5998-3326 5.6.0.0

MSM765zl and MSM4xx 5.6.0.0 (FIPS ONLY) Release Notes

Contents

General information

Important

Software (firmware) version 5.6.0.0 is functionally equivalent to software version 5.5.3.x but it adds FIPS certification. Version 5.6.0.0 should ONLY be used by those requiring FIPS certification. Those not requiring FIPS certification should instead use a non-FIPS-certified version such as 5.5.3.x or 5.7.x.

Applicable products

MSM software release 5.6.0.0 applies to the **HP MSM765zl Mobility Controller J9370A** plus these six dual-radio 802.11n Access Points (APs):

Model	WW	TAA (FIPS for Americas)
MSM430	J9651A	J9654A
MSM460	J9591A	J9655A
MSM466	J9622A	J9656A

("WW" identifies worldwide versions for all other MSM-supported countries except the Americas, Japan, and Israel.)

Important: The generic term "controller" is sometimes used in place of "MSM765zl Controller." The generic term "AP" is sometimes used in place of "MSM430," "MSM460," and "MSM466."

FIPS certification and compliance

This 5.6.0.0 software release provides FIPS certification for the HP products identified above under *Applicable products*. Please visit this NIST public web site for critical configuration and operating instructions: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2012.htm

On this NIST web page, look for certifications under **Hewlett-Packard Development Company, L.P.** There is one certification (# 1769) for the HP MSM765zl Mobility Controller J9370A and related switch equipment, and a second certification (# 1715) for the MSM430, MSM460, and MSM466 Dual Radio 802.11n APs.

Here is how the certification information looks on the NIST web site:

#1769:

HP 5406 zl [1], HP 5412 zl [2], HP 8206 zl [3] and HP 8212 zl [4] Switches with the HP MSM765zl Mobility Controller

(Hardware Version: (J8697A [1], J8698A [2], J9447A [3] and J9091A [4] [B]); Management Modules: (J8726A [1,2] and J9092A [3,4] [B]); Power Supply: (J9306A: one [1,3] or two [2,4]); Support Module: (J9095A [3,4] [B]); Fabric Module: (J9093A: two [3,4] [B]); Blank Plate: (5069-8563: four [1], ten [2], five [3] or eleven [4]); Opacity Shield Kits: (J9710A [1], J9711A [2], J9712A [3] and J9713A [4]); High Performance Fan Trays: (J9721A [1], J9722A [2], J9723A [3] and J9724A [4]); with (HP Gig-T/SFP+ V2 zl Mod: J9536A; HP Mobility Controller: J9370A [A] and Tamper Evident Seal Kit: J9709A) [1,2,3,4]; Firmware Version: 5.6.0 [A] and K.15.07.0003 [B])

(When operated in FIPS mode with the tamper evident seals and opacity shields installed as indicated in the Security Policy)

Validated to FIPS 140-2

Security Policy

Consolidated Validation Certificate

Vendor Product Link

#1715:

HP MSM430 Dual Radio 802.11N TAA AP [1], HP MSM430 Dual Radio 802.11N AP (WW) [2], HP MSM430 Dual Radio 802.11N AP (JP) [3], HP MSM460 Dual Radio 802.11N TAA AP [4], HP MSM460 Dual Radio 802.11N AP (WW) [5], HP MSM460 Dual Radio 802.11N AP (JP) [6], HP MSM466 Dual Radio 802.11N TAA AP [7], HP MSM466 Dual Radio 802.11N AP (WW) [8] and HP MSM466 Dual Radio 802.11N AP (JP) [9]

(Hardware Versions: J9654A [1], J9651A [2], J9652A [3], J9655A [4], J9591A [5], J9589A [6], J9656A [7], J9622A [8] and J9620A [9] with FIPS kit J9740A; Firmware Version: 5.6.0)

(When operated in FIPS mode and with the tamper evident seals installed as indicated in the Security Policy)

Validated to FIPS 140-2

Security Policy

Consolidated Validation Certificate

Vendor Product Link

Note: For regulatory reasons, HP does not support the MSM4xx Japan models (J9652A, J9589A and J9620A) at this time with V5.6.0.0.

Caution: **ONLY the HP equipment listed on the NIST web site is certified for FIPS compliance.**

Caution: **FIPS certification is only provided with software version 5.6.0.0.**

Caution: **To ensure that you maintain FIPS compliance, ONLY use FIPS-compliant products in your network.**

Avoid products that are not specifically listed as FIPS certified

To maintain FIPS compliance you should not use other products on your network that are not FIPS certified. For example, do not use MSM APs such as MSM3xx, MSM410, and MSM422, and do not use PCM/PMM/IDM, and GMS (Guest Management Software). **Non-certified products have not been tested with this release and are therefore not supported in this release.**

Mandatory Security Policies

For both the MSM765zl Controller and the MSM430, MSM460, and MSM466 APs, on the NIST web site, select the respective **Security Policy** link to launch the detailed document describing how to prepare, configure, and operate the listed products in a FIPS-compliant manner. **It is mandatory to follow all directions in this document to ensure FIPS-compliant product operation.** Information in the Security Policies takes precedence over all other HP documentation.

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 available to customers that have purchased a maintenance and support agreement.

If you install v5.5.3.x after installing v5.6.0.0 software

Important: If you choose to install v5.5.3.x software on the MSM765zl after installing and using v5.6.0.0 software, the MSM765zl must be reset to factory defaults. It is recommended you perform this as follows:

- In 5.6.0.0, save your MSM765zl configuration.
- Install v5.5.3.x software.
- Reset the MSM765zl to factory defaults.
- Restore the MSM765zl configuration from your backup.

Known issues

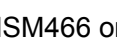
The following known issues are present in this release:

MSM765	MSM4xx	Description
✓	✓	An SNMPv3 user account with SHA/AES encryption fails to retrieve some OIDs, returning an “unknown user name" error.
✓		When a VSC is configured to use 802.1X and an egress VLAN, a wireless client roaming from one AP to another may end up on another VLAN that is not the one configured for egress.
✓		When two or more transactions from the same user occur within a two hour time frame, the second transaction is not processed.
✓	✓	The use of the % character is not allowed in the WPA pre-shared key
✓		When the controller internal RADIUS server is under heavy load (200 or more users authenticating simultaneously), RADIUS authentication fails for some users. A message similar to this appears in the system log: `...radius exceeds data memory.`
✓		APs located 16 or more hops away from a DHCP server may become unreachable by the controller due to timeouts.
✓		Active Directory authentications are not following the trust-relationship between servers.
✓	✓	(Applies to Country=**Egypt**.) The HT40 channel is not available.
✓		(Applies to 802.1X authentication with local RADIUS server.) Sessions time out too quickly, requiring users to re-log in.
✓	✓	The auto channel feature does not respect the channel exclusion list, allowing the radio to select excluded channels.
✓		When wireless clients authenticate with an external RADIUS server with the controller acting as a RADIUS client, the controller generates duplicate RADIUS ID in the packets, causing the RADIUS server to terminate the user session.
✓		The MAC authentication process may restart and cause the controller to reboot.
✓		When the PRIMARY-WEB-SERVER-STATUS-URL or the SECONDARY-WEB-SERVER-STATUS-URL are configured for a user account profile, after authentication, the user is not forwarded to external web-sites.
✓		(Applies to controller Teaming.) SOAP function **ControlledNetworkGetWirelessAssociatedClientStatus** is not working.
✓		When attempting to add a controlled AP, the CLI command **product type** does not work.
✓	✓	When automatic channel selection is triggered at almost the same time on two (or more) neighboring APs, the APs may wrongly be set to the same channel

MSM765	MSM4xx	Description
✓		If an AP is set to use a country code where the 20/40MHz automatic channel width selection is allowed, and then the AP gets changed to another country code where the 20/40MHz setting is not allowed, the controller fails to recognize and synchronize the APs.
✓	✓	When a WPA2 Enterprise wireless client disassociates, the AP incorrectly adds the following warning message to the system log: **warning eapolserver: <Access Point ID> Unable to update Interim Traffic (mac-address=<client MAC address>)** In this context, this warning can be safely ignored.
	✓	When a wireless client leaves the VSC without terminating the session, the location aware server does not confirm the session termination and a excessive number of messages similar to the following appear in the system log: `Discarded disassociation notice request due to session-id not matching the current user's session-id. Discarded disassociation notice request due to user not being associated.`
✓		When the country code is set to Turkey, teamed controllers are not able to synchronize.
✓		When an 802.1X authentication client egresses to a VLAN dynamically assigned from a RADIUS server and then the client roams between APs, after the roaming, the client is no longer able to reach the VLAN and it does not get an IP address lease.
✓		If the controller is configured for static NAT mapping, the **Extend ingress to egress interface** option on the DHCP relay configuration page does not work.
✓		When configuring an AP with two Mobility Traffic Manager (MTM) VSCs with the same settings but different names and SSIDs on radios 1 and 2 respectively, clients lose connectivity when roaming between radios.
✓		When the number of simultaneous connected clients approaches the maximum number permitted, high CPU utilization is experienced, possibly causing a controller restart. The system log indicates that “iappd" is consuming the CPU.
✓		(Applies only to a country code setting of Saudi Arabia.) The controller cannot synchronize configuration to the MSM430/460/466 APs.
✓		Some traffic from a client connected to an access-control VSC (tunneled between the access point and the controller) is detected at the switch where the access point is connected.
✓		Wireless users authenticating to an Active Directory server are able to authenticate when using the full realm name, but they cannot authenticating when using the NetBIOS name.
	✓	When IP filters are enabled and a wireless client connects to the VSC, the AP reboots. Disable IP filters to avoid this issue.

MSM765	MSM4xx	Description
	✓	The MSM430 configured to use radio 2 only drops connections from some wireless clients.
✓		In cases where there are more than one controller sharing the same egress VLAN for an Access-Controlled VSC, and the **DHCP relay and Extend VSC egress subnet to VSC ingress subnet** options are enabled, it is possible that the same IP address will be active on more than one controller at the same time, causing more than one controller to answer ARP requests for this IP address, leading to incorrect behavior. To avoid this when more than one controller is sharing the same egress VLAN, set DHCP lease time to at least 10 minutes.
✓		When mal-formed RADIUS packets are encountered, all wireless client sessions are unexpectedly dropped simultaneously.
✓		Clients roaming to untagged VLANs cannot communicate with the network.
✓		On a controller team, when an interim team manager takes over after the primary team manager becomes inoperative, active access controlled users may experience problems logging in.
✓	✓	(Remote Syslog only.) If in the management tool you add a remote log with the name “\” the remote log cannot be deleted except by the CLI or SOAP. Avoid using this name.
	✓	Some 802.11b clients cannot associate with the MSM430, MSM460, and MSM466 APs. Ensure that the Multicast rate is a basic rate (1, 2, 5.5 or 11Mbps for 802.11b).
✓	✓	If an AP that is provisioned on a non-DFS channel has its configuration changed to a DFS channel by a controller, the AP may unexpectedly restart. Once it restarts it synchronizes with the controller and operates normally.
✓		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 has 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.
✓		With Mobility Traffic Manager (MTM) enabled and high levels of ARP broadcast packets (approximately 30% or more of the traffic), CPU utilization reaches 100%.
✓		When a less specific static route is configured after a more specific static route has been configured, the controller forwards packets incorrectly.
✓		In a controller team, the client event log may be empty for some APs.

MSM765	MSM4xx	Description
✓		When using Active Directory running on Windows 2008R2, access controlled users fail to be authenticated when a team master becomes unavailable and a secondary controller takes over.
✓		When the Internet port change state (up or down), the routing table for a VLAN might not get recreated.
✓	✓	Some wireless client stations experience dropped voice calls due to long delays when roaming between APs.
✓		Mobility Traffic Manager may not function correctly when a controller team is managing 500 or more APs.
✓		Static NAT mappings are incorrectly limited to a maximum of 63 entries by the CLI. The management tool provides for a full 200 entries.
✓		If you configure one of the servers on the **Network > DNS** page with the same IP address that is assigned to the controller, the controller may become unresponsive.
✓		Wireless clients fail to be authenticated when the controller is configured to use an Active Directory server with a NetBIOS name that differs from the Windows domain name. To avoid this problem, make both names the same.
✓		(Teaming mode only.) After a software update, some APs may get stuck in the “waiting for manager” state. As a workaround, delete the AP from the configuration and add it again. It is insufficient to just perform a Remove/Re-discover of the AP.
✓		(Local mesh only.) If you use a VLAN for discovery, you need to define a separate VLAN for the wireless data traffic.
✓		(Remote Syslog only.) If in the management tool you add a remote log with the name “\” the remote log cannot be deleted except by the CLI or SOAP. Avoid using this name.
✓	✓	A radio cannot be set to monitor mode if it is currently assigned to a VSC using the **Transmit/receive on** setting under **Virtual AP**. As a workaround, first assign the VSC to another radio, then enable monitor mode.
✓	✓	RADIUS profile names must be less than 20 characters in length.
✓	✓	If a VSC is configured to support **Band steering**, you must first disable **Band steering** before changing the **Transmit/receive on** option from **Radio 1 and 2** to a single radio. Failure to do this results in configuration errors in the log file.
✓	✓	If you add an AP to a group that is not bound to any VSC, the AP is never able to synchronize. You must always bind a group to a VSC before you add APs to the group.
✓		The AP Status page incorrectly displays the regulatory domain that is defined for a group. This is only a display issue. The regulatory domain defined for the group is active.

MSM765	MSM4xx	Description
✓	✓	The wireless MIBs do not completely support all new features in this release.
✓	✓	When configuring radio settings, if you modify the value for "Channel" and then change any "Transmit power control" setting without first saving, the setting for "Channel" reverts to its previous value.
✓		When in teaming mode, the "Reserve AP capacity for failover" setting has been removed. You can discard this issue as the changes section in the release notes have a topic devoted to this.
✓		The MSM7xx controllers are vulnerable to DNS Cache Snooping for the DNS service. The DNS service is enabled by default on the LAN interface of the MSM controller and does not run on the INTERNET interface. The vulnerability allows anonymous users to query the cache using tools such as dig and to gain knowledge about sites that are visited by the local community by inspecting the TTL values found for non-recursive queries found in the DNS cache. The DNS cache option has been left enabled in this release to allow for improved dns and browser performance. To eliminate the MSM7xx controllers from having this vulnerability, if desired, the DNS cache option may be disabled by disabling the **DNS cache** option on the **Network > DNS** page of the management tool. A discussion of the potential risks of allowing DNS cache information to be queried anonymously is available here: www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf
✓	✓	If an AP is part of a group that is bound to six VSCs, and all the VSCs are configured to broadcast their SSIDs, the AP may only broadcast SSIDs for five of the six APs. If this problem occurs, making any change to the VSC configuration will fix the issue.
	✓	(E-MSM430, E-MSM460, and E-MSM466 only.) sFlow  samples do not include the extended field for 802.11 Tx information.
✓		Using sFlow with more than 80 APs may cause the controller to respond slowly to SNMP requests. To limit the number of sFlow APs that are being sampled, use the "Advanced Configuration" option on the "Controller >> Tools > sFlow page".
✓	✓	In controlled mode, for Band steering to be enabled in a VSC bound to this AP type, both of these conditions must be met: • Both radios are in access point mode or access point and local mesh mode. • One radio is set to 802.11n/a and the other is set to 802.11n/b/g.
✓		When using Mobility Traffic Manager with more than two controllers, if a wireless client roams between two APs managed by different controllers, its traffic may be blocked. The wireless client must re-associate with the network to resume traffic flow.

MSM765	MSM4xx	Description
✓		If teaming is enabled and then disabled, sFlow will not turn on. The controller needs to be restarted for sFlow to work again.
✓		A mobility client that egresses onto its home network locally at the AP that it is associated with will not be shown in the **Controller >> Status > Mobility > Mobility clients** table.
✓	✓	When the country (regulatory domain) for a group is set to a country that does not permit 802.11n on the 5 GHz band, the AP will not be able to synchronize with the controller. This is because radio 1 on these APs defaults to 802.11n 5GHz. To enable these APs to synchronize, disable radio 1 on the **Controlled APs >> Configuration > Radio** list page.
✓		If you enable provisioning under **[***AP name***] > Provisioning** before enabling global provisioning under **Controller >> Controlled AP > Provisioning**, configuration changes will not be applied to the AP. As a workaround, disable provisioning for the AP, synchronize it, re-enable provisioning for the AP, and then synchronize it again.
✓		When you use the **Remove and Rediscover** action on the **Controlled APs >> Overview Discovered APs** page, the APs interfaces are duplicated in sFlow.
✓		(Only when using SNMP to monitor a controller team.) SNMP cannot find the statistics for APs that are attached to a non-manager team member because it thinks they are attached to the manager. A SYSLOG message similar to the following appears: `"debug systemagent STATS: GetSystemInfo ConnectRemoteCollector AP=00:03:52:0E:2D:8E error=8 (The remote Id is not fetched)"`
✓	✓	In the SNMP system name, using the `%serial_number%` placeholder with any other text will result in the `%serial_number%` placeholder not being converted to its value.
✓		sFlow initialization time takes too long for a large number of APs. With 40 APs the initialization takes approximately six minutes but an hour for 100 APs.
✓		(Only LLDP in Teaming mode.) An AP with a name that includes a placeholder does not display the correct name when the AP is adopted by a team member.
	✓	(Only Teaming mode.) A previously-associated client (using WPA2 Enterprise) that is the first to attempt to re-authenticate after a controller failover will not be successful. Subsequent clients attempting to authenticate will not have this issue.
✓		An LLDP agent configured on a port that has Transmit disabled might cause LLDP to become unresponsive on all ports.
✓		(Only Teaming mode.) Two RADIUS profiles with the same uniqueid prevent team members from synchronizing. Avoid this issue by not using duplicate uniqueid values.

MSM765	MSM4xx	Description
✓	✓	When a radio is set to Auto Power, the radio always starts with the Maximum allowed value for the specific country and adjusts from that point. Setting the Maximum radio power will have no affect.
✓		(Only Mobility Traffic Manager.) Throughput is low when client traffic is tunneled between two controllers that are not part of the same team.
✓		In some cases, possibly with a slow RADIUS server, 802.1X authentication attempts aborted by the user before completion will accumulate and eventually consume all the available user logins.
✓	✓	APs with layer 2 connectivity to a controller are not able to synchronize if the access-controlled VSC to which they are bound is changed to non-access-controlled.
✓		Controller software cannot be updated from a wireless client using Mobility Traffic Manager.
✓		On a controller team, if a VSC has the **DHCP relay agent** feature enabled with the **Subnet selection** option, the relay does not work properly when the team manager recovers after a shutdown.
✓		The **VSC >> Overview > User sessions** page may show the incorrect VLAN assigned to the user via RADIUS. This is only a display issue. The correct VLAN is used by the controller to tag the user's traffic.
✓		Wireless mobility (Mobility Traffic Manager and legacy subnet-based mobility) will not work if the controllers in the mobility domain require static routes to reach the primary mobility controller.

✓		To support connection to the public access Interface with Firefox 3.6.3, a valid certificate must be installed and the following access list rules must be defined:
		`factory,allow,ACCEPT,tcp,*.thawte.com,80`
		`factory,allow,ACCEPT,tcp,*.verisign.net,80`

✓		When traffic for a roaming client must be tunneled back to their home network across two controllers, broadcast traffic from the home network will not reach the roaming client.
✓		If you configure your DHCP server to support controller discovery by APs using DHCP Option 43, the APs fail to retrieve the controller addresses if other non-HP options are present after the control IP addresses in the DHCP server configuration.
✓		Under heavy tunneled Access Control traffic, clients sometimes lose connectivity for 2 minutes.
✓		To avoid potential problems with AP synchronization, changing VLAN configuration on a VSC should only be done after all APs are fully synchronized.
✓		On the **Controller >> Status > Mobility** page, the **Networks in the mobility domain** table may show duplicate entries in the **Handler** column.
✓		Worldpay credit card payment does not work.

MSM765	MSM4xx	Description
✓		When using the Mobility Traffic Manager, on the **Controller >> Status > Mobility** page, the Visitors table may temporarily show client devices on the wrong AP/controller. This is a display issue that will resolve itself automatically.
✓		The following configuration settings are ignored when loading a configuration file onto a team manager: • VLANs with static IP addresses • GRE configuration settings • System log filter settings
✓		When a RADIUS profile is added or changed on the controller, the software indicates that all controlled APs need to be synchronized. This is unnecessary and causes wireless traffic to be interrupted for clients not authenticated through RADIUS.
✓		The LLDP dynamic naming feature is not supported when controller teaming is active.
✓		If you enable MAC-based authentication in a VSC and a user attempts to login but no user account is defined on the RADIUS server, an error message relating to "iprulesmgr assert" appears in the log.
✓		VMWare clients are unable to get an IP address when access-controlled VSCs are configured to use DHCP relay.
✓		When a controller is an interim manager, the **Security->Firewall** page is not locked. No changes should be made to an interim manager, only a primary manager.

✓		Occasionally during synchronization, a message similar to the following may appear in the log. No action is required:
		`mapconf: SOAP FAULT: SOAP-ENV:Client "Validation constraint violation:`
		`tag name or namespace mismatch in element <Y-MSM:security>`

✓		Specifying an invalid time on the chassis hosting an MSM765zl will result in all controlled APs continuously restarting. Set the correct time on the chassis to avoid this issue.
✓		After a factory reset, restoring a configuration that has WPA2 opportunistic key caching and/or L3 mobility enabled in one or more VSCs will result in a misleading error message being displayed in the VSCs. The error message indicates that validation failed, but fails to indicate the cause of the failure, which is that the required license is not installed. Installing the correct license and restarting the unit corrects the error.

MSM765	MSM4xx	Description

	✓	The online help for the CLI command "rcapture" is incorrect. The correct information is as follows:
		
		Syntax:
		
		`rcapture -u URI [-c count] -i interface`
		
		Description:
		
		Capture data on a port and send it to a file on an FTP server.
		
		Parameters:
		
		`URI`: Address of the FTP site and file where the trace will be saved, for example:
		`ftp://user:pass@ftp.mysite.com/trace.pcap`
		
		`count`: Number of packets to capture.
		
		`interface`: Interface to trace, where:
		
		`eth0` = Internet port
		`eth1` = LAN port
		`wvlan0` = wireless port

✓		Users that are a member of a group of the Parent domain cannot authenticate through Active Directory (AD).
✓		If you enable several network traces at the same time on different interfaces, you may not be able to stop the traces until you restart the controller.
✓		If you enable/disable NAT on the Internet port (or any VLAN associated with the Internet port), the change does not take effect until you restart the controller.
✓		If you change the IP address of a controller that is part of a mobility domain, L3 mobility does not function correctly until you restart all controllers.
✓		There is a problem configuring RIP in a team environment. The Internet port and LAN port work as expected but PPTP has a problem with respect to not appearing as active on other member controllers. The manager controller is set to active but it shows as passive on the other members.
✓		sFlow does not monitor unicast, broadcast, and multicast counters on any Ethernet interfaces. The values for these counters remain at zero.
✓		If you are using static IP address assignment for either the LAN or Internet port and modify the network mask, the default gateway is lost until the controller is restarted.
✓		If you bind an access control VSC to a switch port you either have to configure your VSC with the Client data tunnel enabled or ensure that you have proper ingress VLANs in the VSCs. Otherwise, after authentication, the client will not go through the proper controller VSC.

MSM765	MSM4xx	Description
✓		If you want to assign the Internet port as the Egress network in a VSC binding, it must have a VLAN. Mobility Traffic Manager currently cannot send user traffic onto the Internet port untagged.
✓		When working with a controller team, the LAN ports on all controllers must be connected via a layer 2 network, even if the LAN ports are not being used by your configuration. This enables controllers to exchange important information.
✓		When DHCP relay is configured with the **Extend Internet port subnet to LAN port** option, and you enable DHCP relay support on a VSC with the **Forward to egress interface** option selected, then you should not select more than one VSC egress mapping with an assigned VLAN.
✓		Assigning 192.168.1.1 to the Internet port can cause problem at startup if the Ethernet port is not being used.
✓	✓	When a radio is disabled, its channel and operating information are still displayed on the AP details page, instead of the radio being shown as disabled.
✓		In a controller team, when you add a static NAT mapping, the mapping definition shows the IP address for the stack manager Internet port. It is important to note that the Internet port address is different for each controller in the team.
✓		When you configure a controller to become the first member and manager of a team, the Filter definitions on the **Tools** > **System log** page are lost.
✓		The auto-population of the SNMP system name in the web page does not give the a good serial number when you add characters. In the SNMP page the field 'System name:' is auto-filed with the value: “%serial_number%.” If you add characters at the end of this string and execute the SNMP command you should see the serial number plus the characters you added.
✓		The SOAP sFlow sFlow function GetSflowReceiverTableRow returns the wrong timeout value.
✓		The client data tunnel option to **Allow traffic between wired clients and tunneled wireless clients** has been removed from VSCs in this release. If you are upgrading to this release, an equivalent configuration will be created using the new Mobility Traffic Manager feature.
✓	✓	If there are more than 80 APs shown on the Neighbor page, the following message is logged: "Radio 1's node table is full. Too many nodes in the surroundings (max is 256)."

MSM765	MSM4xx	Description
✓	✓	An AP fails to indicate that its configuration is not synchronized when defining provisioning settings. This occurs when you select an AP in the Network Tree and then click **Provisioning > Connectivity**, disable the **Inherited** checkbox, and then define provisioning settings. When you click **Save** the AP should go into the unsychronized state to indicate that configuration changes need to be sent to the AP. However, the AP stays in the synchronized state and must be restarted for the changes to take effect.
✓	✓	When working with a controller team, if you reset an AP, the AP will be discovered with state "Suspicious" and need to be authorized. This is normal. However, if after this a network failure forces the AP to associate with another controller in the team, the AP will incorrectly become "Suspicious" and need to be authorized again.
✓	✓	If the radio is set to operate in 802.11n/g mode, it continues to provide support for 802.11b mode. You can fix this behavior by removing support for the 802.11b modes in each VSC (under **Virtual AP > Allowed wireless rates**).
✓		When a VLAN is configured on the Internet port and the VLAN is used for Ingress mapping in a VSC, and you then reconfigure any VSC, you may lose communications on the LAN port. If this occurs, restart the MSM Controller.
✓	✓	The Axis2 SOAP client toolkit has issues dealing with some SOAP responses. It is recommended that you use a different SOAP client toolkit.
✓		When provisioning a static IP address on an AP, the controller does not validate that the default gateway is on the same subnet as the port. You must make sure the gateway is set correctly.
✓	✓	When configuring the **Allowed wireless rates** option under **Virtual AP** in a VSC, the user can disable support for all 802.11n data rates. If the VSC is only operating on 802.11n, then one non-MSC rate must remain operational or the VSC will not function correctly.
✓	✓	Controlled APs are not able to synchronize with a controller when all of the following occur in sequence: **1.** A VSC is defined with its ingress mapping set to a VLAN on the Internet port. **2.** The controller is restarted. **3.** The ingress VLAN is removed in the VSC. To avoid this problem, remove the VLAN before restarting the controller.
✓		DHCP leases do not indicate the correct VSC when using the **subnet per VSC** feature.

MSM765	MSM4xx	Description
✓		The MSM765 does not support the "shutdown" switch chassis functionality using command: **service <slot> shutdown**. This command will cause a reboot of the MSM765 and not a shutdown. Instead, you can effectively shut down an MSM765zl by removing it from the switch chassis after issuing the **service <slot> shutdown** command.
✓		A new default route does not take effect until after restarting.
✓		When Address allocation is set to DHCP server, the MSM765zl does not always correctly set the Gateway address to the IP address assigned to the MSM765zl. In some cases, you must set the Gateway IP address manually.
✓		Status information for non-access-controlled wired users does not appear on the **Status > Bridge > Switch** forwarding table.
✓		After performing a software update, the switch chassis log shows the following message: `HPESP: Services zl Module C is rebooting without a proper shutdown`. This is normal and no action is required.
✓		Enabling NAT support on a VLAN only takes effect after a restart.
✓		In a subscription plan, the **Between** option for **Validity period** is off by one hour when system time is set to automatically adjust for daylight savings time. The effective “Between” hour is hour+1.
✓		Client data tunnel configuration options should not appear on a non-access-controlled VSC.
✓	✓	(APs in Monitor mode only.) A group **other than Default** must be used to monitor both the 2.4 and 5 GHz RF bands.
✓		(Mobility Traffic Manager (MTM) with Opportunistic Key Caching only.) An MTM wireless client sometimes does not get an IP address when a dual-radio AP has both radios enabled with the same VSC and both are part of the mobility domain. As a workaround, do not enable Opportunistic Key Caching in this situation.
✓		Changes to the Egress VLAN of a group do not change the APs in the group into un-synchronized state, so the APs do not get updated with the changes. As a workaround, move the APs temporarily to a different group, synchronize them, then move them back to the desired group and synchronize them again.
✓	✓	(Local mesh environment only.) Provisioning local mesh for a downstream AP at the group level causes a radio configuration conflict. As a workaround, provision local mesh for such APs individually directly on each AP.
✓		When using machine authentication with Active Directory, the client can still gain access even if there is no matching group. Therefore, it is recommended that you do not use machine authentication with Active Directory.

MSM765	MSM4xx	Description
✓		Active Directory Server 2008 logs a warning message when the MSM7xx joins the domain. However, it is still functional. The warning begins with the following text. “The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection. ...” For details, see: http://go.microsoft.com/fwlink/?LinkID=87923
✓		(Applies only when VLANs are configured.) The Network topology diagram (**Controller >> Status > Network Topology**) may display APs on the LAN port instead of the Internet port.
✓		The **default-user-one-to-one-nat** site attribute is never applied. As a workaround, create a user account profile (**Controller >> Users > Account profiles**) and enable **VPN one-to-one-NAT** in the profile.
✓		The Network topology diagram (**Controller >> Status > Network Topology**) does not display accurately for APs that are on different sub-networks. The APs are shown connected to the same router.
✓		(Applies only to clients using Public IP addresses.) A client that is configured with the name of a proxy server, is unable to browse the Internet because the proxy server name is not resolved by the controller.
✓		Notifications (formerly called Traps) defined for Billing record servers are not working in this release.
✓		User tracking (**Controller >> Tools > User Tracking**) does not work for clients using Public IP addresses.
✓		When the same attribute is defined in a subscription plan and an account profile, the subscription plan setting should take priority, but it does not.
✓		If the DNS service is unavailable to a controller, Active Directory authentication can timeout and fail. To fix this, restart the controller or re-join the Active Directory.
✓		The CLI command: "Show radius users" shows only non-access-controlled users.