HP MSM7xx Controllers Release Notes V6.4.2.x

Abstract

These release notes provide important release-related information for MSM software Version 6.4.2.1.

HP Part Number: 5998-6971a
Published: March 2015
Edition: 2

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.

Acknowledgements

Windows® is a U.S. registered trademark of Microsoft Corporation.

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

Description

These release notes provide important V6.4.2.1 release information.

NOTE: In this document, except when identifying specific models, the generic term “controller” is used in place of MSM7xx Controller product names and the generic term “AP” is used in place of MSM3xx / MSM4xx / HP 425 / HP 517 Access Point product names.

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

NOTE: Support for the discontinued MSM710 Controller is available in software versions prior to V6.2.x.

Online documentation

You can download documentation from the HP Support website at www.hp.com/support/manuals. Search by product name or part number.

See also the “New in release” section of the *MSM7xx Controllers Configuration Guide*.

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.

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), MSM325 (J9369A/B).

IMPORTANT: Prior to upgrading to MSM software Version 6.4.2.1, 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 may 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 V6.4.x, V6.3.x, or V6.2.x will disable the NAT feature. HP recommends that you review your existing settings and disable one of these features before upgrading to V6.4.x, V6.3.x or V6.2.x.

Updating software

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.

Downgrading software

If you upgrade to Version 6.4.2.1 and then wish 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 6.4.2.1, those changes will not be present when you downgrade to the previous version.

If you factory reset your device after upgrading to Version 6.4.2.1, your previous configurations will be lost, and when you downgrade to any previous version you will be in a factory reset state.

HP 517 802.11ac Unified Walljack support

Support for the HP 517 802.11ac Unified Walljack was added in MSM software V6.4.0.0. The HP 517 operates only in controlled mode. It is supported by these MSM controllers: MSM720, MSM760, MSM765 zl, and MSM775 zl.

For more information, see the following documents, available online:

- *HP 517 802.11ac Unified Walljack Quickstart*
- *HP 517 802.11ac Unified Walljack Installation Guide*
- *HP 517 802.11ac Unified Walljack Configuration Guide*

MSM710 Controller support stops at V6.0.x

Support for the discontinued MSM710 Controller is available in software versions prior to V6.2.x. As of V6.2.0.0, support for the MSM710 is dropped.

Note: The HP 425 and HP 517 are not supported by the MSM710 Controller.

MSM335 AP support stops at V6.3.x

Support for the discontinued MSM335 AP is available in software versions prior to V6.4.0.0. As of V6.4.0.0, support for the MSM335 AP is dropped.

RF Manager software and MSM software version compatibility

RF Manager Versions 5.9.x, 6.0.x, and 6.7.x work with MSM software Version 5.5.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, MSM335[2], HP 425[3])
5.7.5.0/6.0.3.0/6.3.0.0/6.4.0.0/ 6.4.1.0/6.4.2.x	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		
5.5.3.x	6.0.157 or later		
5.5.1.x/5.5.2.x	6.0.154 or later		
5.5.0.x	5.9.203, 6.0.147 or later		

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

[2] MSM335 APs are supported with software V6.3.x or earlier only.

[3] HP 425 requires RF Manager V6.7.769.42 or later.

Notes:

Software Version 6.2.0.0, 6.3.0.0, and 6.4.x.x are compatible with RF Manager versions listed above, but the MSM320, MSM325, and MSM335 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.

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.

Upgrading an MSM7xx Controller to V6.4.2.1 also automatically upgrades any MSM320 and MSM325 Sensors it manages to MSM software V6.4.2.1.

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

GMS (Guest Management Software)

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 6.4.2.0 works with and is required for MSM software Version 6.4.2.x. See also "GMS support for teaming" (page 6).

GMS support for teaming

GMS 6.4.2.0 supports teaming in MSM software V6.4.2.x 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 Invalidity.** 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 **Invalidity** 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:

- Like 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 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.

- 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

The above limitations ONLY apply to controller teams.

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

Note on SOAP function UpdateUserAccountRemovalSettings

The **Removal due to invalidity** option of this function works in a teaming environment. However, the **Removal due to inactivity** option should be avoided when teaming because it could cause the controllers to wrongly remove active accounts.

Changes

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

Version 6.4.2.1 includes the following change:

- [161849] Support for the SSLv3 cryptographic protocol has been removed.

Version 6.4.2.0 includes the following change:

- [153332, 155784] 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 precedes the fix description are used for tracking purposes.

Version 6.4.2.1

There are no additional fixes in Version 6.4.2.1.

Version 6.4.2.0

The following issues have been fixed in Version 6.4.2.0:

- [161625, 162097] The product registration link has been corrected to: https://h10145.www1.hp.com/product/product.aspx
- [160668] (Applies to APs in controlled mode.) False `AP Limit Exceeded` errors might occur, making it not possible to configure an AP.
- [159847, 161171] (Applies to AM (USA) SKU APs only in controlled mode.) Configuring an AP group or a specific AP with a non-supported country, causes the AP to not synchronize and to continuously reboot.
- [159823, 161879] (Applies to all controllers and autonomous APs.) Scheduled configuration backups can cause the controller or autonomous AP to reboot.
- [159792, 161058] (Applies to HP 517, MSM460, MSM466, MSM466-R in controlled mode.) APs being synchronized might get stuck in the **Uploading configuration** state.
- [158697, 159471] (Applies to teaming.) Free access user details are only created on the team manager controller and should not be synchronized with team member controllers.
- [157808, 159342] Excess system log messages similar to the following are 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
  ```

- [157578, 159433] A description of 802.11n is missing from the online help for the wireless client status page.
- [156559, 157028] MTM (Mobility Traffic Manager) traffic is sent to the Internet port or the untagged AP VLAN instead of the VLAN bound to the VSC.
- [156238, 157802] The SOAP command `ExecuteWirelessDisassociateClient` might fail if there are more than 1,000 clients.
- [153965, 154062] When DHCP relay is configured in a VSC with the **Extend subnet to egress** option enabled, the controller may reply to ARP requests for any IP address in the subnet.

- [153864, 158978] (Applies to teaming.) After upgrading to 6.4.x.x with an invalid configuration/provisioning of local mesh on products that do not support it (MSM317 and HP 517), teaming synchronization fails.
- [153683, 162006] 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.
- [152954, 153735] When a synchronized AP on a secure tunnel goes down, the AP loses synchronization. When this happens, the controller might indicate that the AP is synchronized, but the radios appear to be pending or unavailable.
- [152478, 157306] (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.
- [152435, 157041] When running the management tool in Mozilla Firefox, deleting a network profile might cause the management tool to restart.
- [151409, 152949] (Applies to teaming.) After a team is formed and working properly, changing the regulatory domain to certain countries can cause 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.
- [151254, 158507] Wireless client authentication 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
- [151413, 155992] (Applies to use of external DHCP servers.) Upon IP address renewal, wireless clients lose network connectivity, even though they remain associated with the AP.
- [151130, 155990] With LLDP dynamic naming enabled, empty LLDP strings in place of serial numbers cause AP synchronization problems.
- [150976, 158544] In high traffic environments, DNS resolution by the controller can cause authentication delays and require multiple retries by clients.
- [150629, 158549] (Applies to teaming.) When inheritance is enabled, AP configuration changes do not propagate to the team member controllers.
- [150309, 158546] VLAN tag mapping and uplink port data was not included in the output of the CLI show config all command.
- [150082, 154588]The filtering function on the Wireless Clients page does not work properly due to abbreviated AP names or SSIDs adversely affecting the filtering.
- [149260, 155988] Fix to support Class attribute in Accounting request to external RADIUS servers when using non-access-controlled VSCs.
- [148784, 154670] The automated workflows for **Creating a wireless network for employees** and **Creating a wireless network for guests** now allow RADIUS secrets up to 64 characters long as indicated on the **Authentication** > **RADIUS profiles** page.
- [148577, 154041] (Applies to MSM775) Fixed an issue in which the LAN port occasionally operated with poor performance or failed to come up.
- [148482, 157556] In a Microsoft DNS environment with a parent domain and at least two child domains, users may be unable to connect.

- [148373, 158540] When using the **REDIRECT-URL** public attribute with the URL placeholders (**%l** and **%o**), the placeholders are double encoding the requested URL.
- [147293, 158460] When using sFlow, an error message regarding `kernel emergency` is incorrectly displayed and can be ignored.
- [147283, 158457] (Applies to teaming.) When a team manager controller fails over, the team member taking over from the team manager now sends SNMP traps to the IMC server.
- [146207, 157324] After some period of time, a recurring log message appears, similar to:

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

  Network bandwidth is reduced, with the impact becoming more severe with a greater number of APs being adopted by the controller.
- [146156, 156147] (Applies to teaming.) Controller restarts can occur if the team manager interface is defined on a VLAN without IP address. This configuration is not allowed anymore. You must have an IP address on the interface either static or DHCP.
- [145135, 158535] The following missing SOAP commands for handling VSC ID and Station ID MAC delimiters have been added:
  - soapUpdateVirtualSCMACBasedStationIdDelimiterAndCase ($vscName,$stationIdDelimiter, $stationIdMACCase)
  - soapGetVirtualSCMACBasedStationIdDelimiterAndCase($vscName)
- [145061, 155977] (Applies to teaming.) High CPU utilization in a teamed environment with IMC/WSM can cause controllers to become unresponsive or restart.
- [144311, 155973] Issue seen with VSCs set for Public Access control and HTML-based authentication. User rate limit is not applied upon re-association when user disassociates for longer than 5 minutes (unit is turned off).
- [143918, 155971] Missing SNMP OIDs:

  nlcolubris802dot11: 1.3.6.1.4.1.8744.5

  nlcolubrisVirtualApMIB: 1.3.6.1.4.1.8744.5.1
- [143446, 158533] When the **restrict 802.11n clients** option is enabled, wireless clients on the 5 GHz band are unable to reach other clients.
- [143256, 158538] The PayPal service does not accept guest credit card direct purchases.
- [143014, 158531] IDS reports the following warning log messages which can be ignored:

  ```
  [err_channel]802.11a Erroneous channel [1], Interface [r1v16],
  PrismChannel [36]
  ```
- [141866, 158529] Using an external RADIUS server and an access-controlled VSC can cause the MSM7xx Controller to reboot.
- [141161, 153847] (Applies to MSM310, MSM320, MSM422.) Unsupported channels 184,188,192 and 196 are no longer available on APs operating in Japan.
- [140860, 158528] After a software upgrade, if the secondary RADIUS server IP address is not set, the controller will erroneously set it to 0.0.0.0.
- [140725, 153869] NAT one to one and port forwarding rules are now working after a controller reboot.
- [140613, 158530] Using SOAP functions directed to a non-configured IP address causes SOAP to fail and add the following error message to the controller log:

  ```
  websoap: SOAP FAULT: SOAP-ENV:Client "Internal error"
  ```

  ```
  websoap: Unable to communicate with IPRulesMgr, Timeout occurred.
  ```

- [140584, 158462] If the **%** character is used when creating a network profile name, random characters appear in the profile name.
- [139954, 157565] HTML authentication does not work if the user name contains spaces.
- [139862, 152896] The MSM Controller continues to respond to DHCP requests on the LAN port after that feature has been disabled.
- [138441, 157545] Added the following SOAP function to allow mapping of a network profile to a local mesh interface:
  `AddVLANOnLocalMesh()`
- [138382, 155966] The MSM controller uptime value in the management tool is different from the value retrieved using IMC.
- [137987, 157542]Added the following SOAP commands to autonomous mode APs:
  - To configure the Station ID delimiter used in the Called-Station-Id content in the RADIUS request:
    `UpdateVirtualSC8021XStationIdDelimiterAndCase`
    `GetVirtualSC8021XStationIdDelimiterAndCase`
  - To configure the MAC case:
    `GetVirtualSC8021XStationIdDelimiterAndCasem`
    `UpdateVirtualSC8021XStationIdDelimiterAndCasem`
- [137894, 157539] When configuring **Wireless protection** with a **Key source** of **Preshared Key**, the station delimiter and station ID MAC delimiter configuration fields are disabled.
- [136856, 155896] The MSM7xx Controller does not provide a NAS ID value to a customized ACL.
- [134840, 154204] 802.1x authentication of new wireless clients may fail intermittently when configured on a non-Access Controlled VSC.
- [132299, 162168] The controller or AP sends its serial number as its NAS ID to the external RADIUS server, even if the NAS ID value has been manually configured to a user specified value.

Version 6.4.1.0

The following issues have been fixed in Version 6.4.1.0:

- [152176] Controller teams do not synchronize when apostrophe (') characters are used in the AP details **location** field.
- [152004] (Applies to country set to **Turkey**.) Radio settings are missing.
- [152003] When receiving unexpected network traffic, a non-applicable log message similar to this appears:
  `crit webrediret: assert: ../webs.c websParseFirst 900 (text && *text) - re-opening`
- [151983] Connection with IMC might drop when AP group names are longer than 20 characters.
- [151981] When connected through an access controlled VSC using MAC authentication, users randomly lose their connection while roaming between two APs.
- [151978] When a RADIUS profile is deleted and replaced by a new profile, the AP still uses the secret of the deleted profile.
- [151961] (Applies to MSM410, MSM430, MSM460, MSM466, MSM466-R, HP 425.) Autochannel enabled at the AP level (but not system-wide) does not work if the first VSC is disabled and bound to the radio.
- [151923] While using multiple DHCP servers with different IP address subnets in the same network as the AP, some clients do not get an IP address.

- [151844] (Applies to HP 517.) Broadcast and multicasts packets are not always forwarded to wireless clients.
- [151703] Random false radio down detection occurs when system-wide autopower/autochannel is enabled in a dense environment.
- [151516] RRM analysis results cannot be applied when an error similar to this is logged:

```
Mar 18 03:15:45 capacity07 10.214.8.157 err eventmgr:  vacuum_db:2198: SQL error: 10:disk I/O error
Mar 18 03:15:45 capacity07 10.214.8.157 err eventmgr:  Error vacuuming database /flash/events.sqlite
```

- [151514] APs may take longer to synchronize with the controller when some wireless rates have been disabled.
- [151498, 147909] (Applies to Teaming.) Adding two or more new controllers to a team at the same time can result in a deadlock situation with the controllers stuck in an uploading configuration state.
- [150518, 146960] A local mesh master AP is unable to maintain a link to slave APs due to a DFS-initiated channel change.
- [148398] Synchronizing AP configuration changes can be slower if any rates are unchecked in **Allowed wireless rates**. As a workaround, do not uncheck any rates in **Allowed wireless rates**, or wait for the synchronization to complete.
- [142209] (Applies to dual-radio APs.) The utilization of Radio 2 was not taken into account to classify per-bandwidth utilization.

Version 6.4.0.0

The following issues were fixed in Version 6.4.0.0:

- [146418, 147272] The AP is not sending LLC SNAP frames to the switch when a wireless client associates.
- [145873] (Applies to teaming with Country set to **Russia**.) The controller team does not synchronize when any of these channels are manually selected:

  149, 153, 157, 161
- [145015] (Applies to teaming.) APs fail to find the team member controller when using DNS discovery
- [144532] (Applies to teaming.) Network Address Translation (NAT) is not applied to traffic on an access-controlled VSC with an egress VLAN defined, when the wireless client connects through a team member controller.
- [144090] RF Manager 6.7 does not recognize the HP 425 Access Point as an HP branded device. Information about the HP 425 being adopted by the controller is sent to RF Manager, but the information does not get into the RF Manager authorized AP list.
- [143002] Wireless user authentication requests are not shared between Active Directory trusted domains.
- [142934] Rate limiting does not work in the downstream direction for any VSC that uses a VLAN for egress.
- [142419, 143271] After an upgrade, APs may become unsynchronized and not resynchronize when Automatic Power Control for APs is enabled.
- [142194] If you have more than five VLAN interfaces with IP addresses, the controller can experience issues at boot time.
- [142135, 142220] The `GetAuthenticatedusers` SOAP command provides erroneous results for bytes sent and bytes received.

- [140114, 140232] When a single VSC egresses user traffic over different VLANs (depending on AP location) and a client roams from one AP to another, the controller may erroneously detect the user as a Mobility Traffic Manager (MTM) visitor and block their traffic.
- [139714, 141440] (Applies to teaming.) Teaming failover causes Mobility Traffic Manager (MTM) clients traffic to stop, even after the AP is adopted by an alternate team manager controller.
- [139590, 144485] (Applies to teaming.) If using teaming while an access controlled VSC with 802.1x authentication and the **WPA termination** option is enabled, wireless clients might not be able to connect via a team member controller.
- [139451, 140118] (Applies to teaming.) APs adopted by a team member controller can appear to be in the **pending** state on the management tool, even though the APs are operating and providing service.
- [139066, 140645, 126192] When using HTML authentication, the **Continue Browsing** link on the Welcome page erroneously redirects an authenticated user back to the login page.
- [138776] The SNMP MIB for LLDP returns the LldpChassisIdSubtype MAC address in an incorrect format.
- [137987, 143146] When configuring an 802.1x VSC using SOAP, it is not possible to set the **Station ID delimiter** or the **Station ID MAC**.
- [137900] After a software upgrade, an AP might drop packets from the user VLAN over the AP tagged management VLAN.
- [137894, 143158] When configuring a VSC, if the wireless protection key source is changed to use PSK, the **Station ID delimiter** and **Station ID MAC case** configuration fields disappear from the management tool.

  When configuring a VSC using SOAP, if the wireless protection key source is set to use PSK, it is not possible to set the **Station ID delimiter** or the **Station ID MAC**.
- [137313] The SNMP process causes high CPU and high memory usage, which can cause the controller to reboot.
- [143125, 136116] (Applies to teaming.) The team manager controller can lose its default route when a static IP address is configured on the Internet port.

Issues and workarounds

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

These issues are present in this release:

- [162858] (Applies to teaming.) The management tool makes it possible to configure an IP address for the team, even if the address has already been used for the LAN interface. This inappropriate configuration will cause APs discovered on the LAN interface to disconnect. Never attempt to use an address that was already assigned to a controller interface, as the team address. Assign an unused IP address to the team.
- [162373] (Applies to teaming.) When the team manager goes down, the alarm (`ALARM_CS_CONTROLLER_DOWN, ID39`) is not shown on the team member controller that takes over for the former team manager controller.
- [161583, 162367] (Applies to MSM760.) The **Serial port access** section in the management tool under **Controller** >> **Management** > **CLI** is not displayed. Note that you can still log in to the controller and access the CLI using the serial port.
- [160892] On very rare occasions, events and alarms might stop being reported. This might also affect performance of the management interface. The presence of this condition can be confirmed by the presence of a message similar to this in the system log:

  ```
  webs: flush_db:1995: SQL error: 8:attempt to write a readonly database.
  ```

To clear this condition, reboot the controller.

- [160587] The **Validity period** under **Subscription** does not give users access when using the **Between** option (for example, **your time + 5 minutes** and **your time + 30 minutes**). Users configured to use the validity period between two times will be blocked. As a workaround, set a validity period for a subscription plan using the **From** and **Until** options. This allows 'day to day' control over subscription plan usage but not 'hour by hour'.
- [160318] The use of domain name or IP address in the wrong format as part of a DNAT rule parameter causes the controller to reboot. As a workaround, use DNAT rules with a valid domain name or IP address parameter format. For more information, see the *MSM7xx Controllers Configuration Guide*.
- [160118] (Applies to local mesh.) When master and slave APs are sharing the same network connected on the Ethernet port, the local mesh link is not established on autonomous APs when the operating mode is set to **Access point and Local mesh**. The master local mesh status remains as **Locked**, and the slave status is **Searching for master**. As a workaround, set the master operating mode to **Local mesh only** or ensure that master and slave do not share the same network.
- [159609, 160760] (Applies to HP 425, MSM430, MSM46x, HP 517.) The survivability feature may 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 reboots and the controller continues to stay down, clients that were connected before and should be able to re-connect cannot. The problem goes away when the controller comes back up and the APs reconnect.
- [159404] (Applies to HP 425 in controlled mode, with WPA/WPA2 PSK authentication.) With 25 or more users connected to an HP 425 (5 GHz radio), traffic for all users begins to slow and users may notice latency. With 30 or more users connected, the traffic for all users may halt or time out. As a workaround, set the connection limit in the range of 25 to 29
- [158997] 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.
- [154848] HP strongly recommends that for local mesh, the same AP model be used at both ends of the mesh link. If for local mesh, recent APs (MSM430, MSM46x, HP 425) are mixed with older APs (MSM3xx, MSM422), after a software upgrade, the local mesh might stop working.
- [153858, 144309] The SysInfo file cannot be downloaded when the controller has joined an Active Directory domain that is configured to use IPv6. As a workaround, do not configure the Active Directory server for IPv6 when used with an MSM7xx Controller.
- [149596] (Applies to teaming.) 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.
- [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.
- [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.
- [147657] If system-wide Auto-channel/Auto-power is enabled, it is not possible to configure the Auto-channel and Auto-power Interval for an AP radio participating in local mesh.
- [146494] (Applies to HP 517.) The Apple Bonjour features (multicast handling and user profiles) are not supported on the HP 517 wired ports.
- [142469] When using option **Public IP addresses for Guest Access**, and there are more wireless clients than available public IP addresses, the wireless clients with a public IP address already

assigned might lose their address to a new wireless client. As a workaround, make sure that you provision enough public IP addresses to cover the largest anticipated number of concurrent users.

- [140224] (Applies to MSM410, HP 425, MSM430, MSM460, MSM466, 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, IDS must be disabled on the controller if **Access Point and Local Mesh** or **Local Mesh only** operation is required.
- [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.
- [131693] 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.
- [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.
- [129915] Clients using the PPTP VPN server might experience connectivity issues when sending large packets.
- [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.
- [124010] (Applies to MSM410, MSM430, MSM460, MSM466, 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.
- [113398] Wireless clients connected to a VSC that is directly mapped to a VLAN are unable to reach wired clients on the same VLAN.

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 click **Go**. If necessary, select your product from the resulting list.

See also the "New in release" section of the *MSM7xx Controllers Configuration Guide*.

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, or the URL when submitting your feedback.