5998-2612 5.5.3.0

MSM7xx Controllers
5.5.3.0 Release Notes

Introduction

This document applies to these HP MSM products:

Model	Part
MSM710 (E-MSM710) Access Controller	J9328A
MSM710 (E-MSM710) Mobility Controller	J9325A
MSM730 (E-MSM730) Access Controller	J9329A
MSM730 (E-MSM730) Mobility Controller	J9326A
MSM750 (E-MSM750) Access Controller	J9330A
MSM750 (E-MSM750) Mobility Controller	J9327A
MSM760 (E-MSM760) Access Controller	J9421A
MSM760 (E-MSM760) Mobility Controller	J9420A
MSM765zl (E-MSM765zl) Mobility Controller	J9370A

The product models in the above table include alternative product names in parenthesis. For example, the MSM710 is also known as the E-MSM710. Both names refer to the same product. The original product names (without “E-”) are used throughout the rest of this document.

Note that the MSM317 is also referenced in this document, but generally refer to the MSM3xx / MSM4xx Release Notes for MSM317 information.

Release 5.5.3.0

Contents

General information

Terminology

The following terminology is used in these Release Notes and other 5.5.x documentation as follows:

Term	Description
AP	The term “access point” is generally abbreviated as AP.
Controller	Refers to the HP MSM7xx (HP E-MSM7xx) Controllers.

Documentation

You can download documentation from the HP Support Website at: www.hp.com/support/manuals. Search for your product model.

Critical software update required (controlled mode)

(Applies to E-MSM430, E-MSM460, and E-MSM466 operating in controlled mode only.) The flash boot section of these APs can become corrupted over time, resulting in a start up issue. **It is critical that you update your MSM7xx series controllers to version 5.5.2.0 or greater to prevent this issue.**

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.

Updating software

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

About Rev B MSM APs

As of July 1, 2010, Rev B MSM APs are available. This applies to the Rev B version of the following MSM APs: MSM310, MSM310-R, MSM320, MSM320-R, MSM325, MSM335, MSM410, MSM422.

Rev B MSM APs (product number ends with the letter “B” as in “J9xxxB”) ship from the factory with at least software v5.3.5 pre-installed. Rev B MSM APs cannot be downgraded to earlier versions of v5.3.x software. Therefore when adding a Rev B MSM AP to a network of controlled APs, the MSM7xx Controller must be running at least software v5.3.5, otherwise the Rev B MSM AP will not be recognized by an MSM7xx Controller. Only MSM7xx Controllers and MSM Access Points that are covered by a software Care Pack or software Contract can be upgraded from v5.3.*x* or 5.4.*x* to v5.5.0. Please contact HP Support for entitlement determination and download instructions. Support contact information is available on the HP Support Web page at: www.hp.com/networking. Look under Support > ProCurve.

Regulatory information

As of this v5.5.3.0 release, DFS channels (52-64 and 100-140) are now available on these product versions (Americas): E-MSM430 (J9650A), E-MSM460 (J9590A), and E-MSM466 (J9621A). These DFS channels were already available for product versions from other regions.

Information for PCM and PMM software users

PCM 3.20 and PMM 3.10 software supports MSM devices as follows:

- Full support of MSM devices at software version 5.4.2.0 or higher.
- Limited support of MSM devices at software version 5.3.x and 5.4.0.
- No support of MSM devices at software version 5.4.1.

Note: Purchase of PCM 3.20 and/or PMM 3.10 does not entitle you to an upgrade for MSM products. Only MSM products covered by a care pack or contract that includes software upgrades are entitled to upgrades.

Sensors and RF Manager

Sensors (applies to: MSM320, MSM325, MSM335) at version 5.5.3.0 are ONLY compatible with RF Manager version 6.0.157. If your RF Manager appliance is not running version 6.0.157 (or if you will not be upgrading it to that version), DO NOT install v5.5.3.0 software on any MSM7xx Controller that manages sensors used with RF Manager as this will automatically update the sensors and render those sensors incompatible with your RF Manager appliance.

Caution on using the console port password reset feature.

See “Manager login credentials reset” on page 35 and particularly the Caution.

Beamforming

(Only supported on the E-MSM430, E-MSM460, E-MSM466.)

The beamforming feature is available in v5.5.1 and higher for all product versions as follows:

Model	WW	Americas	Japan	Israel
E-MSM430	J9651A	J9650A	J9652A	J9653A
E-MSM460	J9591A	J9590A	J9589A	J9618A
E-MSM466	J9622A	J9621A	J9620A	

Fixes

The following issues have been fixed since release 5.5.2.0:

ID	Description
55920	When the auto channel feature is enabled on the radio page, and the channel exclusion list is set to 1, 6, and 11, most APs incorrectly end up on the same channel.
55778	The auto channel feature fails to select non-overlapping channels in the 2.4GHz band.
53851	HTML-based authentication only works on the team manager. Team members fail to provide HTML authentication. Wireless clients receive the login web page but receive a blank page after providing login credentials.
53254	Mobility Traffic Manager (MTM) clients lose IP connectivity when the egress network is configured to operate over a range of VLANs.
53040	The error message: "Generic Error. (255)" is displayed if an empty username or password is specified when clicking the **Join Realm Now** button on the **Controller >> Authentication > Active Directory** page. A more descriptive error message should be displayed indicating that the username provided does not exist on Active Directory or is ambiguous.
52997	When configuring a VSC, the error message: "When identification of stations is based on IP address only, MAC-based authentication methods cannot be selected." appears only when **Identify stations based on IP address** and **HTML Authentication** options are enabled. It should also appear when any other authentication method is enabled.
52915	In a teaming environment with the location-aware feature enabled the CPU utilization goes very high and this syslog message appears: `SendMessageToListeners: Error sending packet: Resource temporarily unavailable(11) to listener #5(/tmp/busclient.iappd_sc.458.1)`
44471	The **Wireless > Neighborhood** page displays duplicate and erroneous information.
44130	The **Wireless > Neighborhood** page always displays WPA2 regardless of the configuration of neighboring devices.
44083	Updating a Certificate Revocation List (CRL) when an invalid certificate is selected causes the management tool to hang.
43962	(Only E-MSM430, E-MSM460, and E-MSM466.) The beacon/probe shows an incorrect vendor ID.

ID	Description
43875	(Only E-MSM430, E-MSM460, and E-MSM466.) The **Wireless > Neighborhood** page is empty unless a radio is in Monitor mode. At startup the page should be populated even if Monitor mode is not enabled.
43794	The **Update CRL** button is grayed out on team members making it impossible to add/update a CRL for an installed certificate.
43782	The Access Controlled users association table is not updated to remove inactive users.
43747	(Only with Country=New Zealand.) On the radio configuration page, the "Auto 20/40Mhz" channel bonding option for 5 GHz is missing.
43702	The SNMP agent on a team member may cause the member to become inoperable.
43682	When using Internet Explorer 9, if you click on an AP in the Network Tree, the interface may incorrectly select the AP group for that AP instead.
43663	The radio inheritance cannot be removed from an AP group when the group is bound to a WEP-configured VSC.
43620	On the radio configuration page, the **Use maximum power** parameter is not activating maximum radio power.
43602	The SOAP "ControlledNetworkGetInterfaceStatus" and "GetInterfaceStatus" API methods do not return wireless interface information.
43478	Egress VLANs in a VSC binding are not synchronized properly on all managed APs.
43389	Access controlled clients are blocked when trying to reconnect after a log off.
43324	When configuring wireless neighborhood settings, adding a value to **site scan** causes a timeout on the management tool web page.
43253	When a large number of wireless clients are roaming between APs or disconnecting/reconnecting (for example, in a busy public environment) the maximum number of supported wireless clients slowly decreases because internal management cannot keep up with the changes.
43210	Wireless client stations are unable to obtain an IP address if the controller is configured to act as a DHCP relay agent and the clients stations are connected to a VSC configured to egress traffic on the VLAN assigned to the LAN port.
43206	The **Display the Free Access** option (**Controller >> Public access Web content**) is wrongly enabled by default.
43170	LLC broadcast frames are not always sent correctly.
43167	The team manager controller fails to send the initial gratuitous ARP message to the clients when the **Guest VSC** and the **Extend Internet Subnet** options are enabled.
43097	Enabling the **Terminate WPA at the controller** option results in wireless clients not being able to obtain an IP address from the controller DHCP server.
43092	Team member controllers fail to join a team when DNS provisioning is configured.
43038	The **Show Nor Flash Device ID** command on the **Controller >> Tools > System tools** page does not work. (The CLI command does not work either.)

ID	Description
43003	The CLI command **show all config** provides an incorrect value for the total number of users.
42995	On the **VSCs >> Overview > User sessions** page, the VLAN field shows 0 instead of the correct egress VLAN ID when 802.1x or MAC authentication is being used.
42914	Active Directory authentication with Windows 2003 server accepts users when ambiguous search results are returned from an Active Directory server.
42394	Quotation marks are incorrectly disallowed when defining a pre-shared key for WPA.
42364	(Only E-MSM430, E-MSM460, and E-MSM466.) The radio page incorrectly shows the maximum output power as 20dBm. It should be 18dBm or less.
42352	For 802.1X the RADIUS Accounting Start frame is missing the Framed-IP-Address attribute.
42284	The CLI "ps" command does not show the CPU utilization percentage.
42277	The HTML authentication process (Webauth) shows very high CPU utilization of approximately 98% for a long period of time.
42216	(Only MSM710.) Users that log in with the Free Access are intermittently disconnected.
41908	During teaming fail-over a synchronization problem may cause APs to reset.
41796	(Only MSM760 and MSM765zl.) VLANs with static IP addresses are not displayed properly on team members. They are only displayed correctly on the team manager.
41130	If a client station is connected to a switch port on the E-MSM317, it must reboot after its MAC address is removed from the MAC lockout list in order to connect.
41110	Long syslog messages that are sent as traps may be truncated.
39510	Meaningless output occurs on the console in team mode when a user associates. For example: (WRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwr)

Known issues

The following known issues are present in this release:

ID	Description
102860	Clients roaming to untagged VLANs cannot communicate with the network.
102689	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.
56076	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.

ID	Description
56028	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.
55975	With 500 or more wireless users and Mobility Traffic Manager (MTM) enabled, CPU utilization reaches 100% due to high levels of ARP broadcast packets (approximately 30% of the traffic).
55922	When a less specific static route is configured after a more specific static route has been configured, the controller forwards packets incorrectly.
55736	In a controller team, the client event log may be empty for some APs.
55664	When the port of an MSM317 is bound to an access-controlled VSC, wired clients on that port will not obtain the login page or have access to the egress network.
55440	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.
55268	When the Internet port change state (up or down), the routing table for a VLAN might not get recreated.
55195	Some wireless client stations experience dropped voice calls due to long delays when roaming between APs.
54655	Mobility Traffic Manager may not function correctly when a controller team is managing 500 or more APs.
54094	Static NAT mappings are incorrectly limited to a maximum of 63 entries by the CLI. The management tool provides for a full 200 entries.
53737	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.
53704	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.
68485	(E-MSM430, E-MSM460, and E-MSM466 in Monitor mode only.) A group **other than Default** must be used to monitor both the 2.4 and 5 GHz RF bands.
68434	Local Mesh may fail to synchronize when using TKIP. Use AES instead.
66985	(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.
66494	(E-MSM430, E-MSM460, and E-MSM460 with local mesh only.) If you use a VLAN for discovery, you need to define a separate VLAN for the wireless data traffic.

ID	Description
66449	(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.
65602	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.
65511	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.
65508	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.
65437	The wireless MIBs do not completely support all new features in this release.
65402	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.
65384	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.
65252	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
65195	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.
65101	(MSM317 only.) When the wired port requires 802.1x authentication, LLDP-MED LLDPDUs are sent on that port before the connected device authentication has passed.
64824	(MSM710 only.) When configured for PPTP, the user may get disconnected when downloading a large file.
64409	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".

ID	Description
64384	(E-MSM430, E-MSM460, and E-MSM466 only.) 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.
64380	(MSM325 and MSM320 with Sensor only.) For optimum performance, do not use sFlow on more than 80 APs. Select **Controller >> Controlled APs > sFLow > Advanced Configuration** to select the APs that will be sampled.
64307	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.
64174	If teaming is enabled and then disabled, sFlow will not turn on. The controller needs to be restarted for sFlow to work again.
64032	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.
63659	(E-MSM430, E-MSM460, and E-MSM466 only.) 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.
63105	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.
63050	When you use the **Remove and Rediscover** action on the **Controlled APs >> Overview Discovered APs** page, the APs interfaces are duplicated in sFlow.
61234	(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)"`
61080	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.
61052	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.
60775	(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.
60323	An LLDP agent configured on a port that has Transmit disabled might cause LLDP to become unresponsive on all ports.
60119	(Only Teaming mode.) Two RADIUS profiles with the same uniqueid prevent team members from synchronizing. Avoid this issue by not using duplicate uniqueid values.

ID	Description
60109	When you upgrade to v5.5.0 or higher software or from v5.4.x or lower software, or restore from a configuration saved with v5.4.x or lower software, the software loading wait page remains active indefinitely. This occurs because the web default SSL certificate was changed to “wireless.hp.local” in v5.5.0. Click Refresh in your browser to load the management tool home page.
59807	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.
59727	(Only Mobility Traffic Manager.) Throughput is low when client traffic is tunneled between two controllers that are not part of the same team.
59140	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.
57693	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.
56612	Controller software cannot be updated from a wireless client using Mobility Traffic Manager.
56233	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.
55235	When connecting autonomous APs to a controller, traffic is assigned to the default VSC, unless it is on a VLAN, in which case it is assigned to the VSC with matching VLAN ingress definition.
54877	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.
54867	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.

54864	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`

54864	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`

54828	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.

ID	Description
54708	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.
54579	Under heavy tunneled Access Control traffic, clients sometimes lose connectivity for 2 minutes.
54518	To avoid potential problems with AP synchronization, changing VLAN configuration on a VSC should only be done after all APs are fully synchronized.
54482	On the **Controller >> Status > Mobility** page, the **Networks in the mobility domain** table may show duplicate entries in the **Handler** column.
54278	Worldpay credit card payment does not work.
54147	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.
54090	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
54070	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.
53893	The LLDP dynamic naming feature is not supported when controller teaming is active.
53294	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.
53090	(Only MSM317.) On an MSM710, if you use the **Swap the LAN and Internet Jacks** option on the **Controller >> Network > Port configuration** page, the swap works but there are no visual indicators to show that the ports are swapped.
52974	VMWare clients are unable to get an IP address when access-controlled VSCs are configured to use DHCP relay.
52821	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>`
52734	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.

ID	Description
52385	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.
52184	Users that are a member of a group of the Parent domain cannot authenticate through Active Directory (AD).
52159	Drag-and-drop of APs between groups in the Network Tree does not work in the Mozilla Firefox Web browser.
52103	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.
51958	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.
51930	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.
51550	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.
51390	sFlow does not monitor unicast, broadcast, and multicast counters on any Ethernet interfaces. The values for these counters remain at zero.
51064	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.
51013	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.
51013	When you bind the switch port on an MSM317 to an access-controlled VSC, you must do one of the following to ensure that user traffic reaches the VSC. Enable the **Always tunnel client data traffic** option, or assign the same VLAN ID to the port and the VSC ingress.
50983	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.
50351	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.
50330	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.

ID	Description
50138	Assigning 192.168.1.1 to the Internet port can cause problem at startup if the Ethernet port is not being used.
49896	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.
49666	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.
49637	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.
49637	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.
49608	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.
48880	sFlow statistics for the MSM317 switch and Ethernet ports may be incorrect for a few moments.
48745	The SOAP sFlow function GetSflowReceiverTableRow returns the wrong timeout value.
48420	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.
48316	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)."
47551	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.
46883	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.

ID	Description
46021	In a controller teaming environment, the Guest Management Software (GMS) certificate is only installed on the team manager. To avoid problems if the team manager becomes temporarily unavailable, the GMS certificate should be installed on all other controller team members. Manually save and install the certificate as follows: **1.** On the team manager controller, select **Security > Certificate Stores**. **2.** Select the GMS certificate (may be referred to as "VMT") in the **Trusted CA certificate store** box. **3.** Copy the content from **View certificate** and paste it into a text file with a file name that matches the certificate name. **4.** On all other team member controllers, select **Security -> Certificate Stores**. **5.** In **Trusted CA certificate store**, click **Browse**, select the file created in step 3, and then click **Install**.
45744	When controller teaming is used, the Guest Management Software (GMS) cannot host the WEB pages used for the public access interface. As a work around, you must save your pages directly on each controller or use an external RADIUS server to host the WEB pages.
44409	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.
44023	(Only applies to controlled-mode access points in Japan.) Due to regulatory differences for indoor and outdoor access points, one MSM controller must manage indoor access points and another MSM controller must manage outdoor access points.
43744	The management tool incorrectly allows a MSM317 switch port to be bound to an access controlled VSC with **Always tunnel client traffic** enabled. VLANs are not supported by this type of configuration.
43192	Automatic HTML re-authentication works only on the default VSC.
42979	(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.
42949	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.
42402	(E-MSM430, E-MSM460, and E-MSM466 in a 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.

ID	Description
42374	(Teaming mode with MSM317 only.) DHCP relay is unable to forward DHCP requests coming from an MSM317 wired port when an Access Controlled user is not using the default VSC. As a workaround, ensure that Access Controlled MSM317 wired users are on the default VSC.
39994	The Axis2 SOAP client toolkit has issues dealing with some SOAP responses. It is recommended that you use a different SOAP client toolkit.
39822	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.
39804	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.
39364	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.
38814	DHCP leases do not indicate the correct VSC when using the **subnet per VSC** feature.
38770	Billing records formats are empty. To fill the fields, select "Reset to Factory Default Format" for each field.
38754	(Only MSM765zl.) 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.
38750	(Only MSM317.) The MSM317 may generate a **CFG_SYNC_FAILURE** in the log when it synchronizes after a number of configuration changes have been made on the controller. The MSM317 will then restart, apply all changes, and operate normally.
38667	A new default route does not take effect until after restarting.
38621	(Only MSM317.) Applies only when at least one **non-access-controlled VSC** is configured with **Ethernet Switch** as the VSC ingress mapping, and one **access controlled VSC** is configured with a **VLAN** as the VSC ingress mapping.) This message may appear in the system log: `err confighandl Failed to read ingress VLAN information for Virtual Service` This message should be ignored.

ID	Description
38305	(Only MSM317.) Making any configuration change on an MSM317 (or group of MSM317s) results in all wired 802.1X users on the MSM317 (or group of MSM317s) erroneously having their connections terminated during the synchronization process.
38292	(Only MSM765zl.) 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.
38227	Status information for non-access-controlled wired users does not appear on the **Status > Bridge > Switch** forwarding table.
38206	(Only MSM765zl.) 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.
38147	Enabling NAT support on a VLAN only takes effect after a restart.
38079	If Ports 1 to 4 of the MSM317 are bound to a VSC that has WPA enabled with the parameter **Terminate WPA at the controller** selected, then 802.1X wired users that are connected through the port cannot be authenticated.
38047	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.
37529	If a VSC is configured to support WEP with Key source set to Dynamic, **Support static WEP** is displayed, however it is no longer supported.
37356	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.
36881	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
36571	(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.
36379	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.
36282	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.

ID	Description
36182	No Billing records log entry is added when user, who is already logged in, clicks Subscribe on the Session page and then creates another user account.
36134	(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.
36036	Notifications (formerly called Traps) defined for Billing record servers are not working in this release.
35744	User tracking (**Controller >> Tools > User Tracking**) does not work for clients using Public IP addresses.
35717	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.
35625	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.
34103	After creating a management VLAN, traffic across that VLAN may not work unless you reboot.
33467	The CLI command: "Show radius users" shows only non-access-controlled users.
18189	Client data tunnel configuration options should not appear on a non-access-controlled VSC.

Release 5.5.2.0

Fixes

The following issues have been fixed since release 5.5.1:

ID	Description
44144	(Americas SKU (AM) for E-MSM430, E-MSM460 and E-MSM466 only.) A controlled mode AP cannot sync to a controller group configured for any country other than United States.
44015	(Applies to E-MSM430, E-MSM460, and E-MSM466 operating in controlled mode only.) The flash boot section of these APs can become corrupted over time, resulting in a start up issue. It is critical that you update your MSM7xx series controllers to version 5.5.2.0 or greater to prevent this issue.
43178	Undesired log messages appear each time a Spectralink phone goes into power-save mode.

39526	The default public access login page does not work with Apple devices such as the iPhone and iPod. These devices may block popups preventing the user from seeing the login page.You can use one of the three following strategies to resolve this issue:
	• Open **index.asp** for editing and add the useragent check by editing function showsessionpageifnotsubscribe() as follows:
	`function showsessionpageifnotsubscribe()`
	`var useragent = navigator.userAgent;`
	`if (useragent.indexOf('iPod') > -1) {`
	`showSessionPage = false;`
	`}`
	This prevents the MSM7xx Controller from displaying a session page on the device.
	Next, enable the welcome-page and provide a means for the user to access or bookmark the logout URL or access the session-page URL.
	• Or, enable redirect to https and install a certificate.
	• Or, create an access-list to allow access to www.apple.com port 80.

Release 5.5.1

Fixes

The following issues have been fixed since release 5.5.0:

ID	Description
68421	(E-MSM460 only.) After upgrading a controller from 5.3.6 to 5.4.2.0 and then to 5.5.0, or from 5.3.6 to 5.5.0, the E-MSM460 could not be synchronized.
67798	(Teaming mode only.) APs may get stuck in the resetting/uploading configuration states after disabling a radio channel.
67043	An MSM7xx Controller sometimes reboots due to internal problems encountered when a wireless client rapidly switches between VSCs.
66980	Although the E-MSM430 and E-MSM460 permit radio 2 to be set to 802.11n/a (5 GHz band), radio 2 on these devices must be kept set to 802.11n/b/g (2.4 GHz band). Do not attempt to use these devices with both radios configured on the 5 GHz band.
66901	The VSC Multicast rate changes from 6 Mbps to 1 Mbps on 802.11n radios when you restore the configuration on an MSM7xx Controller.
66565	Intermittent 802.1x authentication issues occur with the Apple iPad at software version 4.2.1.
66198	On a local mesh link, continuous user traffic can cause the management traffic to stop. To recover from this condition, disable and then re-enable the radio.
66190	(Mobility Traffic Manager (MTM) only.) If you shut down a controller which is a secondary controller, it will not try to rejoin the MTM primary controller.
66038	(Teaming mode only.) The LLDP civic address is not synchronized between team members.
65752	RADIUS profile names must be less than 20 characters in length.
65622	The PayPal payment feature does not support the **PayPal Payment Review** option or any kind of Deferred Payment.
65447	The MSM317 switch port does not stay disabled when a loop is detected on the port that has Loop Protection enabled.
65195	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.
65089	The **Status > Mobility > Mobility** clients table may sometimes show clients as connected, even though they have been disconnected for several hours.
64692	(Teaming mode only.) Static addresses for VLANs defined on members within the team are only displayed in the management tool of the team manager. The member management tool shows empty fields for the VLAN IP addresses.

ID	Description
64600	(E-MSM430, E-MSM460, and E-MSM466 only.) The **Terminate WPA at the controller** option is not working.
60596	Users cannot authorize on both the Active Directory parent and the child.
59510	IP Connection Tracking on management tool page **Controller >> Status> IP Connection**, is not being displayed with Google Chrome 5.0.375.99. Use the recommended Web browsers.
57746	Active Directory 802.1x authentication does not work when used with Windows Server 2008-R2.
55973	DSCP tag mapping could not be configured. This has been corrected to allow overriding of the default DSCP mappings that are used when you select **DiffServ** as the **Priority mechanism** for **Quality of service** on a VSC. To define a mapping, select **Controller >> Network > IP QoS**, and then specify a decimal number for DSCP tag in the range 0 to 63. Next, select a **Priority level** and then select **Add**. Priority levels map to QoS queues as follows: Voice = Queue 1, Video = Queue 2, Best Effort = Queue 3, Background = Queue 4. **Note:** • Multiple DSCP tags can be assigned to the same priority level if needed. • This override applies to downstream traffic (traffic sent by the AP to wireless clients) only. • This override also affects the QoS setting for local mesh links.
49182	Under a very heavy wireless load, wireless client traffic can become very slow after several large file transfers. Terminating and reassociating client stations does not resolve the issue. The only solution is to restart the AP.

Release 5.5.0

Contents

New features and management tool changes

Note: The newest version of this information is found in the *MSM7xx Controllers Management and Configuration Guide* and in the online help. See "Documentation" on page 2.

This section describes the new/changed features for this release and the related MSM7xx Controllers management tool changes.

Note: For more detailed new feature descriptions, see the *MSM7xx Controllers Management and Configuration Guide* and the online help.

New access points

This release adds support for three new 802.11n dual-radio APs, the E-MSM430, E-MSM460, and E-MSM466. See the *E-MSM430, E-MSM460, and E-MSM466 802.11n Access Points Quickstart* and the *MSM3xx / MSM4xx Access Points Management and Configuration Guide*.

Caution: Important radio configuration information

On the E-MSM430 and E-MSM460, radio 2 must be kept set to 802.11b/g/n mode (2.4 GHz band).

On the E-MSM466, if you set both radios to 802.11n/a mode (5 GHz band), respect the following guidelines:

- You cannot use the six element MIMO antenna because three of its elements are used for the 2.4 GHz band.
- The two three-element antennas should be separated by four feet to get optimal performance. A minimum separation of two feet is required.
- If using the E-MSM466 with outdoor antennas, aim the two antennas in different directions.

Band steering

(Only supported on the MSM422, E-MSM430, E-MSM460, E-MSM466.)

Band steering is a new feature that is designed to help solve dense client issues. When band steering is enabled, APs will attempt to move wireless clients that are capable of 802.11a/n onto the 5 GHz band, thus reducing the load on the slower and more crowded 2.4 GHz band, leaving it for less capable legacy (802.11b/g) clients.

How it works

An AP uses the following methods to encourage a wireless client to associate at 5 GHz instead of 2.4 GHz:

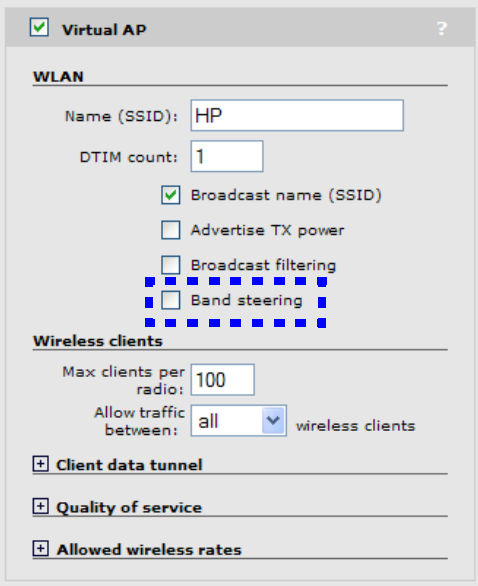
- The AP waits 200ms before responding to the first probe request sent by a client at 2.4 GHz.
- If the AP has learned that a client is capable of transmitting at 5 GHz, the AP refuses the first association request sent by the client at 2.4 GHz.
- Once a client is associated at 5 GHz, the AP will not respond to any 2.4 GHz probes from the client as long as the client's signal strength at 5 GHz is greater than -80 dBm (decibel milliwatt). If the client's signal strength falls below -80 dBm, then the AP will respond to 2.4 GHz probes from the client without delay.

Note: To support band steering, the VSC must be bound to APs with two radios. One radio must be configured for 2.4 GHz operation and the other for 5 GHz operation.

Note: Band steering is temporarily suspended on an AP when the radio configured for 5 GHz operation reaches its maximum number of supported clients.

Configuration

Band steering is configured individually for each VSC (under Virtual AP). For example:

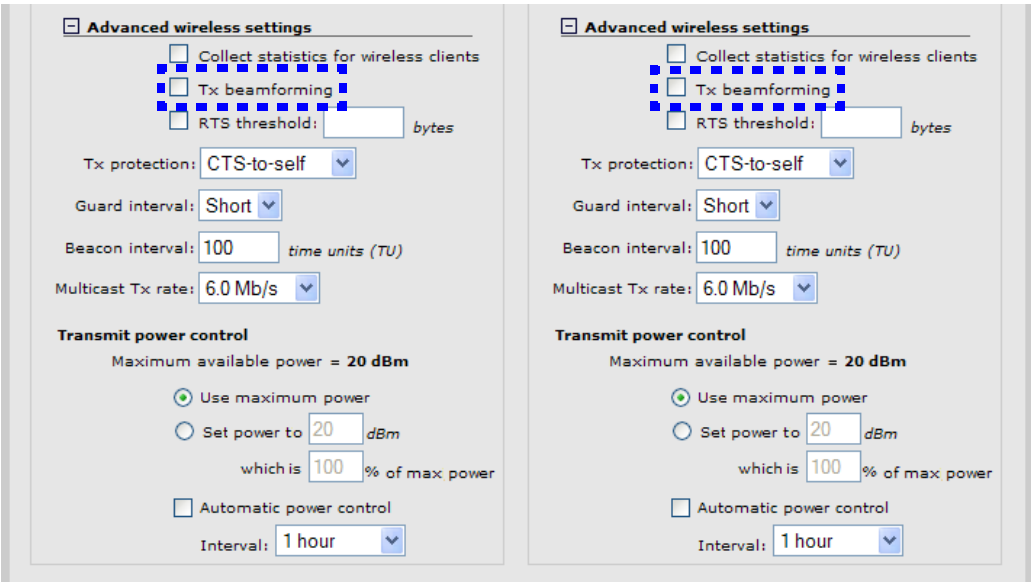


Beamforming

(Only supported on the E-MSM430, E-MSM460, E-MSM466.)

Beamforming is a new feature that is designed to help increase throughput by improving the quality of the signal sent to wireless clients.

Beamforming is configured on the Radios configuration page for an AP (under Advanced wireless settings). For example:



When this option is enabled, APs use beamforming techniques to optimize the signal strength for each individual wireless client. Beamforming works by changing the characteristics of the transmitter to create a focused beam that can be more optimally received by a wireless client.

HP APs support the following two explicit beamforming techniques:

- Non-compressed beamforming, in which the client calculates and sends the steering matrix to the AP.
- Compressed beamforming, in which the client sends a compressed steering matrix to the AP.

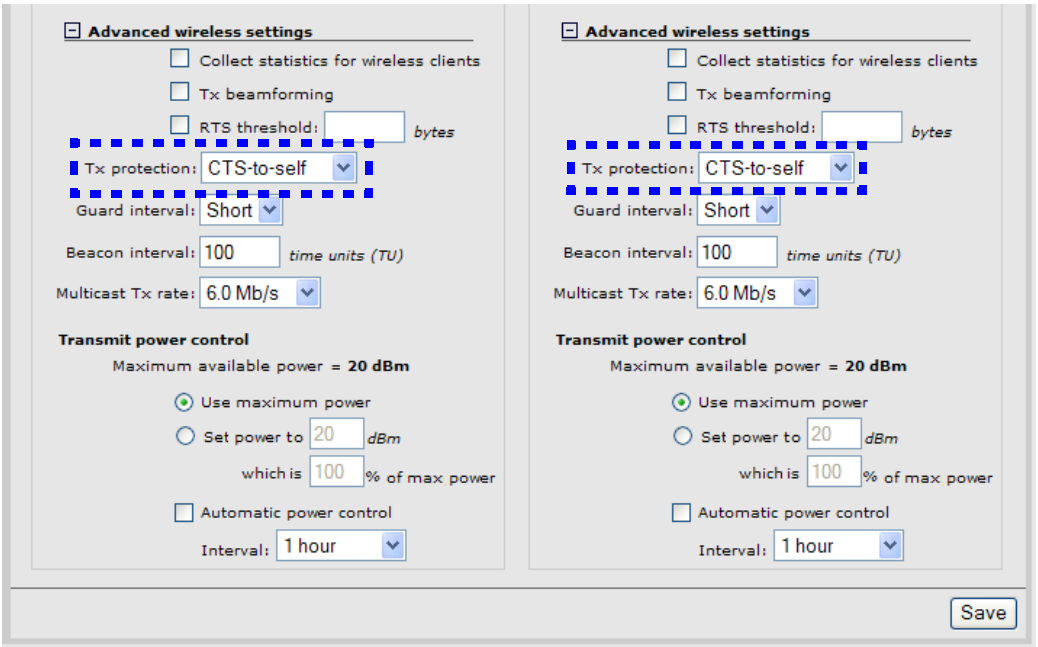
Radio calibration is not required when using either of these two methods.

Note: Beamforming only works with wireless clients that are configured to support it.

Transmission protection

(Only supported on the E-MSM430, E-MSM460, E-MSM466.)

When an AP is operating in an 802.11n mode, and legacy (a/b/g) traffic is present on the same channel as 802.11n traffic, the **Tx protection** feature can be used to ensure maximum 802.11n throughput. It is available on the Radios configuration page (under **Advanced wireless settings**). For example:



The following options are available:

- **CTS-to-self:** 802.11n transmissions are protected by sending a Clear To Send (CTS) frame that blocks other wireless clients from accessing the wireless network.
- **RTS/CTS:** 802.11n transmissions are protected by sending a Request To Send (RTS) frame followed by a CTS frame. This is a more robust, but slightly slower solution than CTS-to-self. However, this method resolves the hidden station problem (where certain legacy stations may not see only a CTS frame).
- **No MAC protection:** This setting gives the best performance for 802.11n clients in the presence of 802.11g or 802.11a legacy clients or APs. No protection frames (CTS-to-self or RTS/CTS) are sent at the MAC layer by the AP. PHY-based protection remains active, which alerts legacy clients to stay off the air while the AP is transmitting data to 802.11n clients. This method of protection is supported by most 802.11g or 802.11a clients, but is not supported for 802.11b-only clients and should not be used if such clients are expected on the network.

Country configuration per group

Country configuration is now set at the group level instead of globally on the controller.

To configure country settings, select either:

Controlled APs >> Configuration > Country

Controlled APs > [*group*] >> Configuration > Country

After changing the country setting, the APs must be synchronized.

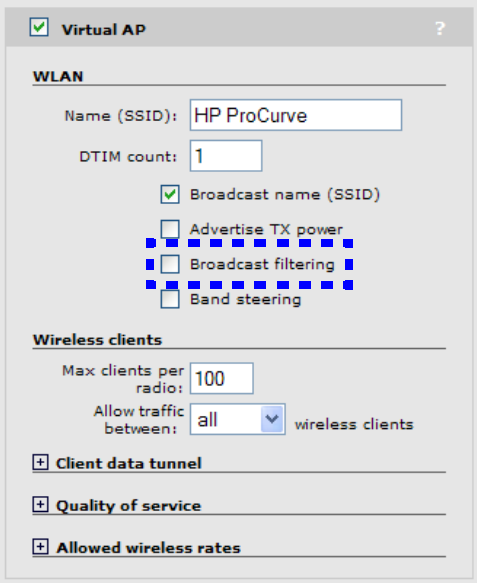
Note: In some regions, APs are delivered with a fixed country setting. If you place an AP with a fixed country setting into a group that has a different country configuration, the AP will fail to be synchronized. (The error **Incompatible settings** will be displayed on the **Controlled APs >> Overview > Discovered APs** page).

Caution: **Selecting the wrong country may result in illegal operation and may cause harmful interference to other systems. Please consult with a professional installer who is trained in RF installation and knowledgeable about local regulations to ensure that the AP is operating in accordance with channel, power, indoor/outdoor restrictions and license requirements for the intended country.**

Broadcast filtering

Broadcast filtering is a new feature that is designed to help conserve wireless bandwidth by filtering out non-essential broadcast traffic.

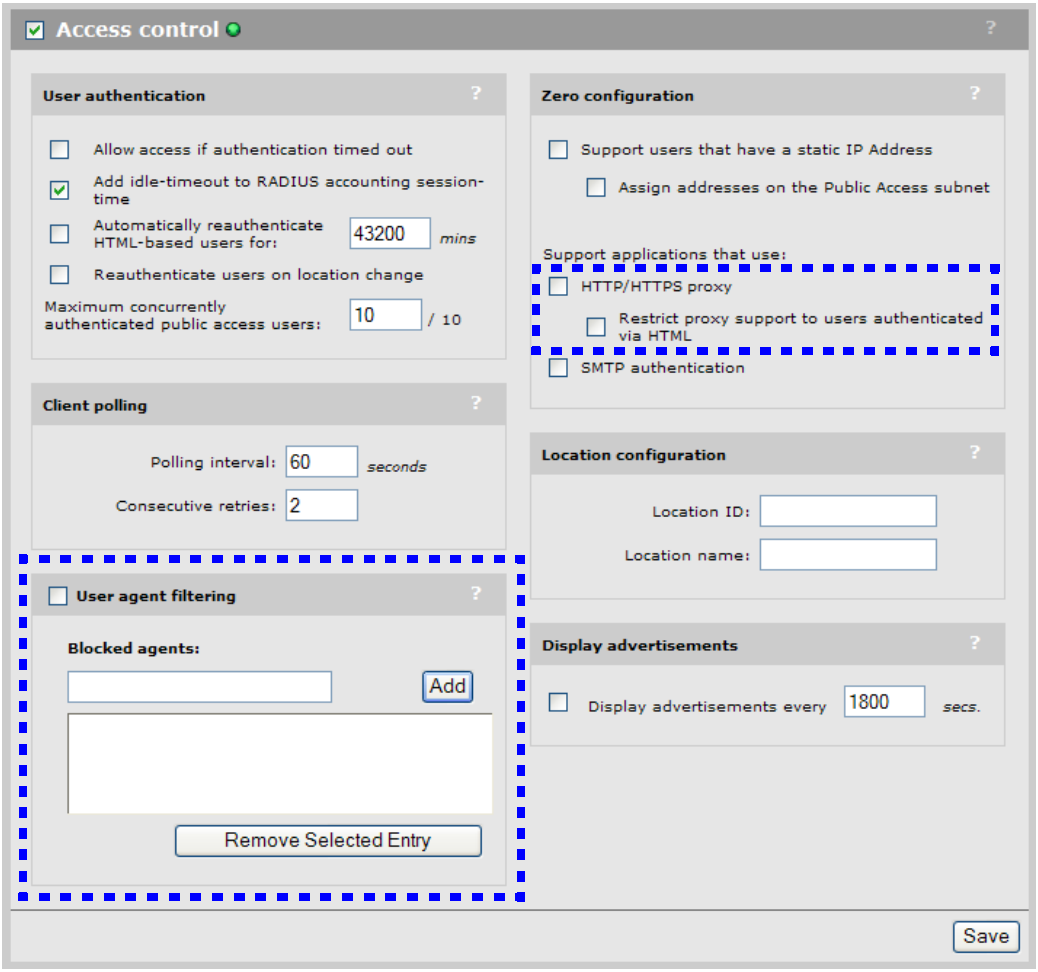
Broadcast filtering is supported by all HP APs. It is configured individually for each VSC (under Virtual AP) as follows:



When broadcast filtering is enabled, the AP filters out all DHCP and ARP broadcasts that are not intended for wireless clients that are known to the AP.

New access control features

The following new features have been added to the **Controller >> Public access > Access control** page.



User agent filtering

This new feature enables you to block HTTP login requests coming from unauthorized client applications. Filtering occurs via the user-agent string that web-based applications use to identify themselves to their peers.

To configure this feature, select **Controller >> Public access > Access control**.

When **User agent filtering** is enabled, the controller checks the user-agent string in all incoming HTTP requests against the **Blocked agents** list. If a match is found, the HTTP request is blocked.

For example, add the word **Torrent** to the list to stop HTTP login requests coming from the BitTorrent 6.3 client application.

A list of user agents strings can be found here:
http://www.useragentstring.com/pages/useragentstring.php

HTTP/HTTPS proxy

The HTTP proxy support option that was available in previous releases has been enhanced to include support for HTTPS.

This allows the controller to support clients that use application software (such as a web browser) configured to use a proxy server for HTTP and HTTPS, without reconfiguration of the application software.

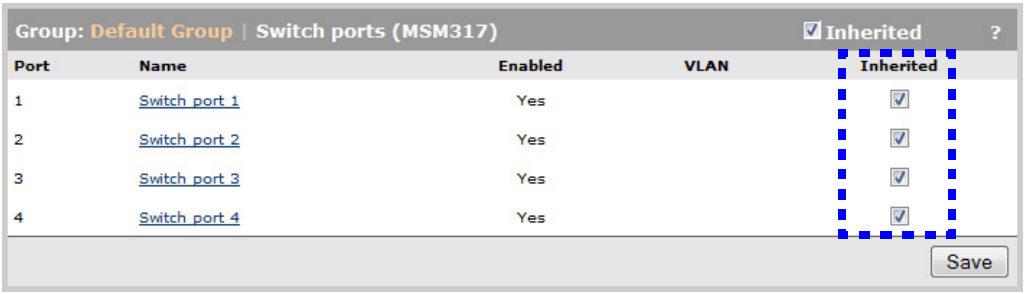
Use the new setting **Restrict proxy support to users authenticated via HTML** to restrict proxy support to users who logged in via the public access login page. Proxy traffic from users authenticated via other methods is blocked.

When this feature is enabled, ensure that clients:

- Do not use a proxy server on ports 21, 23, 25, 110, 443, 8080, or 8090. To support ports 8080 and 8090, change the port settings under **Public access > Web server > Ports**.
- Use the same proxy server address and port number for both HTTP and HTTPS.

Inheritance for MSM317 switch ports

Inheritance of port settings can now be configured individually for each switch port. To do this, select **Controlled APs > [*group*] >> Configuration > Switch ports**.

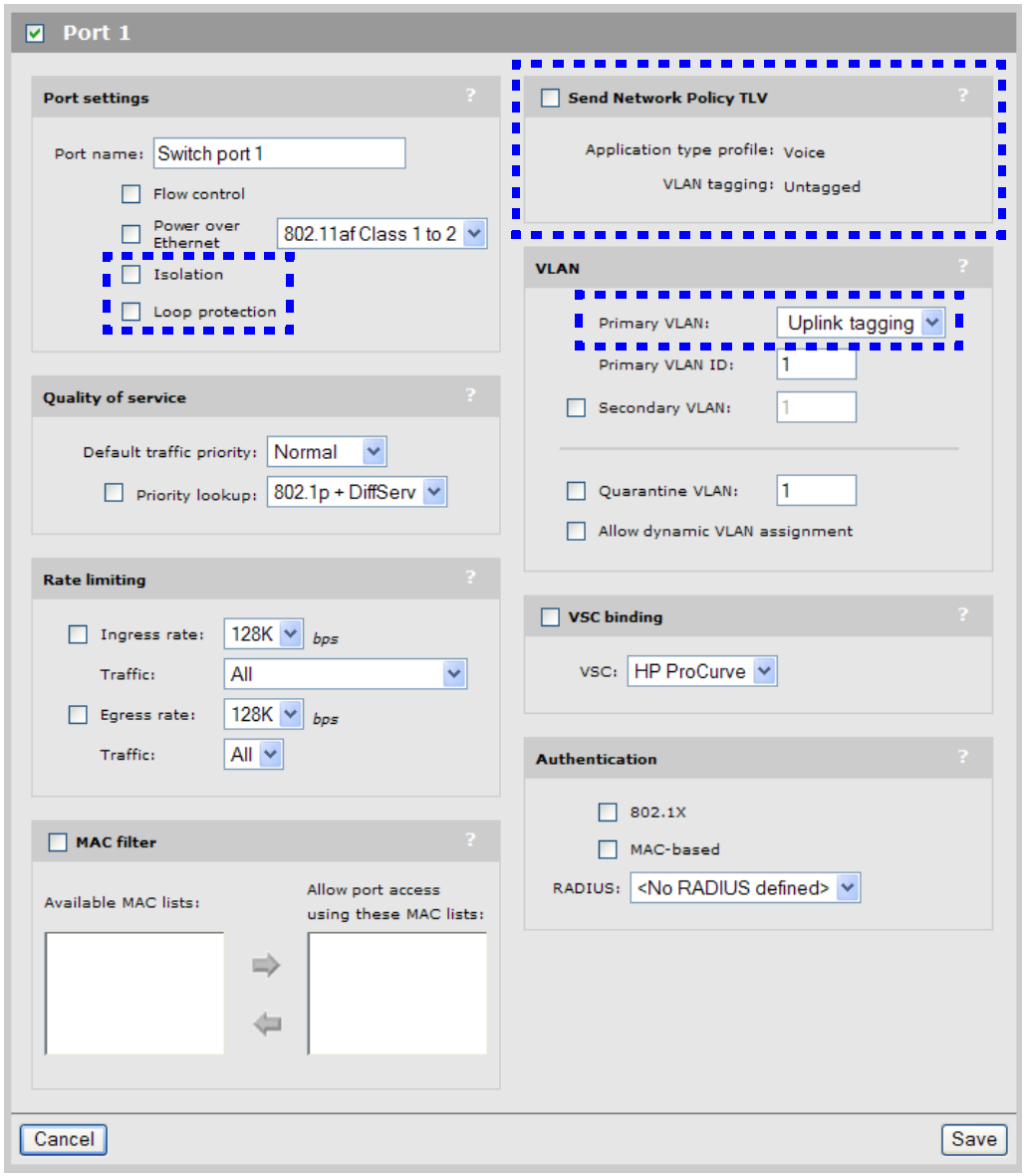


Clear the **Inherited** checkbox at the top of the page and enable individual checkboxes in the table for each port as required.

New MSM317 switch port features

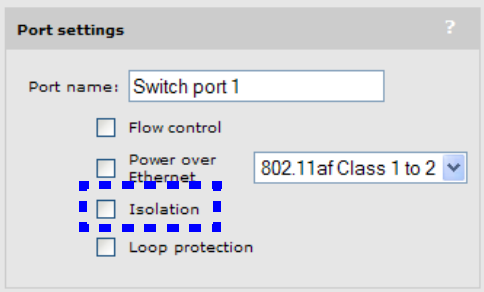
The following new features have been added to the MSM317 switch ports. To configure these features, select **Controlled APs >> Configuration > Switch ports > [***switch-port***]**.

For example, if you select switch port 1, you will see a page similar to this:



Isolation

This new option allows you to isolate individual switch ports on the MSM317.



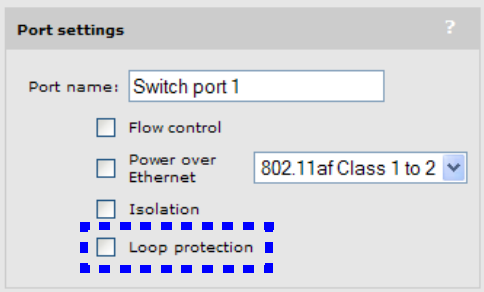
When this feature is enabled, the port only forwards traffic to the Uplink port, and does not forward or receive traffic from any other switch port.

Note: Port isolation is automatically in effect and does not need to be explicitly enabled in the following cases:

- When the port is bound to a VSC which has the **Always tunnel client traffic** option enabled under **Virtual AP > Client data tunnel**.
- When the MSM317 is being managed by a controller team. (In this case the **Always tunnel client traffic** option under **Virtual AP > Client data tunnel** is automatically enabled.

Loop protection

This new feature provides special protection for loops that can occur when using the switch ports on an MSM317.



All APs provide support for the spanning tree protocol (**Configuration > STP** page) to prevent undesirable loops from occurring in the network that may result in decreased throughput. However, when a switch port is connected to client devices at the edge of the network or to unmanaged switches, STP does not work and should be disabled. Instead, loop protection should be enabled.

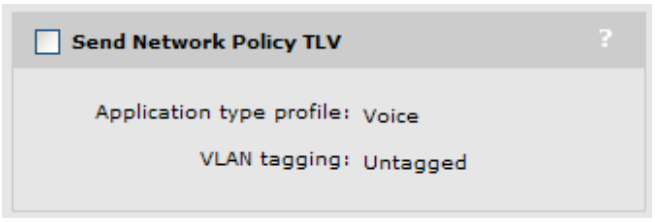
When to use loop protection:

- When 802.1X and/or MAC authentication is enabled on a switch port and a client device is connected to the port. (Network loops may go undetected by STP. For example, STP packets that are looped back to an edge port will not be processed because they have a different broadcast/multicast MAC address from the user's authenticated MAC address.)

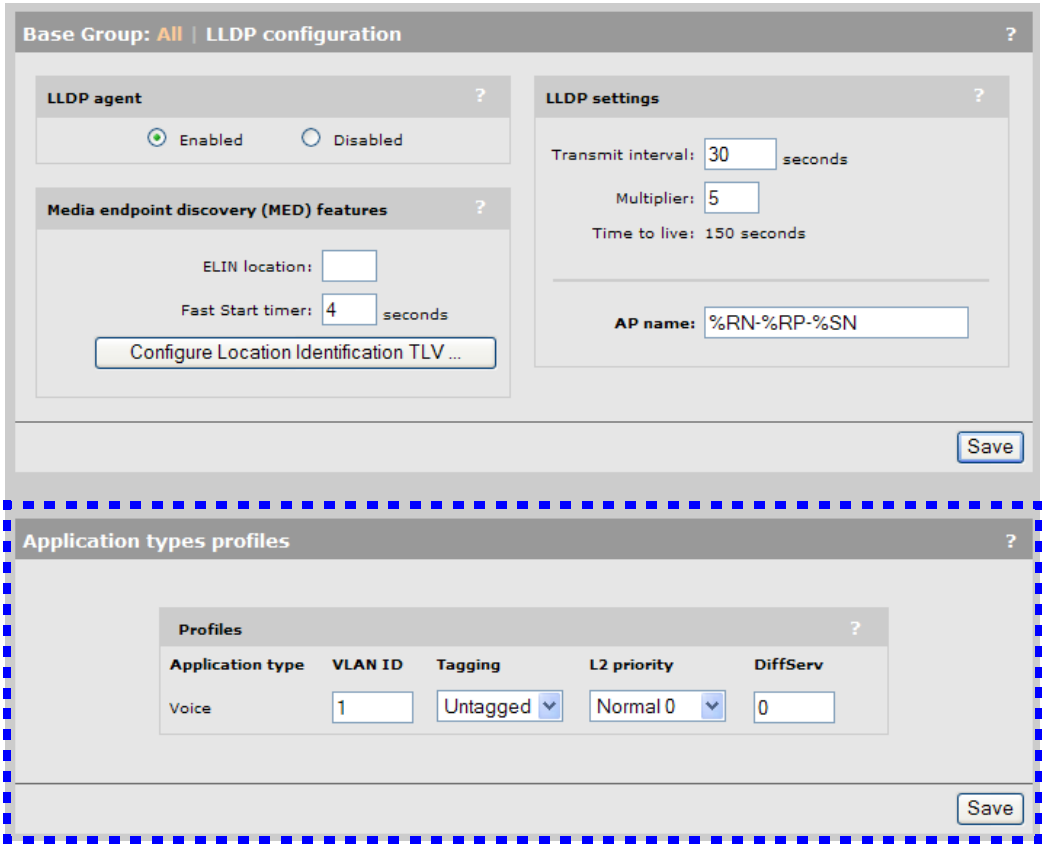
- When a switch port is connected to an unmanaged device. STP cannot detect the formation of loops when there is an unmanaged device on the network that does not process STP packets and simply drops them. Loop protection has no such limitation, and can be used to prevent loops on unmanaged switches.

Send Network Policy TLV

When this new feature is enabled, an MSM317 switch port will send a Network Policy TLV to voice devices such as IP phones, with the values that are defined in the selected application type profile.



In this release, only one application type profile is supported: **Voice**. To configure this profile, select **Controlled APs >> Configuration > LLDP** to open the LLDP configuration page. For example:



Application type profiles

Application type profiles are used to define configuration settings which can be applied to the Application Type field in a Network Policy TLV on a MSM317 switch port.

Application type

This release only supports the **Voice** application type.

VLAN ID
Specify a VLAN ID for this profile. This VLAN will be assigned to the switch port when the profile is used.

VLAN tagging
- **Tagged:** The VLAN is tagged.
- **Untagged:** The VLAN is untagged.

L2 priority
Select the layer 2 priority setting. This setting is used instead of the **Default traffic priority** set for the switch port. Supported settings are:

L2 priority	QoS queue
Low - 1 Low - 2	4
Normal - 0 Normal - 3	3
High - 4 High - 5	2
Very high - 7 Very high - 7	1

DiffServ
This value only applies if **VLAN tagging** is set to **Tagged**.

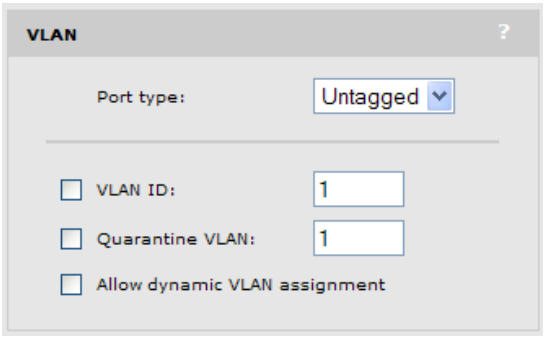
Specify a value for the Differentiated Services codepoint (DSCP) field in IPv4 and IPv6 packet headers (as defined in RFC2474). The codepoint is composed of the six most significant bits of the DS field.

DiffServ codepoint (DSCP) value	QoS queue
> 33	1
26 - 33	2
18 - 25	3
1 - 17	4
0	Disabled

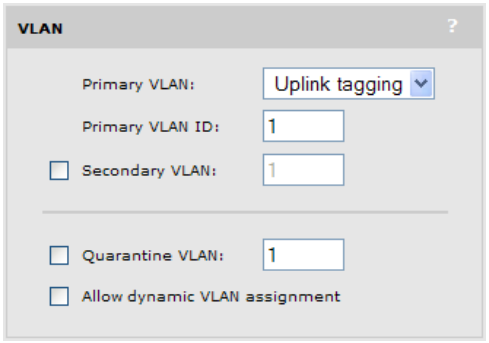
VLAN

This feature has been changed in this release to support a primary and secondary VLAN.

Previous release



This release



Primary VLAN

Possible settings and their effects are as follows:

Option	Incoming traffic on the port	Outgoing traffic on the port	Uplink port
Untagged	Untagged.	Untagged.	Untagged.
Tagged	Tagged with the **Primary VLAN ID**.	Tagged with the **Primary VLAN ID**.	Tagged with the **Primary VLAN ID**.
Uplink tagging	Untagged.	Untagged.	Tagged with the **Primary VLAN ID**.

This table only applies when the following options are disabled:

- Quarantine VLAN
- Allow dynamic VLAN assignment

Notes on Uplink tagging

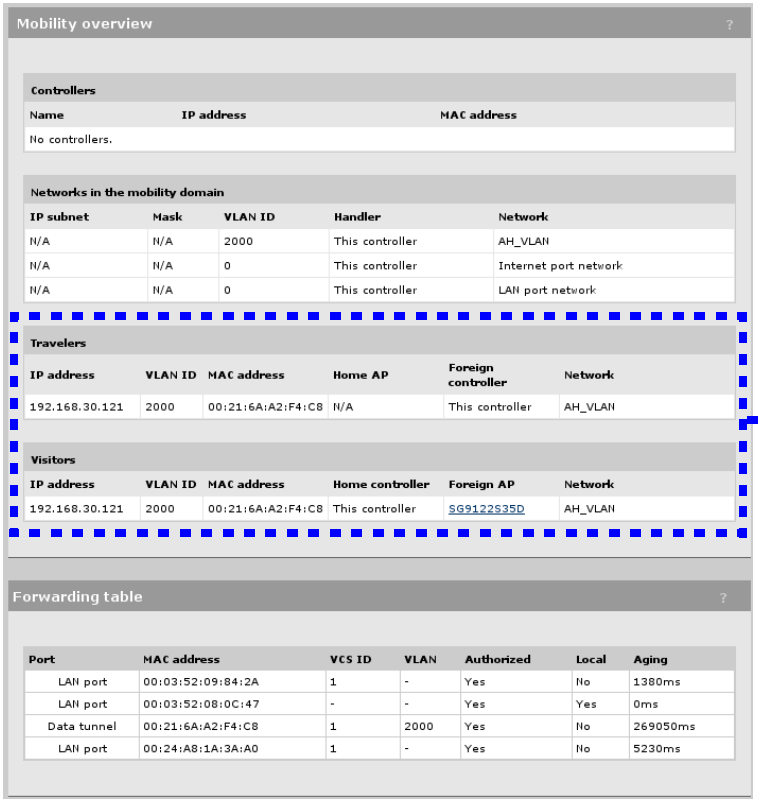
When the **Uplink tagging** option is selected, incoming and outgoing traffic on ports 1 to 4 is untagged. Internally however, the traffic is tagged with the **Primary VLAN ID**. This means that if two ports are set to **Uplink tagging** with different **Primary VLAN ID**s, then traffic cannot be exchanged between the two ports.

For complete information, see the *MSM7xx Controllers Management and Configuration Guide* and the online help.

Improved mobility status information

The mobility overview status page has been redesigned to make it easier to track roaming clients. To see the new page, select **Controller >> Status Mobility**. For example:

Previous release



Mobility overview

Controllers

Name	IP address	MAC address
No controllers.		

Networks in the mobility domain

IP subnet	Mask	VLAN ID	Handler	Network
N/A	N/A	2000	This controller	AH_VLAN
N/A	N/A	0	This controller	Internet port network
N/A	N/A	0	This controller	LAN port network

Travelers

IP address	VLAN ID	MAC address	Home AP	Foreign controller	Network
192.168.30.121	2000	00:21:6A:A2:F4:C8	N/A	This controller	AH_VLAN

Visitors

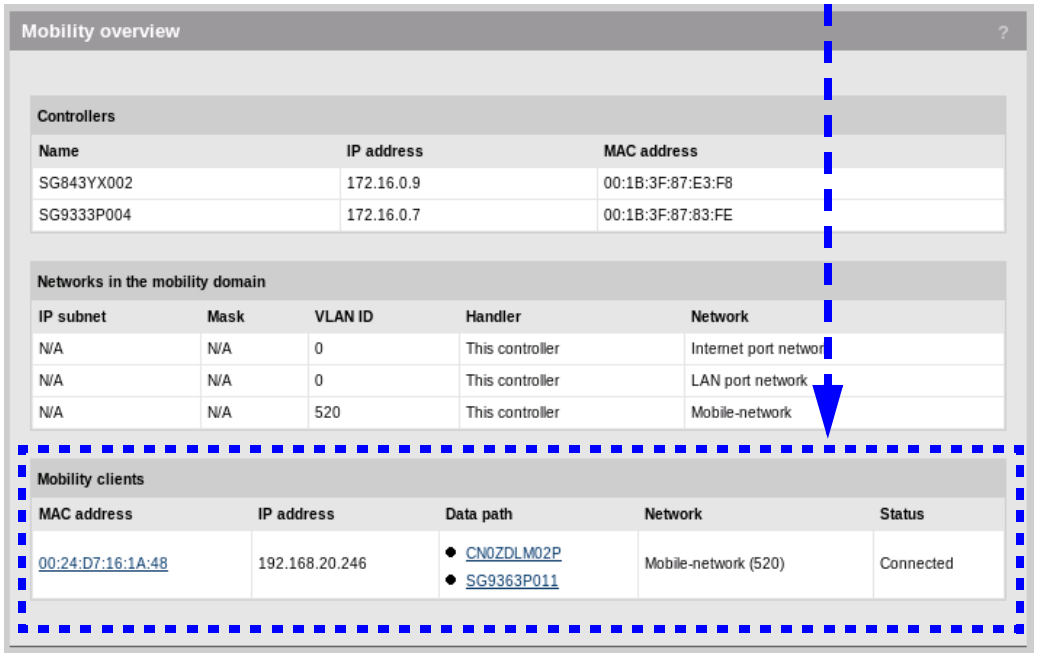
IP address	VLAN ID	MAC address	Home controller	Foreign AP	Network
192.168.30.121	2000	00:21:6A:A2:F4:C8	This controller	SG9122S35D	AH_VLAN

Forwarding table

Port	MAC address	VCS ID	VLAN	Authorized	Local	Aging
LAN port	00:03:52:09:84:2A	1	-	Yes	No	1380ms
LAN port	00:03:52:08:0C:47	-	-	Yes	Yes	0ms
Data tunnel	00:21:6A:A2:F4:C8	1	2000	Yes	No	269050ms
LAN port	00:24:A8:1A:3A:A0	1	-	Yes	No	5230ms

The Travelers and Visitors tables have been replaced by Mobility clients table.

This release



Mobility overview

Controllers

Name	IP address	MAC address
SG843YX002	172.16.0.9	00:1B:3F:87:E3:F8
SG9333P004	172.16.0.7	00:1B:3F:87:83:FE

Networks in the mobility domain

IP subnet	Mask	VLAN ID	Handler	Network
N/A	N/A	0	This controller	Internet port networ
N/A	N/A	0	This controller	LAN port network
N/A	N/A	520	This controller	Mobile-network

Mobility clients

MAC address	IP address	Data path	Network	Status
00:24:D7:16:1A:48	192.168.20.246	CN0ZDLM02P SG9363P011	Mobile-network (520)	Connected

Mobility clients

MAC address
Media access control (hardware) address of the client. Select the address to see a log of mobility-related events for the client. For details, see <x_Xref>Mobility client event log on page 5-34.

IP address
IP address of the client.

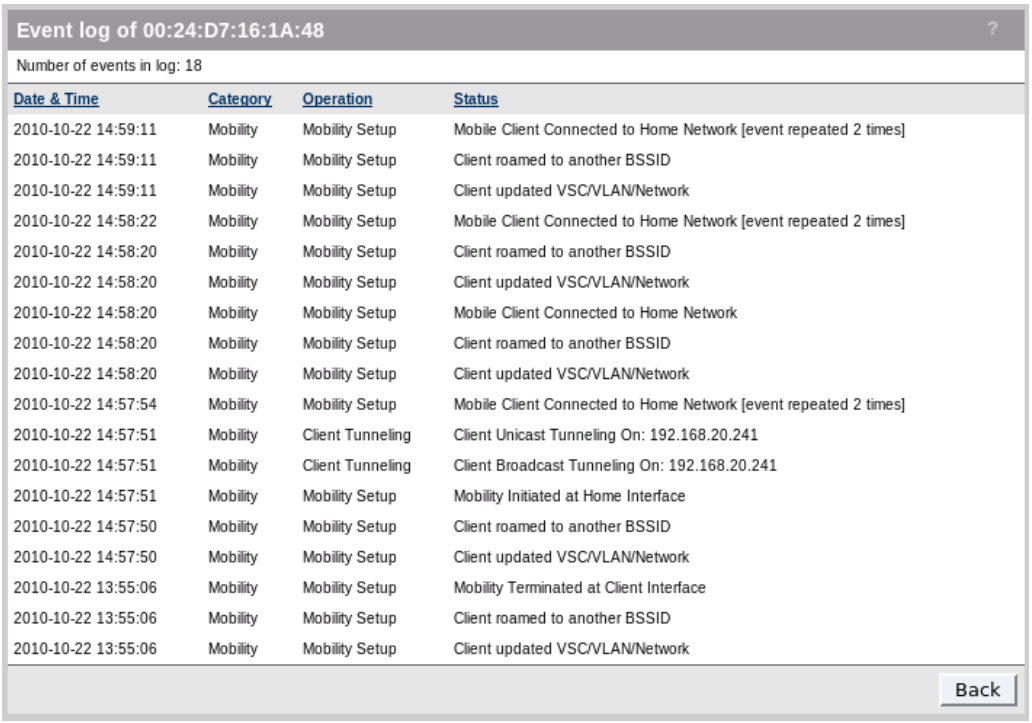
Data path
Lists all the APs and controllers that are in the data path between the client and their home network.

Network
The name of the client's home network.

Status
Possible values are:

- **Connected:** The client is connected to their home network.
- **Blocked:** Client data transfer is blocked because the home network could not be found.

Mobility client event log
This page lists all events for a roaming client.



Event log of 00:24:D7:16:1A:48

Number of events in log: 18

Date & Time	Category	Operation	Status
2010-10-22 14:59:11	Mobility	Mobility Setup	Mobile Client Connected to Home Network [event repeated 2 times]
2010-10-22 14:59:11	Mobility	Mobility Setup	Client roamed to another BSSID
2010-10-22 14:59:11	Mobility	Mobility Setup	Client updated VSC/VLAN/Network
2010-10-22 14:58:22	Mobility	Mobility Setup	Mobile Client Connected to Home Network [event repeated 2 times]
2010-10-22 14:58:20	Mobility	Mobility Setup	Client roamed to another BSSID
2010-10-22 14:58:20	Mobility	Mobility Setup	Client updated VSC/VLAN/Network
2010-10-22 14:58:20	Mobility	Mobility Setup	Mobile Client Connected to Home Network
2010-10-22 14:58:20	Mobility	Mobility Setup	Client roamed to another BSSID
2010-10-22 14:58:20	Mobility	Mobility Setup	Client updated VSC/VLAN/Network
2010-10-22 14:57:54	Mobility	Mobility Setup	Mobile Client Connected to Home Network [event repeated 2 times]
2010-10-22 14:57:51	Mobility	Client Tunneling	Client Unicast Tunneling On: 192.168.20.241
2010-10-22 14:57:51	Mobility	Client Tunneling	Client Broadcast Tunneling On: 192.168.20.241
2010-10-22 14:57:51	Mobility	Mobility Setup	Mobility Initiated at Home Interface
2010-10-22 14:57:50	Mobility	Mobility Setup	Client roamed to another BSSID
2010-10-22 14:57:50	Mobility	Mobility Setup	Client updated VSC/VLAN/Network
2010-10-22 13:55:06	Mobility	Mobility Setup	Mobility Terminated at Client Interface
2010-10-22 13:55:06	Mobility	Mobility Setup	Client roamed to another BSSID
2010-10-22 13:55:06	Mobility	Mobility Setup	Client updated VSC/VLAN/Network

Back

For complete information, see also the *MSM7xx Controllers Management and Configuration Guide* and the online help.

Manager login credentials reset

This new feature provides a secure way to reset the manager login username and password on a controller to their factory default values (**admin**), without having to reset the entire configuration to its factory default settings. To make use of this feature you must be able to access the controller through its console (serial) port, therefore this feature is not supported on the MSM765.

- This feature is enabled by default and also after performing a factory reset.
- This feature is automatically **disabled** after performing a software (firmware) update. You can re-enable this feature if desired.

Caution: **SECURITY: When this feature is enabled, physical security of the console port is extremely important. It is advised that you do not connect unprotected network access to the console port when this feature is enabled.**

For specific directions, see *To reset manager credentials on a controller* in the *MSM7xx Controllers Management and Configuration Guide*.

PayPal support

Support for PayPal has been added to the payment services feature for the public access interface. To take advantage of PayPal you need to:

- Open a PayPal business account and become familiar with your responsibilities as a merchant.
- Obtain basic knowledge of the PayPal Express Checkout API (version 63.0 or higher) so you will be able to successfully customize the PayPal public access web pages if required.

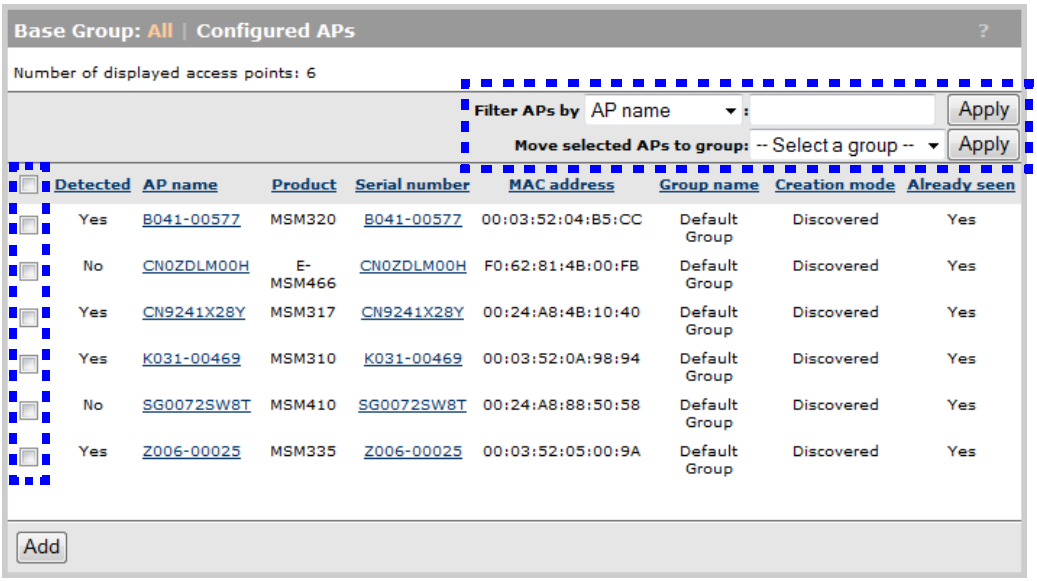
Important

PayPal offers many different methods for deducting funds from a customer account. However, the controller only supports methods that provide immediate resolution. Any kind of deferred payment is not supported. As a result, when PayPal displays payment options to the user, only instant payment options are shown. If a user's PayPal account does not support instant payment, then they will not be able to purchase services.

For complete information, see the *MSM7xx Controllers Management and Configuration Guide* and the online help.

AP management enhancements

Two new features have been added to the help with AP management tasks. To access these features, select **Controlled APs >> Overview > Configured APs** or **Controlled APs > [*Group*] >> Overview > Configured APs**. For example:



Filter APs by

This new filter enables you to more easily find APs on the Configured APs page.

To narrow down the list of APs in the table, select a category and enter text on which to filter the AP list. Click **Apply** to activate the filter.

Available categories include:

- AP name
- Product
- Serial number
- MAC address

To deactivate the filter, clear the filter text and then select **Apply**.

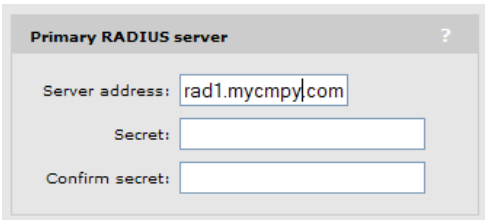
Moving multiple APs between groups

You can now more easily move one or more APs between groups. To move APs, do the following:

1. Use the check boxes in the table to select one or more APs. Click the check box in the table header to select all the APs in the table.
2. To the right of **Move selected APs to group**, select the group into which you wish to move the selected APs.
3. Select **Apply**.

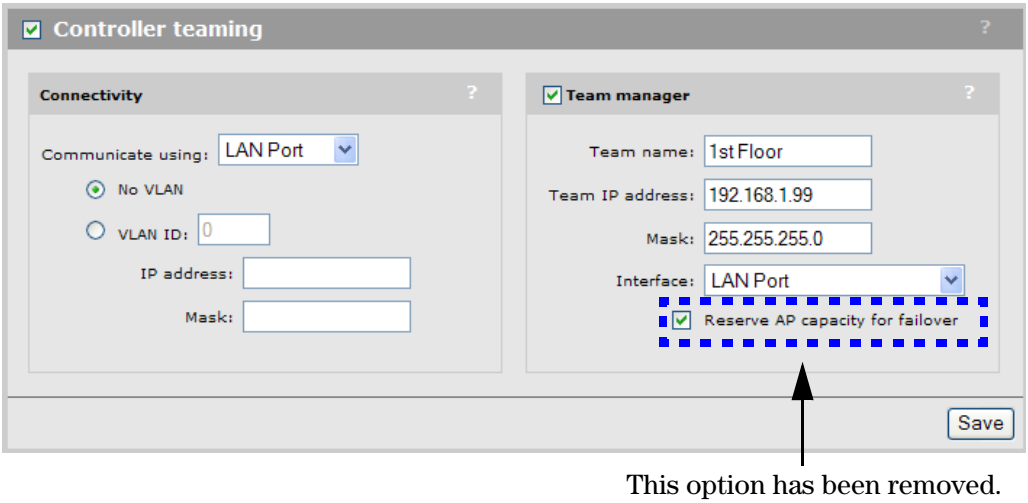
Identify RADIUS server by host name

When defining a RADIUS profile (on the **Controller >> Authentication > RADIUS** page) you can now identify the primary and secondary RADIUS server by their IP address ***or*** their fully-qualified domain name.



Teaming change

The teaming feature **Reserve AP capacity for failover** has been removed from the **Controller >> Management > Teaming** page.



This means that a team can no longer be configured to automatically limit the number of deployed APs to ensure support for N+1 redundancy. Planning for redundancy must now always be done manually. The following is an extract from the online help for this release which describes the new functionality.

> During normal operation, the team manager and team members are in continuous contact to ensure the integrity of the team. This allows for quick detection of an inoperative or unreachable team member, and implementation of failover procedures to ensure continuity of network services.
>
> **Note:** When a team member becomes inoperative and failover occurs, all services provided by the failed controller are temporarily interrupted. Once failover is complete and services return, users that were connected to an access-controlled VSC on this controller must login again.

Supporting N + N redundancy

A controller team can be configured to provide different levels of redundancy, from N + 1 up to N + 3. Use the following formula to calculate the number of team members you will need based on the number of APs that you want to deploy and the required level of redundancy.

Required team members = (*APs* / 200) + *Redundancy_level*

(If there is a remainder after performing the division, round up.)

Where:

- *APs* is the total number of APs you want to deploy. You must buy one license for each controlled AP. Although licenses are installed on individual team members, licenses are pooled across the entire team and are automatically re-allocated when a team member becomes inoperative.
- *Redundancy_level*: This is the number of redundant controllers that you want to support: 1, 2, or 3.

For example:

Number of APs you want to deploy	APs / 200	Number of team members required to support redundancy		
		N + 1	N + 2	N + 3
120	.6	2	3	4
200	1	2	3	4
400	2	3	4	5
440	2.2	4	5	-
520	2.6	4	5	-
600	3	4	5	-
800	4	5	-	-

Another way to look at it is as follows:

Number of team members	Maximum AP licences that can be installed	Maximum APs you can deploy to ensure redundancy		
		N + 1	N + 2	N +3
2	400	200	-	-
3	600	400	200	-
4	800	600	400	200
5	800	800	600	400

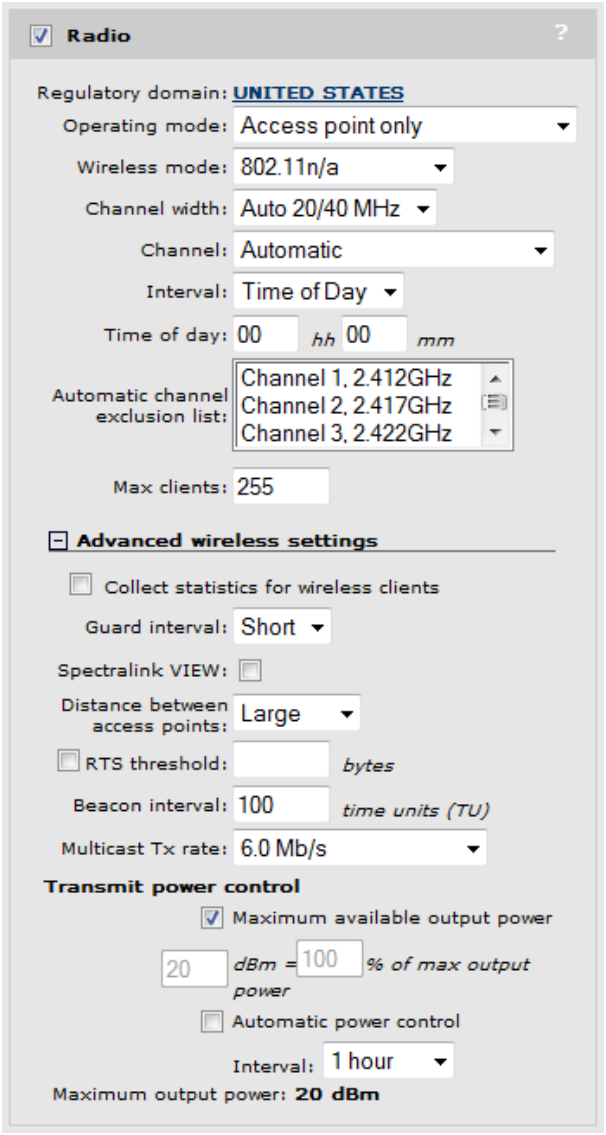
A team supports a maximum of 800 APs and 5 team members.

Radio page changes

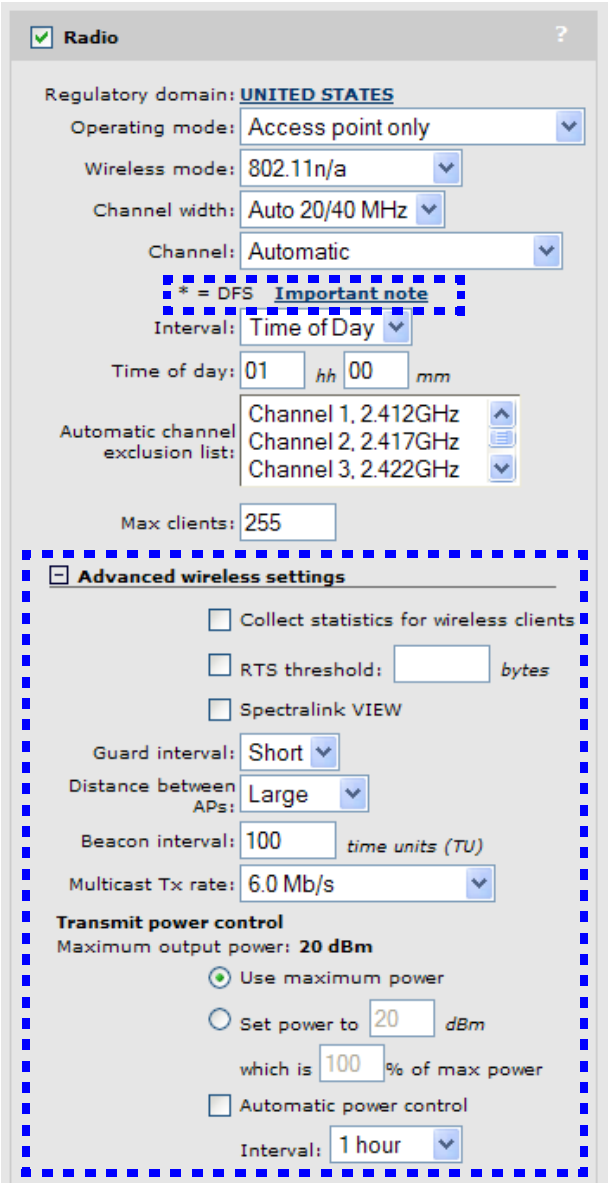
- Advanced wireless options have been re-organized.
- DFS message has been moved into the online help.

(See also the *Wireless Configuration* chapter of the *MSM7xx Controllers Management and Configuration Guide* and the online help.)

Previous release



This release

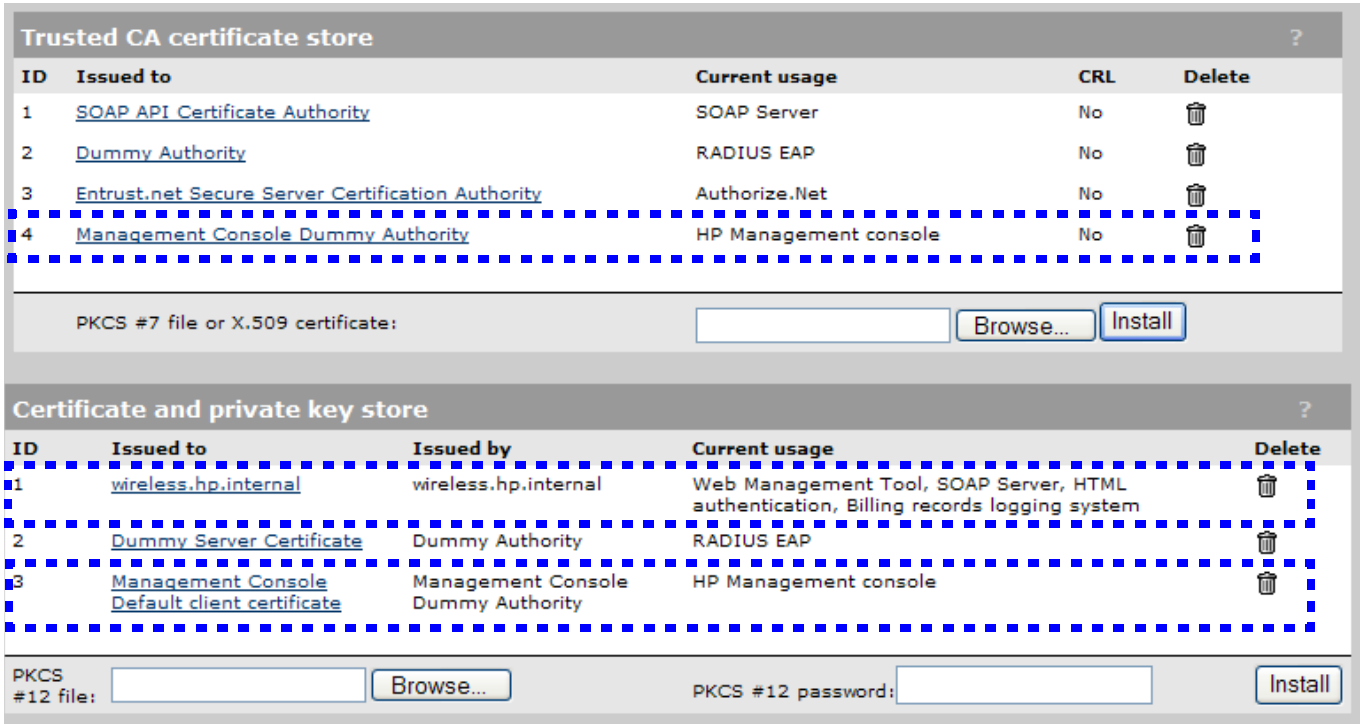


Certificates page changes

The following certificates have been added to support communication with HP PCM/PMM software:

- **Management Console Dummy Authority:** Used when the management tool communicates with HP PCM/PMM software.
- **Management Default client certificate:** This certificate is used to identify the management tool when it communicates with HP PCM/PMM software.

The certificate **wireless.hp.internal** was called wireless.colubris.com in the previous release.



Fixes

The following issues have been fixed since release 5.4.2.0:

ID	Description
48184	If you enable teaming on a controller before installing the Premium license, the controller will not be able to join a team.
50669	When working with a controller team, if you enable the **Terminate WPA at the controller** option on a VSC, then all team members, including the team manager, must be restarted to properly activate the feature.
52310	There is no log message to indicate that the maximum number of clients has been reached on a VSC or on a radio.
53644	If you change the team IP address or change other team-related settings on the team manager, the team manager may lose its IP address. To prevent this from occurring, restart the team manager after making these types of changes.
53948	If you configure the local DHCP server on a VSC to operate on the subnet 192.168.1.x/24, the route for users on this subnet will be deleted if the controller is restarted. The subnet 192.168.1.x/24 should not be used by a DHCP server on a VSC.
54816	When controller teaming is active, creating a second VSC will disconnect any clients connected on the first VSC. A restart of the team is necessary to re-establish the connections
55395	(Only Mobility Traffic Manager.) The MSM765 sometimes reboots due to a memory issue.
56736	APs fail to synchronize when the time zone is set to Iraq or Saudi Arabia.
57491	When adding a new member to a controller team, in some cases the new member will cycle between "Uploading configuration" and "Resetting configuration" states.
59033	When using a controller team, access-controlled clients may be unable to access the network when roaming between APs.
59463	(Only Teaming mode.) The team IP address is lost after changing the system time significantly enough to invalidate the lease received. It is strongly recommended that you use a static IP address for the Internet Port to avoid this issue.
60483	(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.
63392	When you have many clients active on several APs, the client event log can grow large. Since the AP transfers statistics every 15 seconds, this may cause performance issues on the network and on the controller. In some cases, APs may disappear on the controller.
63520	A memory leak occurs when a Mobile Unit is removed from the Aeroscout system.
64284	(MSM317 only.) If the Inherited checkbox for specific configuration settings on an MSM317 is disabled, the MSM317 is incorrectly marked as unsynchronized when changes are made at the group level.