Avaya WLAN 8100 Release Notes

Release 2.0.1
NN47251-400
Issue 07.03
February 2013

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA 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”).

License types

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

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

Heritage Nortel Software

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

Copyright

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

Third Party Components

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

Preventing Toll Fraud

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

Avaya Toll Fraud Intervention

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Purpose of this document

This document provides the latest information on the Avaya WLAN 8100 product and documentation suites for release 2.0.1 as well as information on software upgrades.

It also provides a list of the known and resolved issues for release 2.0.1.

Chapter 2: New in this release

The following sections detail what's new in Avaya Wireless LAN (WLAN) 8100 for Release 2.0.1.

The **Features** section describes new features, and the **Other changes** section describes non-feature changes in Release 2.0.1 .

Features

See the following section for information about feature changes.

AeroScout support

The WLAN 8100 solution supports AeroScout enablement in an AP profile.

Important:

AeroScout enablement is supported only on indoor APs. It is not supported on the AP 8120–O, which is an outdoor AP.

The AeroScout Enterprise Visibility Solution is a third party solution that leverages standard wireless networks infrastructure to accurately locate any asset, and utilize that location to deliver direct benefits such as asset tracking, process automation, theft prevention and increased utilization. AeroScout Tags which are small, battery-powered devices are mounted on equipment or carried by personnel to deliver real-time location of the tracked asset or person. The messages transmitted by the AeroScout Tags are received by access points and are passed along with additional information (e.g. signal strength measurements) to the AeroScout Engine, a core component of the AeroScout visibility system, that calculates the accurate location of the Tag.

For more information, see *Avaya WLAN 8100 Fundamentals* (NN47251–102).

Other Changes

Software upgrade to release 2.0.1 is now supported. The upgrade workflows and procedures in this document are updated.

Chapter 3: Wireless LAN (WLAN) 8100 Upgrade

The following sections describe the high level workflow to upgrade a Wireless LAN (WLAN) 8100 solution to release 2.0.1. It also describes the supported upgrade paths to release 2.0.1.

Table 1: Supported upgrade paths — wireless controllers/APs

Upgrade path	Support
Upgrade 1.0.x to 2.0.1	Not supported
Upgrade 1.1.0 to 2.0.1	Not Supported
Upgrade 1.1.1 to 2.0.1	Supported
Upgrade 1.2.x to 2.0.1	Supported
Upgrade 2.0.0 to 2.0.1	Supported
Migration from 2.0.0 Overlay to 2.0.1 Unified Access	Supported
Migration from 2.0.1 Overlay to 2.0.1 Unified Access	Supported

The following table lists the support level for various installations and upgrade paths.

Table 2: Supported upgrade paths — WMS

Upgrade path	Support
1.0.x to 2.0.1	Requires an un-install followed by a WMS install
1.1.0 to 2.0.1	Requires an un-install followed by a WMS install
1.1.1 to 2.0.1	Upgrade supported
1.2.x to 2.0.1	Upgrade supported
2.0.0 to 2.0.1	Upgrade supported

Note:

When you un-install WMS and then install the current version (for example, when you upgrade from release 1.0.x or release 1.1.x or release 2.0.0 to release 2.0.1, ensure that you back up the license and SMX files during the un-install, and restore these files during the install. For the WMS database, after you perform the install, it is recommended that you import the mobility domains from the wireless controller.

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

Important:

General Upgrade considerations:

- If you are upgrading from release 1.0.x or release 1.1.0, you must first upgrade all the components of the WLAN 8100 (WMS, wireless controller and access points) to release 1.1.1 or release 1.2.x before you upgrade to release 2.0.1 software.
- After you upgrade to release 2.0.1, the release 2.0.1 wireless controller cannot manage access points operating on release 1.0.x or release 1.1.0 software versions. Therefore, you must first upgrade all access points to either release 1.1.1 or release 1.2.x software version before upgrading to release 2.0.1.
- To migrate to a Unified Access deployment, you must first upgrade your existing Overlay solution to either release 2.0.0 or to release 2.0.1.

  For example, if you currently have release 1.2.x of the WLAN 8100 Overlay solution, and you want to migrate the solution to the 2.0.1Unified Access, you must first upgrade to either release 2.0.0 Overlay or release 2.0.1 Overlay.

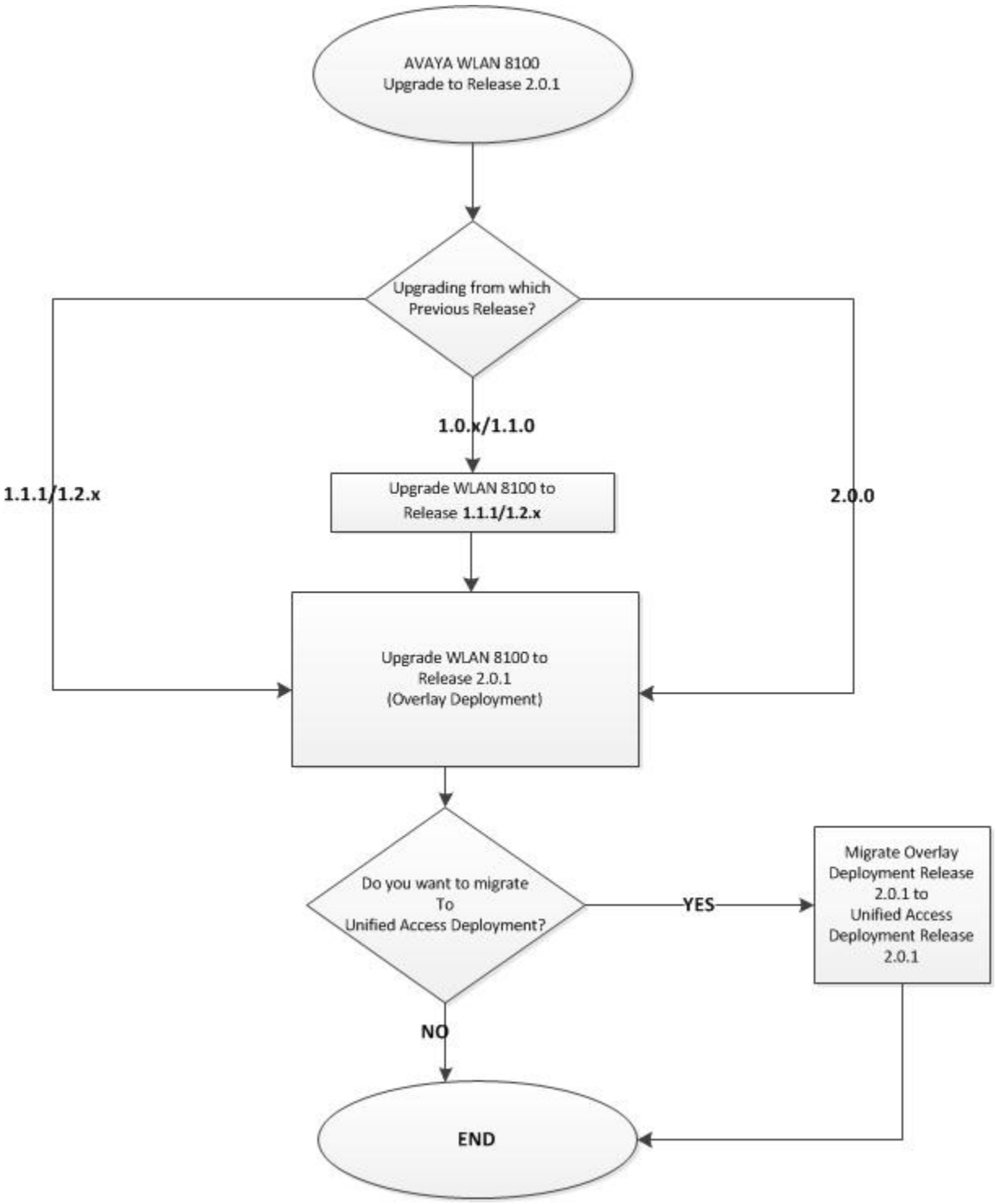


Figure 1: Upgrade WLAN 8100 to release 2.0.1 — workflow

Navigation

Note:

The following sections describe information and detailed procedures to upgrade the WLAN 8100 software to release 2.0.1. For information on software upgrade for prior releases, see the *Avaya WLAN 8100 Upgrade* (NN47251–402) for that release.

- Upgrade of WLAN 8100 to release 2.0.1 Overlay on page 15
- Migration of WLAN 8100 from Overlay to Unified Access on page 33

Chapter 4: Upgrade to Release 2.0.1 Overlay

Upgrade of WLAN 8100 to release 2.0.1 Overlay

The following sections contain information and detailed procedures to upgrade the WLAN 8100 software to release 2.0.1 for an Overlay deployment. It includes procedures to upgrade the Wireless LAN Management System (WMS), the wireless controller (WC), access points (AP), and the WC diagnostics image.

Important:

Before you upgrade the Wireless Controller (WC) and Access Points (AP) to Release 2.0.1 software, you must first upgrade the WMS to release 2.0.1.

WMS releases 1.0.x, 1.1.x, and 1.2.x do not support the WC and APs running on release 2.0.1 software.

Important:

You must upgrade the WC 8180 diagnostics Image to version 1.0.2.0 before upgrading the WC 8180 to version 2.0.1 software.

Note:

AP 8120–O considerations:

- Do not connect AP 8120-O APs to the network until you have upgraded the WMS and WC images to Release 1.2 and above.
- The AP 8120-O only supports 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.

  For more information on upgrading an AP image from an external Web server, see Upgrading an AP image from an external Web server on page 27.

Important:

WMS upgrade considerations:

- If you have release 1.1.1, release 1.2.x or release 2.0.0 of WMS installed, you can either perform a direct *upgrade* to release 2.0.1 WMS or perform a fresh install by uninstalling the previous version and installing the current version. A direct upgrade to WMS release 2.0.1 is supported only from releases 1.1.1, 1.2.x. or 2.0.0.

  For WMS releases older than 1.1.1, you must perform a fresh install.

- If you choose to uninstall the previous version and install the current version, you must perform a database backup.

  Ensure that you also backup the license files, logs and the Site Model files (`.smx` files), as applicable, when you uninstall WMS. Save these files to a location on your computer. Note down the path to the location of the files as you will be prompted to restore the license file during the install.

- If you are performing a WMS upgrade, the system automatically performs a backup of the license, logs, database and the `.smx` files at the following locations:

  - Database: `c:\wms-db_backup.sql`

  - Logs, licenses and `.smx` files: `c:\`

Software image files released with release 2.0.1

Table 3: Software image files released with release 2.0.1

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

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

Component	File Name	File Size (bytes)
AP8120/AP8120-E External Download Image	AP8120-Upgrade_1_1_0_133.tar	8,734,720
WMS Windows 32 Bit	WLAN8100_WMS_1.1.0.133_Windows_32bit.exe	195,070,151
WMS Windows 64 Bit	WLAN8100_WMS_1.1.0.133_Windows_64bit.exe	195,071,771
WMS Linux	WLAN8100_WMS_1.1.0.133_Linux.bin	230,525,556

Related topics:

Upgrade task flow on page 19
Upgrading the Wireless LAN Management System (WMS) to Release 2.0.1 on page 20
Upgrading the WC and AP images on page 23
Importing a mobility domain on page 26
Common upgrade procedures on page 27

Upgrade task flow

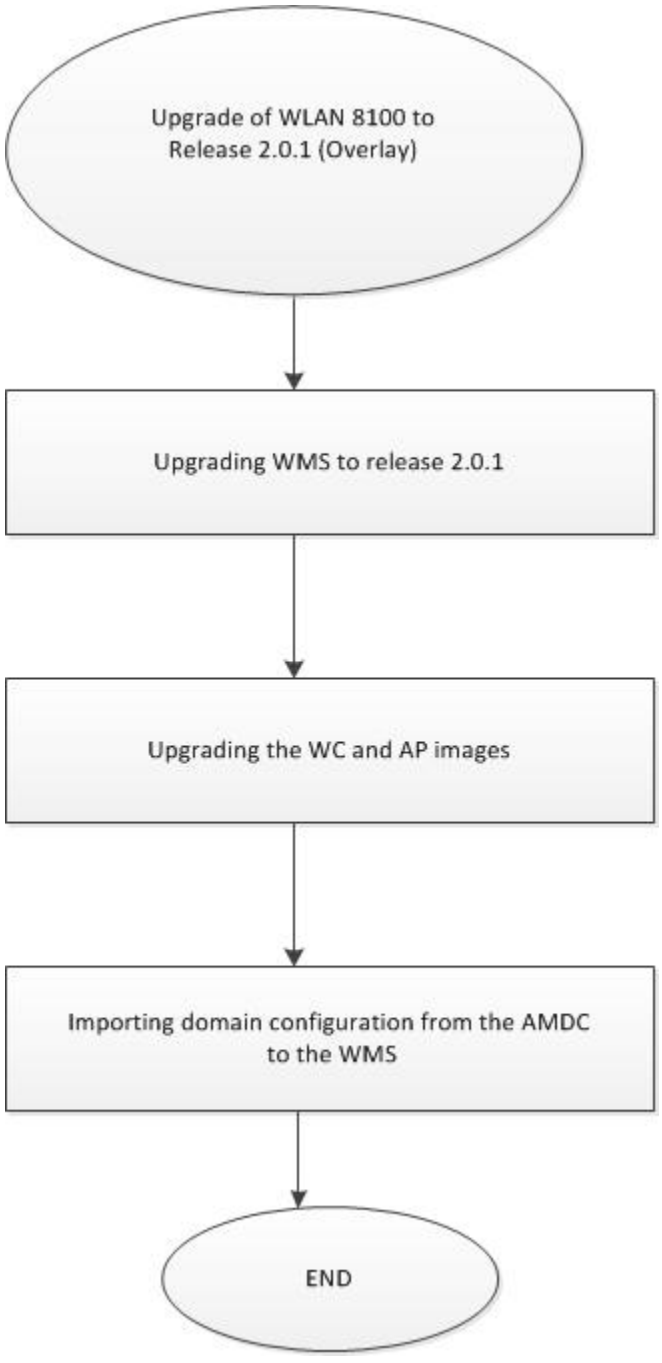


Figure 2: Upgrade WLAN 8100 to release 2.0.1 in Overlay deployment

Upgrading the Wireless LAN Management System (WMS) to Release 2.0.1

If you have a previous version of the WLAN Management System (WMS) installed on your computer, you can upgrade the software to release 2.0.1.

Use this procedure to upgrade the WMS to release 2.0.1. This procedure covers the steps as necessary to upgrade WMS on either the Windows and Linux platforms.

Note:

The WMS upgrade to release 2.0.1 is supported only from releases 1.1.1 or 1.2.x or 2.0.0.

Note:

You can use the WMS release 2.0.1 to manage mobility domains with wireless controllers (WC) running prior releases 1.1.0, 1.1.1 , 1.2.x or 2.0.0. However, the WMS release 2.0.1 cannot manage mobility domains with WCs (controllers) or Access Points (AP) running software release 1.0.x or 1.1.x.

Before you begin

- Ensure that you have administrative privileges on your computer to perform the upgrade.
- Download the latest version of the WMS application software from the Avaya Support site http://www.avaya.com/support.

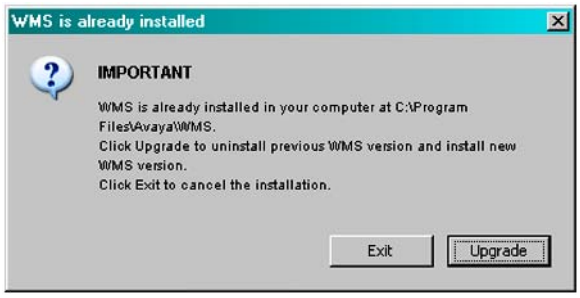
Procedure

1. Launch the WMS installer to begin the upgrade.
   - **On Linux**:

     For information on launching the WMS installer on a Linux platform, see Launching the WMS Installer on a Linux platform on page 22.
   - **On Windows**:

     Change directories to the location of the WMS installer and double-click to launch the installer.

   The WMS installer launches.
2. On the Installation screen, click **Next**.
   The installer detects that WMS is already installed on the computer and displays the following pop-up window.



3. Click **Upgrade**.
   The WMS automatically backs up the required license files, logs, 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 the **WMS Uninstallation Successful** pop up screen to appear. Click **OK**.
4. Click **Next**.
5. 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. It is recommended that you use the default folder.
6. Click **Next**.

   The **MySQL Server Details** window displays. The WMS installer uses the information on this window to install the MySQL Server to support database operations. The default version installed is `5.0.34` and the default server port is `3306`.

   - To retain these default values and proceed with the install, go to step 7.
   - If an instance of the MySQL Server exists on your computer, and you want to use this instance instead, update the fields as follows:

     ⚠ Caution:

     You must ensure that the version on your computer is the same as or later than the default MySQL Server version, for proper operation.

     - Select **Use Existing MySQL Server**
     - Enter the path to the location of the server in the field **MySQL Home**, or click **Choose...** to browse to that location.
     - Enter the server credentials in the **User Name** and **Password** fields.
     - Enter a port number in the **Server Port** field.

       ⚠ Caution:

       The server port must be the port used by the existing MySQL Server version.

If you do not know this port number, ensure that you choose a port that is different from the default server port (3306), so that any existing instance of the MySQL database on the server is not affected.

7. Click **Next**.
8. Under **WMS Port Configuration**, select the ports to be used by the WMS Server for different operations.

   You can choose to retain the default ports. The WMS installer detects 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.
9. Click **Next**.
10. Verify the pre-installation summary and click **Install**. The installation begins. Wait for the **Install Complete** screen to appear.
11. Review the installation status message to ensure that the installation is successful.
12. Click **Done**.
    You can now launch the WMS using your web browser.
13. Import the latest domain configuration from the AMDC of the domain. On the WMS, navigate to **Configuration**, **Mobility Domains**. Right click on **Mobility Domains** and select **Import Domain**. On the **Import Domain from Network** window, click **Import Domain**.
14. Verify the WMS upgrade:
    a. Verify that all the domains are visible and can be monitored through the WMS.
    b. Verify that the license file is restored. In the WMS browser, the bottom bar should display the number of licenses installed as **Licensed to monitor [xx] APs**.
    c. 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**.

Related topics:

Launching the WMS Installer on a Linux platform on page 22

Launching the WMS Installer on a Linux platform

Before you begin

Ensure that the WMS installer executable `WLAN8100_WMS_2.0.1.013_Linux.bin` is at the location `/opt/Avaya/WMS` on your computer.

Procedure

1. Navigate to the location of the WMS installer executable `WLAN8100_WMS_2.0.1.013_Linux.bin`.
2. Set execute permissions on the installer executable file. At the prompt, enter:

   ```
   chmod 777 WLAN8100_WMS_2.0.1.013_Linux.bin
   ```

   To verify permissions, enter:

   ```
   ls -l WLAN8100_WMS_2.0.1.013_Linux.bin
   ```

   Sample output:

   ```
   -rwxrwxrwx 1 root root 200470938 Sep 25 03:07
   WLAN8100_WMS_2.0.1.013_Linux.bin
   ```

3. Run the installer executable. At the prompt, enter:

   ```
   ./WLAN8100_WMS_2.0.1.013_Linux.bin
   ```

   Sample output:

   ```
   #./WLAN8100_WMS_2.0.1.013_Linux.bin
   Preparing to install...
   Extracting the JRE from the installer archive...
   Unpacking the JRE...
   Extracting the installation resources from the installer archive...
   Configuring the installer for this system's environment...

   Launching installer...
   ```

Upgrading the WC and AP images

Use this procedure to upgrade the Wireless Controller (WC) image and subsequently the AP image. Ensure that you read the upgrade procedure once before you begin the upgrade.

In a multiple controller domain environment, ensure that you upgrade the A-MDC first, then the B-MDC, and then the peer controllers.

Before you begin

- You must save a copy of both the binary and ASCII configuration files for the previous version.
- You must keep a copy of the previous binary configuration file (`config.cfg`) if you need to return to the previous version. The upgrade process automatically converts and saves the existing configuration file to a format that is compatible with the new software release. The new configuration file may not be backward compatible.
- Ensure that you have a knowledge of the APs that are currently managed by the WC. After the upgrade, you will need to verify that all APs managed by the controller prior to the upgrade continue to be managed after the upgrade.

Procedure

1. Back up the current configuration (Binary) to the TFTP server or a USB drive. Use one of the following commands:

   ```
   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. Use one of the following commands:

   Note:

   The ASCII configuration is required if the current configuration has to be restored on a WC controller running version 2.0.1. The Binary configuration saved with Releases 1.x..x versions are not compatible with version 2.0.1.

   ```
   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 2.0.1 image to the WC. Use the following command.

   ```
   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.

   Note:

   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 Step 1 to Step 4, 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.

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

   b. Verify the wireless functionality.

      Execute the command `WC8180# show wireless`. Verify that wireless is enabled.

Execute the command `WC8180# show wireless controller status`. Verify that on the AMDC, the Domain Role displays as Active MDC. Verify that the stored primary AP image version displays the new image version 2.0.1.x.

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

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

The time taken for all APs to reach a managed state depends on the total number of APs in the network.

Important:

If it is observed that the configuration is not restored after the image upgrade is complete, restore the configuration from the ASCII configuration saved during Step 2.

6. Upgrade the Access Point image. Execute the command `WC8180# wireless domain ap image-update start`.

   The download of the new AP Image starts on the managed Access Points.

   Important:

   The new AP image is downloaded to the managed APs only for the AP 8120 and the AP 8120 with External Antenna models. If your network consists of an AP 8120-O, then you must download the image for this AP from an external Web server. See Upgrading an AP image from an external Web server on page 27.

   After the image download is complete, the APs reset depending on the configuration of the `domain ap image-update reset-group-size <value>`, where `<value>` is the reset group size expressed as a %age.

   Note:

   The default `group size` and the `reset group size` for the image download is 5%. This implies that 5% of the APs 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 and subsequently reset.

7. Verify that the AP Image upgrade is successful.

   Execute the command `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**.

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

Importing a mobility domain

If a wireless network is configured using the CLI or EDM, you can import the mobility domain configuration into WMS from the Active Mobility Domain Controller (AMDC).

Before you begin

Ensure that you know the management IP address of the Active Mobility Domain Controller (AMDC) of your mobility domain.

About this task

Use this procedure to import mobility domain configuration into WMS from the AMDC.

Note:

After the import, mobility domain configuration in the WMS is entirely overwritten by the domain configuration from the AMDC.

Procedure

1. Log onto the WMS.
2. Navigate to **Configuration, Mobility Domains**.
3. Right click on **Mobility Domains** and select **Import Domain**.

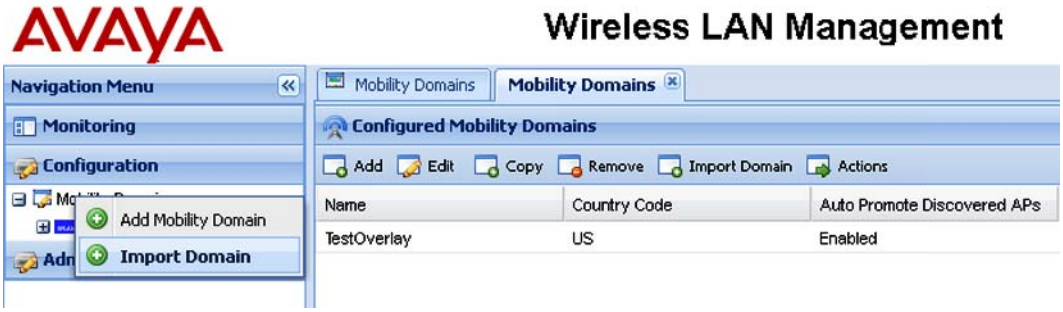
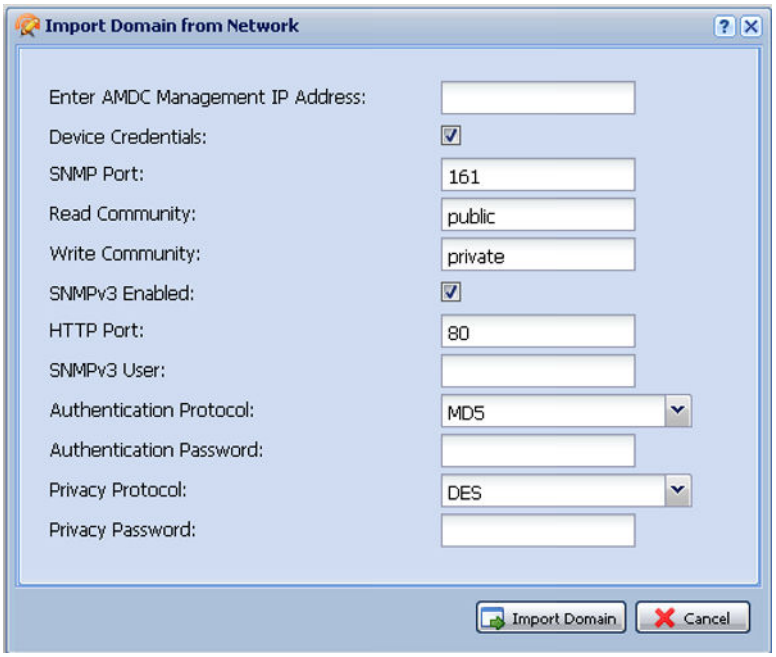


Figure 3: Importing a mobility domain

The **Import Domain from Network** window appears.



4. Enter the Management IP address of the AMDC.
5. Optionally select **Device Credentials** and **SNMPv3Enabled** to specify device credentials and SNMPv3 details before the import.
6. Click **Import Domain**.

Common upgrade procedures

The following sections describe common procedures used when upgrading the WLAN 8100 software.

Related topics:

Upgrading an AP image from an external Web server on page 27
Upgrading the Wireless Controller Diagnostics image to Release 1.0.2.0 on page 30

Upgrading an AP image from an external Web server

This procedure provides information on upgrading access point images downloaded from an external Web server. This section also includes details on how to download and store multiple images on a configurable external Web server.

WLAN 8100 releases 1.1.0 and later support AP image download from an external Web Server in addition to supporting the AP image download from the wireless controller, for the AP 8120 indoor and outdoor models.

Note:

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 configuration across all wireless controllers within the Mobility Domain.

Important:

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

If your network consists of an AP 8120-O, 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.

Use this procedure to upgrade the AP image from an 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.

   In the following example:

   `2.0.1.013` is the version number of the new AP image

   `c:/AP_Images/` is the path to the location of the AP image files on a Web server (running Windows OS).

   `AP8120-Upgrade_2_0_1_013.tar`, `AP8120_E-Upgrade_2_0_1_013.tar` and `AP8120-OAP-Upgrade_2_0_1_013.tar` are AP image files for the AP 8120, AP 8120–E and the AP 8120–O models respectively.

   ```
   WC8180(config-wireless)#domain ap image-update image
   WC8180(config-domain-ap-image)# model ap8120 2.0.1.013 filename c:/
   AP_Images/AP8120-Upgrade_2_0_1_013.tar
   WC8180(config-domain-ap-image)# model ap8120-E 2.0.1.013 filename c:/
   AP_Images/AP8120_E-Upgrade_2_0_1_013.tar
   WC8180(config-domain-ap-image)# model ap8120-O 2.0.1.013 filename c:/
   AP_Images/AP8120-OAP-Upgrade_2_0_1_013.tar
   WC8180(config-domain-ap-image)#model ap8120 2.0.1.013 active
   ```

```
WC8180(config-domain-ap-image)#model ap8120-E 2.0.1.013 active
WC8180(config-domain-ap-image)#model ap8120-O 2.0.1.013 active
```

4. Verify the AP image version and filename configuration. Ensure that the status of the image is active.

   A sample output is as follows.

```
WC8180#sh wireless domain ap image-update
External Download       : Disabled
Http Server IP Address  : 1.1.1.1
Http Server Port        : 80
------------------------------------------------------------------
Model      Version       Filename                          Active
-------- ---------- ----------------------------------------
ap8120    2.0.1.013      AP8120-Upgrade_2_0_1_013.tar     Yes
ap8120-E  2.0.1.013      AP8120_E-Upgrade_2_0_1_013.tar   Yes
ap8120-O  2.0.1.013      AP8120-OAP-Upgrade_2_0_1_013.tar Yes
------------------------------------------------------------------
```

5. 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.

6. Complete a configuration synchronization to push the configuration to all WCs in the domain.

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

7. 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.

8. 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 Wireless Controller Diagnostics image to Release 1.0.2.0

About this task

Wireless Controller (WC) software versions 1.0.0, 1.0.1, or 1.0.2 do not support a Diagnostics image upgrade from the CLI. Use the following procedure to upgrade the WC8180 Diagnostics image while running 1.0.0, 1.0.1, or 1.0.2 software on the Wireless Controller.

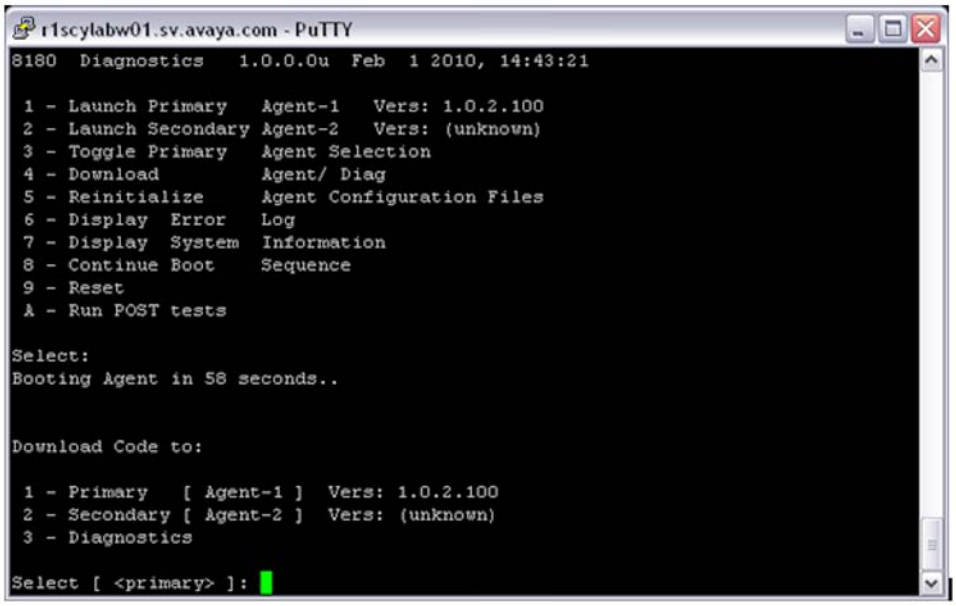
Wireless Controller software version supports the following procedure, as well as upgrading using the CLI download command.

Procedure

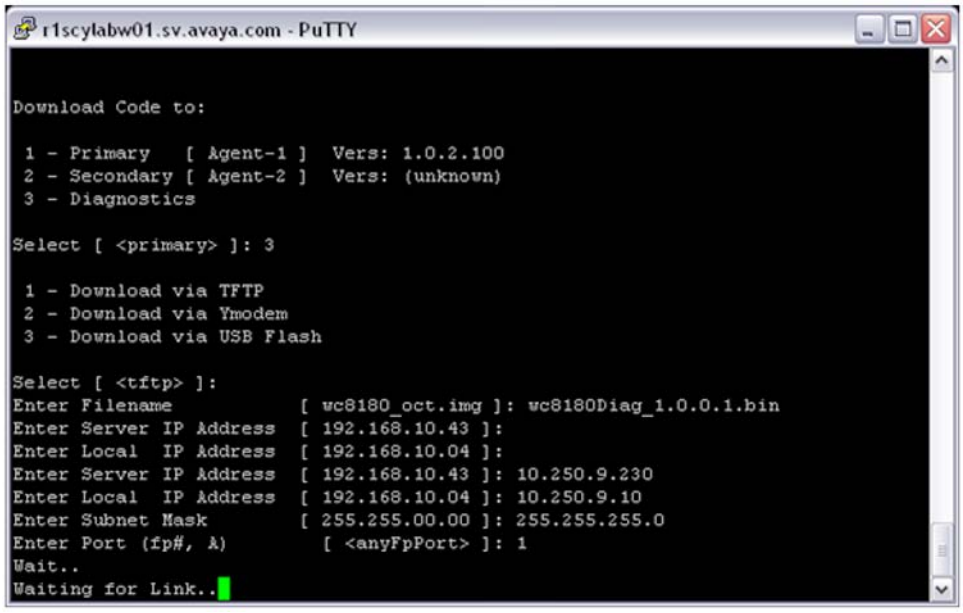
1. When the Wireless Controller is booting, type **<Ctrl + c>** to enter the Diagnostics menu.

   The following output appears:`>> Diag Break Recognized - Wait…`

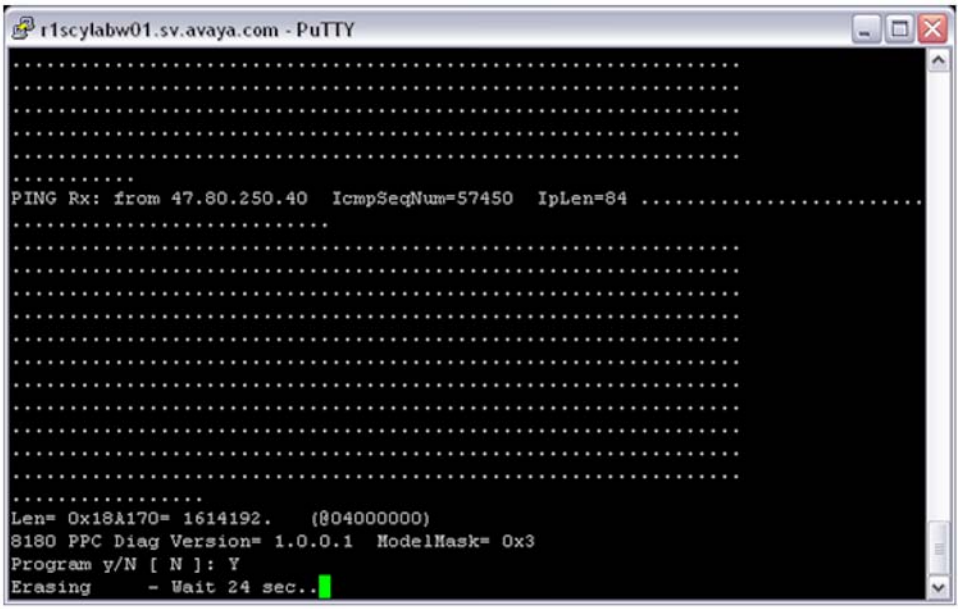
   The Diagnostics menu options appear as follows:



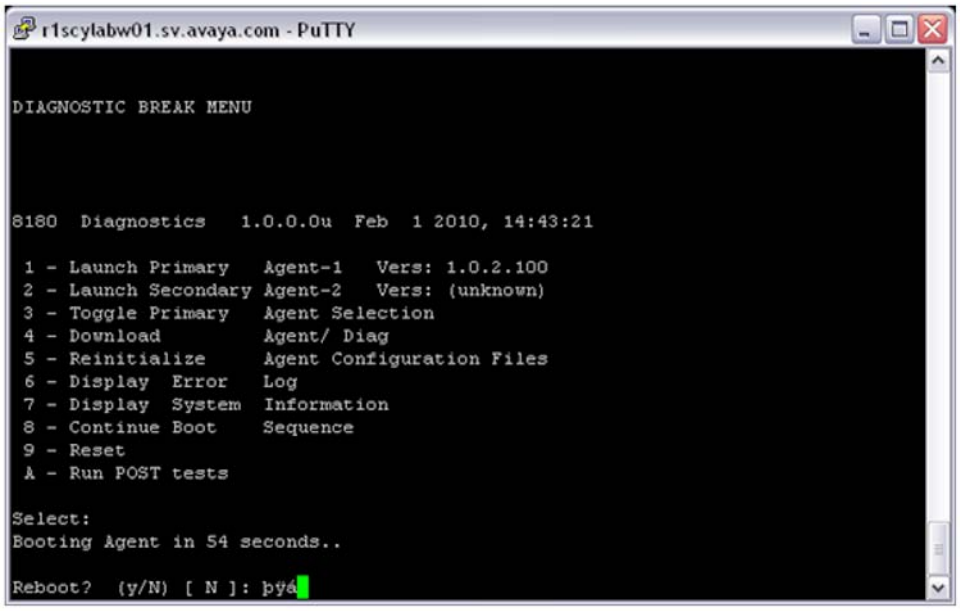
2. At the PPC Diagnostics menu, select option `4 – Download Agent/ Diag .`
3. Select option `3 – Diagnostics`.
4. Enter the required parameters as shown in the following figure.



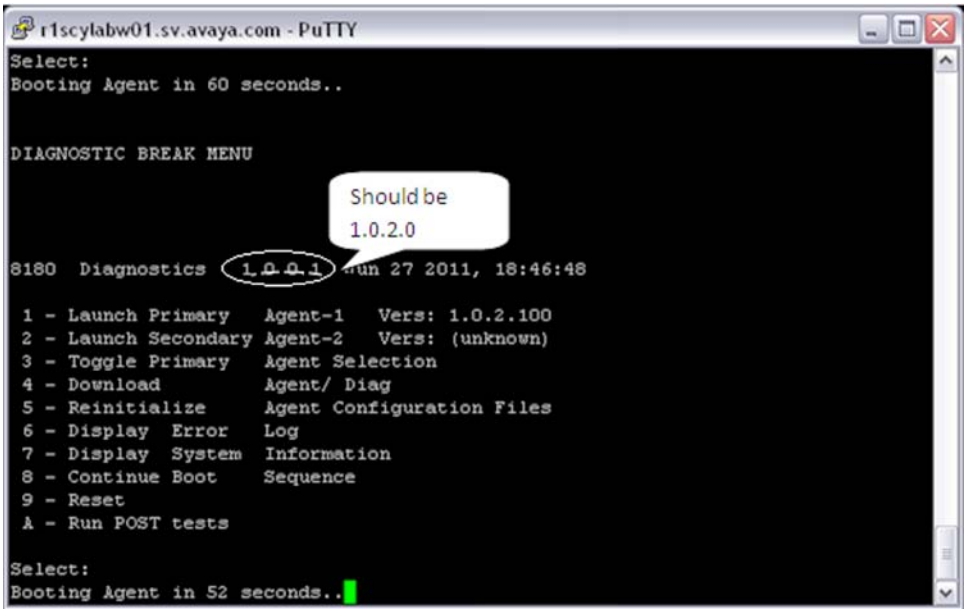
NOTE: `Enter Server IP Address` is the IP address of the TFTP server where the diagnostic image is located. `Enter Port (fp#, A)` option is the physical port connected to the network for TFTP access, this is optional.



5. At the prompt `Program y/N [n]:` type **Y** to program the downloaded diagnostics image to flash.
6. After the image is programmed into the box, the `DIAGNOSTIC BREAK MENU` appears again. Select option `9 - Reset` to reset the box.
7. When prompted to reboot, select **Y**.



8. When the box restarts, verify that the version of the Diagnostics image is 1.0.2.0.



Chapter 5: Migration from Overlay deployment to Unified Access deployment

Migration of WLAN 8100 from Overlay to Unified Access

If you are currently using the WC 8180 in an Overlay deployment and have an ERS 8600/8800 deployed in your core network, you can choose to migrate to the Avaya VENA Unified Access solution.

Note:

The WLAN 8100 release 2.0.1 supports the following migration paths:

- **Migration from release 2.0.0 Overlay to release 2.0.1 Unified Access**

  This can be achieved in one of the following ways:

  - Upgrade to release 2.0.1 Overlay first, and then migrate to release 2.0.1 Unified Access.
  - Migrate to release 2.0.0 Unified Access first, and then upgrade to release 2.0.1 Unified Access.

- **Migration from release 2.0.1 Overlay to release 2.0.1 Unified Access**

Fundamentally, the migration process requires you to disable wireless and change the operational mode of the WC 8180 controller to operate as a Wireless Control Point (WCP).

Important:

The operational mode is a configurable option available only from the ACLI.

Changing the operational mode is permitted only when the WC 8180 is in stand-alone state (not part of a domain), and wireless is disabled on that controller. After the operational mode is changed to WCP, the existing configuration on the controller is automatically converted for operation in Unified Access.

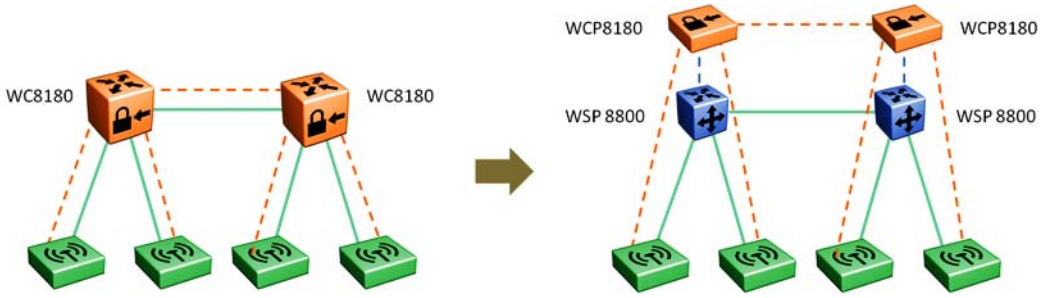
Important:

An operational mode change triggers a reboot of the controller.

The following figure shows an example of migration of a WC 8180 device from the Overlay deployment to the Unified Access deployment.

The ERS 8600/8800 devices in the network must have their software version upgraded to support wireless and the capability to act as wireless switching points (WSP) in the network. ERS 8600/8800 switches acting as WSPs in the mobility domain provide greater wireless data forwarding capacity than the WC 8180 devices. Additionally the WSPs must be added to the Domain WSP database on the WCP and conversely the WSPs must be configured with the corresponding WCP IP addresses.

Older versions of the APs (prior to Release 2.0.1) must become managed, following upgrade to this configuration. An administrator can then upgrade the AP images using internal or external image download methods supported by the WCP device.



The following sections describe the procedures to migrate a Wireless LAN (WLAN) 8100 solution in an Overlay deployment to the Avaya VENA Unified Access, for release 2.0.1.

Related topics:

Migration task flow on page 34
Configuring the ERS 8600/8800 to operate as a WSP on page 35
Configuring the WC 8180 to operate as a WCP on page 36
Verifying that the Unified Access domain is operational on page 38
Removing a mobility domain on page 39
Re-importing AMDC configuration changes to WMS on page 39

Migration task flow

The following task flow shows the required procedures to migrate the WLAN 8100 from Overlay to Unified Access.

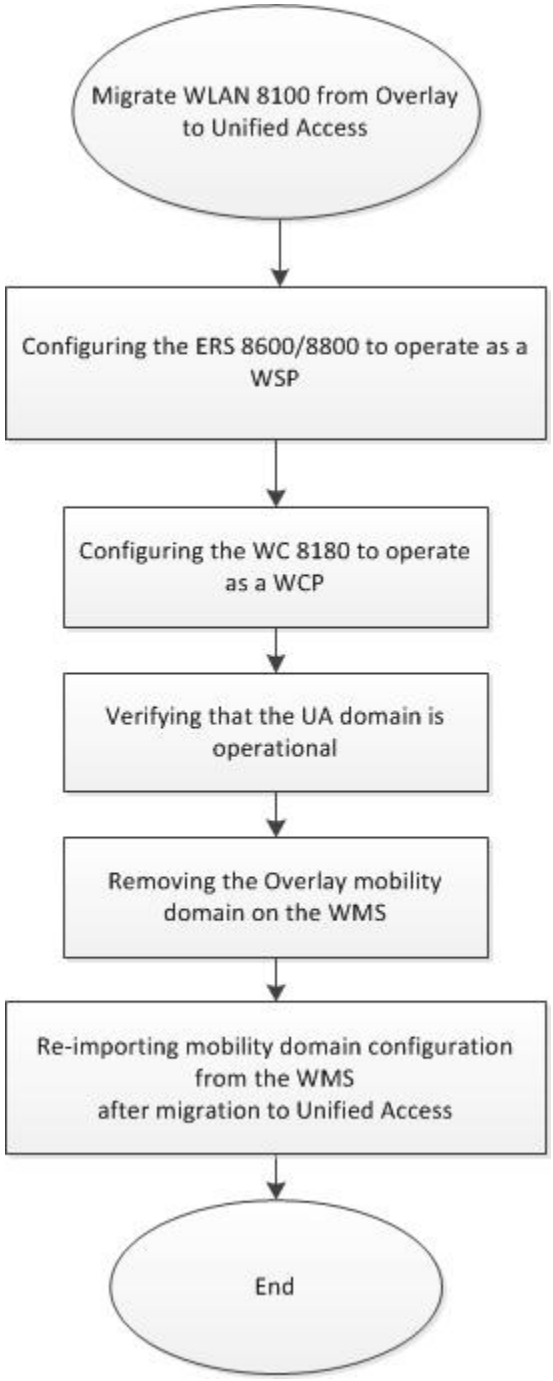


Figure 4: Migration of WLAN 8100 from Overlay to Unified Access

Configuring the ERS 8600/8800 to operate as a WSP

In Unified Access deployments, the Avaya Ethernet Routing Switch (ERS) 8800/8600 serves as the WSP. In this role, the WSP communicates with the WCP (wireless controller) to manage

the mobility context of a mobile client. This means that the WSP manages all user data from an AP onto the network. It terminates the access tunnel from an AP, decapsulates traffic, and inserts traffic onto the wired network. The WSP also maintains mobility tunnels with other WSPs (at the control of the WCP) to allow for user mobility across APs inside a mobility domain.

For information on how to configure the ERS 8600/8800 for operation as a WSP in the WLAN Unified Access solution, see WSP configuration using the ACLI on page 55.

Configuring the WC 8180 to operate as a WCP

Use this procedure to configure the WC 8180 controller to operate as a Wireless Control Point (WCP) in a Unified Access deployment.

Important:

You must perform this procedure on all controllers in the domain using the Avaya command line interface (ACLI). Ensure that you perform this procedure *first* on the AMDC of the mobility domain.

Before you begin

Ensure that the Avaya Ethernet Routing Switches (ERS) 8600/8800 are wireless-enabled and configured to act as Wireless Switching Points (WSP) in the WLAN mobility domain.

Procedure

1. Ensure that the controller is not part of a mobility domain.
   a. Enter the command `show wireless controller domain-membership`. Verify the `Domain Action Status`.

      In the following example, the `Domain Action Status` is `Join Success` indicating that the AMDC is a member of a mobility domain.

      ```
      WC8180(config)#show wireless controller domain-membership
        Domain Name             : Avaya
        Domain Role             : Active MDC
        Domain Action Status    : Join Success
        Action Failure Reason   : None
      ```

   b. Enter the command `wireless controller leave-domain`.

      Enter the domain secret when prompted.

      ```
      WC8180#wireless controller leave-domain
      Enter Domain Secret: ***********
      ```

   c. Verify that the controller is not a member of a mobility domain using the command `show wireless controller domain-membership`.
2. Disable wireless on the controller. Enter the following commands:

   ```
   WC8180# conf t
   WC8180(config)# wireless
   WC8180(config-wireless)#no enable
   ```

Verify that the controller is not wireless enabled using the command `show wireless`. Verify that the Status is `Disabled`.

3. Change the operation mode of the controller to WCP.

   Note:

   When you attempt to change the operation mode of the controller, you are prompted for a reboot. The operation mode of the controller changes to WCP only after the reboot.

   Enter the following commands. When prompted, enter `y` to reboot the controller.

```
WC8180# conf t
WC8180(config)# wireless
WC8180(config-wireless)#operation-mode wcp
  Operation mode change requires a reboot. Continue  (y/n) ? y
```

4. Enter the command `show wireless`. Verify that the status is `disabled` and the operation mode is `WCP`.

   A sample output is as follows. In this sample, the wireless system interface IP of the controller is assumed to be `20.20.20.45`.

```
WCP8180#show wireless
  Operation Mode    : WCP
  Status            : Disabled
  Interface IP      : 20.20.20.45
  TCP/UDP base port : 61000
  Base MAC Address  : 00:24:B5:1F:A8:00
```

5. Enable wireless on the controller. Enter the following command:

```
WC8180# conf t
WC8180(config)# wireless
WCP8180(config-wireless)#enable
```

6. Join the controller to the mobility domain.

   In the following example, you join the controller to a mobility domain named AVAYA.

   The Enter the domain secret when prompted.

```
WCP8180#wireless controller join-domain domain-name AVAYA mdc-address
20.20.20.45
Enter Domain Secret: *****
```

   Verify the join status.

```
WCP8180#show wireless controller domain-membership
Domain Name : AVAYA
Domain Role : Active MDC
Domain Action Status : Join Success
Action Failure Reason : None
WCP8180#
```

Verifying that the Unified Access domain is operational

Use this procedure to verify that the Unified Access domain is operational and the APs and the WSPs are in the managed state.

Before you begin

You have access to the Avaya command line interface (ACLI).

Procedure

1. Verify the operation mode of the AMDC of the domain. On the ACLI, execute the following commands.

   In the following example is the `10.5.60.5` is the Wireless or System interface IP address of the AMDC.

   ```
   WCP8180(config-wireless)#show wireless
   Operation Mode : WCP
   Status : Enabled
   Interface IP : 10.5.60.5
   TCP/UDP base port : 61000
   Base MAC Address : 2C:F4:C5:E9:B6:00
   ```

2. Use the following commands to display the status of the APs managed by the controller and other relevant information. Verify that all APs have a status of `Managed` to provide the configured wireless services.

   ```
   WCP8180#show wireless ap status
   Total APs: 2, Managed APs: 2, Failed APs: 0
   ------------------------------------------------------------------
   AP MAC     WCP IP   WSP IP    WCP     WSP    NeedImg
                             Status Status   Upgrade
   ----------------- -------------- ---------- -----------------
   00:1B:4F:6C:07:40 10.5.60.5 10.1.1.16 Managed Connected Yes
   00:1B:4F:6C:1F:80 10.5.60.5 10.1.1.17 Managed Connected Yes
   ------------------------------------------------------------------
   ```

3. Use the following commands to display the status of the WSPs managed by the controller.

   ```
   WCP8180#show wireless wsp status
   Status - Managed(Managed),PeerManagd(Peer Managed)
   Failed(Connection Failed),Disconcted(Disconnected), Unknown(Unknown)
   ------------------------------------------------------------
   Family  MAC               WSP IP    WCP IP    Status AP PeerWSP
   ------- ---------------- ---------- --------- -------------
   ERS8800 00:21:EA:BB:D0:00 10.1.1.16 10.5.60.5 Managed 1  1
   ERS8800 00:21:EA:BC:90:00 10.1.1.17 10.5.60.5 Managed 1  1
   ------------------------------------------------------------
   Status - Managed(Managed),PeerManagd(Peer Managed)
   Failed(Connection Failed),Disconcted(Disconnected), Unknown(Unknown)
   Total number of WSPs: 2
   ```

Removing a mobility domain

Use this procedure to remove a mobility domain, using the WMS.

Important:

Removing a mobility domain permanently removes the domain and all its configuration from the WMS database. You cannot retrieve the domain configuration once removed.

However, the configuration is removed only from the WMS database and does not affect the actual mobility domain or the controllers in that domain.

Procedure

1. Navigate to **Configuration**, **Mobility Domains**.
2. Select the mobility domain you want to remove and click **Remove**. You can also right-click the domain and select **Remove**.

   A confirmation dialog appears.
3. Click **Yes** to delete the domain.

Re-importing AMDC configuration changes to WMS

Use this procedure to re-import domain configuration from the AMDC into the WMS. Any difference in domain configuration between the WMS and the AMDC possibly due to configuration changes made by a user on the AMDC using either the CLI or the EDM, can be imported to the WMS using this procedure.

Note:

The WMS frequently monitors configuration on the AMDC and compares it with the configuration that was last imported from the AMDC. If a difference is detected, the **Re-import Configuration** button on the WMS is highlighted in orange color. The tool-tip on this button displays further information on the configuration mismatch that caused this indication.

Click the button to initiate re-import of AMDC configuration into the WMS.

Note:

The **Re-import configuration** button is available from all configuration windows on the WMS.

Procedure

1. Navigate to **Configuration**, **Mobility Domains**.
2. On the **Configured Mobility Domains** page, select a mobility domain that has the changes you want to push to the AMDC of the domain, and click **Re-import configuration**.

   The system verifies configuration differences between the AMDC and the WMS and displays a merge report as follows. The report displays details on what was changed on the AMDC, the differences in the existing configuration between the controller and the WMS, and the updates to WMS if the re-import happens successfully.

   The following sample report for domain **Avaya** displays configuration changes that were made on the AMDC using ACLI, in this case the creation of a new network profile **network_034**.

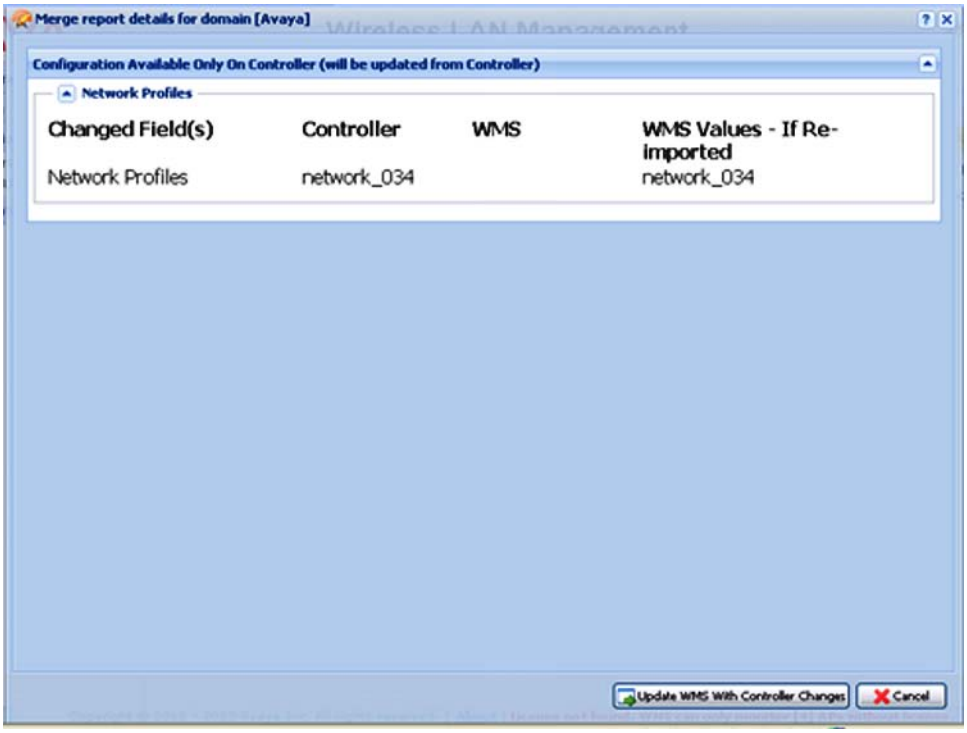


Figure 5: Sample merge report details for domain "Avaya"

3. Review the report and click **Update WMS with Controller changes**.

   The system displays a confirmation if the re-import is successful.

Chapter 6: Captive Portal browser compatibility

The Captive Portal functionality is dependent on client devices and browsers. Although the WLAN 8100 Captive Portal functionality works with most client devices and browsers, the following section describes the client platforms and browsers that are tested by Avaya for releases 1.2.x, 2.0.0 and 2.0.1.

Note:

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

Note:

In releases 1.2.x, 2.0.0 and 2.0.1, 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.

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.x, 2.0.0 and 2.0.1.

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

Applications	Windows operating system						
	2000	XP	XP-64 bit	Vista	Vista 64	7	7–64 bit
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
Safari 3.0	Supp	Supp	Supp	Supp	Supp	Supp	Supp
Safari 4.0	Supp	Supp	Supp	Supp	Supp	Supp	Supp
Safari 5.1.5	Supp	Supp	Supp	Supp	Supp	Supp	Supp
Chrome 20.0.1132.57 m	X	Supp	Supp	X	X	X	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 7: Resolved Issues

The following table identifies known issues from previous software releases that are resolved in software release 2.0.1.

WI ID	Summary
wi01048101	Captive Portal login page intermittently redirects to a blank page.
wi01057286	HTTPS protocol support in HTTP protocol mode.
wi01073972	The CP image name is not consistent following an image import (2.0.1.0).
wi01010308	Retrieving CP image using TFTP with 0.0.0.0 does not pull from all controllers.
CLI	
wi01060444	AP does not forward AeroScout tag packets to the positioning server after capture.
wi01060325	Deleting the default captive portal profile must not be allowed.
wi01059978	Session time sets to 0 when defaulting a captive portal profile.
wi01021459	8180 password security or Stack password.
EDM	
wi01059980	User logout is enabled and session time is 0 when creating Captive Portal profile using the EDM.
wi01051779	SNMP get value error for MIB elements in avWlanMobAgentVlanTable.
wi01024545	WPA-personal key disappears after controller reboots.
Wireless LAN Management System (WMS)	
wi01074887	When creating an AP-Profile using the WMS for the EU region, the 5 GHz radio is disabled for the AP 8120-O.
wi01074802	Certain Packet sizes were not being forwarded from the AP, which caused connection issues with a few applications on Ipad/Iphone.
wi01060155	When applying policies for AP profiles using the WMS, changes are detected between the controller and the WMS.
wi01017853	The WPA key from the network profile got truncated after a reboot.
wi01073973	The Captive Portal Block command sometimes goes into a pending state.
wi01059799	Unable to see the generated certificate in the WMS 2.0 with the controller running release 1.2.1.

WI ID	Summary
wi01047121	WMS CPU or Memory Graphs only display 2 days data on the landing page & the WC dashboard.
wi01035565	Channel and Power values should be displayed in a drop down box while setting them dynamically.
Access Point (AP)	
wi01064338	WMS channel changes for outdoor AP (AP 8120–O) and indoor (AP 8120–E).

Chapter 8: Known Issues

The following table identifies known issues that are present in the software release 2.0.1.

Work Item (WI) ID	Summary
CLI	
wi01035765	Not able to set default threshold value for `auth-fail` client threat.
wi01018263	UA: CLI incorrectly shows ERS800 software version as 1.0.0.0
wi01040703	Mac-address is displayed truncated in the error message while displaying the output for "show wireless security wids-wips rogue-ap-classification "
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.
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.
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.
EDM	
wi01035581	EDM:Changing the Active Field in External Image Upgrade option from True to False or false to True from EDM is not reflected in CLI.
wi01032856	EDM: Deleting random classifier blocks is not possible needs to be orderly deleted
wi01026911	EDM: Adding classifier blocks only in series, random add is not possible.

Work Item (WI) ID	Summary
wi01019753	EDM: 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.
WLAN Management System (WMS)	
wi00905407	When you install WMS on Windows 7 64-bit SP1, a warning pop-up window displays indicating that this version of Windows is not officially supported by this release of the WMS server. This issue is however not seen on Windows 7 32-bit SP1 or Windows Server 2008 SP2.
wi01043005	The controller dashboard Mobility VLAN count is shown `0` and entries are missing compared to the AMDC, when you have the same Mobility VLAN with a different case.
wi01041059	When a static DNS server address is configured on a network interface of the WMS server, HTTPS connection fails.
wi01037700	A BGN Radio Profile (US) created by the WMS has all channels checked as Eligible Channels which is incorrect. The Eligible Channel List for US is 1,6,11 for BGN radio for 20 Mhz.
wi01037989	Re-import of configuration fails when for any profiles or Mobility VLANs configured with the same name but with a different case.
wi01039775	When re-importing a domain, the client user groups which are configured under security context has the `Default` user group missing.
wi01040862	The **Security DB, Local Client DB** database supports a maximum of 1000 users, but you are able to add more than 1000 users using the WMS.
wi01040991	Backed up traps are not restored when you perform a WMS upgrade.
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.
wi01011696	WMS DB backup through the ADMIN tab isn't showing the backup file on the backup/restore page.
wi01017222	Incorrect status of APs when APs of two domains are plotted on the same SMX file are shown in RF views.
wi01004048	The Import policies fail and exception appears in the WMS logs after configuring the Ap-profile profile name as case sensitive.
wi00997374	The WSP Load balance portlet should be present in the Mobility Domain's dashboard.
wi01018671	The bulk edit option does not apply bulk edits for APs from filtered AP profiles but applies for all APs in APDB.
wi00986547	WMS does not support Remote Packet Capture feature.

Work Item (WI) ID	Summary
wi00991412	Certificate mapping data is pushed to peer controllers without `config-sync` through WMS.
Wireless Controller	
wi00981120	Station Isolation feature in release 2.0: When clients are connected to the same radio (Radio1 or Radio2) of an AP, clients will **not** ping or communicate with each other if station isolation is enabled. If the clients are connected to two Radios (Radio1 and Radio 2) on the same AP, even with station isolation enabled, the system **fails** to stop the clients from communicating with each other. Similarly, when clients are connected to different APs in a domain, even with station isolation enabled, the system **fails** to stop the clients from communicating with each other.
wi01042784	User configured values for `Dscp2cos, cos2dscp, wmm2cos, cos2wmm, egressmap` and `ingressmap` reset to default values after a reboot and an image upgrade.
wi00988412	When upgrading, or downgrading from 1.1.1 to 2.0.0, the AP image version on the controller fails to upgrade. Workaround: Upgrade the controller twice so that the AP image is properly downloaded and upgraded.
wi00992409	Sometimes, when connecting to a Captive Portal on a FireFox browser using HTTPS, you see the `SSL Connection Failed` message on the browser. To recover from this issue do the following: • Clear the certificate store. • Restart the browser.
wi01034431	When you upgrade from 1.2.0 to 2.0.0, some custom settings change to default values.
wi01041482	In release 2.0, the basic and supported data rates 1, 2 are disabled by default. You must specifically configure these data rates if required.
wi01015637	Unified Access: A Primary radius server failure causes radius deamon crash and restart when 360 veriwave clients are connected.
wi01015923	In a scaled eight controller domain with 12K clients, several WCs lose cluster connection but recover when one PWC reboots.
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.
wi01017586	Unified Access: osapiMessageSend failed messages is frequently seen when CP clients roam.
wi01018263	Unified Access: The ACLI incorrectly shows ERS software version as 1.0.0.0.

Work Item (WI) ID	Summary
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.
wi01023515	VLAN mgmt IP routing enabled after reboot.
wi01022494	When you enable Auto Promote in overlay, all the APs in AMDC Domain Discovery Table are redirected to BMDC.
wi01003928	The command **`show wireless captive-portal client statistics`** may show inconsistent data across controllers in certain situations.
wi01000513	`LVL7-Wireless-Client-Policy-Dn/Up` attributes are not applied on captive portal clients.
wi01041340	Able to enter the username, start date, and end date older than what the controller currently displays in CLI and EDM.
wi01040385	Bandwidth values set for a specific user/username changes on WC reboot.
wi01029655	Split Plane ACLI: AP is not able to get managed or load balanced when a WCP (having AP's 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.
wi00987931	When a valid radio profile is not mapped within AP profile, AP get stuck at `Apply In Progress` status.
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.
wi01031743	WIDPS: In a domain where AP belongs to multiple countries, AMDC has incorrectly classified Managed AP as rogue AP.
wi01039137	Some APs may pick channel 2 instead of channel 1 due to a known issue. A corresponding log message is generated.
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.

Work Item (WI) ID	Summary
wi01015710	The AP 8120-O (Outdoor AP) radio supports a maximum of 124 CCMP enabled clients or a maximum of 62 TKIP enabled clients.
wi00928771	Configuration of the Captive Portal Max-Bandwidth parameter (with non-default values) changes when you upgrade from release 1.0.x to release 2.0.0.
wi01020470	Captive Portal does not work when a Wireless or System interface has the `Management` flag enabled.
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.
Traps	
wi01036892	The logs `avWlanLostConnectionToBackupMDC` and `avWlanElectedSelfAsBackupMDC` are not generated in syslogs, but the traps are generated for the same.
wi01018960	With topology change events, STP (L2) related traps are seen in WMS Alarms (traps) with OID.
wi01030802	Trap `avWlanLimitsReached` for MDC Capability is not displayed in WMS Alarms
Access point	
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/ roaming delays.
wi00996001	SplitPlane Outdoor AP: ICMP Packets with 2000 bytes size from Wireless Client is dropped even if Jumbo Frames is Enabled in ERS/POE, and the MTU size is set to 9600.
wi00969067	Radio Profile created for AP 8120-O model should limit the maximum value of DTIM to 15, as supported by this AP Model.
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.

WI ID	Summary
EDM	

WI ID	Summary
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.
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.
Mobility Domain	
wi00575533	Due the limited number of non overlapping channels available on the 2.4 GHz Band using channel bonding (40 MHz mode) could result in connectivity issues for some of the older adaptors. **Workaround**: Avaya recommends to use 40 MHz Mode on the 5 GHz Radio and use 20 MHz Mode on the 2.4 GHz Radio on the AP.

WI ID	Summary
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.
Wireless Controller	
wi00984608	Adding a MAC to Blacklist requires enabling MAC Authentication on the Network Profile, which requires users to populate the Whitelist even when it is not intended to be used.
wi01000743	Radius Attributes calling / called station ID not sent in RADIUS request by Wireless Controller during the Captive Portal user authentication via RADIUS.
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.
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.

WI ID	Summary
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.
Wireless LAN Management System	
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.
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.
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.
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.
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.
wi00664791	WMS with Internet Explorer 8 does not display policy names correctly in some instances as policy names appear to be overlapped.
wi00900592	WMS: Monitoring Clients in WMS does not work if http port on WC is non-default
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.

WI ID	Summary
	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.
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. **Workaround**: Applying the configuration a second time pushes the 40MHz configuration to the controller.
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.
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.
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.
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. "
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.

WI ID	Summary
	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.
Traps/Syslog	
wi00576426	Trap message is not generated when a Wireless Client fails MAC Authentication.
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.

Appendix A: WSP configuration using the ACLI

Adding or removing VLANs from the VLAN pool

A WSP services local VLANs only. When a WSP receives a Mobility VLAN that is not local (so it does not service) and that is serviced by another WSP, the Avaya VENA Unified Access software dynamically creates a remote VLAN based on the vlan-reservation list. This remote VLAN is used to transport traffic across a mobility tunnel to a remote WSP.

The Unified Access software manages a pool of VLAN IDs that are reserved for creating these dynamic remote VLANs. This reservation does not allocate any VLAN resources; it just reserves the VLAN ID for remote VLANs. These IDs are for WLAN only; no other application can use them to create a VLAN.

Note:

There is no default pool of VLANs, and it is not required to configure one. If you have only one WSP, there is no need to configure a VLAN pool. However, if you have multiple WSPs, then you should configure a VLAN pool. If you do not have a VLAN pool and a WSP receives an MVLAN, you will receive an error message. Avaya recommends configuring a VLAN pool equal to the total number of MVLANs minus the number of MVLANs serves locally.

The system prevents you from reserving a VLAN ID if it is being used by a local VLAN. It also prevents you from deleting a VLAN ID that is currently in use.

Procedure

1. Log on to WLAN Switch Configuration mode:
   ```
   enable
   configure terminal
   wireless
   switch
   ```
2. To add a list of VLANs to the reserved pool, use the following command:
   ```
   vlan-reservation <vidList>
   ```
3. To remove a list of VLANs from the reserved pool, use the following command:

```
no vlan-reservation <vidList>
```

Example

The following example adds VLAN IDs from 2010 to 2012 and 4094 to the reservation pool.

```
vlan-reservation 2010-2012,4094
```

Variable definitions

Use the data in the following table to use the **`vlan-reservation`** command.

Variable	Value
<vidList>	Specifies a list of VLAN IDs separated by a comma or listed as a range.

Assigning an STG to the remote VLAN

Assign remote VLANs to a spanning tree group in STP mode.

Procedure

1. Log on to Global Configuration mode:
   ```
   enable
   configure terminal
   ```
2. Create a spanning tree ID.
   ```
   spanning-tree stp <1–64> create
   ```
3. Log on to WLAN Switch Configuration mode:
   ```
   wireless
   switch
   ```
4. Assign the spanning tree group to the remote VLAN.
   ```
   remote-vlan-stg <1–64>
   ```

Example

This example assigns spanning tree group 50 to the WLAN remote VLAN.

```
remote-vlan-stg 50
```

Variable definitions

Use the data in the following table to use the **`remote-vlan-stg`** command.

Variable	Value
<1–64, 255>	Specifies a unique number for this STG from 1 to 64. The 255 value clears the configuration.

Configuring a WSP

Configure an ERS 8800/8600 as a WSP so that it can be part of the mobility domain. The required tasks are to assign a system IP address and a management IP address to the WSP and then enable it.

- System IP Address — The WSP uses this address to communicate with other WLAN devices, connect with APs, and terminate all tunnels going to this WSP. Captive Portal Web Server is also hosted on this address.

  Note:

  You must configure the IP address as a circuitless IP (CLIP) address, which is a virtual (or loopback) interface that is not associated with any physical port. You can use the CLIP interface to provide uninterrupted connectivity to your switch as long as there is an actual path to reach the device. For more information about CLIP IP addresses, see *Configuration — IP Routing* (NN46205–523).

- Management IP Address — Wireless Management Software (WMS) uses this address for network management functions. Unlike the Out Of Band management interface, which uses the port IP address on the CPU module, the Management IP Address can be any IP address on the switch that you want to use.

You can also change the default TCP and UDP base port number. Network administrators use the base port number to create simple firewall rules. If you want to change the base port number for security purposes, you have that option.

Before you begin

Before you can set the WSP system IP address or change the TCP and UDP base port number, you must disable Wireless in the WSP.

Procedure

1. Log on to WLAN Switch Configuration mode:
   ```
   enable
   ```

```
configure terminal
wireless
switch
```

2. Optionally, set the WSP management interface IP address. If you do not set an address, the switch uses the chassis management IP address by default.
   `mgmt-ip <A.B.C.D>`
3. Log on to Wireless Configuration mode:
   `exit`
4. Use a CLIP address to set the WSP system IP address:
   `interface-ip <A.B.C.D>`
5. Optionally, change the default TCP and UDP base port number:
   `tcp-udp-base-port <49152-64983>`
6. Enable the WSP:
   `enable`

Example

Set a management interface IP address in WLAN Switch Configuration mode:

```
mgmt-ip 2.2.2.2
```

Log on to Wireless Configuration mode:

```
exit
```

Assign a CLIP interface for the WSP system IP address:

```
interface-ip 1.1.1.1
```

Change the default TCP and UDP base port number to 55000:

```
tcp-udp-base-port 55000
```

Enable the WSP:

```
enable
```

Variable definitions

Use the data in the following table to use the WSP configuration commands.

Variable	Value
interface-ip <A.B.C.D>	Specifies the CLIP interface that the WSP is using for a system IP address.

Variable	Value
mgmt-ip <A.B.C.D>	Specifies the management interface IP address.
tcp-udp-base-port <49152-64983> (optional)	Specifies the TCP and UDP base port number. The range of values is from 49152..64983. All WLAN components (WCPs, APs, other WSPs, access and mobility tunnels) use different TCP and UDP port numbers that are based on different fixed offsets from this base port. The base port number enables network administrators to create simple firewall rules by opening a contiguous IP port range of 16 ports for WLAN communication. **Note:** The base port number must be the same on all WCPs and WSPs in the WLAN domain. This is an optional configuration. You can leave all WCPs and WSPs operating at the default value. **DEFAULT**: 61000
enable	Enables or disables wireless on the ERS 8800/8600. The default is disable. Use the no enable or default enable options to disable the WSP.

Adding or removing a WLAN cluster controller

You can configure up to four WLAN Switch Controllers in the cluster of controllers. Use the following procedure to add or remove a controller from the cluster.

Note:

The Controller that you configure becomes part of the cluster and it may not be the controller that manages this switch. A round-robin algorithm determines which WCP controls which WSP.

Procedure

1. Log on to WLAN Switch Configuration mode:
   ```
   enable
   configure terminal
   wireless
   ```

```
switch
```

2. To add a controller, use the following command and specify the Controller ID number and its IP address:

   ```
   lb-controller <contId:1–4> <A.B.C.D>
   ```

3. To remove a controller, use the following command and specify the Controller ID number:

   ```
   no lb-controller <contId:1–4>
   ```

Example

This example shows how to add all four controllers to the cluster and then remove controller 4.

```
lb-controller 1 10.30.18.18
lb-controller 2 10.30.18.20
lb-controller 3 10.30.18.5
lb-controller 4 10.30.18.6
no lb-controller 4
```

Variable definitions

Use the data in the following table to use the **`lb-controller`** command.

Variable	Value
<contId:1–4> (optional)	Specifies the ID of the WLAN Controller that you want to add or remove from the cluster of WLAN Controllers. The valid numbers are from 1 to 4.
<A.B.C.D>	Specifies the IPv4 address of the WLAN Controller, which must be a unique address within the WLAN domain.

Mapping VLANs to the WSP

Use this procedure to map VLANs to the WSP and perform the following tasks:

- Specify a name to uniquely identify the mobility VLAN.
- Create or delete the VLAN map.

- Specify the L3 mobility mode for the VLAN.
- Define the local VLAN ID, which is then mapped to the Mobility VLAN.
- Set a priority for this VLAN by specifying the weight to assign to it.

Procedure

1. Log on to WLAN Switch Configuration mode:
   ```
   enable
   configure terminal
   wireless
   switch
   ```
2. Use the following command to name the mobility VLAN, create the VLAN map, specify the L3 mobility mode, define the local VLAN ID, and assign a priority weight:
   ```
   vlan-map <name:WORD/0–32> {l3-mobility [none|server]} [lvid <1-4094>] [weight <1-7>]
   ```

Example

This example creates a VLAN map called, *SuperKings*, which is mapped to local VLAN ID 1000. The VLAN map is in server mode so the WSP can act as a server for this VLAN and it's assigned a weight of 7

```
vlan-map SuperKings l3-mobility server lvid 1000 weight 7
```

Variable definitions

Use the data in the following table to use the **`vlan-map`** command.

Variable	Value
<name:WORD/0–32>	Specifies a unique name for this mobility VLAN map. The name can be up to 32 characters. Use the no vlan-map <name:WORD/0–32> option to delete a mobility VLAN map.
{l3-mobility [none|server]}	Specifies the L3 mobility mode for the VLAN map. • `none` — means that L3 mobility is not enabled for this VLAN, but L2 mobility is enabled. • `server` — means that L3 mobility is enabled for this VLAN, and this switch can act as a server for this mobility VLAN.

Variable	Value
	Default: none
[lvid <1-4094>]	Specifies the local VLAN ID number for this map.
[weight <1-7>]	Specifies a weight value to prioritize switches when there are a number of them configured as the server for this VLAN. The switch with the highest number is the winning server. The range of values is from 1 to 7. **Default:** 1

Flushing the WLAN forwarding database

Use this procedure to flush all of the WLAN forwarding database (FDB) entries learned by the WSP. The FDB is a table that contains forwarding information for specific entries. The switch uses this information to forward received frames.

Procedure

1. Log on to Global Configuration mode:
   ```
   enable
   configure terminal
   ```
2. Use the following command to flush the WLAN FDB:
   ```
   clear wireless switch mac-address-entry
   ```

Displaying WSP configuration information

Perform this procedure to view and manage general WSP information.

Procedure

1. Log on to Privileged Exec mode:
   ```
   enable
   ```
2. Display general WSP configuration information:
   ```
   show wireless
   ```
   and

```
show wireless switch
```

Example

```
McLaren:6# show wireless
********************************************************************************
Command Execution Time: MON AUG 27 12:31:55 2012 EST
********************************************************************************
                    TCP UDP
 IP ADDRESS         BASE PORT     STATUS
--------------------------------------------------------------------------------
 1.1.1.2            6100          Enable
```

```
McLaren:6# show wireless-switch
********************************************************************************
Command Execution Time: WED FEB 15 13:57:26 2012 UTC
********************************************************************************
 REMOTE           MANAGEMENT
 VLAN STG         IP
--------------------------------------------------------------------------------
 255              47.17.149.75
```

Job aid

The following table describes the fields in the output for the **`show wireless switch`** command.

Variable	Value
REMOTE VLAN STG	Indicates the remote VLAN spanning tree group number.
MANAGEMENT IP	Indicates the management IP address of the ERS 8800/8600.

Displaying WLAN controllers

Perform this procedure to view information about the WLAN controllers.

Procedure

1. Log on to Privileged Exec mode:
   `enable`
2. Display configuration information for all of the controllers configured on this switch or for a specific controller:

```
show wireless switch lb-controller [<A.B.C.D>]
```

Example

```
McLaren:6# show wireless switch lb-controller
********************************************************************************
Command Execution Time: WED FEB 15 13:58:03 2012 UTC
********************************************************************************
WC ID      WC IP ADDRESS         STATUS
--------------------------------------------------------------------------------
1          10.30.18.18           Configured
2          10.30.18.20           Configured
3          10.30.18.5            Configured
4          10.30.18.6            Active
```

Job aid

The following table describes the fields in the output for the **`show wireless switch lb-controller`** command.

Variable	Value
WC ID	Indicates the WLAN controller ID, which is also used for controller priority. The lower the number is; the higher the priority.
WC IP ADDRESS	Indicates the WLAN controller IP address.
STATUS	Indicates the current status of the WLAN controller. The Active controller is the one currently managing this WSP. The others are Configured as potential backups if the WCP fails.

Displaying WSP peer devices

Perform this procedure to view information about the WSP peer devices.

Procedure

1. Log on to Privileged Exec mode:
   `enable`
2. Display configuration information for all of the WSP peer devices or just for the access (**ap**) or mobility tunnels (**`switch`**):

```
show wireless switch peer-devices [ap | switch]
```

Example

```
McLaren:6# show wireless switch peer-devices
********************************************************************************
Command Execution Time: WED FEB 15 13:58:34 2012 UTC
********************************************************************************
PEER    PEER               PEER            PEER     PEER    LOCAL    TUNNEL
TYPE    MAC                ADDR            UDP PORT STATUS  UDP PORT INTERFACE
--------------------------------------------------------------------------------
MT      00:04:38:0f:b0:00  1.1.1.2         61012    down    61012    WT-5
MT      00:0c:f7:e8:80:00  1.1.1.3         61012    down    61012    WT-3
MT      00:0c:f7:e8:d0:00  3.3.3.3         61012    up      61012    WT-4
MT      00:0e:c0:c1:90:00  4.4.4.4         61012    up      61012    WT-1
MT      00:15:9b:04:80:00  2.2.2.2         61012    up      61012    WT-2
```

Job aid

The following table describes the fields in the output for the **`show wireless switch peer-devices`** command.

Variable	Value
PEER TYPE	Indicates whether the peer is an Access Tunnel (AT) or Mobility Tunnel (MT).
PEER MAC	Indicates the peer's MAC address that uniquely identifies the peer WSP or AP on the other side of the tunnel.
PEER ADDR	Indicates the IP address of the peer WSP or AP.
PEER UDP PORT	Indicates the UDP port that the peer WSP or AP uses for control protocol communication with the local switch.
PEER STATUS	Indicates the current status of the mobility tunnel to this WSP or the access tunnel to the AP.
LOCAL UDP PORT	Indicates the local UDP port that the switch uses for control protocol communication with the WSP or AP tunnels. This is the **`tcp-udp-base-port`** configured on the switch.
TUNNEL INTERFACE	Indicates the name of the tunnel.

Displaying WSP VLANs advertised by peer WSPs

Perform this procedure to view a list of all the Mobility VLANs that are advertised by each peer WSP. A WSP is considered a peer if it has an established mobility tunnel with the local WSP.

Procedure

1. Log on to Privileged Exec mode:
   ```
   enable
   ```
2. Display the Mobility VLANs for all the peer WSPs. You can display the table of VLANs **`by-advertizer`** or **`by-vlan`**:

   ```
   show wireless switch peer-advertized-vlans {by-advertizer | by-vlan}
   ```

Example

```
McLaren:6# show wireless switch peer-advertized-vlans by-advertizer
********************************************************************************
Command Execution Time: WED FEB 22 08:46:25 2012 UTC
********************************************************************************
ADVERTISING PEER MAC     MOBILITY VLAN NAME     PRIORITY
--------------------------------------------------------------------------------
00:0c:f7:e8:d0:00        default-MVLAN          3
00:0c:f7:e8:d0:00        vlc                    1
00:0e:c0:c1:90:00        default-MVLAN          5
00:0e:c0:c1:90:00        sim1                   7
00:0e:c0:c1:90:00        vlc                    1
00:15:9b:04:80:00        SuperKings             4
00:15:9b:04:80:00        pvdemo2                7
00:15:9b:04:80:00        sim2                   7
```

```
McLaren:6# show wireless-switch peer-advertized-vlans by-vlan
********************************************************************************
Command Execution Time: WED FEB 22 08:48:06 2012 UTC
********************************************************************************
MOBILITY VLAN NAME     ADVERTISING PEER MAC     PRIORITY
--------------------------------------------------------------------------------
SuperKings             00:15:9b:04:80:00        4
default-MVLAN          00:0c:f7:e8:d0:00        3
default-MVLAN          00:0e:c0:c1:90:00        5
pvdemo2                00:15:9b:04:80:00        7
sim1                   00:0e:c0:c1:90:00        7
sim2                   00:15:9b:04:80:00        7
vlc                    00:0c:f7:e8:d0:00        1
vlc                    00:0e:c0:c1:90:00        1
```

Job aid

The following table describes the fields in the output for the **`show wireless switch peer-advertized-vlans {by-advertizer | by-vlan}`** command.

Variable	Value
ADVERTISING PEER MAC	Indicates the MAC address that uniquely identifies the peer WSP.
MOBILITY VLAN NAME	Indicates the name of the advertised mobility VLAN advertised by a peer WSP.
PRIORITY	Indicates the priority of the advertised mobility VLAN.

Displaying WSP VLAN mapping

Perform this procedure to view information about the WSP VLAN maps.

Procedure

1. Log on to Privileged Exec mode:
   `enable`
2. Display configuration information for all of the VLAN maps on this switch or for a specific VLAN map:
   `show wireless switch vlan-map [<name:WORD/0–32>]`

Example

```
McLaren:6# show wireless switch vlan-map
********************************************************************************
Command Execution Time: WED FEB 22 09:18:08 2012 UTC
********************************************************************************
MOBILITY                        LOCAL   L3       WEIGHT STATE     WCP-V  ADMIN
VLAN NAME                       VLAN ID MOBILITY                          MAPPED
--------------------------------------------------------------------------------
SuperKings                      1000    server   7      active    yes    yes
default-MVLAN                   0       server   1      active    yes    no
fghj                            1       none     1      inactive  no     yes
pvdemo2                         3       server   5      active    yes    yes
sim1                            0       none     1      active    yes    no
sim2                            0       none     1      active    yes    no
test1                           1007    server   7      inactive  no     yes
vlc                             0       server   1      active    yes    no

8 out of 8 entries in all displayed.
```

Job aid

The following table describes the fields in the output for the **`show wireless switch vlan-map`** command.

Variable	Value
<name:WORD/1–32>	Indicates the name of a specific Mobility VLAN that is a string of 1 to 32 characters.
MOBILITY VLAN NAME	Indicates the unique name of the Mobility VLAN.
LOCAL VLAN ID	Indicates the local VLAN ID, which maps the Mobility VLAN to a locally defined VLAN.
L3 MOBILITY	Indicates the L3 mobility mode for the VLAN. • `none` — means that L3 mobility is not enabled for this VLAN, but L2 mobility is enabled. • `server` — means that L3 mobility is enabled for this VLAN, and this switch can act as a server for this mobility VLAN. **Default:** `none`
WEIGHT	Indicates a weight value to prioritize switches when there are a number of them configured as the server for this VLAN. The switch with the highest number is the winning server. The range of values is from 1 to 7. **Default:** 1
STATE	Indicates whether or not the local VLAN ID (LVID) mapping is in the `Active` state. For the mapping to be `Active`, it must meet the following conditions: • The Mobility VLAN has to be received from (validated by) the WC. • The LVID has to be mapped a value other than 0. • The LVID has to represent a valid local VLAN on this switch.
WCP-V	Indicates whether the Mobility VLAN name for this entry was received from (and thus validated by) the managing controller.

Variable	Value
	Note: This entry is useful for validating mappings that were manually added offline before the switch was associated to the controller.
ADMIN MAPPED	**yes** indicates that the LVID mapping for this entry was set by an administrator. **no** indicates that it was auto-assigned by the switch itself.

Displaying WSP servers for all mobility VLANs

Perform this procedure to view the current VLAN server for each mobility VLAN.

Procedure

1. Log on to Privileged Exec mode:
   `enable`
2. Display configuration information for all of the VLAN servers configured on the WSP:
   `show wireless switch vlan-servers`

Example

```
McLaren:6# show wireless switch vlan-servers
********************************************************************************
Command Execution Time: WED FEB 22 10:31:26 2012 UTC
********************************************************************************
MOBILITY                        CURRENT                  PRIORITY
VLAN NAME                       SERVER MAC
--------------------------------------------------------------------------------
SuperKings                      00:0c:f8:a9:20:00        7
default-MVLAN                   00:0c:f7:e8:d0:00        7
pvdemo2                         00:0c:f8:a9:20:00        5
sim1                            00:0e:c0:c1:90:00        7
sim2                            00:15:9b:04:80:00        7
vlc                             00:0c:f7:e8:d0:00        1

6 out of 6 entries in all displayed.
```

Job aid

The following table describes the fields in the output for the **`show wireless switch vlan-servers`** command.

Variable	Value
MOBILITY VLAN NAME	Indicates the unique ID (MAC address) of the WSP that advertises mobility VLAN.
CURRENT SERVER MAC	Indicates the MAC address of the WSP that is currently selected as the server for this Mobility VLAN.
PRIORITY	Indicates the priority of the mobility VLAN.

Displaying WSP VLAN pool IDs

Perform this procedure to view the list of reserved VLAN IDs and to see if they are currently in use.

Procedure

1. Log on to Privileged Exec mode:
   `enable`
2. Display information for all of the reserved VLAN IDs or for a specific VLAN ID:
   `show wireless switch vlan-reservation [<vidList>]`

Example

```
McLaren:6# show wireless switch vlan-reservation
********************************************************************************
Command Execution Time: WED FEB 22 10:59:52 2012 UTC
********************************************************************************
VLAN ID    IN USE
--------------------------------------------------------------------------------
2010       No
2011       No
2012       No
4094       No

4 out of 4 entries in all displayed.
```

Job aid

The following table describes the fields in the output for the **`show wireless switch vlan-reservation`** command.

Variable	Value
VLAN ID	Indicates a list of VLAN IDs that are reserved. Separate VLAN IDs by a comma or list as a range.
IN USE	Indicates whether a VLAN ID from the reserved pool is in use.

Displaying FDB entries

Perform this procedure to view the WLAN forwarding database (FDB), which contains entries for wireless traffic. This table gets populated when the WSP receives traffic from the AP. You can also clear the entries, if desired.

Procedure

1. Log on to Privileged Exec mode:
   `enable`
2. Display information for all of the FDB entries configured on this switch or for a specific VLAN ID or MAC address:
   `show wireless switch mac–address-entry [vid <value>] [mac <value>]`
3. Use the following command to clear all the FDB entries on the switch or just for a specific VLAN or MAC address:
   `clear wireless switch mac–address–entry [vid <value>] [mac <value>]`

Example

```
McLaren:6# show wireless switch mac–address-entry

********************************************************************************
Command Execution Time: WED FEB 22 13:16:37 2012 UTC
********************************************************************************

================================================================================
                                WLAN Vlan Fdb
================================================================================
VLAN          MAC               REMOTE IP       LOCAL UDP REMOTE UDP
ID    TYPE    ADDRESS           ADDRESS         PORT      PORT       INTERFACE
--------------------------------------------------------------------------------
1    learned  00:11:f9:cf:81:94  1.1.1.1         3001      2001       WT-1002
11   learned  00:1a:8f:10:92:00  2.2.2.2         3002      2002       WT-1003
700  learned  00:1a:8f:10:92:02  3.3.3.3         3003      4004       WT-2003

3 out of 3 entries in all wlan fdb(s) displayed.
```

Job aid

The following table describes the fields in the output for the **`show wireless switch mac-address-entry`** command.

Variable	Value
vid <*value*>	Indicates the VLAN ID associated with the FDB entry.
mac <*value*>	Indicates the MAC address associated with the FDB entry.
VLAN ID	Indicates the local VLAN ID.
TYPE	Indicates the type of entry: • `other` • `invalid` • `learned` • `self` • `static`
MAC ADDRESS	Indicates the unicast MAC address for this FDB entry.
REMOTE IP ADDRESS	Indicates the IP address of the remote endpoint, which can be another WSP or an access point.
LOCAL UDP PORT	Indicates the UDP port used by the local endpoint of the tunnel.
REMOTE UDP PORT	Indicates the UDP port used by the remote endpoint of the tunnel.
INTERFACE	Indicates the name of the tunnel.

Displaying WSP tunnels

Perform this procedure to view information about the WSP access and mobility tunnels.

Procedure

1. Log on to Privileged Exec mode:
   `enable`

2. Display configuration information for all of the tunnels configured on this switch or for a specific tunnel:

   ```
   show wireless switch tunnel [<tunnelIntfId>]
   ```

Example

```
McLaren:6# show wireless switch tunnel
********************************************************************************
Command Execution Time: WED FEB 22 14:00:04 2012 UTC
********************************************************************************

================================================================================
                                WLAN Tunnels
================================================================================
TUNNEL     PEER
INTERFACE  DEVICE ID                    PEER IP :UDP PORT   TYPE     STATUS
--------------------------------------------------------------------------------
WT-1       00:0e:c0:c1:90:00            4.4.4.4 :61012      MT       up
WT-2       00:15:9b:04:80:00            2.2.2.2 :61012      MT       up
WT-3       00:0c:f7:e8:d0:00            3.3.3.3 :61012      MT       up
WT-4       00:0c:f7:e8:80:00            1.1.1.3 :61012      MT       up
WT-5       00:04:38:0f:b0:00            1.1.1.2 :61012      MT       up
WT-6       00:1b:4f:6a:54:80         10.30.3.51 :61012      AT       up
WT-7       00:1b:4f:6a:58:00         10.30.3.52 :61012      AT       up

7 out of 7 entries in all wlan tunnel(s) displayed.
```

Job aid

The following table describes the fields in the output for the **`show wireless switch tunnel`** command.

Variable	Value
TUNNEL INTERFACE	Indicates the name of the tunnel.
PEER DEVICE ID	Indicates the peer's MAC address that uniquely identifies the peer WSP or AP on the other side of the tunnel.
PEER IP	Indicates the IP address of the peer WSP or AP.
UDP PORT	Indicates the UDP port that the peer WSP or AP uses for control protocol communication with the local switch.
TYPE	Indicates whether the peer is an Access Tunnel (AT) or Mobility Tunnel (MT).
STATUS	Indicates the current status of the mobility tunnel to this WSP or the access tunnel to the AP.

Displaying WSP tunnels statistics

Perform this procedure to view the mobility and access tunnel statistics on a WSP and then clear them, if desired.

Note:

When an I/O module goes offline for any reason such as a reset or administratively disabled, the statistics for all WSP tunnels are reset to zero.

Procedure

1. Log on to Privileged Exec mode:
   ```
   enable
   ```
2. Display the statistics for all of the tunnels configured on this switch or for a specific tunnel:
   ```
   show wireless switch tunnel-statistics [<tunnelIdList>]
   ```
3. Display the bridging statistics for all of the tunnels configured on this switch or for a specific tunnel:
   ```
   show wireless switch tunnel-statistics bridging
   [<tunnelIdList>]
   ```
4. Display the keepalive statistics for all of the tunnels configured on this switch or for a specific tunnel:
   ```
   show wireless switch tunnel-statistics keepalive
   [<tunnelIdList>]
   ```
5. Display the routing statistics for all of the tunnels configured on this switch or for a specific tunnel:
   ```
   show wireless switch tunnel-statistics routing
   [<tunnelIdList>]
   ```
6. Use the following command to clear all the tunnel statistics on the switch or for a specific tunnel:
   ```
   clear wireless switch statistics [tunnel-id <tunnelIdList>]
   ```

Example

Display all the tunnel statistics.

```
McLaren:6# show wireless switch tunnel-statistics
********************************************************************************
Command Execution Time: WED FEB 22 14:23:43 2012 UTC
********************************************************************************

================================================================================
                                    TUNNEL STATISTICS
```

```
================================================================================
TUNNEL     PEER                IN     OUT    IN         OUT        IN      OUT
INTERFACE  DEVICE ID           FRAME  FRAME KEEPALIVE  KEEPALIVE  DISCARD  DISCARD
--------------------------------------------------------------------------------
WT-1       00:0e:c0:c1:90:00    298    299    17873     17865      0       0
WT-2       00:15:9b:04:80:00    299    299    17873     17865      0       0
WT-3       00:0c:f7:e8:d0:00    1741   558    17837     17865      0       0
WT-4       00:0c:f7:e8:80:00    1      286    16988     17015      0       0
WT-5       00:04:38:0f:b0:00    1      286    16997     17023      0       0
WT-6       00:1b:4f:6a:54:80    0      1      4371      4391       0       0
WT-7       00:1b:4f:6a:58:00    210    85     4369      4390        0      0
WT-8       00:1b:4f:6a:70:40    80     4611   834       838        0       0

8 out of 8 entries in all wlan tunnel(s) displayed.
```

Display the tunnel bridging statistics.

```
McLaren:6# show wireless switch tunnel-statistics bridging
********************************************************************************
Command Execution Time: WED FEB 22 14:28:21 2012 UTC
********************************************************************************

================================================================================
                     TUNNEL STATISTICS - INTERFACE BRIDGING
================================================================================
TUNNEL     PEER              IN-FRAME  IN-FRAME  IN-FRAME  IN        OUT
INTERFACE  DEVICE ID         UNICAST   MULTICAST BROADCAST DISCARD   FRAME
--------------------------------------------------------------------------------
WT-1       00:0e:c0:c1:90:00 303       0         0         0         303
WT-2       00:15:9b:04:80:00 304       0         0         0         303
WT-3       00:0c:f7:e8:d0:00 2284      0         0         0         674
WT-4       00:0c:f7:e8:80:00 1         0         0         0         286
WT-5       00:04:38:0f:b0:00 1         0         0         0         286
WT-6       00:1b:4f:6a:54:80 0         0         0         0         1
WT-7       00:1b:4f:6a:58:00 295       0         0         0         123
WT-8       00:1b:4f:6a:70:40 80        40        0         0         6180

8 out of 8 entries in all wlan tunnel(s) displayed.
```

Display the tunnel keepalive statistics.

```
McLaren:6# show wireless switch tunnel-statistics keepalive
********************************************************************************
Command Execution Time: WED FEB 22 14:31:17 2012 UTC
********************************************************************************

================================================================================
                          TUNNEL STATISTICS - KEEPALIVE
================================================================================
TUNNEL     PEER              IN        OUT
INTERFACE  DEVICE ID         KEEPALIVE KEEPALIVE
--------------------------------------------------------------------------------
WT-1       00:0e:c0:c1:90:00 18327     18319
WT-2       00:15:9b:04:80:00 18327     18319
WT-3       00:0c:f7:e8:d0:00 18290     18319
WT-4       00:0c:f7:e8:80:00 16988     17015
WT-5       00:04:38:0f:b0:00 16997     17023
WT-6       00:1b:4f:6a:54:80 4823      4845
WT-7       00:1b:4f:6a:58:00 4822      4844
WT-8       00:1b:4f:6a:70:40 1286      1292
WT-9       10:20:30:50:50:d0 52        52
WT-10      10:20:30:50:51:50 49        49
```

Display the tunnel routing statistics.

```
McLaren:6# show wireless switch tunnel-statistics routing
********************************************************************************
Command Execution Time: WED FEB 22 14:32:18 2012 UTC
********************************************************************************

================================================================================
                      TUNNEL STATISTICS - INTERFACE ROUTING
================================================================================
TUNNEL     PEER              IN-FRAME  IN-FRAME  IN-FRAME  OUT-FRAME OUT-FRAME
INTERFACE  DEVICE ID         UNICAST   MULTICAST DISCARD   UNICAST   MULTICAST
--------------------------------------------------------------------------------
WT-1       00:0e:c0:c1:90:00 0         0         0         0         0
WT-2       00:15:9b:04:80:00 0         0         0         0         0
WT-3       00:0c:f7:e8:d0:00 0         0         0         0         0
WT-4       00:0c:f7:e8:80:00 0         0         0         0         0
WT-5       00:04:38:0f:b0:00 0         0         0         0         0
WT-6       00:1b:4f:6a:54:80 0         0         0         0         0
WT-7       00:1b:4f:6a:58:00 0         0         0         0         0
WT-8       00:1b:4f:6a:70:40 0         0         0         0         0
WT-9       10:20:30:50:50:d0 0         0         0         0         0
WT-10      10:20:30:50:51:50 0         0         0         0         0
```

Job aid

The following table describes the fields in the output for the **`show wireless switch tunnel-statistics`** command.

Variable	Value
TUNNEL INTERFACE	Indicates the name of the tunnel.
PEER DEVICE ID	Indicates the peer's MAC address that uniquely identifies the peer WSP or AP on the other side of the tunnel.
IN FRAME	Indicates the number of packets received on the tunnel.
OUT FRAME	Indicates the number of packets transmitted from this tunnel.
IN KEEPALIVE	Indicates the number of keepalive requests received on this tunnel.
OUT KEEPALIVE	Indicates the number of keepalive requests transmitted from this tunnel.
IN DISCARD	Indicates the number of ingress packets that were dropped.
OUT DISCARD	Indicates the number of egress packets that were dropped.

The following table describes the fields in the output for the **show wireless switch tunnel-statistics bridging** command.

Variable	Value
TUNNEL INTERFACE	Indicates the name of the tunnel.
PEER DEVICE ID	Indicates the peer's MAC address that uniquely identifies the peer WSP or AP on the other side of the tunnel.
IN-FRAME UNICAST	Indicates the number of unicast packets received on the tunnel.
IN-FRAME MULTICAST	Indicates the number of multicast packets received on the tunnel.
IN-FRAME BROADCAST	Indicates the number of broadcast packets received on the tunnel.
IN DISCARD	Indicates the number of bridged ingress packets that were dropped.
OUT FRAME	Indicates the number of bridged egress packets that were dropped.

The following table describes the fields in the output for the **show wireless switch tunnel-statistics keepalive** command.

Variable	Value
TUNNEL INTERFACE	Indicates the name of the tunnel.
PEER DEVICE ID	Indicates the peer's MAC address that uniquely identifies the peer WSP or AP on the other side of the tunnel.
IN KEEPALIVE	Indicates the number of keepalive requests received on this tunnel.
OUT KEEPALIVE	Indicates the number of keepalive requests transmitted from this tunnel.

The following table describes the fields in the output for the **show wireless switch tunnel-statistics routing** command.

Variable	Value
TUNNEL INTERFACE	Indicates the name of the tunnel.
PEER DEVICE ID	Indicates the peer's MAC address that uniquely identifies the peer WSP or AP on the other side of the tunnel.

Variable	Value
IN-FRAME UNICAST	Indicates the number of routed unicast packets received on the tunnel.
IN-FRAME MULTICAST	Indicates the number of routedmulticast packets received on the tunnel.
IN-FRAME DISCARD	Indicates the number of routed ingress packets that were dropped.
OUT-FRAME UNICAST	Indicates the number of routed unicast egress packets that were dropped.
OUT-FRAME MULTICAST	Indicates the number of routed multicast egress packets that were dropped.

Appendix B: 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 C: 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.

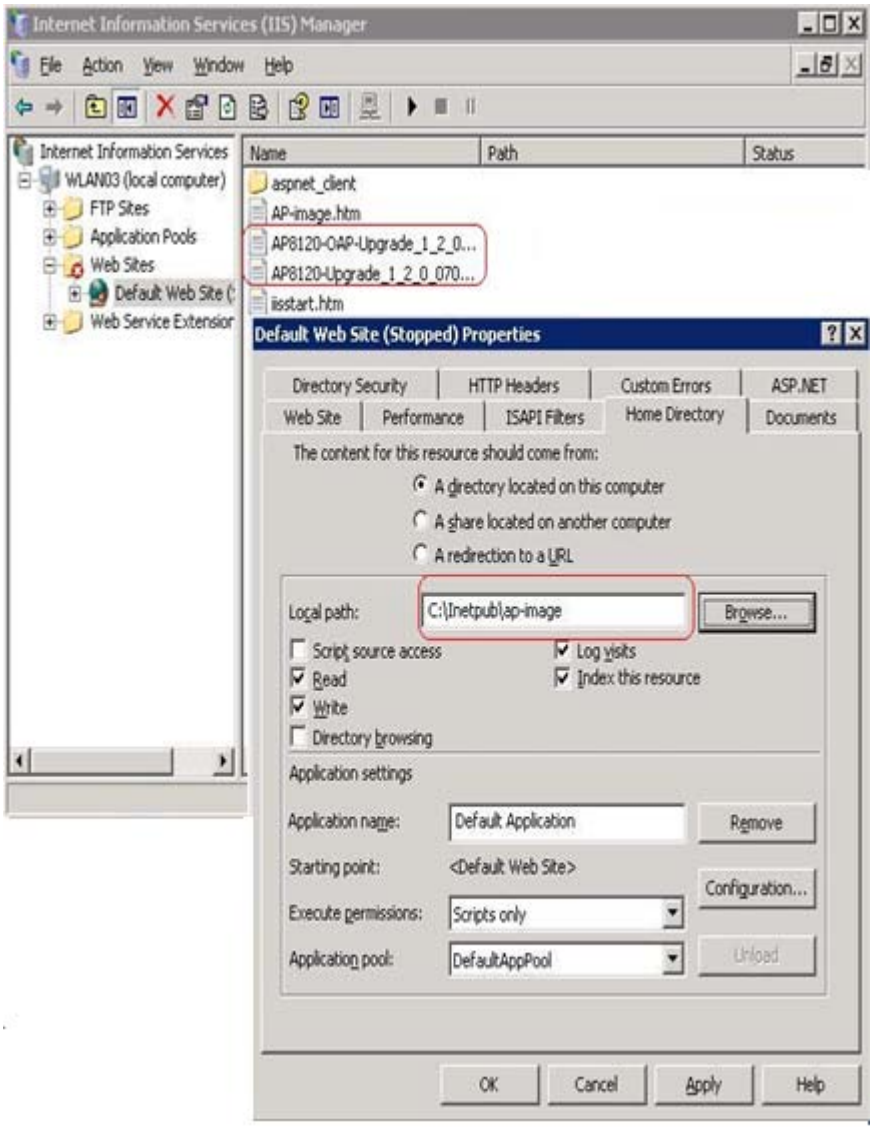


Figure 6: Windows internet information services Home Directory tab

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

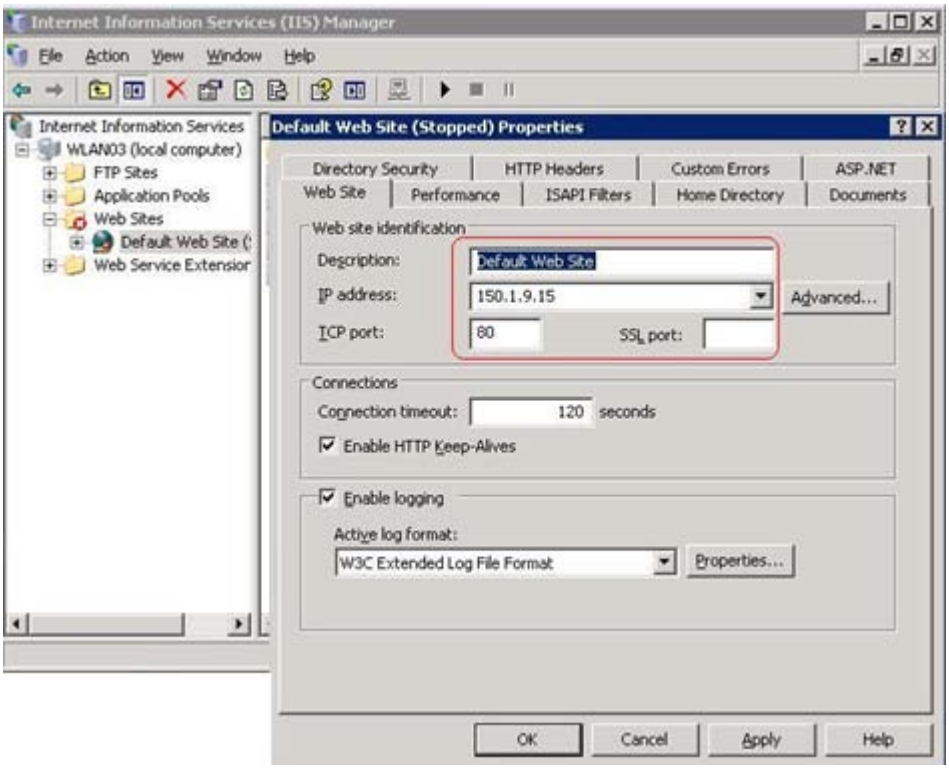


Figure 7: Windows internet information services Web Site tab

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.

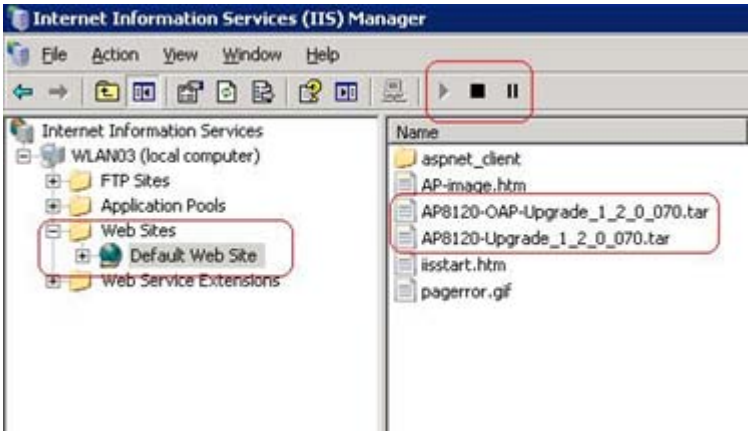


Figure 8: Windows internet information services task service