HP MSM7xx Controllers Release Notes
v6.0.2.2

HP Part Number: 5998-5069
Published: May 2014
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.

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

Version: MSM v6.0.2.2

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 v6.0.2.0 software will disable the NAT feature. It is recommended that you review your existing settings and disable one of these features before upgrading to v6.0.2.0.

Updating software

Update the controller software as described in the "Software updates" section of the *MSM7xx 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 6.0.2.x 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 6.0.2.x, those changes will not be present when you downgrade to the previous version.

If you factory reset your device after upgrading to version 6.0.2.x, 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 6.0.2.x works with and is required for MSM software version 6.0.2.x. 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 higher. 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)
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	Upgraded automatically by RF Manager	Upgraded automatically by MSM7xx Controller
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 6.0.2.x is compatible with RF Manager 6.0.177 and RF Manager 6.7.x, 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 above, you choose to use mismatched software versions, you should first turn off the WLAN Integration in RF Manager.

NOTE: Upgrading an MSM7xx Controller to v6.0.2.x will also automatically upgrade any MSM325 and MSM335 Sensors it manages to MSM software v6.0.2.x.

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

GMS support for teaming

GMS 6.0.2.x supports teaming in MSM software 6.0.2.x 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.

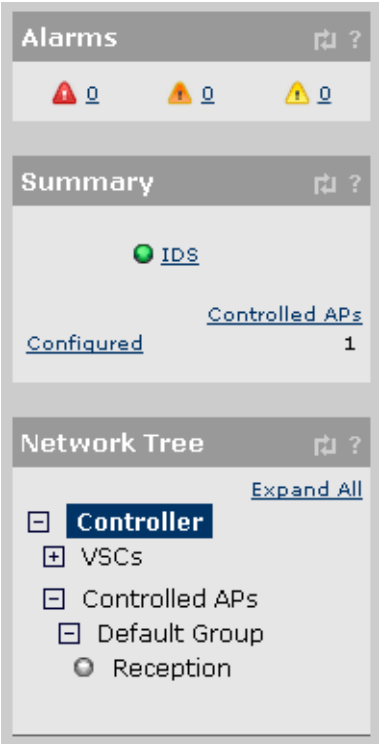
Changes to the management tool interface

A number of recent changes have been made to the management tool interface to support the addition of new features and to enhance usability. The following is an overview of the key changes.

For a description of each new feature, consult the *New in release 6.0.0.x* section of the *MSM7xx Controllers Configuration Guide*.

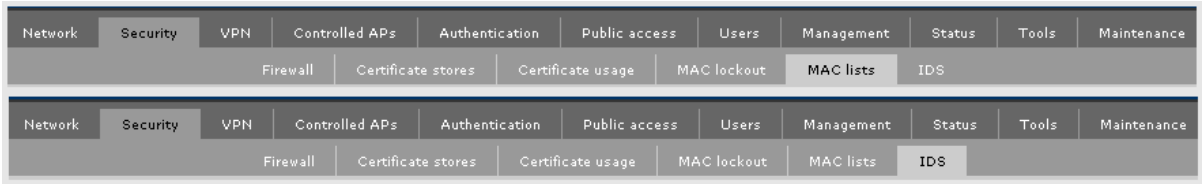
Changes to the left pane

- An **Alarms** box has been added above the **Summary** box.
- The **Summary** box now includes status information for the new IDS feature.



Changes to the Controller menu

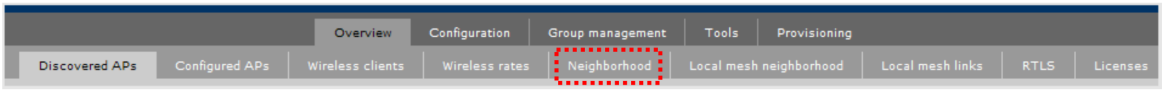
- Two new items have been added to the **Controller >> Security** menu: **MAC lists** and **IDS**.



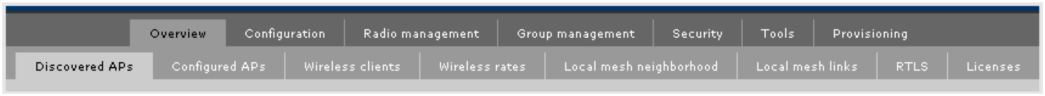
Changes to the Controlled APs menu

- **Overview menu:** The **Neighborhood** page has been moved from the **Overview** menu to the new **Security** menu.

Previous release

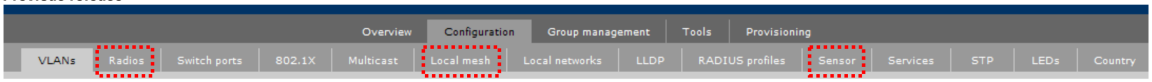


This release



- **Configuration menu:** The **Radios** page has been moved from the **Configuration** menu to the new **Radio management** menu and renamed to **Radio configuration**. The **Local mesh** page has been moved from the **Configuration** menu to the new **Radio management** menu. The **Sensor** page has been moved from the **Configuration** menu to the new **Security** menu.

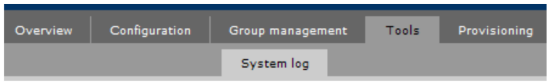
Previous release



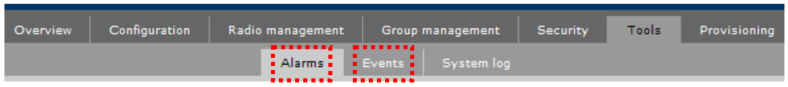
This release

- **Tools menu:** The new **Alarms** and **Events** features have been added to the **Tools** menu.

Previous release

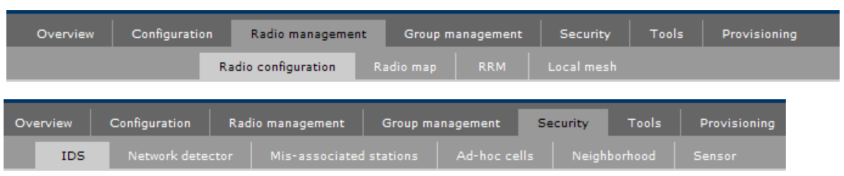


This release



- **New menus:** Two new menus have been added: **Radio Management** and **Security**.

  The **Radio management** menu provides access to radio-related configuration options that were previously on the **Configuration** menu, and includes two new features: **Radio map** and **RRM**. The **Security** menu provides access to the **Neighborhood** and **Sensor** configuration options that were previously on the **Overview** and **Configuration** menus, and includes options for the new IDS feature.



Fixes

This version includes fixes to the following issues:

- The MSM Controller reboots after running **WPA Termination** for an extended period of time (longer than 24 hours).
- (Applies to MSM720, MSM760, MSM765 zl in teaming mode.) Enabling **Access Control** on a VSC with WPA termination and using MTM tunnel user traffic to home VLAN may cause a controller reboot.
- (Applies to MSM720, MSM760, MSM765 zl in teaming mode.) IP routing cache does not flush, potentially causing the controller to behave sluggishly after 24 hours of use.
- An MSM Controller does not send disassociation messages from a Bradford Sentry authenticator to a wireless user.
- The AP **Load Balancing** feature in RRM does not function properly, causing an uneven distribution of clients amongst APs.
- When **Band Steering** is enabled on a VSC and the number of clients connecting to an AP is 100 or more, all association requests are rejected.
- MSM APs are unable to be reclassified as **Authorized** on IDS.
- Aeroscout tags connected through a WDS AP can not be seen in **Mobile View**.
- Wireless clients streaming data or downloading large files may get disconnected, and the following messages are shown in the system log:

  ```
  iprulesmgr: Keep-Alive for station (ip-address='x.x.x.x') failed
  iprulesmgr: Terminating session (session-time='198') for user
  ```

- With **Mobility Traffic Manager** (MTM) enabled on one VSC, users connecting to a non-MTM-enabled VSC may get blocked trying to reach other network resources.
- When an AP is configured to egress traffic on a given VLAN, the wireless clients connecting to the AP fail to receive an IP address from the external DHCP server.
- (Applies to MSM720, MSM760, MSM765 zl.) When teaming is enabled, the following message appears in the system log:

  ```
  GetNewDatabaseConnectionObject: Cannot create the database connection
  object for <IP addr>'
  ```

  This message can be ignored.
- The number of wireless clients shown on **VSC >> Overview > Wireless clients** is not accurate.
- (Applies to MSM720, MSM760, MSM765 zl in teaming mode.) The MSM Controller reboots randomly when L3 roaming is enabled.
- On a wireless deployment with 200 or more access points, after a firmware upgrade to 6.0.1.0, the access points can't synchronize back to the MSM Controllers.
- (Applies to MSM720, MSM760, MSM765 zl.) When a team is configured to authenticate users against an external Active Directory server, it shows an empty Active Directory “joined” status.
- When an access-controlled VSC gets the **Access Control** option removed, the DHCP Server and DHCP relay configuration options are not disabled.

- When trying to downgrade firmware from Version 6.0.x to Version 5.7.x using the Command Line Interface, the controller reboots but does not actually downgrade the firmware.
- The controller GUI may become unresponsive, and the system log reports the following message:

  ```
  monitord Stopping [3,8]: 'webs' [pid 917, up for 188709 sec(s)]
  ```
- When MTM is enabled on a VSC, wireless users are unable to reach network resources (navigate).
- When upgrading from Version 5.5.x to 6.0.x, the **Zero Config** feature is disabled and needs to be re-enabled in order to be used.
- (Applies to MSM720, MSM760, MSM765 zl.) When a VLAN interface is created on the primary controller of a team, the secondary controllers cannot synchronize to the team.
- (Applies to MSM720, MSM760, MSM765 zl.) The IP address for a VLAN interface can not be set on a controller after it has been set up for teaming (even after the controller has left the team).
- (Applies to MSM720, MSM760, MSM765 zl.) The primary controller on a team is unable to remove IDS AP authorization on the secondary controllers.
- The MSM Controller experiences high CPU utilization and eventually reboots when IMC or a similar SNMP intensive software is used to manage the controller or a team of controllers.
- If RRM is enabled, and a controlled AP is configured to use a reserved DFS channel when a radar event is detected, the AP will shut down the radio instead of switching to a different, available channel.
- (Applies to MSM720, MSM760, MSM765 zl.) VLANs cannot be added to a controller if the controller was removed from a team and set to operate in standalone mode.
- (Applies to MSM720, MSM760, MSM765 zl.) Controllers are unable to team when the subscription plan is configured on the primary controller.
- After running an RRM analysis, the list of detected foreign APs cannot be filtered by MAC address.
- When IMC is used to manage the controller, APs may appear grayed out on the **Controller >> Controlled APs** page.
- The IF-MIB SNMP MIB does not contain accurate descriptions for all interfaces.
- Management software such as PMM or IMC may not display all information properly.
- When an MSM Controller is upgraded to a 6.x version from an older version where the **Access Point Name** is not an available option for the System name (**Controlled APs >> Configuration > LLDP**), the **Access Point Name** option should not appear as Enabled.
- HMAC tag secret is now configurable in the Internal Public Access web server.
- There is no RF Manager version 6.7 sensor software update for the MSM325 and MSM335 sensors. An error indicating that there is a version mismatch may be displayed, but the sensors will continue to operate normally.
- The MSM Controller sends RADIUS accounting-request messages without setting a value for the "input/output packets" attribute.
- (Applies to MSM720, MSM760, MSM765 zl in teaming mode.) When a set of MSM Controllers is configured to create a team and communicate using the LAN port, the secondary controllers may fail to synchronize to the primary controllers.
- RRM is not able to automatically configure the settings for a given radio unless 3 co-channel neighbor radios are detected.
- When IDS is enabled, the following error messages are displayed on the system logs:

  ```
  <ip-address>crit store-devices: <serial#> Unable to get type definition
  for type=3a37463a32435d0d
  ```

  ```
  <ip-address>crit store-devices: <serial#> assert:
  payloadserializationapi.c PayloadGetSerializedSize 197
  ```

- The **VSC>>Overview>Wireless Clients** page fails to load when there are more than 3,000 users.
- When RRM is enabled, the following message appears multiple times on the system log:

  `warn rfmgr_sc (radio-tracking-node) Reporter xx:xx:xx:xx:xx:xx unknown`
- (Applies to MSM720, MSM760, MSM765 zl in teaming mode.) When multiple teams of MSM Controllers synchronize to a single iMC server using WSM, the second and subsequent teams of MSM Controllers fail to synchronize with the iMC server.
- MSM Controllers allow the removal of a MAC list that has already been applied to a MAC filter.
- The RRM network completeness analysis may take longer than expected (up to 3 minutes).
- On a system with 1,000 or more RRM radios, CPU utilization may increase by 20% over operation without RRM.
- The message `maximum simultaneous number of RADIUS Requests waiting for answer have been reached` appears when too many RADIUS clients go offline without closing the session properly. The controller sends RADIUS Accounting packets for these idle clients, and they were never cancelled.
- APs exposed to high RF noise fail to return to the default channel that was configured by RRM.
- The following OIDs contained within the COLUBRIS-DEVICE-WIRELESS SNMP MIB object have the same description:

  coDevWirCliStaTrafficAuthorized

  coDevWirCliSta8021xAuthenticated

  coDevWirCliStaMACAuthenticated

  coDevWirCliStaMACFiltered
- If the MSM Controller is configured to use 0.0.0.0 as the DNS server, the APs will reboot.
- The **Duration** column on the **Access Point > Wireless Clients** page incorrectly shows "HH:MM:SS" instead of the actual wireless user connection time.
- Usernames with 30 or more characters are not displayed correctly on the **Wireless Clients** table (**Controller >> Overview > Wireless Clients**).
- After an upgrade, the following assert error message is displayed on the system log after all access points get synchronized to the controller: `assert: rmam_channel_sm.cpp RMAMScanChannelChangeComplete 170 (siContext != NULL).>`.
- When the team leader fails over to an alternate leader, RRM is not updated with the new leader's information and the following error message is displayed on the system log: `store-devices: Client '44:1E:A1:C2:A2:CE' skipped sending entries '12273' to '12281'.`
- An incorrect error message is reported if the user tries to start an RRM analysis while an RRM plan application is in progress. The error reads, `An internal software error occurred` instead of `Cannot start RRM analysis, please wait for the plan application to complete`. In addition, the system log will contain an entry, such as: `<date> <time> err rfmgr_sc:Unexpected RPC return code:-33.`
- The wireless MAC filter for a VSC has been extended to support 256 MAC addresses (instead of the previous limit of 64).

Known issues

These issues are present in this release:

- (Applies to all MSM7xx Controllers.) 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.
- (Applies to all MSM7xx Controllers.) 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.
- An MSM710 controller might reboot when 14 or more fixed leases are added.
- (Applies to all MSM7xx Controllers.) 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 MRM466-R, assert messages appear in logs when upgrading from 5.7.3.0 PMR to 6.0.2.0 PMR. 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 MSM 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 the APs synchronized to a controller report as **Already Seen**.
- 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.