# Avaya WLAN 8100 Release Notes

1.0.0.0
NN47251-400, 01.01

August 20, 2010

**Notice**

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

**Documentation disclaimer**

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

**Link disclaimer**

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

**Warranty**

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

**Licenses**

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

**Copyright**

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

**Third-party components**

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

**Trademarks**

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

**Downloading documents**

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

**Contact Avaya Support**

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

## Contents

# Chapter 1: Avaya WLAN 8100 Documentation Suite

This section contains a description of the Avaya WLAN 8100 documentation suite. Refer to this section for an explanation of the documents, their use, and what information they contain.

## Avaya WLAN 8100 documentation packaging

Avaya technical publications are organized according to a set of job functions. The following list outlines how the Avaya WLAN 8100 documentation suite is organized.

- Product fundamentals
  - Avaya WLAN 8100 Regulatory Information (WC 8180) (NN47251-101)
  - Avaya WLAN 8100 Fundamentals (NN47251-102)
  - Avaya WLAN 8100 Terminology (NN47251-103)
  - Avaya WLAN 8100 Regulatory Information (AP 8120) (NN47251-104)
  - Avaya WLAN 8100 Planning and Engineering (NN47251-200)
- Installation and commissioning
  - Avaya WLAN 8100 Quick Start Guide (NN47251-106)
  - Avaya WLAN 8100 Installation - AP 8120 (NN47251-302)
  - Avaya WLAN 8100 Installation - WC8180 (NN47251-303)
  - Avaya WLAN 8100 Commissioning (NN47251-304)
- Upgrades and patches

  Avaya WLAN 8100 Release Notes (NN47251-400)
- Operations
  - Avaya WLAN 8100 Configuration - WC 8180 (CLI) (NN47251-500)
  - Avaya WLAN 8100 Configuration - WC 8180 (GUI) (NN47251-501)
- Fault and performance management

  Avaya WLAN 8100 Troubleshooting (NN47251-700)

# Roadmap

This section lists and describes the documentation available for the Avaya WLAN 8100 product suite.

## Product fundamentals

Product fundamentals documentation includes overview and reference information about the product and product documentation. The following table lists the product fundamentals documents in the Avaya WLAN 8100 documentation suite.

| Title | Description |
|---|---|
| Avaya WLAN 8100 Regulatory Information (WC 8180) (NN47251-101) | This document provides regulatory information for the Avaya WLAN 8100 WLAN Controller 8180. |
| Avaya WLAN 8100 Fundamentals (NN47251-102) | This document provides an overview of the technologies and products used in the Avaya WLAN 8100 product suite. |
| Avaya WLAN 8100 Terminology (NN47251-103) | This document provides a dictionary of terms and acronyms used in the Avaya WLAN 8100 documentation suite. |
| Avaya WLAN 8100 Regulatory Information (AP 8120) (NN47251-104) | This document provides regulatory information for the Avaya WLAN 8100 Access Point 8120. |
| Avaya WLAN 8100 Planning and Engineering (NN47251-200) | This document provides information on network planning and integration. |

## Installation and commissioning

Installation and commissioning documentation describes the installation of Avaya WLAN 8100 hardware and how to perform initial configuration.

| Title | Description |
|---|---|
| Avaya WLAN 8100 Quick Start Guide (NN47251-106) | This document provides the information and procedures necessary to quickly install the WC 8180 and AP 8120. |
| Avaya WLAN 8100 Installation - AP 8120 (NN47251-302) | This document provides information and procedures for the physical installation of the AP 8120. |

| Title | Description |
| --- | --- |
| Avaya WLAN 8100 Installation - WC8180 (NN47251-303) | This document provides information and procedures for the physical installation of the WC 8180. |
| Avaya WLAN 8100 Commissioning (NN47251-304) | This document provides information and procedures on the initial configuration of the WC 8180 and AP 8120. |

## Upgrades and patches

Upgrade and patch documentation describes the software upgrade process.

| Title | Description |
| --- | --- |
| Avaya WLAN 8100 Release Notes (NN47251-400) | This document provides the latest information on the Avaya WLAN 8100 product and documentation suites as well as information on the installation of software upgrades. |

## Operations

Operations documentation describes the configuration and management of Avaya WLAN 8100 devices.

| Title | Description |
| --- | --- |
| Avaya WLAN 8100 Configuration - WC 8180 (CLI) (NN47251-500) | This document provides information and procedures for the configuration and management of the WLAN Controller 8180 using the command line interface. |
| Avaya WLAN 8100 Configuration - WC 8180 (GUI) (NN47251-501) | This document provides information and procedures for the configuration and management of the WLAN Controller 8180 using the WMS management software. |

## Fault and performance management

Fault and performance management documentation describes fault and performance management techniques.

| Title | Description |
| --- | --- |
| Avaya WLAN 8100 Troubleshooting (NN47251-700) | This document provides troubleshooting information and procedures for the WLAN Controller 8180 and Access Point 8120. |

# Chapter 2: Changing switch software

The software download process occurs automatically without user intervention. This process deletes the contents of the flash memory and replaces it with the desired software image. Do not interrupt the download process. Depending on network conditions, this process make take up to 10 minutes.

When the download process is complete, the switch automatically resets unless the no-reset parameter was used. The software image initiates a self-test and returns a message when the process is complete. An example of this message is illustrated in the following table.

**Table 1: Software download message output**

```
Download Image [/]   Saving Image [-]   Finishing Upgrading Image
```

During the download process the switch is not operational.

The progress of the download process can be tracked by observing the front panel LEDs.

To change the software version running on the switch with CLI, follow this procedure:

1. Access CLI through the Telnet protocol or a Console connection.
2. From the command prompt, use the download command with the following parameters to change the software version: **`download [address <a.b.c.d>] {primary | secondary} {image <image name> | image-if-newer <image name> | diag <image name>} [no-reset] [usb]`**

   The following table explains the parameters for the **`download`** command.

   **Table 2: download command parameters**

| Parameter | Description |
|---|---|
| address <a.b.c.d> | This parameter is the IP address of the TFTP server to be used. The address <ip> parameter is optional and if omitted the switch defaults to the TFTP server specified by the **`tftp-server`** command unless software download is to take place using a USB Mass Storage Device. |
| primary \| secondary | This parameter determines if the image is the primary or secondary image. |
| image <image name> | This parameter is the name of the software image to be downloaded from the TFTP server. |

| Parameter | Description |
|---|---|
| image-if-newer <image name> | This parameter is the name of the software image to be downloaded from the TFTP server if newer than the currently running image. |
| diag <image name> | This parameter is the name of the diagnostic image to be downloaded from the TFTP server. |
| no-reset | This parameter forces the switch to not reset after the software download is complete. |
| usb | In the WC 8180, this parameter specifies that the software download is performed using a USB Mass Storage Device and the front panel USB port. |

3. Press Enter.

# Chapter 3: Usage notes

### General usage notes

The following items should be noted when operating the different elements of the WLAN 8100 solution:

- If the AP 8120 is configured for Wireless IPS, the AP will continue to send rogue mitigation frames for up to 5 minutes if acknowledged by the administrator or until the administrator acknowledges the rogue client. This will happen even if the Rogue Client is disconnected from the network once mitigation starts.
- When a Radius Server configured at a higher priority goes offline, the WC 8180 will start using the next available Radius Server in the configuration. When the high priority Radius Server is recovered, WC 8180 still continues to use a lower priority server for Authentication/Accounting and does not fall back to the high priority server.
- In order to deploy SVP Phones in an environment with WMM enabled, users need to create a QoS Policy to Remark all packets from Call and SVP to BE_AC in order to achieve Best Possible Call Quality. The policies are not required if either WMM is not enabled or if WMM is enabled along with TSPEC.
- In Diffserv Policy Configuration, once a classifier block is associated with a policy, it cannot be dis-associated. The user has to delete the whole policy and recreate it.
- WC 8180 does not store mobility to local VLAN mapping and VLAN server configuration as part of the running config and the ASCII configuration exported. Administrators have to reconfigure these parameters if recovering the box from factory defaults.
- EDM can be very slow and may fail if SSL is enabled on the WC 8180. It is recommended to use CLI to configure the WC8180, if EDM with SSL disabled is not an acceptable configuration.
- EDM does not support Internet Explorer 6 and Internet Explorer 8 in this release. Only Internet Explorer 7 and Firefox 3.x are supported.
- Under Monitoring, the Controller Tab information will be real time. When the user clicks the Refresh button, WMS will refresh the information in real time for the domain. For Access Points and Clients Tabs, since the number of entries could be huge, data is only retrieved at every polling interval of 10 minutes. Clicking on the Refresh button will only refresh the information on the screen, if the WMS server has collected new information at its regular polling interval. However if the administrator is troubleshooting a particular AP or Client, they can open the Dashboard View for that particular AP or Client and show the current information.
- WC 8180 does not support Jumbo Frames for Rel 1.0.0.0
- The context sensitive help system for the Enterprise Device Manager does not contain entries for the tabs listed below. For information on these tabs, refer to the full product documentation.
    - Configuration, QoS, QoS NANA/UBP, Set
    - Configuration, QoS, QoS NANA/UBP, Classifier
    - Configuration, VLAN, Spanning Tree, RSTP, Globals

- Configuration, VLAN, Spanning Tree, RSTP, RSTP Ports
- Configuration, VLAN, Spanning Tree, RSTP, RSTP Status
- Configuration, VLAN, Spanning Tree, RSTP, RSTP Status, RSTP Stats
- Configuration, Edit, File System, Help File Path
- Configuration, Wireless, Security, Widps, Failed AP
- Configuration, Wireless, Security, Widps, Ad Hoc Clients
- Configuration, Wireless, Security, Widps, AP Triangulation NonSentry
- Configuration, Wireless, Security, Widps, AP Triangulation Sentry
- Configuration, Wireless, Security, Widps, AP Rogue Classification
- Configuration, Wireless, Security, Widps, AP DeAuthentication Attack
- Configuration, Wireless, Security, Widps, Detected Client
- Configuration, Wireless, Security, Widps, Client Rogue Classification
- Configuration, Wireless, Security, Widps, Blacklist Status
- Configuration, Wireless, Security, Widps, Detected Client Triangulation
- Configuration, Wireless, Security, Widps, Detected Client Sentry Triangulation
- Configuration, Wireless, Security, Widps, Detected Client Pre-Authentication
- Configuration, Wireless, Security, Widps, Detected Client Roam

# Chapter 4: Known Issues

The following known issues are present in the current software release.

| CR Number | Description |
|---|---|
| **System** | |
| wi00600410 | WC8180 does not initialize correctly upon reset or when Wireless is disabled and re-enabled on the controller. When this happens the Controller does not join the domain and Aps cannot be managed by this controller. In order to recover from this situation, the administrator would have to either disable Wireless and re-enable Wireless or reboot the controller. This issue was not observed during normal switch operation." |
| wi00575545 | Downloading the controller image from a USB will be very slow. It is recommended to download the image from a TFTP server via the LAN interfaces. |
| wi00600511 | The AP Link LED color does not always follow the specification. In some instances the LED was Green indicating 100 mbps link even though the link was operational at 1000 mbps and should have been Blue. |
| wi00600170 | 802.1p Priority for Non IP Packets is not honored by the WC8180 and treats them similar to non prioritized traffic. This issue is not observed for IP Packets and the 802.1p Priority is honored as expected. |
| wi00600595 | IPFix Functionality on the WC8180 allows monitoring of Wireless Traffic with the Source/Destination Address of the Access Point. The Traffic from the Wireless End Points is encapsulated by the Access Point, and IP Fix does not provide statistics for Individual Wireless End Points. |
| wi00600450 | When Peer Controllers are either reset to Factory Defaults or explicitly Leave the Wireless Domain, the stale controller on the AMDC has to be cleared via CLI cmd "wireless domain purge-stale-controllers" before the peer controller tries to join the domain again. If this step is not followed, CLI displays an Internal Error. |
| wi00600354 | CLI command "show wireless ap upgrade-failed" shows the failed AP only until that AP becomes managed. The table is cleared once the AP becomes managed even though image upgrade has failed for that AP. |
| wi00671088 | In some instances when Peer Controllers come up after a reboot, they display config out-of-sync, however they have the correct configuration and are operating as expected. This is expected to be due to the ordering of certain configuration. Manually executing a config-sync from the AMDC will resolve the out-of-sync state. |
| wi00664681 | When a new Radio Profile is created in bgn mode and channel bandwidth set to 40MHz, applying the configuration incorrectly applies |

| CR Number | Description |
|---|---|
| | the channel bandwidth as 20MHz to the controller. Applying the configuration a second time pushes the 40MHz configuration to the controller. |
| **AP** | |
| wi00575533 | Due the limited number of non overlapping channels available on the 2.4GHz Band using channel bonding (40MHz mode) could result in connectivity issues for some of the older adaptors. It is recommended to use 40MHz Mode on the 5GHz Radio and use 20MHz Mode on the 2.4GHz Radio on the AP. |
| wi00576644 | While AP image update process is in-progress, executing "wireless ap image-update <mac>" will result in error. Please wait for the AP image update to complete before initiating image update for other APs. |
| wi00600161 | The commands ""wireless domain ap image-update download-group-size"" and ""wireless domain ap image-update reset-group-size"" are not functional. Please configure the group size of APs that need to be upgraded per iteration while doing a bulk image update using command ""wireless domain ap reset-group-size"". The system will go through multiple iterations until all the APs are upgraded or reset by upgrading/ resetting the larger of 5 APs or that configured under ap reset-group-size. |
| wi00686012 | Even when an AP Profile other than 1 is configured to be the default AP Profile, New APs discovered and auto-promoted are still assigned to AP Profile 1. Administrator has to manually reassign the APs to the required AP Profile. |
| **Captive Portal** | |
| wi00576206 | Captive Portal Client Associated with the AP continues to receive multicast traffic even after the Captive Portal session is closed. |
| wi00600496 | In some instances, when Captive Portal SSID is configured to be the first VAP on the 2.4GHz Radio (Radio 2) of the AP, then Clients Fail to Associate to the AP. Workaround is not to use the first VAP for Captive Portal on Radio 2 (bgn). Radio 1 (an) does not show this issue. |
| wi00600184 | Captive Portal session information for a client connected to a peer controller is not displayed correctly on the controller that becomes AMDC after the original AMDC is shutdown. The Captive Portal Client remains connected to the network as expected and the session information can be obtained from the peer controller to which the client is connected to. |
| wi00600710 | While using https as the protocol for Captive Portal, Firefox complains about the certificate serial number and the issuer. Please delete any previous certificate from the client browser store and re-launch the browser for Captive Portal to work. |
| wi00600616 | Intermittently, "show wireless controller config-sync-status" shows that Captive Portal is out of sync. This is due to the mismatch in the ordering |

| CR Number | Description |
|---|---|
| | of the captive portal binary structures internally and should not impact system behavior. |
| wi00600735 | Captive Portal logout fails after user roams between Aps that are managed by two controllers that do not acting as VLAN server for the mobility vlan. |
| wi00600220 | CLI command "show wireless captive-portal client status detail" does not display certain parameters on the AMDC when client connects to a peer controller on which the output is correct. Now if the CP client roams to a different controller, these values are not displayed on the AMDC as well as the controller where the client is connected. This does not impact the CP Client network connectivity. |
| wi00600313 | Captive Portal Locale settings are not synchronized by the AMDC to the peer controllers. This will result in different portal page when users are connected to APs managed by different controllers. Workaround is to have the peer controllers Leave the wireless domain, apply the Captive Portal Locale settings on the standalone controllers, then join the domain. |
| wi00686032 | When multiple Captive Portal Profiles are created, only the default Captive Portal profile customizations are operational. Even when a user connects to the non default Captive Portal profile, the login page displays customizations from the default Captive Portal profile. |
| wi00601711 | Captive Portal users via Internet Explorer sometimes observe "Page Not Found" error after Logout. The user is logged out correctly. |
| **Security** | |
| wi00600498 | WMS only accepts xx:xx:xx:xx:xx:xx for MAC format and does not accept xx-xx-xx-xx-xx-xx while configuring the MAC Database on the Controller. |
| wi00600133 | When the Radius Profile has a high priority server offline, the WC continues to poll for the offline server intermittently. This could result in client authentication retries if the request came in when the system was polling for the offline server. Workaround is to remove the offline server from the Radius Profile and bring it back online during a maintenance window. |
| wi00576447 | Wildcard entries are not supported for MAC Entries in the MAC Database on the WC 8180. |
| wi00600638 | WMS fails to add a user in the Local User Database if a new user is created without specifying the password. WMS does not indicate any error and reports that the policy is applied successfully. |
| wi00675045 | CLI and EDM allow more than one Radius Accounting Profiles even though only one accounting profile is supported in release 1.0.0.0. |
| wi00601378 | Cannot default the wids rogue-ap trap-interval, wired-detection-interval, ageout adhoc-client. |

| CR Number | Description |
|---|---|
| **Diffserv** | |
| wi00600484 | AMDC fails config sync to Peer Controllers in certain scenarios where Diffserv policies and the policies have empty classifier blocks or empty policies. |
| wi00600212 | In some instances where diffserv policies are not applied to all the network profiles on a radio, then the CLI command ""show wireless diffserv statistics"" does not display client qos statistics. In this scenario, use ""show wireless client qos status"" displays the MAC addresses of all clients to which policies are applied. Using the MAC address of a specific client and executing ""show wireless diffserv statistics <mac>"" will provide the correct statistics for a particular client. " |
| wi00686010 | WMS Diffserv Classifers Table can be sorted either in Ascending or Descending order. Is users do this, then the ordering of the classifers is modified and it cannot be modified to the required order unless all classifiers are deleted and recreated. However this is a display issue only and the configuration is not applied to the controller. It is recommended not to sort the classifier Table in WMS. |
| **Traps/Syslog** | |
| wi00575076 | WC8180 does not generate Trap "ntWlanUnmanagedAPDiscovered" when a new AP is discovered on the network. Syslog reports the corresponding log message. |
| wi00576426 | Trap message is not generated when a Wireless Client fails MAC Authentication. |
| wi00576586 | Only two MDC capable devices should be present in the network. When a 3rd device is configured to be MDC capable the Trap and Log messages to indicate Max Domain MDC Limit Reached event are not generated. |
| wi00600251 | WC8180 fails to generate log messages as expected for Link Down event on the 10Gig Interfaces. |
| wi00600570 | WC8180 fails to generate the traps avwlanClientRoamDetected, avwlanClientAuthenticationFailure, avWlanPeerControllerConfigurationCommandReceived in certain conditions. Monitoring syslogs displays the correct log messages for these events. |
| **CLI** | |
| wi00576289 | The CLI command "show wireless managed-switch" displays incorrect information for the number of clients and number of managed aps on the peer switch. Please user CLI commands "show wireless controller status" and "show wireless domain peer-controller status" |
| wi00575490 | The command output for "show wireless ap vap status" is different on AMDC and BMDC. On the BMDC and Peer Controllers the output only displays the VAPs that are configured. On AMDC the total number of |

| CR Number | Description |
|---|---|
| | VAPs that are allowed on the system are displayed however only the VAPs that are configured have a SSID. This is a display issue and does not impact the system behavior. |
| wi00600554 | On WC8180, "show wireless client status" displays client IP address as 0.0.0.0 in some instances. The controller learns the client IP Address via IP Packets received from the associated client. In instances where the client does not send any IP packets after association or after the client roams to a new AP, the controller will not learn the Client IP address and 0.0.0.0 is displayed in this table. |
| wi00600799 | Intermittently APs managed by the Peer Controllers are not displayed by the AMDC after all the controllers in the domain are reset. WMS and the peer controllers will display the complete list of managed APs in this situation. |
| wi00600228 | Intermittently show wireless controller statistics' and 'show wireless controller tspec-statistics' do not increment properly. |
| wi00600411 | Clearing domain / controller statistics does not clear the Wireless Diffserv statistics. Stats get cleared when a client either disconnects or roams. |
| wi00600206 | In some instances the CLI output for "show wireless domain peer-controller status" on AMDC displays wrong number of APs managed by the peer controllers. CLI command "show wireless ap status" gives the correct number of APs managed in the domain on the AMDC and the command shows the number of APs managed by the switch on the peer controllers. |
| wi00600272 | In some instances it is observed that CLI output for "show wireless security wids-wips rouge-ap-classification <mac>" gets stuck for about a minute before the display is complete and the command prompt is returned. |
| wi00600489 | CLI command "show wireless controller status" incorrectly displays the stored AP image versions as 0.0.0.0. This is a display issue and does not impact the image that is pushed to the APs on AP image upgrade. |
| wi00600314 | CLI command ""show wireless radio-profile channels <profile>"" incorrectly displays multiple entries while the Radio Profile is configured for wids-wips. |
| **EDM** | |
| wi00600593 | EDM fails to create the network profile correctly when the WEP key entered shorter than the required length. Upon correcting the key length, EDM incorrectly creates a network profile with an empty WEP Key value. Use CLI to correct the configuration in this scenario. |
| wi00600540 | TACACS+ Configuration is not available via EDM. Please use CLI for TACACS+ Configuration on the Wireless Controller. |

| CR Number | Description |
|---|---|
| wi00600696 | EDM does not display all the supported channels when the Country Code is different than US. CLI & WMS will display the correct list of supported channels. |
| wi00600121 | Using EDM, users will not be able to clone existing Radio profiles. This is possible via CLI & WMS. |
| wi00600582 | While monitoring Graphs for the 10Gig Interfaces, the counter values in some instances were observed to be very large numbers and in some instances negative numbers. In both the cases the value displayed by EDM is invalid. |
| wi00600583 | While monitoring the Port/Device Graphs on EDM, clearing port statistics via CLI does not clear the statistics in EDM. |
| wi00600416 | EDM cannot be used to reset or update APs managed by the Peer Wireless Controllers. It is recommended to use either CLI or WMS to perform domain wide operations. |
| wi00600204 | EDM displays Error message while configuring Radius Profile with type = accounting while adding a server with priority 1. The server is added successfully but EDM does not indicate that. |
| wi00600241 | EDM does not allow AP Campus Field Configuration. Use CLI/WMS to configure this value if required. |
| wi00600139 | EDM supports only 2 concurrent sessions in this release. Using more than 2 concurrent EDM sessions could degrade EDM & System performance. |
| wi00600384 | EDM displays invalid error message "CommitFailed" when user tries to configure diffserv policies more than the supported limit. EDM should display correct error message similar to CLI |
| wi00653845 | ASCII configuration download fails when initiated via EDM. |
| wi00601467 | EDM/QoS Devices/Priority Q Assign - Range displayed incorrectly as 1-255. Correct Range is 1-8. |
| wi00601390 | EDM/Wireless/NetworkProfile/Edit Profile/Security Tab/Security Mode=wepStatic - The help information for key length is incorrectly displayed as 13 for ASCII and 26 for HEX. Correct key length is 5 for ASCII and 10 for HEX. |
| wi00601389 | EDM/Wireless/Security/Widps/FailedAP tab does not provide all the configuration options available from CLI. |
| wi00601386 | EDM/Wireless/Security/Widps/KnownRogueAP tab does not provide all the configuration options available from CLI. |
| wi00601384 | EDM/Wireless/Security/Widps/RogueAP & Client Controls tab does not display the correct configurable values for WiredNetworkDetectionInterval and DetectedTrapInterval. CLI displays the correct values. |

| CR Number | Description |
|---|---|
| wi00601370 | EDM/Wireless/Security/WIDPS/RF Scan AP Tab shows Avaya AP OIDs as Unknown. |
| **WMS** | |
| wi00576352 | WMS does not allow to swap Mobility Vlan - Local Vlan mapping between two vlans. In order to swap the vlans mapped, both the mobility vlans have to be mapped to none, apply the settings, then change to new values. |
| wi00576035 | WMS takes about 3 minutes to update the MDC Capable Flags if the value is modified via CLI. |
| wi00575540 | When SNMP v3 User is configured for Authentication Protocol=MD5 and Privacy Protocol = None; WMS gets stuck at Apply or Import Policies using this User Credentials. Using DES as the Privacy Protocol resolves this issue. |
| wi00600324 | WMS can get stuck during Importing Policies in SNMPv3 mode with 3DES encryption. On WC8180, it is recommended to use the AES encryption mode. |
| wi00600504 | WMS does not to consistency check when importing CSV File for Blacklist/Whitelist Entries and incorrectly shows that Update is successful. However no entries are created in the database. |
| wi00600702 | WMS will only refresh the Access Point and Client Views in real time every polling interval (10 min). For current state of an AP or a wireless client, right click on the AP/Client to open the dashboard. At this point WMS refreshes the data before displaying the dashboards. |
| wi00600720 | In scenarios where the JPEG file of the Floor Plan used in SMD has a lot of white space around the actual floor plan, importing that into WMS for RF Monitoring will result RF Views incorrectly mapped onto the Floor Plan. It is recommended to crop an additional white spaces around the Floor Plans within the JPEG before using it for RF Planning and Monitoring. |
| wi00600742 | In some situations the AP Radio Power Levels displayed in the WMS RF Views is different from that displayed via "show wireless ap radio status" command in the CLI. |
| wi00600442 | WMS does not display Client location view in the Client Dashboards when multiple APs report the client but the AP that reports the strongest signal is not present in the SMX Floor Plan. To avoid this issue, ensure that all the APs are added correctly to the Floor Plan. |
| wi00686040 | WMS Site Model Tab under Monitoring/Site Views gets stuck in loading when adding Site Model Files using Internet Explorer 8. The smx File gets added correctly, however this can only be viewed by closing and re-opening the browser. This issue is not observed while using Firefox. |
| wi00685809 | Proposed Channels are not displayed correctly in WMS and different from values in CLI after running the Auto-RF Algorithm. |

| CR Number | Description |
|---|---|
| wi00685805 | Auto-RF action is executed on the wrong radio when applied from WMS. The 2.4 and 5 GHz Radios are interchanged. Admin needs to select 5GHz to execute actions on the 2.4GHz Radio and vice versa. |
| wi00685804 | WMS does not allow admin to change the History Depth for Auto-RF in manual mode. The History Depth can be changed via CLI if required while in manual mode. |
| wi00675071 | Changes to the AP static channel and power settings via WMS are not applied to the controller. Duplicate of wi00601113 |
| wi00674990 | Changes to the RF Scan band and RF Scan Duration for a WIDS-WIPS Radio Profile via WMS are not applied to the controller. |
| wi00674985 | WMS does not display the RF Scan Duration for WIDS-WIPS Radio Profiles. Information is available via CLI or on the Radio Profile Edit Screen in WMS. |
| wi00673223 | WMS incorrectly prompts Auto-RF History Depth range as 0-24 instead of 0-10. However any values above 10 will not be accepted by WMS. Duplicate of wi00664708. |
| wi00672326 | In some instances, changing the Auto-RF mode and applying the configuration via WMS resulted in certain APs changing their channel. |
| wi00664805 | Changes to Rate Limiting configuration for the Radio Profile under the Data Rates Tab via WMS are not applied to the controller. |
| wi00664791 | WMS with Internet Explorer 8 does not display policy names correctly in some instances as policy names appear to be overlapped. |
| wi00664708 | WMS incorrectly prompts Auto-RF History Depth range as 0-24 instead of 0-10. However any values above 10 will not be accepted by WMS. |
| wi00601372 | WMS allows unsupported channels to be configured and applying the configuration returns a Success. However these channels are not applied to the controller. |
| wi00601329 | Not able to monitor RF-Views in WMS when logging into WMS using the credentials for a Role - User. |
| wi00601321 | In some instances WMS does not display the AP statistics correctly under the Monitoring Tabs. |
| wi00601113 | Changes to the AP static channel and power settings via WMS are not applied to the controller. |
| wi00601101 | When a new Language code is configured under WMS, Captive Portal; applying the configuration creates a new Captive Portal Profile on the controller. This is not observed when configured via CLI. |

## Importing action commands

The import and export of action commands in ASCII configuration files is not supported in this release. This includes commands such as radius secret and mdc-join. Action commands that are part of a device configuration before an export operation will be excluded during the export operation. Subsequent imports

of the configuration file will not contain the excluded commands. Excluded commands must be manually executed after the import process.

This is very important to keep in mind especially in regards to configuring a new device or updating a device that has been returned to factory defaults. Note the action commands that were part of the pre-export configuration so they can be manually executed after the configuration file is imported.