Avaya WLAN 8100 Release Notes

Release 2.1.0
NN47251-400
Issue 08.06
October 2013

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

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees 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 websites referenced within this site or documentation 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 its hardware and Software (“Product(s)”). 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 website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

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 CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA CHANNEL PARTNER. 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 AVAYA CHANNEL PARTNER; 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”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/licenseinfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product 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 unless expressly authorized by Avaya. 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

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud Intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Website: http://support.avaya.com/. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation 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 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 non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document provides the latest information on the Avaya WLAN 8100 product and documentation suites for release 2.1.0, as well as information on software upgrades.

It also provides information on the following:

- Known and resolved issues for release 2.1.0 software.
- Mobility domain capacity and device capacity for Overlay and Unified Access deployments.

Related Resources

Documentation

For a list of the documentation for this product, see *Avaya WLAN 8100 Documentation Roadmap* (NN47251-100).

Training

Ongoing product training is available. For more information or to register, see http://avaya-learning.com/.

Enter the course code in the *Search* field and click *Go* to search for the course.

Course Code	Course Title
6769X	Avaya Wireless LAN 8100 Implementation and Management
4D00045V	Avaya VENA Unified Access Implementation
Wireless LAN 8100 AIPS credential	

Course Code	Course Title
7D00060A	Wireless LAN 8100 Implementation Assessment (online test)

Avaya Mentor videos

Avaya Mentor videos are available to provide technical content on how to install, configure, and troubleshoot Avaya products.

Videos are available on the Avaya support site, listed under the video document type, and on the Avaya-run channel on YouTube.

To find videos on the Avaya support site, select the product name, and check the *videos* checkbox to see a list of available videos.

Note:

Videos are not available for all products.

To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

- Enter a key word or key words in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: New in this release

The following sections detail what’s new in Avaya Wireless LAN (WLAN) 8100 for Release 2.1.0.

The **Features** section describes new features, and the **Other changes** section describes non-feature changes in Release 2.1.0.

- Features on page 9
- Other Changes on page 10

Features

The following features are new in the WLAN 8100 solution, for release 2.1.0.

- Auto-RF
- AeroScout RTLS support
- Ekahau RTLS support
- Station Isolation
- EAP-SIM and EAP-AKA support
- Tunnel Path MTU
- MAC-based RADIUS authentication
- Wi-Fi Zoning
- LED management on a domain AP database

Additionally, the following are supported in this release:

- Domain AP configuration such as:
    - enabling or disabling individual AP radios
    - saving AP radio or power configuration to the AP database
    - configuring specific domain AP parameters on the AP such as its model, location parameters and controller information.
- Quick configuration utility for the WC 8180, that can be run from the Avaya CLI.

  This utility displays a series of prompts that help you set up the required configuration on the controller.

The following enhancements have been introduced in the Captive Portal feature.

- Open-guest authentication of Captive Portal guest users.
- A 128-character limit on the user name specified in the Captive Portal login page, for RADIUS-based Captive Portal user authentication.
- Certificate Manager support
- DiffServ Policy support
- Increase in the number of Captive Portal IP addresses supported.
- Captive Portal Walled Garden

The WLAN Management System (WMS) has had several enhancements with respect to performance, reliability of the data displayed and consistency, to create a better user experience. Vast improvements have been made in the following areas in the WMS:

- Monitoring capabilities, enhanced user experience with the provision to perform domain-wide actions, and a consistent look-and feel.
- Troubleshooting or diagnostics
- Reporting capabilities

The current release supports additional country codes. For the entire list of country codes supported in this release, see *Avaya WLAN 8100 Fundamentals* (NN47251–102).

This document does not contain feature updates. For more information on the features and enhancements for release 2.1.0, see the *Avaya WLAN 8100 Fundamentals* (NN47251–102).

For more information on the WMS enhancements, see the *Avaya WLAN 8100 GUI Reference* (NN47251–108).

Other Changes

This document contains a high level overview of the WLAN 8100 software upgrade to release 2.1.0, including software image file details. Procedures to actually perform the upgrade have been removed from this document.

For more information on software upgrade to release 2.1.0, see the *Avaya WLAN 8100 Upgrade* (NN47251-402).

Chapter 3: Wireless LAN (WLAN) 8100 Upgrade

The following sections provides a high level overview of the WLAN 8100 Upgrade to release 2.1.0. It outlines the supported upgrade paths for upgrade to release 2.1.0.

For information on software upgrade for prior releases, see the *Avaya WLAN 8100 Upgrade* (NN47251–402) for that release.

Supported upgrade paths

Table 1: Supported upgrade paths — wireless controllers and APs

Upgrade path	Support
Upgrade 1.0.x to 2.1.0	Not supported
Upgrade 1.1.x to 2.1.0	Not supported
Upgrade 1.2.x to 2.1.0	Supported
Upgrade 2.0.x to 2.1.0	Supported
Migration from 2.1.0 Overlay to 2.1.0 Unified Access	Supported

The following table lists the supported upgrade paths for the WLAN Management System (WMS).

Table 2: Supported upgrade paths — WMS

Upgrade path	Support
1.0.x to 2.1.0	Requires an un-install followed by a WMS install
1.1.x to 2.1.0	Requires an un-install followed by a WMS install
1.2.x to 2.1.0	Requires an un-install followed by a WMS install
2.0.x to 2.1.0	Upgrade supported

Note:

After you upgrade or perform fresh install of WMS, it is recommended that you import the mobility domains from the active mobility domain controller (A-MDC) of the respective domains.

When you uninstall a previous version of the WMS and then install the current version (for example, during an upgrade from releases 1.0.x, 1.1.x or 2.0.x to release 2.1.0), ensure that you back up the license and SMX files during the un-install, and restore these files during the install.

For more information on WMS installation or upgrade, and procedures to import mobility domains using the WMS, see the *Avaya WLAN 8100 GUI Reference* (NN47251–108).

WLAN 8100 upgrade workflow for release 2.1.0

Important:

General Upgrade considerations:

- If you are upgrading from release 1.0.x or release 1.1.x, you must first upgrade all the components of the WLAN 8100 (WMS, wireless controller and access points) to release 1.2.x or release 2.0.x before you upgrade to release 2.1.0 software.
- After you upgrade to release 2.1.0, the release 2.1.0 wireless controller cannot manage access points operating on release 1.0.x or release 1.1.0 software versions. Therefore, you must first upgrade all access points to either release 1.1.1 or release 1.2.x software version before upgrading to release 2.1.0.
- To migrate to a Unified Access deployment, you must first upgrade your existing Overlay solution to either release 2.0.x or to release 2.1.0.

  For example, if you currently have release 1.2.x of the WLAN 8100 Overlay solution, and you want to migrate the solution to the 2.1.0Unified Access, you must first upgrade to either release 2.0.x Overlay or release 2.1.0 Overlay.

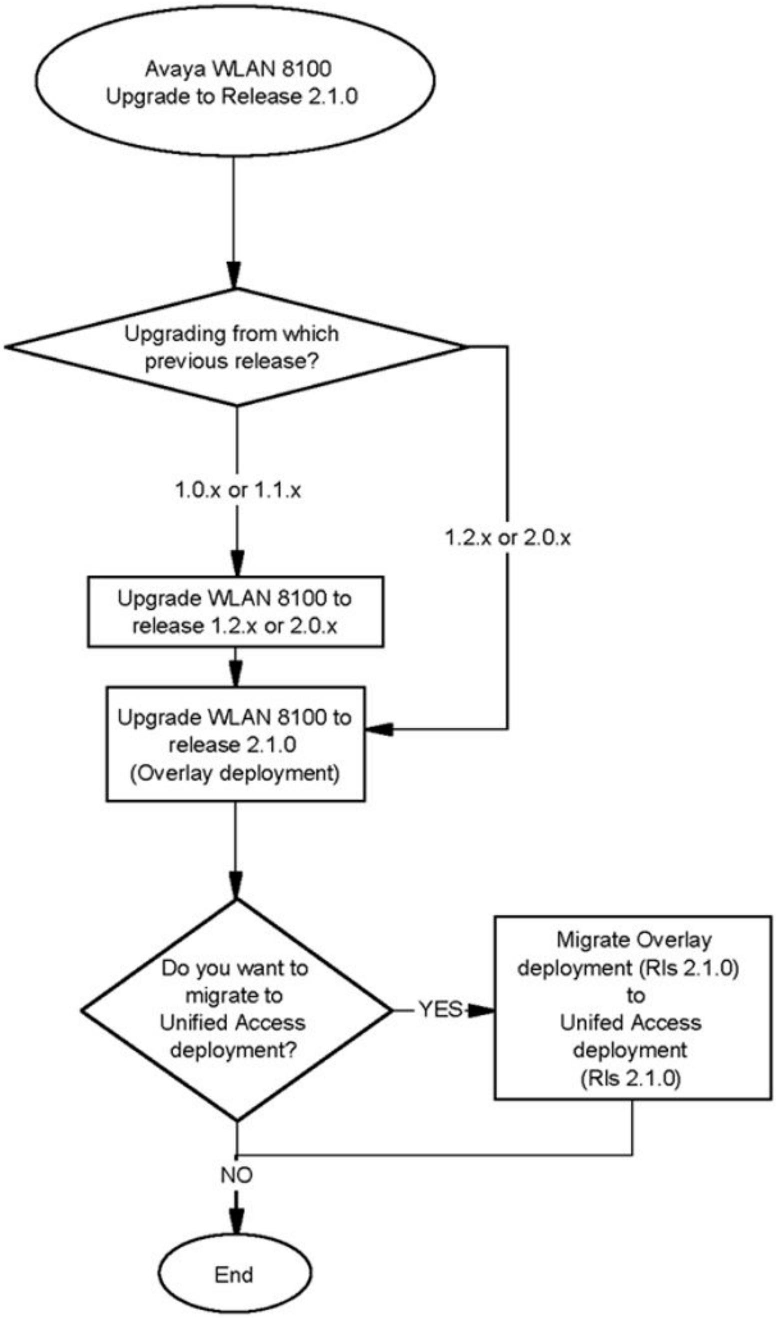

Figure 1: Upgrade WLAN 8100 to release 2.1.0 — workflow

Software image file details

The following sections provided the software image file details for releases 1.2.0, 2.0.0, 2.0.1 and 2.1.0.

Table 3: Software image files released with release 2.1.0

Component	File Name	File Size (bytes)
WC 8180 Controller Image	wc8180_2.1.0.102s.img	46,347,060
AP8120/AP8120–E	AP8120-Upgrade_2_1_0_102.tar	8,933,868
AP8120–O Image **Note:** The AP 8120-O only supports the external image download.	AP8120-OAP-Upgrade_2_1_0_102.tar	6,962,545
WMS Windows 32 bit	WLAN8100_WMS_2.1.0.102_Windows_32 bit.exe	386,924,544
WMS Windows 64 bit	WLAN8100_WMS_2.1.0.102_Windows_64 bit.exe	386,924,544
WMS Linux	WLAN8100_WMS_2.1.0.102_Linux.bin	401,604,608

Table 4: Software image files released with release 2.0.1

Component	File Name	File Size (bytes)
WC 8180 Controller Image	wc8180_2.0.1.013s.img	50,104,320
AP8120/AP8120–E	AP8120-Upgrade_2_0_1_013.tar	8,867,840
AP8120–O Image **Note:** The AP 8120-O only supports the external image download.	AP8120-OAP-Upgrade_2_0_1_013.tar	6,922,240
WMS Windows 32 Bit	WLAN8100_WMS_2.0.1.013_Windows_32 bit.exe	169,133,056
WMS Windows 64 Bit	WLAN8100_WMS_2.0.1.013_Windows_64 bit.exe	169,134,080

Component	File Name	File Size (bytes)
WMS Linux	WLAN8100_WMS_2.0.1.013_Linux.bin	200,470,528

Software image files released with release 2.0.0

Component	File Name	File Size (bytes)
WC 8180 Controller Image	wc8180_2.0.0.084s.img	50,043,712
AP8120/AP8120–E	AP8120-Upgrade_2_0_0_084.tar	8,816,640
AP8120–O Image **Note:** The AP 8120-O only supports the external image download.	AP8120-OAP-Upgrade_2_0_0_084.tar	6,922,240
WMS Windows 32 Bit	WLAN8100_WMS_2.0.0.084_Windows_32bit.exe	169,131,202
WMS Windows 64 Bit	WLAN8100_WMS_2.0.0.084_Windows_64bit.exe	169,133,709
WMS Linux	WLAN8100_WMS_2.0.0.084_Linux.bin	200,468,142

Software image files released with release 1.2.0

Component	File Name	File Size (bytes)
WC8180 Controller Image	wc8180_1.2.0.075s.img	49,567,804
AP8120/AP8120–E	AP8120-Upgrade_1_2_0_075.tar	8,755,200
AP8120–O Image **Note:** The AP 8120-O only supports the external image download.	AP8120-OAP-Upgrade_1_2_0_075.tar	6,871,040
WMS Windows 32 Bit	WLAN8100_WMS_1.2.0.075_Windows_32bit.exe	187,922,006
WMS Windows 64 Bit	WLAN8100_WMS_1.2.0.075_Windows_64bit.exe	187,905,973
WMS Linux	WLAN8100_WMS_1.2.0.075_Linux.bin	213,482,474

Chapter 4: Captive Portal browser compatibility

The Captive Portal functionality is dependent on client devices and browsers. Although the WLAN 8100 Captive Portal functionality works with most client devices and browsers, the following section describes the client platforms and browsers that are tested by Avaya for releases 1.2.x, 2.0.x and 2.1.x. If you have any issues with platforms or browsers not listed in this section, you must open a support ticket.

Note:

The WLAN 8100 Captive Portal functionality is dependent on a wireless client generating DNS requests and soliciting response, or generating HTTP/HTTPS requests. If the client browser does not resolve the domain name and the client does not generate a HTTP/HTTPS request, then that wireless client is not served the Captive Portal login page.

Note:

In releases 1.2.x, 2.0.x, and 2.1.x, when using the Firefox browser and HTTPS as the protocol, Captive Portal may be inoperable initially. To fix this issue, delete existing cookies and any previous certificate from the client browser store and then re-launch the browser for the Captive Portal to work.

The certified mobile device platforms and their default browsers are as follows:

Mobile device platform	Default supported browser
MAC OS X versions: • 10.7.2.5.1 • 10.7.4.6.0 • 10.6.8.5.1.2	Safari
IPAD2 versions: • 4.3.5 • 5.1 • 5.1.1 • 5.0.1 • 6.1	Safari
iPad mini version 6.1	Safari
iPhone version 5.0.1	Safari

Mobile device platform	Default supported browser
Android versions: • 3.2 • 4.0.2 • 4.0.3 • 2.3.4 • 4.1.1	Chrome

The following table identifies the compatibility of Windows operating systems and captive portal browsers that are supported in Release 1.2.x, 2.0.x, and 2.1.x.

Windows operating systems and captive portal browsers support matrix

Applications	Windows operating system						
	2000	XP	XP-64 bit	Vista	Vista 64	Windows 7	7–64 bit
IE 6	Supp	Supp	Supp	X	X	X	X
IE 7	X	Cert	Supp	Cert	Supp	X	X
IE 8	X	Cert	Supp	Supp	Supp	Supp	Supp
IE 9	X	X	X	Cert	Cert	Cert	Cert
IE10	X	X	X	X	X	Cert	X
Firefox 3.X	Supp	Supp	Supp	Supp	Cert	Cert	Cert
Firefox 4.X	Supp	Supp	Supp	Supp	Supp	Supp	Supp
Firefox 5.X	Supp	Supp	Supp	Supp	Supp	Supp	Supp
Firefox 6.X	Supp	Supp	Supp	Supp	Supp	Supp	Supp
Firefox 8.X	Supp	Cert	Supp	Cert	Supp	Cert	Cert
Firefox 3.6.12	X	X	X	Cert	X	X	X
Firefox 14.0.1	X	Cert	X	X	X	X	X
Firefox 10.0.2	X	X	X	X	X	Cert	X
Firefox 19	X	X	X	X	X	Cert	X
Firefox 20.0	X	X	X	X	X	Cert	X
Safari 3.0	Supp	Supp	Supp	Supp	Supp	Supp	Supp
Safari 4.0	Supp	Supp	Supp	Supp	Supp	Supp	Supp
Safari 5.0	X	X	X	X	X	Cert	X
Safari 5.1.5	Supp	Supp	Supp	Supp	Supp	Supp	Supp

Applications	Windows operating system						
	2000	XP	XP-64 bit	Vista	Vista 64	Windows 7	7–64 bit
Chrome 20.0.1132.57 m	X	Supp	Supp	X	X	X	X
Chrome 25	X	X	X	X	X	Cert	X
Opera 11.2	X	X	X	X	X	Supp	Supp

Legend:

- Supp — supported in this release.
- Cert — supported and tested in this release.
- X— not applicable.

Chapter 5: Resolved Issues

The following table identifies issues that are resolved in software release 2.1.0.

WI ID	Summary
CLI	
wi00987931	When a valid radio profile is not mapped within AP profile, AP get stuck at `Apply In Progress` status.
wi01022494	When you enable Auto Promote in overlay, all the APs in AMDC Domain Discovery Table are redirected to BMDC.
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 CLI on Peer controllers will display the complete list of managed APs in this situation.
wi01096556	Security breach in Open + RADIUS MAC authentication: A client gets connected even if the RADIUS server is down.
wi01095479	Captive Portal: Changing the `maximum session timeout` value in a Captive Portal profile.
wi01116712	Captive Portal users are able to authenticate even after the configured `auth end date`.
wi01110939	MAC RADIUS authentication: A client is *disassociated* instead of *de-authenticated* when a controller is waiting on a response from the RADIUS server.
wi01049892	Captive Portal: User name field limit needs to be set to 32 characters.
wi01097922	Captive Portal: The client connection status is displayed incorrectly.
wi00575490	The command `show wireless ap vap status` displays different outputs on the AMDC and BMDC. On the BMDC and Peer Controllers the output only displays the VAPs that are configured. On AMDC the total number of VAPs that are allowed on the system are displayed however only the VAPs that are configured have a SSID.
wi00576289	Wrong information regarding NC and MAP displayed when you execute `show wireless managed-switch`.
wi00664681	Wrong Channel Bandwidth is set when a new b/g/n Radio Profile is created (with default settings). In WMS, when a new Radio Profile is created in bgn mode and channel bandwidth set to 40MHz, applying the configuration incorrectly applies the channel bandwidth as 20MHz to the controller.
wi00671088	Rebooting the B-MDC causes radio profile configuration to go out of sync.

WI ID	Summary
	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 due to the ordering of certain configuration.
wi00882939	While WMS is running, Controller Host CPU spikes can be observed every 10 minutes (or WMS polling Interval). The CPU utilization will return to normal value once WMS poll is complete. CLI responses could be delayed during these spikes.
wi00885085	Implementation of captive-portal mapping does not exist.
wi00900592	Monitoring Clients does not work if the HTTP port on WC is non-default.
wi00904073	In some instances it was observed that the controller remains in Programming and Saving State during Image Download for at least 1hr 15 min during 1.1.0.123 upgrade.
wi00909674	An incorrect AP count is displayed in the domain AP table and the Known AP table on executing `show wireless domain ap database` and `show wireless security wids-wips known-ap`.
wi00981120	When clients are connected to the same radio (Radio1 or Radio2) of an AP, clients will **not** ping or communicate with each other if station isolation is enabled. If the clients are connected to two Radios (Radio1 and Radio 2) on the same AP, even with station isolation enabled, the system **fails** to stop the clients from communicating with each other. Similarly, when clients are connected to different APs in a domain, even with station isolation enabled, the system **fails** to stop the clients from communicating with each other.
wi00983304	CLI command **`show wireless diffserv statistics`** does not display summary statistics information for all clients. Use **`show wireless diffserv statistics <MAC>`** to retrieve information correctly for a wireless client.
wi00984608	Adding a MAC to Blacklist requires enabling MAC Authentication on the Network Profile, which requires users to populate the Whitelist even when it is not intended to be used.
wi01000513	In Overlay deployment, LVL7-Wireless-Client-Policy-Dn/Up attributes are not applied on captive portal clients.
wi01000743	Wireless controller does not send Radius Attributes calling or called station ID in RADIUS request when captive portal is used for authentication.
wi01003635	When a wireless client is connected to a SSID that does not have Captive Portal enabled, the wireless client reconnects (without an explicit disconnect) to a SSID with a Captive Portal enabled, the client will not be able to login for up to 2 minutes. This issue is not observed if the client disconnects to the first SSID before connecting to a CP SSID.
wi01003928	The ACLI command `show wireless captive-portal client statistics` may show inconsistant data across controllers in different situations.

WI ID	Summary
wi01017586	osapiMessageSend function fails when captive-portal clients are in roaming state.
wi01018263	Unified Access: The ACLI incorrectly shows ERS800 software version as 1.0.0.0.
wi01035765	Not able to set default threshold value for `auth-fail` client threat.
wi01036892	The logs `avWlanLostConnectionToBackupMDC` and `avWlanElectedSelfAsBackupMDC` are not generated in syslogs, but the traps are generated for the same.
wi01040385	Bandwidth values set for a specific user (username) changes on wireless controller reboot.
wi01040703	The Mac-Address is displayed in incorrect format in the error message while displaying the output for `show wireless security wids-wips rogue-ap-classification`.
wi01042784	User configured values for `Dscp2cos`, `cos2dscp`, `wmm2cos`, `cos2wmm`, `egressmap` and `ingressmap` reset to default values after a reboot and an image upgrade.
wi01048101	Captive Portal login page intermittently redirects to a blank page.
wi01057286	HTTPS protocol support in HTTP protocol mode.
wi01073972	The CP image name is not consistent following an image import (2.0.1.0).
wi01010308	Retrieving CP image using TFTP with 0.0.0.0 does not pull from all controllers.
wi01060444	AP does not forward AeroScout tag packets to the positioning server after capture.
wi01060325	Deleting the default captive portal profile must not be allowed.
wi01059978	Session time sets to 0 when defaulting a captive portal profile.
wi01021459	8180 password security or Stack password.
wi01015710	The AP 8120-O (Outdoor AP) radio supports a maximum of 124 CCMP enabled clients or a maximum of 62 TKIP enabled clients.
wi00928771	Configuration of the Captive Portal Max-Bandwidth parameter (with non-default values) changes when you upgrade from release 1.0.x to release 2.0.0.
wi01073763	The CLI and EDM become unresponsive after configuring a TACACS+ server using the EDM. Use the CLI to configure TACACS+ server profiles. You cannot insert, edit, or delete TACACS+ server profiles from the EDM.
wi01097044	The AP8120-O intermittently fails to provide statistics report to the controller.
wi01097178	Sometimes the CLI command to show the Auto-RF power plan shows wrong reason code.

WI ID	Summary
wi01119655	Some times restoring binary config on controller results in 'out-of-sync' for "security mac db" component. To recover from the inconsistency, perform Config-Sync operation on AMDC.
Mobility Domain	
wi00928786	When auto-promote is enabled for the domain, the Domain AP Database could display the country-code as US (For North America) and DE (for Europe) even though the Domain Country Code is set to a non US country in NA (non DE country in Europe). This does not impact the AP functionality. The managed AP table (show wireless ap country-code in CLI or WMS Monitoring, Access Points in WMS) shows the correct country code. This discrepancy in Domain AP Database (show wireless domain ap database in CLI or WMS, Configuration, Devices, APs in WMS) can be avoided if Access Points are manually added to the domain ap database.
EDM	
wi00600241	EDM does not allow AP Campus Field Configuration.
wi00600416	Cannot reset APs or update the image on APs managed by the Peer wireless controllers.
wi00601370	In EDM, under **Wireless** > **Security** > **WIDPS** > **RFscanAP**, the RF-scan table displays the OUI for AVAYA APs as `Unknown`.
wi00601390	The wrong help is displayed for 40 bit-WEPkey in the Network Profile Security tab.
wi00973315	EDM does not allow to change the active state of an external AP image entry to true or false after the entry is created. It is recommended that you delete the entries and recreate the with the correct state.
wi01035581	Changing the Active Field in External Image Upgrade option from *True* to *False* or `False` to `True` using the EDM is not reflected in the CLI.
wi01059980	User logout is enabled and session time is 0 when creating Captive Portal profile using the EDM.
wi01051779	SNMP get value error for MIB elements in avWlanMobAgentVlanTable.
wi01024545	WPA-personal key disappears after controller reboots.
wi01070112	Unable to delete VLAN IP interface from the EDM.
Traps/Syslog	
wi01018960	With topology change events, STP (L2) related traps are seen in WMS Alarms (traps) with OID.
wi00576426	Trap message is not generated when a Wireless Client fails MAC Authentication.
Wireless LAN Management System (WMS)	
wi00686010	WMS Diffserv Classifers Table can be sorted either in Ascending or Descending order. If users do this, then the ordering of the classifers is modified and it cannot

WI ID	Summary
	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. **Workaround**: Avaya recommends not to sort the classifier table in WMS.
wi00926746	WMS uninstall process removes the avaya/wms/backup folder and erases any backup files stored in that directory. **Workaround** : Avaya recommends to save the backup file to a folder outside avaya/wms folder to be able to restore WMS configuration after upgrade or re-installation.
wi00883059	Captive Portal Redirect URL configuration with "%" character is not accepted through WMS. **Workaround**: To configure URL with special characters use CLI or EDM.
wi00990733	When APs are moved from one Mobility Domain to another Domain without removing the AP from the Domain Database of the original Domain, WMS RF Views can fail to display AP information correctly.
wi01040991	Backed up traps are not restored when you perform a WMS upgrade.
wi00905407	When you install WMS on Windows 7 64-bit SP1, a warning pop-up window displays indicating that this version of Windows is not officially supported by this release of the WMS server. This issue is however not seen on Windows 7 32-bit SP1 or Windows Server 2008 SP2.
wi01105031	The MAC address of a wireless client appears in the merge report, after performing a *Block* action on the client from the client monitoring screen on WMS.
wi01112330	Radio *admin* configuration failed while using WMS.
wi00664791	WMS_IE/NetworkProfiles/QoS Tab: the policies names are overlapped and cannot be clearly seen with Internet Explorer 8.
wi00929515	The AP database allows a different country code AP (for example, IN) with default AP Profile (for example,US) when the APs are imported using a CSV file.
wi00970620	Managed AP Dashboard under WMS does not display AP Radio Statistics. This information is only available via CLI.
wi00979482	Monitoring: Captive portal user count is not being updated correctly under **Monitoring** > **Mobility Domain** > **Captive Portal** tab.
wi00981511	Monitoring: WMS Captive Portal tab has functionality missing to display Captive Portal session attributes, client actions, sorting, and filtering, etc.
wi00985958	Monitoring: The Domain dashboard tables are locked and tables cannot be resized making it extremely difficult to view contents of certain tables.
wi00986863	WMS allows Diffserv classifiers to be deleted when they are being used in a Diffserv policy.
wi01004048	The Import policies fail and exception appears in the WMS logs after configuring the Ap-profile profile name as case sensitive.

WI ID	Summary
wi01011696	WMS DB backup through the **Admin** tab is not showing the backup file on the backup or restore page.
wi01018671	The bulk edit option does not apply bulk edits for APs from filtered AP profiles but applies for all APs in APDB.
wi01030802	Trap `avWlanLimitsReached` for MDC Capability is not displayed in WMS Alarms.
wi01037700	A BGN Radio Profile (US) created by the WMS has all channels checked as Eligible Channels which is incorrect. The Eligible Channel List for US is 1,6,11 for BGN radio for 20 Mhz.
wi01037989	Re-import of configuration fails for any profile or Mobility VLAN configured with the same name but with a different case.
wi01039775	When re-importing a domain, the client user groups which are configured under security context has the default user group missing.
wi01040862	The **Security DB, Local Client DB** database supports a maximum of 1000 users, but you are able to add more than 1000 users using the WMS.
wi01074887	When creating an AP-Profile using the WMS for the EU region, the 5 GHz radio is disabled for the AP 8120-O.
wi01074802	Certain Packet sizes were not being forwarded from the AP, which caused connection issues with a few applications on Ipad/Iphone.
wi01060155	When applying policies for AP profiles using the WMS, changes are detected between the controller and the WMS.
wi01017853	The WPA key from the network profile got truncated after a reboot.
wi01073973	The Captive Portal Block command sometimes goes into a pending state.
wi01059799	Unable to see the generated certificate in the WMS 2.0 with the controller running release 1.2.1.
wi01047121	WMS CPU or Memory Graphs only display 2 days data on the landing page & the WC dashboard.
wi01035565	Channel and Power values should be displayed in a drop down box while setting them dynamically.
wi01118076	The Auth start and Auth end date parameters in the user database must be reset by issuing *no command* before modifying the value.
wi01087433	When you upgrade the WLAN 8100 to release 2.1.0, after you upgrade the WMS and controllers in the domain, you must ensure that you re-import configuration from the AMDC of the domain. This is especially important if you added Captive Portal users (*local users* in releases prior to release 2.0.0) on the WMS before the upgrade. Captive Portal user configuration on the WMS is lost after an upgrade and you must explicitly re-import this configuration from the AMDC.

WI ID	Summary
wi01078101	Unable to launch EDM for a controller, when a non-default HTTP port is configured on the controller.
wi01096933	On the **Mobility Domains** landing page, the **Domain Statistics** graph for the **bytesDropped** data menu option is not displayed.
wi01096951	For mobility domains configured in a Unified Access deployment, the count of mobility VLANs was displayed as 0 on some WSPs.
wi01096961	For a mobility domain configured in the Unified Access deployment, the AP Uptime generates incorrect information for APs whose managed time is more than one hour in the graphical representation in PDFs.
wi01097098	For mobility domains in Unified Access deployment, the Management Connectivity status displays blank WSP entries.
wi01097334	The Management Connectivity status does not update the down time after the AMDC becomes unreachable.
wi01095987	On the **Monitoring** > **Captive Portal Clients** page, the traffic summary graphs on the **CP Status** page are not populated. However, the corresponding **Captive Portal Clients** monitoring page displays the graphical data correctly.
wi01096754	On the **Monitoring** > **Controllers** page, when you click **Port Mirroring**, the **Port Mirroring** dialog box displays numbers instead of text in the **Allow Traffic** and **Mode** columns, for a port mirroring instance.
wi01091769	On the **Mobility Domain** > **Details of Domain** > **Domain Reports**, when you click the **AP Inventory** report, it displays AP Model and IP address incorrectly.
wi01091521	Context sensitive help does not exist for Custom Graph Browsers.
wi01091343	The Alarm count is displayed incorrectly on all monitoring pages.
wi01092290	On the **Monitoring** > **Controllers** page, on the **Controllers Summary** dialog box, clicking the **Managed APs**, **Auth Clients** and **Mobility VLAN** links does not display the respective pages.
wi01091001	On the **Monitoring** > **Access Points** page, export to a CSV file does not export all default and non-default columns in CSV format, for managed APs.
wi01089906	On some monitoring dashboards, the legends for the graphs are not displayed.
wi01088470	The **Monitoring** > **WIDS** > **Rogue Clients** page displays wrong count numbers.
wi01088464	On the **Monitoring** > **Access Points** > **Rogue Client Detected** page, for an given AP, the search field does not work.
wi01088146	On the **Monitoring** > **Access Points** > **Rogue AP Detected** page, for a given AP the search field does not work.
wi01087725	On the **Monitoring** > **Switching Points** page, the Domain Alarms panel is not displayed.
wi01087429	Navigate to the **Mobility Domain** > **Configuration**. Select a domain and click **Action** and choose **AP Load Balancing** from the drop down list. The

WI ID	Summary
	confirmation message does not display after issuing an AP loadbalance from WMS.
wi01090921	On the **Monitoring** > **Access Points** page, in the **Details for the AP** pane, entries are not displayed for **Neighbor AP**.
wi01090465	On the **Monitoring** > **WIDS** > **Adhoc Clients** page, in the Adhoc client reporting, the AP state entry is not being purged and updated.
wi01090175	On the **Monitoring** > **WIDS** > **Ad Hoc Clients** page, there is no **actions** button to select an action.
wi01090129	On the **Monitoring** > **WIDS** > **Ad Hoc Clients** page, there is no search functionality of ad-hoc client monitoring.
wi01087433	Captive Portal users and user groups appear in the merge report though they are present on both the Controller and WMS after upgrading from 2.0.0 to 2.1.0.
wi01063978	On the **Configuration** > **Policy** > **Radio Profile** pane, when you click **Edit** and select the **Data Rates** tab, Multicast Tx rates are not setting Tx rates as per the drop down list.
wi01091287	On the **Configuration** > **Devices** > **Controllers** page, blank status message is displayed after the VLAN configuration is edited.
wi01080590	While installing WMS on Windows 7 64bit, controls like **cancel**, **previous** and **next** appears in normal text instead of as a check box.
wi01079910	The error message **WMS is already installed** does not display like in other platforms, when upgrading on RH5.2.
wi01095036	You cannot install WMS software license on a Non-English language operating system.
wi01095128	Auto-RF: Incorrect default value for APA minimum power configuration, while creating a new domain on WMS.
Access Point (AP)	
wi01039137	Some APs may pick channel 2 instead of channel 1 due to a known issue. A corresponding log message is generated.
wi00996001	SplitPlane Outdoor AP: ICMP Packets with 2000 bytes size from Wireless Client is dropped even if Jumbo Frames is Enabled in ERS/POE, and the MTU size is set to 9600.
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.
wi01064338	WMS channel changes for outdoor AP (AP 8120–O) and indoor (AP 8120–E).
Wireless Controller	
wi00891828	When Captive Portal IP Interfaces are deleted and re-created multiple times, wpsProcessCpIpUpdates or wdpmCpInterfaceSet Error Messages can be

WI ID	Summary
	observed intermittently and the operation fails. Retrying the operation will be successful.
wi00909047	Doing configuration changes that would require config sync in a large scale setup with thousands of users connected could impact domain stability. It is recommended not to make configuration changes in a live environment with thousands of clients connected to the Wireless network.
wi01020470	Captive Portal does not work when a Wireless or System interface has the `Management` flag enabled.
wi00988412	When upgrading, or downgrading from 1.1.1 to 2.0.0, the AP image version on the controller fails to upgrade. Workaround: Upgrade the controller twice so that the AP image is properly downloaded and upgraded.
wi00992409	Sometimes, when connecting to a Captive Portal on a FireFox browser using HTTPS, you see the `SSL Connection Failed` message on the browser. To recover from this issue do the following: • Clear the certificate store • Restart the browser
wi01034431	When you upgrade from 1.2.0 to 2.0.0, some custom settings change to default values.
wi01015923	In a scaled eight controller domain with 12K clients, several WCs lose cluster connection but recover when one PWC reboots.
wi01023515	VLAN mgmt IP routing enabled after reboot.
wi01031743	WIDPS: In a domain where AP belongs to multiple countries, AMDC is incorrectly classified Managed AP as rogue AP.
wi01041482	In release 2.0, the basic and supported data rates 1, 2 are disabled by default. You must specifically configure these data rates, if required.
wi01100446	The *client qos status* command on the Wireless Controller does not show the correct bandwidth Up and Down values.
wi01095968	The AP8120-O treats open client as a CP client and puts it in UNAUTH state when captive portal is disabled for the network profile.
wi01096278	For the outdoor AP AP8120-O, the controller does not allow the user to configure an eighth VAP for Outdoor APs in 5GHz and 2.4 GHz radios.
wi01096053	When captive portal is disabled on the network profile, CP sessions are not removed on Peer controllers.
wi01097506	When a new network profile is created, MAC validation is enabled by default, whereas it should be disabled.
wi01095024	When a wireless client roams from Outdoor AP to an Indoor AP for the first time, the username field is not populated for RADIUS clients.

WI ID	Summary
wi01087315	For network profile configuration using the ACLI, MAC Validation with RADIUS is supported with security mode WPA-Enterprise. Ideally, it should not be supported.
wi01082302	AP load balancing: The AMDC do not update load-balance **controller-lb-status** table after peer controller leaves the domain.
wi01081872	Backup ASCII config and restore shows **Out-of sync** for CP, Auto-Rf, Radius Auth, Network-profile and Security DB.
Mobility Domain	
wi00575533	Due the limited number of non overlapping channels available on the 2.4 GHz Band using channel bonding (40 MHz mode) could result in connectivity issues for some of the older adaptors. **Workaround**: Avaya recommends to use 40 MHz Mode on the 5 GHz Radio and use 20 MHz Mode on the 2.4 GHz Radio on the AP.

Chapter 6: Known Issues

Known issues in release 2.1.0

The following table identifies known issues in the WLAN 8100 software, for release 2.1.0.

Work Item (WI) ID	Summary
Command Line Interface (CLI)	
wi01111850	The CLI command **`show wireless ap-profile`** on the A-MDC shows the status of an AP profile as *configured*, if there are no active APs associated to the AP Profile on the A-MDC.
wi01118431	When you execute the **`show wireless network-profile/ap-profile cos2wmm/wmm2cos/dscp2cos/cos2dscp`** command without the profile ID, the command execution is successful but no data gets displayed.
wi00970357	Configuring an *Auth End Date* that is earlier than the *Auth Start Date* in the Captive Portal user database is possible.
wi01122207	The WC 8180 quick configuration utility does not: • allow the mapping of a newly created network profile to a newly created AP-profile • allow the management VLAN as a client VLAN
wi01041340	Configuring an *Auth Start Date* and an *Auth End Date* (for Captive Portal users) that is later than the current date on the controller, is possible using the CLI and the EDM. Also, the system does not allow you to create a user entry with the same start and end date.
wi01097227	A brief service interruption occurs when RADIUS MAC validation is done using Packet Fence Server RADIUS and Guest Registration functionality.
WLAN Management System (WMS)	
wi01129130	Unable to reuse *SNMP* community after notify-view. Controllers allows you to create two different community strings (Notification and RW) with the same name. Ideally, controller should display an error message. **Workaround:** Use two different names for Notification community and RW community. Or while creating Notification community give the new community permissions for RO and RW along with Notification.
wi01079972	Site Model Designer may not work correctly in non-US or non-English localized Windows. **Workaround**: Use a US or English localized OS to launch the SMD.

Work Item (WI) ID	Summary
wi01015637	Unified Access: A Primary RADIUS server failure causes RADIUS deamon crash and restart when 360 wireless clients are connected at the same time.
wi01085983	On the **Mobility Domain** > **Configuration** > **Domain Name** > **Devices** > **Wireless Controllers**, sorting is case sensitive. That is sorting does not work when *Label* and *Campus* have same name but differ only in their `case`.
wi01089860	On the **Configuration** > **Security** > **Captive Portal Users** page, Captive portal user groups do not display the count.
wi01091628	Redirect URL accepts special characters that are not supported, such as the `+`, `&` and `#` characters.
wi01092057	All the MVLANs and their corresponding mappings are displayed on a single page and takes a long time to load if, for example, there are 3000+ MVLANs.
wi01093392	Navigate to any *Custom graph* browser. Custom graphs displayed should be displayed only for the chosen data source value. If the value *Packets transmitted* is chosen, the graph is displayed for packets received, transmitted and total. The same thing is seen for Bytes and packets received, transmitted and dropped.
wi01107560	The *save-to-db* option to set channel and power of an AP that is available on the CLI but not on WMS.
wi01111683	An error displays and the system is unable to map AP identities on the SMD through the WMS server, with JAVA version 7 on Windows 7.
wi01114808	Navigate to **Mobility Domain** > **Configuration** > **Domain name** > **Devices** > **Wireless Controllers** and edit the A-MDC. The merge report displays incorrect information after certificate mapping on the WMS.
wi01115602	The back up of the controller running configuration during the controller image upgrade using the **Image Update** option on the WMS, performs a back up of the binary configuration. But there is no option to perform an ASCII configuration backup.
wi01117064	The WMS does not display the AP Port speed and Duplex status for a discovered AP.
wi01118873	The Client Dashboard continues to show the previous session's *Station Isolation* status.
wi01117859	The CAC-AP downgrades voice packets when the ACM bandwidth is exceeded.
wi01085785	Packet Fence needs to support VLAN assignment using the VLAN name. Currently, Packet Fence assigns VLANS to the connecting wireless client based only on *VLAN-id* and not *VLAN-name* (mobility VLAN name).
wi01070846	The merge report displays configuration differences between WMS and Controller even though there are no actual differences in values.
wi01081207	Launch WMS client using IE10 on Win7,W2k8-64b and Win8. When you right-click on the **Configuration** navigation menu, the menu does not display.

Work Item (WI) ID	Summary
wi01081216	On the WMS, the **Site Model** and **RF View** pages display in compatibility mode only for Internet Explorer (IE) 10 on Windows 7, Windows 8 and Windows 2000 (W2k864b), even if the Active scripting and scripting are enabled under **Tools** > **Internet Options** > **Security** > **Security Settings**
wi01079907	WMS install on RH 6.3- 64–bit fails. There is no support for Linux 64–bit on the installer.
wi01098204	The `Show wireless ap status` command displays the configuration status of the AP. • If External Download is **Enabled** (applicable for all AP models), the system checks against the configured external image version to the current image version on the AP. If the versions on the AP and configured external version are different, the **Need Image** flag is set to *yes*. • If External Download is **Disabled**, specifically for outdoor APs (AP 8120–O), the AP software version is compared with configured active external download version irrespective of whether external image download is enabled or not, since internal download is not supported.
wi01123921	To update the domain AP image, on the **Mobility Domain** dashboard navigate to **Actions** > **Updtae** > **APs Image** and configure the HTTP server type, AP model, image version and file name and click **OK**. This configuration is pushed to WC , which issue the config sync to change the **Need update image** from *No* to *Yes*. The transition from *No* to *Yes* can take few seconds depending on the number of APs in the domain. It is recommended that you wait for about 10 seconds so that all APs are marked for upgrade before confirming the upgrade in the pop up window.
Enterprise Device Manager (EDM)	
wi01085303	On the **Wireless** > **Crypto** > **Certificate** > **Insert** page, the system is able to create a certificate with the **common name** as an empty string and with an empty **Validity** field.
wi01059400	The Chrome browser does not support EDM help files. It displays an error.
wi01070132	Mobility VLANs are not listed in ClientConfigVLAN table when scaled up.
wi01071060	The Client Station discovery reason is not synchronized between the EDM and the CLI.
Wireless Controller	
wi01089025	The existing AP image details are not removed after modifying the external AP image server details (for example, the IP address).
wi01096236	An authenticated Captive Portal client does not block multicast when the session is removed.
wi01098583	The Domain and Controller statistics get reset after all the APs in a domain are reset.

Work Item (WI) ID	Summary
wi01120506	The Wireless Controller upgrade screen fails to display, when the default bundled controller image file is deleted.
wi01048400	When TSPEC Video is enabled on the radio profile, Apple iPads and iPhones running IOS 6 have difficulty connecting to the network.
wi01081062	After enabling **Station Isolation** on a network profile, the **dropped pkts** and **dropped bytes** counters for wireless clients do not get updated.

Known issues from releases prior to release 2.1.0

The following table identifies known issues that are present from previous software releases.

Work Item (WI) ID	Summary
Command Line Interface (CLI)	
wi00600411	Clearing domain or controller statistics does not clear the Wireless Diffserv statistics. The statistics get cleared when a client either disconnects or roams.
Enterprise Device Manager (EDM)	
wi00971732	Radio Profile created via EDM, and ACLI uses different default value, i.e. 802.11 mode, channel bandwidth, eligible channel, DTIM.
wi01032856	Deleting random classifier blocks is not possible needs to be orderly deleted
wi01026911	Adding classifier blocks only in series, random add is not possible.
wi01019753	Wrong error tab is printed while inserting the same mac-address of the controller in the location database.
wi01025812	Stop, Restart and deletion of multiple capture instances is not possible via 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. **Workaround**: Use the CLI to correct the configuration in this scenario.
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.
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.
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.

Work Item (WI) ID	Summary
wi00653845	ASCII configuration download fails when initiated via EDM.
WLAN Management System (WMS)	
wi01043005	The controller dashboard Mobility VLAN count is displayed as `0` and no entries exist when compared with the AMDC, when you configure Mobility VLANs with the same name but differ only in their case.
wi01041059	When a static DNS server address is configured on a network interface of the WMS server, HTTPS connection fails.
wi01029481	Applying a policy (push) to the controller fails for already managed APs when WIDS—WIPS radio profiles are mapped.
wi01015716	Heatmap displayed is incorrectly for 802.11n APs in WMS-RF Views.
wi01017222	Incorrect status of APs when APs of two domains are plotted on the same SMX file are shown in RF views.
wi00997374	The WSP Load balance portlet should be present in the Mobility Domains dashboard.
wi01016048	For a connected Captive Portal client, a Captive Portal enabled network profile with the Bandwidth Up/Down parameter configured can have the value overridden by the Radius attribute for Bandwidth. In such a case, the command `show wireless client qos status` shows the network profile value instead of the Radius applied value for Bandwidth. But the command `show wireless captive-portal client status detail` for the same client reflects the correct value.
wi00986547	WMS does not support Remote Packet Capture feature.
wi00991412	Certificate mapping data is pushed to peer controllers without `config-sync` through WMS.
wi00990774	While configuring Captive Portal interfaces via WMS, the consistency check to prevent use of WC 8180 Management IP address as a Captive Portal IP interface is missing.
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. **Workaround**: Avaya recommends to crop 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.
wi00908763	WMS RF Views do not take Cable Length for External Antenna AP into account when displaying coverage area in the floor plans.
Wireless Controller	

Work Item (WI) ID	Summary
wi01017356	Unified Access: AP8120-E becomes unmanaged and reboots when throughput test is executed for frame size 256 with WPA2-Personal
wi01015951	Clients entries remain in AMDC.
wi01016430	Clients take time to authenticate when radius offload is enabled and one of the radius servers is down.
wi01036393	Load Balance status for few APs with respect to WCP and WSP shows as unknown though the preferred and alternate WCP are configured in the domain AP database.
wi01035879	Though the APs are connected to correct WCP and WSP, one of the APs in the domain incorrectly shows LB method as LL when the LB metric is CBFS.
wi01030273	When the WSP fails, clients attached to its APs do not roam and experience a traffic loss of 12-15 seconds.
wi01024946	When you execute **`show logging system`** command in overlay, some of the Mobility Switch related log messages are not displayed.
wi01023522	In a very intermittent situation, the Management IP becomes inactive after reboot or upgrade.
wi01029655	Unified Access ACLI: AP is not able to get managed or load balanced when a WCP (having APs Mac in the AP Database) is redirecting the same AP to the WCP which does not have AP MAC entry in the AP Database Table.
wi00985604	In UA mode, need to prevent AP sending Beacons/Probes when WCP is in failed state.
wi01003062	When Static WEP is configured without key value, the privacy bit is set to 0.
wi01040859	Unable to enter radius profile name with special characters '-' and '_' in EDM.
wi01013916	If Health Check is disabled, a Radius server failover between the primary and secondary Radius servers does not happen, when primary Radius Server goes down.
wi00575545	Downloading the controller image from a USB will be very slow. **Workaround**: Avaya recommends to download the image from a TFTP server through the LAN interfaces.
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.
Access Points	
wi00991245	When Band Steering is enabled it is observed that some Dual-Band roaming Clients are still associate with 2.4 GHz radio. This is dependant on client behavior. AP8120/8120-E attempt to steer the client to 5 GHz only once to avoid association or roaming delays.

Work Item (WI) ID	Summary
wi00969067	Radio Profile created for AP 8120-O model should limit the maximum value of DTIM to 15, as supported by this AP Model.
Captive Portal	
wi01004565	The AP 8120-O requires that you map the Network Profiles to the VAP IDs sequentially. If a VAP ID is left blank and a higher VAP ID is mapped to a Network Profile, Captive Portal clients connecting to that SSID can receive Open Network Access.
Security	
wi00576447	Wildcard entries are not supported for MAC Entries in the MAC Database on the WC 8180.
Diffserv 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. **Workaround**: Use the MAC address of a specific client and execute "show wireless diffserv statistics <mac>" to provide the correct statistics for a particular client. "
E911	
wi00839411	CPU spikes during E911 auditing.
wi00839405	E911: AP and client auditing did not finish within the configured interval (5 minutes) and could overlap. **Workaround**: Avaya recommends to configure the interval as 10 minutes or more.

Chapter 7: Mobility domain platforms and capacity

The types of platforms supported and the capacity of the platforms can vary depending on the deployment model and WLAN 8100 software release.

The Wireless LAN controller (WC 8180) provides the ability to register and support up to 512 WLAN 8100 series Access Points. The Wireless Controller WC 8180-16L provides the ability to register and support up to 16 Access Points.

In previous releases, for example, where 32 APs were present in a small deployment with 2 WC8180-16Ls, even though the mobility domain had support for 32 APs, each WC8180-16L could support only 16 APs. If either controller was lost, the total active APs reduced from 32 to 16 to meet the hardware limit of the single remaining WC8180-16L. However from release 2.0 onwards, the WC8180-16L controller permits up to 32 APs to be managed.

Note:

The WC8180-16L can be unlocked using a specific *KeyCode* to reuse the same hardware, and expand hardware support for up to 512 APs.

Access Point licenses from all wireless controllers are pooled within the Active Mobility Domain Controller (AMDC) of the domain. When a controller is added to the domain, the base AP Licenses as well as expansion licenses on the controller are made available for all controllers within the domain. However, the total number of licenses of all APs within the domain, must not extend beyond the hardware capacity limits of the WC 8180 or WC 8180-16L.

The following sections describe the mobility domain platforms and capacity for the Overlay and Unified Access deployments of the WLAN 8100 solution.

Overlay deployment products and capacity

The following tables show the Overlay deployment platform products and capacity, for release 2.1.0.

Table 5: Overlay deployment platforms (Release 2.1.0)

WC platforms	AP/WC	AP platforms
8180	512	8120/8120-E/8120-O
8180-16L	16 (32 failover)	8120/8120-E/8120-O

Table 6: Overlay mobility domain capacity (Release 2.1.0)

Maximum APs	2048
Maximum wireless controllers (WC)	8/16**
Maximum Wireless Networks	64
Maximum mobility VLANs	4000
Maximum mobility VLANs per AP	64
Maximum wireless networks per AP	32 (16 for each radio)
Maximum mobility VLANs per controller	2048
Maximum number of APs in the domain AP database	4096
Maximum number of wireless clients in the domain	10,000
Maximum number of Captive Portal clients	8192 *
Maximum number of Captive Portal IP interfaces	80

Key:

- * Indicates maximum CP sessions supported in a domain with multiple controllers. The recommended limit is 1024 sessions if a single controller is used in the domain.
- ** Indicates 8 controllers with highly scaled APs and 16 when APs are not scaled to the maximum on the controllers.

Avaya VENA Unified Access deployment products and capacity

The following tables show the Unified Access deployment platform products and capacity, for release 2.1.0.

Note:

The AP 8120–O is not supported in a Unified Access deployment.

Table 7: Unified Access deployment platforms (Release 2.1.0)

WCP Platform	AP/WCP	WSP Platform	AP/WSP	AP platforms
8180	512	ERS 8800	1024	8120/8120-E

WCP Platform	AP/WCP	WSP Platform	AP/WSP	AP platforms
8180-16L	16 (32 failover)	ERS 8800	1024	8120/8120-E

Table 8: Unified Access mobility domain capacity (Release 2.1.0)

Maximum APs	2048
Maximum wireless control points (WCP)	8/16**
Maximum Wireless Networks	64
Maximum Mobility VLANs	4000
Maximum Mobility VLANs per AP	64
Maximum Wireless Networks per AP	32 (16 for each radio)
Maximum mobility VLANs per controller	2048
Maximum number of APs in the domain AP database	4092
Maximum number of wireless clients in the domain	10,000
Maximum number of Captive Portal clients	8192 *
Maximum number of Captive Portal IP interfaces	80
Maximum ERS 8800 WSPs	8
Key: • * Indicates maximum CP sessions supported in a domain with multiple controllers. The recommended limit is 1024 sessions if a single controller is used in the domain. • ** Indicates 8 controllers with highly scaled APs and 16 when APs are not scaled to the maximum on the controllers.	

Device capacities

The following table describes the device capacities for release 2.1.0.

Parameter	WC 8180	WC8180–16L	AP 8120/E/O
VLANs (Supported and User configurable)	256 and 247	256 and 247	0
IP Interfaces	128	128	1
GE Ports	24	24	1

Parameter	WC 8180	WC8180–16L	AP 8120/E/O
10 GE Ports	2	2	0
MAC Addresses	1,024	1,024	32
L2/L3 Forwarding Table (MAC table)	16K	16K	n/a
MCST Forwarding table	240	240	n/a
ARP	32K	32K	n/a
Static Routes	512	512	n/a