HP MSM7xx Controllers Release Notes
v6.3.0.2

HP Part Number: 5998-5387
Published: December 2014
Edition: 4

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.

Version: MSM v6.3.0.2

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 / HP 425 Access Point product names.

Product models

This document applies to these HP products:

Model	Part
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
MSM775 zl Premium Controller	J9840A

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 6.3.0" 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), MSM335 (J9356A/B).

IMPORTANT: Prior to upgrading to MSM software version 6.3.0.x, 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 v6.3.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 v6.3.x or v6.2.x.

Updating software

Update the controller software as described in the "Software updates" section of the *MSM7xx Controllers Configuration Guide*. 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 6.3.0.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 6.3.0.x, those changes will not be present when you downgrade to the previous version.

If you factory reset your device after upgrading to version 6.3.0.x, your previous configurations will be lost, and when you downgrade to any previous version you will be in a factory reset state.

Bonjour feature

Support for the Apple Bonjour feature is added in this release. Support is provided in the form of a Bonjour gateway plus related traffic management and filtering capability. For more information, see "Managing Bonjour traffic" in the *MSM7xx Controllers 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 is not supported by the MSM710 Controller.

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 6.3.0.x works with and is required for MSM software version 6.3.0.x. See also "GMS support for teaming" (page 5).

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*, MSM325, MSM335)
5.7.5.0/6.3.0.x	6.7.769 or later	Upgraded automatically by RF Manager.	Upgraded automatically by MSM7xx Controller.
5.7.4.0/6.2.0.x	6.0.185, 6.7.769 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		

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

NOTE: Software version 6.2.0.0 and 6.3.0.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.

NOTE: If you choose to use mismatched software versions with RF Manager 6.0.177 or later, you should first turn off the WLAN Integration in RF Manager.

NOTE: Upgrading an MSM7xx Controller to v6.3.0.x also automatically upgrades any MSM320, MSM325, and MSM335 Sensors it manages to MSM software v6.3.0.x.

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

GMS support for teaming

GMS 6.3.0.x supports teaming in MSM software 6.3.0.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

Version 6.3.0.2 includes the following change:

- 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

There are no additional fixes included in Version 6.3.0.2.

Version 6.3.0.1 includes fixes to the following issues:

- (Applies to HP 425.) The potential for a flash memory error was detected in the software. This error has a low probability of occurrence, but if it does occur, the unit might reboot.
- The HP 425 Access Point spontaneously reboots every few days.
- (Applies to Radio Resource Management (RRM).) Online help for channel difference has been clarified to match the implementation.
- When using a local mesh link between two or more APs and following the application of a new channel allocation plan, the slave AP might disconnect from the master at periodic intervals. Although it reconnects a few seconds later, this has a negative impact on traffic carried through the link.
- (Applies to teaming.) During the synchronization of the controllers, it is possible that HP 425 APs attempting to discover their controller are not able to do so, and are stuck in this discovery phase until the whole team of controllers is rebuilt.
- If **Terminate WPA at the controller** is enabled in a VSC, the controller may randomly reboot.
- When an AP loses the communication channel with its controller and then reconnects, wireless clients that are still connected to the AP through a Mobility Traffic Manager (MTM) VSC will have their traffic blocked by the AP.

- (Applies to MSM422.) 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 HP 425, MSM410, MSM422, MSM430, MSM460, MSM466, MSM466-R.) An access controlled VSC using MAC-based authentication with the MAC filtering **ALLOW** option enabled, allows clients to connect.
- 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.
- The MSM Controller reboots after running **WPA Termination** for an extended period of time (longer than 24 hours).
- (Applies to teaming.) Enabling **Access Control** on a VSC with WPA termination and using MTM tunnel user traffic to home VLAN may cause a controller reboot.
- An MSM Controller does not send disassociation messages from a Bradford Sentry authenticator to a wireless user.
- 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.
- 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.
- When IMC is used to manage the controller, APs may appear grayed out on the **Controller >> Controlled APs** page.

Known issues

These issues are present in this release:

- 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. As a workaround, in RF Manager, manually authorize all SSIDs associated with the HP 425.
- 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.
- In some conditions, the controller can experience issues at boot time. If you have more than five VLAN interfaces with IP addresses, HP strongly recommends that you use Static IP addresses on your VLANs.
- The "**%**" character causes random characters to appear in the name on the controller when used in creating a profile name. As a workaround, do not use the "**%**" character when creating a profile name.
- (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.
- If using teaming while an access controlled VSC with 802.1x authentication and the **WPA termination** option is enabled, wireless clients may not be able to connect via a team member controller. As a workaround, disable **WPA termination** or use **WPA termination** with **Mobility Traffic Manager** (MTM) enabled and access control disabled.
- 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.

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