Hewlett Packard
Enterprise

HP MSM7xx Controllers and MSM Access Points Version 5.7.8.1 Release Notes

Abstract

These release notes provide important release-related information for MSM software Version 5.7.8.1.

Part Number: 5200-0200a
Published: July 2016
Edition: 2

Acknowledgements

Contents

MSM software V5.7.8.1

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

Model	WW	Americas	TAA	Israel
MSM430	J9651A	J9650A	J9654A	J9653A
MSM460	J9591A	J9590A	J9655A	J9618A
MSM466	J9622A	J9621A	J9656A	J9619A
MSM466-R	J9716A	J9715A		J9718A

”WW” identifies worldwide regions not otherwise explicitly named.

Model	WW	USA	Japan	Israel
MSM410	J9427A/B/C	J9426A/B	J9529A/B	J9616A
MSM422	J9359A/B	J9358A/B	J9530A/B	J9617A
MSM310	J9379A/B	J9374A/B	J9524A/B	
MSM310-R	J9383A/B	J9380A/B		
MSM317	J9423A	J9422A	J9423A	
MSM320	J9364A/B	J9360A/B	J9527A/B	
MSM320-R	J9368A/B	J9365A/B	J9528A/B	
MSM325	J9373A/B	J9369A/B		
MSM335	J9357A/B	J9356A/B		

IMPORTANT: The Israel MSM466-R (J9718A) requires software Version 5.7.1.0 or later. Earlier versions cannot be used.

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 5.7.8.1 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 V5.7.8.1 software will disable the NAT feature. These two features are incompatible, and the combination although not validated prior to V5.7.1.0 is now enforced. HP recommends that you review your existing settings and disable one of these features before upgrading to V5.7.8.1.

Updating software

(Not applicable to MSM317.) For autonomous APs, update the software as described in the “Software updates” section of the *MSM3xx / MSM4xx APs Configuration Guide*.

For controlled APs, including the MSM317, 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 5.7.8.1, and then want to return to the version (older than V5.7.1.0) 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 5.7.8.1, those changes will not be present when you downgrade to the previous version.

If you factory reset your device after upgrading to Version 5.7.8.1, your previous configurations will be lost, and when you downgrade to any previous version you will be in a factory reset state.

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)
5.7.8.1/5.7.8.0/5.7.7.0/5.7.6.0/5.7.5.0	6.7.769	Upgraded automatically by RF Manager	Upgraded automatically by MSM7xx Controller
5.7.4.0	6.0.185		
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 V5.7.8.1 automatically upgrades any MSM325 and MSM335 Sensors it manages to MSM software V5.7.8.1 and sensor code to V6.7.769.

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 (Guest Management Software)

IMPORTANT: As of October 2015, GMS version numbering has changed. GMS version 2.0 is the version to use with MSM software version 5.7.8.1.

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**.

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 pages 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.

Compatibility/interoperability

SSLv3 support

Support for the SSLv3 cryptographic protocol has been removed.

Changes

NOTE: The numbers that precede the change description are used for tracking purposes.

Version 5.7.5.0 and later include the following change:

- [**153332**, **155788**] 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

NOTE: The numbers that precede the fix descriptions are used for tracking purposes.

Version 5.7.8.1

The following fixes are included in Version 5.7.8.1:

- [**210278**, **210857**] Fixed an issue in which the SNMP agent was not able to retrieve certain MIB OIDs.
- [**198801**, **210856**] Fixed an issue in which the controller was slow to respond to SNMP requests.
- [**185422**, **193377**] (Applies to MSM422) This release includes a more robust fix for this issue, covering more cases and preventing the issue from occurring.

Version 5.7.8.0

The following fixes were included in Version 5.7.8.0:

- [**197207**] Fixed an issue in which a controller team would not synchronize when country code was set to South Korea and a static channel was set to 149, 153, 157, or 161.
- [**189108**] Fixed an issue in which a controller team would not synchronize when using a fixed DFS channel for the first radio on an MSM422.
- [**185422**] Fixed an issue in which the MSM422 caused client connectivity issues by occasionally reducing its transmit power to a very low level.

Version 5.7.7.0

The following fixes were included in Version 5.7.7.0:

- [**175433**, **176496**] (Applies to teaming with Mobility Traffic Manager (MTM).) Fixed an issue in which MTM functionality would be adversely affected in a controller team, with frequent messages added to the system log that were similar to the following:

  ```
  GetNewDatabaseConnectionObject: Cannot create the database connection object for 'x.x.x.x'
  ```

- [**174058**, **176402**] (Applies to DHCP relay on the non-default port 68.) Fixed an issue in which, when a client moved between two 802.1X access controlled VSCs, the user session would show the IP address of the previous session and the client could not reach the gateway. This did not occur on the default port 67.
- [**173386**, **173620**] Fixed an issue in which, if a remote syslog server was configured with a name longer than 25 characters, team synchronization would not complete successfully.
- [**173066**, **176494**] Fixed an issue in which an AP configured for automatic channel selection could select a channel experiencing severe interference (possibly related to radar DFS), resulting in wireless clients being unable to connect.
- [**173065**, **176498**] (Applies to HP 425, MSM410, MSM430, MSM460, MSM466, MSM466-R.) Fixed an issue where, under certain conditions, an AP could sometimes restart upon changing channel.
- [**172677**, **176489**] (Applies to MSM422.) Fixed an issue in which the AP radio signal power level would decrease so much that the wireless client had to be in very close proximity of the AP to remain connected.
- [**171009**] Fixed an issue in which a message similar to this was displayed in the controller system log when adopting a factory reset AP (functionality was not impacted):

  ```
  Post-commit application error occurred in confighandler IP:
  ```

- [**170911**] Fixed an issue in which, when configuring a new or factory-reset autonomous AP, getting to the end user license agreement page after entering credentials and clicking **Click here to learn how to get GPLv2 sources**, the new window would display the end user license agreement again instead of the GPL version 2 page.
- [**170910**] Fixed an issue in which, when configuring a new or factory-reset autonomous AP and getting to the end user license agreement page after entering credentials, the GPL version 2 license button was disabled.
- [**162454**, **172721**] (Applies to MSM422 radio 1 with any encryption set (WPA2, WPA, WEP).) Wireless clients with a MAC address with the first digit equal to 0x8 or higher will force the clients to always use software encryption, causing high CPU utilization on the AP and possible AP reboot.

Version 5.7.6.0

The following fixes were included in Version 5.7.6.0:

- [**163319**, **161741**, **170631**, **169359**, **170721**] Fixed issues related to performance and stability (AP/Controller reboots and crashes as well as optimization of some general throughput issue) that became apparent as this older software was being used in larger, more demanding network environments.
- [**162522**, **170098**] (Applies to MSM317, MSM320, MSM325, MSM422.) Fixed an issue in which, as wireless clients connected and disconnected, the AP would get into a state of 100% CPU utilization which caused slow performance, or in some cases an AP reboot.
- [**160682**] (Applies to MSM720.) Fixed an issue in which, when creating a new access-controlled VSC with the DHCP Server per VSC option enabled, a bogus error similar to the following is logged:

  ```
  Error reading VSC Access Control
  ```

- [**153105**, **169871**] (Applies to VSCs with Opportunistic Key caching and MTM (Mobility Traffic Manager) enabled.) Fixed an issue that caused roaming clients to end up on a VLAN different than the one assigned by the RADIUS server.
- [**152864**, **169872**] (Applies to MSM720 with teaming.) Fixed an issue in which having wireless client traffic going out an egress VLAN using a non-access controlled VSC, and then having the same traffic ingressed to another controller to perform HTML authentication, the authentication would fail.

Version 5.7.5.0

The following fixes were included in Version 5.7.5.0:

- [**161625**, **162093**] The product registration link has been corrected to:

  https://h10145.www1.hp.com/product/product.aspx

- [**161580**, **162260**] Under **Network** > **Address Allocation** > **Configure DHCP Server**, no more than three IP addresses can be configured for controller discovery.
- [**161490**] The maximum power configured for auto power is not respected. Auto-power controlled radios may be set to the maximum power value supported by the radio.
- [**160770**, **162251**] (Applies to MSM720 with teaming.) Under **Network** > **IP interfaces**, the IPv4 interfaces are not displayed.
- [**158697**, **159467**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) Free access user details are only created on the team manager controller and should not be synchronized with team member controllers.
- [**157578**, **159467**] A description of 802.11n is missing from the online help for the wireless client status page.
- [**156238**, **157802**] The SOAP command `ExecuteWirelessDisassociateClient` might fail if there are more than 1,000 clients.
- [**153965**, **157358**] When DHCP relay is configured in a VSC with the **Extend subnet to egress** option enabled, the controller may reply to ARP requests for any IP address in the subnet.
- [**152478**, **157302**] (Applies when the addressing type (static/DHCP) of the egress interface is changed, or the IP address of the egress interface changes.) Fixed an issue in which DHCP relay functionality stopped working if an access controlled VSC is mapped to an egress interface that is associated with a VLAN on the Internet port, with NAT disabled, and the VSC's DHCP relay **Forward to egress interface** option is enabled.

- [**151413**, **157316**] (Applies to use of external DHCP servers.) Upon IP address renewal, wireless clients lose network connectivity, even though they remain associated with the AP.
- [**151254**, **158503**] Wireless client authentication stops functioning under a combination of all the following circumstances:
    - There is one VSC configured for Active Directory authentication and one VSC configured for local authentication
    - A client authenticates on the VSC with Active Directory
    - Clients try authenticating on the VSC with local authentication
- [**150977**, **154623**] (Applies to MSM317, MSM320, MSM325, MSM422.) As wireless clients connect and disconnect, the AP can get into a state of 100% CPU utilization which causes slow performance, or in some cases an AP reboot.
- [**150976**, **157999**] In high traffic environments, DNS resolution by the controller can cause authentication delays and require multiple retries by clients.
- [**149941**, **157370**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) AP group names longer than 20 characters can cause temporary brief communication interruptions between teamed controllers and IMC, making the **Wireless Service Information** tab unavailable or causing it to display inaccurate data.
- [**149294**, **151580**] When a RADIUS profile is deleted and replaced with a new profile, the AP still uses the secret of the deleted profile.
- [**149260**, **157632**] Fix to support Class attribute in Accounting request to external RADIUS servers when using non-access-controlled VSCs.
- [**148527**, **157360**] (Applies to MSM422.) In a busy RF environment, for example, with lost HT frames and retransmissions, in which the MSM422 can transmit frames to a station in power saving mode and then become busy while retransmitting frames to this station. During this time (multiple seconds), the MSM422 does not send any frames to other stations.
- [**148482**, **157552**] In a Microsoft DNS environment with a parent domain and at least two child domains, users may be unable to connect.
- [**145660**, **157642**] 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.
- [**145576**, **148874**] When connected through an access controlled VSC using MAC authentication, users randomly lose their connection while roaming between two APs.
- [**144472**, **151249**] (Applies to MSM430, MSM460, MSM466, MSM466-R.) The AP cannot send large multicast packets to wireless clients.
- [**143918**, **157639**] Missing SNMP OIDs:

  nlcolubris802dot11: 1.3.6.1.4.1.8744.5

  nlcolubrisVirtualApMIB: 1.3.6.1.4.1.8744.5.1
- [**142401**, **157340**] If the AP name includes spaces, using the option Use AP name as DHCP client hostname can cause the dhcpd process to fail.
- [**141161**, **153844**] (Applies to MSM310, MSM320, MSM422.) Unsupported channels 184, 188, 192, and 196 are no longer available on APs operating in Japan.
- [**140725**, **153865**] NAT one to one and port forwarding rules are not working after a controller reboot.
- [**140662**] APs adopted by a controller still show as **no** in the Controlled APs **Already seen** column.
- [**139954**, **157563**] HTML authentication does not work if the user name contains spaces.

- [**135977**, **157560**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) Clients associated with a non-access controlled VSC protected with 802.1x authentication are disassociated and can no longer re-associate after teaming has failed over from one team manager to an alternate controller.
- [**135211**, **159336**] (Applies to MSM430 and MSM460 WW SKU with country set to **Qatar**.) In the 5725–5850 MHz band (Channels 149/153/157/161/165), the default (and maximum) EIRP power of 23 dBm has been corrected to 20 dBm.
- [**135040**, **154104**] (Applies to MSM410.) The AP shows that 255 wireless client stations are associated, even though very few are actually associated.

Version 5.7.4.0

The following fixes were included in Version 5.7.4.0:

- [**147271**, **147929**] (Applies to MSM410, MSM430, MSM460, MSM466, MSM466-R.) The SNMP OID `coDot11AssociationTable` does not return the connected clients when the AP is in autonomous mode.
- [**146418**, **147272**] The AP is not sending LLC SNAP frames to the switch when a wireless client associates.
- [**145449**] Software updates timeout when using Google Chrome unless the refresh feature is disabled.
- [**144532**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) 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.
- [**143002**] Wireless users authentication requests are not shared between Active Directory trusted domains.
- [**142135**, **142220**] The `GetAuthenticatedusers` SOAP command provides erroneous results for bytes sent and bytes received.
- [**142419**, **143271**] After an upgrade, APs may become unsynchronized and not resynchronize when APC (Automatic Power Control) for APs is enabled.
- [**141866**, **143274**] 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')
  ```

- [**141634**] Clients using HTML authentication do not get the Welcome page when they use an External SSL Certificate that has hostnames containing upper case letters.
- [**140860**, **143142**] 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.
- [**140114**, **140232**] 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.
- [**139714**, **141440**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) Teaming failover causes Mobility Traffic Manager (MTM) clients traffic to stop, even after the AP is adopted by alternate manager controller.
- [**139451**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) 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.
- [**139066**, **140645**] When using HTML authentication, the **Continue Browsing** link on the Welcome page erroneously redirects an authenticated user back to the login page.
- [**138776**] SNMP MIB for LLDP returns `LldpChassisIdSubtype` MAC address in an incorrect format.

- [**138775**, **142005**] IMC is unable to draw a topology diagram because SNMP ifOperStatus MIB erroneously returns **DOWN**.
- [**138441**, **143155**] SOAP command is not available for a local mesh interface to be mapped to a VLAN.
- [**138382**, **147082**] System uptime shown in the management tool does not match the uptime retrieved through SNMP.
- [**137987**, **143146**] When configuring an 802.1x VSC using SOAP, it is not possible to set the **Station ID delimiter** or the **Station ID MAC**.
- [**137957**] A VSC with Opportunistic Key caching (Fast Roaming) enabled, fails to authenticate users against certain RADIUS servers.
- [**137900**] After a software upgrade, an AP may drop packets from user VLAN over the AP tagged management VLAN.
- [**137894**, **143158**] 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**.
- [**137313**] SNMP process causes high CPU and high memory usage, which can cause the controller to reboot.
- [**136856**] When a customized URL is created for a public access VSC, the controller erroneously sends an empty NAS-ID value.
- [**134864**, **143231**] Rate limiting of the ingress VLAN configured on the RADIUS server does not get applied when the user is authenticated.
- [**136116**, **143125**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) The team manager controller can lose its default route when a static IP address is configured on the Internet port.
- [**134840**, **143114**] 802.1x authentication of new wireless clients may fail intermittently when configured on a non-Access Controlled VSC.
- [**134589**, **135268**] (Applies to MSM430, MSM460, MSM466, MSM466-R.) If a local mesh connection is broken because one of the AP fails, the other AP erroneously copies radio 2 configuration settings to radio 1.
- [**134271**] (Applies to MSM430, MSM460, MSM466, and MSM466-R.) The AP may experience wireless service interruptions and log the following message:

  ```
  Possible hang detected return code 256, resetting radio 1
  ```
- [**132813**] An MSM410 may experience sporadic reboots.
- [**131704**] When two APs are configured for a local mesh connection using a DFS channel, and at least one of the APs detects a DFS interference and switches to a non-DFS channel, the local mesh link goes down and is not automatically restored.
- [**131430**] Online help for the SOAP command `UpdateLocalMeshProfileDynamicAddressing` incorrectly indicates that the allowed downtime value must be entered in seconds instead of milliseconds.
- [**131427**] The SOAP command `UpdateManagementConsole` is not available for autonomous APs.
- [**131425**] The SOAP command `UpdateLoginMessage` is not available for autonomous APs.

- [**131408**] (Applies to MSM410, MSM430, MSM460, MSM466, MSM466-R.) When an access point is using local mesh and is then moved to another switch port the access point may fail to synchronize to the controller.
- [**130288**, **134447**] (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.
- [**130180**] 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.
- [**130044**] 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.
- [**129916**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) Enabling teaming on the controller may cause an incorrect DHCP lease to the Internet Port when it has a VLAN tagged on it.
- [**129764**] (Applies to MSM430, MSM460, MSM466, MSM466–R.) Radio hang warning messages, similar to the following, are incorrectly displayed on the system log:

  ```
  warning monitord CN18D3359L Possible hang detected return code 256,
  resetting radio 1
  ```

- [**129477**] 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)
  ```

- [**129476**] 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).`
- [**129469**] The HTTP proxy process incorrectly limits the number of supported connections to 1,024.
- [**129328**] RADIUS login credentials are appended with a space, causing the RADIUS server to fail authentication.
- [**129025**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) APs located remotely (synchronized through layer 3 connectivity) may lose synchronization to a team of MSM controllers.
- [**128543**] When a group of APs is configured to use a restricted list of available channels for automatic channel selection and all APs are rebooted (i.e. power outage), many of the APs will select the first channel on the list instead of distributing amongst all channels.
- [**128227**] 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.
- [**128029**] 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)
  ```

- [**128018**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) When teaming is enabled and SNMP is used to poll the `ipAddressIfIndex` MIB, the **tun1** interface returns a value of -1.
- [**128017**] 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`.
- [**127808**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) 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
  ```

- [**127072**] Updated OpenSSH version to 6.1.
- [**127018**] When configuring provisioning with a Static IP address for an AP or group of APs (**Access Point Group >> Provisioning**), if the entered IP address is invalid (begins with 0, for example), the returned error message is not clear: `ERROR UNKNOWN (-8).`
- [**126778**] The web interface is not accessible when the browser only supports Transport Layer Security, version 1 (TLSv1).
- [**126749**] (Applies to MSM430, MSM460, MSM466, MSM466-R.) When L3 Mobility is enabled, an AP is adopted by the controller and an error similar to following may appear in the system log:

  ```
  eapolserver: <serial number> Error while getting BSSID for virtual AP: <AP name> eapolserver: <serial number> WIRELESS_essid_get_status(wvlan0) cfgerr:(22) syserr:(Invalid argument)
  ```

- [**126736**] MSM422 radios may hang, blocking internet connections.
- [**126554**] 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
  ```

- [**126480**] 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.
- [**126445**] The **Cambodia** country code does not show up on the available country list.
- [**126370**] 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.
- [**126039**] Not all of the sort by column options available on the **(AP Group) >> Overview > Wireless Rates** page are operational.
- [**125936**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) 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.
- [**125878**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) 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.

- [**125872**] 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.
- [**125397**] 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.
- [**125327**] 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
  ```

- [**125196**] The **Mobility Clients** table on the web (**Controller >> Status > Mobility**) incorrectly displays information for MTM-blocked clients.
- [**125099**] When MTM blocks a wireless user, the web incorrectly displays the user as **Connected** on the Mobility Clients table (**Controller >> Status > Mobility**).
- [**125082**] (Applies to MSM430, MSM460, MSM466, MSM466–R.) When using 2 or more APs for a local mesh, if one of the APs is restarted, the local mesh link is not automatically recovered after it is back online.
- [**125069**] APs with a VSC that is configured to advertise transmit power incorrectly set the power value to -1 on beacon frames.
- [**124883**] 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.
- [**124700**] MSM controllers may present high CPU usage due to a process named **statspoller** and the number of wireless clients increases to (400 or more).
- [**124592**] After upgrading, the MSM controller may display the following error message on the system log:

  ```
  Query error on PublicAccessUser status table
  ```

- [**124557**, **124558**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) 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)
  ```

- [**124249**] When using the CLI command `disassociate controlled-ap wireless client [MAC]`, the following error message is displayed on the console:

  ```
  Invalid system action <180>
  ```

- [**123645**] The MSM controller does not allow using a URL or FQDN server name when configuring an external system log server.
- [**123355**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) 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.
- [**123334**] (Applies to MSM410, MSM430, MSM460, MSM466, MSM466–R.) If a radio's wireless mode is configured to 802.11a (not 802.11n/a), the following message is displayed on the system log: `stats_expor WIRELESS_get_txpower WRONG MODE=2`.
- [**122729**] Extended SOAP functionality to support retrieving of wireless users session ID.
- [**122528**] The values returned for SNMP queries to MIB objects “ipAddrTable”, “ipAddressTable”, and “ifTable” are not the same.

- [**121820**] 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.
- [**121407**] The controller ignores the values configured for the **Primary-DNAT-Server** RADIUS attribute.
- [**120982**] 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.
- [**120835**] 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='')
  ```

- [**119720**] When WDS (local mesh) is used, the slave AP will scan for a link to the master AP if SNR falls to a value below the minimum recommended for operation.
- [**119317**] 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.
- [**119030**] The MSM410 will not synchronize with the controller after a factory reset.
- [**118557**] (Applies to MSM410, MSM430, MSM460, MSM466, MSM466-R.) When automatic channel selection is enabled and uses a list of allowed channels from the channel exclusion list, two or more neighboring APs select the first channel from the availability list instead of selecting different channels.
- [**118142**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) 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`.
- [**117443**] Autonomous APs may experience high CPU utilization caused by a process named **eapolserver**.
- [**114909**] 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`.
- [**114777**] 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**.
- [**113201**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) 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.
- [**111138**] 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.
- [**107193**] On a standalone AP, the Help files for *IGMP snooping helpers* and *IPv6 ulticast to Unicast conversion* (both on **Home >> Wireless > Multicast**) show the same content.
- [**102694**] (Applies to MSM410, MSM430, MSM460, MSM466, MSM466-R.) Automatic channel selection in the 2.4 GHz band only works on channels 1, 6, and 11. If you add one or more of these channels to the exclusion list then the AP will remain on channel 1.
- [**102663**] 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.

- [**54333**] If an AP configured to use Quiet or Awake LED modes (**Controlled APs >> Configuration > LEDs**) reboots, the configured LED settings are ignored when the AP is back online.
- [**53600**] The help file content for the 802.1x settings on standalone APs (**Home > Authentication > 802.1x**) does not describe the Accounting Start Delay feature.
- [**42058**] (Applies to MSM430, MSM460, MSM466, MSM466-R.) When a local mesh master node switches to a new channel, it may take slave nodes up to two minutes to follow and synchronize on the new channel.

Issues and workarounds

NOTE: The numbers that precede the issue descriptions are used for tracking purposes.

The following issues are present in release 5.7.8.1:

- [**178324**] (Applies to MSM760.) When downgrading from V5.7.8.1 to an earlier version, the controller might not complete the reboot process. As a workaround, reset (power cycle) the controller.
- [**170798**] In the **Configure initial controller settings** automated workflow, the **Login message** editing cannot include line breaks. Create the **Login message** without line breaks, and if desired add the line breaks later (not within the automated workflow).
- [**162423**] (Applies to autonomous APs.) When **Allow 802.11n clients only** is configured, WEP is erroneously allowed. As a workaround, do not select WEP when using this 11n only option.
- [**162356**] Although this does not affect the user ability to log in, user names containing special characters configured on an external RADIUS server do not display correctly on the controller. To be able to see the user names correctly on the controller, do not use special characters in the user names.
- [**161561**] LLDP friendly AP names can have a maximum length of 32 characters, however this limit is not enforced. As a workaround, do not enter names longer than 32 characters.
- [**161430**] A double quote character (") is not supported in the local user account password. If you attempt to use this character, a misleading message similar to the following is displayed:

  ```
  The shared secret is invalid.
  ```

- [**161172**] The management tool inadvertently allows option **Extend VSC Egress subnet to VSC ingress subnet** to be enabled when NAT is used on VLANs mapped to the Internet interface. As a workaround, disable NAT on VLANs mapped to the Internet interface when using the **Extend VSC Egress subnet to VSC ingress subnet** option.
- [**161060**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) When NAT is enabled on the Internet interface of the team member controllers, a controller team cannot be formed. As a workaround, disable NAT on the controller Internet interface, and then create the team.
- [**160846**] (Applies to MSM430, MSM460, MSM466, MSM466-R in regions that support channel 13.) Auto channel in the 2.4 GHz band usually chooses channel 1, 6, or 11, whereas channel 1, 7 or 13 is better. As a workaround, either manually configure the desired channel (without using auto channel) or configure the channel exclusion list to only allow channels 1, 7, and 13.
- [**160656**] When using 802.1X with EAP/TLS local authentication, if the certificate is signed with SHA256, wireless clients might be unable to connect. If re-issuing the certificate is not possible, you will need to upgrade MSM software version V6.0.0.0 or later.

- [**160623**] (Applies to MSM765 zl.) After upgrading to V5.7.3.0 SR2 from V5.7.3.0 SR1, Active Directory authentication may fail with an Invalid User error logged. As a workaround, downgrade to V5.7.3.0 SR1.
- [**160553**] (Applies to MSM410, MSM422, MSM430, MSM460, MSM466, MSM466-R with radio channel width of Auto 20/40 MHz.) The AP can make a sub-optimal channel choice if there are neighbor radios operating in 40 MHz wide channels with a (-1) channel extension. The AP might choose to operate within the same channel but with a (+1) extension. As a workaround, avoid using (-1) channel extensions on neighbor radios. Alternatively, manually configure the radio channel and do not use Auto 20/40 MHz, or use the channel exclusion list to exclude channels with (+1) channel extensions.
- [**147065**] Broadcast and multicast traffic is blocked between MTM clients.
- [**146938**, **147585**] RADIUS task might restart when 200 or more wireless clients are attempting to login simultaneously.
- [**146226**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) In teaming, with **Extend VSC egress subnet** enabled, team member replies to ARP broadcasts in non-AC VSCs that use the default egress VLAN.
- [**146257**] Bandwidth limitation is ignored when the (max-input/max-output) attribute is assigned to the user account .
- [**146220**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) When a team manager is restored with its previous teaming configuration, the elected manager continues to be the team manger with the team members synchronized to it. The workaround is to disable teaming on each member, and then enable teaming again.
- [**146100**] Wireless clients on two different radios of an AP, that are connected to the same access-controlled VSC with DHCP configured, and have **extend VSC egress subnet to VSC ingress subnet** set, are unable to communicate with each other.
- [**134326**] MTM is not supported when APs are adopted by controllers using NAT.
- [**126192**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) 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.
- [**125385**] High bandwidth multicast streaming may cause high CPU levels in the MSM317.
- [**124976**] 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.
- [**124810**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) 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.
- [**124734**] Wireless clients connected to an access controlled VSC are sometimes unable to reach the default gateway.
- [**124602**] APs may randomly stop advertising a VSC, preventing wireless clients from connecting. As a workaround, restart the AP.

- [**124521**] 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.
  ```

- [**124350**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) 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.
- [**122699**] 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.
- [**121271**] 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).
- [**120256**] 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.
- [**118234**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) APs controlled by a team member controller report the serial number instead of the configured system name.
- [**117831**] When **Autopower** is enabled, the performance of radio 1 on the MSM422 drops. As a workaround, disable Autopower.
- [**114342**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) 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.
- [**114127**] 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.
- [**113398**] 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.
- [**113214**] 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).
- [**104907**] When sFlow is enabled, it cannot be disabled unless there is at least one controlled AP.
- [**104117**] The **show config** CLI command generates an **unable to read configuration** error in the management tool system log.
- [**104067**] (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**.
- [**104037**] (Applies to MSM430, MSM460, MSM466, MSM466-R.) If Radio 1 is disabled, channel 1 cannot be used on Radio 2. As a workaround, enable Radio 1.

- [**103493**] (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.
- [**102691**] (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.
- [**56028**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) 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.
- [**55755**] (Applies to MSM430, MSM460, MSM466, MSM466-R.) The APs support a maximum of 125 WPA2 clients per radio.
- [**55244**] (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.
- [**54779**] When setting the SNMP system log trap level below **Warning**, no traps will be generated.
- [**54667**] Regardless of the actual 802.11 standard and speed, sFlow always reports the speed as 11 Mbps and the standard as 802.11b.
- [**54524**] (Applies to MSM410.) You must add an extra VLAN to pass traffic over a local mesh link in controlled mode. In earlier MSM410 software versions you could discover and pass data over the same VLAN. You now cannot send data over the discovery VLAN.
- [**53549**] (Applies to MSM422, MSM430, MSM460, MSM466, MSM466-R.) The Band Steering feature will have no impact when the 5 GHz radio operates on a DFS channel. As a workaround, select a non-DFS channel, or if using auto-channel, exclude all DFS channels from the available channel list.
- [**53003**] 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.
- [**52536**] VPN-based IPSec clients are unable to connect to MSM7xx Controllers, resulting in display of messages similar to this: **XAUTH wrong UserId or Password**.
- [**43527**] (Applies to MSM720, MSM760, MSM765 zl with teaming.) 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.
- [**43496**] 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.

- [**42003**] There is no SNMP MIB support for Port Trunking on the MSM720.
- [**41480**, **42847**] (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.
- [**39191**] 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.

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.

The following limitations apply to controller teams only:

- `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`

NOTE: The **Removal due to invalidity** option of the `UpdateUserAccountRemovalSettings` function works in a teaming environment. However, do not use the **Removal due to inactivity** option when teaming because it could cause the controllers to wrongly remove active accounts.

Although enabled in MSM software release V5.7.8.1, 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`

Contacting HP

For additional information or assistance, contact HP Networking Support:

www.hp.com/networking/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

HP security policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

To find security bulletins:

1. Go to the HP Support Center website at **www.hp.com/go/hpsc**.
2. Enter your product name or number and click **Go**.
3. Select your product from the list of results.
4. Click the **Top issues & solutions** tab.
5. Click the **Advisories, bulletins & notices** link.

To initiate a subscription to receive future HP Security Bulletin alerts via email, sign up at:

h41183.www4.hp.com/signup_alerts.php?jumpid=hpsc_secbulletins

Related information

Documents

To find related documents, see the HP Support Center website:

www.hp.com/support/manuals

Enter your product name or number, and then click **Go**. If necessary, select your product from the resulting list.

Websites

- Official HP Home page: **www.hp.com**
- HP Networking: **www.hp.com/go/networking**
- HP product manuals: **www.hp.com/support/manuals**

- HP download drivers and software: **www.hp.com/s**
- HP software depot: **www.software.hp.com**
- HP education services: **www.hp.com/learn**

Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). Include the document title and part number, version number, or the URL when submitting your feedback.