HP MSM7xx Controllers Release Notes
v6.2.1.0

HP Part Number: 5998-6166
Published: June 2014
Edition: 2

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 v6.2.1.0

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 / 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.

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 6.2.1.0, 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 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 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 v6.2.1.0 software will disable the NAT feature. HP recommends that you review your existing settings and disable one of these features before upgrading to v6.2.1.0.

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 6.2.1.0 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 6.2.1.0, those changes will not be present when you downgrade to the previous version.

If you factory reset your device after upgrading to version 6.2.1.0, 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 requires web browser with SSLv3 support

For the MSM web-based management tool, use Microsoft Internet Explorer 8 or later, or Mozilla Firefox 17 or later. SSLv3 is now mandatory. SSLv3 is supported by Microsoft Internet Explorer 8 but must be enabled. Microsoft Internet Explorer 9 and later only uses SSLv3. Mozilla Firefox also supports SSLv3 but it may need to be enabled or you may need to update to a more recent version.

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 6.2.1.0 works with and is required for MSM software version 6.2.1.0. 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 and higher. 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)
6.2.0.x/6.2.1.0	6.0.185, 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	6.0.177 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.x.x is compatible with RF Manager 6.0.185 and 6.7.769, 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 v6.2.1.0 will also automatically upgrade any MSM320, MSM325, and MSM335 Sensors it manages to MSM software v6.2.1.0.

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

GMS support for teaming

GMS 6.2.1.0 supports teaming in MSM software 6.2.1.0 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 6.2.0.0.

- 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 apply to controller teams only.

Although enabled in MSM software release 6.2.0.0, 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.

Fixes

Version 6.2.1.0 includes fixes to the following issues:

- In dense environments, false "Radio down" alarms can be raised.
- In high traffic environments, DNS resolution by the controller can cause authentication delays and require multiple retries by clients.
- If a user deletes a RADIUS profile and re-creates it with a new secret key, this setting does not come into effect until another modification is made to the RADIUS profile.
- (Applies to teaming.) AP group names longer than 20 characters may prevent IMC from properly communicating with the MSM7xx Controller.
- (Applies to teaming.) When inheritance is enabled, AP configuration changes do not propagate to the team member controllers.
- The Internet network interface NAT option is disabled.
- The MSM7xx Controller restarts after a client tries to authenticate with the Windows 2008 R2 RADIUS server.
- A beacon containing an invalid channel occurs when multiple SSIDs are configured on the same radio.
- VLAN tag mapping and uplink port data was not included in the output of the CLI `show config all` command.

- Configuration backup using IMC fails for all MSM devices.
- The **firmware updates** feature does not work properly.
- The following misleading error message has been removed:

  ```
  <CONTROLLER NAME> <IP ADDRESS> debug webredirect: SSL Error occurred
  while reading: error:140760FCSL routines: SL23_GET_CLIENT_HELLO:unknown
  protocol (336027900)
  ```

- 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.
- When user is authenticating with a remote trusted domain, if LDAP information cannot be retrieved and a user group is not found, the user is still allowed to log in.
- An MSM7xx Controller can reboot during heavy simultaneous authentication traffic load.
- Whenever a wireless client roams from one AP to another using MAC Authentication, the client session is terminated and does not restart until the client issues a new DHCP request.
- The MSM Controller continues to respond to DHCP requests on the LAN port after that feature has been disabled.
- HTML authentication does not work if the user name contains spaces.
- The PayPal service does not accept guest credit card direct purchases.
- Using SOAP functions directed to a non-configured IP address causes SOAP to fail and add the following error message to the controller log:

  ```
  websoap: SOAP FAULT: SOAP-ENV:Client "Internal error" websoap: Unable
  to communicate with IPRulesMgr, Timeout occurred.
  ```

- Using an external RADIUS server and an access controlled VSC can cause the MSM7xx Controller to reboot.
- 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 should be.
- The SOAP command `GetAuthenticatedUsers` was deprecated. The new function `GetAuthenticatedUsersSessions` can be used instead.
- In high capacity environments such as teaming with a large number of APs and with LLDP in use, APs can randomly lose synchronization during high traffic periods.
- On a rare occasion, when a wireless client roams from one AP to another, the client traffic stops until it moves to a new AP and the following error message appears on the controller log:

  ```
  iprulesmgr: The RADIUS Accounting Request packet (id='17') received
  contains a Called-Station-Id attribute (length='33') that isn't
  recognized as being a MAC address, this may affect Location-Aware
  related functionnalities such as restriction or incorrect VSC
  assignment.
  ```

- When using HTML authentication, the **Continue browsing** link incorrectly redirects the wireless client back to the home page.
- Added the following SOAP function to allow mapping of a network profile to a local mesh interface: `AddVLANOnLocalMesh()`
- Added the following SOAP commands to autonomous mode APs:
  - To configure the Station ID delimiter used in the Called-Station-Id content in the RADIUS request:
    `UpdateVirtualSC8021XStationIdDelimiterAndCase`

`GetVirtualSC8021XStationIdDelimiterAndCase`

- To configure the MAC case:
  `GetVirtualSC8021XStationIdDelimiterAndCasem`
  `UpdateVirtualSC8021XStationIdDelimiterAndCasem`

- When configuring **Wireless protection** with a **Key source** of **Preshared Key**, the station delimiter and station ID MAC delimiter configuration fields are disabled.
- The MSM7xx Controller does not provide a NAS ID value to a customized ACL.
- (Applies to teaming.) The team manager controller can lose its default route when a static IP address is assigned to the Internet port.
- When using sFlow, an error message regarding "kernel emergency" is incorrectly displayed and can be ignored.
- (Applies to teaming.) When team manager controller fails over, the team member taking over from the team manager sends SNMP traps to the IMC server.
- (Applies to MSM430, MSM460, MSM466, MSM466-R) An AP may incorrectly apply configuration settings that were provisioned through a local mesh link.
- When the supplicant sends the RADIUS packet from a VLAN different than that of the ingress VLAN, 802.1x authentication fails for wired clients.
- When a wireless client associates with a non-access controlled VSC, an L2 update frame is not always sent.
- If defined hostnames in an SSL certificate contain uppercase letters, the wireless client does not display the Welcome HTML page.
- The MSM controller uptime value in the management tool is different from the value retrieved using IMC.
- The following missing SOAP commands for handling VSC ID and Station ID MAC delimiters have been added:
  - soapUpdateVirtualSCMACBasedStationIdDelimiterAndCase ($vscName,$stationIdDelimiter, $stationIdMACCase)
  - soapGetVirtualSCMACBasedStationIdDelimiterAndCase($vscName)
- The MSM7xx Controller does not apply a bandwidth restriction to wireless clients that are connected through a third-party AP.
- (Applies to teaming.) If you are setting up a team with Russia selected as the location, the team member controllers can fail to synchronize to the team manager controller.
- When the "restrict 802.11n clients" option is enabled, wireless clients on the 5 GHz band are unable to reach other clients.
- (Applies to teaming.) APs failed to find the team member controllers when using DNS discovery.
- The CLI command, `ids ap <MAC ADDR> authorize` fails with the following error message:
  `ERROR: Unable to create the IDS Neighborhood`
- When Radio Resource Management is enabled, some APs might reject configuration settings from the controller and cause the controller to reboot.
- Mobility Traffic Manager clients get disconnected when roaming from one AP to another.
- Internet port bandwidth control does not limit download (controller to client) bandwidth.
- The MSM7xx Controller does not apply the VSC rate limit settings received from an external RADIUS server.

- When a VLAN is configured as an egress VLAN and also to be monitored by IDS, wireless traffic is blocked.
- (Applies to teaming.) When a MAC list is deleted from a team member controller, the team member controller may experience a reboot and the APs are synchronized to the team manager.
- (Applies to teaming.) When using teaming and WPA termination at the controller, wireless clients that are connected through a team member controller might not get a DHCP lease.
- VLAN tag settings might not be removed after an AP reboot, causing new DHCP leases to be on the incorrect VLAN or denied.
- The MSM7xx Controller might fail to apply VLAN settings to an AP when only the default VSC is configured.
- (Applies to teaming.) The management tool might show that there are no APs synchronized on the team member controllers, even though there are.
- The MSM7xx Controller can experience reboots if a VSC is configured to use **WPA2 & PSK** and **Terminate WPA at the controller** is enabled.
- (Applies to controllers with a Premium licence installed) The MSM7xx Controller forwards incorrect DHCP requests when more than 32 VSCs are configured.
- 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.
- If the **%** character is used when creating a profile name, random characters appear in the name on the controller.
- (Applies to teaming.) When teaming is enabled, wired clients connected to the MSM317 ports are not able to authenticate.
- Wireless clients connected to an access-controlled VSC might get a DHCP lease on the default VLAN instead of the egress VLAN configured for the VSC.
- (Applies to teaming.) Wireless clients connected to an 802.1x non-access-controlled VSC are disconnected when the team manager fails over to an alternate team manager.
- (Applies to teaming.) When a team manager recovers after a failover, some of the APs synchronized to the alternate team manager automatically reset to synchronize back to the recovered team manager.

Known issues

These issues are present in this release:

- (Applies to teaming.) If the team manager fails, the interim team manager will enable RRM severe interference mitigation and AP load balancing, even if these options were disabled by the administrator. As a workaround, promote the interim team manager to team manager, and then disable undesired options.
- (Applies to teaming.) When there are a large number of APs associated with a team of controllers, IMC may incorrectly report that a controller team is unreachable. The situation should recover after a short time.
- (Applies to MSM720 when authenticating several clients.) Teamed controllers Home displays Authentication system without any value and Authenticated users as n/a. It is not possible to see if the Authentication system is running and how many clients are authenticated.
- (Applies to teaming.) Due to an SNMPD issue, AP group names longer than 20 characters might prevent IMC from properly communicating with the MSM7xx Controller. As a workaround, use less than 20 characters when naming AP groups
- If **Terminate WPA at the controller** is enabled in a VSC, the controller may randomly reboot. As a workaround, do not enable the **Terminate WPA at the controller** option.

- (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.
- (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. As a workaround, use only the **DENY** option.
- 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.
- 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.
- 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.