopping [292,8]: 'zebra -P 0 -f /flash/etc/zebra.conf' [pid 31218, up for 7 sec(s)]
```

[**225225**] Fixed an issue in which a team of controllers failed to form after upgrading from version 6.3.X.X with an invalid switch port tagging configuration. This invalid configuration was not possible with the Web interface, only via SOAP calls.

Web interface

[**221729**] (Applies to Simplified UI.) Fixed an issue in which an access-controlled VSC's egress VLAN, configured using the advanced UI, was getting cleared when the VSC (WLAN) was further modified in the simplified UI.

Version 6.6.5.0

The following fixes were included in release 6.6.5.0:

Access points

[**217063**] (Applies to Autonomous APs - HP 425, HP 560, MSM410, MSM430, MSM460, MSM466, MSM466-R) Fixed an issue in which the object **coDot11MulticastReceivedFrameCount** in the table **coDot11CountersTable** in the **MIB COLUBRIS-IEEE802DOT11.my** returned an incorrect value.

Authentication

[**216389**] Fixed an issue in which a wireless client failed to be authenticated when switching between two VSCs on the same AP that were configured with different EAP authentication methods. For example, when a client disconnected from a VSC configured to use EAP-PEAP and then connected to another VSC configured to use EAP-LEAP.

[**211548, 216761**] Fixed an issue in which a wireless client failed to be authenticated when connected to a VSC configured to support both local and remote MAC authentication.

[**207190, 210854**] Fixed an issue in which re-authentication sometimes failed when local MAC authentication was configured on a VSC. The following error message was seen in the system log:

```
crit iprulesmgr: assert: iprulesmgr.c AuthenticateIPRulesMgrMACStation 9604 ((radiusProfileIndex - 1) >= 0 && (radiusProfileIndex - 1) < MAX_RADIUS_PROFILES).
```

[**131693**] (Applies to MSM410, HP 425, MSM430, MSM460, MSM466, and MSM466-R.) Fixed an issue in which iPads, iPods, and iPhones were not able to authenticate using the secondary RADIUS server with the default configuration.

Miscellaneous

[**214044**] Fixed an issue on the Discovered APs page in which radio icons were dimmed, and status and statistics information was not updated, for synchronized APs with almost 248 days of uptime.

[**211749, 217265**] Fixed an issue in which a wireless client was sometimes given an incorrect IP address after re-associating with an AP, because the client was assigned to the wrong VLAN.

[**155118**] (Applies to HP 560.) Fixed an issue in which the QoS counters for radio 1 were not incremented on the **Status > Wireless** page.

Performance

[**210924**] (Applies to MSM422) Fixed an issue in which the transmit power occasionally dropped to a very low level. (Release 6.6.4.0 included a fix for this issue. The fix in this release covers more cases and prevents the issue from occurring.)

Radio features and configuration

[**178131**] (Applies to HP 517.) Fixed an issue in which wireless clients connected to different VSCs on the same AP were able to communicate even though the VSCs had the **Allow traffic between clients** option set to **no**.

SNMP

[**210278, 211873**] Fixed an issue in which SNMP failed to retrieve certain MIB OIDs.

Synchronization and discovery

[**201356**] Fixed an issue in which the controller detected APs on a VLAN for which device discovery was disabled.

Version 6.6.4.0

The following fixes were included in release 6.6.4.0:

Access points

[**199405**] (Applies to MSM430, MSM460, MSM466, MSM466-R, and HP 560.) Fixed an issue in which, when an AP previously used with a Unified controller was converted for use with an MSM controller, the message **err kernel ecc unrecoverable error** was displayed in the system log, even though the AP was functioning properly.

[**197061**] (Applies to MSM430, MSM460, MSM466, MSM466-R and HP 560) Fixed an issue in which, when an AP was running MSM software version 6.6.0 to 6.6.3, it was not able to convert to HP Unified mode and connect to a Unified controller.

Authentication

[**193514, 182944**] (Applies to non access-controlled VSCs that are using 802.1X or MAC-based authentication.) Fixed an issue in which, when a VSC was configured to support authentication and accounting on different RADIUS servers, if the accounting server was unreachable, wireless clients were not able to connect to the VSC and authenticate for the amount of time configured for **Retry timeout** under the RADIUS profile used for accounting.

[**192622**] Fixed an issue in which, when Opportunistic Key Caching was enabled and the controller was used for 802.1X authentication, a warning message similar to the following may have been logged when a client roamed from one AP to another:

iprulesmgr: Discarding RADIUS Accounting Request (id='111') from RADIUS Client (ip-address='169.254.0.5',port='33919') because of missing username. (Check your RADIUS Secret configuration.)

The message repeated every 10 seconds, but client connectivity and traffic was not impacted. The message stopped being logged when the client roamed back to the original AP, or the AP was rebooted.

Controller teaming

[**197524**] Fixed an issue in which wireless clients were disconnected or dropped when a large controller team with many APs was handling a heavy traffic load. For example, a team with five controllers and 800 APs handling 2000 wireless client stations.

[**190902**] Fixed an issue in which, when a controller team was handling a heavy traffic load, a controller sometimes stopped transmitting on one of its network ports.

[**184019**] Fixed an issue in which, when an AP was initially discovered on a team member and then moved from one AP group to another group, the team member reported a validation error when synchronizing the AP, then reset itself to factory defaults and took 15 minutes to resynchronize with the team manager.

[**183563**] Fixed an issue in which, when a controller team was upgraded to version 6.6.x.x from any earlier release, team synchronization failed if a VSC configured with WPA (TKIP) wireless protection was bound to an AP radio which was configured to only allow 802.11n and/or 802.11ac wireless clients.

[**179997**] (Applies to access-controlled VSCs) Fixed an issue in which, when a wireless client roamed from an AP connected to a team member to an AP connected to the team manager, it was not authorized and did not receive an IP address.

Documentation / online help

[**200360**] (Applies to MSM720.) The following note has been added to the online help and the *MSM7xx Controllers Configuration Guide* in the section **About the default network profiles**: To avoid connectivity issues on the MSM720, do not configure the Internet network profile with an IP address on the subnet 192.168.1.0/24.

[**199401**] The following note has been added to the online help and the *MSM7xx Controllers Configuration Guide* in the section **Configuring a RADIUS server profile**: After editing a RADIUS server profile, it is recommended that you restart all APs that are bound to the VSC that is using the edited profile.

Miscellaneous

[**201223**] Fixed an issue in which, when running a trace on any network interface on a controller (using **Tools > Network Trace**), if the trace ended with the message **Trace too big, trace stopped**, any subsequent traces on controlled AP interfaces also failed to capture packets.

[**191150**] (Applies to MSM430, MSM460, MSM466, and MSM466-R.) Fixed an issue in which an AP was not synchronizing with a controller after it was upgraded from 5.7.x.x to 6.6.x.x, downgraded back to 5.7.x.x, and then upgraded again to 6.6.x.x.

RADIUS

[**138664**] Fixed an issue in which, when a VSC was configured for non-access controlled MAC-based authentication and was using a RADIUS server for accounting, the following counters were missing from the accounting stop packets:

- Acct-Input-Packets
- Acct-Output-Packets
- Acct-Input-Octets
- Acct-Output-Octets

Wireless connectivity

[**190800**] (Applies to HP 560.) Fixed an issue in which, when radio 1 was configured to operate on channels 36-64, some wireless clients experienced poor performance and kept disconnecting from the AP.

[**183583**] Fixed an issue in which, when a controller was configured with many VLANs, wired client stations might not receive an IP address when connecting to an AP. This issue occurred when an AP discovered a controller on a certain VLAN, and then reconnected on the default VLAN after being restarted or losing the connection to the controller.

Version 6.6.3.0

The following fixes were included in release 6.6.3.0:

Authentication

[**174692**] Fixed an issue in which wireless clients were unable to authenticate when connected to a VSC configured to use the controller for authentication, when the controller was configured to act as a RADIUS proxy. If the **Always try primary server first** option was enabled, and the primary RADIUS server was down or inaccessible, the controller did not reissue the authentication request to the secondary RADIUS server.

Controller teaming

[**190569**] Fixed an issue in which synchronization of team members failed after editing or deleting a VSC that had user accounts referencing the VSC (in the **Restrict this account to these VSCs** field). Synchronization also failed when the controller software was updated.

[**183761**] Fixed an issue in which synchronization of team members took a long time after changes were made to a VSC profile.

[**161693**] Fixed an issue in which the RADIUS profile setting **Override NAS ID when acting as a RADIUS proxy** was not properly synchronized on team members.

Miscellaneous

[**182212**] Fixed an issue in which a controller could occasionally restart when handling a heavy load of MTM traffic.

[**177758**] (Applies to the HP 560 only.) Fixed an issue that caused the HP 560 to intermittently reboot when receiving frames larger than the Ethernet MTU.

[**170865**] Fixed an issue in which, when a user was connected to a VSC with a VSC egress mapping configured, the egress VLAN ID value for the user was displayed as 0, instead of the VLAN value configured for the network profile.

Performance

[**175921**] Fixed an issue in which wireless clients experienced delays or timeouts connecting to secure web sites via HTTPS when the controller was configured as an HTTP proxy.

Ports and interfaces

[**178161**] (Applies to the MSM720 controller only.) Fixed an issue in which if port trunking was configured, and the controller was restarted, a temporary network loop (lasting several seconds) was present until the port trunk configuration was applied.

Radio features and configuration

[**183562**] (Applies to HP 425, HP 517, and HP 560.) Fixed an issue in which changes made to radio settings for these APs in the controlled APs base group were not inherited by AP groups that were created before the introduction of these APs.

SNMP

[**184023**] (Applies to MSM720.) Fixed an issue in which SNMP traps were not sent for Ethernet port Up/Down events.

Web interface

[**190847**] (Applies to the Simplified UI.) Fixed an issue in which the dashboard failed to display historical data when the time zone configured on the controller ended with **:30**.

Wireless connectivity

[**179867**] (Applies to dual-radio APs.) Fixed an issue that resulted in wireless clients losing network connectivity when roaming between radios on an AP with many active wireless clients. (Apple MacBook clients were particularly sensitive to this issue.)

Version 6.6.2.0

The following fixes were included in release 6.6.2.0:

Authentication

[**171524, 172352**] (Applies to all supported APs.) Fixed an issue in which, on some wireless clients, 802.1X authentication might take several seconds to complete.

[**169813**] (Applies to Active Directory.) Fixed an issue where if you attempted to use a single quote character (') in an Active Directory group name, the controller displayed a blank error message (banner across the top of the page).

[**162454, 172726**] (Applies to MSM422 radio 1 with any encryption set (WPA2, WPA, WEP).) Fixed an issue in which wireless clients with a MAC address with the first digit equal to 0x8 or higher force the clients to always use software encryption, causing high CPU utilization on the AP and possible AP reboot.

CLI

[**159942, 174968**] Fixed an issue in which during an SSH session, CLI command `disassociate controlled-ap wireless client` sometimes failed to work properly, resulting in the client not being disassociated and the SSH session being prematurely terminated.

Controller teaming

[**176861**] Fixed an issue in which a controller team failed to form after upgrading from a version older than 6.5.0.0, when using the following configuration for a radio:

- Channel exclusion list preventing the use of any 40 MHz wide channel.
- Channel width set to auto.
- Short guard interval.

[**173386, 173622**] Fixed an issue in which, if a remote syslog server was configured with a name longer than 25 characters, team synchronization would not complete successfully.

[**171643, 172703**] Fixed an issue in which RADIUS communications might be adversely affected because the 802.1X Called-station-id values were not properly synchronized with all team member controllers when a configuration change was made.

[**169843**] Fixed an issue in which controller serial port settings configured on a team manager controller were not propagated to team member controllers.

[**169836, 173372**] Fixed an issue in which, if any controller in a team failed to provide system information, an error was logged, and no system information was returned for any of the controllers in the team.

[**168815, 172365**] (Applies to the MSM317 and HP 517 with **Send Network Policy TLV** enabled on their switch ports.) Fixed an issue in which controller teams failed to synchronize if the primary VLAN IDs of the AP switch ports were the same as the VLAN ID configured in the LLDP profile.

[**149596, 151901**] Fixed an issue in which, if the team manager failed, the interim team manager would enable RRM severe interference mitigation and AP load balancing, even if these options were disabled by the administrator.

DHCP

[**170785, 174245**] Fixed an issue in which, whenever a wireless client roamed from one AP to another using MAC Authentication, the client session was terminated and did not restart until the client issued a new DHCP request.

IDS (Intrusion Detection System)

[**131182**] Fixed an issue in which re-deploying an AP from one controller to another controller generated false attacks reported by IDS on the original controller.

IMC (Intelligent Management Center)

[**172388**] Fixed an issue in which IMC triggered log messages similar to the following. These log messages no longer appear.

```
2015... [ERROR (0)] [THREAD(1636)] [CWlanHPDevAccessor::convertErrorCode]
(Error)Device return error msg:
```

```

2015... [ERROR (0)] [THREAD(1636)] [CWlanHPDevAccessor::convertErrorCode]
(Error)Device return error code:8

2015... [INFO (0)] [THREAD(1636)] [CWlanHPDevAccessor::convertErrorCode]
(Info)Dev return error.

2015... [INFO (0)] [THREAD(1636)] [CWlanHPDevAccessor::convertErrorCode]
(Info)responses {

op_id: 1

opControlledNetworkGetNeighborhoodScanningSettings {

    error {

        errorCode: COMMAND_NOT_SUPPORTED

        errorMessage: ""

        errorLevel: FATAL

```

[**157935**] Fixed an issue in which a controller would not communicate with an IMC server when the IMC server was identified with a FQDN (fully-qualified domain name).

Local mesh

[**174365**] Fixed an issue on the local mesh profile page where duplicate nodes might be displayed for radios not operating in local mesh mode.

[**168569**] (Applies to autonomous-mode APs with auto channel.) Fixed an issue in which a slave AP in a local mesh configuration might transmit incorrect channel information in the beacon when using auto channel. When this occurred, client devices could not associate with the slave AP.

[**130021**] (Applies to MSM410, MSM430, MSM460, MSM466, and MSM466-R in controlled and autonomous mode, and the HP 425 in controlled mode.) Fixed an issue where a Dynamic Local Mesh Slave configured in Promiscuous Mode will not establish a link even in the presence of multiple Masters.

Logging

[**153280**] (Applies to HP 560.) Fixed an issue in which, when **Protected Management Frames (802.11w)** were enabled on an AP, invalid management frames were dropped as required by the 802.11w standard, but log messages were not generated to indicate that this had occurred.

Miscellaneous

[**173309, 178218**] (Applicable to MSM4xx and HP 560) Fixed an issue related to the OBSS (Overlapping BSS) that can result in connectivity issues for some older wireless client devices operating in the 2.4 GHz band. The OBSS IE is no longer included in the beacon unless the AP is operating in 802.11b/g/n in Auto 20/40.

[**173065, 180885**] (Applies to HP 425, MSM410, MSM430, MSM460, MSM466, MSM466-R.) Fixed an issue where, under certain conditions, an AP could sometimes restart when changing channels.

[**158997, 169509**] Fixed an issue in which, if a controller was configured as an access gateway rather than an AP controller, and the number of user connections exceeded 500, users would be disconnected with **host not found** messages displayed in their browsers.

[**126170**] (Applies to all controllers.) Fixed an issue in which APs that were flagged as Admin Down were not excluded when determining whether an RRM analysis could be run.

Ports and interfaces

[**175833**] Fixed an issue in which the MSM controller firewall was not blocking incoming DNS requests on the Internet port.

Radio features and configuration

[**169632**] (Applies to MSM422 in controlled mode.) Fixed an issue in which, moving an AP configured for a non-802.11n radio mode into a group to which a WEP-enabled VSC is bound, falsely triggered an error similar to the following:

```
Invalid AP configuration: VSC x is configured with WEP security and a radio is configured for 802.11n
```

RADIUS

[**169808**] Fixed an issue in which public access attributes (defined on the **Controller >> Public access > Attributes** page) did not support inclusion of the double quote character (") and the right-angle bracket (>) (in this order) anywhere within the same attribute, regardless of whether there are intervening characters between the double quote and the right-angle bracket. Attribute definitions containing these two characters (in this order) did not function properly and were displayed incorrectly.

[**168716**] Fixed an issue in which, as indicated in the documentation, RADIUS accounting is not supported when WPA opportunistic key caching is enabled. However, the user interface did not prevent these two options from being activated at the same time. The symptom of this unsupported configuration attempt was client devices appearing as "N/A" in the client name list.

[**162460, 173302**] Fixed an issue in which, under certain circumstances, RADIUS accounting packets might have contained incorrect information. This might have occurred when an initial authentication was terminated abnormally and a subsequent authentication by the client device completed successfully.

SNMP

[**127299**] Fixed an issue in which the SNMP OIDs that report information about the configuration of the Autochannel feature `COLUBRIS-DEVICE-WIRELESS-MIB coDevWirIfStaAutoChannelEnabled` and `coDevWirIfStaAutoChannelInterval` may have reported incorrect information.

SOAP

[**172362, 173104**] Fixed an issue in which the SOAP command `UpdateLEDsOperatingMode` was not functional.

Synchronization and discovery

[**172302**] (Applies to all controllers for AP provisioning with controller-based provisioning settings.) Fixed an issue in which AP discovery could fail when entering "names to search for" to discover APs using DNS.

Upgrades

[**177203, 181304**] (Applies to HP 560) Fixed an issue in which, if certain data rates were disabled on radio 1 of the HP 560, the AP would sometimes reboot unexpectedly.

VSC (virtual service community)

[**174058, 176390**] (Applies to DHCP relay on the non-default port 68.) Fixed an issue in which, when a client moved between two 802.1X access controlled VSCs, the user session would show the IP address of the previous session and the client could not reach the gateway. This did not occur on the default port 67.

[**173721**, **181425**] Fixed an issue in which a message similar to the following might have been logged for the AP if the first VSC in an AP group was deleted from the group: AP is not associated with any VSC

[**171654**, **172282**] Fixed an issue in which, when a VSC is configured for 802.1X authentication using an external RADIUS server, the RADIUS Accounting STOP packets sent to the RADIUS server were missing the Acct-Session-ID.

Web interface

[**172189**] Fixed an issue in which, when upgrading from software version 6.4.x (or earlier) to version 6.6.x, the **Controlled APs** and the **Wireless clients** tables might not display properly due to web browser cache content.

Wireless connectivity

[**172677**, **176492**] (Applies to MSM422.) Fixed an issue in which the AP radio signal power level would decrease so much that the wireless client had to be in very close proximity to the AP to remain connected.

[**110393**] Fixed an issue in which Windows 7 wireless clients using WPA2 and a session timeout would be disconnected during the key exchange after re-authentication.

Version 6.6.0.0

The following fixes were included in release 6.6.0.0:

CLI

[**161583**, **162366**] (Applies to MSM760.) Fixed an issue in which the **Serial** port access section in the management tool under **Controller >> Management > CLI** was not displayed. Note that you could still log in to the controller and access the CLI using the serial port.

Controller teaming

[**162994**, **169518**] Fixed an issue in which wireless users authenticated by Active Directory could be restricted to a VSC subset according to the Active Directory group in which they belonged. If such wireless users were connected through an AP that was managed by a team member controller, the users were not properly restricted to the VSC subset.

[**162373**] Fixed an issue in which, when the team manager went down, the alarm (`ALARM_CS_CONTROLLER_DOWN`, ID39) was not shown on the team member controller that took over for the former team manager controller.

[**158228**] Fixed an issue in which, if an SNMPv3 user was configured in an SNMP Trap receiver on the team member controller, and the SNMPv3 user account was then deleted from the team manager controller, after a software upgrade, the team member controller could get stuck in a loop resetting and downloading a configuration.

[**151409**, **168447**] Fixed an issue in which, after a team was formed and working properly, changing the regulatory domain to some countries caused team synchronization failures to occur after an upgrade from 5.3.x.x to 5.7.x.x, followed by an upgrade to 6.0.x.x.

IDS (Intrusion Detection System)

[**166610**, **168110**] Fixed an issue in which IDS reported false positive “honeypot/evil twin AP IDS” alarms in the following two scenarios:

- When IDS was not enabled and the user imported an IDS csv file that manually authorized APs, the problem occurred upon IDS enable.
- When a Controlled AP radio MAC address was missing in the configuration file of a team manager controller (which could occur when some APs were discovered by the team member controller).

[**160516**] (Applies to HP 560.) Fixed an issue in which, when used as an IDS sensor, radio 1 could not detect ad-hoc cells and update misassociated client station and ad-hoc cells pages.

IMC (Intelligent Management Center)

[**137197**] When IMC establishes a connection to the MSM7xx Controller, the following error messages are displayed on the system log. These messages can be safely ignored.

```
err pmmclient: setVLANSubsectionIndexFromVLANNetworkProfileName: Unknown vlan name 'Internet port network'.
```

```
err pmmclient: setVLANSubsectionIndexFromVLANNetworkProfileName: Unknown vlan name 'LAN port network'.
```

```
err pmmclient: DB: Unable to prepare the SQL statement.
```

```
err pmmclient: Could not get data from the database.
```

Local mesh

[**166401, 169412**] (Applies to autonomous APs with dynamic local mesh links.) Fixed an issue in which a VLAN created and mapped to a dynamic wireless mesh link, with the IP address mapped to that link, although correctly configured (and existing), was not listed in the interface list (**Network > IP Interface** page).

[**163761**] (Applies to HP 560 APs configured with 802.11ac, 80 MHz channel width, with local mesh on radio 1; and radio 2 of the slave AP configured with 802.11n/b/g, 20 MHz channel width, access point only.) Fixed an issue in which, in this configuration, clients were unable to connect to the slave AP (radio 2) VSC.

Logging

[**157808, 167620**] Fixed an issue in which excess system log messages similar to the following were appearing:

```
Aug 21 12:27:54.738 warn A0:48:1C:56:7D:A7
```

```
kernel:hp_ieee80211_rrm_probereq_allow_send: Radio table is full, respond to probe request
```

[**153466**] Fixed an issue in which unneeded warning messages appeared in the system log when an AP was configured to use channel 11 or 13, and the AP was changed from n/b/g 20 MHz channel width to 40 MHz channel width.

Miscellaneous

[**170640**] (Applies to MSM7xx Controllers.) Fixed an internal issue related to the apparent exposure of a database-related port (TCP port 5432) that could falsely lead to a PCI compliance audit failure.

[**159609, 161063**] (Applies to HP 425, MSM430, MSM460, MSM466, and HP 517.) Fixed an issue in which the survivability feature did not work after an AP reboot. An AP that had synchronized to a controller continued to work even if the controller went down. However, if the AP rebooted and the controller continued to stay down, clients that were connected before and should have been able to re-connect, could not.

MTM (Mobility Traffic Manager)

[**153105, 163787**] (Applies to VSCs with Opportunistic Key caching and MTM enabled.) Fixed an issue that caused roaming clients to end up on a VLAN different than the one assigned by the RADIUS server.

[**147065**, **167617**] Fixed an issue in which broadcast and multicast traffic was blocked between MTM clients.

Performance

[**152755**, **152753**] (Applies to MSM310, MSM317, MSM320, MSM325, and MSM422.) Improved RRM performance for these APs and eliminated related connectivity loss and a possible grayed out antenna that could occur when CPU utilization reached 100%.

Public access interface

[**160318**] Fixed an issue in which the use of a domain name or IP address in the wrong format as part of a DNAT rule parameter, caused the controller to reboot.

Radio features and configuration

[**167467**, **168669**] (Applies to RRM with DFS channels (5 GHz).) Fixed an issue in which, when an AP was operating on a DFS channel under high RF interference and a new plan was applied, the radio would go to the planned channel but, due to the high interference, might have requested another channel. If the channel assigned was different from the plan, wireless client connection was no longer allowed on the 5 GHz radio.

[**166184**, **171400**] (Applies to 802.11b/g radio modes.) Fixed an issue in which, when **Local Auto-Channel** with **Interval** was configured, APs might not have accepted wireless connections.

[**131154**] (Applies to MSM410, MSM430, MSM460, MSM466, and MSM466-R in autonomous mode.) Fixed an issue in which, after a reboot or a modification of the radio configuration, some error messages might have been generated by `rfmgr_ap`. These messages did not indicate a malfunction and could be ignored. The services offered by the radio worked properly.

[**128028**] (Applies to MSM320 and MSM325 in autonomous mode.) Fixed an issue in which, after upgrading to firmware 6.0, MSM320 and MSM325 sensors working in autonomous mode might have presented GUI instability when a radio or radios were setup to work in Network Detector mode.

RADIUS

[**162146**, **169531**] Fixed an issue in which, when there was heavy RADIUS traffic load (authentication and accounting) going through the controller, the controller might have experienced higher than usual CPU utilization, and performance sluggishness might have been experienced.

Regional specifics

[**159549**] (Applies to HP 425.) Fixed an issue in which, although the management tool allowed countries **Sri Lanka** or **Papua New Guinea** to be selected, these countries should not have been selected because they were not supported by the AP.

Routing

[**160371**, **172300**] Fixed an issue in which, on occasion, a client device would lose connectivity by getting assigned an IP address on the wrong subnet (due to incorrect egress from a controller), making it necessary to reassociate or reconnect.

SNMP

[**160932**, **167623**] Fixed an issue in which these two SNMP trap descriptions displayed in the web management tool were not fully descriptive: **AP Rebooting should be AP rebooting due to config changes** **AP not responding should be AP cannot complete discovery in time**

Synchronization and discovery

[**167266, 169497**] Fixed an issue in which, when configuring static IP addresses in provisioning mode (**AP > Provisioning** with **Static** under **Assign IP address Via**), upon AP restart, it could not be synchronized by the controller. Symptoms included display of the message `resetting AP` and all LEDs blinked simultaneously.

VSC (virtual service community)

[**159792, 171987**] (Applies to HP 517, MSM460, MSM466, and MSM466-R in controlled mode.) Fixed an issue in which APs being synchronized might have gotten stuck in the **Uploading** configuration state.

[**159082**] Fixed an issue in which some clients might not have been able to connect to a particular wireless network if the VSC had both **Protected Management Frames** (802.11w) and **Terminate WPA at the Controller** enabled. These were mutually exclusive options, even though the V6.6.x.x software did not enforce mutual exclusivity.

VPN

[**129915**] Fixed an issue in which clients using the PPTP VPN server might have experienced connectivity issues when sending large packets.

Web interface

[**159677, 171914**] Fixed an issue in which the management tool might have restarted when attempting to sort a list of user sessions by **VSC**, **Idle time**, or **VLAN**, when the list included non-Access Controlled clients.

Wireless connectivity

[**144472, 151253**] (Applies to MSM430, MSM460, MSM466, and MSM466-R.) Fixed an issue in which the AP could not send large multicast packets to wireless clients.

Issues and workarounds

NOTE: The number that precedes the issue description is used for tracking purposes.

Version 6.6.9.1

The following issues are present in release 6.6.9.1:

GMS

[**214804**] If the time and time zone settings on the controller and GMS do not match, GMS assumes that newly created user accounts are expired and automatically deletes them. To resolve this issue, adjust the time and time zone settings so that they match on the controller and GMS, and restart the controller.

IDS (Intrusion Detection System)

[**247372, 248165**] (Applies to all controllers with the Intrusion Detection System (IDS) enabled.) When there are network connectivity issues, controlled APs can occasionally be falsely marked as rogue (with a "Rogue AP active" alarm raised on the controller).

Workaround:

1. Ensure that IDS is enabled globally.
2. Export the list of all APs into a `csv` file using **Controlled APs > Security > Neighborhood > Import/Export > Export**.

3. Modify the `csv` file by copying the complete content displayed under heading "Controlled APs" and pasting it under heading "Manually authorized APs."

NOTE: It is recommended to modify the `csv` file with a compliant editor to avoid any problems later when importing the `csv` file back into the controller.

4. Save the modified `csv` file locally.
5. Disable AP discovery, restart the controller, and wait for it to come up again.
6. Upload the modified `csv` file to the controller using **Controlled APs > Security > Neighborhood > Import/Export > Import**.
7. Re-enable AP discovery.

[**140224**] (Applies to MSM410, HPE 425, MSM430, MSM460, MSM466, and MSM466-R.) When the Intrusion Detection System (IDS) is enabled, AP radios on that (team of) controllers must not be configured in **Access Point and Local Mesh** or **Local Mesh only**. As a workaround, disable IDS on the controller if the **Access Point and Local Mesh** or **Local Mesh only** operation is required.

Miscellaneous

[**149463**] sFlow is not supported on the HPE 517.

Performance

[**156546**] (Applies to HP 560.) Some Broadcom-based 802.11ac client devices experience reduced throughput performance when associated with an AP with **Protected Management Frames (802.11w)** enabled in the VSC.

Radio features and configuration

[**156664**] (Applies to HP 560.) When radio 1 is configured as an IDS sensor, special UDP packets (for rogue AP identification) are not generated and therefore, rogue detection is not possible on radio 1.

[**124010**] (Applies to MSM410, MSM430, MSM460, MSM466, and MSM466-R in autonomous mode.) The Neighborhood Scanning feature configured to scan on all channels only scans on channels within the regulatory domain's approved channel list rather than all channels in the respective band. For example, with the location set to the **United States**, **Neighborhood Scanning** will not scan channels 12 or 13 since they are not part of the U.S. regulatory domain. This is true in both the 2.4 GHz and 5 GHz bands. There is no workaround.

VLANs

[**161352, 164799**] If a VLAN is mapped to a wired port, and is also used as the management VLAN, access to an AP is lost when removing the VLAN assignment from the port. As a workaround, after removing the VLAN assignment from the port, reboot the AP to restore connectivity.

Web interface

[**169799**] The Payment URL validity check is not performed sufficiently. As a workaround, for the Payment URL, enter only characters that are valid in a URL.

Wireless connectivity

[**172357**] (Applies to the HP 560.) Some Android phones (observed on Android 4.1.2) that roam between the AP (configured for WPA2 with 802.11w (protected management frames)) and another AP that does not support 802.11w, might experience temporary connectivity problems as they roam between APs. Upgrading your phone to the latest supported Android version, might solve the problem.

SOAP function limitations for controller teaming environment

The functions discussed in this section may be of interest to developers who make use of SOAP to communicate and configure devices, especially when creating and managing user accounts on a controller. The following SOAP function calls that were not available in previous versions are re-enabled in MSM software Version 6.2.0.0 or later.

The following limitations apply to controller teams only:

- `UpdateUserAccountMaxConcurrentSession`: The user account limit is per controller instead of being applied globally to the team.
- `UpdateUserAccountValidity`: This function will return an error if subscription plans are selected to set the account validity.
- `ExecuteUserAccountLogout`: The action of logging out a user will only take effect if the user is logged in on the team manager.
- `UpdateUserAccountRemovalSettings`

NOTE: The **Removal due to invalidity** option of the `UpdateUserAccountRemovalSettings` function works in a teaming environment. However, do not use the **Removal due to inactivity** option when teaming because it could cause the controllers to wrongly remove active accounts.

Although enabled in MSM software release 6.2.0.0 or later, the following SOAP functions should not be used on a controller team. If you attempt to use any of these functions when teaming is enabled, an error is returned.

- `ExecuteBackupUserAccountsPersistentData`
- `ExecuteUserAccountRenewPlan`
- `AddSubscriptionPlan`
- `DeleteSubscriptionPlan`
- `DeleteAllSubscriptionPlans`
- `UpdateSubscriptionPlanName`
- `UpdateSubscriptionPlanOnlineTimeState`
- `UpdateSubscriptionPlanValidityPeriodState`
- `UpdateSubscriptionPlanOnlineTime`
- `UpdateSubscriptionPlanValidityPeriodMethodState`
- `UpdateSubscriptionPlanValidityPeriodFor`
- `UpdateSubscriptionPlanValidityPeriodBetween`
- `UpdateSubscriptionPlanValidityPeriodFrom`
- `UpdateSubscriptionPlanValidityPeriodUntil`
- `UpdateSubscriptionPlanBooleanAttribute`

- UpdateSubscriptionPlanIntAttribute
- UpdateSubscriptionPlanBandwidthLevelAttribute

Documentation updates and corrections

Online help

Although referenced in the online help, the MSM335 AP is not supported in release 6.4.0.0 or later.

HP MSM SNMP MIB Reference Guide

The following objects in the COLUBRIS-VIRTUAL-AP-MIB are obsolete:

- coVirtualApAuthenMode
- coVirtualApAuthenProfileIndex
- coVirtualApUserAccountingEnabled
- coVirtualApUserAccountingProfileIndex
- coVirtualApDefaultUserRateLimitationEnabled
- coVirtualApDefaultUserMaxTransmitRate
- coVirtualApDefaultUserMaxReceiveRate
- coVirtualApDefaultUserBandwidthLevel

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.

Procedure

1. Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
2. A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

To find security bulletins:

- Go to the Hewlett Packard Enterprise Support Center website at www.hpe.com/support/hpesc.
- Enter your product name or number and click **Go**.
- Select your product from the list of results.
- Click the **Top issues & solutions** tab.
- Click the **Advisories, bulletins & notices** link.

To initiate a subscription to receive future Hewlett Packard Enterprise Security Bulletin alerts via email, sign up at:

h41360.www4.hpe.com/alerts-signup.php?jumpid=hpesc_secbulletins

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/info/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 information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline 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.