HP MSM7xx Controllers Release Notes
v5.7.4.0

HP Part Number: 5998-5725
Published: March 2014
Edition: 1

Acknowledgements

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

Version: MSM v5.7.4.0

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 AP 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 Center 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 5.7.4.0 from version 5.7.2.0 or earlier, 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 the following 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 v5.7.4.0 software will disable the NAT feature. These two features are incompatible, and the combination although not validated prior to 5.7.1.0 is now enforced. HP recommends that you review your existing settings and disable one of these features before upgrading to v5.7.4.0.

Updating software

Update the controller software as described in the "Software updates" section of the *MSM7xx Controllers Configuration Guide*. When the controller is updated, it automatically updates all of its controlled devices to the same software version.

Downgrading software

If you upgrade to version 5.7.4.0, and then want to return to the version that you had been running prior to upgrading, the configuration that you used originally with that version will still be available.

If you have made configuration changes while using version 5.7.4.0, those changes will not be present when you downgrade to the previous version.

If you factory reset your device after upgrading to version 5.7.4.0, 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: 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 5.7.4 works with and is required for MSM software version 5.7.4.0. 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)
5.7.4.0	6.0.185	Upgraded automatically by RF Manager	Upgraded automatically by MSM7xx Controller
5.7.1.x/5.7.2.0/5.7.3.0	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: If, with RF Manager 6.0.x you choose to use mismatched software versions, you should first turn off the WLAN Integration in RF Manager.

NOTE: Upgrading an MSM7xx Controller to v5.7.4.0 automatically upgrades any MSM325 and MSM335 Sensors it manages to MSM software v5.7.4.0 and sensor code to v6.0.185.

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

Clear web browser cache before launching management tool

In the management tool the Automated Workflow pages use updated JavaScript files. If your web browser cache contains old versions of these files you might see JavaScript errors. If this occurs, clear your web browser cache and re-launch the management tool.

Configuring Teaming on the MSM720

For important information on how to configure Teaming on the MSM720, consult the *Controller teaming* chapter in the *MSM7xx Controllers Configuration Guide*. Note also that these sections in the *MSM7xx Controllers Configuration Guide* supersede MSM720 teaming-related information in the management tool online help.

GMS support for teaming

GMS 5.7.4 supports teaming in MSM software 5.7.4.0 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.
- On the **Service Controller** tab, the two items **IS_TEAMED** and **MANAGER_STATE** should be ignored because they are not accurately updated.

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. Although not available in MSM software version 5.7.0.x, the following SOAP function calls are re-enabled in MSM software version 5.7.3.0 or later, some with limitations as follows:

- 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 5.7.4.0, 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.

Required changes for custom pages

The product now encodes the required form parameter with an HMAC tag that is calculated over the URL and a secret that precedes the URL. The product also now validates that the tag is present in the request before using the associated URL.

Due to the complexity of those pages and the flexibility offered by our Public Access HTML pages mechanism, the upgrade of those page cannot be done through software. In addition, the source of those pages may be located outside of the product. As a result, manual steps are required by the owner of those pages to modify them to ensure that they properly use the new ASP (server-side function) to prepend the HMAC tag.

When using custom pages (i.e. defined by site attributes login-page, custom-pages) that run within the controller but are sourced elsewhere, or if you have customized the pages within the controller, you must make the following changes:

1. Locate and edit the HTML page containing the post towards the "/goform/HtmlLoginRequest" (in the factory provided page it would be the "index.asp" file). Then, modify the occurrence of the HTTP form variable specification for the variables "success_url", "error_url" and "subscription_url" as follows:

Originally...	Change to...
`<input type="hidden" name="error_url" value="/index.asp" />`	`<input type="hidden" name="error_url" value="<% AspCreateHMACPair("/index.asp"); %>" />`
`<input type="hidden" name="success_url" value="<% write(GetWebFullURL("http")); %>/transport.asp" />`	`<input type="hidden" name="success_url" value="<% AspCreateHMACPair(GetWebFullURL("http"), "/transport.asp"); %>" />`
`<input type="hidden" name="subscription_url" value="<% write(GetWebFullURL("https")); %>/subscribe.asp" />`	`<input type="hidden" name="subscription_url" value="<% AspCreateHMACPair(GetWebFullURL("https"), "/subscribe.asp"); %>" />`

2. In the set of pages provided to you as example, there are two other occurrences under the page name "purchase_approved.asp" and "purchase_failed.asp". You will want to proceed with the same change for the variables found there since they are using the same HTTP form action value, "/goform/HtmlLoginRequest" (as shown below):

Originally (purchase_failed.asp and purchase_approved.asp)...	Change to...
`<input type="hidden" name="error_url" value="/index.asp" />`	`<input type="hidden" name="error_url" value="<% AspCreateHMACPair("/index.asp"); %>" />`

3. After you have made the necessary changes to remote pages that run within the controller but are sourced elsewhere, you must retrieve the modified pages to the controller before they can be used.

NOTE: If you are using a remote "login-url" to provide HTML authentication and you are sending "error_url", "success_url", "subscription_url", or "original_url" from a remote server, they will not be used. You must configure the local page equivalent (index.asp, transport.asp, subscribe.asp) which will be used. The "original_url", which provides redirection to the page entered by the user prior to authentication will not work.

Teaming fixes

The following teaming-related issues are fixed in this release:

- Network Address Translation (NAT) is not applied to traffic on access-controlled VSC with an egress VLAN defined, when the wireless client connects through a team's secondary controller.
- Teaming failover causes Mobility Traffic Manager (MTM) clients traffic to stop, even after the AP is adopted by alternate manager controller.
- APs adopted by a team member may appear to be in the "pending" state on the GUI, even though the APs are operating and providing service.
- The team manager controller can lose its default route when a static IP address is configured on the Internet port.
- Enabling teaming on the MSM760 may cause an incorrect DHCP lease to the Internet Port when it has a VLAN tagged on it.
- APs located remotely (synchronized through layer 3 connectivity) may lose synchronization to a team of MSM controllers.

- When teaming is enabled and SNMP is used to poll the “ipAddressIfIndex” MIB, the "tun1" interface returns a value of -1.
- When a new VSC is added on a team of controllers, the adoption of APs may take longer than 5 minutes and the following error message may be displayed on the system log: `Local1.Critical 10.214.2.78 kernel: CN18DWY0JG Invalid VSC unique ID received = 0.`
- Wireless clients cannot roam from an AP that is synchronized to a secondary teamed controller to an AP that is synchronized to the primary controller on the team.
- When a mobility domain (MTM) groups with teamed controllers and each MSM controller is configured to egress traffic on a different VLAN, ARP responses to wireless clients are not on the egress VLAN.
- When using teaming, if a non access-controlled VSC binding is removed from an AP group, the following error message repeatedly appears on the system log until the APs in the group are rebooted: `iwtest: WIRELESS_get_private_int(wvlan0) cfgerr:(101) syserr:(Network is unreachable).`
- A wireless client connected to an AP that is synchronized to the team's primary controller looses network connectivity if the primary controller reboots and the AP is synchronized to a secondary controller.
- When using teaming, the **Controller >> Public Access > Web Content** does not allow saving a customized page and returns the following error message: `The user account creation limit is invalid.`
- When a team of controllers is upgraded, APs adopted by a secondary controller may not be adopted by the same controller and require adoption by the primary controller.

Other fixes

The following other issues are fixed in this release:

- The AP is not sending LLC SNAP frames to the switch when a wireless client associates.
- Software updates timeout when using Google Chrome unless the refresh feature is disabled.
- Wireless users authentication requests are not shared between Active Directory trusted domains.
- The "GetAuthenticatedusers" SOAP command provides erroneous results for bytes sent and bytes received.
- After an upgrade, APs may become unsynchronized and not resynchronize when APC (Automatic Power Control) for APs is enabled.
- The controller logs the following messages and possibly reboots:

```
monitord: Stopping [1,5]: 'iprulesmgr -f -t 10 -i br0' [pid 8848, up for 167 sec(s)]
monitord: Starting [1,2]: 'iprulesmgr -f -t 10 -i br0' (pid='8966')
```

- Clients using HTML authentication do not get the Welcome page when they use an External SSL Certificate that has hostnames containing upper case letters.
- 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.
- 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 an MTM visitor and block their traffic.
- When using HTML authentication, the "Continue Browsing" link on the Welcome page erroneously redirects an authenticated user back to the login page.
- SNMP MIB for LLDP returns LldpChassisIdSubtype MAC address in an incorrect format.

- IMC is unable to draw a topology diagram because SNMP ifOperStatus MIB erroneously returns "DOWN."
- System uptime shown in the management tool does not match the uptime retrieved through SNMP.
- When configuring an 802.1x VSC using SOAP, it is not possible to set the "Station ID delimiter" or the "Station ID MAC."
- A VSC with Opportunistic Key caching (Fast Roaming) enabled, fails to authenticate users against certain RADIUS servers.
- After a software upgrade, an AP may drop packets from user VLAN over the AP tagged management VLAN.
- 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."
- SNMP process causes high CPU and high memory usage, which can cause the controller to reboot.
- When a customized URL is created for a public access VSC, the controller erroneously sends an empty NAS-ID value.
- Rate limiting of the ingress VLAN configured on the RADIUS server does not get applied when the user is authenticated.
- 802.1x authentication of new wireless clients may fail intermittently when configured on a non-Access Controlled VSC.
- (Applies to MSM410, MSM430, MSM460, MSM466, MSM466-R.) APs get "configuration commit timeout" message intermittently when operation modes (WDS, Access Point, Monitor) are changed using SOAP commands.
- If a VSC is bound to an AP group when MTM is enabled, clients connecting to the VSC may experience problems leasing an IP address from an external DHCP server.
- When an unauthorized wireless client uses a web browser configured with an external proxy server attempts to navigate to an HTTPS web page, the controller ignores the request but does not redirect the client to the authentication web page.
- When HTTP proxy is enabled for public access users and HTTP connections are prematurely closed (clients are requesting too many web pages in a short amount of time), it may cause a crash of the HTTPproxy process, as shown in the following system logs:

  ```
  httpproxy: assert: proxy.c HandleIPRulesMgrIPCHTTPProxyResponse 3543
  (aConnection->mServer.mSocket != -1)
  ```

  ```
  httpproxy: assert: proxy.c SendRequest 1639
  (aConnection->mServer.mSocket != -1)
  ```
- When HTTP proxy is enabled for public access users, the following log message is displayed on system log: `assert: proxy.c OpenServerSocket 2106 (aConnection->mServer.mSocket == -1).`
- The HTTP proxy process incorrectly limits the number of supported connections to 1,024.
- RADIUS login credentials are appended with a space, causing the RADIUS server to fail authentication.
- On the MSM720, when an ethernet interface is changed from one group (trunk) to another (**Controller >> Network > Ports**), the VLAN mapping from the previous group is not removed.
- When the Zero Config is enabled (**Controller >> Public Access**), the controller displays the following error message on the system log: `assert: proxy.c OpenDNSResolveIPCSocket 2388`

`(errno != EMFILE). socket() with Connection 32103 ipc failed: Too many open files (24).`

- When a Mobility domain is created and an unknown wireless client connects to a VSC, the following incorrect error log message is displayed: `the client is blocked to unknown VLAN ID was returned`.
- Updated OpenSSH version to 6.1.
- The web interface is not accessible when the browser only supports Transport Layer Security, version 1 (TLSv1).
- When a new VSC is created and APs are synchronized to the controller, the following error messages are displayed on the system log:

  `IAPP could not get SSID status`

  `IAPP Could not allocate vap record`

  `Failed to read VSCs configuration`
- When APs are configured to use automatic channel selection and create a Local Mesh link, if one of the APs reboots, the local mesh link is not restored when the AP is back online.
- The Cambodia country code does not show up on the available country list.
- If the "Display free access" option is enabled when configuring **Controller >> Public Access > Web Content**, the web does not allow changing the value for the account validity time.
- Not all of the sort by column options available on the **(AP Group) >> Overview > Wireless Rates** page are operational.
- After upgrading, 802.11b/g data rates are automatically disabled from the radio, preventing wireless clients (802.11b/g only) from connecting to the VSC.
- If an MTM-blocked user performs a DHCP lease request on a VSC that is configured to egress VLAN, the DHCP server provides an IP address instead of blocking the DHCP transaction.
- On the MSM720, after using the `show vlan` command on the CLI, the following error messages appear on the system log:

  `assert: cfg.c AllocCfg 122 (internalData && !*internalData)`

  `assert: Clean the pointer before calling AllocCfg, Struct Type 28`
- The "Mobility Clients" table on the web (**Controller >> Status > Mobility**) incorrectly displays information for MTM-blocked clients.
- When MTM blocks a wireless user, the web incorrectly displays the user as "Connected" on the Mobility Clients table (**Controller >> Status > Mobility**).
- When band-steering is enabled on the controller, it may return error messages indicating that the maximum number of clients on a radio has been reached.
- MSM controllers may present high CPU usage due to a process named "statspoller" and the number of wireless clients increases to (400 or more).
- After upgrading, the MSM controller may display the following error message on the system log: `Query error on PublicAccessUser status table`.
- When using the CLI command, `disassociate controlled-ap wireless client [MAC]`, the following error message is displayed on the console: `Invalid system action <180>`.
- The MSM controller does not allow using a URL or FQDN server name when configuring an external system log server.
- Extended SOAP functionality to support retrieving of wireless users session ID.
- The values returned for SNMP queries to MIB objects “ipAddrTable”, “ipAddressTable”, and “ifTable” are not the same.

- If the name of a local mesh profile is left as a blank space, the controller does not allow changes to be made to profile settings after saving the configuration.
- The controller ignores the values configured for the "Primary-DNAT-Server" RADIUS attribute.
- RADIUS accounting "STOP" messages sent by the controller to an external RADIUS server do not include the input/output values as part of the message.
- If a controller is unable to find its configured DNS during startup, the 802.1x user connections to an external RADIUS server are rejected, and the following error message is displayed: `Discarding RADIUS Access Request due to failure to resolve the primary address of the associated RADIUS profile (name='').`
- The changes to the "Default user data rates" setting applied to an access-controlled VSC do not immediately impact wireless users after saving the configuration.
- When using 802.1x and opportunistic key caching, the following message appears multiple times on the system log: `Discarding RADIUS Request (id='157') from RADIUS Client (ip-address='169.254.0.50',port='32771') as the maximum simultaneous number of RADIUS Requests waiting for answer have been reached.`
- Users accounts that are authenticated using 802.1x and have been inactive for a long period of time (1 hour or more) show up as Active at **VSCs >> Overview > User Sessions**.
- The number of users reported at **VSCs >> Overview > User sessions** does not match the number of Authenticated users shown at the controller's Home page.
- When a less specific IP route (172.0.0.0/8, for example) is configured on the MSM controller after a more specific IP route (172.16.100.0/24, for example), the controller incorrectly gives priority to the more specific IP route.

Known teaming issues

The following teaming-related issues are present in this release:

- In teaming, with "Extend VSC egress subnet" enabled, team member replies to ARP broadcasts in NON-AC VSCs that use the default egress VLAN.
- When a team manager is restored with its previous teaming configuration, the elected manager continues to be the team manger with the teamm members synchronized to it. The workaround is to disable teaming on each member, and then enable teaming again.
- When teaming is enabled, HTML authenticated users are incorrectly redirected to the Login page after clicking on the **Continue Browsing** link on the Welcome page.
- If a team of controllers configured with default IP routes is upgraded from 5.5.x to 5.7.1.0, the team then fails to synchronize. This is due to the team members losing the team VLAN IP address and the team manager having static IP routes configured. As a workaround, manually re-add the team VLAN IP address to the team members, and remove the default routes (if any) from the team manager controller prior to the upgrade. Then, add the routes again after the controllers are upgraded and the team is formed.
- When teaming is enabled, team member controllers incorrectly report error messages in the system log that indicate that the controller is unable to resolve the external RADIUS server host name. Though error messages are displayed, the controller is capable of resolving the RADIUS server name.
- APs controlled by a team member controller report the serial number instead of the configured system name.
- When roaming from an AP managed by the team manager to another AP managed by a team member, wireless clients may experience a delay of up to 15 seconds when trying to reach other wireless clients on the same VSC.

- (Applies to PCM interacting with APs controlled by an MSM7xx Controller team.) You cannot use PCM to manually disable sampling and statistics for active sFlow agents on APs controlled by a team. As a workaround, use the management tool on the team manager, and disable the AP sFlow agent on page **Controller >> Tools > sFlow**.
- A controller that has DNS discovery settings defined on the **Controlled APs >> Provisioning > Discovery** page may be unable to synchronize with a team in the following two scenarios:
  - If the team members have different DNS discovery settings configured, the controller will not be able to synchronize.
  - If the team initially has no DNS discovery settings configured, the controller will be able to synchronize. However, if the DNS settings on the team are then changed, the controller will no longer be able to synchronize.
- Teaming redundancy is not implemented for the sFlow feature. Therefore, upon team manager controller failover to a team member, sFlow will be shown as disabled on the team member that is temporarily filling the master role. As a workaround, manually configure the team, enabling the temporary manager as the real manager controller, and enabling sFlow on this manager controller.

Other known issues

These other issues are present in this release:

- Broadcast and multicast traffic is blocked between MTM clients.
- Radius task might restart when 200 or more wireless clients are attempting to login simultaneously.
- Bandwidth limitation is ignored when the (max-input/max-output) attribute is assigned to the user account .
- Wireless clients on two different radios of an AP, that are connected to the same Non AC VSC with DHCP configured, and have "extend VSC egress subnet to VSC ingress subnet" set, are unable to communicate with each other.
- MTM is not supported when APs are adopted by controllers using NAT.
- APs may fail to be synchronized to the controller and display error messages in the system log similar to following: `crit maestro_sc assert: doublelinklist.c RemoveDoubleLinkedListNode 311`. As a workaround, restart the controller and try AP synchronization again.
- Wireless clients connected to an access controlled VSC are sometimes unable to reach the default gateway.
- If a wireless client is redirected to an external login server when using HTML authentication, an incorrect error message similar to the following appears in the system log: `The user is configured with an HTTP proxy yet the product is not configured with support for HTTP proxy therefore we cannot redirect this request.`
- When a wireless client roams from one AP to another, the controller fails to send a RADIUS accounting stop message to the external RADIUS server.
- The web interface under **Controller >> Overview > AP details** shows an incorrect number of connected wireless clients. As a workaround, get the statistics from another source (SNMP, for example).
- Local Mesh APs may fail to synchronize with the controller after a software upgrade. When this occurs, reset the affected APs by pressing the reset button or by power cycling them.
- When a controlled AP configuration is updated after a MAC address is added or removed from the allowed stations list, other wireless clients associated with the same VSC lose connectivity until they are reauthenticated. As a workaround, reauthenticate the wireless clients.

- Wireless clients connected to an AP adopted on the controller Internet interface are not able to ping and communicate with other wireless clients on the same VSC that are connected to an AP adopted on the controller LAN interface. As a workaround, use IP routes or external routing mechanisms.
- When a second VSC is added, wireless clients on the first VSC are not able to ping each other (although wireless clients can ping their default gateway and retain network connectivity).
- When sFlow is enabled, it cannot be disabled unless there is at least one controlled AP.
- The **show config** CLI command generates an **unable to read configuration** error in the management tool system log.
- (Applies to HTML authentication on an access-controlled VSC with Active Directory as the authentication server.) Authenticated users are not displayed on the **Controller > Controlled APs >> Overview > Wireless clients** page.
- (Applies to MSM410, MSM430, MSM460, MSM466, MSM466-R.) If a radio Channel setting of **Automatic** is enabled and all APs (affected by this issue) happen to boot up at the same time, for example after a power outage, then they are likely to end up on the same channel. This will happen mostly with autonomous APs. APs managed by an MSM7xx Controller are less likely to experience this. As a workaround, APs can be restarted/re-synchronized at specific intervals or fixed channels can be selected.
- (Applies to MSM720 with Mobility Traffic Manager (MTM).) Egressing traffic on the Internet network and Access network is not supported. Egressing traffic onto a user-created network profile is supported.

  (Applies to MSM710, MSM760, and MSM765 with Mobility Traffic Manager (MTM).) Egressing traffic on a network profile mapped to the Internet port is not supported. Egressing traffic onto a network profile mapped to the LAN port or mapped to any VLAN interface is supported.
- When setting the SNMP system log trap level below **Warning**, no traps will be generated.
- There is no Spanning Tree Protocol (STP) loop protection for the MSM720, so avoid interconnecting two or more ports that are on the same VLAN.
- VPN-based IPSec clients are unable to connect to MSM7xx Controllers, resulting in display of messages similar to this: **XAUTH wrong UserId or Password**.
- The maximum quantity of CA certificates and Client certificates that can be installed on the system is 50 certificates each. In some cases when adding more than 45 certificates of either type, the certificate names may disappear and an access error may be generated when selecting a different management tool menu. As a workaround, restart the controller.
- There is no SNMP MIB support for Port Trunking on the MSM720.
- (Applies to USA and Canada.) System Time is not being set back one hour when DST ends at 2:00 a.m. on the first Sunday in November.
- If you want to assign the Internet port as the Egress network in a VSC binding, it must have a VLAN. Mobility Traffic Manager cannot send user traffic onto the Internet port untagged.