Release Notes for Avaya WLAN 8100

Release 3.0
NN47251-400
Issue 10.02
July 2014

© 2014 Avaya Inc.

All Rights Reserved.

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 may generally make available to users of its products and Hosted Services. 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 Avaya hardware and software. 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 or such successor site as designated by Avaya. 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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN 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 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. “Software” means Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. “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. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

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, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, 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 or Hosted Service 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”). As required, 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 or such successor site as designated by Avaya. 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, Hosted Service(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, Hosted Service(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 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, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction 5
Purpose 5
Related Resources 5
Documentation 5
Training 5
Viewing Avaya Mentor videos 6
Support 6
Chapter 2: New in this release 7
Features 7
Other Changes 8
Chapter 3: Wireless LAN (WLAN) 8100 Upgrade 9
Software image file details 12
Chapter 4: Captive Portal browser compatibility 15
Chapter 5: Resolved Issues 18
Chapter 6: Known Issues 20
Chapter 7: Mobility domain platforms and capacity 26
Overlay deployment products and capacity 26
Avaya VENA Unified Access deployment products and capacity 27
Device capacities 28

Chapter 1: Introduction

Purpose

This document provides the latest information on the Avaya WLAN 8100 product and documentation suites for release 3.0, as well as information on software upgrades.

It also provides information on the following:

- Known and resolved issues for release 3.0 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 *Documentation Reference for Avaya WLAN 8100*, 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	
7D00060A	Wireless LAN 8100 Implementation Assessment (online test)

Viewing Avaya Mentor videos

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

About this task

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

Procedure

- To find videos on the Avaya Support website, go to support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to 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 website.

    Note:

    Videos are not available for all products.

Support

Go to 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 *Release Notes for Avaya WLAN 8100*, NN47251-400 for Release 3.0.

Related Links

Features on page 7
Other Changes on page 8

Features

See the following sections for information about the feature changes:

- Support for External Captive Portal on page 7
- Support for Link Layer Discovery Protocol (LLDP) on page 7
- Bonjour Gateway support on page 8

For information on the WMS enhancements and on Avaya Command Line Interface (CLI) commands, see *Using WMS and EDM on Avaya WLAN 8100*, NN47251-108 and *ACLI Commands Reference for Avaya WLAN 8100*, NN47251-107 respectively.

For more information on feature fundamentals, see *Feature Overview for Avaya WLAN 8100*, NN47251-102.

Support for External Captive Portal

Wireless LAN Cotroller 8100 can support external captive portal with patented floating CPIP mapping method and RFC 5176 Change of Authorization (CoA) to achieve a linearly scaling standalone external captive portal solution that is designed for both large and small deployment. WLAN 8100 users can provide their own external captive portal based on design guideline from Avaya.

The WLAN controller leverages RFC 5176 CoA (Change of Authorization) to support small, medium, and large scale deployments.

Support for Link Layer Discovery Protocol (LLDP)

The Link Layer Discovery Protocol (LLDP) is a data link layer protocol in the Internet Protocol Suite used by network devices for neighbor identity and capability discovery. Avaya AP advertises its status to the neighbors and relays the information and status about the LLDP neighbors to its managing wireless controller.

LLDP support on AP can advertise its status, capabilities, and process information from other LLDP neighbors. Eg. PoE switches.

Bonjour Gateway support

Bonjour is a service discovery protocol of Apple. Bonjour locates devices such as printers, other computers, and the services that those devices offer on a local network using multicast domain name system (mDNS) service records. Bonjour can be extended across subnets by using *Avaya WLAN 8100 Bonjour Gateway feature*, which selectively relays service discovery packets across networks without using external gateway or custom router configuration.

Related Links

New in this release on page 7

Other Changes

This document contains a high level overview of the WLAN 8100 software upgrade to release 3.0, including software image file details. Procedures to actually perform the upgrade have been removed from this document.

For more information on software upgrade, see the *Applying Upgrades and Patches to Avaya WLAN 8100*, NN47251-402.

Related Links

New in this release on page 7

Chapter 3: Wireless LAN (WLAN) 8100 Upgrade

The following sections provides a high level overview of the WLAN 8100 Upgrade to release 3.0. It outlines the supported upgrade paths for upgrade to release 3.0.

For information on software upgrade for prior releases, see the *Applying Upgrades and Patches to Avaya WLAN 8100*, NN47251-402 for that release.

Supported upgrade paths

Table 1: Supported upgrade paths — wireless controllers and APs

Upgrade path	Support
Upgrade 1.x to 3.0	Not supported
Upgrade 2.x.x to 3.0	Supported
Migration from 3.0 Overlay to 3.0Unified 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.x.x to 3.0	Requires an un-install followed by a WMS install
2.x.x to 3.0	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.x.x to release 2.x.x), 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 *Using WMS and EDM on Avaya WLAN 8100*, NN47251-108.

WLAN 8100 upgrade workflow for release 3.0

Important:

General Upgrade considerations:

- If you are upgrading from release 1.x.x, you must first upgrade all the components of the WLAN 8100 (WMS, wireless controller and access points) to release 2.x.x, before you upgrade to release 3.0 software.
- The release 3.0 wireless controller cannot manage access points operating on release 1.x.x software versions. Therefore, you must first upgrade all access points to release 2.x.x software version before upgrading to release 3.0.
- To migrate to a Unified Access deployment, you must first upgrade your existing Overlay solution to release 3.0

  For example, if you currently have release 2.x.x of the WLAN 8100 Overlay solution, and you want to migrate the solution to the 3.0 Unified Access, you must first upgrade to release 3.0 Overlay.

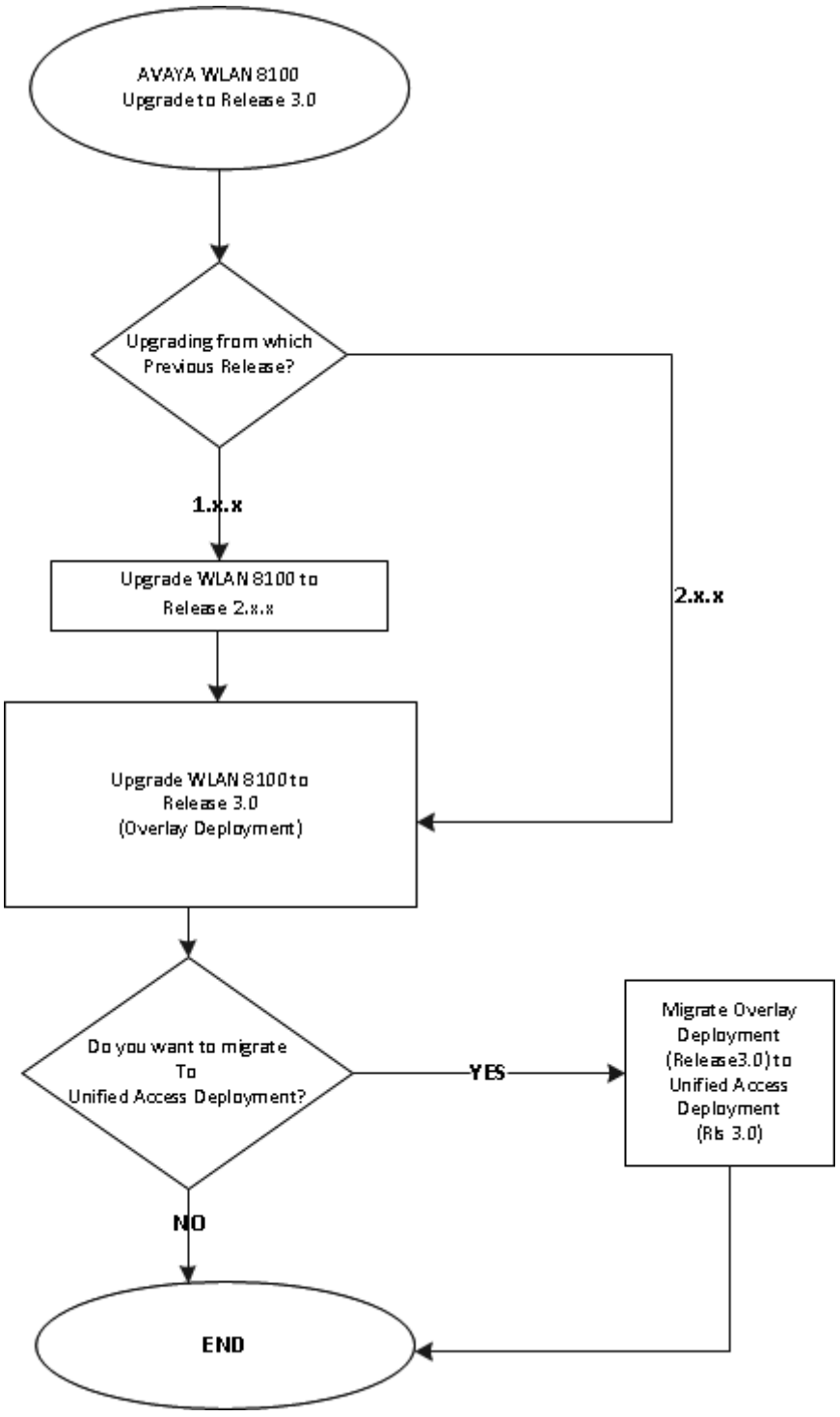

Figure 1: Upgrade WLAN 8100 to release 3.0 — workflow

Related Links

[Software image file details](#) on page 12

Software image file details

The following sections provided the software image file details for releases 1.2.0, 2x.x and 3.0.

Table 3: Software image files released with release 3.0

Component	File Name	File Size (bytes)
WC 8180 Controller Image	wc8180_3.0.0.076s.img	46,880,756
AP8120/AP8120–E	AP8120-Upgrade_3_0_0_076.tar	9,205,760
AP8120–O Image **Note:** The AP 8120-O only supports the external image download.	AP8120-OAP-Upgrade_3_0_0_076.tar	7,219,200
WMS Windows 32 bit	WLAN8100_WMS_3.0.0.076_Windows_32bit.exe	389,157,961
WMS Windows 64 bit	WLAN8100_WMS_3.0.0.076_Windows_64bit.exe	389,320,374
WMS Linux	WLAN8100_WMS_3.0.0.076_Linux.bin	403,255,481

Table 4: Software image files released with release 2.1.1

Component	File Name	File Size (bytes)
WC 8180 Controller Image	wc8180_2.1.1.029s.img	46,450,840
AP8120/AP8120–E	AP8120-Upgrade_2_1_1_029.tar	8,939,520
AP8120–O Image **Note:** The AP 8120-O only supports the external image download.	AP8120-OAP-Upgrade_2_1_1_029.tar	6,963,200
WMS Windows 32 bit	WLAN8100_WMS_2.1.1.029_Windows_32bit.exe	387,927,085
WMS Windows 64 bit	WLAN8100_WMS_2.1.1.029_Windows_64bit.exe	388,076,381
WMS Linux	WLAN8100_WMS_2.1.1.029_Linux.bin	402,010,812

Table 5: 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	AP8120-OAP-Upgrade_2_1_0_102.tar	6,962,545

Component	File Name	File Size (bytes)
Note: The AP 8120-O only supports the external image download.		
WMS Windows 32 bit	WLAN8100_WMS_2.1.0.102_Windows_32bit.exe	386,924,544
WMS Windows 64 bit	WLAN8100_WMS_2.1.0.102_Windows_64bit.exe	386,924,544
WMS Linux	WLAN8100_WMS_2.1.0.102_Linux.bin	401,604,608

Table 6: 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_32bit.exe	169,133,056
WMS Windows 64 Bit	WLAN8100_WMS_2.0.1.013_Windows_64bit.exe	169,134,080
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

Related Links

Wireless LAN (WLAN) 8100 Upgrade on page 9

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.x.x and 3.0. 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.x.x, and 3.0, 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

Mobile device platform	Default supported browser
iPhone version 5.0.1	Safari
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.x.x, and 3.0.

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
Chrome 20.0.1132.57m	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 3.0.

WI ID	Summary
CLI	
wi01153306	Corrected the wrong radio MAC address seen in "show wireless ap radio power status"
wi01144871	Fixed wrong description in the radio-profile for command "incorrect-frame-no-ack"
wi01154898	Fixed an issue related to Station Isolation which was causing the learnt IP and MAC of the client getting resetted
wi01148419	Added fix to not display client-policy in "show wireless diffserv statistics" if the qos-mode is disabled in network profile.
Wireless LAN Management System (WMS)	
wi01164712	Edit a packet capture profile instance and try to remove client MAC. The client MAC was not getting removed. This got fixed.
wi01161423	Added AP Radio statistics details in AP browser export
wi01160735	AP Label field got added to Managed APs' page in the AP Inventory report.
wi01160642	Added Client statistics details in Client browser export
wi01160396	Added support for sorting based on SNR on Client browser.
wi01159255	New column added under AP Monitoring screen for total Clients based on Radio 1 and Radio 2.
wi01156933	Added Client traffic summary graph and Radio statistics graph for AP
wi01155425	Fix added to not allow to delete default mvlan if it mapped to a network profile
wi01145428	AP Statistics Link added to WMS QuickLinks
wi01145425	Domain Statistics Link added to WMS QuickLinks
wi01144857	Controller Statistics Link added to WMS QuickLinks
wi01175284	When exported, CSV shows wrong client transmit rate while WMS shows the correct value. This got fixed
Access Point (AP)	
wi01159817	Fixed AP memory leak when the diffserv policy pushed from radius server gets removed
wi01154366	AP8120-O is now certified for Malaysia. Added support for Malaysia country code and channels on outdoor AP

WI ID	Summary
wi01143619	Added support for 4 triangulation entries instead of 3 for AP and clients for better location accuracy
wi01141059	The supported AP radio channels are not updating when radio profile changed from 40MHz to 20MHz and then to 40MHz for both radios. Fixed for all AP models.
wi01134789	Added support for a maximum number of 64 AP-profiles, network-profiles and 128 radio-profiles.
wi01158502	Fixed random call drop issue seen with Ascom phones caused by client deauth trigged by the AP. Also fixed a case in which clients were not able to connect because of beacon failure.
Wireless Controller	
wi01151951	Added Client Band Steering and Client Association Load Balancing support on AP8120-O
wi01147524	Controller was allowing to change the dot11n parameters on radio profiles created for a/b/g. Added restriction to not allow this.
wi01173160	Strange characters show up on the customized CP login page on some clients because of corruption of the stored files.
wi01174512	Fixed misaligned CLI output of "show wireless client neighbor-ap"
wi01175221	Controller pushed a channel which is not supported by the AP configured with Qatar country code causing the radios to be shut down.
wi01153147	Fixed controller reset issue with log “WPS - WCP health check failure”

Chapter 6: Known Issues

Known issues in release 2.1.1

The following table identifies known issues in the WLAN 8100 software for release 2.1.1.

Work Item (WI) ID	Summary
WLAN Management System (WMS)	
wi01140675	Some of the clients display gap in Clients Traffic Summary graph in the Scaling setup. The packets received by the client are not displayed in the client traffic summary graph by WMS.
wi01141931	Neighbor-AP browser does not display AP entry when only 2.4GHz VAPs are detected.
wi01139793	The Update operation fails for changes in data rates in a Radio profile.

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.
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.
WLAN 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 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.

Work Item (WI) ID	Summary
	Workaround: Avaya recommends not to sort the classifier table in 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.
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.

Work Item (WI) ID	Summary
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.
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.
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.
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.
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.

Work Item (WI) ID	Summary
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.
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	
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.

Work Item (WI) ID	Summary
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.
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 3.0.

Table 7: Overlay deployment platforms (Release 3.0)

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

Table 8: Overlay mobility domain capacity (Release 3.0)

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 3.0.

Note:

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

Table 9: Unified Access deployment platforms (Release 3.0)

WCP Platform	AP/WCP	WSP Platform	AP/WSP	AP platforms
8180	512	ERS 8800	1024	8120/8120-E
8180-16L	16 (32 failover)	ERS 8800	1024	8120/8120-E

Table 10: Unified Access mobility domain capacity (Release 3.0)

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 3.0.

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
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