HP MSM7xx Controllers Release Notes
v6.4.0.0

HP Part Number: 5998-5810
Published: May 2014
Edition: 1

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Acknowledgements

Windows® is a U.S. registered trademark of Microsoft Corporation.

Apple®, Bonjour®, iPad®, iPhone®, and iPod® are trademarks of Apple Inc. iPod is for legal or rightholder-authorized copying only. Don't steal music.

Version: MSM v6.4.0.0

Description

These release notes provide important release-related information.

NOTE: In this document, except when identifying specific models, the generic term "controller" is used in place of MSM7xx Controller product names and the generic term "AP" is used in place of MSM3xx / MSM4xx / HP 425 / HP 517 Access Point product names.

Product models

This document applies to these HP products:

Model	Part
MSM720 Access Controller	J9693A
MSM720 Premium Mobility Controller	J9694A
MSM720 Access Controller (TAA)	J9695A
MSM720 Premium Mobility Controller (TAA)	J9696A
MSM760 Access Controller	J9421A
MSM760 Premium Mobility Controller	J9420A
MSM765 zl Premium Mobility Controller	J9370A
MSM775 zl Premium Controller	J9840A

Online documentation

You can download documentation from the HP Support website at: www.hp.com/support/manuals. Search by product name or part number.

See also the "New in release 6.4.0.0" section of the *MSM7xx Controllers Configuration Guide*.

Software Updates and Licensing portal

The Software Updates and Licensing portal provides access to the latest software updates to customers with a support contract. An HP Passport is required to access the Software Updates and Licensing portal at www.hp.com/go/hpsoftwareupdatesupport and it is available to customers who have purchased a maintenance and support agreement.

Mandatory channel change required prior to software upgrade; discontinue use of channel 132

Applies to these Americas/USA models: MSM410 (J9426A/B), MSM422 (J9358A/B), MSM430 (J9650A), MSM460 (J9590A), MSM466 (J9621A), MSM466-R (J9715A), MSM310 (J9374A/B), MSM310-R (J9380A/B), MSM320 (J9360A/B), MSM320-R (J9365A/B), MSM325 (J9369A/B).

IMPORTANT: Prior to upgrading to MSM software version 6.4.0.0, all applicable APs (autonomous or controlled) that are manually configured to use channel 132 must be either reconfigured to use a different channel or be reconfigured to use auto channel. This is required because channel 132 is no longer available for use.

NOTE: Due to a problem with AP channel use validation, a banner similar to this may appear at the top of the Home screen: `AP CNxxxxxxxx, Radio 1 channel configuration has been set to autochannel because the previously configured channel is not supported by this version of software.` The same message is added to the system log. These messages can be safely ignored.

Software configuration change may be required prior to upgrade

If the MSM7xx Controller is configured with the NAT feature enabled (default setting) and with the **Extend VSC egress subnet to VSC ingress subnet** feature enabled (disabled by default), the MSM software v6.4.x, v6.3.x, or v6.2.x will disable the NAT feature. HP recommends that you review your existing settings and disable one of these features before upgrading to v6.4.x, v6.3.x or v6.2.x.

Updating software

Update the controller software as described in the "Software updates" section of the *MSM7xx Controllers Configuration Guide*. After the controller update is complete, it automatically updates all of its controlled devices to the same software version.

Downgrading software

If you upgrade to version 6.4.0.0 and then wish to return to the version that you had been running prior to upgrading, the configuration that you used originally with that version will still be available.

If you have made configuration changes while using version 6.4.0.0, those changes will not be present when you downgrade to the previous version.

If you factory reset your device after upgrading to version 6.4.0.0, your previous configurations will be lost, and when you downgrade to any previous version you will be in a factory reset state.

MSM management tool requires web browser with SSLv3 support

NOTE: A web browser that supports SSLv3 is mandatory for running the MSM web-based management tool. SSLv3 is supported by Microsoft Internet Explorer 7 and 8 but must be enabled. Microsoft Internet Explorer 9 and later uses SSLv3 only. Mozilla Firefox also supports SSLv3 but support may need to be enabled or you may need to update to a more recent version.

HP 517 802.11ac Unified Walljack support

Support for the HP 517 802.11ac Unified Walljack is added in this release. The HP 517 operates only in controlled mode. It is supported by these controllers: MSM720, MSM760, MSM765 zl, and MSM775 zl.

For more information, see the following documents, available online:

- *HP 517 802.11ac Unified Walljack Quickstart*
- *HP 517 802.11ac Unified Walljack Installation Guide*
- *HP 517 802.11ac Unified Walljack Configuration Guide*

MSM710 Controller support stops at v6.0.x

Support for the discontinued MSM710 Controller is available in software versions prior to v6.2.x. As of v6.2.0.0, support for the MSM710 is dropped.

Note: The HP 425 and HP 517 are not supported by the MSM710 Controller.

MSM335 AP support stops at v6.3.x

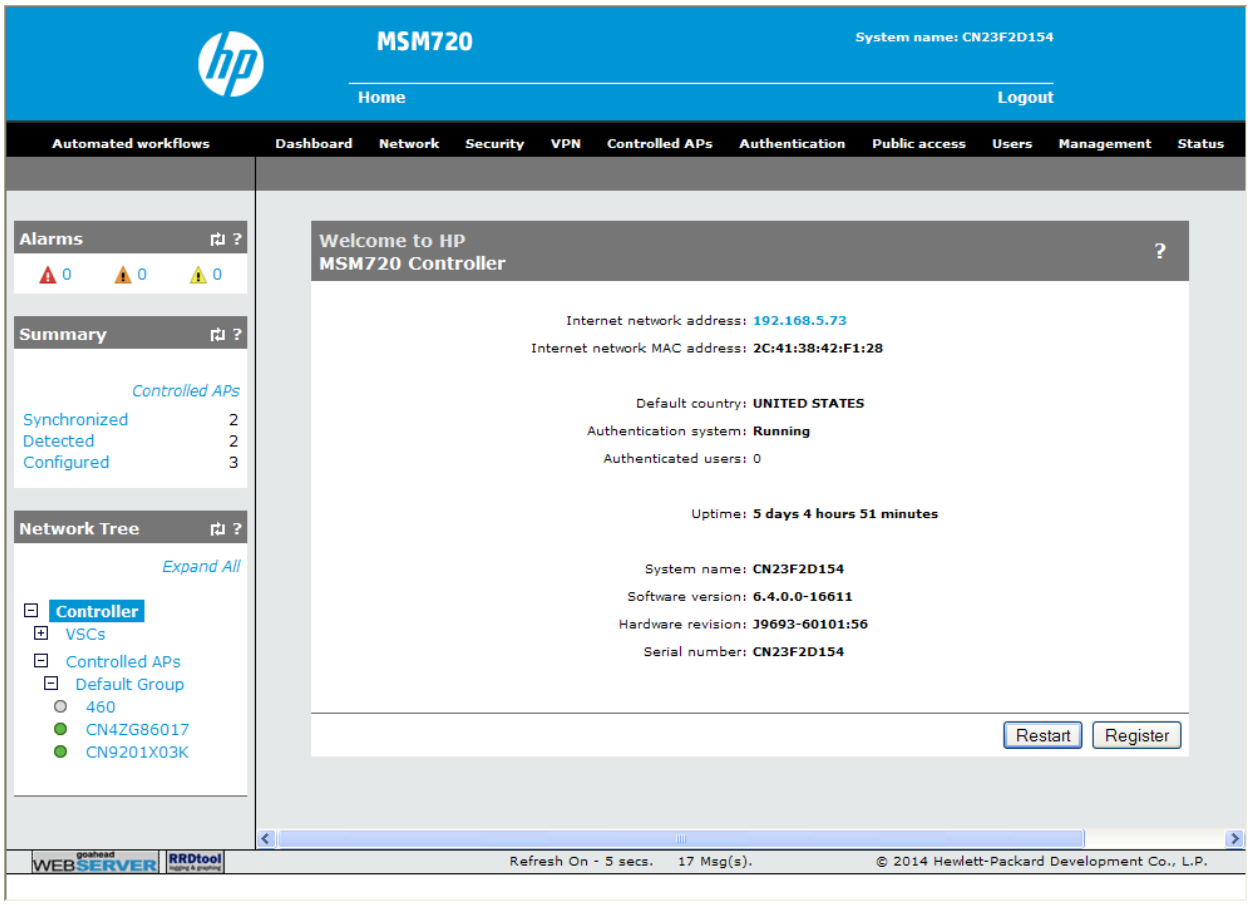
Support for the discontinued MSM335 AP is available in software versions prior to v6.4.x. As of v6.4.0.0, support for the MSM335 AP is dropped.

Changes to the management tool

The following changes have been made to the management tool in this release.

Color and layout changes

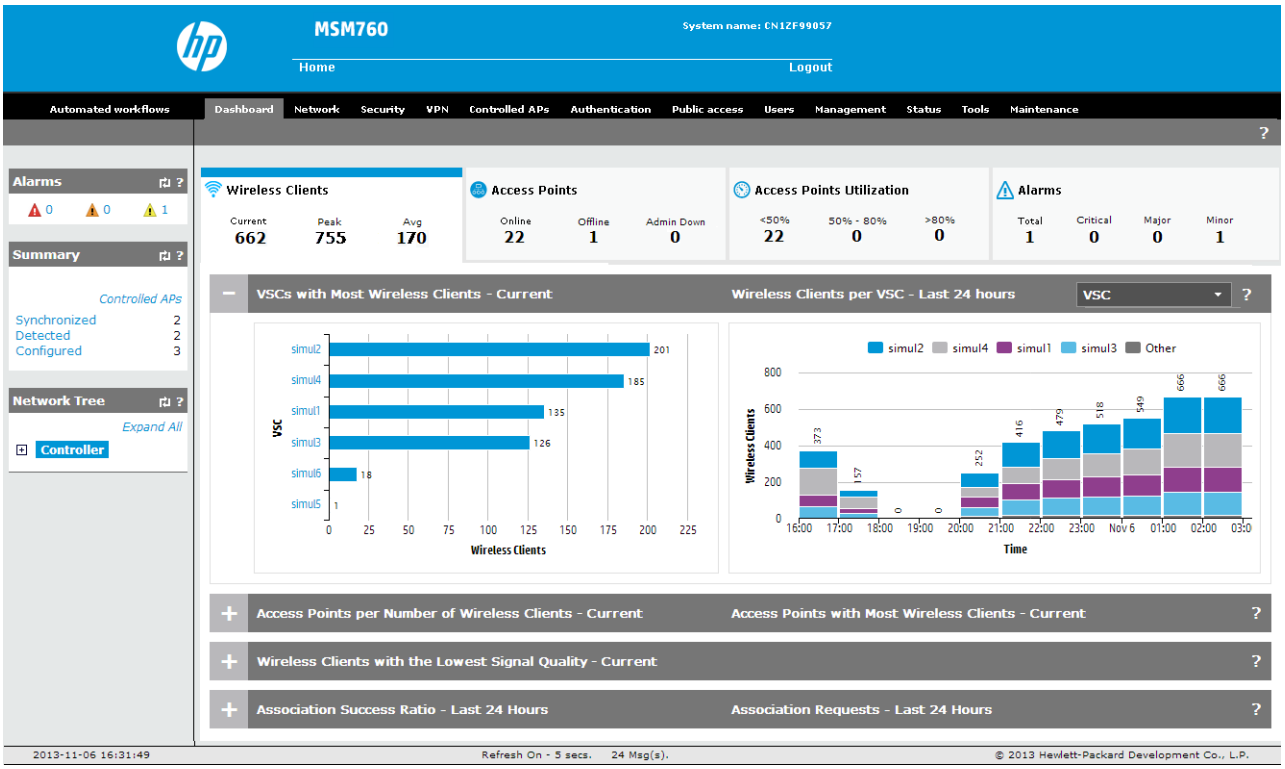
The management tool interface has been updated with minor changes to the color scheme and the layout of some pages. These changes are aesthetic and do not affect the functionality of the pages. For example:



Dashboard feature has been added

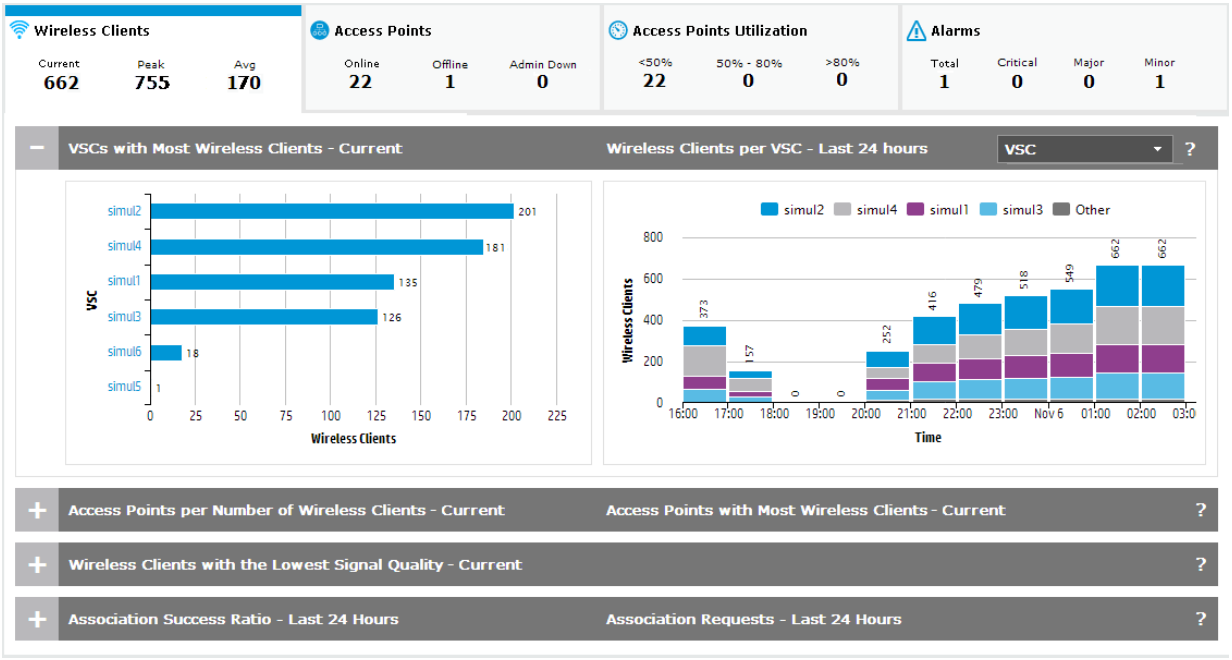
This release includes a new dashboard feature that provides network administrators with a quick way to view key information about the wireless network operation. It uses charts and graphs to display status and statistics, and shows 24-hour history for a number of items.

To view the dashboard, select **Controller >> Dashboard**.



Dashboard groups information into four categories. The top of each tab provides summary statistics for each category.

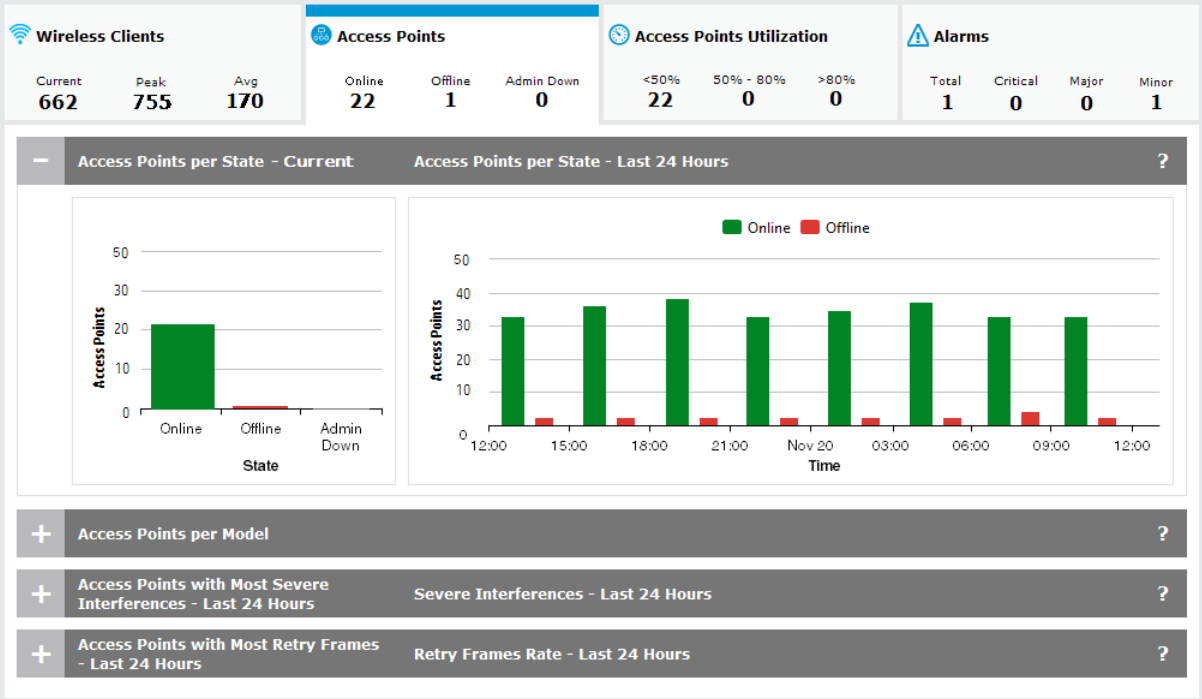
- **Wireless Clients**: Provides information about the wireless clients connected to all controlled APs. For example:



The tab title indicates the number of wireless clients in each of the following categories:

- **Current**: Total number of wireless clients that are currently connected.
- **Peak**: Maximum number of wireless clients that were connected during the last 24 hours.
- **Avg**: Average number of wireless clients that were connected during the last 24 hours.

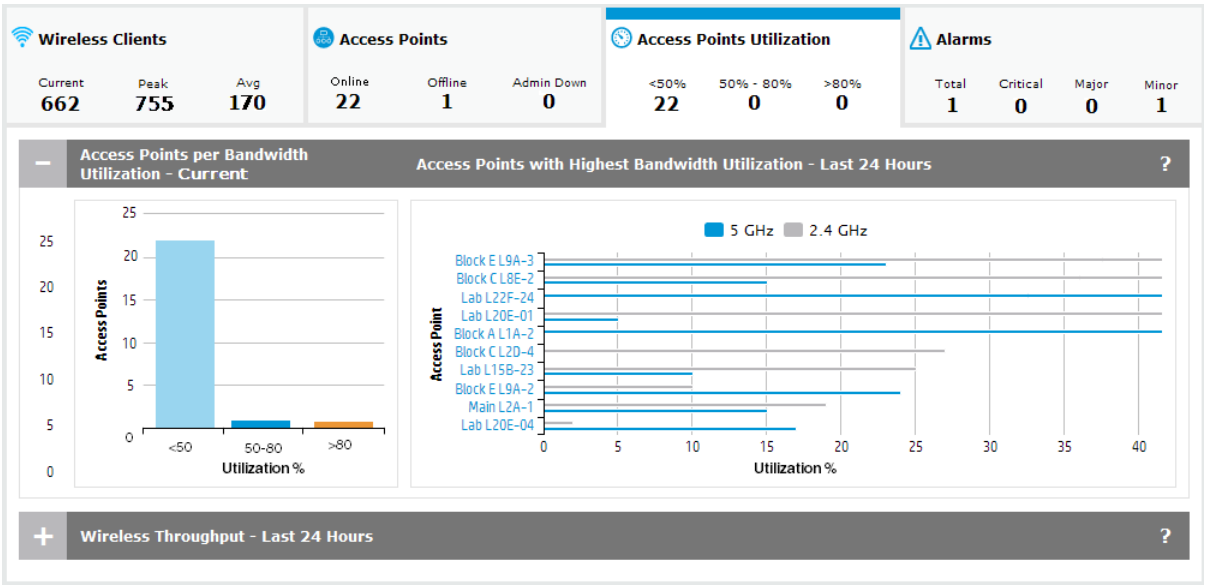
- **Access Points**: Provides information about all controlled APs. For example:



The tab title indicates the number of APs in each of the following states:

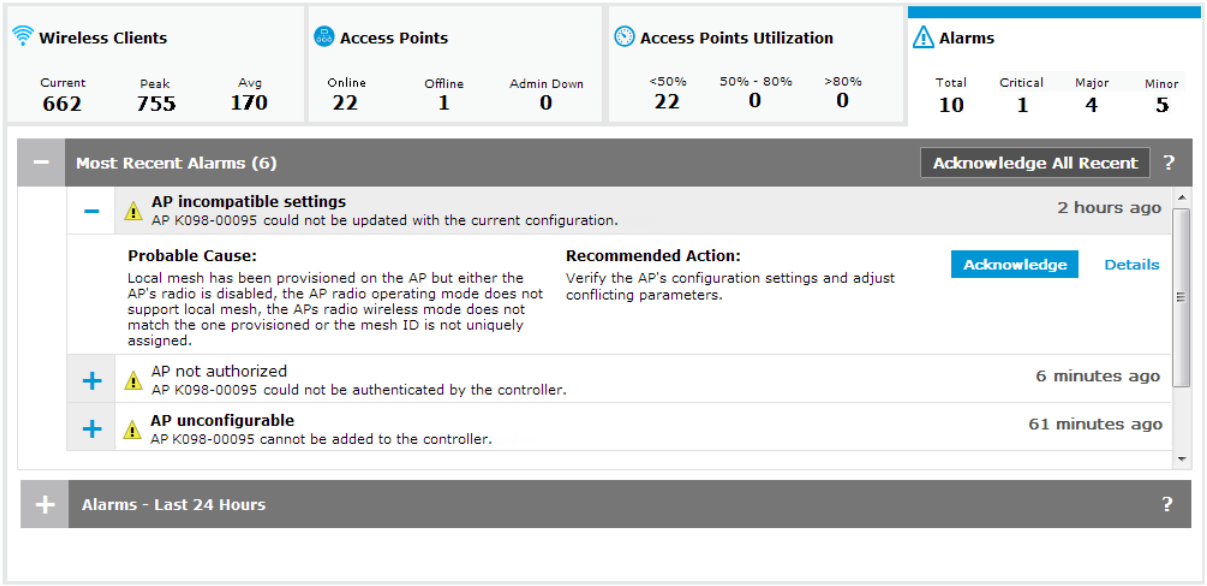
- **Online**: The number of APs that are able to exchange management information with the controller.
- **Offline**: The number of APs that have stopped sending management information to the controller. Rediscovery might re-establish the connection. If not, the APs might have lost power or a network failure has occurred. The APs will have a diagnostic value of **Not responding** on the **Controller >> Controlled APs > Discovered APs** page. APs that are flagged as **Admin Down** do not appear in this count.
- **Admin Down**: The number of APs that are **Offline** and have been manually set to **Admin Down** (Administratively Down) by an administrator. This state is used to flag an AP that is known to be offline. For example, for maintenance or relocation.

- **Access Points Utilization**: Information about the utilization of controlled APs. For example:



The tab title displays the number of APs currently operating in each bandwidth utilization range: <50%, 50% - 80%, >80%. The percent utilization is calculated by comparing the total throughput (transmitted/received) of all radios on an AP for the last minute against the maximum throughput that the radios could theoretically achieve. (Only *online* APs with radios that are enabled and operating in *access point* and/or *local mesh* mode are included.)

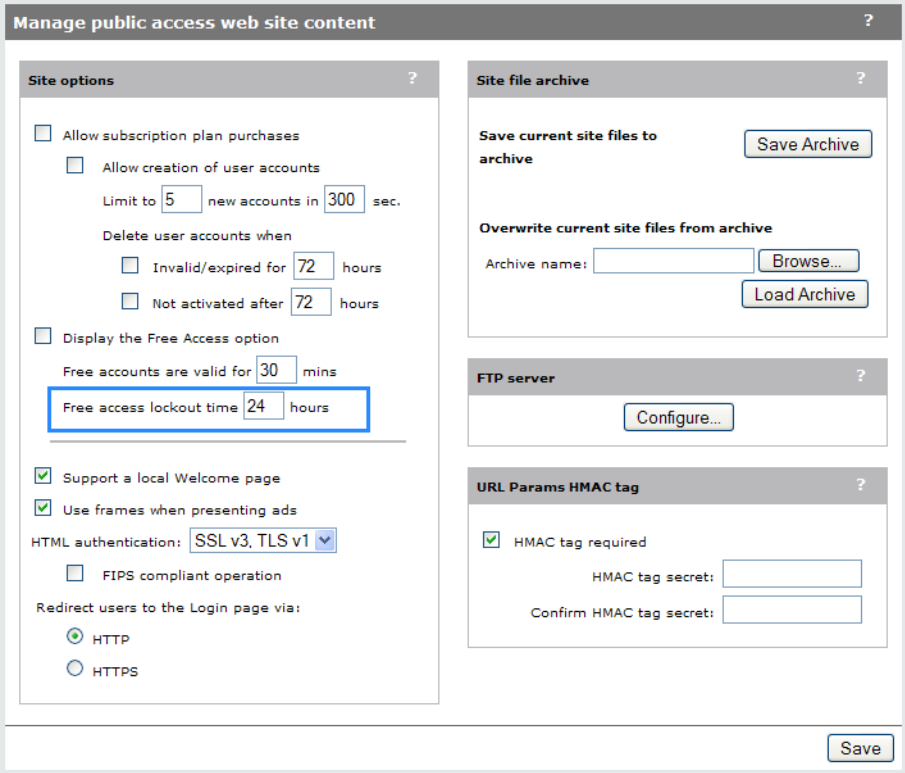
- **Alarms**: A summary of all active alarms. For example:



The tab title displays the total number of active alarms for each severity.

Free access lockout time feature added

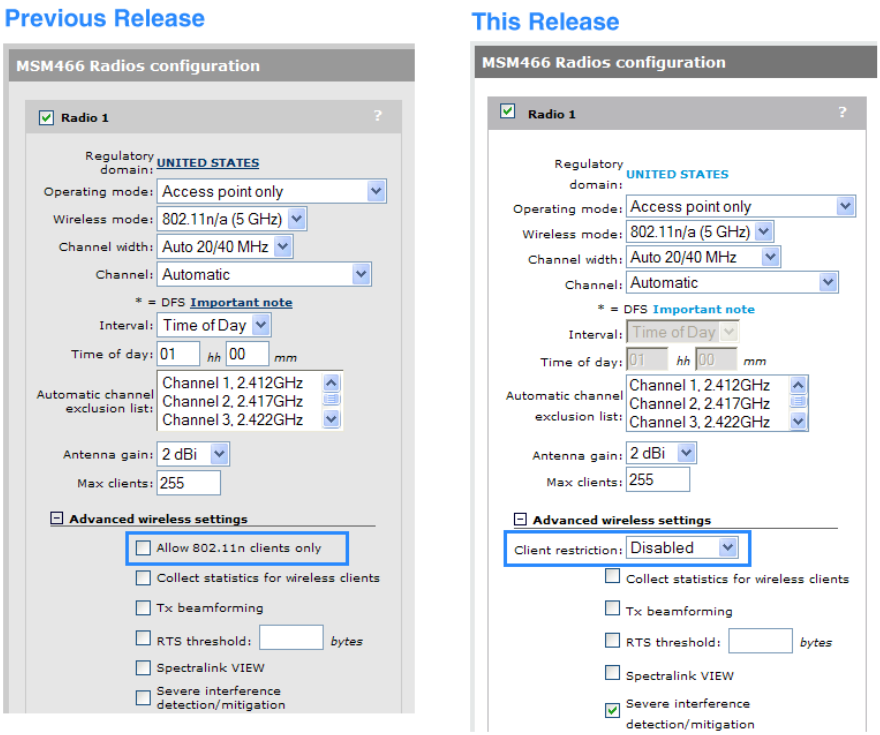
The free access lockout time feature has been added to the **Controller >> Public access > Web content** page. It enables administrators to specify how many hours a user is blocked from using the free account option after their initial free account expires.



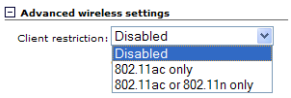
When a user creates a free account, the controller records the MAC address of the client station from which the user logged in. When the free access period expires, this MAC address is then blocked from reusing the free access option for the specified number of hours. If you change the setting for this parameter while a user is blocked, the user remains blocked until after the original setting expires. Range: 1 to 720 hours:

Allow 802.11n clients only parameter renamed

The parameter **Allow 802.11n clients only** on the **Controlled APs >> Radio management > Radio configuration** page has been renamed to **Client restriction**, and new settings have been added to support 802.11ac clients on the HP 517.



New configuration options for the HP 517 have been added.



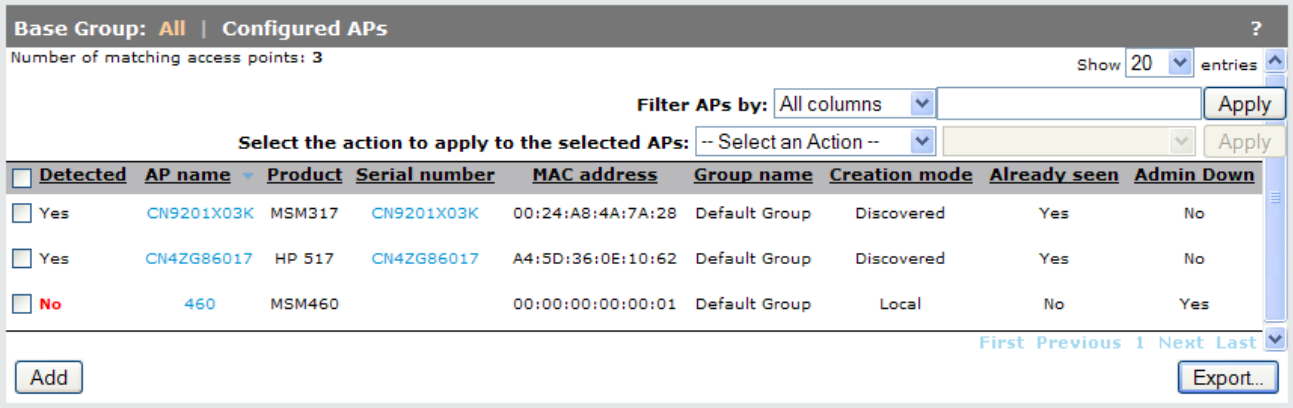
Use this parameter to restrict access to the wireless network to specific types of wireless clients.

NOTE: This parameter is only configurable when **Wireless mode** supports 802.11ac or 802.11n.

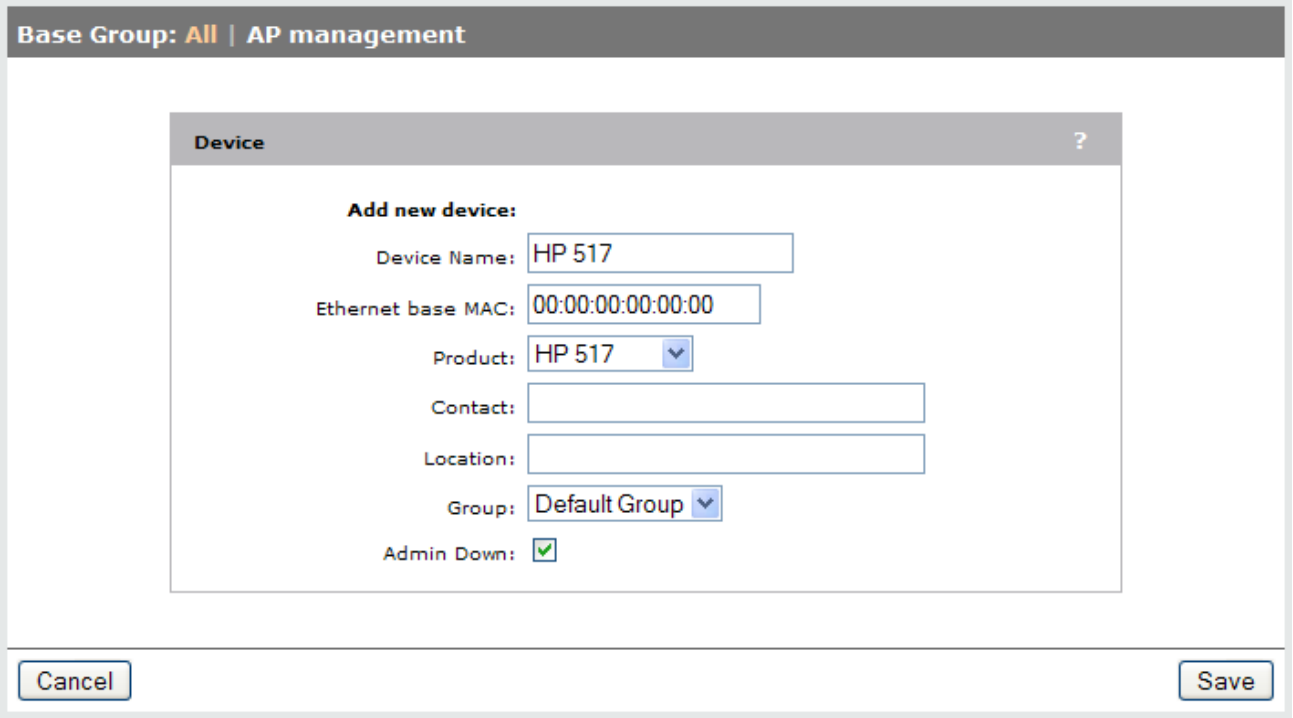
- **802.11n only:** Only wireless clients supporting 802.11n can connect. This prevents 802.11a/b/g client stations from accessing the wireless network.
- **802.11ac only:** Only wireless clients supporting 802.11ac can connect. (HP 517 only.)
- **802.11ac or 802.11n only:** Only wireless clients supporting 802.11ac or 802.11n can connect. (HP 517 only.)

Admin Down parameter added

A new parameter, called Admin Down, has been added. This parameter can be used to flag an AP that is offline for a known reason (such as maintenance or relocation) to differentiate it from other APs that are offline for unknown reasons (network failure, power failure, or other issues that prevent them from communicating with the controller).



This parameter is configurable when editing an AP that is inactive (not responding), or when adding a new AP.



GMS (Guest Management Software)

HP GMS simplifies centralized guest-account creation from any Microsoft Windows-based computer. It provides centralized, real-time management of visitor accounts and sessions with a configurable visitor session duration per account. The intuitive user interface is designed for receptionists and clerical staff with minimal training. Working with HP MSM7xx Controllers, secure login prevents unauthorized account creation, and the reporting feature records all account management activity for audits. A digital certificate secures all communications between GMS and the MSM7xx Controller. For details and download instructions, consult the *Guest Management Software Release Notes*. Search for "Guest Management Software" at www.hp.com/support/manuals.

NOTE: GMS 6.4.0.0 works with and is required for MSM software version 6.4.0.0. See also "GMS support for teaming" (page 13).

RF Manager software and MSM software version compatibility

RF Manager versions 5.9.x, 6.0.x, and 6.7.x work with MSM software version 5.5.x or later. However, to use the WLAN Integration feature in RF Manager 6.0.x or 6.7.x, the RF Manager and MSM software versions must be matched as follows:

MSM7xx software version	Compatible RF Manager versions	Sensor devices version	
		Sensor-only devices (MSM415)	AP/Sensor combo devices (MSM320[1], MSM325, MSM335[2], HP 425[3])
6.3.0.0/6.4.0.0	6.7.769 or later	Upgraded automatically by RF Manager.	Upgraded automatically by MSM7xx Controller.
6.2.0.0	6.0.185, 6.7.769 or later		
5.7.1.x/5.7.2.0/6.0.0.1/6.0.1.x	6.0.177 or later		
5.7.0.2/5.7.0.3/5.7.0.4	6.0.162 or later		
5.5.3.x	6.0.157 or later		
5.5.1.x/5.5.2.x	6.0.154 or later		
5.5.0.x	5.9.203, 6.0.147 or later		

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

[2] MSM335 APs are supported with software v6.3.x or earlier only.

[3] HP 425 requires RF Manager v6.7.769.42 or later.

NOTE: Software version 6.2.0.0, 6.3.0.0, and 6.4.0.0 are compatible with RF Manager versions listed above, but the MSM320, MSM325, and MSM335 sensors may appear orange and indicate that there is a version mismatch. This is expected and the sensors will function normally. Note also, that with RF Manager 6.7.769, these sensors will function at an RF Manager 6.0.x feature level.

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

NOTE: Upgrading an MSM7xx Controller to v6.4.0.0 also automatically upgrades any MSM320 and MSM325 Sensors it manages to MSM software v6.4.0.0.

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

GMS support for teaming

GMS 6.4.0.0 supports teaming in MSM software 6.4.0.0 with the following limitations:

- **Only the team manager controller is supported.** GMS interacts only with the team manager controller and not member controllers.
- **Subscription plans not supported.** User sessions are not synchronized across all members in a team. Therefore, subscription plans are not supported on a controller team. User accounts cannot have **Validity** set to **Subscription Plan**. **Custom Validity** is the only choice for **Validity**.
- **Automatic account removal only supported for Invalidity.** Due to a lack of synchronization between team members and the team manager, automatic account removal due to **Inactivity** is not supported on a controller team. Automatic account removal due to **Invalidity** is supported on a controller team.
- **Maximum number of concurrent sessions not supported.** Since this option is per controller, it is not supported in a team. This option is fixed at **Unlimited** for controller teams.

Configuring the service controller in GMS (when teaming is used):

- Do NOT configure a controller in GMS when the team manager controller is not available and a team member is temporarily taking its place.
- GMS interacts only with the team manager controller, you cannot add a team member as the controller.
- Any attempt to add a team member as a service controller in GMS will be rejected, with the following message displayed: *"An error occurred while uploading the CA to the Service Controller. Please check if the Services Controller is a member of a team. If teamed, please add the Service Controller using the team IP or team manager IP."*
- It is best to use the team IP address for the controller configuration.
- If you specify the team manager controller IP address, GMS detects that it is the team manager controller and automatically adds the controller using the team IP address. This confirmation message is displayed: *"The Service Controller you are trying to add is the team manager. GMS will add this Service Controller using the team IP address instead of the Service Controller IP address."* This is normal.
- On the **Service Controller** tab, the **Edit Service Controller** button cannot be used to edit the controller information for teamed controllers (parameters such as Team IP, HTTP port number, and SOAP port number). Attempts to do this cause this message to be displayed: *"Editing Service Controller details is not supported. If the details are altered, please delete and add the Service Controller using the Add device wizard."* As the message indicates, delete and then add the controller back with the wizard, specifying the changed values.

Adding/editing user accounts in GMS when the team manager is unavailable:

- Like when teamed controllers are not used and the controller becomes unavailable, if the team manager controller becomes unavailable, users can still be added and edited in GMS but the controller (team manager) is not updated until it comes back online.
- In this case when adding/editing user accounts, the following prompt is displayed: *"The selected team is in standby mode. GMS will add the account once the team manager is active. Do you want to continue?"* Select **Yes** to add/edit the account in GMS only for now, with automatic update of the team manager controller upon its availability.

SOAP function limitations for teaming environment

The functions discussed in this section may be of interest to developers who make use of SOAP to communicate and configure devices, especially when creating and managing user accounts on a controller. The following SOAP function calls that were not available in previous versions are re-enabled in MSM software version 6.2.0.0 or later.

- UpdateUserAccountMaxConcurrentSession: The user account limit is per controller instead of being applied globally to the team.
- UpdateUserAccountValidity: This function will return an error if subscription plans are selected to set the account validity.
- ExecuteUserAccountLogout: The action of logging out a user will only take effect if the user is logged in on the team manager.
- UpdateUserAccountRemovalSettings

The above limitations ONLY apply to controller teams.

Although enabled in MSM software release 6.2.0.0 or later, the following SOAP functions should not be used on a controller team. If you attempt to use any of these functions when teaming is enabled, an error is returned.

- ExecuteBackupUserAccountsPersistentData
- ExecuteUserAccountRenewPlan

- AddSubscriptionPlan
- DeleteSubscriptionPlan
- DeleteAllSubscriptionPlans
- UpdateSubscriptionPlanName
- UpdateSubscriptionPlanOnlineTimeState
- UpdateSubscriptionPlanValidityPeriodState
- UpdateSubscriptionPlanOnlineTime
- UpdateSubscriptionPlanValidityPeriodMethodState
- UpdateSubscriptionPlanValidityPeriodFor
- UpdateSubscriptionPlanValidityPeriodBetween
- UpdateSubscriptionPlanValidityPeriodFrom
- UpdateSubscriptionPlanValidityPeriodUntil
- UpdateSubscriptionPlanBooleanAttribute
- UpdateSubscriptionPlanIntAttribute
- UpdateSubscriptionPlanBandwidthLevelAttribute

Note on SOAP function UpdateUserAccountRemovalSettings

The **Removal due to invalidity** option of this function works in a teaming environment. However, the **Removal due to inactivity** option should be avoided when teaming because it could cause the controllers to wrongly remove active accounts.

Fixes

Version 6.4.0.0 includes fixes to the following issues:

- The AP is not sending LLC SNAP frames to the switch when a wireless client associates.
- (Applies to teaming with Country set to **Russia**.) The controller team does not synchronize when any of these channels are manually selected:

  149, 153, 157, 161
- (Applies to teaming.) APs fail to find the team member controller when using DNS discovery
- (Applies to teaming.) Network Address Translation (NAT) is not applied to traffic on an access-controlled VSC with an egress VLAN defined, when the wireless client connects through a team member controller.
- RF Manager 6.7 does not recognize the HP 425 Access Point as an HP branded device. Information about the HP 425 being adopted by the controller is sent to RF Manager, but the information does not get into the RF Manager authorized AP list.
- Wireless user authentication requests are not shared between Active Directory trusted domains.
- Rate limiting does not work in the downstream direction for any VSC that uses a VLAN for egress.
- After an upgrade, APs may become unsynchronized and not resynchronize when Automatic Power Control for APs is enabled.
- If you have more than five VLAN interfaces with IP addresses, the controller can experience issues at boot time.
- The "GetAuthenticatedusers" SOAP command provides erroneous results for bytes sent and bytes received.

- When a single VSC egresses user traffic over different VLANs (depending on AP location) and a client roams from one AP to another, the controller may erroneously detect the user as a Mobility Traffic Manager (MTM) visitor and block their traffic.
- (Applies to teaming.) Teaming failover causes Mobility Traffic Manager (MTM) clients traffic to stop, even after the AP is adopted by an alternate team manager controller.
- (Applies to teaming.) If using teaming while an access controlled VSC with 802.1x authentication and the **WPA termination** option is enabled, wireless clients might not be able to connect via a team member controller.
- (Applies to teaming.) APs adopted by a team member controller can appear to be in the **pending** state on the management tool, even though the APs are operating and providing service.
- When using HTML authentication, the **Continue Browsing** link on the Welcome page erroneously redirects an authenticated user back to the login page.
- The SNMP MIB for LLDP returns the LldpChassisIdSubtype MAC address in an incorrect format.
- When configuring an 802.1x VSC using SOAP, it is not possible to set the **Station ID delimiter** or the **Station ID MAC**.
- After a software upgrade, an AP might drop packets from the user VLAN over the AP tagged management VLAN.
- When configuring a VSC, if the wireless protection key source is changed to use PSK, the **Station ID delimiter** and **Station ID MAC case** configuration fields disappear from the management tool.

  When configuring a VSC using SOAP, if the wireless protection key source is set to use PSK, it is not possible to set the **Station ID delimiter** or the **Station ID MAC**.
- The SNMP process causes high CPU and high memory usage, which can cause the controller to reboot.
- (Applies to teaming.) The team manager controller can lose its default route when a static IP address is configured on the Internet port.

Known issues

These issues are present in this release:

- (Applies to teaming.) If the team manager fails, the interim team manager will enable RRM severe interference mitigation and AP load balancing, even if these options were disabled by the administrator. As a workaround, promote the interim team manager to team manager, and then disable undesired options.
- On the **Overview** > **Wireless clients** page, the scroll bar might be missing (or partially hidden) when viewed with Mozilla Firefox. The page displays properly when viewed with Microsoft Internet Explorer.
- Synchronizing AP configuration changes can be slower if any rates are unchecked in **Allowed wireless rates**. As a workaround, do not uncheck any rates in **Allowed wireless rates**, or wait for the synchronization to complete.
- (Applies to MSM720.) A timeout can occur when attempting to obtain the Sysinfo file from an MSM720 team manager when the team manager is under heavy load.
- (Applies to Teaming.) Adding two or more new controllers to a team at the same time can result in a deadlock situation with the controllers stuck in an uploading configuration state. As a workaround, remove and then rediscover the controllers.
- If system-wide Auto-channel/Auto-power is enabled, it is not possible to configure the Auto-channel and Auto-power Interval for an AP radio participating in local mesh.
- A local mesh master AP is unable to maintain a link to slave APs due to a DFS-initiated channel change. As a workaround, do not use DFS channels when using local mesh.

- (Applies to HP 517.) The Apple Bonjour features (multicast handling and user profiles) are not supported on the HP 517 wired ports.
- The SysInfo file cannot be downloaded when the controller has joined an Active Directory domain that is configured to use IPv6. As a workaround, do not configure the Active Directory server for IPv6 when used with an MSM7xx Controller.
- When using option **Public IP addresses for Guest Access**, and there are more wireless clients than available public IP addresses, the wireless clients with a public IP address already assigned might lose their address to a new wireless client. As a workaround, make sure that you provision enough public IP addresses to cover the largest anticipated number of concurrent users.
- The "**%**" character causes random characters to appear in the name on the controller when used in creating a profile name. As a workaround, do not use the "**%**" character when creating a profile name.
- (Applies to MSM410, HP 425, MSM430, MSM460, MSM466, MSM466-R.) When **Intrusion Detection System** (IDS) is enabled, AP radios on that (team of) controller(s) should not be configured in **Access Point and Local Mesh** or **Local Mesh only**. As a workaround, IDS must be disabled on the controller if **Access Point and Local Mesh** or **Local Mesh only** operation is required.
- When IMC establishes a connection to the MSM7xx Controller, the following error messages are displayed on the system log:

  ```
  err pmmclient: setVLANSubsectionIndexFromVLANNetworkProfileName: Unknown vlan name 'Internet port network'.
  ```

  ```
  err pmmclient: setVLANSubsectionIndexFromVLANNetworkProfileName: Unknown vlan name 'LAN port network'.
  ```

  ```
  err pmmclient: DB: Unable to prepare the SQL statement.
  ```

  ```
  err pmmclient: Could not get data from the database.
  ```

  These messages can be safely ignored.
- iPads/iPods/iPhones cannot authenticate using the secondary RADIUS server with the default configuration. As a workaround, reduce the retry interval in the RADIUS Profile configuration to 5 seconds.
- Re-deploying an AP from one controller to another controller might generate false attacks reported by IDS on the original controller. As a workaround, reboot the controller after removing the AP.
- Clients using the PPTP VPN server might experience connectivity issues when sending large packets.
- The SNMP OIDs that report information about the configuration of the Autochannel features "COLUBRIS-DEVICE-WIRELESS-MIB coDevWirIfStaAutoChannelEnabled" and "coDevWirIfStaAutoChannelInterval" may report incorrect information on the MSM410, MSM430, MSM460, MSM466, and MSM466-R.
- (Applies to MSM410, MSM430, MSM460, MSM466, MSM466-R in autonomous mode.) The Neighborhood Scanning feature configured to scan on all channels only scans on channels within the regulatory domain's approved channel list rather than all channels in the respective band. For example, with the location set to the United States, Neighborhood Scanning will not scan channels 12 or 13 since they are not part of the U.S. regulatory domain. This is true in both the 2.4 GHz and 5 GHz bands. There is no workaround.
- Wireless clients connected to a VSC that is directly mapped to a VLAN are unable to reach wired clients on the same VLAN.