Avaya WLAN 8100 Release Notes

1.2.0.0
NN47251-400, 04.01
April 2012

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 Web sites 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 Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, 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

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

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, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Purpose of this document

This document provides the latest information on the Avaya WLAN 8100 product and documentation suites as well as information on the installation of software upgrades.

Chapter 2: New in this release

The following sections detail what's new in Avaya Wireless LAN (WLAN) 8100 for Release 1.2. The following list identifies the new features introduced in this release.

Hardware

WLAN 8100 Outdoor Access Point (AP8120-O)

Software

Captive Portal stability improvements

Releases' 1.1.1 and 1.2.0 address a number of defects in the Captive Portal functionality to improve overall Captive Portal usability and system stability. Refer to the Resolved Issues chapter for a detailed list of all resolved limitations.

> ✱ **Note:**
>
> The WLAN 8100 Captive Portal functionality is dependent on the wireless client generating a HTTP or HTTPS request. If the client browser does not resolve the domain name, the client does not generate a HTTP/HTTPS request and the wireless clients do not receive the Captive Portal login page. In environments without a DNS server, the captive portal page does not display after upgrading and clients cannot connect to the captive portal network.

WMS enhancements

- The WMS server uses HTTP for monitoring and polling. Release 1.2 enhances the WMS Server background polling performance by retrieving data from devices using HTTP instead of SNMP. However this requires that you must enable both SNMP and Web on the WC for WMS to work properly.

WMS usability improvements

Trap

- Updated the Trap descriptions based on the SNMP Notifications description for easy understanding.

Upgrade

- Added upgrade support to WMS installer which prevents the manual un-installation of an existing installation. The release 1.2 WMS installer detects the exiting installation and performs the upgrade easily.

Bulk change

- Added support to bulk edit domain APs common parameters based on selected domain APs or all domain APs. If no domain APs are selected then all APs are selected. The user can only bulk update fields which are common across APs.

Hide mode-id

- Removed or Hide ID numbers. Instead of Radio ID numbers, the radio displays in user readable format.

Apply Policy Button

- Double–clicking on the Configuration tab opens the "Configured Mobility Domains" tab. This tab has options to display all configured Mobility Domains. You can select a Mobility Domain and click on "ShowAndApplyConfig" to display configuration differences between the AMDC and WMS. You can then choose to apply policies to the AMDC from the WMS.

Monitoring screen enhancements

- Edit managed AP configuration from Wireless Access Points screen. Click on AP MAC address to edit AP configuration. This configuration change still requires Apply Policy to push changes to the AMDC.
- The Wireless Controllers screen provides a link to view APs managed by a specific controller by clicking on the AP Count for the controller.
- The Wireless Access Points screen provides a link to view clients connected to a specific AP by clicking on the Client Count for the Access Point.
- The WMS Monitoring screens maintain a sort criteria across pages when entries are displayed in multiple screens.

  Note:

  It is a known issue that sorting option only sorts the entries displayed in the page and does not sort across all the entries in the table.
- Refined the search functionality in the AP Monitoring Wireless Access Points screen, by giving options to search based on Campus, Building, Floor & Sector.

Chapter 3: Avaya WLAN 8100 Documentation Suite

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

Avaya WLAN 8100 documentation packaging

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

- **Product fundamentals**
    - *Avaya WLAN 8100 Regulatory Information — WC 8180* (NN47251-101)
    - *Avaya WLAN 8100 Fundamentals* (NN47251-102)
    - *Avaya WLAN 8100 Regulatory Information — AP 8120* (NN47251-104)
    - *Avaya WLAN 8100 Quick Start Guide* (NN47251-106)
    - *Avaya WLAN 8100 WC 8180 CLI Reference* (NN47251-107)
    - *Avaya WLAN 8100 WC 8180 GUI Reference* (NN47251-108)
    - *Avaya WLAN 8100 Regulatory Information — AP 8120 with External Antenna* (NN47251-109)
    - *Avaya WLAN 8100 Regulatory Information — AP 8120–O* (NN47251-110)
- **Planning and engineering**
    - *Avaya WLAN 8100 Planning and Engineering* (NN47251-200)
- **Installation and commissioning**
    - *Power Supply Unit for Wireless Controller 8100 Series* (NN47251-105)
    - *Avaya WLAN 8100 Installation — AP 8120 Series* (NN47251-302)
    - *Avaya WLAN 8100 Installation — WC 8180* (NN47251–303)
    - *Avaya WLAN 8100 Installation — SFPs and XFPs* (NN47251–306)
    - *WLAN 8100 AP 8120-O Quick Installation* (NN47251–307)
- **Operations**
    - *Avaya WLAN 8100 Configuration* (NN47251-305)
- **Upgrades and patches**

  - *Avaya WLAN 8100 Release Notes* (NN47251-400)
  - *Upgrading the Wireless Controller Diagnostics Image to Release 1.0.2.0* (NN47251-401)
  - *Avaya WLAN 8100 Upgrades* (NN47251-402)
- **Fault and performance management**
  - *Avaya WLAN 8100 Troubleshooting* (NN47251-700)
  - *Avaya WLAN 8100 Logs Reference* (NN47251-701)

Roadmap

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

Product fundamentals

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

Title	Description
Avaya WLAN 8100 Regulatory Information — WC 8180 (NN47251-101)	This document provides regulatory information for the Avaya WLAN 8100 wireless controller (WC 8180).
Avaya WLAN 8100 Fundamentals (NN47251-102)	This document provides an overview of the technologies and features used in the Avaya WLAN 8100 product suite.
Avaya WLAN 8100 Regulatory Information — AP 8120 (NN47251-104)	This document provides regulatory information for the Avaya WLAN 8100 access point (AP 8120). This document also provides safety considerations and installation instructions for the AP 8120 hardware.
Avaya WLAN 8100 Quick Start Guide (NN47251-106)	This document provides the information and procedures necessary to quickly complete the initial configuration of the WC 8180 and AP 8120.
Avaya WLAN 8100 WC 8180 CLI Reference (NN47251-107)	This document provides information and procedures for the configuration and management of the WLAN wireless controller 8180 using the command line interface (CLI).

Title	Description
Avaya WLAN 8100 WC 8180 GUI Reference (NN47251-108)	This document provides information and procedures for the configuration and management of the WLAN wireless controller 8180 using the wireless management system (WMS).
Avaya WLAN 8100 Regulatory Information — AP 8120 with External Antenna (NN47251-109)	This document provides regulatory information for the Avaya WLAN 8100 AP 8120 with External Antenna
Avaya WLAN 8100 Regulatory Information — AP 8120–O (NN47251-110)	This document provides regulatory information for the Avaya WLAN 8100 outdoor access point (AP 8120–O). This document also provides safety considerations and installation instructions for the AP 8120–O hardware.

Installation and commissioning

Installation and commissioning documentation provides information and procedures for installing the product hardware and software, and performing the initial configuration.

Title	Description
Power Supply Unit for Wireless Controller 8100 Series (NN47251-105)	This document provides information on how to install the power supply unit (PSU) for the WLAN WC 8180.
Avaya WLAN 8100 Installation - AP 8120 Series (NN47251-302)	This document provides information and procedures for the physical installation of the AP 8120 , the AP8120 with External Antenna, and the AP 8120–O.
Avaya WLAN 8100 Installation - WC8180 (NN47251-303)	This document provides information and procedures for the physical installation of the WC 8180.
Avaya WLAN 8100 Installation -SPFs and XFPs (NN47251-306)	This document provides installation instructions and technical specifications for small form factor pluggable (SFP) transceivers and 10 gigabit SFP (XFP) transceivers.
Avaya WLAN 8100 Quick Installation Guide (NN47251-307)	This document provides concise and visual instructions on how to install and mount the WLAN 8100 equipment, and how to perform the initial configuration.

Upgrades and patches

Upgrade and patch documentation describes the software upgrade process.

Title	Description
Avaya WLAN 8100 Release Notes (NN47251-400)	This document provides the latest information on the Avaya WLAN 8100 product and documentation suites as well as information on the installation of software upgrades.
Upgrading the Wireless Controller Diagnostics Image to Release 1.0.2.0 (NN47251-401)	This document provide information and procedures on how to upgrade the WLAN 8100 system to Release 1.0.2.0 software.
Avaya WLAN 8100 Upgrades (NN47251-402)	This document provide information and procedures on how to upgrade the WLAN 8100 system, details all valid upgrade paths, image details, and image management processes.

Operations

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

Title	Description
Avaya WLAN 8100 Configuration (NN47251-305)	This document provides workflows and procedures for the configuration and management of the WLAN 8100 wireless controller (WC 8180). You can perform these procedures through the command line interface (CLI), wireless management system (WMS), and EDM interfaces.

Fault and performance management

Fault and performance management documentation enables you to manage faults, and measure and optimize the performance of the product.

Title	Description
Avaya WLAN 8100 Troubleshooting (NN47251-700)	This document provides troubleshooting information and procedures for the WLAN 8100 wireless controller (WC 8180) and the access

Title	Description
	points (AP 8120, AP 8120 with External Antenna, and AP 8120–O).
Avaya WLAN 8100 Logs Reference (NN47251-701)	This document provides a reference for the log messages generated by the system.

Chapter 4: Upgrading WLAN 8100 software

This chapter contains instructions on how to change WLAN 8100 software, including how to upgrade the wireless LAN management system (WMS), wireless controller (WC), access points (AP), and the WC diagnostics images.

The following table identifies the software images that are part of Release 1.2.0.

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 external download Image	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

The following table identifies the software images that are part of Release 1.1.0.

Software Image Files Released with Release 1.1.0

Component	File Name	File Size (bytes)
WC8180 Image	wc8180_1.1.0.133s.img	49,513,064
WC8180 Diagnostics	wc8180_1.0.2.0_diag.bin	3,152,332
AP8120/AP8120-E External Download Image	AP8120-Upgrade_1_1_0_133.tar	8,734,720
WMS Windows 32Bit	WLAN8100_WMS_1.1.0.133_Windows_32bit .exe	195,070,151
WMS Windows 64Bit	WLAN8100_WMS_1.1.0.133_Windows_64bit .exe	195,071,771

Component	File Name	File Size (bytes)
WMS Linux	WLAN8100_WMS_1.1.0.133_Linux.bin	230,525,556

Important:

You must upgrade the WC 8180 diagnostics Image to version 1.0.2.0 after upgrading the WC 8180 to version 1.1.0 or 1.2.0 software.

Important:

Before you upgrade the Wireless Controller (WC) and Access Points (AP) to Release 1.2.0 software, you must first upgrade the WMS to Release 1.2.0. WMS Rel 1.0.x and 1.1.x versions do not support the WC and APs running Release 1.2.0 software.

Note:

Do not connect AP 8120-O APs to the network until you have upgraded the WMS and WC images to Release 1.2.0.

Note:

The AP 8120-O only supports the external AP image upgrade, which requires that you configure a Web server. Unlike the upgrade process for the AP 8120 and the AP 8120 with External Antenna, you cannot upgrade the AP 8120-O from the AP image stored on the WC.

Upgrading the Wireless LAN Management System to Release 1.2.0 software

About this task

You can use the Wireless LAN Management System (WMS) Release 1.2.0 to manage mobility domains with wireless controllers (WC) running Release 1.2.0 or Release 1.1.x. WMS Release 1.2 cannot manage Mobility Domains with WCs or Access Points (AP) running Release 1.0.x software.

Before you proceed with the upgrade, you must back up the SMX files, license files, and the database. On the WMS server, you can find the license files and SMX files in the following folders:

- <wms-install-folder>\smx-repository
- <wms-install-folder>\lsm\licenses

You can take the database backup from the WMS application itself. From the Navigation menu in the WMS interface, go to **Administration**, **Database Backup**, **Backup**.

Complete the following procedure to upgrade the WMS to Release 1.2.0. You must have Admin privileges (administrator on Windows and root on Linux) to upgrade the WMS

Procedure

1. Download the latest version of the WMS application from Avaya Support Portal at http://support.avaya.com/css/appmanager/public/support/Downloads/P0615
2. Launch the WMS executable file.
3. Select **Language**.
4. Click **OK**.
5. In the Installation screen, click **Next**.
   The installer detects that WMS is already installed on the computer.
6. In the pop up screen, click **Upgrade**.
   The WMS automatically backs up the required license files, database files, and SMX files if available, and automatically uninstalls the existing WMS installation. Depending on the database size, the uninstall process can take several minutes. Wait for WMS Uninstallation Successful pop up screen to appear.
7. In the WMS Uninstallation Successful pop up screen, click **OK**.
8. Choose the installation path in the field provided.
   If you do not choose WMS installation folder for the installation path, the default path is used. Avaya recommends that you use the default folder.
9. Click **Next**.
10. WMS installs a version of MySQL Server to support database operations.

    Note:

    If an instance of MySQL Server already exists on the installation server, and you want to use this instance, enter the details. You can use an existing version of MySQL but it is not recommended. Leave the **Use existing MySQL** server check box unselected unless you are an advanced MySQL administrator.

    If MySQL Server does not exist on the server, or if you are unsure of an existing installation, click **Next** to allow WMS do a clean installation of MySQL Server.
11. Under WMS Port Configuration, select the ports to be used by the WMS Server for different operations.

    Note:

    Avaya recommends using the default port configuration unless the ports conflict with any other application.
12. Click **Next**.

    Note:

    The WMS installer can detect if there are any conflicts between the ports it uses by default and those already in use on the server. If conflicts exist, you are prompted to enter new port values.
13. You can choose to install the optional Guest Portal Application.

Note:

The Guest Portal Application is a trial application that can help you configure and manage the Local User Database for Captive Portal Authentication if required. This is currently an unsupported application.

14. Review the installation options you selected.
15. Click **Install** to proceed with WMS Installation

    Wait for the Install Complete screen to appear.
16. Review the installation status message to ensure that the installation is successful.
17. Click **Done**.

    You can now launch the WMS through your Web browser.
18. Verify the WMS upgrade:
    1. Verify that all the domains are visible and can be monitored through the WMS.
    2. Verify that the license file is restored. In the WMS browser, the bottom bar should display the number of licenses installed —> **Licensed to monitor [xx] APs**.
    3. If Site View is configured, verify that the SMX files are restored. Click **Monitoring**, **Site Views**, **Site Model**. Highlight the SMX file to be activated, then click **Activate**.

Upgrading the Wireless Controller image

In a multiple controller domain environment, Avaya recommends to upgrade the A-MDC , the B-MDC, and then the peer controllers.

Complete the following procedure to perform an upgrade of the Wireless Controller (WC) image.

Procedure

1. **Back up the current configuration (Binary) to the TFTP server or USB drive**

   ```
   WC8180# copy config tftp address <tftp server address>
   filename <config file name to use>
   ```

   OR

   ```
   WC8180# copy config usb filename <config file name to use>
   ```
2. **Back up the ASCII configuration to the TFTP server or USB drive**

You are required to configure the ASCII if the current configuration has to be restored on a the WC controller running version 1.2.0. The Binary configuration saved with Releases 1.0.x or 1.1.x versions are not compatible with version 1.2.0.

```
WC8180# copy running-config tftp address <tftp server
address> filename <config file name to use>
```

OR

```
WC8180# copy running-config usb filename <config file name to
use>
```

3. **Download the 1.2.0 image to the WC**

   ```
   WC8180# download address <tftp server address> image <file
   name>
   ```

   The image download begins followed by saving the image to the system.

   The WC resets after the image download is complete.

   The total download and saving process can take approximately 15 to 20 minutes, depending on the network connection speed between the TFTP server and the WC. The WC reboot after the image download takes approximately 3 to 5 minutes.

4. **Repeat Steps 1 to 3 for all the WCs in the Mobility Domain.**

5. **Verify that the WC Image update is successful.**

   a. Verify that the WC booted with the correct image.

      `WC8180# show sys-info` > Verify that the software version is correct.

   b. Verify the wireless functionality.

      `WC8180# show wireless` > Verify that wireless is enabled.

      `WC8180# show wireless controller status` > Verify that on the AMDC, the Domain Role shows up as AMDC. Verify that the stored primary AP image version is showing the new image version 1.2.0.x.

      `WC8180# show wireless domain peer-controller status` > Verify that on AMDC, Peer Controller state is correct.

      `WC8180# show wireless ap status` > Verify that the APs that were managed prior to the upgrade are in a managed state.

      The time that it takes to have all the APs managed depends on the total number of APs in the network.

      Note: If you observe that the configuration is not restored after the image upgrade is complete, restore the configuration from the ASCII configuration saved during STEP 2.

      Note:

      Release 1.1.0 has a known limitation (wi00988841) in which the controller image download process does not program the controller or AP image correctly. You can verify for this issue by using the **`show wireless`** `controller status` command. This limitation is resolved in Release 1.2.0. **Workaround**: Repeat step 3 of the download process.

6. **Upgrade the Access Point image**

   ```
   WC8180# wireless domain ap image-update start
   ```

   The new AP image downloads to the managed access points based on the **`domain ap image-update download-group-size`**. After the image download is complete, the APs are reset based on the configuration of the **`domain ap image-update reset-group-size`**

   Note:

   The default download group size and reset group size of the image download is 5%. This results in 5% of the APs to download the image and reset per iteration. The process continues until all the managed APs in the domain are upgraded to the new AP image version.

7. **Verify that the AP Image upgrade is successful**

   `WC8180# show wireless ap status`> Verify that all the APs that were managed prior to the upgrade are in a managed state and the **Need Image Upgrade** flag is set to **No**.

   `WC8180# show wireless ap status detail`> Verify that the software version points to the new upgraded software image.

Upgrading the access point image from an external Web server

This section provides information about image upgrades for the access point (AP). This section also includes details on how to download and store multiple images on a configurable external Web server. For instructions on setting up Web services in Windows, see Setting up internet information services in the Windows operating system on page 51.

WLAN 8100 Releases 1.1.0 and above supports the AP image download from the external Web Server in addition to supporting the AP image download from the wireless controller for the AP 8120 and AP 8120 with External Antenna models. This feature is disabled by default and you must complete the required configuration to enable the external image download within the Mobility Domain. You must also synchronize the configuration to all the wireless controllers within the Mobility Domain.

If deploying only the AP 8120 and AP 8120 with External Antenna models in the network, then perform the AP image update directly from the image stored on the wireless controller.

If installing an AP 8120-O in the network, then configure all the APs in the domain, including the AP 8120 and AP 8120 with External Antenna for upgrade using the external image download.

Important:

While the AP image update process is in-progress, executing an image update for another AP with the command

```
wireless ap image-update <mac>
```

results in an error. Wait for the AP image update to complete before initiating the image update for other APs.

Use the following procedure to upgrade the AP image from and external Web server.

You must configure the A-MDC as shown in the following procedure to configure the Mobility Domain for an external image download.

1. Configure the Web server IP address.

   ```
   WC8180(config-wireless)#domain ap image-update server-ip <IP address>
   ```

2. If the Web server is enabled on a port other than port 80, configure the port on the WC.

   ```
   WC8180(config-wireless)#domain ap image-update server-port <Port number>
   ```

3. Configure the AP image version and filename for each AP model in the domain, and make the image version active.

   ```
   WC8180(config-wireless)#domain ap image-update image
   WC8180(config-domain-ap-image)# model ap8120    1.2.0.075 filename <path/
   filename>
   WC8180(config-domain-ap-image)# model ap8120-E 1.2.0.075 filename <path/
   filename>
   WC8180(config-domain-ap-image)# model ap8120-O 1.2.0.075 filename <path/
   filename>
   WC8180(config-domain-ap-image)#model ap8120    1.2.0.075 active
   WC8180(config-domain-ap-image)#model ap8120-E 1.2.0.075 active
   WC8180(config-domain-ap-image)#model ap8120-O 1.2.0.075 active
   ```

   where

   1.2.0.075 is the version number of the new AP image

   path is the location of the AP image under the Web server home directory

   filename is the AP image file name that corresponds with the AP model

4. Enable External AP Image Download.

   ```
   WC8180(config-wireless)#domain ap image-update external-download
   ```

   Note:

   The AP 8120 and AP 8120 with External Antenna use the same image file. The AP 8120-O uses a different image file.

5. Complete a config-sync to push the configuration to all WCs in the domain.

   ```
   WC8180#wireless controller config-sync
   ```

6. Upgrade the AP image.

   ```
   WC8180# wireless domain ap image-update start
   ```

   The download to the APs initiates on the new AP image. When the image download is complete, the APs reset based on the configuration of the domain ap image-update reset-group-size.

7. Verify that the AP image upgrade is successful.

   ```
   WC8180# show wireless ap status
   ```

   Verify that all the APs that were managed prior to the upgrade are in a managed state and the Need Image Upgrade flag is set to **No**.

   ```
   WC8180# show wireless ap status detail
   ```

   Verify that the software version points to the new upgraded software image.

   Note:

   When using the external image update, the “need image upgrade” flag for the AP (under AP status) shows whenever an AP running image is different from the image version configured for the external image download. The CLI command **`show wireless ap status`** shows the flag “Image Upgrade needed = Yes” whenever a configuration contains the wrong version number, even if the AP has loaded the correct image.

Importing policies from the Wireless Controller into the WMS

After the Wireless Controller (WC) upgrade is complete, you must import policies into the WMS from the A-MDC in the Mobility Domain

Navigate to **WMS** > **Configuration** > right-click on **Mobility Domains** > select **Import Policies** and enter the management IP of the AMDC.

Chapter 5: Captive Portal browser compatibility

Captive Portal functionality is dependent on client devices and browsers. Although WLAN 8100 Captive Portal functionality is expected to work with most client devices and browsers, the following section describes the client platforms and browsers that are tested by Avaya in WLAN 8100 Release 1.2.

Note:

The WLAN 8100 Captive Portal functionality is dependent on the wireless client generating a HTTP or HTTPS request. If the client browser does not resolve the domain name, the client does not generate a HTTP/HTTPS request and the wireless clients do not receive the Captive Portal login page. In environments without a DNS server, the captive portal page does not display after upgrading and clients cannot connect to the captive portal network.

Note:

While using HTTPS as the protocol for Captive Portal in Release 1.2, Firefox makes the captive portal inoperable. To fix this, delete any previous certificate from the client browser store and re-launch the browser for the Captive Portal to work.

If you have any issues with platforms or browsers not listed in this section, you must open a support ticket.

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

In addition to the platforms listed in the following table, the following platforms and browsers are also certified:

- Mac OS X 10.7 — Safari 5.1
- iPhone, iPod Touch, and iPad 2 — iOS 5.0 and 5.1
- Android 2.1 and 3.1

Windows operating systems and captive portal browsers support matrix

Applications	Windows operating system						
	2000	XP	XP-64 bit	Vista	Vista 64	7	7–64 bit
IE 6	Supp	Supp	Supp	X	X	X	X
IE 7	X	Supp	Supp	Supp	Supp	X	X
IE 8	X	Cert	Supp	Supp	Supp	Supp	Supp
IE 9	X	X	X	Cert	Cert	Cert	Cert
Firefox 3.X	Supp	Supp	Supp	Supp	Cert	Cert	Cert

Applications	Windows operating system						
	2000	**XP**	**XP-64 bit**	**Vista**	**Vista 64**	**7**	**7–64 bit**
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
Safari 3.0	Supp	Supp	Supp	Supp	Supp	Supp	Supp
Safari 4.0	Supp	Supp	Supp	Supp	Supp	Supp	Supp

Legend:

- Supported — supported in this release.
- Certified — supported and tested in this release.
- X— not applicable.

Chapter 6: Resolved Issues

The following table identifies previous known issues from software release 1.2 that are resolved in the current software release.

WI ID	Summary
Captive Portal	
wi00983298	Captive Portal Memory Leak observed in logout process while running Captive Portal stress tests with users logging in and logging out continuously resulting in Wireless Controller rebooting.
wi00980681	While using Captive Portal Authentication, WC 8180 crashes with "WCP critical - Out of memory" error in multiple customer environments.
wi00987957	Captive Portal users cannot be authenticated in some instances where Captive Portal Clients are roaming during authentication.
wi00966387	Captive Portal session is removed when wireless client gets disassociated from 802.11 network. This will require users to constantly enter user credentials on devices going into power save, like smart phones and tablets.
wi00971450	Short DHCP lease time impacts on Captive Portal session validation.
wi00973412	After Captive Portal user authentication, Captive Portal does not redirect the browser Web page to the URL the user had initially requested when redirect is enabled.
wi00986422	Wireless Controller reboots when assigning same CPIP for different Captive Portal profiles via WMS.
wi00985543	Wireless Controller acting as A-MDC went into a lock up state when trying to connect the Captive Portal client.
wi00982516	In some instances where multiple Captive Portal clients are trying to authenticate simultaneously via HTTPS protocol, SSL connection limit exceed message is observed on the client browser trying to authenticate. This will prevent Captive Portal clients from authenticating on the network.
wi00980668	In scenarios where the client is associated with an AP managed by the Wireless Controller, but Captive Portal Authentication is happening via the Captive Portal IP interface on a different WC, the client association information can be wrong, resulting in user authentication requests to fail.
wi00979085	In some instances, wireless clients trying to authenticate via the Captive Portal page cannot get the Captive Portal Authentication page due to memory leak in the Captive Portal login process and users cannot log on to the network.

WI ID	Summary
wi00977897	When multiple wireless clients are causing Captive Portal Login and Logout transactions at the same time, a WC 8180 deadlock condition is observed between different processes.
wi00992552	When a Factory Reset is performed on the WC 8180 and reconfigured for Captive Portal, the self-signed certificate generated for Captive Portal reuses the same certificate ID is before. It is observed that Client Devices using Firefox Browser (that were connected to this network via Captive Portal prior to factory reset) cannot authenticate via Captive Portal due to Certificate Error. Firefox creates a security alert when it compares new certificate from the Wireless Controller and the stored certificate in the browser cache. This is due the certificates having the same serial number, same issuer but a different issued date. This will prevent a user to login via the captive-portal page.
wi00984819	Default captive portal profile locale settings are deleted when all the Captive Portal IP interfaces are deleted.
wi00984750	Captive Portal customization returning maxFileSizeExceded error for 5 MB file.
wi00983288	It is intermittently observed that the Captive Portal Login page is not downloaded completely, resulting in a check box not appearing on the Login page, etc preventing users from Captive Portal authentication.
wi00975782	After user authenticates via Captive Portal login, the browser Home button takes the user to the EDM page of the Wireless Controller.
wi00994690	In some instances Captive Portal IP configuration change is not updated on the APs managed by peer controllers until the APs are reset.
CLI	
wi00988921	CLI: Sometimes CLI "clear wireless ap statistics" command throwing an Error message.
wi00983306	The WC 8180 CLI incorrectly displays ap radio status as up and channel as 1 even when the radio is disabled or not configured in the AP Profile.
wi00983302	WC 8180 CLI incorrectly shows the radio status as up and when AP is not managed under "show wireless ap radio status" command.
wi00983292	CLI command "default captive-portal tftp-server " does not clear TFTP server entry as expected.
EDM	
wi00992574	From EDM, when the controller 5 GHz radio profile is only configured with DFS channels as eligible channels or the AP Static channel in the domain AP database is set to a DFS channel, the configuration is not applied correctly to the AP radios.
Wireless Controller	
wi00992376	WC 8180 Auto-RF algorithm incorrectly selects channels with low error rate to be reassigned.

WI ID	Summary
wi00985069	AP 8120 does not handle client inactivity properly when clients enter power-save mode frequently resulting in disassociating wireless clients unexpectedly.
wi00992177	It is observed that in some instances the WC 8180 reboots on issuing "show ip igmp router alert" command via the CLI.
wi00991627	The Wireless Controller does not age out Neighbor Clients per the configured/default age out time. This results in the Neighbor Client Database to grow up to 2 Million Entries in environments with high WLAN utilization. In these scenarios, the processing of these large neighbor reports from the Access Points could result in the controller having high CPU utilization and domain instability which could result in AP Failures. This fix ensures that Neighbor Client observed by the AP Radio are aged out in one hour.
wi00988841	Intermittently the AP image was not downloaded correctly to the controller during controller image download resulting in AP iImage upgrade failure after controller image upgrade.
wi00986092	In some instances, the Wireless Controller reboots while executing CLI cmd "show wireless client info".
wi00974228	Intermittently, broadcast packets are not forwarded by the radio resulting in ARP failure for Wireless Clients.
wi00984576	Wireless Controller config-sync fails when an entry in Blacklist is moved to Whitelist. However when a new entry is manually added to the whitelist, and config-sync is performed, configuration is synchronized for both entries across all controllers correctly.
wi00975025	Enabling SSH secure mode on the WC 8180 forcefully disables SNMP/TELNET/HTTP.
wi00896043	Enhancement to increase total number of Whitelist and Blacklist MAC address list from 1k to 4k.
wi00942973	RADIUS VLAN attribute does not work correctly with Juniper SBR server.
wi00576008	Enhancement to support WPA Hex key type for wpaPersonal security mode.
wi00908407	Client with dual band radio cards keep hopping between AP radios. Sometimes they end up in associated state without any data-path connection.
wi00961676	Enhancement to retain AP licenses on factory or partial boot. To remove the license file use the command "clear license".
wi00994042	When wireless clients are connected to the AP for extended duration, clients go through WPA2 Re Key process. When multiple clients go through re-key process at the same time, intermittent AP resets were observed.
wi00998524	It is observed that AP 8120 resets when hit by broadcast storm on the AP subnet, where large amount of non wireless traffic is flooded to the AP Ethernet port.
Wireless LAN Management System	
wi00991177	WMS does not update controller status correctly when A-MDC fails in the mobility domain and the B-MDC transitions to become the A-MDC. This can result in

WI ID	Summary
	monitoring dashboards to display incomplete information as well as to apply policies to fail after configuration changes.
wi00989813	Cannot log in to WMS client even when valid correct credentials are used after installation in some environments.
wi00980425	WMS Monitoring -> RF map incorrectly shows the AP as ‘up’ even when AP is in failed state and the controller and WMS monitoring views shows the same AP as ‘down’.
wi00993543	Captive Portal clients are not displayed in Captive Portal Profile Dashboard under **Monitoring** -> **Mobility Domain** -> **Captive Portal** -> **Captive Portal Profile** -> **Captive Portal Profile Dashboard**.
wi00993531	WMS does not display avWlanElectedSelfAsActiveMDC and avWlanLostConnectionToBackupMDC Traps under **Monitoring** -> **Mobility Domain** -> **Alarms** when the A-MDC of the Mobility Domain fails and the B-MDC becomes the A-MDC.
wi00993509	WMS fails to display Traps generated by the A-MDC which transitioned from B-MDC to A-MDC due to original A-MDC failure.
wi00989816	WMS Mobility Domains Summary tab shows incorrect information for Managed APs and Clients after A-MDC failure.
wi00985518	WMS Expanded Navigation Trees close automatically when navigating between Monitoring and Configuration screens.
wi00984914	Captive Portal clients are not displayed correctly under **Monitoring** -> **Mobility Domain** -> **Captive Portal Screens**.
wi00984882	Captive Portal IP addresses are not displayed correctly under **Monitoring** -> **Mobility Domain Summary** -> **Mobility Domain Dashboard** screen.
wi00984644	Cannot configure APs for static channels using WMS under **Configuration** -> **Mobility Domain** -> **Devices** -> **APs** -> **Edit AP** -> **Radio Tab**.
wi00984610	When Wireless Controllers are configured with System IP and Management IP to be the same IP interface, the WMS cannot display monitoring data.
wi00983296	Captive Portal client entry is not deleted in WMS **Monitoring** -> **Mobility Domain** -> **Captive Portal** screen, when a CP session is deleted due to session time expiring. The client is removed on the Wireless Controller correctly and is required to reauthenticate to get on the network.
wi00982769	WMS Mobility Domain dashboard does not display AP load balancing status Information under **Monitoring** -> **Mobility Domains Summary** -> **Mobility Domain Dashboard**.
wi00982393	WMS AP Dashboard does not display Neighbor AP and Neighbor Clients correctly under **Monitoring** -> **Mobility Domain** -> **APs** -> **Managed AP Dashboard**.

The following table identifies known issues from previous software releases that are resolved in current software release 1.2.

WI ID	Summary
Wireless Controller	
wi00900158	Intermittently, MDC Controller Password is reset to "None". When this happens, the controller will not be able to join or leave the domain. Issue is not easily reproducible. Workaround is to reconfigure the password on the controller by issuing the command “no controller mdc-capable” and then “controller mdc-capable” this command will ask to create a password for the domain.
Access Point	
N/A	
Captive Portal	
wi00927481	While using CP IP Interface Feature, Captive Portal Session is not cleared on the controller hosting the CP IP correctly when the Captive Portal Client is associated to an AP managed by a different Wireless Controller and the client disconnects. The session is deleted after the CP Client Idle Time out or Session Time out expires.
Security	
N/A	
WMS	
N/A	
Diffserv Policies	
N/A	
Traps/Syslog	
N/A	
CLI	
N/A	
E911	
N/A	
EDM	
N/A	

Chapter 7: Known Issues

The following table identifies known issues that are present in the current software release 1.2.

WI ID	Summary
AP 8120–O	
wi00990268	For AP 8120-O deployments in EU, due to Regulatory Restrictions, Non DFS Channels are not allowed on 5 GHz Radio. To prevent Regulatory violation of AP 8120-O until DFS Certification is complete, Radio 1 (5 GHz) cannot be enabled. However, in order to apply configuration correctly to the AP a Radio Profile has to be created for 5 GHz and applied to Radio 1 while creating the AP Profile.
wi00969067	Radio Profile created for AP 8120-O model should limit the maximum value of DTIM to 15, as supported by this AP Model.
CLI	
wi00992079	CLI command "show wireless radio-profile detail" incorrectly shows the maximum supported clients for the AP 8120-O radio as 200 instead of 127.
wi00989274	CLI command "show wireless security radius server" always shows the Accounting Server as Down even though the Accounting Server is operational. Radius Health Check feature is only available for RADIUS Authentications servers. Hence the status should be displayed as N/A for Radius Accounting server instead of displaying as down.
wi00988920	CLI command "show wireless ap radio status" and "show wireless ap status detail" show incorrect information with respect to radio status and client status for APs managed by the Peer controller when user disables Radios of the AP Profile associated with these APs and does a config-sync. The Peer controller managing the AP however shows that configuration is applied correctly. Display information is corrected if APs are reset.
wi00985512	CLI command "show wireless ap-profile" on 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.
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.
wi00898859	CLI Command "show wireless domain ap database country-code XX" can take a very long time based on the number of APs in the mobility domain - (about 7 min with 4K APs).
wi00600206	In some instances the CLI output for "show wireless domain peer-controller status" on AMDC displays wrong number of APs managed by the peer controllers. CLI command "show wireless ap status" gives the correct number of APs managed in

WI ID	Summary
	the domain on the AMDC and the command shows the number of APs managed by the switch on the peer controllers.
wi00928850	When you use the "Default" command in CLI to default the age-out parameters under "Security Wids" context, it sets the age-out value to 1440 mins instead of 24 mins.
EDM	
wi00973315	EDM does not allow to change the active state of an external AP image entry to true/false after the entry is created. It is recommended that you delete the entries and recreate the with the correct state.
Wireless Controller	
wi00961948	It is observed that iPad running Flare Application cannot interoperate with when TSPEC Video is enabled on the Radio Interface. It is recommended that you disable TSPEC Video on the Radio Profile. Use "no tspec acm-mode video" under radio profile configuration.
wi00993055	Wireless Controller incorrectly generates trap avwlanprefAltcontrollerreachedmaxcapacity when the AP tries to join the preferred controller, which is down.
wi00989364	Auto-RF Power Plan algorithm incorrectly proposes new power settings for the failed AP.
wi00985473	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.
wi01001300	When the Captive Portal is enabled or disabled on the network profile, the configuration is not being applied to the peer controllers and access points unless the captive-portal profile-id is reconfigured. **Workaround** Re-execute the command to configure the captive-portal profile-id when the captive portal setting is disabled and then enabled on the network profile.
wi01000743	Radius Attributes calling / called station ID not sent in RADIUS request by Wireless Controller during the Captive Portal user authentication via RADIUS.
wi00999744	After rebooting the WC 8180, the AP 8120-O configuration of an AP 8120-O profile for a specific country in the Domain AP database does not restore. This issue is not observed if the AP profiles have both the AP 8120 and AP 8120-O with a specific country.
wi01004165	When the Mobility Domain has Radio or AP Profiles created for the AP 8120-O with only one country code (default domain country code), the command **`show running configuration`** doesn't show the AP model in the Radio Profile / AP Profile details. When the ASCII configuration file is saved and configuration restored, the Radio Profile is then created for the AP model AP 8120 and can result in the AP 8120-O running in an unmanaged state. **Workaround**: Restore the configuration file using binary config files or manually edit the ASCII configuration file to include "ap-model ap8120-O" in the Radio Profile or AP profile creation command.

WI ID	Summary
Wireless LAN Management System	
wi00989816	It is observed that iPad running Flare Application cannot interoperate with when TSPEC Video is enabled on the Radio Interface. It is recommended to disable TSPEC Video on the Radio Profile. "no tspec acm-mode video" under radio profile configuration.
wi00993544	Captive Portal Network Status is not displayed under **Monitoring** -> **Mobility Domain** -> **Captive Portal** -> **Captive Portal Profile** -> **Profile Dashboard**. This is redundant with the Captive Portal Profile Status and has to be removed.
wi00993043	Sorting Entries in WMS Monitoring Tables does not sort the entire database. It sorts entries only the entries on a per page basis.
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.
wi00990270	AP Profile and Radio Profiles always have country code selected as US instead of matching the Country Code of the Mobility Domain. This requires users to explicitly choose the correct Country Code when creating the AP Profiles and Radio Profiles.
wi00990232	In some instances, while importing large database entries via CSV file (MAC DB, AP DB etc), it is observed that the WMS client browser window is stuck in the process of importing even after the entries are successfully imported into the database. Opening a new client window displays the correct information. Users are required to close the browser window that is stuck and open a new window.
wi00988365	High Wireless Controller Host CPU utilization is observed while using WMS to monitor Mobility Domain with more large number of Captive Portal clients. Issue observed with greater than 1000 Captive Portal users in the network.
wi00986863	WMS allows Diffserv classifiers to be deleted when they are being used in a Diffserv policy.
wi00985958	WMS Monitoring Dashboard tables cannot be resized making it extremely difficult to view contents of certain tables.
wi00984065	In some cases it is observed that WMS can take up to 30 seconds when retrieving Wireless clients entries from the controller.
wi00982011	When WMS is used as a Trap receiver, the WMS database can grow significantly large with more than 100 000 alarms, causing upgrade issues or issues deleting all these traps in the future. It is recommended that you acknowledge Traps frequently in order to keep the alarms database under 100 000 entries.
wi00981511	WMS Captive Portal tab has functionality missing to display Captive Portal session attributes, client actions, sorting, and filtering, etc.
wi00979482	Captive portal user count is not being updated correctly under **Monitoring** -> **Mobility Domain** -> **Captive Portal** tab.

WI ID	Summary
wi00974611	When the AP is incorrectly configured in the AP database (AP Model, Country Code, etc) and the AP remains in the Discovered AP Database, this AP is not displayed in the WMS under Discovered APs as shown in the CLI.
wi00971732	Radio Profile created via WMS, EDM, and ACLI uses different default value, i.e. 802.11 mode, channel bandwidth, eligible channel, DTIM.
wi00970620	Managed AP Dashboard under WMS does not display AP Radio Statistics. This information is only available via CLI.
wi00970614	It is observed that the SMD Applet is cached in some client machines and the cached version is launched even when launching from and upgraded WMS client. This can be checked by checking the version of the SMD application from the **About** tab of the application. If it does not match the WMS version, then clear the browser cache and relaunch the application.
wi00982446	Captive Portal users cannot be de-authenticated from the **Monitoring** -> **Mobility Domain** -> **Captive Portal** page. Clients can be de-authenticated from the Wireless Clients page only.
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.
wi00989348	When executing an AP image download or AP reset actions, the WMS displays action as successful when it sends the message to the controller, which could mislead users into thinking that the action was successful. Users must go back to monitoring tables to verify that the action was successful.
wi01000224	When a new Domain is created through the WMS, the merge report upon Apply Policies shows an invalid 5 GHz channel list of up to 216. To successfully use Apply Policies, the maximum channel list for 5 GHz radios are up to 165.
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.
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.

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

Wi Number	Description
Wireless Controller	

Wi Number	Description
wi00600170	802.1p Priority for non-IP Packets is not honored by the WC 8180 and treats them similar to non prioritized traffic. This issue is not observed for IP Packets and the 802.1p Priority is honored as expected.
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.
wi00896183	Jumbo frames ingressing from a Wireless Client do not get forwarded out to the Wired Network by the Wireless Controller.
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.
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.
wi00671088	In some instances when Peer Controllers come up after a reboot, they display config out-of-sync, however they have the correct configuration and are operating as expected. This is expected to be due to the ordering of certain configuration. **Workaround**: Manually executing a config-sync from the AMDC will resolve the out-of-sync state.
wi00909674	When the Wireless Controller is moved from one mobility domain to another, it is recommended to clean up the configuration on the Wireless Controller by doing defaulting the box configuration.
wi00904073	In some instances it was observed that the controller is stuck in Programming/Saving State during Image Download.
wi00909612	When restoring an ascii backup to a system, the restore fails when creating vlan. **Workaround**: Edit the ascii config file and remove the vlan, for example vlan 20, (the vlan already exists on the system) from the line. Or, restore using binary config if one is available.
Mobility Domain	
wi00575533	Due the limited number of non overlapping channels available on the 2.4GHz Band using channel bonding (40MHz mode) could result in connectivity issues for some of the older adaptors. **Workaround**: Avaya recommends to use 40MHz Mode on the 5GHz Radio and use 20MHz Mode on the 2.4GHz Radio on the AP.

Wi Number	Description
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.
wi00929515	AP Country Code consistency check with Default AP Profile Country Code while importing Domain AP Database entries from a CSV file.
Access Point	
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.
Captive Portal	
wi00891828	When Captive Portal IP Interfaces are deleted and re-created multiple times, wpsProcessCpIpUpdates or wdpmCpInterfaceSet Error Messages can be observed intermittently and the operation fails. Retrying the operation will be successful.
wi00928771	Configuration with non-default values set for Captive Portal HTTPS port and Max-Bandwidth change after upgrading from ver 1.0.x to ver 1.1.0. These values have to be reconfigured after the upgrade.
wi00904833	Wireless Controller System IP can be exposed to the Captive Portal user if System IP is used as the Captive Portal IP. The Captive Portal IP should be different from the Wireless Controller System IP.
wi00891116	In scenarios where Captive Portal Message strings are customized with longer than 254 characters, show running-config and copy running-config commands do not display/copy the customized strings correctly. This could cause an issue when configurations are restored using the saved ASCII configuration files. This will not impact Captive Portal Customization functionality in run time. **Workarounds**: The following Workarounds are available: 1) In case of restoring configuration on the same software release, restore the configuration from binary configuration file. 2) The configuration can also be restored through WMS 3) If the above two workarounds are not acceptable, Captive Portal customization via the Downloaded Locale File is recommended.
wi00906368	In scenarios where the Captive Portal Client fails to download the Captive Portal HTML File correctly, the Captive Portal Page displays some garbage characters.
wi00884585	Intermittently Captive Portal Sessions cannot be de-authenticated using the "wireless captive-portal client-deauthenticate captive-portal-profile <id>"

Wi Number	Description
	command. Use "wireless captive-portal client-deauthenticate network-profile <id>" to de-authenticate clients.
Security	
wi00576447	Wildcard entries are not supported for MAC Entries in the MAC Database on the WC 8180.
WMS	
wi00576035	WMS takes about 3 minutes to update the MDC Capable Flags if the value is modified via CLI.
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.
wi00664791	WMS with Internet Explorer 8 does not display policy names correctly in some instances as policy names appear to be overlapped.
wi00601329	Not able to monitor RF-Views in WMS when logging into WMS using the credentials for a Role - User.
wi00900592	WMS: Monitoring Clients in WMS does not work if http port on WC is non-default
wi00925454	Under WMS Monitoring Tabs, Sorting entries only sorts contents on the active page of the Tab instead of all the entries in the Tab.
wi00883059	Captive Portal Redirect URL configuration with "%" character is not accepted through WMS. **Workaround**: To configure URL with special characters use CLI or EDM.
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/re-installation.
wi00929392	**Workaround**: For Linux WMS installations: move the wms/lsm directory to a different location before installing the new version. The WMS installation process on Linux can fail if the wms/lsm directory is present during installation.
wi00664681	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.

Wi Number	Description
	Workaround: Applying the configuration a second time pushes the 40MHz configuration to the controller.
wi00929502	In WMS, setting an Image Version as Active (set to "True" under Domain Name (Right Click) and Edit Settings/AP Image Download for active filename) is not always applied to the controller. **Workaround**: Retrying the Apply Policies, pushes the configuration to the controller.
wi00929519	Rel 1.1 WMS saves Alarms Data to the backup SQL File. If there are a lot of Traps in the database at the time of backup, the SQL File size can become large (above 750MB) and restoration can take a long time (above 30 minutes) or fail in some instances.
wi00897369	Site Model Designer may not work correctly in non-US/English localized Windows. **Workaround**: Use a US/English localized O/S to launch SMD.
wi00908763	WMS RF Views do not take Cable Length for External Antenna AP into account when displaying coverage area in the floor plans.
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. "
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. **Workaround**: Avaya recommends not to sort the classifier table in WMS.
wi00925228	Intermittently Diffserv Policies applied to client via Radius Attributes are not applied correctly. **Workaround**: Diffserv policies created on the controller are applied as expected.
Traps/Syslog	
wi00576426	Trap message is not generated when a Wireless Client fails MAC Authentication.
wi00890955	The Wireless Controller fails to generate "avWlanAPDeniedAdmissionToMDNoLicense" and "avWlanAPUtilizationOverflow" trap as expected.
CLI	

Wi Number	Description
wi00576289	The CLI command "show wireless managed-switch" can display incorrect information for the number of clients and number of managed aps on the peer switch in some instances. **Workaround**: Please user CLI commands "show wireless controller status" and "show wireless domain peer-controller status"
wi00575490	The command output for "show wireless ap vap status" is different on AMDC and BMDC. On the BMDC and Peer Controllers the output only displays the VAPs that are configured. On AMDC the total number of VAPs that are allowed on the system are displayed however only the VAPs that are configured have a SSID. This is a display issue and does not impact the system behavior.
wi00600554	On WC8180, "show wireless client status" displays client IP address as 0.0.0.0 in some instances. The controller learns the client IP Address via IP Packets received from the associated client. In instances where the client does not send any IP packets after association or after the client roams to a new AP, the controller will not learn the Client IP address and 0.0.0.0 is displayed in this table.
wi00600799	Intermittently APs managed by the Peer Controllers are not displayed by the AMDC after all the controllers in the domain are reset. WMS and the CLI on Peer controllers will display the complete list of managed APs in this situation.
wi00600411	Clearing domain / controller statistics does not clear the Wireless Diffserv statistics. Stats get cleared when a client either disconnects or roams.
wi00600272	In some instances it is observed that CLI output for "show wireless security wids-wips rouge-ap-classification <mac>" gets stuck for about a minute before the display is complete and the command prompt is returned.
wi00876681	CLI: "show wireless client association controller" displays wrong info when client roams from AMDC to PWC .
wi00927048	In some instances BMDC Peer Controllers do not show accurate information for the number of AP's for AP Database and Known AP Database. The actual entries in the database are accurate.
wi00930198	CLI Command "show wireless captive-portal profile status" on AMDC displays incorrect "Auth User count" when CP clients are associated to Peer CP-IP address.
wi00930200	CLI: CP "Authenticated Users" count shows negative values
wi00928890	CLI: Inconsistent behaviour across CLI's for country code Case (lower upper)
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.

Wi Number	Description
wi00842513	E911 - Roaming traps are not sent to trap receiver during switch failure.
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.
wi00600540	TACACS+ Configuration is not available via EDM. Please use CLI for TACACS+ Configuration on the Wireless Controller.
wi00600416	EDM cannot be used to reset or update APs managed by the Peer Wireless Controllers. **Workaround**: Avaya recommends to use either the CLI or WMS to perform domain wide operations.
wi00600204	EDM displays Error message while configuring Radius Profile with type = accounting while adding a server with priority 1. The server is added successfully but EDM does not indicate that.
wi00600241	EDM does not allow AP Campus Field Configuration. **Workaround**: Use the CLI/WMS to configure this value (if required).
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.
wi00601390	EDM/Wireless/NetworkProfile/Edit Profile/Security Tab/Security Mode=wepStatic - The help information for key length is incorrectly displayed as 13 for ASCII and 26 for HEX. **Workaround**: The correct key length is 5 for ASCII and 10 for HEX.
wi00601370	EDM/Wireless/Security/WIDPS/RF Scan AP Tab shows Avaya AP OIDs as Unknown.

Appendix A: Upgrading the Wireless Controller Diagnostics image to Release 1.0.2

About this task

Use the following procedure to upgrade the Wireless Controller Diagnostics image to a Release 1.0.2 image.

When using the Diagnostics menu to upgrade a Diagnostics image on Wireless Controllers running Releases 1.1.0, 1.0.0, 1.0.1, or 1.0.2 code streams, refer to the instructions listed in the Diagnostics image upgrade document on the support portal.

> **Important:**
>
> You can upgrade the Diagnostics image using CLI only after the Wireless Controller is upgraded to the Release 1.1.0 image or higher.

Procedure

1. **`WC8180# download address <tftp server address> diag <diagnostics image name>`**

   The new diagnostics image downloads to the controller and reset the controller.

2. After the controller boots up, verify that the diagnostics image upgrade is successful

   `WC8180# show sys-info` > The firmware version should display the new image.

Appendix B: Downgrading the Wireless Controller

About this task

In situations where the WLAN 8100 network needs to be downgraded from 1.1.0 to any 1.0.0/1.0.1/1.0.2 Release, complete the following procedure.

> **Important:**
>
> The WC 8180 Rel 1.1 configuration file is not backward compatible with Rel 1.0 code streams and if used the configuration will default. This could result in loss of connectivity to the controller via Telnet/WMS/EDM.

> **Important:**
>
> When downgrading the wireless controller from 1.1 to 1.0.x, the AP 8120-E (with external antenna) is also downgraded but is recognized by the controller as AP 8120. When the controller is upgraded back to 1.1, this results in the APs to be unmanaged. To fix the unmanaged AP, complete the following:
>
> 1. Delete the corresponding AP Database entry for AP 8120-E.
> 2. Add the database back with the database as being AP 8120.
> 3. Upgrade the AP to Rel 1.1.
> 4. Reconfigure the database entries to AP 8120-E for the AP.
>
> and . At this time,

The administrator requires console access to the Wireless Controller to restore the controller configuration.

The administrator requires access to the License file. The License file stored on the controller will be deleted after downgrading and has to be re-installed.

If the configuration from the Controller running Release 1.1 needs to be saved, follow Step 1 and Step 2.

Procedure

1. **Backup the current configuration (Binary) to the TFTP server or USB drive.**

   ```
   WC8180# copy config tftp address <tftp server address> filename
   <config file name>
   ```

   OR

   ```
   WC8180# copy config usb filename <config file name>
   ```

2. **Backup the ASCII Configuration to the TFTP server or USB drive**

The ASCII configuration is required if the current configuration has to be restored on a WC controller running version 1.0.0, 1.0.1 or 1.0.2 software. The Binary configuration saved with 1.1.0 version will not be compatible with 1.0.0, 1.0.1 or 1.0.2 versions.

```
WC8180# copy running-config tftp address <tftp server address>
filename <config file name>
```

OR

```
WC8180# copy running-config usb filename <config file name>
```

3. **Reset the Wireless Controller to the default configuration**

   ```
   WC8180# boot default
   ```

   Ensure the partial default option is used to retain the management IP and Licenses on the controller.

4. **Download the 1.0.x image to the Wireless Controller if required**

   a. `WC8180# show boot image`

      Verify the 1.0.x image that is required for the downgrade is available on the controller. If it is not available, download the required image.

   b. `WC8180# download address< tftp server address> secondary < image file name>`

      The Wireless Controller resets to factory defaults after the controller boots up with the 1.0.x software image.

5. **Restore the configuration on the Wireless Controller**

   After the Controller is downgraded to the required software, connect to the controller and restore the configuration using the binary configuration file that was saved prior to upgrade to 1.1.0.

   a. **Option 1: Using the Binary configuration file saved with the 1.0.x code stream**

      Loading the configuration from the USB:

      ```
      WC8180# copy usb config filename <file name>
      ```

      Loading the configuration from the TFTP server:

      Do the preliminary controller configuration to get connectivity to the TFTP server.

      Download the configuration from the TFTP server

      ```
      WC8180# copy tftp config address <TFTP Server IP> filename <file
      name>
      ```

   b. **Option 2: Using the ASCII configuration file saved with the 1.1.0 code stream**

      Loading the configuration from the USB:

      ```
      WC8180# configure usb filename <file name>
      ```

      Loading the configuration from the TFTP server:

      ```
      WC8180# configure network address <TFTP Server IP> filename <file
      name>
      ```

6. **Restore the License file on the Wireless Controller**

You must re-install the License file on the Wireless Controller after the image downgrade from software version 1.1.0 to 1.0.x . If the License file is not readily available, it can be downloaded from Avaya Licensing Portal.

a. Loading the License file from the USB

   `WC8180# copy usb license filename <License file name>`

b. Loading the License file from the TFTP server

   `WC8180# copy tftp license address <TFTP Server IP> filename <License file name>`

c. Resetting the Wireless Controller after installing the License file.

   `WC8180# boot`

7. **Repeat Steps 1 to 5 for all the Wireless Controllers in the Mobility Domain**.

8. **Verify that the Wireless Controller image downgrade is successful**

   a. Verify that the Controller has the correct image

      `WC8180# show sys-info` > Verify that the software version is correct.

   b. Verify the wireless functionality

      `WC8180# show wireless` > Verify that wireless is enabled

      `WC8180# show wireless controller status` > Verify that on AMDC, the Domain Role shows up as AMDC

      `WC8180# show wireless domain peer-controller status` > Verify that on AMDC, the Peer Controller state is correct.

      `WC8180# show wireless controller license-info` > Verify that the Licenses are loaded correctly.

      `WC8180# show wireless ap status` > Verify that the APs that were managed prior to the downgrade are in managed state.

      The time that takes to manage all the APs depends on the total number of APs in the network.

9. **Access Point image downgrade**

   `WC8180# wireless domain ap image-update start`

   This download initiates on the new AP Image to the Access Points. After the image download is complete, the APs will reset based on the of the **`domain ap image-update reset-group-size`** configuration.

10. **Verify that the AP image downgrade is successful**

    `WC8180# show wireless ap status` > Verify that all the APs that were managed prior to the image update are in a managed state and the **Need Image Upgrade** flag is set to **No**.

    `WC8180# show wireless ap status detail` > Verify that the software version points to the new software image.

11. **Import policies from the Wireless Controller into the WMS**

After the Wireless Controller downgrade is complete, it is recommended to Import Policies into WMS from the AMDC in the Mobility Domain

Navigate to **WMS** > **Configuration** > **Mobility Domains** > **Import Policies** and enter the management IP of the AMDC.

Appendix C: A-MDC switchover detection on WMS

Switchover detection and WMS action

The WMS has a built in mechanism by which it polls the A-MDC and other domain controllers of each domain it manages. The polls take place at three-minute intervals to confirm that the current A-MDC is still in control of the domain. If there is any change of A-MDC in the domain due to any of the following scenarios then complete the following three steps in WMS to synchronize data from the new A-MDC.

Complete the following steps to synchronize data with the new A-MDC:

1. Collect all configuration data from the new A-MDC and overwrite the old configuration data.
2. Clear monitoring data from the database.
3. Use the scheduler to schedule the new A-MDC for routine data polling at an interval of 10 minutes.

Switchover scenarios

1. **A-MDC is not reachable from WMS**
    a. Reboot of the active A-MDC.
    b. A-MDC management communication link failure.
    c. Change of configuration on the A-MDC by CLI or EDM or, change in firewall policy of the customer's network resulting in the SNMP and HTTP ports being blocked.
2. **Permanent outage of A-MDC**
    a. RMA
    b. Prolong power outage
3. **Split Domain - Link down between A-MDC and B-MDC and both assumes A-MDC role**

Behavior of current solution

Monitoring data can show up after a maximum of 15 minutes, depending up on the size of the network and amount of data to be collected from the controller.

Workaround

It is recommended that you refresh the following screens by using the **Refresh from controller** button.

Note:

Ensure you list all monitoring screens by using the **Refresh from controller**, not by using the **Refresh from WMS Server** button. For traffic trending, in the Mobility Domain dash board there is no refresh button and therefore data is updated within 15 minutes of the new A-MDC being detected.

Details of detection mechanism for various scenarios and WMS action implications

1. **A-MDC is not reachable from WMS**

    a. Reboot of active A-MDC

    In case of a reboot of the A-MDC, the B-MDC becomes the A-MDC. The WMS polling routine will not get any response from the A-MDC if the A-MDC is still rebooting. Upon communication failure, the WMS queries peer controllers (including the B-MDC) one by one to see any of the peer controllers returns an A-MDC IP address that is different from that of the current A-MDC. If the WMS finds new A-MDC, then the WMS proceeds with the data synchronization steps.

    If the WMS doesn't find the new A-MDC, then the domain is still in flux and the WMS takes no action. Traps can still be seen on the **Monitoring, Alarm** screen. In the next cycle of polling, after three minutes, the WMS talks to the A-MDC. If by this time the A-MDC has recovered, then it provides a new A-MDC IP address to the WMS. The WMS proceeds with the data synchronization steps.

    If the A-MDC has not recovered, then the WMS queries peer controllers (including the B-MDC) to get information about the new A-MDC. If the WMS finds a new A-MDC, then it proceeds with the data synchronization steps. If the WMS does not find a new A-MDC, the cycle repeats every three minutes.

    b. A-MDC management communication link failure

    c. Change of configuration on the A-MDC by CLI or EDM or, change in firewall policy of the customer's network resulting in the SNMP and HTTP ports being blocked.

    In this scenario, the assumption is that the WMS was able to talk to the A-MDC but only the management link to the A-MDC has failed. or communication between the A-MDC and the WMS server has been blocked. This means that all peer controllers, as well as the B-MDC, are able to talk to the A-MDC but only the WMS is unable to talk to the A-MDC. The WMS continues to attempt to collect data from the A-MDC at every data polling interval of 10 minutes. At this point, no alarm is raised for this failure, however, you should continue to refer to *WLAN 8100 Troubleshooting* (NN47251–700).

2. **A-MDC is not reachable from the WMS**

    a. RMA

    b. Prolong power outage

    The detection steps are the same as 1 a

3. **Split domain – Link down between the A-MDC and the B-MDC, and both assume the A-MDC role**

    This is a transient situation in the domain and can happen if there is a communication failure between the A-MDC and the B-MDC. One example of this scenario is if the network switch connected to the A-MDC reboots. The WMS cannot talk to the A-MDC, and no action is taken. However, if the WMS cannot communicate with the A-MDC because of temporary network issues, but other peer controllers return the B-MDC as a new A-MDC, then the WMS assumes that an A-MDC switchover has taken place. The WMS proceeds with a data synchronization. However, in the next cycle of detection, if after the three–minute interval there is a resolution between the A-MDC and the B-MDC, then the WMS uses the latest A-MDC in the domain and continues with the data synchronization.

Appendix D: Internet Web services setup

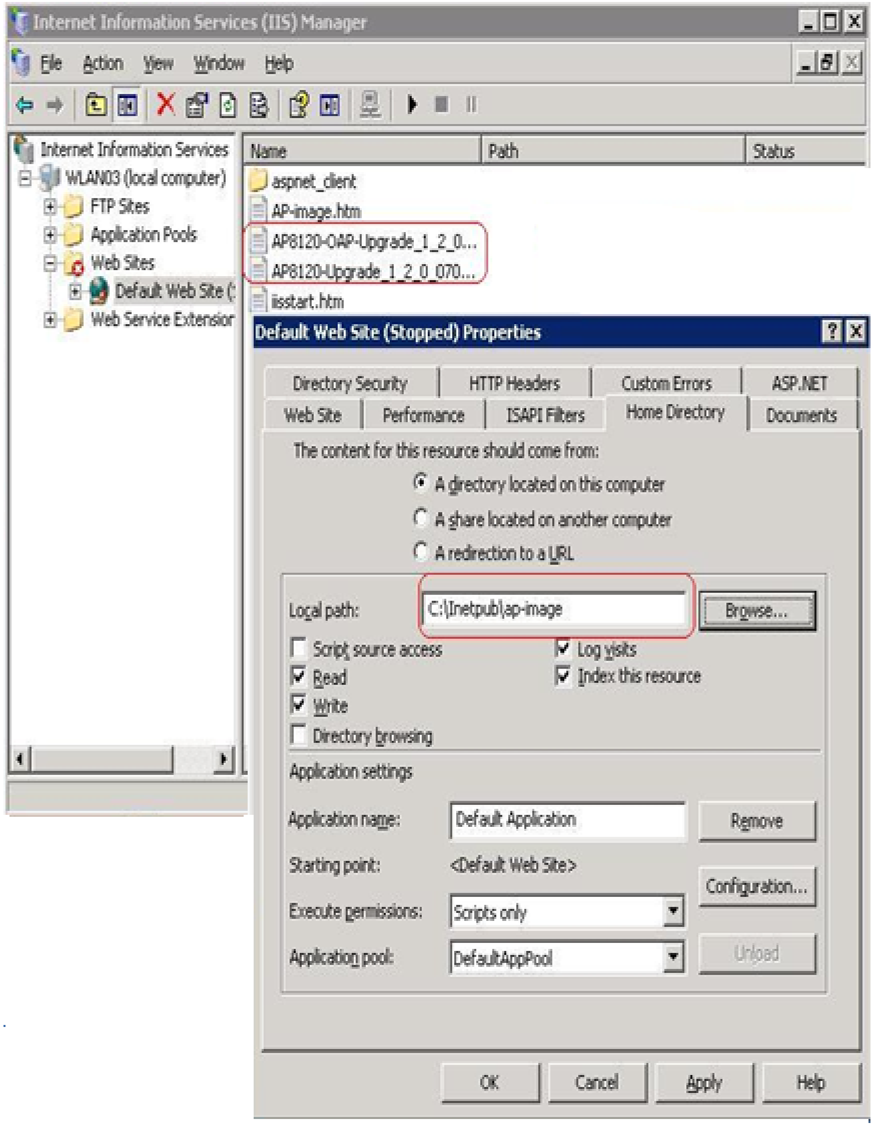
This chapter describes how to setup the Internet Information Web services on the Windows operating system.

Setting up internet information services in the Windows operating system

Use the following procedure to setup internet information services in the Windows operating system.

Procedure

1. On your PC navigate to: **Start, Programs, Administrative Tools, Internet Information Services**.
2. Copy the files from the new user created folder in **c:\Inetpub\ap-image. Ap-image**.
3. Browse the same folder in the local path field under the **Home Directory** tab. Enable the read and write permissions as shown in the following graphic.



aspnet_client
AP-image.htm
AP8120-OAP-Upgrade_1_2_0...
AP8120-Upgrade_1_2_0_070...
iisstart.htm

The content for this resource should come from:

● A directory located on this computer
○ A share located on another computer
○ A redirection to a URL

Local path: C:\Inetpub\ap-image

☐ Script source access
☑ Read
☑ Write
☐ Directory browsing
☑ Log visits
☑ Index this resource

Application settings

Application name: Default Application

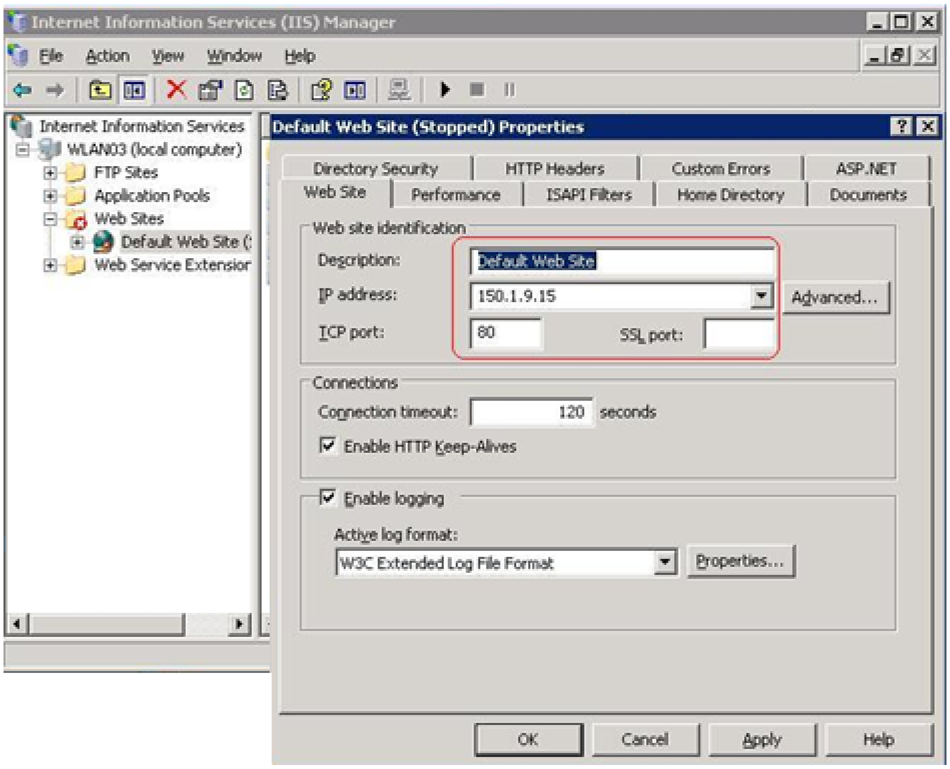
Starting point: <Default Web Site>

Execute permissions: Scripts only

Application pool: DefaultAppPool

Figure 1: Windows internet information services Home Directory tab

4. Select the **Web Site** tab and provide the IP address and TCP Port as shown in the following graphic.



Web site identification

Description: Default Web Site

IP address: 150.1.9.15

TCP port: 80 SSL port:

Connections

Connection timeout: 120 seconds

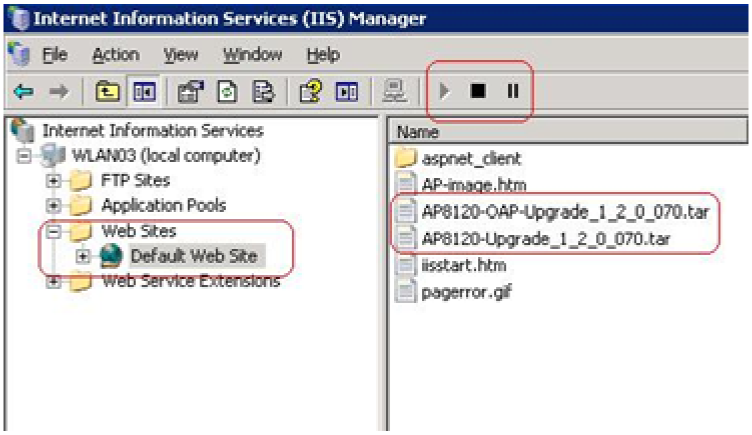
☑ Enable HTTP Keep-Alives

☑ Enable logging

Active log format: W3C Extended Log File Format

Figure 2: Windows internet information services Web Site tab

5. Click on the **task** button to run the task service and ensure that the IIS server is reachable from the wireless controller and the access point network.



aspnet_client

AP-image.htm

AP8120-OAP-Upgrade_1_2_0_070.tar

AP8120-Upgrade_1_2_0_070.tar

iisstart.htm

pagerror.gif

Figure 3: Windows internet information services task service