

HP MSM7xx Controllers and MSM Access Points Version 6.5.3.0 Release Notes

Abstract

These release notes provide important release-related information for MSM software Version 6.5.3.0.

HP Part Number: 5998-8216
Published: July 2015
Edition: 1



© Copyright 2014, 2015 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Acknowledgments

Microsoft® and Windows® are U.S. registered trademarks of the Microsoft group of companies.

Apple®, Bonjour®, iPad®, iPhone®, and iPod® are trademarks of Apple Inc. iPod is for legal or rightholder-authorized copying only. Don't steal music.

Intel® is a trademark of Intel Corporation in the U.S. and other countries.

sFlow® is a registered trademark of InMon Corp.



Contents

MSM software V6.5.3.0.....	6
Description.....	6
Products supported.....	6
Upgrade information.....	7
Prerequisites.....	7
Mandatory channel change required prior to software upgrade; discontinue use of channel 132.....	7
Software configuration change might be required prior to upgrade.....	7
Software Updates and Licensing portal.....	7
Upgrading restrictions and guidelines.....	8
Transitioning APs from Unified controllers to use MSM software.....	8
HP 560 autonomous mode.....	8
Downgrading software.....	8
Compatibility/interoperability.....	8
SSLv3 support.....	8
MSM management tool	8
RF Manager software and MSM software version compatibility.....	9
Local mesh.....	9
GMS (Guest Management Software) for controllers.....	9
Enhancements.....	10
New AP support.....	10
802.11w support.....	10
New installation configuration wizard.....	10
RADIUS attributes for groups.....	10
Firmware load on reboot.....	10
Changes.....	10
Fixes.....	10
Version 6.5.3.0.....	10
Authentication.....	10
CLI.....	11
Controller teaming.....	11
DHCP.....	11
Miscellaneous.....	11
MTM (Mobility Traffic Manager).....	11
RADIUS.....	11
Routing / traffic flow.....	12
SOAP.....	12
Synchronization and discovery.....	12
VSC (virtual service community).....	12
Web interface.....	12
Version 6.5.2.0.....	12
Authentication.....	12
Controller teaming.....	12
DHCP.....	13
IDS (Intrusion Detection System).....	13
Local mesh.....	13
Logging.....	13
Miscellaneous.....	13
Radio features and configuration.....	13
RADIUS.....	14
SNMP.....	14

SOAP.....	14
Synchronization and discovery.....	14
VSC (virtual service community).....	14
Web management tool.....	14
Wired connectivity.....	15
Wireless connectivity.....	15
Version 6.5.1.0.....	15
Controller teaming.....	15
DHCP.....	16
Local mesh.....	16
Logging.....	16
Miscellaneous.....	16
MTM (Mobility Traffic Manager) (controllers).....	16
Radio features and configuration.....	16
Regional specifics.....	17
Routing/traffic flow.....	17
SOAP.....	17
Synchronization and discovery.....	17
Web management tool.....	17
Wired connectivity.....	17
Wireless connectivity.....	17
Version 6.5.0.1.....	18
Documentation/online help.....	18
IMC (Intelligent Management Center).....	18
Local mesh.....	18
Radio features and configuration.....	18
Regional specifics.....	18
Scheduled backups.....	18
Upgrades.....	18
Wireless connectivity.....	18
Version 6.5.0.0.....	19
Authentication.....	19
Controller teaming.....	19
DHCP.....	19
Local mesh.....	19
Performance.....	19
Radio features and configuration.....	19
RADIUS.....	19
Regional specifics.....	20
Routing/traffic flow.....	20
Synchronization and discovery.....	20
VSC (virtual service community).....	20
Web management tool.....	20
Wireless connectivity.....	20
Issues and workarounds.....	20
Version 6.5.3.0.....	21
Authentication.....	21
Controller teaming.....	21
DHCP.....	21
IDS (Intrusion Detection System).....	21
IMC (Intelligent Management Center).....	22
Local mesh.....	22
Logging.....	23
Miscellaneous.....	23
Performance.....	23

Radio features and configuration.....	23
RADIUS.....	23
SNMP.....	24
Synchronization and discovery.....	24
VPN.....	24
VSC (virtual service community).....	24
Web management tool.....	24
Wireless connectivity.....	25
GMS support for controller teaming.....	25
SOAP function limitations for controller teaming environment.....	26
Documentation updates and corrections.....	27
Contacting HP.....	27
HP security policy.....	28
Related information.....	28
Documents.....	28
Websites.....	28
Documentation feedback.....	28

MSM software V6.5.3.0

Description

This document provides important V6.5.3.0 release information.

Products supported

This document applies to these HP 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					Model
WW ¹	Americas	TAA	Japan	Israel	
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				Model
WW ¹	USA	Japan	Israel	
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

Product number				Model
WW ¹	USA	Japan	Israel	
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.

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 V6.5.3.0.

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 6.5.3.0, 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 CNxxxxxxxxx, 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 or higher will disable the NAT feature. HP 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 HP Passport is required to access the Software Updates and Licensing portal at www.hp.com/go/hpsoftwareupdatesupport and it is available to customers who have purchased a maintenance and support agreement.

Upgrading restrictions and guidelines

(Not applicable to HP 425 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 560
- HP 425
- 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 6.5.3.0 and then want to return to the version 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 6.5.3.0, those changes will not be present when you downgrade to the previous version.

If you factory reset your device after upgrading to Version 6.5.3.0, your previous configurations will be lost, and when you downgrade to any previous version you will be in a factory reset state.

Compatibility/interoperability

SSLv3 support

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

MSM management tool

To run the web-based management tool, use at least Internet Explorer 8 or Firefox 18.

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)
6.5.3.0/6.5.2.0/6.5.1.0/6.5.0.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 V6.5.3.0 also automatically upgrades any MSM320 and MSM325 Sensors it manages to MSM software V6.5.3.0.

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

Local mesh

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

GMS (Guest Management Software) for controllers

HP 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. The intuitive user interface is designed for receptionists and clerical staff with minimal training. Working with HP MSM7xx Controllers, secure login prevents unauthorized account creation, and the reporting feature records all account management activity for audits. A digital certificate secures all communications between GMS and the MSM7xx Controller. For details and download instructions, consult the *Guest Management Software Release Notes*. Search for "Guest Management Software" at www.hp.com/support/manuals.

NOTE: GMS 6.5.2.0 works with and is required for MSM software Version 6.5.3.0 See also "GMS support for controller teaming" (page 25).

Enhancements

Version 6.5.0.0 and higher includes the following:

New AP support

This release adds support for the HP 560 802.11ac Dual Radio Access Point.

802.11w support

(Applies to HP 560 only.) This new VSC configuration option provides enhanced security for WPA2 traffic by protecting unicast and multicast management action frames.

New installation configuration wizard

To help you perform the initial setup of the controller, a new configuration wizard is presented at startup. As a result, the **Configure initial controller settings** workflow has been removed from the **Automated workflows** feature.

RADIUS attributes for groups

(Applies to external RADIUS servers.) A new set of RADIUS attributes has been added allowing configuration of upload limits, download limits, and throughput rates for groups of users. Limits can be defined in terms of packets or octets (bytes). When a group quota is reached, the sessions for all users in the group are terminated.

Firmware load on reboot

This new feature enables a firmware update to occur automatically when an AP is restarted.

Changes

NOTE: The numbers that precede the change description are used for tracking purposes.

Version 6.5.0.0 and later includes 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 numbers that precede the fix description are used for tracking purposes.

Version 6.5.3.0

These fixes are included in this release:

Authentication

[**171524**, **172351**] (Applies to all supported APs.) Fixed an issue in which, on some wireless clients, 802.1X authentication might have taken several seconds to complete.

[**162454**, **172725**] (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 would force the clients to always use software encryption, causing high CPU utilization on the AP and possible AP reboot.

CLI

[**170920**] Fixed an issue that occurred when issuing the `ip-qos` profile CLI command with a new profile name (i.e., one not already created). Instead of the new profile being created, an error message similar to the following was logged:

```
% ERROR: IP QoS profile creation failed (Error reading the IP QoS profile).
```

[**155942, 174967**] 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

[**173386, 173621**] 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, 172702**] Fixed an issue in which RADIUS communications might have been 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.

[**162994, 169519**] 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.

DHCP

[**170785**] Fixed an issue that occurred 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.

Miscellaneous

[**167319, 172560**] (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.

[**158997, 169510**] Fixed an issue that occurred when a controller was configured as an access gateway rather than an AP controller and the number of user connections exceeded 500. Users might have become disconnected with “host not found” messages in their browsers.

MTM (Mobility Traffic Manager)

[**167222, 171514**] (Applies to MSM760, MSM765 zl, and MSM775 zl.) Fixed an issue in which the controller might have crashed/restarted when handling heavy Mobility Traffic Manager (MTM) traffic loads (3000 to 4000 active MTM clients).

RADIUS

[**162460, 168864**] 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.

[**162146, 170679**] 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.

Routing / traffic flow

[**160371**, **172299**] 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.

SOAP

[**170342**, **171862**] (Applies to autonomous APs.) SOAP command `GetPortMACAddress` for **Port_1**, returns error 1003 `Internal error`.

Synchronization and discovery

[**172121**, **172531**] Fixed an issue in which APs would not synchronize with a controller when all but the lowest data rates were disabled in a VSC.

VSC (virtual service community)

[**173721**] 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

[**159792**, **171986**] (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.

[**150164**, **173397**] (Applies to HP 517.) Fixed an issue in which switch port-related errors during VSC configuration always indicated **Switch port 1** regardless of the actual switch port.

Web interface

[**159677**, **171915**] 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.

[**161021**, **170234**] Fixed an issue in which the **IP Connection Tracking** stats were not displaying with Microsoft Internet Explorer 11.

Version 6.5.2.0

These fixes are included in this release:

Authentication

[**167611**, **169507**] (Applies to MSM7xx Controllers, with VSC authentication configured as non-Access Controlled, WPA2/Enterprise, 802.1X, with Active Directory authentication.) Fixed an issue in which authentication could stop working after upgrading MSM software from V6.4.x.x to V6.5.x.x.

Controller teaming

[**170713**] (Applies to HP 560.) Fixed an issue in which changing the **Country** setting from a country that supports 80 MHz channel widths to one that does not, caused the AP to no longer synchronize with the controller.

[**169708**, **171446**, **171008**] Fixed an issue that occurred after a team manager controller to team member controller failover. The SNMP notification receivers setting made on the team manager controller was not available on the team member controller, causing SNMP notifications to the SNMP trap listener not to be made.

[**169472**, **170335**] Fixed an issue in which AeroScout AP tracking failed when an AP controlled by a team manager became controlled by a team member controller (either because of a failover or a reboot).

[**166198**] (Applies to some combinations of Country, Radio mode, Channel, and Channel width.) Fixed an issue in which teamed controllers might fail to synchronize when upgrading from software Versions 6.4.x or earlier to software Versions 6.5.0.x or 6.5.1.x.

[**151409, 168445**] 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.

DHCP

[**167481, 169523**] (Applies to MSM7xx Controllers.) Fixed an issue in which DHCP responses were forwarded on port(s) for which the DHCP server is not enabled.

[**123459, 167756**] Fixed an issue in which DHCP maximum lease checking was not effective when setting up multiple VSCs because the maximum leases could be exceeded. The internal DHCP server could stop giving IP addresses, and the DHCP process could restart.

IDS (Intrusion Detection System)

[**166610, 168109**] 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).

Local mesh

[**166401, 169413**] (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).

[**163708, 171516**] (Applies to HP 560.) Fixed an issue in which, with local mesh master and slave APs configured on radio1 in 802.11ac mode (80 MHz channel width), clients could not connect to a wireless network configured on radio 2 of the slave AP.

Logging

[**157808**] 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
```

Miscellaneous

[**169233, 169461**] Fixed an issue in which APs or controllers could reboot after 198 or 248 days of uninterrupted uptime.

Radio features and configuration

[**169719**] Fixed an issue in which, when RRM was not enabled and **AutoChannel** with **Interval/Time of Day** was enabled, the radio could become unresponsive.

[**167467, 168668**] (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, 170992**] (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.

[**159979, 171001**] (Applies to HP 517.) Fixed an issue in which, in high noise or densely populated 2.4 GHz RF environments, the HP517 could refuse to accept and/or disconnect wireless clients.

[**155093, 171229**] (Applies to HP 560.) Fixed an issue in which configured data rates might not have been applied on the HP 560 802.11ac Radio. This might have shown up as some packets being transmitted at rates that were disabled.

RADIUS

[**148784**] Fixed an issue in which automated workflows restricted RADIUS secrets to a length of 16 characters whereas a length of up to 64 characters was allowed elsewhere in the web management tool.

SNMP

[**160932**] 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

SOAP

[**164499, 168870**] Fixed an issue in which the SOAP command `updateLocalMeshProfileDynamicAddressing` value **Allowed Downtime** was interpreted as seconds instead of milliseconds.

Synchronization and discovery

[**167266, 169498**] 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)

[**157342**] (Applies to HP 560.) Fixed an issue in which, when the VSC option `Upstream Diffserv tagging` was enabled, the 802.1p field for the non-WMM client upstream traffic should have been marked according to the DSCP packet priority. However, for the clients connected to the HP 560 radio 1, the 802.1p upstream marking was always 0.

Web management tool

[**168690**] Fixed an issue in which some alarms (for example: `AP disabled VSC Due to 802.11w settings`) appeared on the **Alarms** tab but did not appear under **Most Recent Alarms** on the Dashboard.

[**167729, 168882**] (Applies to MSM7xx Controllers.) Fixed an issue in which on some occasions, the Dashboard metric fields were blank, and a message similar to this was logged:

```
...err webs: extweb Problem with socket Resource temporarily unavailable  
11
```

[**167369**] (Applies to MSM7xx Controllers.) Fixed an issue in which **Alarms, Events, Neighborhood,** and **Radios-map** filter settings were not retained when navigating to a different web management tool page.

[**163059, 166525**] Fixed an issue in which long user names, AP names, and SSIDs were truncated in the list of wireless users, and the entire name could not be seen.

[**165527**] (Applies to MSM7xx Controllers.) Fixed an issue in which, after upgrading software and then enabling the **Inherited** option under **AP > Provisioning > Connectivity**, an error similar to the following error was logged, and you were not able to disable the **Inherited** option:

```
Jan 28 11:39:15 172.16.5.11 err > capacity05 webs: Error creating redirection to group
```

Wired connectivity

[**160780, 164555**] Fixed an issue in which, after rebooting an AP configured with a non-access controlled VSC with an egress VLAN configured, while the controller was not reachable, wireless clients could not communicate with the wired network.

Wireless connectivity

[**166392, 169466**] (Applies to HP425, HP560, MSM410, MSM430, MSM460, MSM466, and MSM466-R.) Fixed an issue in which the Alcatel IP phone model 8118 was not able to connect to the AP.

[**166382, 170345**] Fixed an issue in which wireless clients using the **WhatsApp** app might have triggered an unexpected reboot of the MSM7xx Controller, with messages similar to these logged:

```
httpproxy: assert: proxy.c AppendTxBuffer 3925  
(aSocketConnection->mSocket != -1).
```

```
monitord: Unexpected termination for process 'httpproxy' [pid 1220, up  
for 4 sec(s)]
```

```
Normal Reboot excessive restarts, 20 restarts in 5 minutes after 30  
minutes of uptime
```

[**161028**] (Applies to MSM410, MSM430, MSM460, MSM466, and MSM466-R.) Fixed an issue in which connectivity issues might have been experienced with clients implementing an aggressive power saving mode, such as some Chromebooks.

[**160363, 171430**] Fixed an issue in which, when a wireless client quickly roamed between APs connected to the same controller, the wireless client was unnecessarily dropped and reconnected, resulting in reduced throughput performance.

Version 6.5.1.0

These fixes are included in this release:

Controller teaming

[**162844, 165426**] Fixed an internal problem that prevented new AP configurations from being created. Errors similar to this were logged:

```
Dec 5 07:29:36 err webs DB: database is locked on DB_GetIntFromSQLStatement
```

```
Dec 5 07:29:36 err webs DB: Unable to prepare the SQL statement
```

[**160770, 162255**] (Applies to MSM720.) Under **Network > IP interfaces**, the IPv4 interfaces are now displayed.

[**152864, 163577**] (Applies to MSM720.) When having wireless client traffic going out an egress VLAN using a non-access controlled VSC, and then having the same traffic ingressed to another controller to perform HTML authentication, the authentication now succeeds.

[**151653, 163778**] Fixed an issue in which the number of APs per controller limit was prematurely reached (indicated as `AP limit exceeded`) due to controller/AP synchronization issues.

[**145061, 162512**] Fixed an issue that occurred when high CPU utilization in a teamed environment with IMC/WSM caused controllers to become unresponsive or restart.

DHCP

[**161637, 164459**] (Applies to DHCP used on a VLAN interface.) Fixed an issue in which malformed DHCP packets could occur because of DHCP discover packet truncation. This occurred with long client names (15 or more characters).

[**161580, 162264**] Fixed an issue in which under **Network > Address Allocation > Configure DHCP Server**, no more than three IP addresses could be configured for controller discovery.

Local mesh

[**163827, 164976**] (Applies to local mesh on MSM430, MSM460, MSM466, MSM466-R, and HP 560.) In the web management tool, pages **Wireless > Local mesh** and **Status > Local mesh** no longer report different SNR values for the same devices.

[**163027, 164513**] In a local mesh network, the WDS peers are no longer wrongly counted as normal wireless clients in the **Wireless clients** tab, causing an incorrect (high) wireless client count to be reported.

[**146343, 164558**] Fixed an issue in which the **Wireless > Overview** page displayed local mesh links in addition to the expected wireless clients.

Logging

[**144317, 157475**] Fixed an issue that caused the System Log to fill with repetitive occurrences of the following message:

```
Unexpected Termination for process dhclient ...
```

Miscellaneous

[**160190, 162986**] Fixed an issue in which manually adding a timeserver, and then pressing **Enter** on the keyboard instead of clicking the **Add** button, caused the timeserver configuration to not be saved.

MTM (Mobility Traffic Manager) (controllers)

[**161348, 164566**] Fixed an issue in which the **Mobility Overview** page displayed some APs more than once and did not display other APs.

[**153105, 163786**] (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.

Radio features and configuration

[**161744, 163368**] (Applies to RRM (Radio Resource Management) with radios using DFS channels.) Fixed an issue in which RRM would not start, with logged error:
Waiting for network to become complete...

[**160938**] (Applies to HP 560 radio 1.) Monitor Mode Clear-to-Send frames are now being captured.

[**159609, 160760**] (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 has synchronized to a controller continues to work even if the controller goes down. However, if the AP rebooted and the controller continued to stay down, clients that were connected before and should be able to re-connect, could not.

[**151335, 165221**] (Applies to MSM410, MSM430, MSM460, MSM466, MSM466-R, and HP 425.) Fixed an issue that occurred when autochannel was enabled at the AP level (but not system-wide). Autochannel did not work if the first VSC was disabled and bound to the radio.

Regional specifics

[**159976, 162048**] (Applies to teaming.) Fixed an issue in which the controller team did not synchronize after the team manager adopted a JA model AP that is using an 802.11j channel (184, 188, 192, 196) and a country other than Japan is selected.

[**159847, 160221**] (Applies to AM (USA) model APs only in controlled mode.) Fixed an issue that occurred when configuring an AP group or a specific AP with a non-supported country, that caused the AP to not synchronize and to continuously reboot.

Routing/traffic flow

[**163089**] (Applies to HP 560.) Fixed an issue in which custom wireless security filters on the egress side (packets to the network) of the HP 560 radio 1, did not work.

[**140725, 158833**] NAT one-to-one and port forwarding rules now work as expected after a controller reboot.

SOAP

[**165330, 165893**] The SOAP `InstallFirmware` command now works as expected.

[**155752, 164505**] Acceptance of the EULA (end user license agreement) via SOAP is now properly registered so that unnecessary additional EULA prompting from within the web management tool does not occur.

Synchronization and discovery

[**152954, 163781**] When a synchronized AP on a secure tunnel goes down, the AP loses synchronization. When this happens, the controller now indicates that the AP is not synchronized.

Web management tool

[**162429**] The product registration link has been corrected to:

<https://h10145.www1.hp.com/product/product.aspx>

Wired connectivity

[**162226**] Fixed an issue in which a wired user was unable to get an IP address (through DHCP) from the controller when connected to an ingress VLAN range of the controller.

Wireless connectivity

[**162863**] (Applies to the HP 560 with radio 1 set to **Access Point Only** mode.) Fixed an issue that occurred under some circumstances (many clients disconnecting at the same time, for example), in which not all wireless client disconnections were correctly counted, eventually preventing new clients from associating due to maximum clients per AP limits.

[**160668, 165122**] (Applies to APs in controlled mode.) False `AP Limit Exceeded` errors that made it not possible to configure an AP, no longer occur.

[**157731, 164710**] (Applies to HP 425, HP 560, MSM410, MSM430, MSM460, MSM466, and MSM466-R.) Fixed an issue in which erratic beacon output gave the false impression that there was a problem with the AP Wi-Fi signal. This could be observed in Wi-Fi diagnostic tools, and in a high density environment, wireless clients could roam needlessly due to their interpretation of the beacons.

Version 6.5.0.1

These fixes are included in this release:

Documentation/online help

[**162797**] Online help for the VSC setup page now includes the HP 560 in the list of APs that support band steering. Band steering is supported for the HP 560.

IMC (Intelligent Management Center)

[**153683, 162007**] When the list of mis-associated clients transported to IMC in a single SOAP call exceeds 100 clients, the management console on the controller no longer shows **Not Running** and the controller does not lose connection with IMC.

Local mesh

[**161691**] (Applies to an HP 560 configured for local mesh on channel 36.) The slave HP 560 AP is able to establish a link with the master AP.

[**160842, 161939**] If an Autonomous AP with a tagged default VLAN ID configured for Port 1 is also a member of a local mesh, the AP no longer becomes unreachable via the tagged default VLAN after a restart.

Radio features and configuration

[**161198**] Fixed an issue that caused the HP 560 5 GHz radio (radio 1) to stop transmitting, which was more likely to occur when the scan ratio was configured with a value greater than the default of 0.5%.

Regional specifics

[**157517, 161924**] (Applies to HP 425 with countries that do not support channel 36 such as **Qatar, China, or Taiwan.**) Fixed an issue in which, after a power cycle, radio 1 failed to provide the configured wireless services.

[**135211, 159548**] (Applies to MSM430, and MSM460 WW SKU with country set to **Qatar.**) In the 5725–5850 MHz band (Channels 149/153/157/161/165), the default (and maximum) EIRP power of 23 dBm has been corrected to 20 dBm.

Scheduled backups

[**159823, 162660**] (Applies to all controllers and autonomous APs.) Scheduled configuration backups no longer cause the controller or autonomous AP to reboot.

Upgrades

[**151926**] After upgrading to V6.5.0.0, the mobility controller discovery option will be disabled only if the feature is improperly configured. That is, if neither the primary controller option is checked nor the primary controller address set.

Wireless connectivity

[**162259**] (Applies to MSM410, HP 425, MSM430, MSM460, MSM466, MSM466-R, and HP 560) UDP packets less than 8 bytes in length are no longer dropped instead of being bridged from the wireless network to the Ethernet side.

Version 6.5.0.0

These fixes are included in this release:

Authentication

[**151254**, **158508**] Wireless client authentication no longer stops functioning under the following circumstances:

- There is one VSC configured for Active Directory authentication and one VSC configured for local authentication.
- A client authenticates on the VSC with Active Directory.
- Clients try authenticating on the VSC with local authentication.

Controller teaming

[**149941**, **157372**] AP group names longer than 20 characters, no longer cause temporary brief communication interruptions between teamed controllers.

DHCP

[**151413**, **157319**] (Applies to use of external DHCP servers.) Fixed an issue in which upon IP address renewal, wireless clients lost network connectivity, even though they remained associated with the AP.

Local mesh

[**147657**] If system-wide Auto-channel/Auto-power is enabled, it is now possible to configure the Auto-channel and Auto-power Interval for an AP radio participating in local mesh.

Performance

[**150977**, **157337**] (Applies to MSM317, MSM320, MSM325, and MSM422.) As wireless clients connect and disconnect, the AP no longer gets into a state of 100% CPU utilization which caused slow performance, or in some cases an AP reboot.

[**148577**, **154038**] (Applies to MSM775) Fixed an issue in which the LAN port occasionally operated with poor performance or failed to come up.

[**148527**, **151989**] (Applies to MSM422.) Fixed an issue that occurred in a busy RF environment, for example, with lost HT frames and retransmissions, in which the MSM422 could transmit frames to a station in power saving mode and then become busy while retransmitting frames to this station. During this time (multiple seconds), the MSM422 did not send any frames to other stations.

[**146207**, **157325**] Fixed an issue in which after some period of time a recurring log message appeared, similar to:

```
Jan 15 12:46:36 10.214.8.157 MSM775 debug statspoller: Process jpatch died with return code 11
```

Network bandwidth was reduced, with the impact becoming more severe with a greater number of APs being adopted by the controller.

Radio features and configuration

[**149181**, **152767**] (Applies to HP 425 with RRM (Radio Resource Management) enabled.) Configuring aggressive scan parameters (dwell time under 200 ms) for radios in monitor mode no longer unnecessarily degrades AP performance.

RADIUS

[**149260**, **157633**] Fix to support Class attribute in Accounting request to external RADIUS servers when using non-access-controlled VSCs.

Regional specifics

[**141161**, **157631**] (Applies to MSM310, MSM320, and MSM422.) Unsupported channels 184, 188, 192, and 196 are no longer available on APs operating in **Japan**.

Routing/traffic flow

[**152478**, **157307**] Applies when the addressing type (static/DHCP) of the egress interface is changed, or the IP address of the egress interface changes.) Fixed an issue in which DHCP relay functionality stopped working if an access controlled VSC is mapped to an egress interface that is associated with a VLAN on the Internet port, with NAT disabled, and the VSC's DHCP relay **Forward to egress interface** option is enabled.

Synchronization and discovery

[**148398**] Synchronizing AP configuration changes are no longer affected if any **Allowed wireless rates** check boxes are cleared.

VSC (virtual service community)

[**150817**, **155252**] (Applies to MSM410, MSM430, MSM46x, and HP 425.) A VSC can now be saved when the radio is operating on a channel that was dynamically selected due to DFS.

Web management tool

[**151947**, **157352**] APs now accurately report the number of wireless stations associated with the APs instead of reporting the maximum number allowed (255).

[**151657**, **157339**] All wireless clients are now properly displayed on the **Wireless Clients** page.

[**150082**, **154710**] Fixed an issue in which the filtering function on the **Wireless Clients** page did not work properly due to abbreviated AP names or SSIDs adversely affecting the filtering.

[**140584**] The "%" character no longer causes random characters to appear in the name on the controller when used in creating a profile name. You can now use the "%" character when creating a profile name.

[**135040**, **154107**] The correct number of clients is reported instead of the maximum number allowed (255).

Wireless connectivity

[**160173**, **160899**] (Applies to MSM410, MSM430, MSM46x, and HP 425.) Fixed an issue in which clients could associate with an AP and receive a DHCP address but they could not ping their gateway. A client device with certain Intel-based 802.11ac wireless devices (with uapsd enabled by default) and using Intel wireless driver Version 16.x or 17.x stopped transferring data frames after a few minutes.

[**156396**] Fixed an issue in which the AP did not broadcast beacons.

[**144311**, **157477**] Fixed an issue that occurred when a wireless client disassociated and then reassociated after a interval of more than 5 minutes, and the bandwidth restrictions imposed by the user account did not take effect.

[**142469**] When using option **Public IP addresses for Guest Access**, if there are more wireless clients than available public IP addresses, the wireless clients with a public IP address already assigned do not lose their address to a new wireless client.

Issues and workarounds

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

Version 6.5.3.0

The following issues are present in this release:

Authentication

[**169813**] (Applies to Active Directory.) If you attempt to use a single quote character (') in an Active Directory group name, the controller displays a blank error message (banner across the top of the page). Do not use the single quote character in an Active Directory group name.

Controller teaming

[**169843**] Controller serial port settings that are configured on a team manager controller are not propagated to team member controllers. If team member controller serial port access is desired, configure the serial port on the controller before making it part of a team.

[**169836**] If any controller in a team fails to provide system information, an error is logged, and no system information is returned for any of the controllers in the team.

[**168815, 172366**] (Applies to the MSM317 and HP 517 with **Send Network Policy TLV** enabled on their switch ports.) Controller teams fail to synchronize if the primary VLAN IDs of the AP switch ports are the same as the VLAN ID configured in the LLDP profile. Do the following to work around this issue:

1. Disable **Send Network Policy TLV** on every AP switch port that has it enabled.
2. Change the LLDP profile for each of those ports to use a VLAN ID that is different from the primary VLAN ID.
3. Re-enable **Send Network Policy TLV** on the AP switch ports.

[**162994, 169519**] Wireless users authenticated by Active Directory can be restricted to a VSC subset according to the Active Directory group in which they belong. If such wireless users are connected through an AP that is managed by a team member controller, the users are not properly restricted to the VSC subset. As a workaround, make sure that all APs are managed by the team manager controller by using provisioning.

[**158228**] If an SNMPv3 user is configured in an SNMP Trap receiver on the team member controller, and the SNMPv3 user account is then deleted from the team manager controller, after a software upgrade, the team member controller can get stuck in a loop resetting and downloading a configuration. As a workaround, ensure that the team manager and team member controllers are synchronized before performing any software upgrade.

[**149596**] If the team manager fails, the interim team manager will enable RRM severe interference mitigation and AP load balancing, even if these options were disabled by the administrator. As a workaround, promote the interim team manager to team manager, and then disable undesired options.

[**148260**] (Applies to MSM720.) A timeout can occur when attempting to obtain the `sysinfo` file from an MSM720 team manager when the team manager is under heavy load.

DHCP

[**170785**] Whenever a wireless client roams from one AP to another using MAC Authentication, the client session is terminated and does not restart until the client issues a new DHCP request. As a workaround, use a non-access-controlled VSC.

[**157512, 169486**] If a network that has DHCP servers on multiple VLANs experiences DHCP server delays or interruptions, APs might allow clients to associate without getting an IP address. You can consider provisioning a specific discovery VLAN to help prevent this.

IDS (Intrusion Detection System)

[**160516**] (Applies to HP 560.) When used as an IDS sensor, radio 1 cannot detect ad-hoc cells and update Mis-associated client station and Ad-hoc cells pages. Radio 2 can be used to provide this coverage if needed.

[**140224**] (Applies to MSM410, HP 425, MSM430, MSM460, MSM466, and MSM466-R.) When **Intrusion Detection System** (IDS) is enabled, AP radios on that (team of) controller(s) should 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.

[**131182**] Re-deploying an AP from one controller to another controller might generate false attacks reported by IDS on the original controller. As a workaround, reboot the controller after removing the AP.

IMC (Intelligent Management Center)

[**172388**] IMC may trigger log messages similar to the following. These log messages can be safely ignored.

```
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**] An MSM7xx Controller will not communicate with an IMC server when the IMC server is identified with a FQDN (fully-qualified domain name). As a workaround, identify the IMC server by its IP address.

[**137197**] When IMC establishes a connection to the MSM7xx Controller, the following error messages are displayed on the system log:

```
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.
```

These messages can be safely ignored.

Local mesh

[**168569**] (Applies to autonomous-mode APs with auto channel.) A slave AP in a local mesh configuration might transmit incorrect channel information in the beacon when using auto channel. When this occurs, client devices cannot associate with the slave AP. As a workaround, configure the slave AP to operate with a fixed channel.

[**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.) In this configuration, clients are unable to connect to the slave AP (radio 2) VSC. As a workaround, create a local mesh connection between the two HP 560 APs using a mode other than 802.11ac.

[**130021**] (Applies to MSM410, MSM430, MSM460, MSM466, and MSM466-R in controlled and autonomous mode, and the HP 425 in controlled mode.) A Dynamic Local Mesh Slave configured in Promiscuous Mode will not establish a link even in the presence of multiple Masters. As a workaround, specify a Local Mesh Group ID in the Local Mesh Profile.

Logging

[**153466**] Unneeded warning messages appear in the system log when an AP is configured to use channel 11 or 13 and the AP is changed from n/b/g 20 MHz channel width to 40 MHz channel width.

[**153280**] (Applies to HP 560.) When **Protected Management Frames (802.11w)** is enabled on the HP 560, invalid management frames are dropped as required by the 802.11w standard, but no log messages are generated to indicate that this event has occurred.

Miscellaneous

[**158997, 169510**] When a controller is configured as an access gateway rather than an AP controller and the number of user connections exceed 500, users can become disconnected with host not found messages in their browsers. As a workaround, only use this type of configuration when less than 500 users are expected. Or include controlled APs for user connection.

[**149463**] (Applies to HP 517.) sFlow is not supported on the HP 517.

Performance

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

Radio features and configuration

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

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

As a workaround, temporarily remove the group binding to the WEP-enabled VSC, then move the AP into the group, and finally, re-bind the VSC to the group.

[**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.

[**131154**] (Applies to MSM410, MSM430, MSM460, MSM466, and MSM466-R in autonomous mode.) After a reboot or a modification of the radio configuration, some error messages may be generated by `rfmgr_ap`. These messages do not indicate a malfunction and can be ignored. The services offered by the radio will work properly.

[**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.

RADIUS

[**169808**] Public access attributes (defined on the **Controller >> Public access > Attributes** page) do 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) will not function properly and will be displayed incorrectly. Either delete the attribute and re-create it without the unsupported special characters or edit the attribute, removing the unsupported special characters.

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

[**162146, 170679**] When there is heavy RADIUS traffic load (authentication and accounting) going through the controller, the controller might experience higher than usual CPU utilization, and performance sluggishness might be experienced.

[**131693**] (Applies to MSM410, HP 425, MSM430, MSM460, MSM466, and MSM466-R.) iPads/iPods/iPhones cannot authenticate using the secondary RADIUS server with the default configuration. As a workaround, reduce the retry interval in the RADIUS Profile configuration to 5 seconds.

SNMP

[**127299**] The SNMP OIDs that report information about the configuration of the Autochannel features "COLUBRIS-DEVICE-WIRELESS-MIB coDevWirIfStaAutoChannelEnabled" and "coDevWirIfStaAutoChannelInterval" may report incorrect information.

Synchronization and discovery

[**172302**] (Applies to all controllers for AP provisioning with controller-based provisioning settings.) AP discovery might fail when entering "names to search for" to discover APs using DNS. As a workaround, search for every DNS service name you need (one after the other in the same session), and finally, enable Discover using DNS, enable Base Group: All | Discovery, then select Save and synchronize the APs.

[**156141**] (Applies to HP 560.) The AP can take several minutes to synchronize with a controller when creating or deleting a VSC with **Protected Management Frames (802.11w)** enabled.

VPN

[**129915**] Clients using the PPTP VPN server might experience connectivity issues when sending large packets.

VSC (virtual service community)

[**174939**] The **VSC User Sessions** page cannot be sorted by clicking the VSC column.

[**159792**] (Applies to HP 517, MSM460, MSM466, and MSM466-R in controlled mode.) APs being synchronized might get stuck in the **Uploading** configuration state. As a workaround, for each VSC, under **Allowed wireless rates**, for the 802.11n and 802.11ac **Wireless** mode, enable the 1 Mbps and 6 Mbps rates; enable at least one MCS rate and ensure that there are no more than 31 disabled rates.

[**159082**] Some clients might not be able to connect to a particular wireless network if the VSC has both **Protected Management Frames (802.11w)** and **Terminate WPA at the Controller** enabled. These are mutually exclusive options, even though the V6.5.x.x software does not enforce mutual exclusivity.

Web management tool

[**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.

[**159677**] The management tool may restart when attempting to sort a list of user sessions by VSC, Idle time or VLAN, when the list includes non-Access Controlled clients. You must log in again.

[**148443**] On the **Overview > Wireless clients** page, the scroll bar might be missing (or partially hidden) when viewed with Mozilla Firefox. The page displays properly when viewed with Microsoft Internet Explorer.

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.

[**168364**] (Applies to Apple MacBook OSX clients connecting to an HP 560 with radio 1 in the 5GHz band.) Clients may lose network connectivity when they awake from sleep mode. As a workaround, consider disabling the Energy Saver option for **Wake for network access** and **Wake for Wi-Fi network access** options.

GMS support for controller teaming

GMS 6.5.2.0 supports teaming in MSM software 6.5.3.0 with the following limitations:

- **Only the team manager controller is supported.** GMS interacts only with the team manager controller and not member controllers.
- **Subscription plans not supported.** User sessions are not synchronized across all members in a team. Therefore, subscription plans are not supported on a controller team. User accounts cannot have **Validity** set to **Subscription Plan**. **Custom Validity** is the only choice for **Validity**.
- **Automatic account removal only supported for Inactivity.** Due to a lack of synchronization between team members and the team manager, automatic account removal due to **Inactivity** is not supported on a controller team. Automatic account removal due to **Inactivity** is supported on a controller team.
- **Maximum number of concurrent sessions not supported.** Since this option is per controller, it is not supported in a team. This option is fixed at **Unlimited** for controller teams.

Configuring the service controller in GMS (when teaming is used):

- Do not configure a controller in GMS when the team manager controller is not available and a team member is temporarily taking its place.
- GMS interacts only with the team manager controller, you cannot add a team member as the controller.
- Any attempt to add a team member as a service controller in GMS will be rejected, with the following message displayed: *"An error occurred while uploading the CA to the Service Controller. Please check if the Services Controller is a member of a team. If teamed, please add the Service Controller using the team IP or team manager IP."*
- It is best to use the team IP address for the controller configuration.
- If you specify the team manager controller IP address, GMS detects that it is the team manager controller and automatically adds the controller using the team IP address. This confirmation message is displayed: *"The Service Controller you are trying to add is the team manager. GMS will add this Service Controller using the team IP address instead of the Service Controller IP address."* This is normal.
- On the **Service Controller** tab, the **Edit Service Controller** button cannot be used to edit the controller information for teamed controllers (parameters such as Team IP, HTTP port number, and SOAP port number). Attempts to do this cause this message to be displayed: *"Editing Service Controller details is not supported. If the details are altered, please delete and add the Service Controller using the Add device wizard."* As the message indicates, delete and then add the controller back with the wizard, specifying the changed values.

Adding/editing user accounts in GMS when the team manager is unavailable:

- As when teamed controllers are not used and the controller becomes unavailable, if the team manager controller becomes unavailable, users can still be added and edited in GMS but the controller (team manager) is not updated until it comes back online.
- In this case when adding/editing user accounts, the following prompt is displayed: The selected team is in standby mode. GMS will add the account once the team manager is active. Do you want to continue? Select **Yes** to add/edit the account in GMS only for now, with automatic update of the team manager controller upon its availability.

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 MSM710 Controller and MSM335 AP are not supported in release 6.5.0.x.
- The Protect Management Frames (802.11w) section in the online help contains the following statement:

Only disable this option if you are having connectivity issues with 802.11w client stations, and disabling this option resolves the issues. Otherwise, this option should always be enabled.

Ignore this help text, and refer to the following text instead:

To avoid compatibility issues with incorrect 802.11w implementations, the Protect Management Frames feature is disabled by default. It should only be enabled if your client stations provide a proper 802.11w implementation. One way to test this is to enable 802.11w support, and then see if wireless throughput decreases for a client station. If it does, the 802.11w implementation on the client is incompatible, and Protected Management Frame feature should not be enabled.

See also “Performance” (page 23) issue 156546.

HP MSM SNMP MIB Reference Guide v6.5.0.x

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

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

Contacting HP

For additional information or assistance, contact HP Networking Support:

<http://www.hp.com/networking/support>

Before contacting HP, collect the following information:

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

HP security policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

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

To find security bulletins:

1. Go to the HP Support Center website at www.hp.com/go/hpsc.
2. Enter your product name or number and click **Go**.
3. Select your product from the list of results.
4. Click the **Top issues & solutions** tab.
5. Click the **Advisories, bulletins & notices** link.

To initiate a subscription to receive future HP Security Bulletin alerts via email, sign up at: http://h41183.www4.hp.com/signup_alerts.php?jumpid=hpsc_secbulletins

Related information

Documents

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

<http://www.hp.com/support/manuals>

Enter your product name or number, and then click **Go**. If necessary, select your product from the resulting list.

Websites

- Official HP Home page: <http://www.hp.com>
- HP Networking: <http://www.hp.com/go/networking>
- HP product manuals: <http://www.hp.com/support/manuals>
- HP download drivers and software: <http://www.hp.com/support/downloads>
- HP software depot: <http://www.software.hp.com>
- HP education services: <http://www.hp.com/learn>

Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hp.com). Include the document title and part number, version number, or the URL when submitting your feedback.