HP MSM7xx Controllers Release Notes
v6.0.3.0

HP Part Number: 5998-6968
Published: October 2014
Edition: 1

Acknowledgements

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

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

Version: MSM v6.0.3.0

Description

These release notes provide important release-related 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 Access Point product names.

Product models

This document applies to these HP products:

Model	Part
MSM710 Access Controller	J9328A
MSM710 Mobility Controller	J9325A
MSM720 Access Controller	J9693A
MSM720 Premium Mobility Controller	J9694A
MSM720 Access Controller (TAA)	J9695A
MSM720 Premium Mobility Controller (TAA)	J9696A
MSM760 Access Controller	J9421A
MSM760 Premium Mobility Controller	J9420A
MSM765 zl Premium Mobility Controller	J9370A

Online documentation

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

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), MSM335 (J9356A/B).

IMPORTANT: PRIOR to upgrading to MSM software version 6.0.2.x, all applicable APs (autonomous or controlled) that are manually configured to use channel 132 must be either re-configured to use a different channel or be re-configured 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 Auto 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 v6.0.3.0 software will disable the NAT feature. HP recommends that you review your existing settings and disable one of these features before upgrading to v6.0.3.0.

Updating software

Update the controller software as described in the "Software updates" section of the *MSM Controllers Configuration Guide*. Once the controller is updated, it automatically updates all of its controlled devices to the same software version.

Downgrading software

If you upgrade to version 6.0.3.0 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 6.0.3.0, those changes will not be present when you downgrade to the previous version.

If you factory reset your device after upgrading to version 6.0.3.0, your previous configurations will be lost, and when you downgrade to any previous version you will be in a factory reset state.

MSM management tool now requires web browser with SSLv3 support

NOTE: Starting with MSM software version 5.7.0.3, a web browser that supports SSLv3 is mandatory for running the MSM web-based management tool. SSLv3 is supported by Microsoft Internet Explorer 7 and 8 but must be enabled. Microsoft Internet Explorer 9 only uses SSLv3. Mozilla Firefox also supports SSLv3 but support may need to be enabled or you may need to update to a more recent version.

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 (GMS) Release Notes*. Search for "Guest Management Software" at www.hp.com/support/manuals.

NOTE: GMS 6.0.3.0 works with and is required for MSM software version 6.0.3.0. See also "GMS support for teaming" (page 5).

RF Manager software and MSM software version compatibility

RF Manager versions 5.9.x and 6.0.x work with MSM software version 5.5.x and later. However, to use the WLAN Integration feature in RF Manager 6.0.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*, MSM325, MSM335)
6.0.3.x	6.7.769 or later	Upgraded automatically by RF Manager	Upgraded automatically by MSM7xx Controller
5.7.1.x/5.7.2.0/6.0.0.1/6.0.1.x/6.0.2.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		

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

NOTE: Software version 6.0.3.x is compatible with RF Manager 6.7.769, but the 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: If with RF Manager 6.0.177 or later, you choose to use mismatched software versions, you should first turn off the WLAN Integration in RF Manager.

NOTE: Upgrading an MSM7xx Controller to v6.0.3.x will also automatically upgrade any MSM325 and MSM335 Sensors it manages to MSM software v6.0.3.x.

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

GMS support for teaming

GMS 6.0.3.0 supports teaming in MSM software 6.0.3.0 with the following limitations:

- **Only the team manager controller is supported.** GMS interacts only with the team manager controller and not team 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 6.0.2.0 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 6.0.2.0 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.

Fixes

This version includes fixes to the following issues:

- The web interface generates critical errors when using the Paypal feature and HTML authentication.
- An active directory user that belongs to several active directory groups, fails to authenticate as belonging to a child domain while the controller is joined to the parent domain
- (Applies to teaming.) The team manager controller periodically backs up its events database to all team member controllers. It was possible for this backup operation to timeout on a team of MSM720 controllers handling many access controlled clients.
- (Applies to teaming.) High CPU utilization in a teamed environment with IMC/WSM can cause controllers to become unresponsive or restart.
- Radios that have lower-than-normal signal levels are not reported in a `Radio down` alarm.
- The **Controller VSC** > **Wireless Clients** page does not list any clients connected even though some are connected.
- Accounting requests of non-access-controlled clients on a VSC configured for 802.1X authentication with an external RADIUS server, does not include the class attribute.
- Missing SNMP OIDs:
  colubris802dot11: 1.3.6.1.4.1.8744.5
  colubrisVirtualApMIB: 1.3.6.1.4.1.8744.5.1
- A user is able to authenticate after revoking the client certificate.
- In high-traffic environments, false `Radio down` alarms are raised.
- (Applies to MSM720.) During periods of high CPU usage, the MSM720 home page might not update the authentication system information.
- In Japan, restricted 802.11j channels are visible.
- In a Microsoft DNS environment with a parent domain and at least two child domains, users may be unable to connect.

- When Radio Resource Management is enabled, some APs might reject configuration settings from the controller and cause the controller to reboot.
- Spaces are not allowed in the user name for HTML authentication.
- The system log lists repetitive occurrences of a message similar to this:

  ```
  Unexpected Termination for process "dhclient -cf /etc/maestro -dhclient.conf
  -d hostname CN15DWY10C -q eth0.108" (pid 18656, up for 1 sec(s))
  ```

- (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.
- Mobility Traffic Manager client data path setup issues occur when two controllers are involved.
- Internet port bandwidth control now applies in the downstream direction when the VSC uses a VLAN for the egress mapping.
- 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).
- In certain upgrade scenarios, it is possible for the RADIUS server configuration to be configured with an invalid server.
- (Applies to teaming.) When the team manager shuts down, the AP moves to a team member. The client remains connected, but traffic stops and the client status appears as `Blocked: Home network unknown`. When the team manager reboots, the client remains in the blocked state.
- (Applies to teaming.) Clients associated with a non-access controlled VSC protected with 802.1x authentication are disassociated and can no longer re-associate after teaming has failed over from one team manager to an alternate controller.

Issues and workarounds

These issues are present in this release:

- The MSM controller blocks the authentication of all VSC users when a user authentication is initiated with an active directory server and the user belongs to the parent group as well as the child group but the child groups domain controller is unreachable from the MSM controller.
- The SOAP command `ExecuteWirelessDisassociateClient` might fail if there are more than 1,000 clients.
- When a controller location is set to Morocco, APs can fail to synchronize when a radio is set to 802.11n and the 5 GHz band is being used for local mesh.
- AP group names longer than 20 characters can prevent IMC from properly communicating with the MSM7xx Controller.
- (Applies to teaming with access-controlled clients.) Under conditions such as heavy DHCP request volume, the controller logs a false duplicate IP address error, even though no other client has the same IP address. This causes the client to be removed.
- Changing the address type (static/DHCP) or IP address of the network interface can result in the DHCP relay being unsynchronized with the controller. When this occurs, wireless clients are unable to obtain an IP address because the DHCP server transactions are never completed.

  As a workaround, reboot the controller or disable and then re-enable the DHCP relay.
- An attempt to configure a new VSC or modify an existing VSC when the AP channel is dynamically changed due to DFS, can result in a configuration error.
- The automated workflows for **Creating a wireless network for employees** and **Creating a wireless network for guests** do not allow RADIUS secrets up to 64 characters long as indicated on the **Authentication** > **RADIUS profiles** page. The limit is 16 characters.

- One-to-one NAT entries no longer work after a power loss or reset.
- 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.

  As a workaround, remove the device information from the web GUI for the AP using **Device management** > **AP management**. The AP resynchronizes.
- (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.

  As a workaround, manually change Radio 1 back to its original setting. For example, if Radio 1 was set to 2.4 GHz b/g in the working scenario, select **Controlled APs** > **Radio Management**, select the AP, and then set its radio mode.
- (Applies to MSM410, MSM430, MSM460, MSM466, MSM466-R.) When the first VSC is bound to an access point group but not enabled, autochannel can use channel 36 only.
- If a user deletes a RADIUS profile and re-creates it with a new secret key, this setting does not come into effect until a subsequent modification is made to the RADIUS profile.
- In high traffic environments, DNS resolution by the controller can cause authentication delays and require multiple retries by clients.
- The controller continues to respond to DHCP requests on the LAN port after that feature has been disabled.
- An MSM710 controller might reboot when 14 or more fixed leases are added.
- The controller uptime value in the management tool is different from the value retrieved using IMC.
- A wireless client moving to a wired connection is not asked to re-authenticate when using 802.1x and an external Active Directory server, but it should be.
- Using SOAP commands directed to a non-configured IP address causes SOAP to fail and add an error message similar to this to the controller log:

  ```
  websoap: SOAP FAULT: SOAP-ENV:Client "Internal error"
  websoap: Unable to communicate with IPRulesMgr,  Timeout occurred.
  ```
- When using sFlow, an error message regarding `kernel emergency` is incorrectly displayed and can be ignored.
- (Applies to teaming.) The team manager controller can lose its default route when a static IP address is assigned to the Internet port.
- The SOAP command `GetAuthenticatedusers` provides erroneous results for bytes sent and bytes received.
- (Applies to MSM410.) The MSM7xx Controller 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.
- When using HTML authentication, the **Continue browsing** link incorrectly redirects the wireless client back to the home page.
- (Applies to teaming.) When teaming is enabled, HTML authenticated users are incorrectly redirected to the Login page after clicking **Continue Browsing** on the Welcome page.
- The power displayed in the radio map of a specific AP web page could be inaccurate. The power in the radio map at the group level is reported correctly.
- When SNMP is processing a query with a large response, the controller will not respond to SNMP queries from other sources on the network until the current operation is completed.
- Rogue APs cannot be authorized using the CLI and the following error message is logged:

  ```
  IDS CLI - cli: DB: database is locked (DB_IDSReadAPAuthorizationTable)
  ```

- (Applies to MSM720, MSM760, and MSM765 zl Controllers in teaming mode.) Slave controllers in teaming might not sync with the interim master to form the team. Rebooting the unsynchronized controller resolves the issue.
- In configurations that include an MSM466-R, assert messages appear in logs when upgrading from v5.7.3.0 to v6.0.2.0. These messages can be ignored.
- IDS reports the following warning log messages which can be ignored:

  ```
  ids_sensor gets a lots of warning logs: [err_channel]802.11a Erroneous
  channel [1], Interface [r1v16], PrismChannel [36]
  ```

- With IDS, users cannot manually classify a **Rogue** AP as **Authorized** (Manual).
- When IMC establishes a connection to the 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.
- After a reboot, not all APs synchronized to a controller report as **Already Seen**.
- (Applies to teaming.) Controllers in a team with several hundred APs may experience trouble with connections to IMC.
- MTM is not supported when APs are adopted by controllers using NAT.
- 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.
- In controlled mode, the filter settings for the web system log shown at the AP level do not work. The default values are always used (severity level higher than or equal to warning). As a workaround, use a remote system log server to capture AP system logs below warning level.
- (Applies to MSM720, MSM760, MSM765 zl.) 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.
- (Applies to MSM720, MSM760, MSM765 zl.) In some cases, the network subnet information about rogue APs reported by the intrusion detection system (IDS) is incorrect. The IP address will display as 0.0.0.0.
- (Applies to MSM720, MSM760, MSM765 zl.) In the system logs page, only the logs local to the manager show up when selecting **Team** in the network tree. Selecting **Controllers** shows logs for all members. Directly selecting the manager controller shows no logs.
- Clients using the PPTP VPN server might experience connectivity issues when sending large packets.
- The SNMP OIDs that report information about the configuration of the Autochannel features “COLUBRIS-DEVICE-WIRELESS-MIB coDevWirIfStaAutoChannelEnabled” and “coDevWirIfStaAutoChannelInterval” may report incorrect information on the MSM410, MSM430, MSM460, MSM466, and MSM466-R.
- 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. This affects the MSM410, MSM430, MSM460, MSM466, and MSM466-R. There is no workaround.

- Wireless clients connected to a VSC that is directly mapped to a VLAN are unable to reach wired clients on the same VLAN.