Quick Start Overlay Deployment Configuration for Avaya WLAN 8100

Release 3.0
NN47251-106
Issue 07.01
June 2014

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

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

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Software” means Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

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

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

Heritage Nortel Software

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

Copyright

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

Third Party Components

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

Preventing Toll Fraud

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

Avaya Toll Fraud Intervention

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

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

Contents

Chapter 1: Introduction

Purpose

Use this Quick Start Guide to configure the Avaya WLAN 8100 system to provide basic Wireless LAN services using Open Authentication.

This document covers the basic configuration for Wireless LAN services. This document does not cover all the functionality required for a typical enterprise network and is intended to be used in a demo/test environment. For configuration workflows in a typical enterprise network, see *Configuring an Overlay Deployment on Avaya WLAN 8100*, NN47251-305.

Related Resources

Documentation

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

Training

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

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

Course Code	Course Title
6769X	Avaya Wireless LAN 8100 Implementation and Management
4D00045V	Avaya VENA Unified Access Implementation
Wireless LAN 8100 AIPS credential	
7D00060A	Wireless LAN 8100 Implementation Assessment (online test)

Viewing Avaya Mentor videos

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

About this task

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

Procedure

- To find videos on the Avaya Support website, go to support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

    Note:

    Videos are not available for all products.

Support

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

Chapter 2: New in this release

The following sections detail what's new in *Quick Start Overlay Deployment Configuration for Avaya WLAN 8100*, NN47251-106, for release 3.0.

Related Links

Features on page 7
Other changes on page 8

Features

See the following sections for information about the feature changes:

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

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

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

Support for External Captive Portal

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

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

Support for Link Layer Discovery Protocol (LLDP)

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

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

Bonjour Gateway support

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

Related Links

New in this release on page 7

Other changes

There are no other changes to this document for release 3.0.

Related Links

New in this release on page 7

Chapter 3: Wireless LAN (WLAN) 8100 configuration overview

The wireless LAN (WLAN) 8100 solution supports the following deployment models:

- **Avaya Overlay**:

  In this deployment, the Wireless Controller 8180 (WC) controls/manages Access Points (AP) over a control channel and data is tunneled between APs and the WC over an access tunnel. Two or more WCs in the domain form a cluster, with a mesh of control channels and data tunnels between each other.

- **Avaya VENA Unified Access**:

  In this deployment, the Wireless Controller is deployed in the control-plane only mode of operation of the 8180 platform. This device then hosts only wireless control function and is called a wireless control point (WCP). A switch such as the Avaya ERS 8600/8800 introduced into the network, tunnels traffic (data) and is known as the wireless switching point (WSP). The APs and WSPs tunnel traffic between each other over an access tunnel and the WSPs tunnel traffic between each other over a mobility tunnel.

For more information about these deployment models and the complete solution, see the WLAN 8100 product documentation suite at http://www.avaya.com.

Important:

This document describes the WLAN configuration for the Overlay deployment only. For information on wireless LAN configuration for Unified Access deployments, see *Quick Start Unified Access Deployment Configuration for Avaya WLAN 8100*, NN47251-111.

Related Links

Avaya WLAN 8100 system components on page 10
WLAN network design on page 10
Configuration requirements on page 11
Configuration options on page 12
Configuration workflow on page 12

Avaya WLAN 8100 system components

System components for the WLAN 8100 Overlay deployment solution:

- WLAN Controller 8180
- WLAN Access Points (AP)

  The supported AP models are:

  - AP 8120 (indoor AP)
  - AP 8120–E (indoor AP with external antenna)
  - AP 8120 with Outdoor Antenna (AP 8120–O)
- WLAN Management Software 8100

Important:

The Wireless Controller (WC) 8180 requires licenses to manage the Access Points. The license activation code for the controller, and the instructions to generate the license file are in the paper package that is included as part of the controller shipment.

Related Links

Wireless LAN (WLAN) 8100 configuration overview on page 9

WLAN network design

The following is a sample network design for configuration in an Overlay deployment.

Note:

The configuration procedures in this document are based on this network design.

Figure 1: WLAN 8100 Overlay network design example

Related Links

Wireless LAN (WLAN) 8100 configuration overview on page 9

Configuration requirements

The following components are required to achieve the configuration described in this document:

- Wireless Controller (WC) 8180
- Access Points (AP)

  Access Points can be of one the following models:

  - AP 8120 (indoor AP)
  - AP 8120–E (indoor AP with external antenna)
  - AP 8120–O (outdoor AP)
- Power over Ethernet (PoE) switch or power injector for AP

- DHCP server
- wireless client
- WLAN Management System (WMS) software server (optional)
- wired client (optional for WMS or EDM use)

Related Links

Wireless LAN (WLAN) 8100 configuration overview on page 9

Configuration options

Use one of the following tools to configure the WLAN 8100:

- Command line interface (CLI)
- WLAN Management System 8100 (WMS) software
- Enterprise Device Manager (EDM)

Related Links

Wireless LAN (WLAN) 8100 configuration overview on page 9

Configuration workflow

The following workflow describes the procedures to configure wireless LAN services on the WLAN 8100.

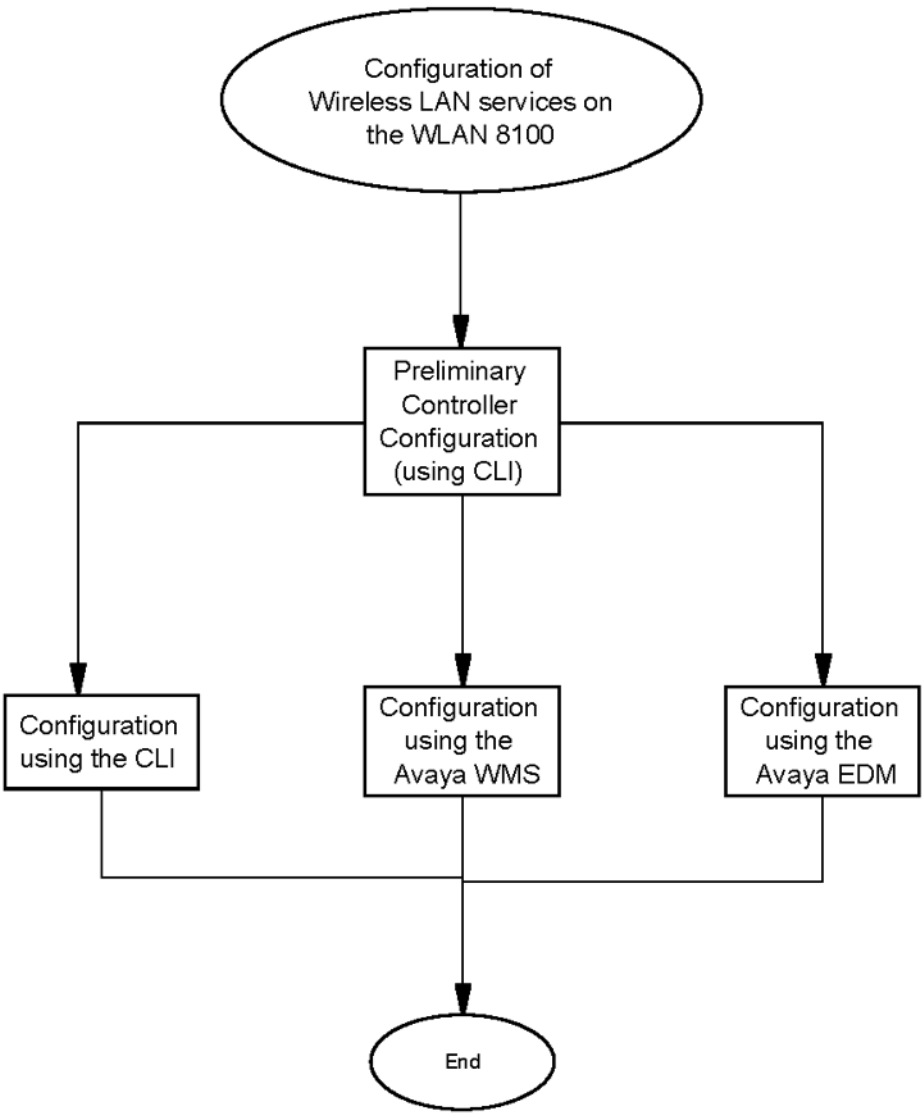


Figure 2: Configuration of Wireless LAN services on the WLAN 8100

Navigation

- Completing preliminary controller configuration on page 15

  Important:

  Preliminary configuration on the WLAN Controller (WC) 8180 must be completed using the command line interface (CLI).

  You can complete the remainder of the configuration using the either the CLI, the WLAN Management System (WMS) or the Enterprise Device Manager (EDM).

- Configuring the Wireless Controller — using the CLI on page 21
- Configuring the Wireless Controller — using the WMS on page 50
- Configuring the Wireless Controller — using the EDM on page 76

Related Links

Wireless LAN (WLAN) 8100 configuration overview on page 9

Chapter 4: Completing preliminary controller configuration

Use this procedure to complete preliminary configuration on the Wireless Controller (WC) 8180.

Important:

You must complete the preliminary controller configuration using the command line interface (CLI).

Before you begin

- Ensure that you have read and understood the fundamentals of WLAN configuration for wireless services. See Wireless LAN (WLAN) 8100 configuration overview on page 9.

  For further information, see *Feature Overview for Avaya WLAN 8100*, NN47251-102.
- Remove the WC 8180 device from its packaging. Ensure you have the following hardware components and materials:
  - Wireless Controller (WC) 8180 device
  - console cable
- Ensure that you have obtained a license and have applied it to the WLAN controller WC 8180. For more information on applying the controller license file, see Applying the Wireless Controller license file on page 18.

Procedure

1. Power on the WC 8180.
2. When the WC 8180 is up, connect the console cable.
3. Verify that the baud rate and other console parameters are properly configured. You can view console parameters using the PuTTY application.
   a. Open a PuTTY session.
   b. On the left-hand-side tree view, click **Serial**.
   c. Verify that the parameters are configured as follows:

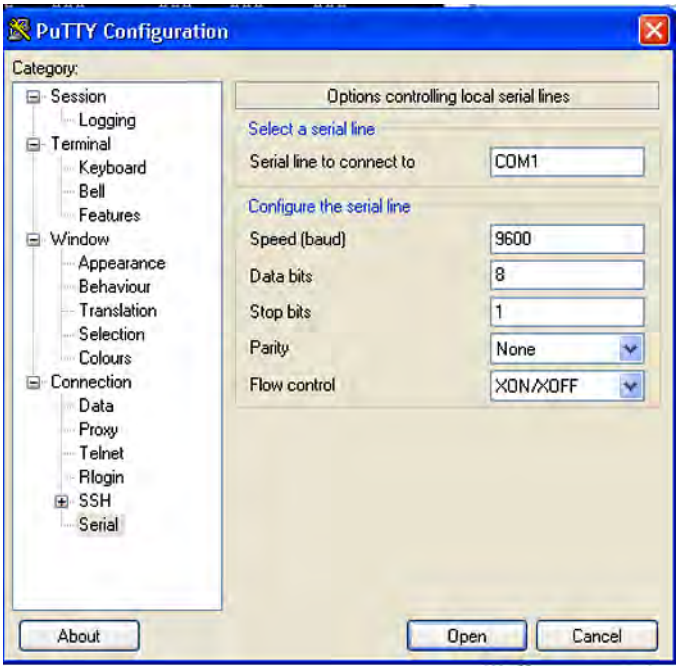


Figure 3: Console configuration

4. Press **Ctrl+Y** to start.
5. On the MENU screen, select **Command Line Interface** to go to the CLI.

   You are now connected to the WC 8180 device.
6. Configure the VLAN.

   The following example uses `VLAN 20` as the VLAN to provide management and wireless services.

```
WC8180>en
WC8180#configure t
Enter configuration commands, one per line. End with CNTL/Z.
WC8180(config)#vlan create 20 name mgmt-wireless type port
WC8180(config)#vlan members remove 1 1-26
WARNING: STP configuration may be lost on selected ports. You may
need to reconfigure the ports manually.
WC8180(config)#vlan members add 20 1-4
WC8180(config)#vlan mgmt 20
```

   Important:

   Before you create the management interface IP, you must create the management VLAN. After you create the interface IP, you cannot make further changes to the management VLAN.
7. Configure an IP interface for the VLAN.

```
WC8180(config)#interface vlan 20
WC8180(config-if)#ip address 20.20.20.45 255.255.255.0
WC8180(config-if)#exit
WC8180(config)#ip route 0.0.0.0 0.0.0.0 20.20.20.1 1
WC8180(config)#ip route 0.0.0.0 0.0.0.0 20.20.20.1 enable
```

```
WC8180(config)#ip routing
WC8180(config)#show ip route
================================================================================
                                                Ip Route
================================================================================
DST             MASK            NEXT            COST    VLAN PORT PROT TYPE PRF
--------------------------------------------------------------------------------
0.0.0.0         0.0.0.0         20.20.20.1      10       20   12    S  IB     5
20.20.20.0      255.255.255.0   20.20.20.45     1        20   ----  C  DB     0
Total Routes: 2
--------------------------------------------------------------------------------
TYPE Legend:
I=Indirect Route, D=Direct Route, A=Alternative Route, B=Best Route, E=Ecmp Route,
U=Unresolved Route, N=Not in HW
WC8180(config)#
```

Verify creation of the VLAN IP interface.

```
WC8180(config)#show vlan ip
================================================================================
Vid  ifIndex Address         Mask            MacAddress        Offset  Routing
================================================================================
Primary Interfaces
--------------------------------------------------------------------------------
20   10020   20.20.20.45     255.255.255.0   00:24:B5:1F:7F:80 1      Enabled
--------------------------------------------------------------------------------
% Total of Primary Interfaces: 1
WC8180(config)#
```

8. Enable TELNET and SNMP access.

```
WC8180(config)#
WC8180(config)#telnet-access enable
WC8180(config)#
WC8180(config)#snmp-server enable
WC8180(config)#
```

9. Verify controller connectivity with the L2 switch.

```
WC8180#ping 20.20.20.1
Host is reachable
WC8180#
```

10. Configure the Wireless system interface.

    Use `VLAN 20` for the Management interface, Wireless system interface and Wireless client connectivity. In large enterprise networks, these can be separate VLANs to isolate network management traffic from wireless traffic.

```
WC8180#conf t
Enter configuration commands, one per line.  End with CNTL Z.
WC8180(config)#wireless
WC8180(config-wireless)#interface-ip 20.20.20.45
```

11. Enable the wireless system interface configured in Step 9, using the following command input.

```
WCP8180(config)#wireless
WCP8180(config-wireless)#enable
```

    Verify that wireless system interface is configured and enabled.

```
WCP8180#show wireless
Operation Mode : WC
```

```
Status : Enabled
Interface IP : 20.20.20.45
TCP/UDP base port : 61000
Base MAC Address : 00:24:B5:1F:9F:00
WCP8180#
```

12. Configure the controller to be Mobility Domain Controller (MDC) capable.

```
WCP8180(config-wireless)#controller mdc-capable
% Domain password should be between 10-15 characters long.
% Password must contain a minimum of 2 upper, 2 lowercase letters
% 2 numbers and 2 special characters like !@#$%^&*()
Enter domain password: **********
Verify Domain password: **********
WCP8180(config-wireless)#
```

Verify that the controller is MDC-capable.

```
WCP8180#show wireless controller info
MDC-Capable : Enabled
WCP8180#
```

The WC 8180 is now provisioned for wireless services and to act as a wireless control point (WCP) in the mobility domain.

13. Create a mobility domain and join the controller with the mobility domain.

In this example, you create a mobility domain named `AVAYA`.

```
WCP8180#wireless controller join-domain domain-name AVAYA mdc-address 20.20.20.45
Enter Domain Secret: *****
Use 'show wireless controller domain-membership' to see join status.
WC8180#show wireless controller domain-membership
Domain Name             : AVAYA
Domain Role             : Active MDC
Domain Action Status    : Join Success
Action Failure Reason   : None
WCP8180#
```

Next steps

Continue configuration using one of the following interfaces:

- **CLI**: See Configuring the Wireless Controller — using the CLI on page 21
- **WLAN Management System (WMS)**: See Configuring the Wireless Controller — using the WMS on page 50
- **Enterprise Device Manager (EDM)**: See Configuring the Wireless Controller — using the EDM on page 76

Related Links

Applying a license file to a wireless controller on page 18

Applying a license file to a wireless controller

Use this procedure to apply a license file to the Wireless Controller (WC) 8180.

Before you begin

- Ensure that you have obtained the license file(s) for all controller(s) in your mobility domain, from Avaya Data Licensing portal. To obtain a license from the Avaya Data Licensing portal, see Obtaining licenses from the Avaya Data Licensing portal on page 108.
- Ensure that you have copied the license file(s) on to a TFTP server that the WC can reach, or you have stored the file(s) on a USB stick. This procedure provides the appropriate commands to apply the license file using the command line interface (CLI).

Procedure

1. Use Telnet or the console port on the WC to connect to the WLAN 8100 Controller CLI.
2. Log in as the Administrator if the user name and password is configured.
3. On the MENU screen of the WC 8180, select `Command Line Interface` to go to the CLI.
4. Apply the license file from a TFTP server. Execute the following command from the WLAN 8100 CLI in `privExec (#)` mode.

   ```
   copy tftp license address <IP Address> filename <License filename>
   ```

   where <IP Address> is the IP address of the TFTP server.

   Note:

   The correct license file contains the MAC address of the controller that the license file is being copied onto. After you download the licence file onto the WC, you must reboot the WC using the `boot` command.

5. Alternatively, execute the following command to apply the license file from a USB stick.

   ```
   copy usb license filename <License filename>
   ```

6. Verify that the license is installed correctly.

   ```
   WC8180#show wireless controller license-info
   Platform AP Capacity       : 512
   Licensed AP Capacity       : Unlimited
   AP License Count           : 64
   AP License Used Count      : 0
   WC8180#
   ```

   If the license is installed correctly, the `AP License Count` indicates the correct number of licensed access point (s) (AP) that can connect to the controller.

7. Read the WLAN 8100 online documentation for more detailed information and store your License Certificate in a secure place for future reference.

Example

In the following example, `640024B51F7F00.lic` is the 64 AP license file downloaded for the controller.

Use the following command to download the license file from a TFTP server (with IP address `20.20.20.9`).

```
WC8180#copy tftp license address 20.20.20.9 filename 640024B51F7F00.lic
License successfully downloaded.
NOTE:  system must be rebooted to activate license.
WC8180#boot Reboot the unit(s) (y/n) ? y Rebooting . . .
```

Use this command to download the license file from a USB stick.

```
WC8180#copy usb license filename 640024B51F7F00.lic
License successfully downloaded.
NOTE:  system must be rebooted to activate license.
WC8180#boot Reboot the unit(s) (y/n) ? yRebooting . . .
```

Related Links

Completing preliminary controller configuration on page 15

Chapter 5: Configuring the Wireless Controller — using the CLI

Use this procedure to configure the Wireless Controller (WC) 8180 using the Avaya command line interface (CLI).

Note:

This section describes the configuration of various WLAN features such as DiffServ, Client Band Steering, Station Isolation, Auto-RF, Client Load Balancing, Wi-Fi Zoning, LLDP support on AP, Bonjour Gateway support, LED management on a domain AP database and Remote Packet Capture using the CLI. It also describes how to enable support for third-party real-time location systems such as AeroScout and Ekahau.

For more information on the WLAN supported features, see:

- The *Feature Overview for Avaya WLAN 8100*, NN47251-102.
- The *ACLI Commands Reference for Avaya WLAN 8100*, NN47251-107, for a complete list of configuration commands for each of the features.

Before you begin

- Ensure that you complete the preliminary controller configuration using the CLI. See Completing preliminary controller configuration on page 15.

Procedure

1. Physically connect Access Points (AP) to the network.

   Note:

   The AP 8120 is powered by Power over Ethernet (PoE). You can connect a PoE switch or an external power injector to the AP.

2. Configure the DHCP server for AP discovery.

   The AP 8120discovers the controller IP addresses using DHCP option 43 or DNS.

   This example uses the DHCP option 43. The Option 43 setting must be `08 08 41 56 41 59 41 20 41 50 01 04 14 14 14 2D`, where `14 14 14 2D` is the HEX representation of the controller IP `20.20.20.45`. For details on how to configure the DHCP server, see DHCP server configuration for access points on page 105.

3. Discover the APs. Execute the following steps:
   a. Ensure the APs are connected to the DHCP server.
   b. Power on the APs by connecting them to the PoE switch or external power injector.

      When the AP receives the controller information from the DHCP server, it automatically connects to the controller and all discovered APs are placed in the Discovered AP database on the controller.
4. Verify that the connected APs are discovered by the controller.

```
WC8180(config-wireless)#show wireless domain ap discovered
Total number of discovered AP: 3
    ------------------------------------------------------------------------
    AP MAC            AP IP           Model   Serial Number
    ----------------- --------------- ------- --------------------------------
    00:24:B5:65:65:60 54.54.54.5      AP8120  LBNNTMJXAC004V
    00:24:B5:65:65:C0 54.54.54.6      AP8120  LBNNTMJXAC006L
    5C:E2:86:0F:51:60 54.54.54.8      AP8120  LBNNTMJXAC018N
    ------------------------------------------------------------------------
WC8180(config-wireless)#
```

5. Auto-promote discovered APs to be managed by the controller. All APs managed by the controller are populated in the Domain AP database.

   You can also, if required, manually add APs to the domain AP database (see Step 16 in this procedure).

   Note:

   Auto-promotion enables all discovered APs to be automatically promoted to the controller-managed state as soon as they are discovered.

```
WC8180(config-wireless)#
WC8180(config-wireless)#domain auto-promote-discovered-ap
% Warning: AP database will be synchronized after running config-sync
command.
WC8180(config-wireless)#
```

6. Display the AP status.

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

```
WC8180#show wireless ap status
Total APs: 3, Managed APs: 3, Failed APs: 0
    ------------------------------------------------------------------------------
    AP MAC             AP IP            Controller IP    Status        Need Image

                 Upgrade
    -----------------  ---------------  ---------------  -------------  ----------
    00:24:B5:65:65:60  54.54.54.5       20.20.20.45      Managed        Yes
    00:24:B5:65:65:C0  54.54.54.6       20.20.20.45      Managed        Yes
    5C:E2:86:0F:51:60  54.54.54.8       20.20.20.45      Managed        Yes
    ------------------------------------------------------------------------------
WC8180#
```

7. (Optional) Configure Wi-Fi Zoning on a specific radio, on a specific domain AP.

Note:

Alternatively, Wi-Fi Zoning can be configured for AP radios using radio profiles (see step 32 in this procedure for more details).

Wi-Fi Zoning enables you to control the physical region of connectivity around an access point (AP) by using the received signal strength indicator (RSSI) measurements of a clients 802.11 transmission as an indicator of its distance from the access point (AP).

Wi-Fi Zoning allows you to define a Wi-Fi association zone and a roaming zone around an AP in a mobility domain. These zones are specified using client RSSI thresholds value (in dBm) from the AP.

Note:

The allowed range for the Wi-Fi association zone and roaming zone thresholds is `-99` to `-1` dBm. The values `0` and `-100` dBm are used for disabling and auto-configuration, respectively. However, in current release the value `-100` dBm disables Wi-Fi zoning.

Choose a value depending on the physical distance between the APs and also the AP transmission power. The recommended range for optimal zoning is `-90` dBm to `-65` dBm. When you configure the Wi-Fi association zone and roaming zone thresholds for an AP, always ensure that the Wi-Fi association zone thresholds is greater than or equal to the Wi-Fi roaming zone thresholds. For example, if the Wi-Fi association zone thresholds is `-65` dBm, then configure the Wi-Fi roaming zone thresholds as either `-80` dBm or `-65` dBm.

For more information on Wi-Fi Zoning configuration, see *ACLI Commands Reference for Avaya WLAN 8100*, NN47251-107.

In this example, you configure the Wi-Fi association zone and roaming zone with threshold value `-50` dBm and `-65` dBm respectively, on radio 1 of the AP with MAC address `5C:E2:86:0F:51:60`.

```
WC8180(config-wireless)#domain ap 5C:E2:86:0F:51:60
Entering domain AP (mac = 5C:E2:86:0F:51:60) configuration mode..
```

```
WC8180(config-domain-ap)#radio ?
  <1-2>  Radio Interface
WC8180(config-domain-ap)#radio 1
WC8180(config-domain-ap)#radio 1 assoc-zone -50
WC8180(config-domain-ap)#radio 1 roam-zone -65
```

Verify Wi-Fi Zoning configuration on the domain AP.

```
WC8180#show wireless domain ap database 5C:E2:86:0F:51:60 detail
-------------------------------------------------------
AP MAC                  : 5C:E2:86:0F:51:60
   Label                :
   Model                : AP8120
   Country Code         : US
   Serial Number        : LBNNTMJXAC019M
   Profile ID           : 1
   Preferred Controller : 0.0.0.0
   Alternate Controller : 0.0.0.0
   Location
      Campus            :
```

```
      Building          :
      Floor             :
      Sector            :
   Radio 1
      Channel           : Automatic Adjustment
      Power             : Automatic Adjustment
      External Antenna  : N/A
      Extension Cable   : N/A
      Assoc-zone        : -50  dBm
      Roam-zone         : -65  dBm
      Admin-Enable      : True
   Radio 2
      Channel           : Automatic Adjustment
      Power             : Automatic Adjustment
      External Antenna  : N/A
      Extension Cable   : N/A
      Assoc-zone        : Auto
      Roam-zone         : Auto
      Admin-Enable      : True
-------------------------------------------------------
```

8. (Optional) You can control the state of LEDs (on or off) on a domain AP. For example, you can turn off LEDs on a domain AP so that people who are in the same location as the AP are not disturbed by either *blinking* or *on* LEDs.

   Note:

   By default, the **LED state** on a domain AP is set to `Normal(On)`, that is, the LED lights are turned on.

   Use the following command to turn off LEDs on a domain AP. In the following example, you update a domain AP with MAC address `5C:E2:86:0F:51:60`.

```
WC8180(config)#wireless
WC8180(config-wireless)#domain ap 5C:E2:86:0F:51:60
Entering domain AP (mac = 5C:E2:86:0F:51:60) configuration mode...
WC8180(config-domain-ap)#led-state off
```

   Perform a controller configuration synchronization to apply changes to the AP.

   Note:

   After you make changes to a domain AP, you do not need to reset the AP. From release 2.1 onwards, the wireless controller `config-sync` operation synchronizes configuration changes across the domain, and an AP reset is not required.

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

   Verify that the LED state on the domain AP is set to `Off`.

```
WC8180#show wireless domain ap database 5C:E2:86:0F:51:60 detail
```

```
-------------------------------------------------------
AP MAC                  : 5C:E2:86:0F:51:60
   Label                :
   Model                : AP8120-E
   Country Code         : VE
   Serial Number        : 11JX192F001P
   Profile ID           : 13
   Preferred Controller : 192.168.11.3
   Alternate Controller : 0.0.0.0
   LED-State            : Off
```

```
   Location
      Campus            :
      Building          :
      Floor             :
      Sector            :
   Radio 1
      Channel           : 36
      Power             : 60
      External Antenna  : WL81AT070E6
      Extension Cable   : 3-ft
      Assoc-zone        : Auto
      Roam-zone         : Auto
      Admin-Enable      : True
   Radio 2
      Channel           : 11
      Power             : 60
      External Antenna  : WL81AT070E6
      Extension Cable   : 3-ft
      Assoc-zone        : Auto
      Roam-zone         : Auto
      Admin-Enable      : True
-------------------------------------------------------
Total number of entries in AP database = 1
```

9. (Optional) Perform an AP image upgrade if an AP image upgrade is required. You can perform the image upgrade on a single AP or on all managed APs in the domain (bulk upgrade).

   Bulk AP image upgrade

```
WCP8180#
WCP8180#wireless domain ap image-update start
WCP8180#
```

   Single AP image upgrade

```
WCP8180#
WCP8180#wireless ap image-update ?
H.H.H  AP MAC Address
WCP8180#wireless ap image-update 00:24:B5:65:65:60
```

10. After you apply the image upgrade to the APs, verify the upgrade status. Verify that the `Need Image Upgrade` field is set to `No`.

```
WC8180#show wireless ap status
Total APs: 3, Managed APs: 3, Failed APs: 0
    ---------------------------------------------------------------------------
    AP MAC             AP IP            Controller IP    Status        Need Image

                  Upgrade
    -----------------  ---------------  ---------------  ------------  ----------
    00:24:B5:65:65:60  54.54.54.5       20.20.20.45      Managed        No
    00:24:B5:65:C0     54.54.54.6       20.20.20.45      Managed        No
    5C:E2:86:0F:51:60  54.54.54.8       20.20.20.45      Managed        No
    ---------------------------------------------------------------------------
WC8180#
```

11. Complete the following steps to create profiles (network, radio and AP profiles). These steps are provided for demonstration purposes.

Important:

When you configure profiles in the network (such as AP profiles, network profiles and radio profiles) ensure that you configure the profile name to be unique across the network, for each of the profiles.

Also ensure that you do not configure profile names that have similar characters or letters and differ only in their *case*.

12. Create a mobility VLAN.

    In this example, you configure a mobility VLAN named `Mobile-Clients`.

```
WC8180(config-wireless)#
WC8180(config-wireless)#domain mobility-vlan Mobile-Clients
WC8180(config-wireless)#
WC8180(config-wireless)#show wireless domain mobility-vlan
    ------------------------------------------------
    Mobility VLAN Name                Status
    --------------------------------  ----------------
    default-MVLAN                     Active
    Mobile-Clients                    Active
    ------------------------------------------------
WC8180(config-wireless)#
```

13. (optional) Configure multicast DNS relaying in WC.

    a. Enable mDNS relay across the VLANs.

```
WC8180(config-mDNS)# mDNS-relay enable
WC8180#show wire multicast-dNS
multicast DNS Relay Mode: Enabled
```

    b. Configure required mobility VLANs under Scan-list and enable relaying of multicast DNS traffic across these MVLANs.

    In this example, you configure a mobility VLAN named `Mobile-Clients` under Scan-list.

```
WC8180(config-mDNS)# scan-list Mobile-Clients
WC8180#show wire multicast-dNS scan-list
--------------------------------
Vlan Name
--------------------------------
Mobile-Clients
--------------------------------
```

    c. Use this command to enable an existing Filter-rule:

```
WC8180(config-mDNS)# filter-rule <filter-rule name> state <enable>
```

    Note:

    By default, Filter-rules *airplay, airprint, and raop* are in enable state and the remaining are in disabled state.

    d. (optional) Enable Location-based-relay.

Note:

Configure location (*campus, building, floor and sector*) parameters in the AP database.

```
WC8180(config-mDNS)# location-based-relay enable
Wc8180#show wireless multicast-dNS location-based-relay
multicast DNS location based Relay Mode: Enabled
```

14. Configure an authentication RADIUS profile.

    Radius profiles are associated with Radius servers for authentication of wireless clients. In this example, you create a RADIUS profile named `rad-srvr-profile`.

    ```
    WCP8180(config-security)#radius profile rad-srvr-profile type auth
    ```

    Configure RADIUS server selection based on priority:

    ```
    WC8180(config-security)#radius profile rad-srvr-profile type auth server-selection
    priority
    ```

    Verify creation of the RADIUS profile.

    ```
    WCP8180#show wireless security radius profile

    Total radius profiles: 1, auth: 1, acct: 0
    Radius Profile                  Type            Server-selection
    ------------------------------- ------------------------------
    rad-srvr-profile                Authentication    Priority
    WCP8180#
    ```

15. Configure the RADIUS servers (IP addresses `10.1.1.104`).

    RADIUS servers manage authentication of users and devices connected to the wireless network.

    Use the following commands to configure mandatory health-check and server selection parameters for both the RADIUS servers.

    a. Configure the server priority for the RADIUS servers.

       Enter a priority number in the range `1` to `65535`.

       ```
       WC8180(config-security)#radius server 10.1.1.104 rad-srvr-profile priority 1
       ```

    b. Configure the RADIUS server secret.

       ```
       WC8180(config-security)#radius server 10.1.1.104 rad-srvr-profile secret

       Enter server secret: ********
       Verify server secret: ********
       ```

    c. Configure the health check interval.

       Enter a time in seconds and in the range `0` to `100`. A value of `0` indicates that health check is disabled.

       ```
       WC8180(config-security)#radius server 10.1.1.104 rad-srvr-profile health-check-
       interval 2
       ```

    d. Configure the health-check user name and password (for the user name):

       ```
       WC8180(config-security)#radius server 10.1.1.104 rad-srvr-profile health-check-
       user <user-name-1>
       ```

```
WC8180(config-security)#radius server 10.1.1.104 rad-srvr-profile health-check-
password
Enter health check password: ******
```

Verify RADIUS server configuration:

```
WC8180#show wireless security radius server

Total radius servers: 1
Server IP       Radius Profile                   Port# Priority Status
--------------- -------------------------------- ----- -------- -------
10.1.1.104      rad-srvr-profile                 1812  1        UP
WC8180#
```

16. Configure the Captive Portal (CP) profile `PRF-CP` using the following command input.

    Important:

    For the Captive Portal to work properly, ensure that the Wireless or System interface of the AMDC does not have the `Management` flag enabled.

    Important:

    If you want to host the Captive Portal on a guest VLAN, ensure that the Captive Portal IP address is an active VLAN interface IP on any controller in the domain, except the Management VLAN IP address, the System VLAN IP address, or the wireless interface IP address of that controller. The Captive Portal IP address must physically exist on one of the domain controllers.

```
WCP8180(config-wireless)#captive-portal enable

WCP8180(config-wireless)#captive-portal profile 1
Entering captive-portal-profile (id = 1) ...

WCP8180(config-cp-profile)#profile-name PRF-CP
```

Verify creation of the CP profile.

```
WCP8180#show wireless captive-portal profile
-------------------------------------------------------------------
Id   Profile Name                      Protocol Mode  User Logout
---  --------------------------------  -------------  -----------
 1   PRF-CP                              http          Enabled
-------------------------------------------------------------------
Total number of captive portal profile: 1
```

17. Configure the Captive Portal (CP) user database using the following command input:

    To configure the Captive Portal user database, you:

    - Create a user group.
    - Create a Client Portal user and add the user to the user group (configure membership).

    Note:

    You can create a maximum of 10 user groups and assign up to 1000 users to each user group.

```
WCP8180(config-security)#user-db group UG-guest

WCP8180(config-security)#user-db user-name guest password
```

```
Enter user password: ********
Verify user password: ********

WCP8180(config-security)#user-db membership guest  UG-guest
```

Important:

When you configure a Captive Portal user, if you optionally configure the `Auth Start Date` and `Auth End Date` parameters, ensure that you first *reset* the dates before you configure the new dates.

You can reset the dates using the following commands:

```
WCP8180(config-security)#no user-db user-name guest start-date
WCP8180(config-security)#no user-db user-name guest end-date
```

Verify user group creation.

```
WCP8180#show wireless security user-db group

User group
--------------------------------
Default
UG-guest

WCP8180#
```

Verify user creation.

```
WCP8180#show wireless security user-db user-name

Total local user: 1

  User name:                guest
  Session Timeout(sec.):    0
  Idle Timeout(sec.):       0
  Max BW Up(bps):           0
  Max BW Down (bps):        0
  Max In Octets:            0
  Max Out Octets:           0
  Max Total Octets:         0
  Auth Start Date:          0000-0-0
  Auth End Date:            0000-0-0

WCP8180#
```

Verify membership of user in user group.

```
WCP8180#show wireless security user-db membership
User                            Group
------------------------------- --------------------------------
default                         Default
guest                           UG-guest

WCP8180#
```

18. (Optional) Configure Captive Portal Walled Garden hosts for Captive Portal users in the Captive Portal profile.

    Sometimes, a Captive Portal user may need to access network resources in the intranet or public Web sites from an enterprise network, without requiring to first undergo Captive Portal authentication. To support these user requirements, the WLAN 8100 allows configuration of

IP addresses of Web hosts in a Captive Portal profile so that the user can access these hosts without the need for authentication. This is known as the Captive Portal Walled Garden.

Configure the Walled Garden host names (IP addresses). In the following example, `74.125.226.198` is a sample IP address of a Web host server.

```
WCP8180(config-wireless)#captive-portal profile 1
Entering captive-portal-profile (id = 1) ...
WCP8180(config-cp-profile)#walled-garden hostname 74.125.226.198
```

Configure the Walled Garden host type.

Important:

The Walled Garden host type currently supported is the IP address.

```
WC8180(config-cp-profile)#walled-garden hostname 74.125.226.198 type ip-addr
```

19. (Optional) Configure Diffserv (Differentiated services). DiffServ specifies a simple and scalable mechanism for classifying and managing network traffic and providing quality of service (QoS) to wireless clients, on modern IP networks.

    Important:

    Ensure that you configure DiffServ policy and classifier block names that are unique across the network. Do not configure policy and classifier names that have similar letters and characters and differ only in their *case*.

    Configure a Diffserv classifier block named `classifier1` using the following command.

    In this example, you configure a classifier block element to match the client MAC address `01:02:03:04:05:06`. The corresponding subnet mask used is `ff:ff:ff:ff:ff:ff`. Replace these values with those appropriate to your network.

    ```
    WC8180(config)#wireless
    WC8180(config-wireless)#diffserv classifierblock classsifier1
    WC8180(config-diffserv-classifierelement)#match src-mac 01:02:03:04:05:06 mask
    ff:ff:ff:ff:ff:ff
    ```

    You can configure other DiffServ classifier block options (elements) as required.

    For example, you can use the following commands to configure classifier block elements to match the client source IP address (`src-ip`), destination IP address (`dest-ip`) or Ethernet Type (`ethtype`).

    ```
    WC8180(config-diffserv-classifierelement)#match dst-ip ?
      A.B.C.D
    ```

    ```
    WC8180(config-diffserv-classifierelement)#match src-ip ?
      A.B.C.D
    ```

    ```
    WC8180(config-diffserv-classifierelement)#match ethtype ?
      <0x600-0xFFFF>  Ethernet Type in HEX
    ```

Important:

Considerations when configuring classifier block elements:

- When you configure a classifier block to match the source/destination client IP address or a client MAC address, you must configure a proper mask to ensure that the classifier block is applied to traffic from only the specified client and not all clients within the subnet.

  For example, if you configure the classifier block to *drop* packets for a client IP address of `10.1.20.5`, a mask of `255.255.255.0` drops the packets on **all** clients within the subnet. To ensure that the packets are dropped for traffic from only the specified client, you must set the mask to `255.255.255.255`.

  Similarly, if you configure a classifier block for a a client MAC address `01:02:03:04:05:06`, for example, ensure that you set the subnet mask to `ff:ff:ff:ff:ff:ff`.

- When you configure a classifier block, you can configure any value for `EthType` parameter. However, only if you set the `EthType` parameter to `0x0800` (hex), you can configure other classifier block parameters such as `protocol`, `dest-ip`, `src-ip`, `ipDscp`, `IpPrescedence` `IpTos`, `src-port` and `dst-port`.

20. (Optional) Configure a Diffserv policy named `policy1` and associate the configured classifier block `classifier1` with this policy. Use the following command:

    In this example, `allow` is a sample action associated with the classifier block `classifier1`. The `allow` action allows packets or traffic that match the criteria specified in the classifier block configured in Step 15.

    ```
    WC8180(config-diffserv-classifierelement)#diffserv policy policy1
    WC8180(config-diffserv-policy)#classifierblock classifier1 allow
    ```

21. (Optional) Verify Diffserv classifier details. Use one off the following commands.

    Command with sample output:

    ```
    WCP8180#sh wireless diffserv classifierblock
    Classifier Blocks
    -----------------
    c1
    Total number of classifier blocks: 1
    ```

    Command with sample output:

    ```
    WCP8180(config-diffserv-policy)#show wireless diffserv classifierblock classifier1
    detail
    Classifier block classifier1
    ------------------------
    Element ID: 1
    Src Mac:          01:02:03:04:05:06
    Src Mac Mask:     FF:FF:FF:FF:FF:FF
    ```

22. (Optional) Verify Diffserv policy details. Use one of the following commands.

Command with sample output:

```
WCP8180#sh wireless diffserv policy
Policy Names
----------------------------
p1

Total number of policies: 1
```

Command with sample output:

```
WCP8180(config-diffserv-policy)#show wireless diffserv policy policy1 detail
Policy Name                    Classifierblocks          Action
-------------------         ---------------------------    --------
policy1                        classifier1               Allow
```

23. (Optional) Associate the DiffServ classifier block with the DiffServ policy.

```
WCP8180(config-wireless)#diffserv policy p1
Diffserv policy exists - 10
WCP8180(config-diffserv-policy)#classifierblock c1 remark-cos 6?
WC8180(config-diffserv-policy)#classifierblock c1 remark-dscp 46
```

Important:

If you use a DSCP value of `48/56` and a cos value of `7`, the Access Point (AP) overrides the DSCP priority and changes its priority to `0`. This causes a change in the traffic priority.

Some DSCP priorities are specifically marked for network control traffic and these DSCP priorities must not be used in uplink traffic from wireless clients. The set of DSCP priorities that are overridden by the AP is implicitly derived from the *QoS egressmap* table maintained in the AP. All DSCP priorities mapped to 802.1p priority 7 are considered to be network control packet priority. For the default QoS egressmap, DSCP priorities 48 and 56 are considered as network control packet priorities and are overridden on the client generated uplink packets.

When an AP detects client packets with DSCP values set to a network control packet priority, the AP resets the DSCP value on those packets to 0.

For more information on the *QoS egressmap* table and the WLAN 8100 DSCP priority, see the *Feature Overview for Avaya WLAN 8100*, NN47251-102.

24. Configure a network profile.

In this example, you configure a network profile named `AVAYA-Demo` and associate it with the mobility VLAN `Mobile-Clients`. You also associate the Captive Portal profile with this network profile.

Important:

When you configure an SSID for a network profile, ensure that it is unique across the network. SSIDs can have a maximum of 32 characters.

Also, ensure that you do not configure SSIDs that have similar characters but are different only in their *case*. For example do not configure SSIDs *avaya-demo* and *AVAYA-DEMO* within the same network.

```
WC8180(config-wireless)#network-profile 2
Creating network-profile (id = 2) ...
WC8180(config-network-profile)#profile-name AVAYA-Demo
WC8180(config-network-profile)#ssid AVAYA-Demo
WC8180(config-network-profile)#mobility-vlan Mobile-Clients
WC8180(config-network-profile)#security-mode wpa-enterprise
WC8180(config-network-profile)#captive-portal enable profile-id 1
WC8180(config-network-profile)#exit
```

Verify creation of the network profile.

```
WC8180(config-wireless)# WC8180(config-wireless)#show wireless network-profile 2
------------------------------------------------------------------------
Id  Profile Name        Mobility VLAN       Security Mode  Captive Portal
-- ------------------ ------------------ -------------- --------------
2 AVAYA-Demo           Mobile-Clients      wpa-enterprise      Enabled
------------------------------------------------------------------------
WC8180(config-wireless)#

WC8180(config-wireless)#show wireless network-profile 2 detail
    Network Profile ID                              : 2
    Name                                : AVAYA-Demo
    SSID                                : AVAYA-Demo
    Hide SSID                           : No
    Mobility Vlan Name                  : Mobile-Clients
    No Response to Probe Request        : Disabled
    Captive Portal Mode                 : Enabled
    User Validation                     : open
    Captive Portal Profile Id           : 1
    Local User Group                    : Default
    RADIUS Authentication Profile Name  :
    RADIUS Accounting Profile Name      :
    RADIUS Accounting Mode              : Disabled
    Security Mode                       : wpa-enterprise
    MAC Validation                      : Disabled
    Wireless ARP Suppression            : Disabled
WC8180(config-wireless)#
```

25. (Optional) Enable MAC validation on the network profile, for validation of client devices in the network using MAC addresses.

    The current release supports MAC validation against a local whitelist database or against a remote RADIUS server. You can choose one of the following methods of MAC validation.

    - **Validation against a local whitelist**:

      Use the following command to set the MAC validation mode as `local-whitelist` in the network profile.

      In the following example, you set the MAC validation mode as `local-whitelist` on the network profile `NP-employee`.

      ```
      WC8180(config-wireless)#network-profile 2
      Entering network-profile (id = 2)configuration mode...
      WC8180(config-network-profile)#mac-validation mode local-whitelist
      ```

Important:

When MAC validation is enabled, all wireless clients are blacklisted by default. To enable the client to access the wireless network, you must manually add the client MAC address to the whitelist table. Whitelist clients are displayed as `known` in the detected client table.

Configure a whitelist and blacklist device database to support client device MAC validation.

Configure blacklist device database using the following command:

- Configure a whitelist device database using the following command.

  Note:

  When you configure whitelist devices, you can optionally configure a device name. Enter a string with a maximum length of 32 characters that is unique across the network.

  Ensure also that you do not configure device names that have similar characters or letters but differ only in their *case*.

  In the following example, you configure a sample whitelist device with MAC address `00:11:22:33:44:55` and name `whitelist-device1`.

```
WC8180(config-security)#mac-db whitelist 00:11:22:33:44:55 name whitelist-
device1
```

  Verify whitelist device configuration using the following command:

```
WCP8180#show wireless security mac-db whitelist
```

- Enable blacklist MAC filtering and configure a blacklist device database using the following commands:

  Enable blacklist MAC filtering:

```
WC8180(config-security)#mac-filter-blacklist
```

  Configure a blacklist device database using the following command. In this example, you configure a sample blacklist device with MAC address `00:11:22:33:44:66` and name `blacklist-device1`.

```
WC8180(config-security)#mac-db blacklist 00:11:22:33:44:66 name blacklist-
device1
```

  Note:

  Ensure that blacklisted client device name has a maximum length of 32 characters that is unique across the network. Ensure also that you do not configure device names that have similar characters or letters but differ only in their *case*.

  Verify blacklist MAC filtering and blacklist device configuration using the following commands:

```
WCP8180#show wireless security mac-db blacklist
```

```
WCP8180#show wireless security mac-filter-blacklist
```

- **Validation against a remote RADIUS server**:

  When the MAC-validation mode is configured as **Radius**, then MAC address of a client device is verified against a remote database interfaced by a RADIUS server. This is useful in enterprise networks that support the Bring Your Own Device (BYOD) policy, personally-owned devices, IT issued devices and guests.

  Note:

  MAC-Validation mode cannot be configured as **Radius** when the security mode configured in a network profile is one of the following:

  - WPA or WPA2 enterprise
  - 802.1X (Dynamic Wep)

  To configure the MAC-validation mode as **Radius**, the network profile must be configured with one of the following security modes:

  - wpa-personal
  - wep-static
  - open

  Important:

  Ensure that the MAC addresses of wireless client devices (to be validated against the RADIUS server) are configured on the RADIUS server. Ensure also that the MAC addresses are configured on the RADIUS server in the format `aabbccddeeff`, that is without colons and in small letters.

- Use the following command to set the MAC validation mode as `radius` in the network profile.

  In the following example, you configure the MAC validation mode as `radius` on the network profile `NP-guest` with the security mode as `open`.

```
 WC8180(config-wireless)#network-profile 4
Entering network-profile (id = 4)configuration mode...
WC8180(config-network-profile)#mac-validation mode radius
```

- Map the RADIUS profile `rad-srvr-profile` configured in step 2, to the employee network profile `NP-guest` configured in step 15.

```
WC8180(config-network-profile)#radius authentication-profile rad-srvr-profile
```

For more information on configuration for radius profile and server details, see *ACLI Commands Reference for Avaya WLAN 8100*, NN47251-107.

26. (Optional) Enable Station Isolation on the network profile `network-profile 2`.

```
WC8180(config-wireless)#network-profile 2
Entering network-profile (id = 2)configuration mode...
WC8180(config-network-profile)#station-isolation enable
WC8180(config-network-profile)#end
```

Verify that Station Isolation is enabled on the Network profile.

```
WC8180#show wireless network-profile 2
```

```
-------------------------------------------------------------------------------
---------
Id  Profile Name        Mobility VLAN       Security Mode  Captive Portal  Station
Isolation
-- ------------------- ------------------- -------------- ---------------
----------------
2   AVAYA-Demo          Mobile-Clients      open           Enabled
Enabled
-------------------------------------------------------------------------------
---------
```

```
WC8180(config-wireless)#show wireless network-profile 2 detail
Network Profile ID                                  : 2
Name                                : AVAYA-Demo
SSID                                : AVAYA-Demo
Hide SSID                           : No
Mobility Vlan Name                  : Mobile-Clients
No Response to Probe Request        : Disabled
Captive Portal Mode                 : Enabled
User Validation                     : open
Captive Portal Profile Id           : 1
Local User Group                    : Default
RADIUS Authentication Profile Name  :
RADIUS Accounting Profile Name      :
RADIUS Accounting Mode              : Disabled
Security Mode                       : open
MAC Validation                      : Disabled
Wireless ARP Suppression            : Disabled
Raduis offload                                      : Disabled
Station Isolation Mode              : Enabled
```

27. Enable **client-QoS** and Domain **AP-client-QoS** and map the created Diffserv policy to the `AVAYA-Demo` network profile, to prioritize WMM (Wireless Multi-Media) traffic in the network. By default, in WMM, voice traffic has a higher priority over video traffic. You can, for example, configure DiffServ policies to reverse this traffic priority in the network.

    For example, to enable client QOS and configure the DiffServ policy `policy1` on the network profile, execute the following commands.

```
WC8180(config-wireless)#network-profile 2
Creating network-profile (id = 2) ...
WC8180(config-network-profile)#client-qos enable
WC8180(config-network-profile)#client-qos diffserv {up} policy1
```

Verify the network profile client-QOS. Use the following command:

```
WC8180(config-network-profile)#show wireless network-profile client-qos 2
```

```
-------------------------------------------------------------
 Network   Client             Diffserv Policy Name
 Profile    QoS     ------------------------------------
   Id       Mode           Down                 Up
--------  --------  ------------------  ------------------
    2     Enabled                          policy1
-------------------------------------------------------------
```

Enable AP-client-QoS:

```
WC8180#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
WC8180(config)#wireless
WC8180(config-wireless)#domain ap-client-qos
WC8180(config-wireless)#
```

Verify AP-client-QoS mode:

```
WC8180#show wireless domain info
  Country Code                        : US
  AP QoS Mode                         : Enabled
  Roaming Timeout                     : 30 seconds
  TSPEC Violation Report Interval     : 300 seconds
  Auto Promote for Discovered APs     : Disabled
  AP Image Update Download Group Size : 5 %
  AP Image Update Reset Group Size    : 5 %
  AP Reset Group Size                 : 5 %
  AP Reconnection Timeout Interval    : 60
  Configured Load Balancing Metric    : least-load
```

28. Associate the configured Captive Portal profile `PRF-CP` with the network profile `AVAYA-Demo`.

```
WC8180(config-wireless)#network-profile 2
Creating network-profile (id = 2) ...
WC8180(config-network-profile)#captive-portal enable profile-id 1
WC8180(config-network-profile)#user-validation local
WC8180(config-network-profile)#user-group UG-guest
```

To view a network profile by network profile ID, use the following command. For example, view the `Avaya-Demo` network profile.

```
WC8180#show wireless network-profile 2
------------------------------------------------------------------------
Id  Profile Name        Mobility VLAN       Security Mode  Captive Portal
--- ------------------- ------------------- -------------- --------------
  2 NP-employee         MV-EMP              wpa-enterprise    Enabled
------------------------------------------------------------------------
WC8180#
```

29. Use one of the following commands to view the Captive Portal network status.

```
show wireless captive-portal network-status
show wireless captive-portal network-status CP-profile <CP-profile-Id>  network-
profile <network-profile-id>
show wireless captive-portal network-status network-profile <network-profile-id>
CP-profile <CP-profile-Id>
```

30. Configure the Access radio profiles (RP) using the following command input. Configure `A-N` and `BG-N` radio profiles to support different radio frequencies.

The following examples shows the creation of `A-N` and `BG-N` radio profiles with the country code specified as `US` and the AP model specified as `ap8120/E`. For an outdoor AP, specify the AP model as `ap8120-O` in the command.

```
WC8180(config-wireless)#radio-profile 3 country-code US ap-model ap8120/E access-
wids a-n
Creating a radio-profile (id = 3) with country-code = US and ap-model AP8120/E...
WC8180(config-radio-profile)#profile-name A-N
WC8180(config-radio-profile)#exit
```

```
WC8180(config-wireless)#radio-profile 4 country-code US ap-model ap8120/E access-
wids bg-n
Creating a radio-profile (id = 4) with country-code = US and ap-model AP8120/E...
WC8180(config-radio-profile)#profile-name BG-N
WC8180(config-radio-profile)#exit
```

31. Verify creation of all radio profiles using the following command.

```
WC8180(config-radio-profile)#show wireless radio-profile
-------------------------------------------------------------------------
Id   Profile Name       AP         802.11        Operation    Auto
                       Model       Mode           Mode       Ch.
-- ------------------------------ --------- --------------- --------
1  Default-5GHz       AP8120/E  802.11a/n       access-wids  Yes
2  Default-2dot4GHz   AP8120/E  802.11bg/n      access-wids  Yes
3  A-N                AP8120/E  802.11a/n       access-wids  Yes
4  BG-N               AP8120/E  802.11bg/n      access-wids  Yes
-------------------------------------------------------------------------
Total number of radio profiles: 4
```

To view the radio profile configuration in detail, use the command:

```
show wireless radio-profile <profile Id> detail
```

32. Enable Client band steering and load balancing on the configured Access radio profiles.

Client Band Steering is a technique used to increase the overall capacity of a dual-band wireless network composed of multiple APs that use both the 2.4 GHz and 5.0 GHz radios.

Client stations predominantly support 2.4GHz. Many modern client stations have dual-band support yet tend to favor connection to 2.4GHz networks (although some popular modern clients still only support 2.4GHz, e.g. the Apple iPhone 4). As a result, dual-band networks have the 2.4GHz band heavily utilized, and the 5GHz band under utilized. The objective of Client Band Steering is to encourage 5GHz capable client stations to use the 5GHz radio instead of the 2.4GHz radio, leaving the 2.4GHz radio for stations that only support 2.4GHz.

As part of Client load-balancing configuration, you enable/disable the Load balancing. After you enable load balancing, you configure the following parameters:

- utilization-start (%) — Utilization level at which client association load balancing begins
- utilization-cutoff (%) — Client association load balancing cutoff. If this threshold is exceeded, all further client associations are refused.

Note:

This cutoff is useful so that controller CPU utilization is maintained at an optimum level. If CPU utilization goes beyond 100%, it causes the controller to restart which in turn results in an unprecedented controller outage.

Enable client band steering and load balancing using the following commands:

```
WC8180(config-wireless)#radio-profile 3
Entering radio-profile (id = 3) configuration mode...
WC8180(config-radio-profile)#band-steering enable
WC8180(config-radio-profile)#load-balance enable
WC8180(config-radio-profile)#load-balance utilization-start 30
WC8180(config-radio-profile)#load-balance utilization-cutoff 60
```

```
WC8180(config-wireless)#radio-profile 4
Entering radio-profile (id = 3) configuration mode...
WC8180(config-radio-profile)#band-steering enable
WC8180(config-radio-profile)#load-balance enable
WC8180(config-radio-profile)#load-balance utilization-start 30
WC8180(config-radio-profile)#load-balance utilization-cutoff 60
```

33. (Optional) Configure Wi-Fi Zoning on the configured Access radio profiles. Alternatively, Wi-Fi Zoning can be configured individually for each AP radio using the domain AP database (see step 7).

    Wi-Fi Zoning allows you to define a Wi-Fi association zone and a roaming zone around an AP in the mobility domain. These zones are specified using client RSSI thresholds value in dBm from the AP. The allowed range for both association zone and roaming zone thresholds is from `−99` to `-1` dBm. The values `0` and `-100` dBm are used for disabling and auto-configuration, respectively. However, in current release the value `-100` dBm disables Wi-Fi zoning. Choose a value depending on the physical distance between the APs and also the AP transmission power. The recommended range for optimal zoning is `-90` dBm to `-65` dBm.

    Note:

    When you configure the Wi-Fi association zone and roaming zone thresholds for an AP, always ensure that the Wi-Fi association zone thresholds is greater than or equal to the Wi-Fi roaming zone thresholds. For example, if Wi-Fi association zone thresholds value is `-65` dBm, then configure Wi-Fi roaming zone with thresholds value `-80` dBm or `-65` dBm.

    In the following example, you Configure Wi-Fi association zone and roaming zone on a radio profile named `BG-N` with profile ID `4` .

```
WC8180(config-wireless)#radio-profile 4
Entering radio-profile (id = 4) configuration mode...
```

```
WC8180(config-radio-profile)#assoc-zone ?
<-100 - 0> Enter the RSSI value in dBM.0(Disabled), -1 to -99, -100(Auto)
WC8180(config-radio-profile)#assoc-zone -50
WC8180(config-radio-profile)#roam-zone ?
<-100 - 0> Enter the RSSI value in dBM.0(Disabled), -1 to -99, -100(Auto)
WC8180(config-radio-profile)#roam-zone -50
```

    Verify Wi-Fi association zone and roaming zone configuration on the radio profile in detail.

```
WC8180#show wireless radio-profile 4 detail
```

    Sample Output:

```
WC8180(config-radio-profile)#show wireless radio-profile 20 detail
Radio Profile Id: 4
    Name                                  : BG-N
    Configuration Model                   : AP8120/E
    Country Code                          : US
    Operation Mode                        : access-wids
    IEEE 802.11 Mode                      : 802.11bg/n
    RF Scan - Duration                    : 10 msec
    RF Scan - Other Channels              : Yes
    RF Scan - Other Channels Scan Interval : 60 sec
    Broadcast/Multicast Rate Limiting     : Disabled
    Broadcast/Multicast Rate Limit (Normal): 50 pkts/sec
    Broadcast/Multicast Rate Limit (Burst) : 75 pkts/sec
    Beacon Interval                       : 100 msec
    DTIM Period                           : 3
    Fragmentation Threshold               : 2346
    RTS Threshold                         : 2347
    Short Retry Limit                     : 7
    Long Retry Limit                      : 4
    Max Transmit Lifetime                 : 512 msec
```

```
    Max Receive Lifetime                    : 512 msec
    Max Clients                             : 200
    Auto Channel Adjustment Mode            : Yes
    Auto Power Adjustment Mode              : Yes
    Auto Power Minimum                      : 40 %
    Non-Auto Transmit Power                 : 80 %
    WMM(Wi-Fi Multimedia Mode)              : Enabled
    Band Steering Mode                      : Disabled
    Load Balancing Mode                     : Disabled
    Load Balance Utilization Start          : 30 %
    Load Balance Utilization Threshold      : 60 %
    Channel Bandwidth                       : 40 MHz
    Primary Channel                         : Lower
    802.11n Protection Mode                 : Auto
    SGI(Short Guard Interval)               : Enabled
    STBC(Space Time Block Code) Mode        : Enabled
    Multicast Transmit Rate                 : Auto
    APSD(Auto Power Save Delivery) Mode     : Enabled
    No ACK for Incorrectly Received Frames : Disabled
    RRM(Radio Resource Measurement)         : Enabled
    Association Zone Threshold              : -50 (dBm)
    Roaming Zone Threshold                  : -50 (dBm)
```

34. Create an AP profile and assign network and radio profiles to it.

    In the following example, you create an AP profile named `AP-Profile-1`.

```
WC8180(config-wireless)#ap-profile 2
Creating ap-profile (id = 2) ...
WC8180(config-ap-profile)#profile-name AP-Profile-1
WC8180(config-ap-profile)#radio 1 profile-id 3 enable
WC8180(config-ap-profile)#radio 2 profile-id 4 enable
WC8180(config-ap-profile)#network 1 1 profile-id 2
WC8180(config-ap-profile)#network 2 1 profile-id 2
WC8180(config-ap-profile)#exit
```

```
WC8180(config-wireless)#show wireless ap-profile network 2
    ------------------------------------------------------------------
    AP Profile Id  Radio Id  VAP Id  Network Profile Id  Radio Operation
    -------------  --------  ------  ------------------  ---------------
    2                 1                1                   2           On
    2                 2               1                   2           On
    ------------------------------------------------------------------
    WC8180(config-wireless)#show wireless ap-profile radio 2
    ---------------------------------------------------
    AP Profile Id  Radio Id  Radio Profile Id  Radio Status
    -------------  --------  ----------------  ------------
    2                 1                3               On
    2                   2                4                   On
    ---------------------------------------------------
```

35. (Optional) Enable AeroScout real-time location system (RTLS) support on the AP profile named `AP-Profile-1`.

    Important:

    You can enable AeroScout support only on indoor APs. It is not supported on the AP 8120–O, which is an outdoor AP.

```
WC8180(config-wireless)#ap-profile 2
Entering ap-profile (id = 2) configuration mode..
WC8180(config-ap-profile)#aeroscout enable
```

Verify that AeroScout is enabled on the AP profile.

```
WC8180#show wireless ap-profile 2 detail
AP Profile Id: 2
    Name                : AP-Profile-1
    Country Code        : IN
    AP Model            : Avaya APs (AP8120/AP8120-E)
    Is Default Profile? : No
    AE Protocol Support : Enable
    Status              : Associated & Modified
```

36. (Optional) Enable LLDP operation on an AP.

```
WC8180(config-wireless)#ap-profile 1
Entering ap-profile (id = 1) configuration mode..
WC8180(config-ap-profile)#lldp-status ?
   rxOnly Enable receive only
   txAndRx Enable transmit and receive
   txOnly Enable transmit only
WC8180(config-ap-profile)#lldp-status rxOnly
```

Verify that LLDP is enabled on the AP profile.

```
WC8180(config-ap-profile)#show wireless ap-profile 1 detail
   AP Profile Id: 1
   Name : Default
   Country Code : US
   AP Model : Avaya APs (AP8120/AP8120-E)
   Is Default Profile? : No
   AE Protocol Support : Disable
   Ekahau Tag Blink Mode : Disable
   Ekahau Server IP : 0.0.0.0
   Ekahau Server UDP Port : 8569
   LLDP status : rxOnly
   Status : Configured
```

For more information on LLDP configuration, see *Avaya WLAN 8100 CLI Reference* , NN47251–107.

37. (Optional) Enable Ekahau RTLS support on the AP profile named `AP-Profile-1`.

    Important:

    You can enable Ekahau support only on indoor APs. It is not supported on the AP 8120–O, which is an outdoor AP.

```
WC8180(config-wireless)#ap-profile 2
Entering ap-profile (id = 2) configuration mode..
WC8180(config-ap-profile)#ekahau enable
```

Verify that Ekahau support is enabled on the AP profile.

```
WC8180#show wireless ap-profile 2 detail
AP Profile Id: 2
    Name                    : AP-Profile-1
    Country Code            : IN
    AP Model                : Avaya APs (AP8120/AP8120-E)
    Is Default Profile?     : No
    Ekahau Protocol Support : Enable
    Status                  : Associated & Modified
```

38. (Optional) Configure Auto-RF channel plan and power plan.

Configure the Auto-RF channel-plan for the `a-n` and `bg-n` radio frequency bands, using the following options:

```
WC8180(config-wireless)#auto-rf channel-plan a-n ?
  history-depth  Set channel plan history depth
  interval       Set interval used for "interval" plan mode
  mode           Set channel plan mode
  time           Set time used for "time" plan mode
WC8180(config-wireless)#
```

```
WC8180(config-wireless)#auto-rf channel-plan bg-n ?
  history-depth  Set channel plan history depth
  interval       Set interval used for "interval" plan mode
  mode           Set channel plan mode
  time           Set time used for "time" plan mode
WC8180(config-wireless)#auto-rf channel-plan bg-n
```

Configure the Auto-RF power-plan using the following options:

```
WC8180(config-wireless)#auto-rf power-plan ?
  mode                Set power plan mode
  threshold-strength  Configure the threshold strength in dBm to be used for
                      the power adjustements
```

Note:

Auto-RF power plan has the following modes:

- Auto
- Manual

The default power plan mode is `Auto`.

Note:

The default power plan threshold strength is `−85 dBm`.

For more information on Auto-RF configuration, see *ACLI Commands Reference for Avaya WLAN 8100*, NN47251-107.

39. Manually add APs to the Domain AP database. APs (specifically the AP MAC addresses) must be added to the Domain AP database to provide wireless services.

    Note:

    This is an optional step. Perform this step if you need to manually promote an AP to be managed by the controller. If your system is configured for auto-promotion (Step 5 in this procedure), all discovered APs are automatically added to the Domain AP database and are promoted to be managed by the controller.

    Using this command, you can also modify other AP parameters. Modification of other parameters is however not shown in the following command sequence. For each domain AP, assign new profile-id (example 2).

```
WC8180(config-wireless)#domain ap 00:24:B5:65:65:60
Entering domain AP (mac = 00:24:B5:65:65:60) configuration mode...
WC8180(config-domain-ap)#profile-id 2
WC8180(config-domain-ap)#exit
WC8180(config-wireless)#
```

40. Apply the wireless configuration to all APs.

```
Do config-sync to apply changes to AP.
WC8180#
WC8180#wireless controller config-sync
WC8180#
```

Note:

In earlier releases of the WLAN 8100, configuration changes made to the domain AP database required a manual AP reset for the changes to take effect. From release 2.1 onwards, the wireless controller `config-sync` operation synchronizes configuration changes across the domain, and an AP reset is not required.

41. Display the AP status.

The following commands show the status and other relevant information, of the APs. All APs must have the status as `Managed` to be able to provide the configured wireless services.

```
WC8180#show wireless ap status
    Total APs: 3, Managed APs: 3, Failed APs: 0
    ------------------------------------------------------------------------------
    AP MAC             AP IP            Controller IP    Status         Need Image

                              Upgrade
    -----------------  ---------------  ---------------  -------------  ----------
    00:24:B5:65:65:60  54.54.54.5       20.20.20.45      Managed          No
    00:24:B5:65:C0  54.54.54.6       20.20.20.45      Managed          No
    5C:E2:86:0F:51:60  54.54.54.8       20.20.20.45      Managed          No
    ------------------------------------------------------------------------------
```

```
WC8180#show wireless ap status detail
    Total APs: 3, Managed APs: 3, Failed APs: 0
    ------------------------------------------------------------------
    AP (MAC=00:24:B5:65:65:60)
        IP Address                          : 54.54.54.5
        Status                              : Managed
          WC Assignment-Method                : Least-Load
          AP Label                            :
        Hardware Type                       : Avaya AP8120
        Software Version                    : 1.0.0.0
        Serial Number                       : LBNNTMJXAC004V
        Location                            :
        Age (since last update)             : 0d:00:00:03
        System Up Time                      : 0d:00:31:33
        Discovery Reason                    : Controller IP via DHCP
        Managing Controller                 : Local Controller
        Controller IP Address               : 20.20.20.45
        WC Managed Time                     : 0d:18:01:55
        Profile Id                          : 2
        Profile Name                        : ap_002
        Configuration Apply Status          : Success
        Authenticated Clients               : 0
        Configuration Failure Error         :
        Reset status                        : Not Started
        Code Download Status                : Not Started
        Image Upgrade Needed                : No
        Ap Techdump Status                  : Not Started
          Ap Techdump Status                  : Not Started
          Hardware Version                    : R03
          AP port speed and duplex mode       : FullDuplex1000
     AP LED Status                       : LED-OFF
------------------------------------------------------------------
```

```
........
........
........
WC8180#
```

42. Display the AP VAP (SSID) status.

    Note:

    The SSID configured in the SSID Settings pane uniquely identifies your wireless network to which mobility clients connect to.

```
WC8180#show wireless ap vap status
AP MAC Address: 5C:E2:86:0F:51:60
    ------------------------------------------------------------------------
    Radio
    # of Auth
    VAP Id    VAP MAC Address           SSID                        Clients
    --------  -----------------  -------------------------------  ---------
    1 / 1    5C:E2:86:0F:51:60  AVAYA-Demo                        0
    2 / 1    5C:E2:86:0F:51:70  AVAYA-Demo                        1
    ------------------------------------------------------------------------
Total Number of AP(s): 1
WC8180#
```

43. Display the AP radio status.

```
WC8180#show wireless ap radio status
    ------------------------------------------------------------------------------
    AP MAC           Radio Operation Channel Power 802.11 Mode     Auth Clients
    ---------------- ----- --------- ------- ----- --------------- ------------
    2                   On    5         80      802.11b/g/n           1
    ------------------------------------------------------------------------------
WC8180#
```

44. Ensure that the mobility VLAN is mapped to the local VLAN.

    Important:

    Mobility VLAN to local VLAN mapping must be configured for all controllers in a mobility domain.

    In this example, the mobility VLAN `Mobile-Clients` is mapped to the local VLAN with lvid 20. The local VLAN is configured during preliminary controller configuration.

```
WC8180(config-wireless)#switch vlan-map Mobile-Clients lvid 20
WC8180(config-wireless)#show wireless switch vlan-map
-------------------------------------------------------------
Mobility VLAN Name       LVID  State  Role WCP-V Admin Mapped
------------------       ----  -----  ---- -------------------
default-MVLAN            0     Active None Yes   No
mgmt-wireless            20    Active None Yes   Yes
-------------------------------------------------------------
Total Number of Mobility VLANs = 2
WC8180#
```

45. (Optional) Configure one or more capture profiles for a mobility domain.

    Capture profiles are used for remote packet capture. Remote packet capture enables live debugging to troubleshoot client related issues. It can also be used to monitor traffic in a wireless network. After you configure a capture profile, you must apply these profiles to

specific access points (AP) within the mobility domain to start a packet capture. You can configure up to 4 capture profiles.

In the following example, you configure a capture profile named `sample-capture` with profile Id `2`.

Note:

A default capture profile with profile Id `1` is automatically created. You can choose to use this profile or configure a suitable one using the following steps.

```
WCP8180 (config-wireless)#capture-profile 2
Entering capture-profile (id = 2) ...
WCP8180(config-capture-profile)#profile-name sample-capture
```

Verify configuration of the capture profile, using one of the following commands. In the following example, `172.16.9.10` is the IP address of the Observer host PC and the observer port is `37008`.

```
WCP8180# show wireless capture-profile 2
------------------------------------------------------------
Id  Profile Name        Observer IP    Observer Port
--- ------------------------ --------------- -------------
 2 sample-capture       172.16.9.10        37008
------------------------------------------------------------
```

Or

```
WCP8180# show wireless capture-profile 2 detail
Capture Profile ID: 2
    Name                                : sample-capture
    Observer IP Address                 : 172.16.9.10
    Observer UDP Port                   : 37008
    Filter Promiscous mode              : Disabled
    Filter Interfaces                   : All Radios
    Filter Flow direction               : Transmit and Receive
    Filter SSID                         :
    Filter Client MAC                   : 00:00:00:00:00:00
    Filter 802.11                       : data
    Filter Duration                     : 300
    Filter SNAP Length                  : 128
```

Important:

In Wireshark, when the packet length exceeds the configured snap length in the capture profile, the captured packets are displayed as **Malformed**. The default value of the snap length is 128 and the value can be modified between 32 and 1024.

Adjust the snap length to prevent malformed packets.

To verify configuration of all capture profiles, use the following command:

```
WCP8180# WCP8180 (config-wireless)#show wireless capture-profile detail
```

46. At this point the wireless network is ready for client connectivity. Verify wireless client connectivity on the `AVAYA-Demo` network.

Scan for wireless networks and connect a wireless client to the network `AVAYA-Demo`. Verify the client status and details on the WC.

```
WC8180#show wireless client status
    Total number of clients: 1
    ---------------------------------------------------------------------------
    Client           Client        Associated      Mobility        Status
    MAC Address       IP Address      Controller   VLAN
    ----------------- -------------- --------------- -------------- -------------
    00:21:91:7F:02:B4 20.20.20.203    20.20.20.45     Mobile-Clients
Authenticated
    ---------------------------------------------------------------------------
WC8180#
WC8180#show wireless client status detail
Total number of clients: 1
Client (MAC=00:21:91:7F:02:B4)
  Client IP Address                       : 20.20.20.203
  User Name                               : student1
  SSID                                    : AVAYA-Demo
  Mobility Vlan                           : Mobile-Clients
  Status                                  : Authenticated
  Captive Portal Authenticated User       : No
  Transmit Data Rate                      : 64 Mbps
  Inactive Period                         : 0d:00:00:15
  Age (since last update)                 : 0d:00:00:03
  Network Time                            : 0d:09:40:47
  Associating Controller                  : Local Controller
  Controller IP Address                   : 20.20.20.45
  802.11n Capable                         : Yes
  STBC Capable                            : No
  AP MAC Address                          : 70:38:EE:89:C7:A0
  BSSID                                   : 70:38:EE:89:C7:B0
  Radio Interface                         : 2
  Channel                                 : 11
  Network Profile ID                      : 2
  NetBios Name                            :
  Gateway IP                              : 10.1.29.1
  Gateway MAC                             : 00:19:69:91:00:43
  Radio Resource Measurement (RRM)        : Unsupported
    Location Report Requests              : Unsupported
    AP Detection via Beacon Table Report  : Unsupported
    Beacon Active Scan Capability         : Unsupported
    Beacon Passive Scan Capability        : Unsupported
    Channel Load Measurement              : Unsupported
  RSSI (%)                                : 46
  Signal Strength (dBm)                   : -49
  Noise (dBm)                             : -95
WC8180#
```

47. Monitor and troubleshoot wireless clients using Remote Packet Capture.

    To use the Remote Packet Capture feature, start a packet capture instance on the AMDC. You need an observer host PC to view the packet capture.

    Important:

    Before you start a packet capture, ensure that you do the following on the Observer host PC.

    - Download the Netcat application from the Web, to a location on your PC.
    - Open a UDP port for listening.

Important:

If you do not open the UDP port on the observer host then the capture device receives the `ICMP port unreachable` error for every capture packet in the capture stream. This severely impacts the performance.

- Launch Netcat.

  On a Windows machine, execute the following command at the location of installation of Netcat. In the following example, `172.16.9.10` is the IP address of the Observer host PC and the observer port is `37008`.

  ```
  D:\RPC\NetCat>nc -l -u -p 37008 -s 172.16.9.10 -v
  listening on [172.16.9.10] 37008 ...
  ```

  On a Linux machine, execute the command `nc –l –u <port number>`.

- Launch Wireshark to capture frames.
  - In Wireshark, ensure that you configure the CAPWAP UDP data port correctly. To decode the information packets correctly, this port must be the same as that opened for listening on the observer host PC. On Wireshark, navigate to **Edit**, **Preferences**, **CAPWAP**. Update the field **CAPWAP data UDP port**.
  - Also ensure that you deselect **Swap Frame Control**.

Use the following command to start a packet capture. In this example, `00:24:B5:65:65:60` is the MAC address of the AP to which you want to associate the capture profile. The profile ID of the Capture profile `sample-capture` (configured in step 33) is `2`.

```
WC8180# wireless capture-instance start ap 00:24:B5:65:65:60 profile 2
```

View capture instances as follows:

To view capture instances for a specific AP:

```
WC8180# show wireless capture-instance ap <ap-mac>
```

To view capture instances for a specific profile:

```
WC8180# show wireless capture-instance profile <profile-Id>
```

To view all capture instances:

```
WC8180# show wireless capture-instance
```

48. (Optional) Configure filters for the capture profile `sample-capture` to customize your packet capture. You can set one of the following packet capture filters:
    - **client-mac**: to filter capture by client MAC address
    - **include-beacons**: to Include 802.11 beacons in capture data
    - **include-control**: to include 802.11 control frames in capture data
    - **include-data**: to include 802.11 data in capture data
    - **include-mgmt**: to include 802.11 mgmt frames other than probes/beacons in the capture data

- **include-probes**: to include 802.11 probes in capture data
- **ssid**: to filter capture by ssid

For example, if you want to troubleshoot a wireless client (with MAC address `00:88:99:88:77:66`), configure the filter `client-mac` in the capture profile `sample-capture` as follows:

```
WCP8180 (config-wireless)#capture-profile 2
Entering capture-profile (id = 2) ...
WCP8180(config-capture-profile)#filters client-mac 00:21:91:7F:02:B4
```

Verify filter configuration using the following command:

```
WCP8180# show wireless capture-profile 2 detail
Capture Profile ID: 2
    Name                                : sample-capture
    Observer IP Address                 : 172.16.9.10
    Observer UDP Port                   : 37008
    Filter Promiscous mode              : Disabled
    Filter Interfaces                   : All Radios
    Filter Flow direction               : Transmit and Receive
    Filter SSID                         :
    Filter Client MAC                   : 00:21:91:7F:02:B4
    Filter 802.11                       : data
    Filter Duration                     : 300
    Filter SNAP Length                  : 128
```

49. (Optional) To monitor network activity, you can enable the promiscuous mode in the capture profile `sample-capture` as follows.

    The Promiscuous mode is a mode of operation in which every data packet transmitted can be received and read by a network adapter thus allowing your computer to read frames intended for other machines or network devices. The promiscuous mode must be supported by each network adapter as well as by the input/output driver in the host operating system.

    To enable promiscuous mode, use the following command:

    ```
    WCP8180(config-wireless)#capture-profile 2
    Entering capture-profile (id = 2) ...
    WCP8180(config-capture-profile)#promisc-mode enable
    ```

    To disable promiscuous mode, use the command:

    ```
    WCP8180(config-capture-profile)# no promisc-mode
    ```

50. (Optional) View the DiffServ statistics.

    Use the following command to view the DiffServ statistics for all clients.

    ```
    WCP8180#show wireless diffserv statistics
    ```

    Sample Output:

    ```
    WCP8180#show wireless diffserv statistics
    ---------------------------------------------
       Client MAC      Direction    Policy Name
    -----------------  ------------ --------------
    00:05:03:01:00:01  Uplink       p1
    00:05:03:01:00:01  Downlink     p1
    00:05:03:02:00:01  Uplink       p1
    ```

```
00:05:03:02:00:01  Downlink     p1
```

Use the following command to view the DiffServ statistics for a specific client MAC address. In the following example, `00:05:03:01:00:01` is a sample client MAC address.

```
WCP8180#show wireless diffserv statistics 00:05:03:01:00:01
```

Sample Output:

```
WC8180#sh wireless diffserv statistics 00:05:03:01:00:01

Client (MAC=00:05:03:01:00:01)  Policy: p1
Direction: Uplink

ClassifierBlock Name           Hits
-------------------------------------------
    c1                         10280

Client (MAC=00:05:03:01:00:01)  Policy: p1
Direction: Downlink

ClassifierBlock Name           Hits
-------------------------------------------
    c1                         0
```

Use the following command to view the DiffServ statistics in detail.

```
WC8180#sh wireless diffserv statistics detail
```

Sample Output:

```
WC8180#sh wireless diffserv statistics detail

Client (MAC=00:05:03:01:00:01)  Policy: p1
Direction: Uplink

ClassifierBlock Name           Hits
-------------------------------------------
    c1                         11280

Client (MAC=00:05:03:01:00:01)  Policy: p1
Direction: Downlink
ClassifierBlock Name           Hits
-------------------------------------------
    c1                         0

Client (MAC=00:05:03:02:00:01)  Policy: p1
Direction: Uplink

ClassifierBlock Name           Hits
-------------------------------------------
    c1                         0

Client (MAC=00:05:03:02:00:01)  Policy: p1
Direction: Downlink

ClassifierBlock Name           Hits
-------------------------------------------ly---
    c1                         0
WC8180#
```

Chapter 6: Configuring the Wireless Controller — using the WMS

Use this procedure to configure the Wireless Controller (WC) 8180 using the WLAN Management System (WMS) 8100 software.

Note:

This section describes the configuration of various WLAN features such as DiffServ, Client Band Steering, Station Isolation, Auto-RF, Client Load Balancing, Wi-Fi Zoning, LED management on a domain AP database, LLDP support, Bonjour Gateway support, and Remote Packet Capture using the WMS. It also describes enabling support for third-party Real Time Location Systems (RTLS) such as AeroScout and Ekahau.

For more information on the WLAN supported features, see:

- The *Feature Overview for Avaya WLAN 8100*, NN47251-102.
- The *Using WMS and EDM on Avaya WLAN 8100*, NN47251-108, for a list of configuration procedures to configure the various WLAN features using the WMS.

Before you begin

- Obtain a license for the WMS software. To obtain a license from the Avaya Data Licensing portal, see Obtaining licenses from the Avaya Data Licensing portal on page 108.
- Install the WMS software. For more information, see Installing the WLAN Management System software on page 110.
- Complete preliminary controller configuration (WC 8180) using the command line interface (CLI). See Completing preliminary controller configuration on page 15. This is mandatory before you can configure the controller using the WMS.
- Ensure that the WMS has network connectivity to the controller.

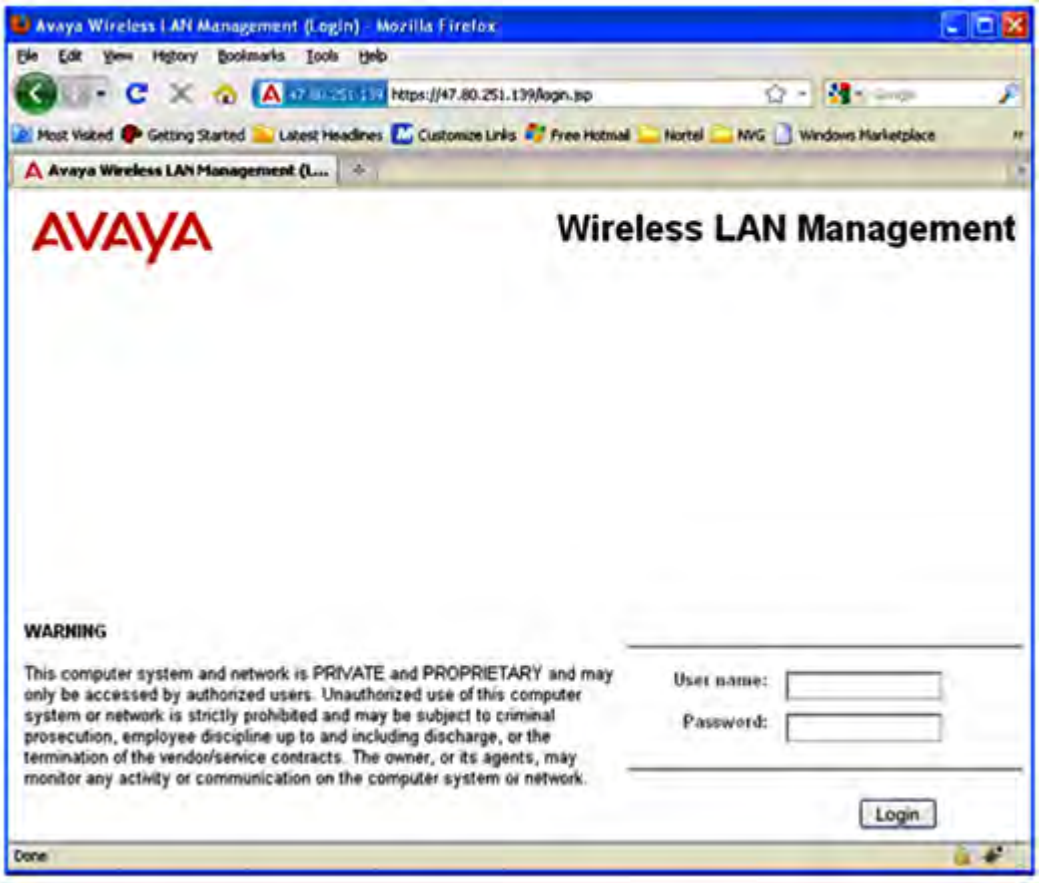
Procedure

1. Connect to the WMS 8100 graphical user interface (GUI). On a browser instance, enter the WMS server IP address in the address bar.

   Note:

   The WMS server IP address is the IP address of the machine where you installed the WMS. You can also use a loopback IP address if you launch the browser from the same machine where you installed the WMS.

   The following figure shows that the WMS is installed on a machine with IP address `47.80.251.139`, and the WMS server is using the default port.



2. Log on to the WMS.

   The default login credentials are **admin** (username) and **admin** (password).

3. Import policies from the AMDC of the domain.

   Ensure that you know the correct management IP address of the Active Mobility Domain Controller (AMDC) of your mobility domain, to import policies from.

   Note:

   If you suspect that the management IP address of the AMDC was changed (using the Avaya CLI, for example) after you installed WMS, you must first delete all domains on the WMS before you proceed to import policies using the new management IP address. This ensures that the WMS displays the most recent configuration that is on the AMDC.

   To delete a domain on the WMS, navigate to **Configuration**, **Mobility domains**. Select a domain to delete and click **Remove**. Removing a mobility domain permanently removes the domain and all its configuration from the WMS database. However, the configuration is removed only from the WMS database and does not affect the actual mobility domain configuration on the AMDC.

   a. On WMS, navigate to **Configuration** > **Mobility Domains**.

b. Right click **Mobility Domains** on the left-hand-side navigation tree, and click **Import Policies**.

   The **Import Policies from AMDC** dialog box appears.

c. Enter the Management IP address of the AMDC.

d. Click **Import Policies**.

4. Physically connect the Access Points (AP) to the network.

   Note:

   The AP 8120 is powered by Power over Ethernet (PoE) through either a PoE switch or an external power injector.

5. Configure the DHCP server for AP discovery.

   Note:

   The Avaya AP 8120 discovers the controller IP addresses using DHCP option 43 or DNS. This example uses the DHCP option 43. The Option 43 setting must be `08 08 41 56 41 59 41 20 41 50 01 04 14 14 14 2D`, where `14 14 14 2D` is the HEX representation of the controller IP address `20.20.20.45`.

   For a step-by-step procedure to configure the DHCP server, see DHCP server configuration for access points on page 105.

6. Power on the APs by connecting them to the PoE switch or power injector.

7. Verify that the APs are connected to the DHCP server. Perform the following steps.

   a. Launch the DHCP Server Manager.

   b. Navigate to **DHCP**, **<your DHCP server>**, **Address Leases**.

   c. Ensure that the IP addresses of all APs are listed.

   The APs connected to the DHCP server receive controller information. The APs then automatically connect to the controller.

8. View the Discovered AP database. Discovered APs are APs that are physically connected to the controller but not yet managed by the controller.

   Navigate to **Configuration, Mobility Domains, <Domain Name>, Devices, Discovered APs**.

   Verify that all APs and their details are listed correctly in the **Discovered APs** page.

9. Configure auto-promotion of discovered APs. Auto-promotion enables all discovered APs to be automatically promoted to the controller-managed state as soon as they are discovered.

   a. Navigate to **Configuration, Mobility Domains, <Domain Name>**.

   b. Right click **<Domain Name>**, and select **Edit Settings**.

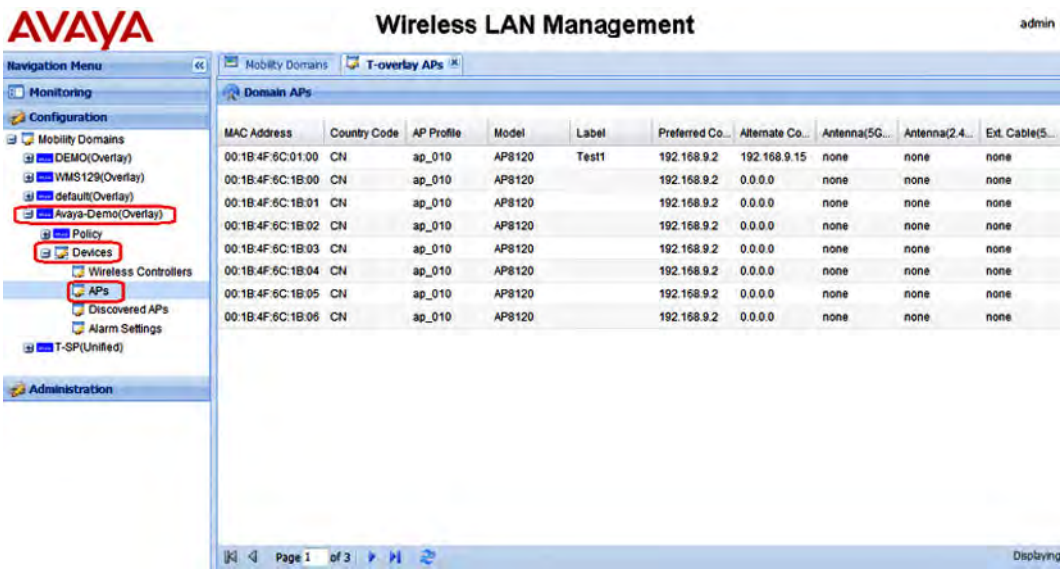
      The **Edit <Domain Name> Domain Settings** window displays.

c. Select **Promote Discovered APs** and click **Save**.

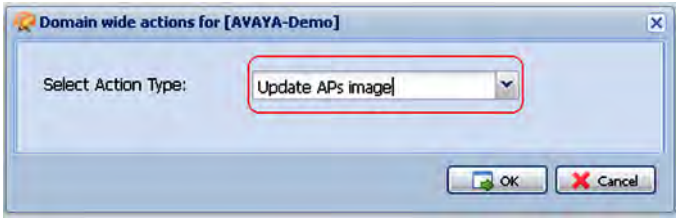
10. View the promoted APs in the Domain AP database. Only those APs in the Domain AP database are managed by the AMDC of the domain.

    Navigate to **Configuration, Mobility Domains, <Domain Name>, Devices, APs**.

    The promoted APs are listed in the **Domain APs** page.



11. Perform an image upgrade on all APs.
    a. Navigate to **Configuration, Mobility Domains, <Domain Name>**.
    b. Right-click on the **<Domain Name>**, and select **Domain Actions**.
    c. From the **Select Action Type** drop-down list, click **Update APs Image**.
    d. Click **OK**.



12. Configure the policies using the WMS.

    Note:

    Existing default policies are imported into the WMS from the AMDC of the domain, when you perform *Import Policies* in step 2. You can use the following steps to configure additional policies, as required.

    Policy configuration involves configuring mobility VLANs and profiles such as the network profiles, radio profiles, AP profiles (for Access Points) and Captive Portal profiles on the AMDC. You also verify connectivity of the AMDC with other components of the WLAN solution such as the Wireless Access Points (AP), to provide wireless services to wireless clients.

Important:

When you configure profiles in the network (such as AP profiles, network profiles and radio profiles) ensure that you configure the profile name to be unique across the network, for each of the profiles.

Also, ensure that you do not configure profile names that have similar characters or letters and differ only in their *case*.

13. Create a mobility VLAN.
    a. Navigate to **Configuration** > **Mobility Domains** > **<Domain Name>** > **Policy** > **Mobility Profiles**.
    b. On the right-hand-side pane, click **Add**.

       The **Mobility Profile** window displays.
    c. In the **Mobility VLAN** field, enter a name (for example, `Mobile-Clients`).
    d. Select the *mDNS Scan list* check box, to add the mobility VLAN name under scan-list.

       This enables the required mobility VLAN to relay multicast DNS traffic across different networks.

    e. Click **Add**.
14. (Optional) Configure multicast domain name system (mDNS). The Wireless Controller monitors mDNS Gateway services and by monitoring those Bonjour advertisements from the source or host, responds back to Bonjour clients when a request for service is initiated. You can configure *Bonjour Gateway* solution on the Avaya WLAN 8100 by enabling the relay mode.

    Important:

    After you configure Mobility Profiles, you can apply the mDNS service configuration to the Mobility VLAN on the selected domain.

    a. Navigate to **Configuration** > **Mobility Domains** > **<Domain Name>** > **Policy** > **mDNS Services**.
    b. On the **mDNS Services** pane, click **Add**.

       The **mDNSServices** window opens.
    c. Enter the filter name in the **Filter Name** field.
    d. In the **Service Name** field, enter the name of the mDNS service that you want to be relayed across or within the networks.

e. Select the **Enable** check box, to enable the filter rule for the respective service name.

f. In the **Protocol** field, select the protocol type.

g. In the **Filter Mode** field, select the parameters either **Permit** or **Deny** for the filter rule.

Note:

You can configure up-to 25 filter rules out of which nine rules are configured by default.

15. Configure a **Captive Portal** profile.

Important:

For the Captive Portal to work properly, ensure that the Wireless or System interface of the AMDC does not have the `Management` flag enabled.

Important:

If you want to host the Captive Portal on a guest VLAN, ensure that the Captive Portal IP address is an active VLAN interface IP on any controller in the domain, except the Management VLAN IP address, the System VLAN IP address, or the wireless interface IP address of that controller. The Captive Portal IP address must physically exist on one of the domain controllers.

a. Navigate to **Configuration**, **Mobility Domains**, **<Domain Name>**, **Policy**, **Captive Portal**, **Profiles**.

b. On the **Captive Portal** pane, click **Add**.

The **Captive Portal Profile** window displays.

c. In the **Profile Name** field, enter a name, for example, `PRF-CP`. Enter values for other fields as applicable or retain defaults.

d. Click **Add** to create the Captive Portal (CP) profile.

16. Configure the user database.

To configure the user database, you:

- Create a user group.
- Create a Client Portal user and add the user to the user group (configure membership).

Note:

You can create a maximum of 10 user groups and assign up to 1000 users to each user group.

Navigate to **Configuration**, **Mobility Domains**, **<Domain Name>**, **Policy**, **Security**, **Captive Portal Users**.

Create a user group.

a. In the **Users Groups** pane, click **Add**.

b. Enter a group name (for example, `UG-guest`) and click **Add**.

Create a user and assign the user to the user group.

a. In the **Users DB** pane, click **Add**.

   The **Client DB** window displays.

b. In the **General** tab, enter a name (for example, `guest`) and password for the user.

c. In the **Groups** tab, select the user group you created (`UG-guest`) from the **Available User Groups** and move it to the **Selected User Groups**.

d. Click **Add**.

17. (Optional) Configure Captive Portal Walled Garden hosts in the Captive Portal profile.

    Sometimes, a Captive Portal user may need to access network resources in the intranet or public Web sites from an enterprise network, without requiring to first undergo Captive Portal authentication. To support these user requirements, the WLAN 8100 allows the configuration of the IP addresses of Web hosts in a Captive Portal profile so that the user can access these hosts without the need for authentication. This is known as the Captive Portal Walled Garden.

    a. Navigate to **Configuration**, **Mobility Domains**, **<Domain Name>**, **Policy**, **Captive Portal**, **Profiles**.

    b. Click the **Walled Garden Hosts** tab.

    c. In the **Walled Garden Host Names** pane, click **Add**.

       The **Add New Walled Garden Host** dialog box appears.

    d. In the **Add New Walled Garden Host** dialog box, select the host type from the **Type** drop-down list and enter the IP address of the host in the **IP Address** field.

    e. Click **Ok**.

18. Configure Diffserv. Differentiated services or DiffServ specifies a simple and scalable mechanism for classifying and managing network traffic and providing quality of service (QoS) to wireless clients, on modern IP networks.

    Important:

    Ensure that you configure DiffServ policy and classifier block names that are unique across the network. Do not configure policy and classifier names that have similar letters and characters and differ only in their *case*.

    Configure a Diffserv classifier block named `classifier1`. Repeat these steps to configure multiple classifier blocks.

    a. Navigate to **Configuration**, **Mobility Domains**, **<Domain Name>**, **DiffServ**, **Classifiers**.

    b. Click **Add.**

       The **DiffServ classifier block** dialog box appears.

    c. Enter a name in the **Classifier Name** field (`classifier1`) and click **Add**.

Note:

The classifier name must be unique across the network and in the range of 1 to 31 characters.

The configured classifier appears in the **DiffServ Classifiers** pane.

d. (Optional) To delete a classifier, select a classifier from the list and click **Remove**.

Configure classifier block elements for the classifier `classifier1`.

a. Select the classifier `classifier1` in the **DiffServ Classifiers** pane.

The **Classifier block [<classifier-name>] Element (s)** pane displays.

b. Click **Add.**

The **DiffServ classifiers block elements** dialog box appears.

c. Select an appropriate classifier block element using the **Element Type** drop-down list and click **Add**.

Important:

When you configure a classifier block to match the source or destination client IP address or a client MAC address, you must configure a proper mask to ensure that the classifier block is applied to traffic from only the specified client and not all clients within the subnet.

For example, if you configure the classifier block to drop packets for a client IP address of `10.1.20.5`, a mask of `255.255.255.0` drops the packets on all clients within the subnet. To ensure that the packets are dropped for traffic from only the specified client, you must set the mask to `255.255.255.255`.

Similarly, if you configure a classifier block for a client MAC address `01:02:03:04:05:06`, for example, ensure that you set the subnet mask to `ff:ff:ff:ff:ff:ff`.

Configure a Diffserv policy named `policy1` and associate the configured classifier block `classifier1` with this policy.

a. Navigate to **Configuration**, **Mobility Domains**, **<Domain Name>**, **DiffServ**, **Policies**.

b. Click **Add**.

The **DiffServ policy name** dialog box opens.

c. Enter a name in the **Policy Name** field (`policy1`) and click **Add**.

The newly created policy `policy1` appears in the **DiffServ Policies** pane.

d. Select the newly added policy `policy1`.

e. In the **Policy Classifiers [policy1]** pane, click **Add**.

The **DiffServ policy block** dialog box opens. Associate a classifier and a policy block action with the DiffServ policy.

f. From the **Classifier Name** drop-down menu, select the classifier `classifier1`.

g. From the **Action** drop-down menu, select one of the following options:

- markCos

  Enter a value in the range 0 to 7, in the **Action Mark Cos** field.

- markIpDscp

  Enter a value in the range 0 to 63, in the **Action IP DSCP** field.

- markIpPrecedence

  Enter a value in the range 0 to 7, in the **Action Ip Precedence** field.

- drop
- allow

  Important:

  If you use a DSCP value of `48/56` and a cos value of `7`, the Access Point (AP) overrides the DSCP priority and changes its priority to `0`. This causes a change in the traffic priority.

  Some DSCP priorities are specifically marked for network control traffic and these DSCP priorities must not be used in uplink traffic from wireless clients. The set of DSCP priorities that are overridden by the AP is implicitly derived from the *QoS egressmap* table maintained in the AP. All DSCP priorities mapped to 802.1p priority 7 are considered to be network control packet priority. For the default QoS egressmap, DSCP priorities 48 and 56 are considered as network control packet priorities and are overridden on the client generated uplink packets.

  When an AP detects client packets with DSCP values set to a network control packet priority, the AP resets the DSCP value on those packets to 0.

  For more information on the *QoS egressmap* table and the WLAN 8100 DSCP priority, see the *Feature Overview for Avaya WLAN 8100*, NN47251-102.

h. Click **Add**.

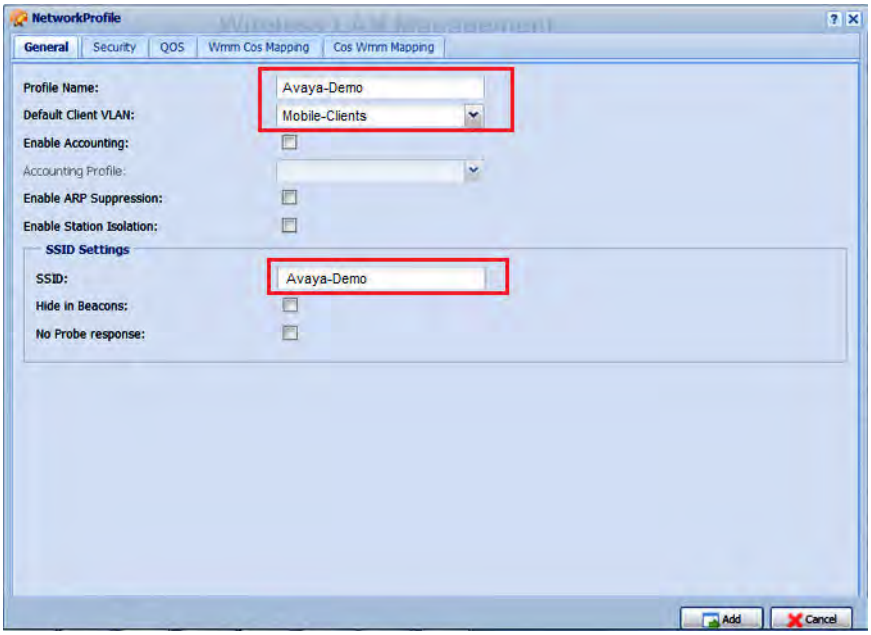
19. Configure a network profile.

a. Navigate to **Configuration**, **Mobility Domains**, **<Domain Name>**, **Policy**, **Network Profiles**.

b. On the **Network Profiles** pane, click **Add**.

The **Network Profile** window displays.

c. Enter the following information in the **General**, **Security** and the **QoS** tabs. Retain default values for the other fields.



In the **General** tab, do the following.

- **Profile Name**: Enter a name, for example, `AVAYA-Demo`.
- **Default Client VLAN**: Select `Mobile-Clients` from the drop down list.
- (Optional) **Enable Station Isolation** : Select the check box to enable station isolation on a network profile.
- Enter an SSID for the network profile (for example, `AVAYA-Demo`).

  Note:

  The SSID configured in the SSID Settings pane uniquely identifies your wireless network to which mobility clients connect to.

  Important:

  When you configure an SSID for a network profile, ensure that it is unique across the network. SSIDs can have a maximum of 32 characters.

  Also, ensure that you do not configure SSIDs that have similar characters but are different only in their *case*. For example do not configure SSIDs *avaya-demo* and *AVAYA-DEMO* within the same network.

In the **Security Settings** tab do the following:

- From the **802.11 Security Mode** drop-down menu, select **wpaPersonal**.
- (Optional) **Enable MAC Validation** : Select the check box to enable validation of MAC addresses of client devices in the network.

When you select this check box, all new client devices to the wireless network are automatically blacklisted by the controller and denied access to wireless services. To enable wireless services for a blacklisted device, you must explicitly remove this device from the blacklist and configure this device as white-listed.

- **MACValidationMode**: Select the client device MAC validation mode. The options are:
  - local Whitelist: The client MAC address is validated against a local Whitelist database. On successful verification, the client device is granted network access.
  - radius: The client MAC address is validated against a remote RADIUS server.

- In the **WPA Personal** pane, enter a pass phrase in the **WPA Key** field.

In the **QoS** tab, do the following:

- Select **Enable Client QoS**.
- Specify the **Upstream** and **Downstream** bandwidth limits in bps as applicable.
- In the **DiffServ** pane, select the DiffServ policy `policy1` from the drop-down lists in the **Upstream** and **Downstream** fields, as applicable.

d. Click **Add** to create the network profile.

After you create the network profile **Avaya-Demo**, ensure that you map the created Diffserv policy to the network profile, to, for example, prioritize WMM (Wireless Multi-Media) traffic in the network.

By default, in WMM, voice traffic has a higher priority over video traffic. You can, for example, configure DiffServ policies to reverse this traffic priority in the network.

20. Enable Captive Portal globally.

a. Navigate to **Configuration**, **Mobility Domains**, **<Domain Name>**, **Policy**, **Captive Portal**, **General Settings**.

b. Click **Edit**.

The **Captive portal global** window displays.

c. Select **Enable Captive Portal** and click **Update**.

21. Configure the **Captive Portal (guest)** network profile and associate the Captive Portal profile with this network profile.

a. Navigate to **Configuration**, **Mobility Domains**, **<Domain Name>**, **Policy**, **Network Profiles**.

b. On the **Network Profiles** pane, click **Add**.

The **Network Profile** window displays.

c. Enter details as follows. You can default values for the other fields.

In the **Security** tab, do the following:

- Select **Enable Captive Portal**.

- In the **Captive Portal** drop-down menu, select the Captive Portal profile you created in step 3.

In the **General** tab, do the following:

- In the **Profile Name** field, enter a name, for example, `NP-guest`
- In the **User Group** field, select the user group you created in Step 4 (`UG-guest`).
- In the **Default Client VLAN**, select the mobility VLAN **MV-GUEST** from the drop down list.
- In the **Captive Portal User Validation**, select **LocalSecurityDB** from the drop-down list.
- In the SSID settings pane, enter an SSID for the network profile (for example, `Guest`).

  Note:

  The SSID configured in the SSID Settings pane identifies your wireless network to which mobility clients connect to.

- Click **Add** to create the network profile.

22. Configure the access radio profiles. You typically configure `A-N` and `BG-N` access radio profiles to support different radio frequencies. Repeat these steps to create additional access radio profiles.

    When you create an access radio profile, you also enable client band steering, Wi-Fi zoning and load balancing on the configured access radio profile.

    Client Band Steering is a technique used to increase the overall capacity of a dual-band wireless network composed of multiple APs that use both the 2.4 GHz and 5.0 GHz radios.

    Client stations predominantly support 2.4 GHz. Many modern client stations have dual-band support yet tend to favor connection to 2.4GHz networks (although some popular modern clients still only support 2.4 GHz, e.g. the Apple iPhone 4). As a result, dual-band networks have the 2.4 GHz band heavily utilized, and the 5 GHz band under utilized. The objective of Client Band Steering is to encourage 5GHz capable client stations to use the 5 GHz radio instead of the 2.4 GHz radio, leaving the 2.4 GHz radio for stations that only support 2.4 GHz.

    Note:

    Client Band Steering is optional step, but is highly recommended.

    As part of *Client load balancing*, you enable or disable the load balancing. After you enable load balancing, you configure the following parameters:

    - utilization-start (%) — Utilization level at which client association load balancing begins
    - utilization-cutoff (%) — Client association load balancing cutoff. If this threshold is exceeded, all further client associations are refused.

Note:

This cutoff is useful so that controller CPU utilization is maintained at an optimum level. If CPU utilization goes beyond 100%, it causes the controller to restart which in turn results in an unprecedented controller outage.

(Optional) Configure *Wi-Fi Zoning* to create Wi-Fi association and roaming zone thresholds for APs in your deployment, to restrict the scale of connectivity and to reduce the scale of users that connect to the system. Wi-Fi zoning is typically configured on APs in BYOD deployments such as in stadiums, public-hotspots or trade-shows, where user density is the critical factor for efficient connectivity with an AP.

Note:

The allowed range for the Wi-Fi association zone and roaming zone thresholds is `-99` to `-1` dBm. The values `0` and `-100` dBm are used for disabling and auto-configuration, respectively. However, in current release the value `-100` dBm disables Wi-Fi zoning.

Choose a value depending on the physical distance between the APs and also the AP transmission power. The recommended range for optimal zoning is `-90` dBm to `-65` dBm.

When you configure the Wi-Fi association zone and roaming zone thresholds for an AP, always ensure that the Wi-Fi association zone thresholds is greater than or equal to the Wi-Fi roaming zone thresholds.

For example, if the Wi-Fi association zone thresholds is `-65` dBm, then configure the Wi-Fi roaming zone thresholds as either `-80` dBm or `-65` dBm.

a. Navigate to **Configuration**, **Mobility Domains**, **<Domain Name>**, **Policy**, **Radio Profiles**.

b. In the **Access Radio Profiles** pane, click **Add**.

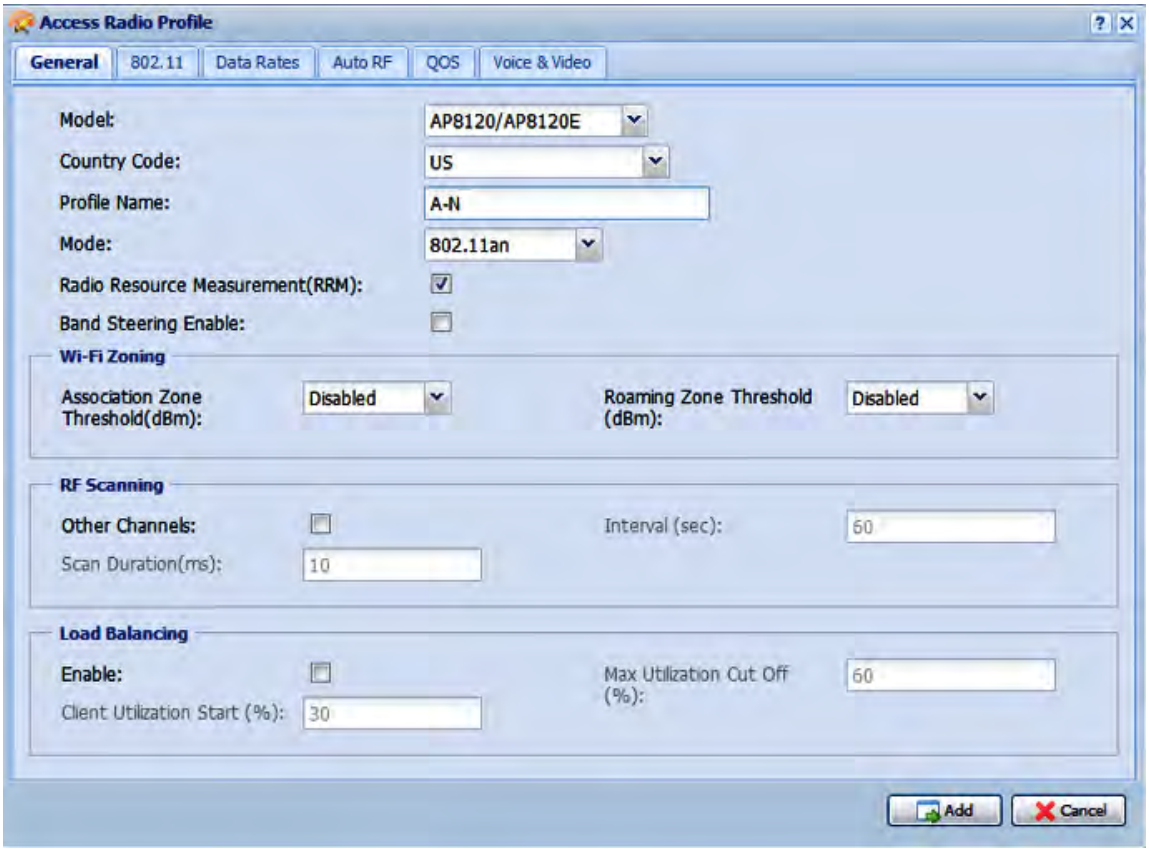
The **Access Radio Profile** window displays.

Create the `A-N` Access radio profile.

a. In the **General** tab, enter details as follows. Retain default values for the other fields.

- **Profile Name**: Enter a name, for example, `A-N`.
- **Mode**: Select **802.11an** from the drop down list.
- To enable Client Band Steering, select **Band Steering Enable**.
- To enable Wi-Fi Zoning:
  - In the **Association Zone Threshold (dBm)** field, select an RSSI thresholds value in the range **-99** to **-1** dBm. Selecting **Disable** or **Auto** disables the association zone enforcement.
  - In the **Roaming Zone Threshold (dBm)** field, select an RSSI thresholds value in the range **-99** to **-1** dBm. Selecting **Disable** or **Auto** disables roaming zone enforcement.

- To enable Client Load Balancing:
  - Select the **Enable** check box.
  - In the **ClientLBUtilizationStart** field, enter a number in the range 0–100.
  - In the **ClientLBUtilizationCutOff** field, enter a number in the range 1–100.



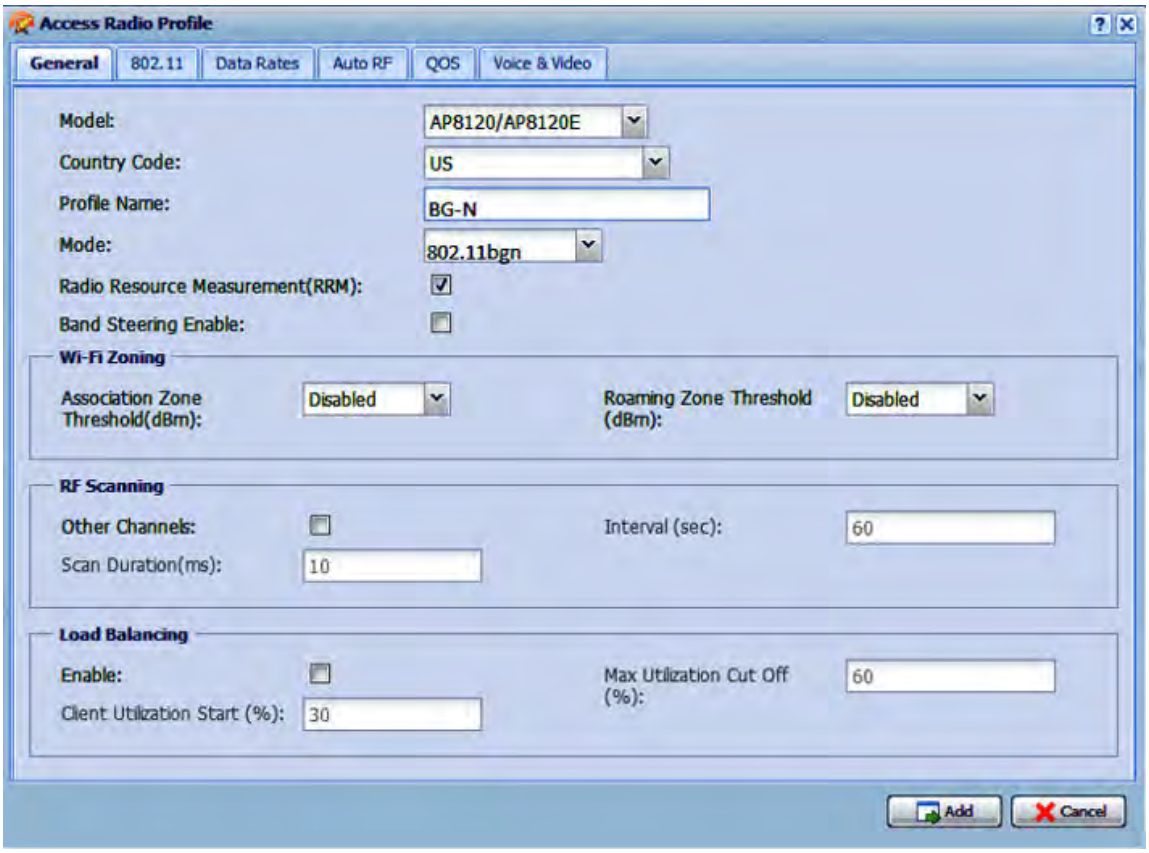
b. Click **Add** to create the access radio profile.

Configure the `BG-N` Access radio profile.

a. In the **General** tab, enter details as follows. Retain default values for the other fields.

- **Profile Name**: Enter a name, for example, `BG-N`.
- **Mode**: Select **802.11bgn** from the drop down list.
- To enable Wi-Fi Zoning:
  - In the **Association Zone Threshold (dBm)** field, select an RSSI threshold value in the range **-99** to **-1** dBm. Selecting **Disable** or **Auto** disables the association zone enforcement.
  - In the **Roaming Zone Threshold (dBm)** field, select an RSSI threshold value in the range **-99** to **-1** dBm. Selecting **Disable** or **Auto** disables roaming zone enforcement.
- To enable Client Band Steering, select **Band Steering Enable**.

- To enable Client Load Balancing:
  - Select the **Enable** check box.
  - In the **ClientLBUtilizationStart** field, enter a number in the range 0–100.
  - In the **ClientLBUtilizationCutOff** field, enter a number in the range 1–100.



b. Click **Add** to create the access radio profile.

23. Create the Access Point (AP) profile. You then associate the AP profile with appropriate radio and network profiles.
    a. Navigate to **Configuration**, **Mobility Domains**, **<Domain Name>**, **Policy**, **AP Profiles**.
    b. Click **Add**.

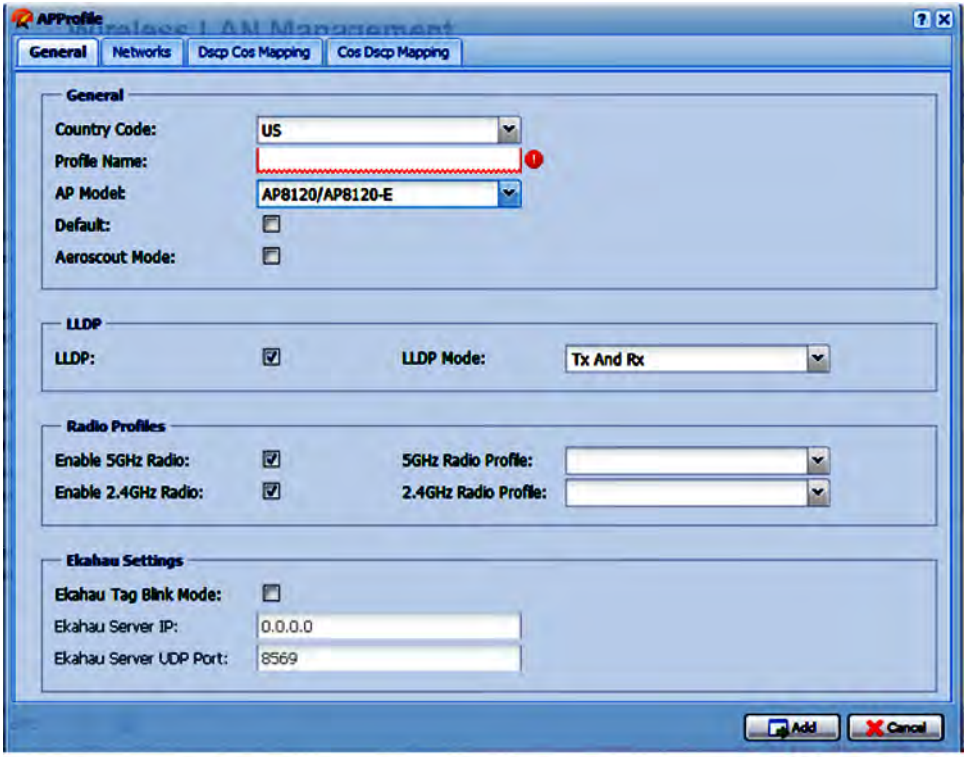
       The **AP Profile** window displays.
    c. In the **General** tab, enter details as follows.
       - **Profile Name** : Enter a profile name, for example `AP-Profile-1`.
       - **AP Model** : Select the AP model from the drop down list.
       - **Aeroscout Mode** : Optionally, select the check box to enable AeroScout on the AP profile.
    d. In the **LLDP** pane, select the **LLDP** check box to enable LLDP support, and select the **LLDP Mode** from the drop-down menu.

e. In the **Radio Profiles** pane, from the drop-down menu, select the appropriate radio profile based on the radio frequencies.

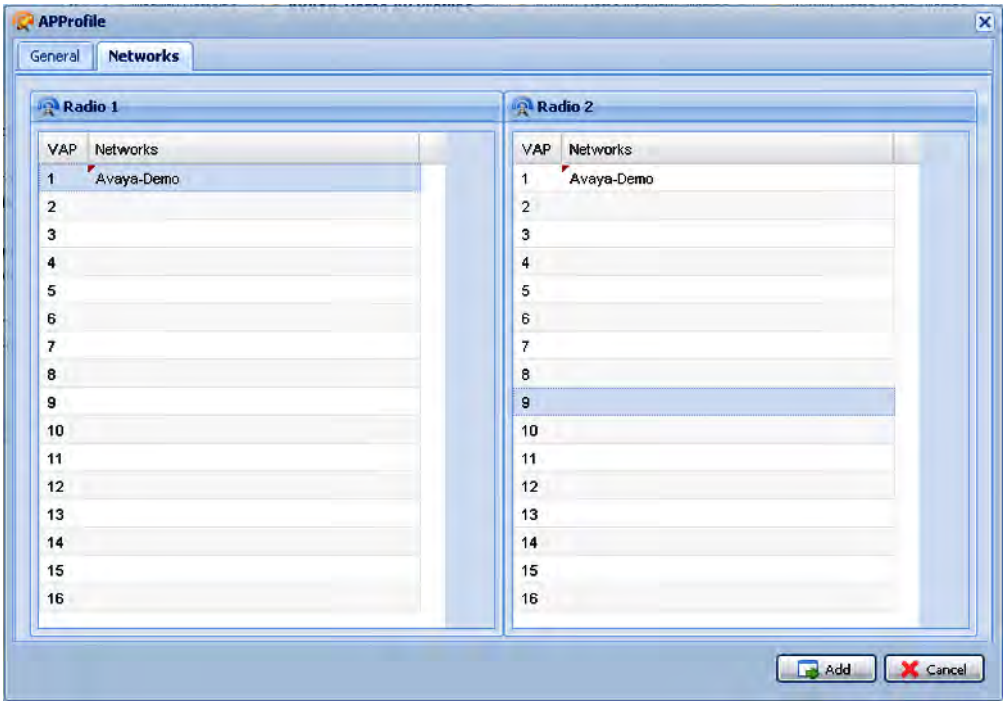
- Select `A-N` as the 5GHz radio profile.
- Select `BG-N` as the 2.4 GHz radio profile.

f. In the **Ekahau Settings** pane:

- Select the **Ekahau Tag Blink Mode** check box to enable the Ekahau tag blink mode on the AP.
- Enter the appropriate values in **Ekahau Server IP** and **Ekahau Server UDP Port** fields.



g. In the **Networks** tab, add the network profile `AVAYA-Demo` to the Radio 1 and Radio 2 tables by double clicking each field and selecting the profile from the down menu.



h. Click **Add** to create the profile.

24. (Optional) If required, manually add additional Access Points (AP) directly to the Domain AP database to promote these APs to be managed by a controller.

Note:

Perform this step only if you need to manually promote an AP to be managed by the controller. If your system is configured for auto-promotion, all discovered APs are automatically added to the Domain AP database and are promoted to be managed by the controller.

a. Navigate to **Configuration, Mobility Domains, <Domain Name>, Devices, APs**.

b. The **Domain APs** window opens, displaying the list of APs currently added to the Domain AP database.

c. Click **Add**.

d. In the **General** tab, ensure that you fill the appropriate fields.

Variable	Value
Country Code	The country code of the location of the AP. Select a country code from the drop-down list.
MAC Address	The AP MAC address.
Model	The model number. • AP8120 • AP8120-E

Variable	Value
	• AP8120-O **Important:** The AP8120-O model is not supported in a Unified Access deployment. **Note:** Selecting the AP8120-E enables the Antenna and External Cable fields in the **Radios** tab.
Label	The label value.
Profile	Select an AP profile to associate with the AP, from the drop-down menu.
Preferred WC (Preferred WCP for Unified Access deployments)	The IP address of the preferred controller (WC/WCP depending on the deployment).
Alternate WC (Alternate WCP for a Unified Access deployments)	The IP address of the alternate controller (WC/WCP depending on the deployment).
Preferred WSP (for a Unified Access deployments)	The IP address of the preferred wireless switching point (WSP).
Preferred WSP (for a Unified Access deployments)	The IP address of the alternate wireless switching point (WSP).
LED	Use this field to select the LED state **Normal(On)** or **off** for the APs in the domain AP database. **Note:** By default **Normal(On)** LED state is enabled on a domain AP database.
The following rows describe the **Radio Controls** pane fields for **5 GHz and 2.4 GHz radios**. In all fields, select appropriate values from the drop-down lists provided.	
Administration	Use this field to **On** or **Off** the Radio in the given AP MAC Address.
WIFI Association Zone	Specify RSSI thresholds value in dBm, from -99 to -1 dBm. You can also select **Disabled** or **Auto** to reset the zone setting to a disabled state with no association zone enforcement.
WIFI Roaming Zone	Specify RSSI thresholds value in dBm, from -99 to -1 dBm. You can also select **Disabled** or **Auto** to reset the zone setting to a disabled state with no roaming zone enforcement.
The following rows describe the **Radios** pane fields for **5 GHz and 2.4 GHz radios**.	

Variable	Value
In all fields, select appropriate values from the drop-down lists provided.	
Channel	The radio channel settings.
Power (%)	The radio power settings (expressed as a % age)
Antenna	Applies only to the AP8120-E: select the 70° or 180° external antenna.
Ext.Cable	Applies only to the AP8120-E: select 3 or 10 foot plenum rated cables.
The following rows describe the **Location** pane.	
Campus	The Campus (location) of the AP.
Building	The Building (location) of the AP.
Floor	The Floor (location) of the AP.
Sector	The Sector (location) of the AP.

25. (Optional) To improve network performance, the Auto-RF feature enables you to automatically adjust channel and power of the managed access points in a mobility domain. View and configure Auto-RF power plan and channel plan settings on an AP.

    a. To view the current power and channel plan settings, navigate to **Configuration**, **Mobility Domains**, **<Domain Name>**, **Policy**, **Auto-RF**.

    - The **General Settings** pane displays the current Auto-RF settings. If you need to modify them, click **Edit**.

      Make the necessary changes and click **Update** to save your changes.
    - The **Proposed Manual Power** pane displays the proposed settings for the Auto-RF power tuning.
    - The **Proposed Manual Channel Plan** pane displays the current channel plan settings.

    b. To apply selected actions for Auto-RF management, click **Actions**.

    From the **Select Action Type** drop-down menu, select an action and click **OK**, to initiate the action.

    For detailed information on Auto-RF configuration using the WMS, see the *Using WMS and EDM on Avaya WLAN 8100*, NN47251-108.

26. Map the mobility VLAN to the local VLAN.

    Note:

    Mobility VLAN to local VLAN mapping must be configured for all controllers in a mobility domain.

    In this example, you map the mobility VLAN **Mobile-Clients** with the local VLAN **mgmt-wireless**.

    a. Navigate to **Configuration, Mobility Domains, <Domain Name>, Devices, Wireless Controllers**.

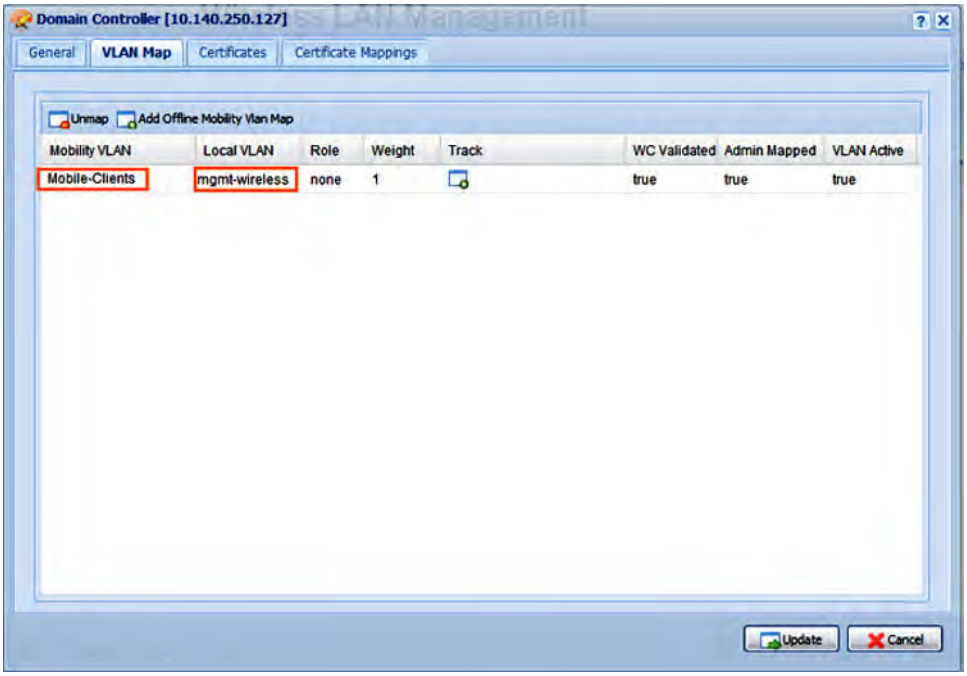
    The **Controllers in Domain** window opens and displays a list of controllers in the mobility domain.

b. Select a controller from the list and click **Edit**.

   The **Domain Controller [Management IP]** window displays.

c. Click the **VLAN Map** tab. Ensure that the mobility VLAN `Mobile-Clients` is mapped with the local VLAN `mgmt-wireless`.

d. Click **Update**.



27. Apply the WMS configuration changes to the AMDC of the mobility domain.

    a. Navigate to **Configuration, Mobility Domains, <Domain Name>, Policy**.

    b. Right-click on **Policy** and click **Review/Commit**.

       The system verifies configuration differences between the WMS and the AMDC, and displays a merge report. The report displays details on what was changed on the WMS, the differences in the existing configuration between the WMS and the controller and the updates on the controller if the changes are successfully applied.

    c. Review the report and click **Apply Changes on Controller** to push WMS configuration to the AMDC.

       The system then generates a status report. The report indicates the action on the AMDC configuration (create, update or delete). It also indicates a reason for failure if the action failed.

    d. Click **Close** on the status report window.

28. If you made changes to any domain AP configuration parameters (for example, if you updated an AP profile), you must reset the individual AP for the changes to take effect.

Perform the following steps to reset an individual AP.

a. Navigate to **Monitoring, Mobility Domains, <Domain Name>, Wireless Access Points**.

   The list of access points in the domain and their details are displayed.

b. From the list, select the access point that you want to reset.

   Details about the access point are displayed in the **Details for selected AP** panel.

   Note:

   The **Details for selected AP** panel is a collapsible panel. If this pane is collapsed, you can expand it by clicking the button provided on the extreme right-hand-corner of this panel.

c. In the **AP actions** pane, click **Reset**.

29. The wireless network is now ready for client connectivity. Scan for wireless networks and connect wireless clients to the `Avaya-Demo` network.

    Wireless clients are typically devices such as PDAs and laptops that utilize wireless services.

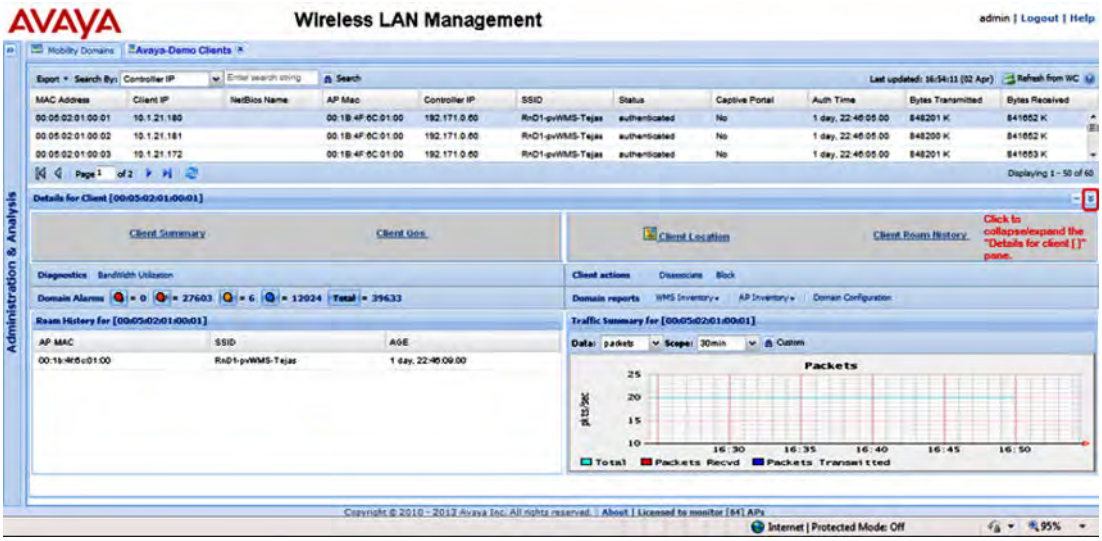
30. Verify wireless client connectivity status and other details on the controller.

    a. On the WMS, navigate to **Monitoring**, **Mobility Domains**, **<Mobility Domain Name>**, **Wireless Clients**.

       The wireless clients in the domain and their details are displayed.

       You can click a particular column to sort the information displayed in that column in ascending or descending order. You can also change the order or location of the columns by dragging and dropping them at the desired location. You can show or hide a column by clicking the button on the right-hand-side of any column and selecting or deselecting the appropriate column.

       To refresh wireless client information on this window from the WMS database, click the refresh button at the bottom of this pane.



b. To refresh client information from the AMDC of the domain, click **Refresh from WC**. This may take a few minutes to complete.

   Note:

   Wireless client information is automatically refreshed from the AMDC after a finite polling interval. The default polling interval is 10 minutes.

c. To view further monitoring details of a wireless client, select a client from the list.

   The details are displayed in the **Details for client [<client-mac-address>]** pane. You can expand or collapse this pane by clicking the button on the top-right corner of this pane.

d. To view the client dashboard, right-click on a client entry and select **Show Associated Client Dashboard**. The client dashboard displays at a glance valuable real-time status information about the wireless clients. You can also double-click a client entry to view the corresponding dashboard.

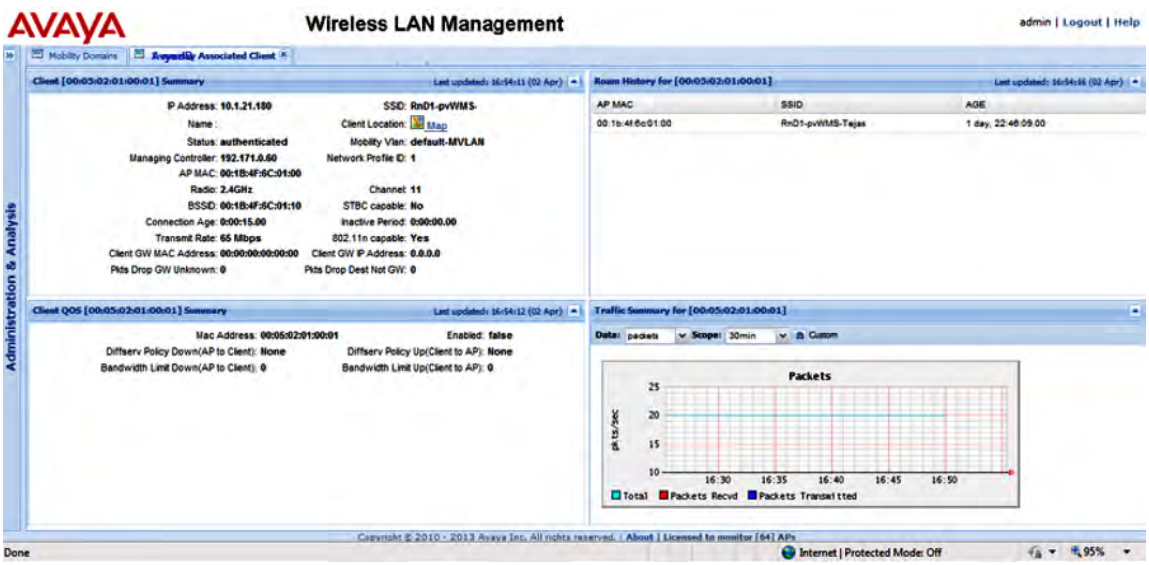


Figure 4: Associated Client Dashboard

Note:

The **Associated Client Dashboard** is automatically refreshed every 5 minutes if the dashboard window is active (open) on the WMS.

For further details on monitoring wireless clients and viewing the **Associated Client Dashboard**, see the *Using WMS and EDM on Avaya WLAN 8100*, NN47251-108.

31. (Optional) Monitor wireless APs in the mobility domain.

    a. Navigate to **Monitoring**, **Mobility Domains**, **<Domain Name>**, **Wireless Access Points**.

    The access points in the domain and their details are displayed.

    You can click a particular column to sort the information displayed in that column in ascending or descending order. You can also change the order or location of the columns by dragging and dropping them at the desired location. You can show or hide a column by clicking the button on the right-hand-side of any column and selecting or deselecting the appropriate column.

    To refresh access point information on this window from the WMS database, click the refresh button at the bottom of this pane.

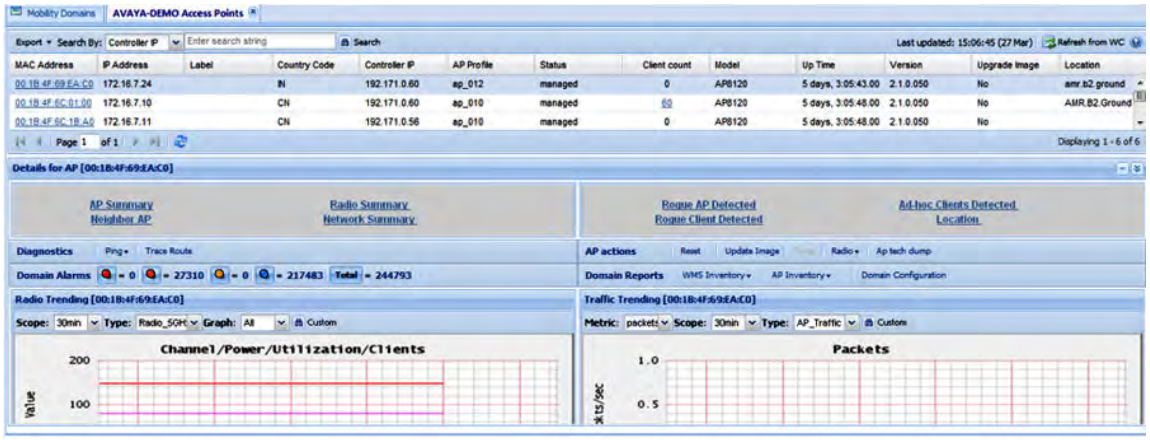


Figure 5: Monitoring wireless access points (AP)

b. To refresh AP information from the AMDC (managing wireless controller), click **Refresh from WC** on the top right corner of this page. This may take a few minutes to complete.

   Note:

   AP information is automatically refreshed from the AMDC after a finite polling interval. The default polling interval is 10 minutes.

c. To view further monitoring details of an AP, select an AP from the list. The details are displayed in the **Details for AP [<Ap-mac-address>]** pane. You can expand or collapse this pane by clicking the button on the top-right corner of this pane.

d. To view the Access Point dashboard, right-click on an AP entry and select **Show Managed AP Dashboard**. You can also double-click an AP entry to view the corresponding dashboard. The **Managed AP Dashboard** displays at a glance, valuable real-time status information about the APs.

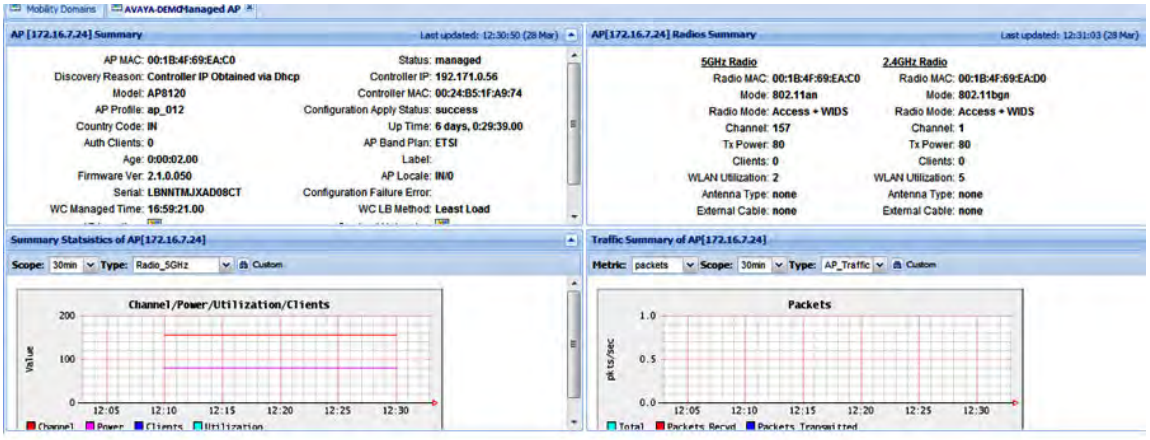


Figure 6: Managed AP dashboard

Note:

The **Managed AP dashboard** is automatically refreshed every 5 minutes if the dashboard window is active (open) on the WMS.

For further details on monitoring APs and viewing the **Managed AP Dashboard**, see the *Using WMS and EDM on Avaya WLAN 8100*, NN47251-108.

Chapter 7: Configuring the Wireless Controller — using the EDM

Use this procedure to configure the Wireless Controller (WC) 8180 using the Enterprise Device Manager (EDM).

Note:

This section describes the configuration of various WLAN features such as DiffServ, Client Band Steering, Station Isolation, Auto-RF, Client Load Balancing and Remote Packet Capture using the EDM. It also describes the enablement of support for third-party real-time location systems such as AeroScout and Ekahau.

For more information on the WLAN supported features, see:

- The *Feature Overview for Avaya WLAN 8100*, NN47251-102.
- The *ACLI Commands Reference for Avaya WLAN 8100*, NN47251-107, for a complete list of configuration commands for each of the features.

Before you begin

- Ensure that you have completed the preliminary controller configuration. See Completing preliminary controller configuration on page 15.

  This is mandatory before you can configure the controller using the EDM.
- Ensure that the controller has a management interface IP address that is reachable from the PC hosting the EDM.

Procedure

1. Log on to Enterprise Device Manager (EDM).

   To log on to the EDM, open a browser instance and enter:

   ```
   http://<management Interface IP address of the controller>
   ```

2. Create a mobility domain and join the controller with the mobility domain.
   a. Navigate to **Configuration, Wireless, Controller**.

      The **Controller** panel displays.

   b. Click the **Config** tab. Enter the following values:

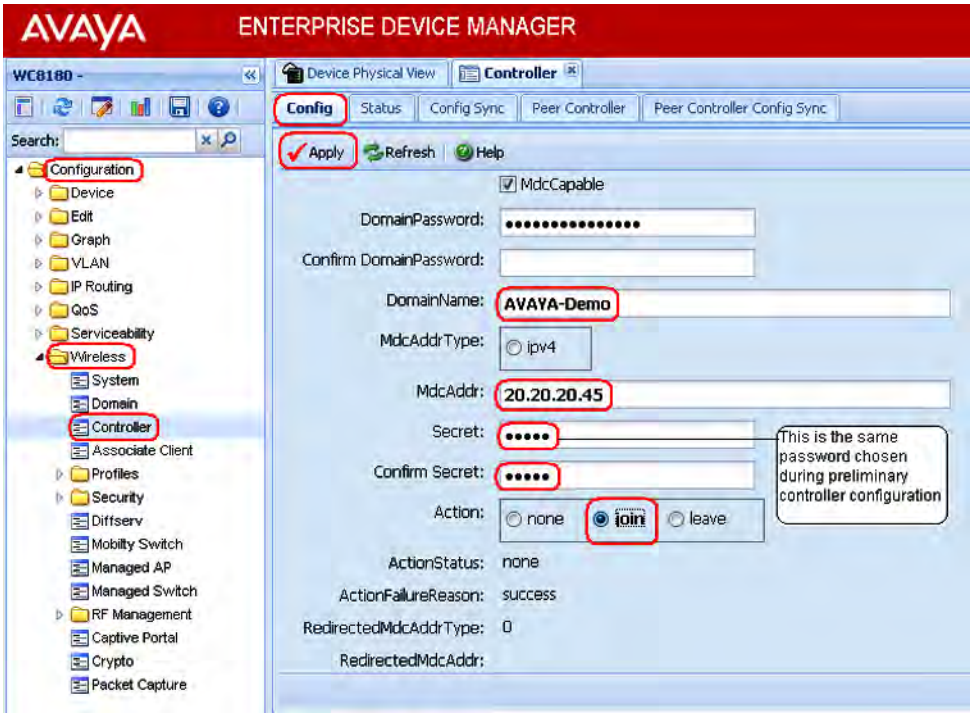
      - **Domain Name**: Name of the mobility domain to be created. For example, enter `AVAYA-Demo`.
      - **MdcAddr**: The wireless system interface IP address. Enter `20.20.20.45`.
      - **Secret**: MDC password

        Note:

        The MDC password is the same password you set when you configured the WC to be MDC capable. See Completing preliminary controller configuration on page 15.

   c. In the **Action** field, select **Join**.

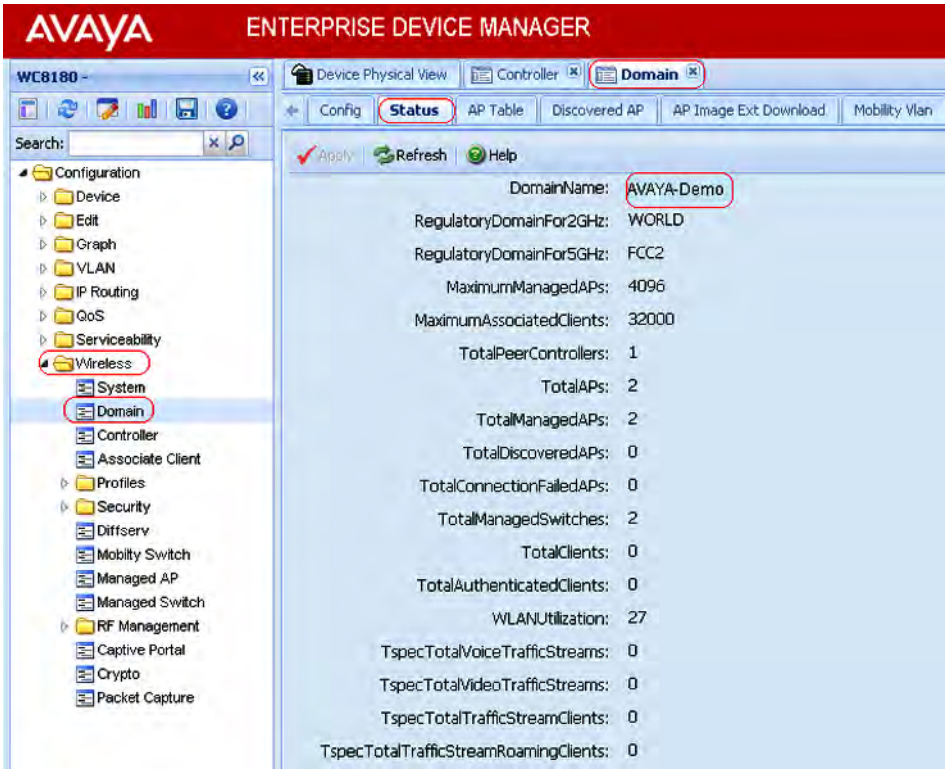
   d. Click **Apply**.



3. Verify mobility domain configuration.
   a. Navigate to **Configuration, Wireless, Domain**.

      The **Domain** panel displays.

   b. Click the **Status** tab. Verify the mobility domain configuration details.



4. Physically connect the Access Points (AP) to the network.

   Note:

   The AP 8120 is powered by Power over Ethernet (PoE) through either a PoE switch or an external power injector.

5. Configure the DHCP server for AP discovery.

   Note:

   The Avaya AP 8120 discovers the controller IP addresses using DHCP option 43 or DNS. This example uses the DHCP option 43. The Option 43 setting must be `08 08 41 56 41 59 41 20 41 50 01 04 14 14 14 2D`, where `14 14 14 2D` is the HEX representation of the controller IP address `20.20.20.45`.

   For a step-by-step procedure to configure the DHCP server, see DHCP server configuration for access points on page 105.

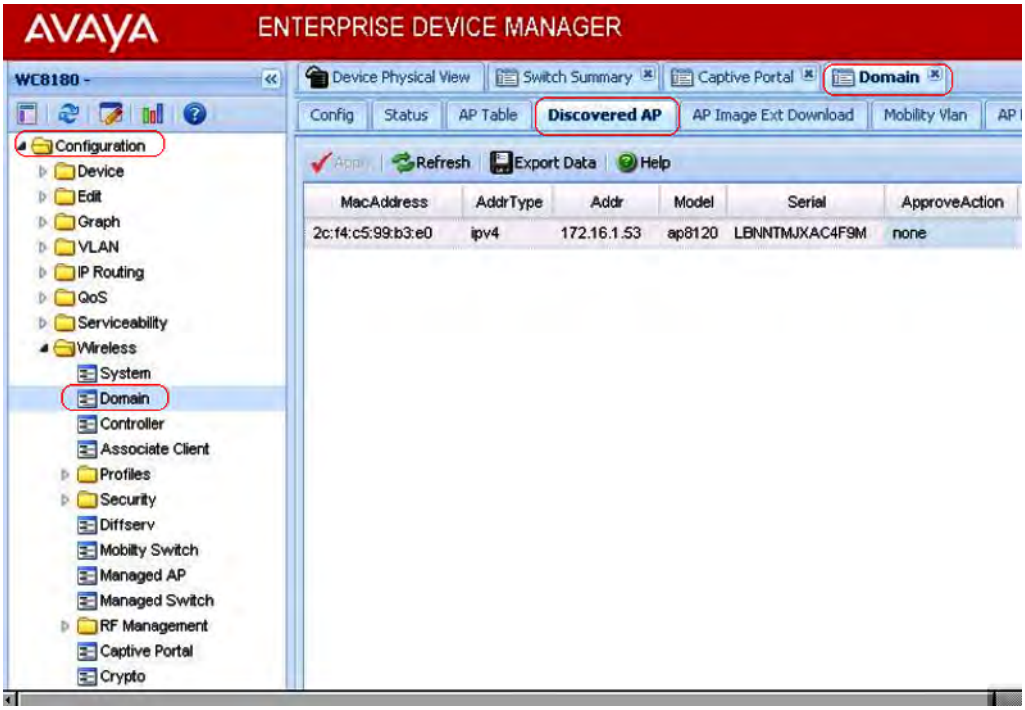
6. Power on the APs by connecting them to the PoE switch or power injector.
7. Verify that the APs are connected to the DHCP server. Perform the following steps.
   a. Launch the DHCP Server Manager.
   b. Navigate to **DHCP**, **<your DHCP server>**, **Address Leases**.
   c. Ensure that the IP addresses of all APs are listed.

Once the AP receives the controller information from the DHCP server, the AP connects to the controller. All discovered APs appear in the Discovered AP database on the wireless controller.

8. Verify the Discovered AP database.
   a. Navigate to **Configuration**, **Wireless**, **Domain**.

      The **Domain** panel displays.

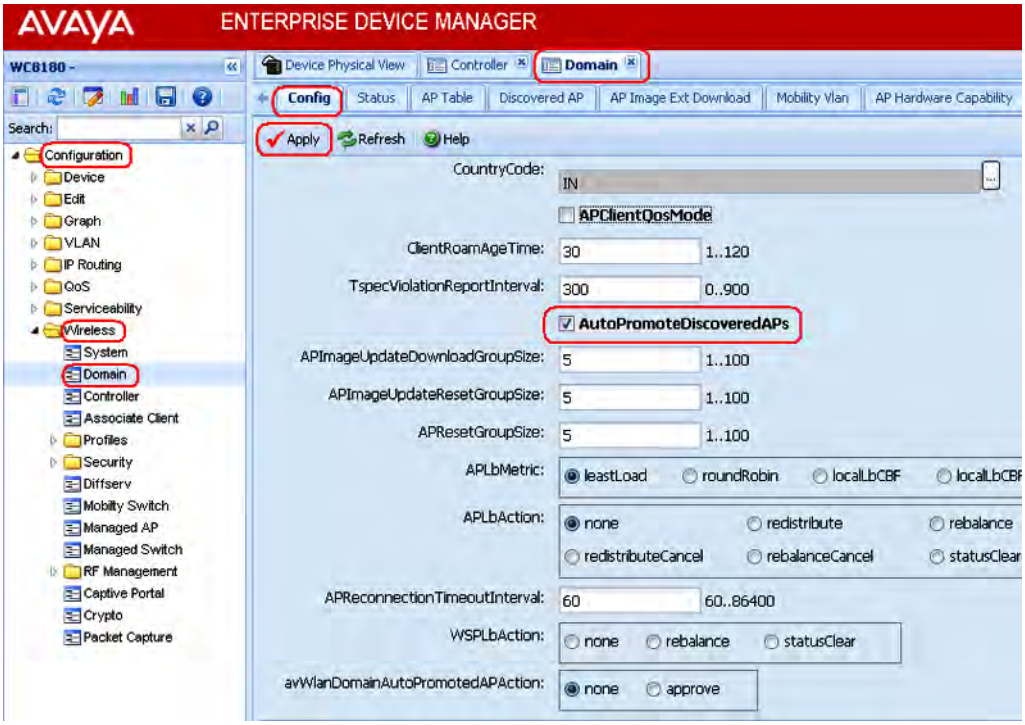
   b. Click the **Discovered AP** tab. Verify that all APs and their details (including the MAC addresses) are correctly listed.



9. Enable auto-promotion of discovered APs. Auto-promotion enables all discovered APs to be automatically promoted to the controller-managed state as soon as they are discovered.
   a. Navigate to **Configuration**, **Wireless**, **Domain**.

      The **Domain** panel displays.

   b. On the **Config** tab, select the **AutoPromoteDiscoveredAPs** checkbox.
   c. Click **Apply**.



10. Verify the AP status.

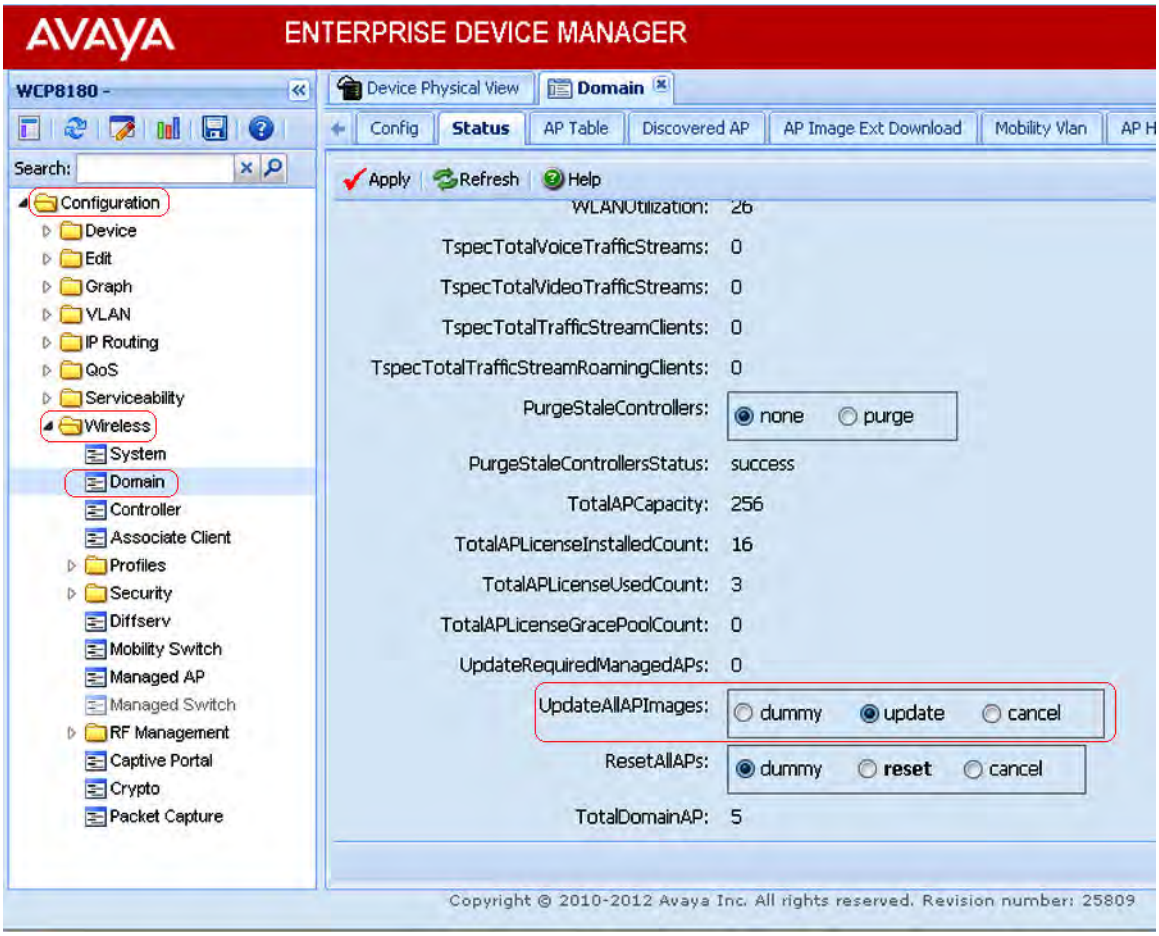
    a. Navigate to **Configuration**, **Wireless**, **Domain**.

       The **Domain** panel displays.

    b. Click the **AP Table** tab. Verify that an entry exists for all APs connected to the domain. An entry for an AP in this table indicates that this AP is managed by the controller of the domain.

11. Perform a bulk image upgrade of all APs.
    a. Navigate to **Configuration**, **Wireless**, **Domain**.

       The **Domain** panel displays.
    b. Click the **Status** tab.
    c. On the **UpdateAllAPImages** option button, select **Update**.
    d. Click **Apply**.



12. Complete the following steps to create profiles (network, radio and AP profiles) using the EDM. These steps are provided for demonstration purposes.

    Important:

    When you configure profiles in the network (such as AP profiles, network profiles and radio profiles) ensure that you configure the profile name to be unique across the network, for each of the profiles.

    Also, ensure that you do not configure profile names that have similar characters or letters and differ only in their *case*.

13. Create a mobility VLAN.

    a. Navigate to **Configuration**, **Wireless**, **Domain**.

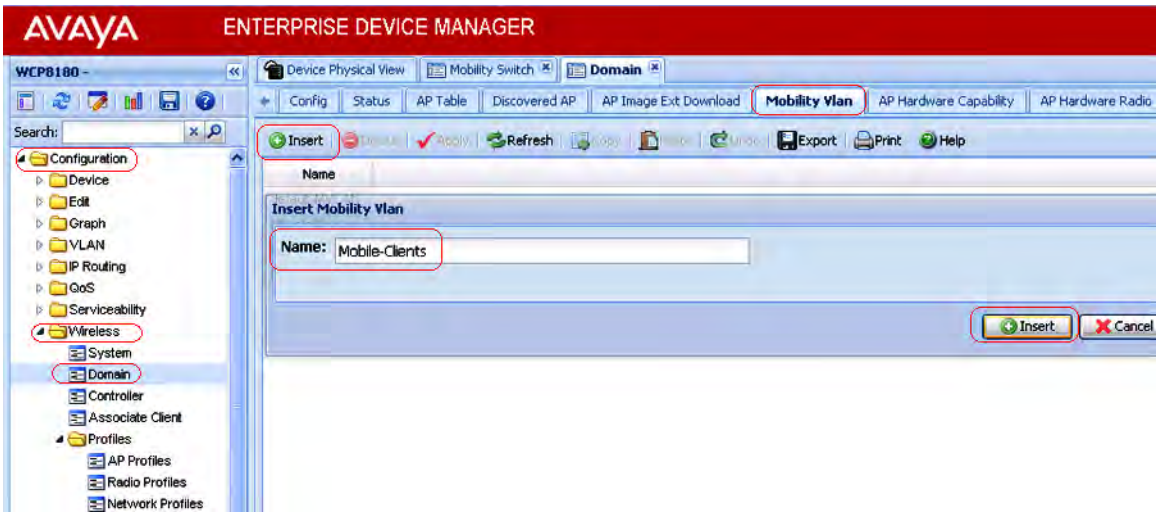
       The **Domain** panel displays.

    b. On the **Mobility VLAN** tab, click **Insert**.

       The **Insert Mobility Vlan** window displays.

    c. Enter a name for the Mobility VLAN that you want to create, for example, `Mobile-Clients`.

d. Click **Insert**.



14. Create a Captive Portal (CP) profile.

Important:

For the Captive Portal to work properly, ensure that the Wireless or System interface of the AMDC does not have the `Management` flag enabled.

Important:

If you want to host the Captive Portal on a guest VLAN, ensure that the Captive Portal IP address is an active VLAN interface IP on any controller in the domain, except the Management VLAN IP address, the System VLAN IP address, or the wireless interface IP address of that controller. The Captive Portal IP address must physically exist on one of the domain controllers.

a. Navigate to **Configuration**, **Wireless**, **Captive Portal**, and click on the **Profile** tab.

b. Click **Insert**.

The **Insert Profile** screen appears.

c. Enter a name, for example, `PRF-CP`. Enter values for other fields as applicable or retain defaults.

d. Click **Insert** to create the Captive Portal (CP) profile.

15. (Optional) Configure a Captive Portal walled garden.

Sometimes, a Captive Portal user may need to access network resources in the intranet or public Web sites from an enterprise network without requiring to first undergo Captive Portal authentication. To support these user requirements, the WLAN 8100 solution now allows the configuration of the IP addresses of Web hosts in a Captive Portal profile so that the user can access these hosts without the need for authentication. This is known as the Captive Portal Walled Garden.

When a Captive Portal Walled garden is configured, unauthenticated users can access certain hosts in the network by specifying the IP addresses of those hosts in Captive portal profiles.

a. Navigate to **Configuration**, **Wireless**, **Captive Portal**.

b. Click the **Profile** tab.

c. Select a Captive Portal profile and click **Walled Garden**.

d. On the **Walled Garden** tab, click **Insert**.

The **Insert Walled Garden** dialog box displays.

e. In the **Host** field, enter the Walled Garden host IP address in the format `xx:xx:xx:xx`. The supported host type is Ipv4.

f. Click **Insert**.

16. Configure the Captive Portal (CP) user database.

Navigate to **Configuration**, **Wireless**, **Security**, **Security**.

Configure a CP user.

a. Click the **Local DB Client** tab.

b. Click **Insert**.

The **Insert local DB client** window appears.

c. Enter a name (for example, `guest`) and password and click **Insert**.

Configure a CP user group.

a. Click the **Local DB Client Group** tab.

b. Click **Insert**.

The **Insert local DB client group** window appears.

c. Enter a group name (for example, `UG-guest`) and click **Insert**.

Associate the user with the user group.

a. Click the **Local DB Client Group Associate** tab.

b. Click **Insert**.

c. Enter the user name (for example, `guest`) and the user group name you want to associate this user with (`UG-guest`).

d. Click **Insert**.

17. Configure Diffserv. Differentiated services or DiffServ specifies a simple and scalable mechanism for classifying and managing network traffic and providing quality of service (QoS) to wireless clients, on modern IP networks.

Important:

Ensure that you configure DiffServ policy and classifier block names that are unique across the network. Do not configure policy and classifier names that have similar letters and characters and differ only in their *case*.

As part of DiffServ configuration, you:

- configure a DiffServ classifier block
- associate classifier block elements with the classifier block
- configure a DiffServ policy and associate the classifier block with the DiffServ policy

Configure a Diffserv classifier block named `classifier1`. Repeat these steps, if required, to configure multiple classifier blocks.

a. Navigate to **Configuration**, **Wireless**, **DiffServ**.

b. Click the **Classifier Block** tab.

c. Click **Insert**.

The **Insert Classifier Block** window appears.

d. Enter a name in the **Classifier Name** field, for example, `classifier1`, and click **Insert**.

Configure classifier elements for the classifier block `classifier1`. You can configure multiple classifier elements for the classifier block.

a. Select the classifier block `classifier1` and click **Element**.

The **Insert Classifier Element** dialog box appears

b. In the **Classifier Element** tab, click **Insert**.

c. The **Id** field displays the classifier element Id. You can choose to retain this Id or update it.

d. In the **MatchEntryType** field, select a classifier element to be applied to traffic data packets. Update a value for the selected criteria in the field provided.

e. Click **Insert** to insert the classifier element.

Configure a Diffserv policy `policy1` and associate the configured classifier block `classifier1` with this policy.

a. Navigate to **Configuration**, **Wireless**, **DiffServ**.

b. Click the **Policy** tab.

c. Click **Insert**.

The **Insert Policy** window appears.

d. Enter a policy name in the **Name** field, for example, `policy1` and click **Insert**. Ensure that the policy name is unique across the network.

Associate the configured classifier block `classifier1` with the DiffServ policy `policy1`

a. Select the policy `policy1` and click **Classifier Block**.

   The **Insert Policy Classifier Block** dialog box displays.

b. Click the button besides the **ClassifierBlockId** field and select the configured classifier block `classifier1` from the pop-up dialog box.

c. Select one of the following options in the **EntryType** field, and configure appropriate values for these options in the additional fields provided.

   - markCos
   - markIpDscp
   - markIpPrecedence
   - drop
   - allow

   Important:

   If you use a DSCP value of `48/56` and a cos value of `7`, the Access Point (AP) overrides the DSCP priority and changes its priority to `0`. This causes a change in the traffic priority.

   Some DSCP priorities are specifically marked for network control traffic and these DSCP priorities must not be used in uplink traffic from wireless clients. The set of DSCP priorities that are overridden by the AP is implicitly derived from the *QoS egressmap* table maintained in the AP. All DSCP priorities mapped to 802.1p priority 7 are considered to be network control packet priority. For the default QoS egressmap, DSCP priorities 48 and 56 are considered as network control packet priorities and are overridden on the client generated uplink packets.

   When an AP detects client packets with DSCP values set to a network control packet priority, the AP resets the DSCP value on those packets to 0.

   For more information on the *QoS egressmap* table and the WLAN 8100 DSCP priority, see the *Feature Overview for Avaya WLAN 8100*, NN47251-102.

d. Click **Insert**.

18. Configure a network profile.

    Note:

    Optionally configure the following in the network profile:

    - Station Isolation of wireless clients in the network:

      Station Isolation prevents traffic from one wireless client in a mobility VLAN inadvertently reaching another wireless client on the same mobility VLAN. This is required typically in environments such as a hotel or public hot spots. The word *station* refers to mobile devices or clients that are compliant with IEEE 802.11 a/b/g/n

standards. These devices include lap-tops, smart phones and PDAs, wireless handsets and RFID tags.

- MAC-based authentication (or MAC validation):

  In this method of authentication, the MAC address of a mobile client is used as a credential for authentication. For MAC validation to be performed, it must be first be enabled in a network profile.

  MAC based authentication is done in one of the following ways:

  - using blacklists and whitelists
  - authenticating against a remote RADIUS server

- Captive Portal (guest) user authentication

a. Navigate to **Configuration, Wireless, Profiles, Network Profiles**.

b. On the **Network Profile** tab, click **Insert**.

   The **Insert Network Profile** dialog box appears.

c. Update the fields as follows and click **Insert** to save your changes.

Variable	Value
Id	Enter the Id to uniquely identify the wireless network. The range is 1 to 64.
Name	Enter a name for the network profile, for example, `AVAYA-Demo`. **Important:** Ensure that the profile name is unique across the network. Ensure also that you do not create profile names that have similar letters and characters, but are different only in their *case*.
ARPSuppressionEnabled	Select to enable ARP suppression.
LocalUserGroup	Enter a local user group name with a maximum of 32 characters.
ClientConfigVlan	Specify a mobility VLAN to associate with the network profile. The default Mobility VLAN Name is used if you do not provide an explicit client VLAN assignment. Click the button beside the **ClientConfigVlan** field. A pop-up window displays a list of the configured mobility VLANs. Select `Mobile-Clients` (created in step 13) from the list. You can click **Refresh** to refresh the list of configured mobility VLANs. Select a mobility VLAN and click **Ok**.

Variable	Value
UserValidation	Select the appropriate Captive Portal user validation mode. The options are: • open—Validation is using any user name. • radius—Validation is using the Active Directory. • local Security DB—Validation is using the local security database. • openGuest—No login credential validation happens and the user is neither prompted to enter a user name nor a password.
StationIsolationEnabled	Select to enable Station Isolation on the network profile.
WirelessGWMacAddr	Specify the MAC address of the wireless gateway of the mobility VLAN. Enter the gateway MAC address in the format `xx:xx:xx:xx:xx:xx`. **Note:** This field is enabled only if Station Isolation is enabled on the network profile.
SSID Settings	
SSID	Enter the SSID name with which wireless clients will associate. **Important:** When you configure an SSID for a network profile, ensure that it is unique across the network. SSIDs can have a maximum of 32 characters. Also, ensure that you do not configure SSIDs that have similar characters but are different only in their *case*. For example, do not configure the SSIDs *avaya-demo* and *AVAYA-DEMO* within the same network.
SSIDHideInBeacons	Select to enable or disable the inclusion of SSID in AP beacons.
NoProbeResponse	If client broadcasts probe requests to all available SSIDs this option controls whether or not the system will respond to the probe request.
802.1x settings	
SessionKeyRefreshPeriod	Enter the 802.1x session key refresh period. The value can either be 0 or in the range 0 to 86400.
GroupKeyRefreshPeriod	Enter the group key period. Enter a refresh period in seconds. The value can either be 0 or in the range is 0 to 86400.
RADIUS settings	
RadiusOffload	Select to enable RADIUS offload.

Variable	Value
AuthenticationRP	Enter the profile name of the configured Authentication RADIUS profile. The range is 0 to 32 characters.
RadiusAccountingEnabled	Select to enable RADIUS accounting.
AccountingRP	Enter the profile name of the configured Accounting RADIUS profile. The range is 0 to 32 characters.
Security	
MacValidation	Select to enable validation of MAC addresses of client devices in the network. When you select this check box, all new client devices to the wireless network are automatically blacklisted by the controller and denied access to wireless services. To enable wireless services for a blacklisted device, you must explicitly remove this device from the blacklist and configure this device as white-listed.
MACValidationMode	Select the client device MAC validation mode. The options are: • local Whitelist: The client MAC address is validated against a local Whitelist database. On successful verification, the client device is granted network access. • radius: The client MAC address is validated against a remote RADIUS server.
802.11 Security	Select to enable 802.11 security.
SecurityMode	Select one of the following security modes: • open • wepStatic • wep802.1x • wpaPersonal • wpaEnterprise

d. Click **Insert**.

19. Apply the DiffServ policy `policy1` to the network profile.

a. Navigate to **Configuration**, **Wireless**, **Profile**, **Network Profiles**.

b. Select the network profile you created in step 18 and click **Edit Profile**.

c. Click the **QoS** tab.

d. In the DiffServ section, click the button beside the **DiffServPolicyDown** field.

e. In the **DiffServPolicyDown** window, select `policy1` (the DiffServ policy that you created in step 5), and click **Ok** to save changes.

f. You can similarly configure the **DiffServPolicyUp** field with the DiffServ policy `policy1`.

g. Click **Apply** to save your changes.

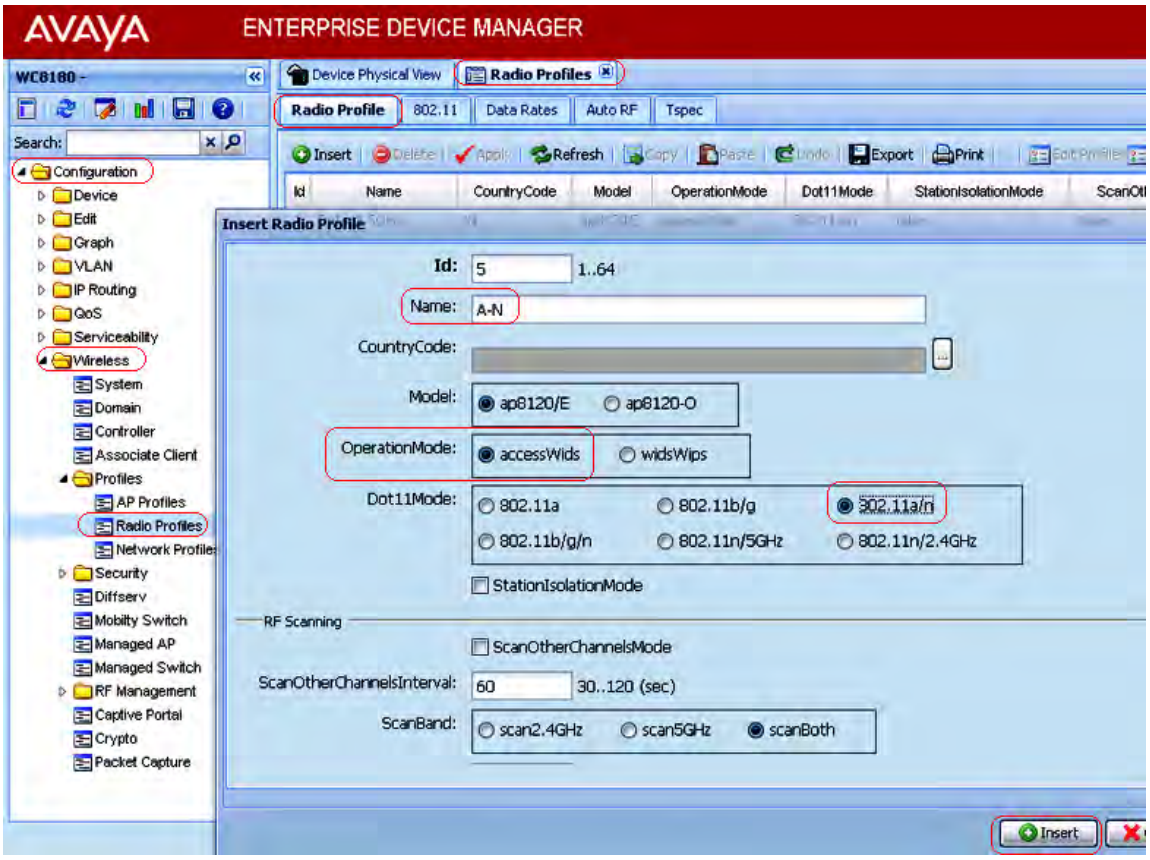
20. Create access radio profiles. In this example, you create `a-n` and `bg-n` radio profiles based on the radio frequency.

    a. Navigate to **Configuration, Wireless, Profiles, Radio Profiles**.

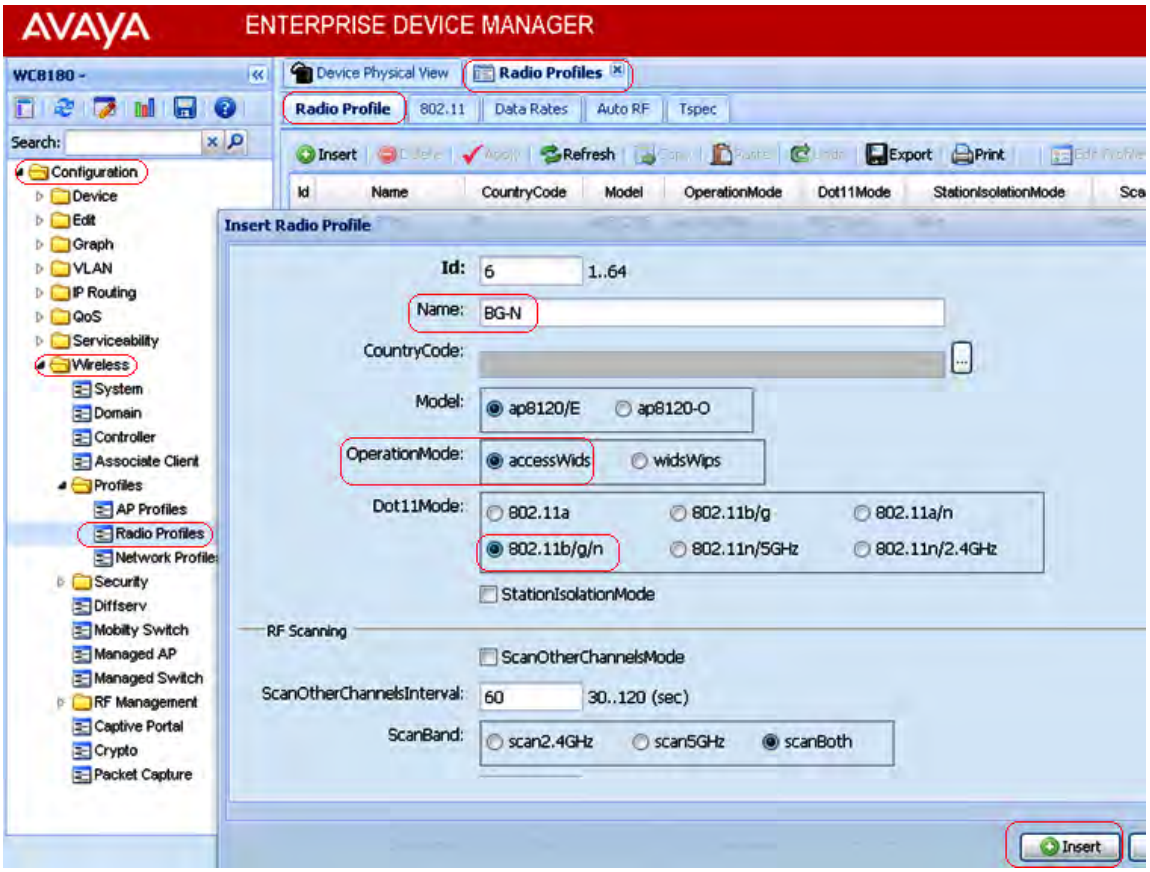
    b. On the **Radio Profiles** pane, click **Insert**.

    The **Insert Radio Profile** window displays.

    c. For an `a-n` radio profile, update the fields as shown in the following figure, and click **Insert**.



d. For a `bg-n` radio profile, update the fields as shown in the following figure, and click **Insert**.



21. Enable client band steering and load balancing on the configured Access radio profiles. This step is optional but is highly recommended.

    Client Band Steering is a technique used to increase the overall capacity of a dual-band wireless network composed of multiple APs that use both the 2.4 GHz and 5.0 GHz radios.

    Client stations predominantly support 2.4GHz. Many modern client stations have dual-band support yet tend to favor connection to 2.4GHz networks (although some popular modern clients still only support 2.4GHz, e.g. the Apple iPhone 4). As a result, dual-band networks have the 2.4GHz band heavily utilized, and the 5GHz band under utilized. The objective of Client Band Steering is to encourage 5GHz capable client stations to use the 5GHz radio instead of the 2.4GHz radio, leaving the 2.4GHz radio for stations that only support 2.4GHz.

    As part of Client load-balancing configuration, you enable/disable the Load balancing. After you enable load balancing, you configure the following parameters:

    - utilization-start (%) — Utilization level at which client association load balancing begins
    - utilization-cutoff (%) — Client association load balancing cutoff. If this threshold is exceeded, all further client associations are refused.

Note:

This cutoff is useful so that controller CPU utilization is maintained at an optimum level. If CPU utilization goes beyond 100%, it causes the controller to restart which in turn results in an unprecedented controller outage.

Enable client band steering for the `A-N` radio profile. Repeat for the `BG-N` radio profile.

a. Navigate to **Configuration**, **Wireless**, **Profiles**, **Radio Profiles**.

   The list of configured radio profiles are displayed.

b. Select the radio profile and click **Edit Profile**.

c. In the **General** tab, in the Load balancing section, select **LoadBalancingMode**.

d. In the **ClientLBUtilizationStart** field, enter a number in the range 0–100.

e. In the **ClientLBUtilizationCutOff** field, enter a number in the range 1–100.

f. Select **BandsteeringMode**.

22. Optionally configure one or more capture profiles for a mobility domain.

    Capture profiles are used for remote packet capture. Remote packet capture enables live debugging to troubleshoot client related issues. It can also be used to monitor traffic in a wireless network. After you configure a capture profile, you must apply these profiles to specific access points (AP) within the mobility domain to start a packet capture.

    Note:

    You can configure up to 4 capture profiles.

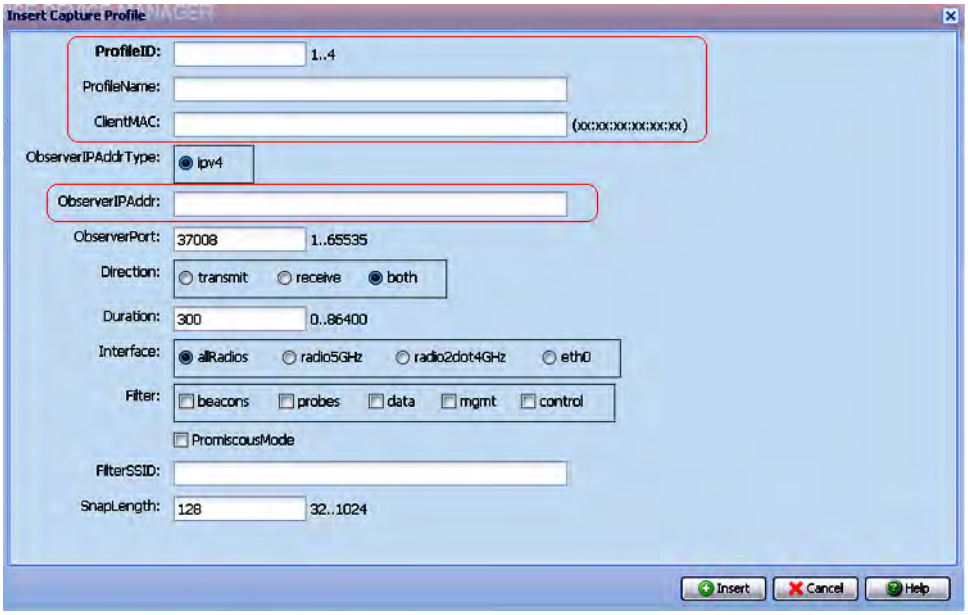
    You can choose to use the default capture profile (profile Id `1`), or configure a suitable capture profile as follows.

    a. Navigate to **Configuration**, **Wireless**, **Packet Capture**.

    b. Click the **Capture Profile** tab.

    c. Click **Insert**.

       The **Insert Capture Profile** dialog displays.



Update the following fields and click **Insert**.

- **Profile ID**: Enter a number in the range 1 to 4.
- **ProfileName**: Enter a name for the profile.
- **ClientMAC**: Enter a client MAC address.
- **ObserverIPAddr**: Enter the IP address of the observer host PC.

  Important:

  The default value of the snap length is 128 and the value can be modified between 32 and 1024.

  In Wireshark, when the packet length exceeds the configured snap length in the capture profile, the captured packets are displayed as **Malformed**. If you see the presence of malformed packets, adjust the snap length to an appropriate value.

23. Create an Access Point (AP) profile and associate the AP profile with appropriate radio and network profiles.

    Create an AP profile `AP-Profile-1`.

    Note:

    You can optionally configure the AP profile for AeroScout and Ekahau RTLS support.

    - AeroScout support:

      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 benefits such as asset tracking, process automation, theft prevention and increased utilization.

- Ekahau RTLS support:

  The Ekahau Real-Time Location System (RTLS) is a fully automated tracking solution that continuously monitors the location of assets and people in a wireless network.

a. Navigate to **Configuration, Wireless, Profiles, AP Profiles**.

b. On the **AP Profile** tab, click **Insert**.

   The **Insert AP Profile** dialog box appears.

c. Update the fields as follows and click **Insert** to create the AP profile.

Variable	Value
Id	Enter the entry ID value.
Name	Enter the name of the AP profile.
Country Code	Select the country code from the drop-down list. **Note:** When creating an AP profile, specify a country code or use the default 'primary' country code of the domain. To change a country code after a profile has been created you must delete the AP profile and create a new profile. Multiple-country domain names support a maximum of 32 countries.
Model	Select the model number.
ModelDefault	Select this check box to enable the default model.
(Optional configuration) To enable AeroScout support on the AP profile	
AeroscoutMode	Select to enable AeroScout RTLS support on the AP. The AeroScout feature provides location-based services for wireless networks. **Note:** The AeroScout feature is not supported on Outdoor APs (AP8120–O).
(Optional configuration) To enable of Ekahau RTLS support on the AP profile	
EkahauTagBlinkMode	Select to enable the Ekahau tag blink mode on the AP.
EkahauServerAddrType	Select the Ekahau server address type. The supported address type is ipv4.
EkahauServerAddress	Enter the Ekahau server IP address. The format is `xx:xx:xx:xx`.
EkahauServerUdpPort	Enter the Ekahau server UDP port number. The default port number is 8569. The range is 1024 to 65535.

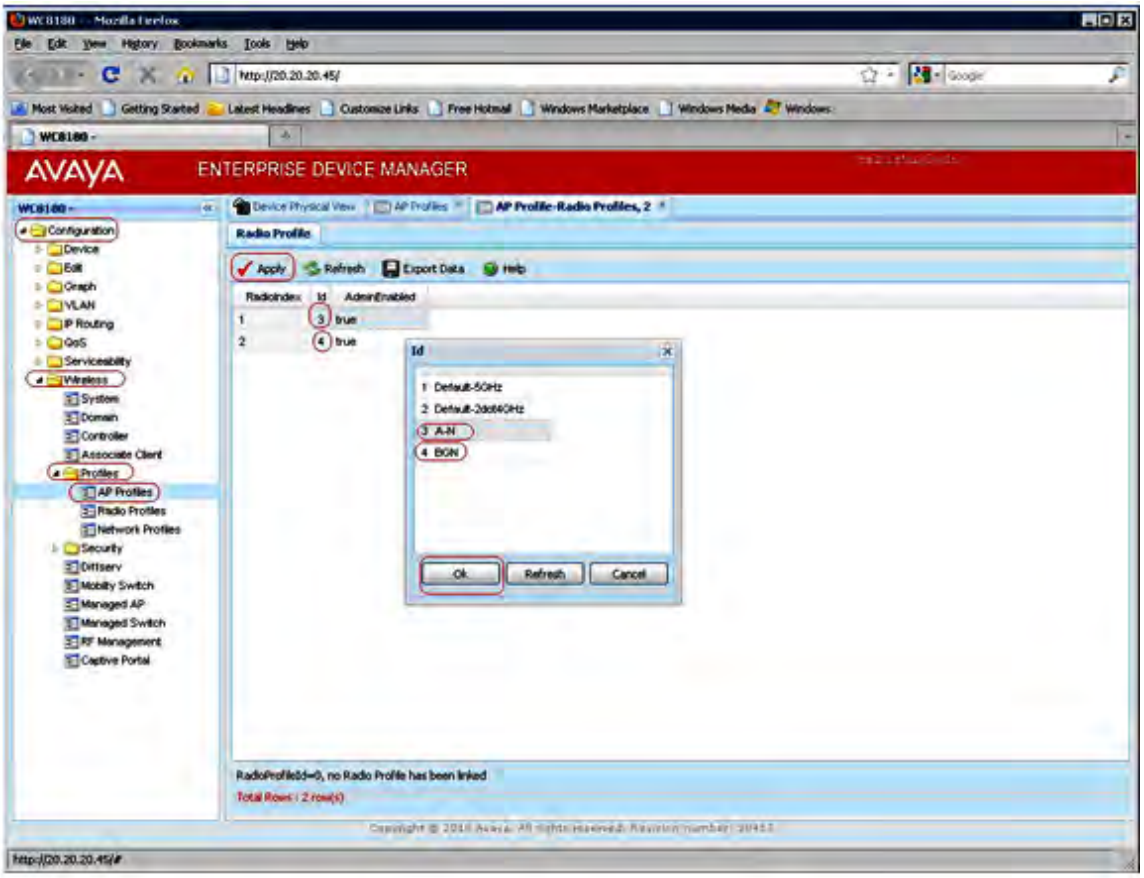
Associate the AP profile `AP-Profile-1` with configured access radio profiles.

a. Select the AP profile and click **Radio Profiles**, as shown in the following figure.

b. On the **AP Profile-Radio Profiles** tab, assign the configured `a-n` and `bg-n` access radio profiles to the two AP radios (displayed as RadioIndex 1 and 2).

Tip:

Double-clicking on the **Id** field displays a pop-up window that allows you to select the created access radio profiles to associate the AP profile with.



c. Click **Apply** to save your changes.

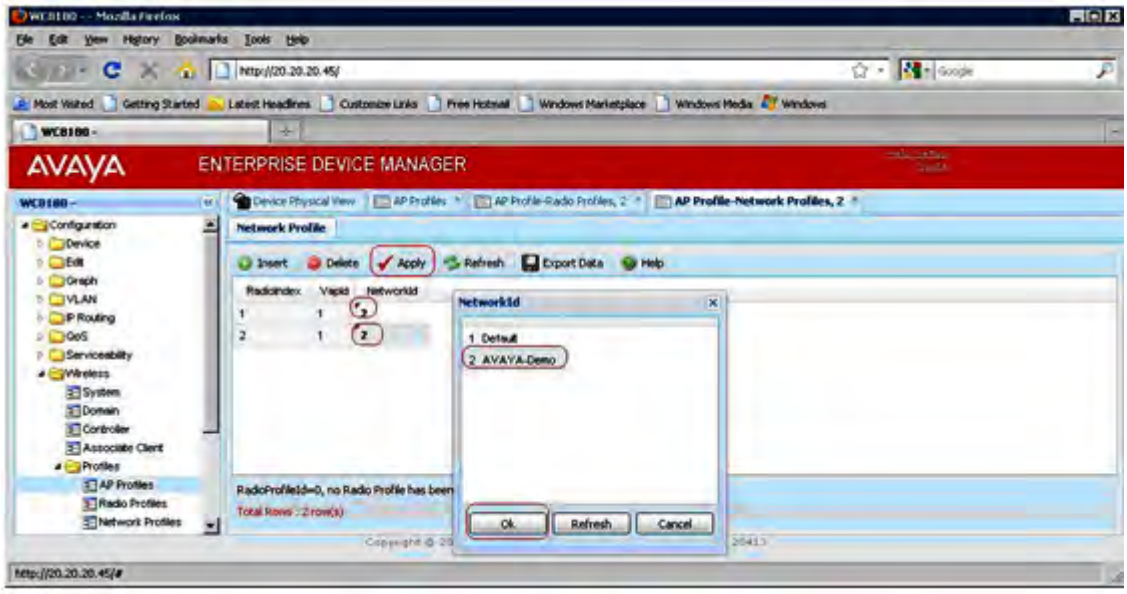
Associate the AP profile `AP-Profile-1` with configured network profiles.

a. To associate a network profile with the `AP-Profile-1`, select the AP profile from the list and click **Network Profiles**.

b. On the **AP Profile-Network Profiles** tab, map configured network profiles (for example, the configured network profile `AVAYA-Demo`) to the two AP radios (displayed as RadioIndex 1 and 2).

Tip:

Double-clicking the **NetworkId** field displays a pop-up window that allows you to select the network profile to associate the AP profile with.



24. (Optional) Configure Auto-RF channel plan and power plan. Configure the Auto-RF channel-plan for the a-n and bg-n radio frequency bands.

    Auto-RF power plan has the following modes:

    - Auto
    - Manual

    Configure the Auto-RF power plan.

    a. Navigate to **Configuration**, **Wireless, RF Management**, **Auto-RF**.
    b. Click the **Power Plan** tab.

       The current power plan status is displayed in the Status pane.
    c. Select the power plan adjustment mode in the **AdjustmentMode** field. The options are `manual` and `auto`.

       The default power plan mode is `Auto`
    d. Select the manual proposed adjustment action in the **ManualProposedAdjustmentAction** field. The options are `none`, `start` and `clear`.

       This field is applicable only if the power plan adjustment mode is `manual`.
    e. Specify the power plan threshold strength in the **ThresholdStrength** field.

       The range is `-99 dBm` to `-1 dBm`. The default power plan threshold strength is `-85 dBm`.

    Configure the Auto-RF channel plan.

    a. Navigate to **Configuration**, **Wireless, RF Management**, **Auto-RF**.
    b. Click the **Channel Plan** tab.
    c. Configure the Auto-RF channel plan using the following fields provided.

Variable	Value
Id	Displays the AP radio Id — 802.11a/n or 802.11b/g/n
Mode (Configurable)	The channel plan tuning adjustment mode for managed AP radios (802.11b/g/n and 802.11a/n). Double-click to display a drop-down list and select the channel plan configuration mode. The options are: • manual • interval • time
Interval (Configurable)	The interval (in hours) at which to perform *manual* channel plan tuning. Double-click to enter the interval in hours. The range is 1–24.
Time (Configurable)	The next scheduled time in minutes at which to perform channel plan tuning. Double-click to enter the time. The range is 0 to 1439 minutes. 0 minutes stands for midnight.
HistoryDepth (Configurable)	The channel plan history-depth. Double-click to enter the history-depth. The range is 0 to 10.
Operational	Displays the operational status of the channel plan tuning adjustment.
LastIterationStatus	Displays the last channel plan adjustment iteration number.
ManualAction (Configurable)	The selected *manual* channel adjustment action. Double-click to display a drop-down list and select an action. The options are: • None • Start- Run the Proposed Channel Adjustment algorithm. • Apply- Apply the same to network. • Clear- Clear the calculated 802.11a/b/g/n channel plan.
ManualStatus	Displays the status of the manual channel plan adjustment.
LastAlgorithmTime	Displays the date and timestamp of the last channel plan adjustment.

d. Click **Apply** to save your changes.

25. Manually add the Access Points (AP) to the Domain AP database to promote the APs to be managed by the controller of the domain.

    Note:

    Perform this step if you need to manually promote an AP to be managed by the controller. If your system is configured for auto-promotion (Step 9 in this procedure), all

discovered APs are automatically added to the Domain AP database and are promoted to be managed by the controller.

a. Navigate to **Configuration**, **Wireless**, **Domain**.

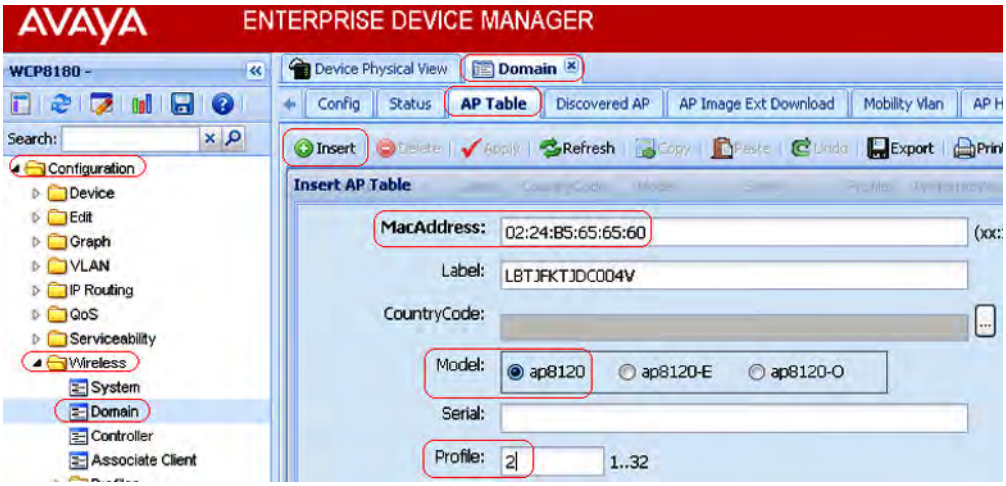
b. On the **AP Table** tab, click **Insert**.

The **Insert AP Table** window displays.

c. Enter AP details including the AP MAC address as shown in the following figure.

Tip:

Locate the AP MAC address on the back of the physical AP.



d. Click **Insert**.

26. Map the mobility VLAN to the local VLAN.

a. Navigate to **Configuration, Wireless, Mobility Switch**.

b. Click the **Agent Vlan** tab.

c. Click on the row that shows the mobility VLAN `Mobile-Clients`.

d. Double-click the **LVID** field. A pop-up displays the VLAN IDs. Select the VLAN ID `20`.

e. Click **Apply**.

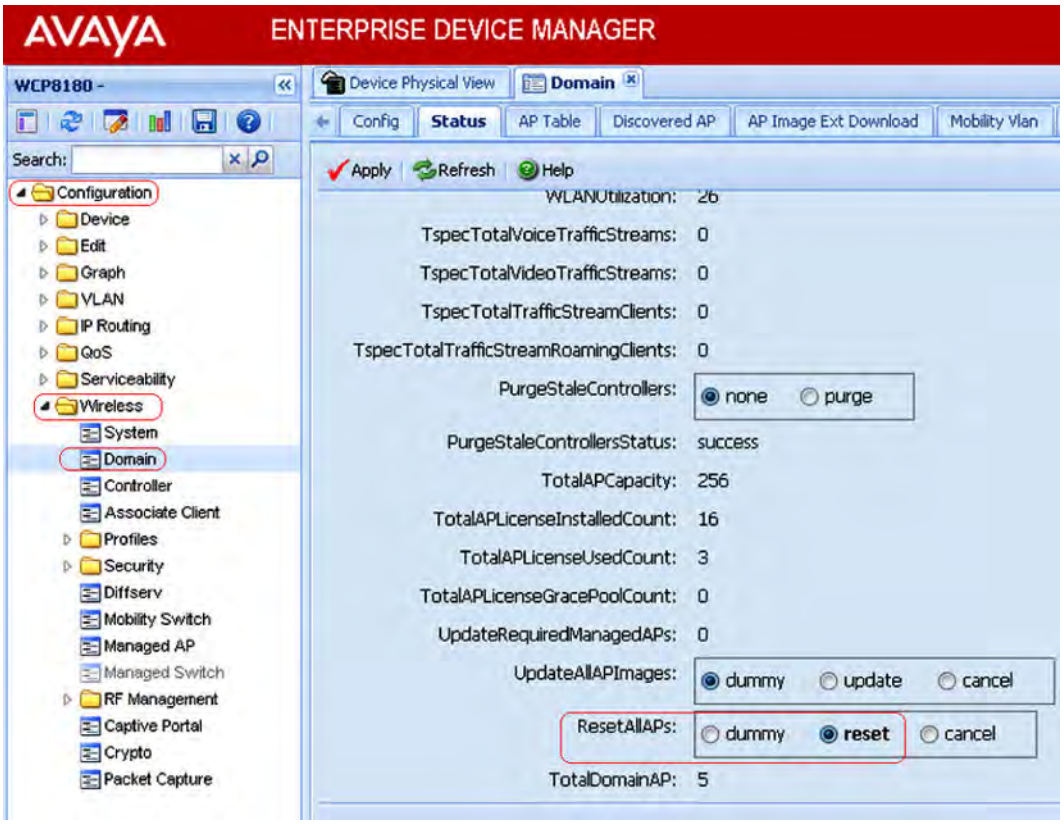
27. Optionally, if you made changes to any domain AP-related parameters (for example, the AP profile), you must reset the AP to apply the changes.

    a. Navigate to **Configuration, Wireless, Domain**.

    b. Click the **Status** tab.

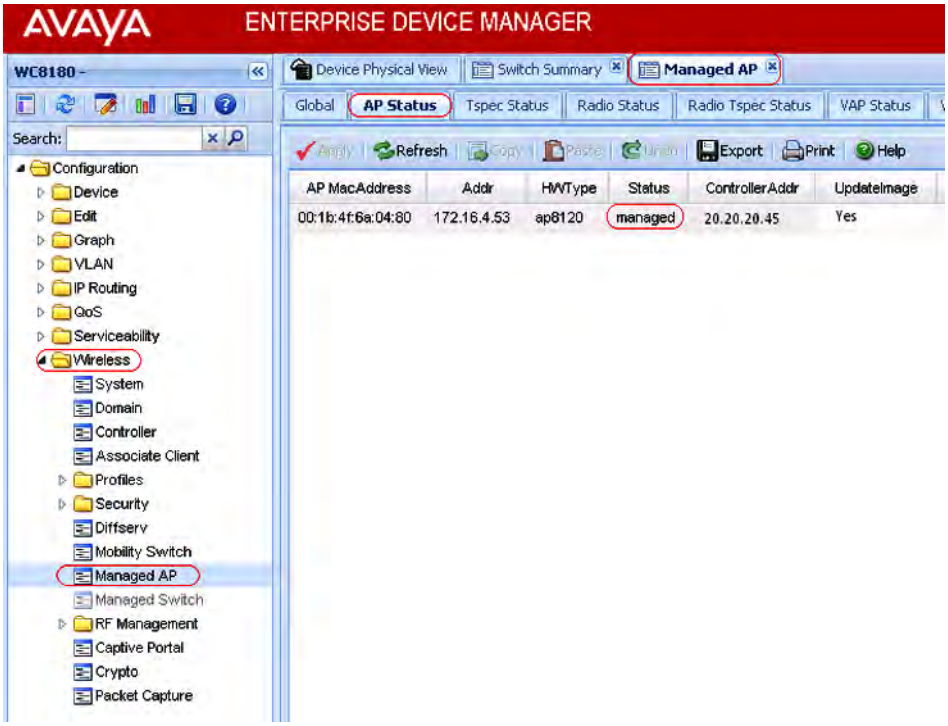
    c. In the **Reset All APs** option button, click **reset**.

    d. Click **Apply**.



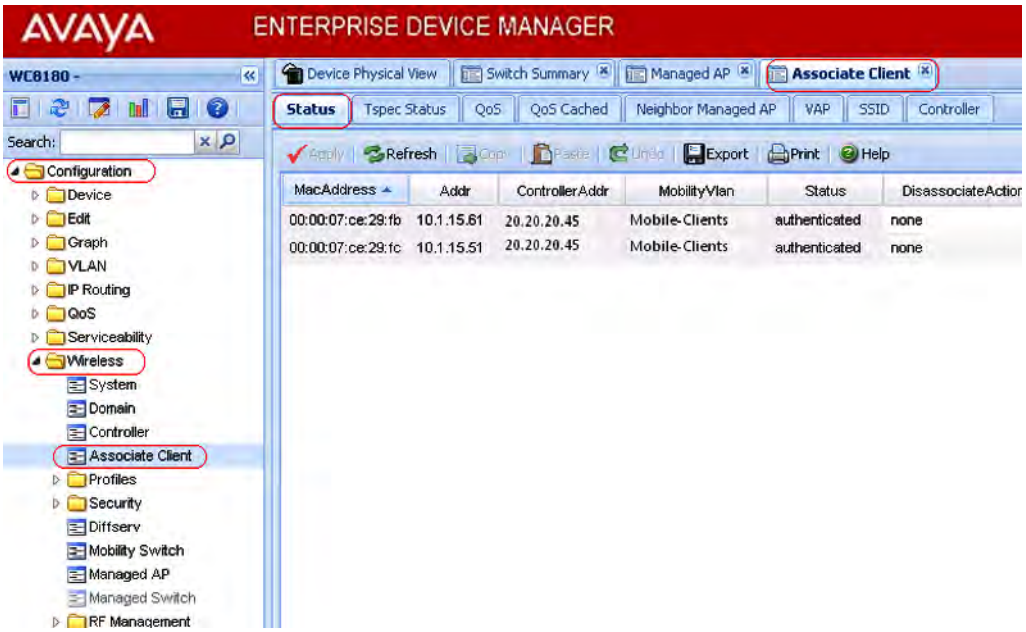
The wireless network is now ready for client connectivity.

28. To verify the wireless client connectivity, scan for wireless networks and connect a wireless client to the `AVAYA-Demo` network.
29. Monitor the wireless APs.
    a. Navigate to **Configuration, Wireless, Managed AP**.
    b. View the **AP Status** tab.



30. View the wireless client status.
    a. Navigate to **Configuration, Wireless, Associated Client**.

b. Click the **Status** tab.



31. You can also monitor wireless clients in the mobility domain using the remote packet capture feature. You must assign the capture profile configured in step 20, to an AP and then start a packet capture instance on the AMDC. You need an observer host PC to view the packet capture.

    To use the Remote Packet Capture feature, start a packet capture instance on the AMDC. You need an observer host PC to view the packet capture.

    Important:

    Before you start a packet capture, ensure that you do the following on the Observer host PC.

    - Download the Netcat application from the Web, to a location on your PC.
    - Open a UDP port for listening.

      Important:

      If you do not open the UDP port on the observer host then the capture device receives the `ICMP port unreachable` error for every capture packet in the capture stream. This severely impacts the performance.

    - Launch Netcat.

      On a Windows machine, execute the following command at the location of installation of Netcat. In the following example, `172.16.9.10` is the IP address of the Observer host PC and the observer port is `37008`.

      ```
      D:\RPC\NetCat>nc -l -u -p 37008 -s 172.16.9.10 -v
      listening on [172.16.9.10] 37008 ...
      ```

On a Linux machine, execute the command `nc -l -u <port number>`.

- Launch Wireshark to capture frames.
  - In Wireshark, ensure that you configure the CAPWAP UDP data port correctly. To decode the information packets correctly, this port must be the same as that opened for listening on the observer host PC. On Wireshark, navigate to **Edit**, **Preferences**, **CAPWAP**. Update the field **CAPWAP data UDP port**.
  - Also ensure that you deselect **Swap Frame Control**.

a. To start a packet capture, navigate to **Configuration**, **Wireless**, **Packet Capture**.

b. To start a packet capture, click the **Capture Action** tab.

Update the following fields.

- **APMAC**: Enter the MAC address of the AP to associate the capture profile with.
- **ProfileID**: Enter the profile Id of the capture profile configured in step c.
- **Action**: Click **start**.

  Note:

  Select **stop**, **restart** or **delete** to stop, restart or delete a packet capture respectively.

- Click **Apply**.

c. View packet capture instances and their status. Click the **Capture Instance** tab.

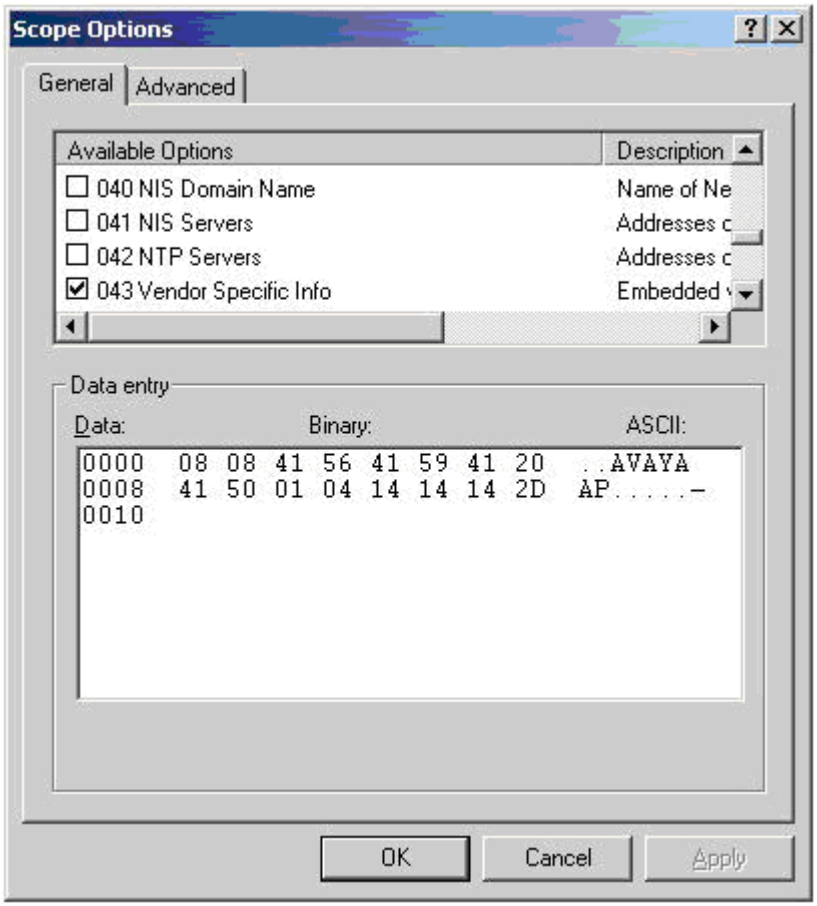
The details of all the capture instances, including details on the associated AP MAC addresses, the capture profile Ids and the status for each capture instance are displayed.

Appendix A: DHCP server configuration for access points

The WLAN 8100 solution requires configuration of DHCP Option 43 to ensure proper operation of Access Points (AP) and the solution overall. Complete this configuration before you attempt any operations that require network connectivity between the controller and APs. This configuration is dependent on the type of DHCP server in use in the network environment. Avaya recommends the use of either a Windows 2003 server or a Linux-based DHCP server.

Configuring the Windows server

1. Launch the DHCP Server Manager.
2. Navigate to **DHCP, <your-DHCP-server>, Scope, Scope Option, Option 043**.
3. Configure Sub-Option 8 as **AVAYA AP** with hexadecimal values for Domain Controller IP addresses.
4. Click **OK**.
5. In the following example,the Wireless Controller (WC) IP as `20.20.20.45` and its respective Hexadecimal value is `14:14:14:2D`.



Configuring the Linux server

Complete the following procedure on the Linux server.

1. Edit **dhcpd.conf (/etc/dhcp.conf)**.
2. Configure Sub-Option 8 as **AVAYA AP** with hexadecimal values for domain controller IP addresses.

   Note:

   Optionally, you can specify a UDP port for communications.
3. Restart **dhcpd**.

   For example, a Linux entry for Option 43 with controller addresses 20.20.20.45 and using port 61000 appears as follows:

```
option vendor-encapsulated-options 08:08:41:56:41:59:41:20:41:50 = 'AVAYA AP'
:01:04:14:14:14:2D = 20.20.20.45
:03:02:EE:48 = '61000'
```

   The actual Option 43 entry is

```
option vendor-encapsulated-options 08:08:41:56:41:59:41:20:41:50
:01:04:14:14:14:2D
:03:02:EE:48
```

where

- 08:08:41:56:41:59:41:20:41:50 – sub-option 08, length 8, “AVAYA AP”
- 01:04:14:14:14:2D – option IP, length 4, “20.20.20.45”
- 03:02:EE::48 – option port, length 2, “61000”.

Note:

The access point uses UDP port 61000 by default if Option 43 does not include the UDP port number.

Appendix B: Obtaining licenses from the Avaya Data Licensing portal

Before you begin

Ensure that you know the following:

- Ensure that you know your License Authorization Code (LAC).
- If you want to obtain licenses for WC 8180 controllers, you must record the MAC address of each controller on which you want to enable software features.

  Note:

  You need only a single MAC address for each controller. To find the MAC address from the console menu interface using the Avaya command line interface (CLI), use the `show sys-info` command in `privExec '#'` mode.

Procedure

1. Access the Avaya electronic licensing portal. On a browser instance, enter http://www.avayadatalicensing.com/.

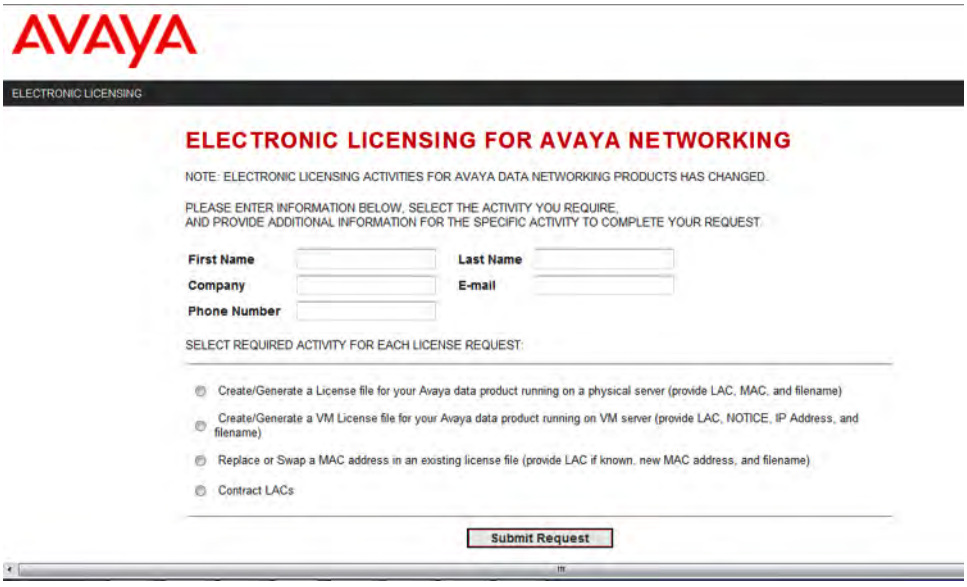


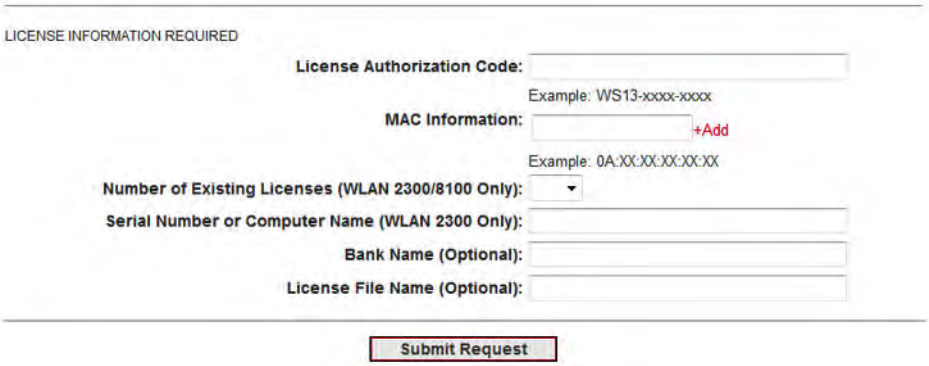
Figure 7: Avaya electronic licensing portal

2. Enter information in the fields provided.
3. Select the required activity using the option buttons provided.

Perform the following steps to create or generate a new license:

a. Select the option `Create/Generate a License file for your Avaya data product running on a physical server (provide LAC, MAC and filename).`

   Additional fields appear as follows:



b. Update the following mandatory information:

   - Enter the License Authorization Code
   - Enter the M AC address in the format `XX:XX:XX:XX:XX:XX`.
   - Select the number of existing licenses from the drop-down list.

4. Click **Submit Request**.

   You receive a confirmation for the request on the e-mail address that you provided. You also receive the license file on the same e-mail address typically within 24 hours.

Appendix C: Installing the WLAN Management System software

Use this procedure to install the current release of the WLAN Management System (WMS) software on Windows Server 2003, Windows 2008, or Linux platforms. This procedure covers the steps as necessary to install WMS on either the Linux or Windows platforms.

This procedure also describes additional steps that you need to perform if you have a previous version of WMS installed.

Before you begin

- Ensure that you have administrative privileges on your computer to perform the install.
- Download the latest version of the WMS application software from the Avaya Support site http://www.avaya.com/support.
- If you have a previous version of the WMS installed, you can either upgrade the WMS, or uninstall the previous version and perform a fresh install.

  Upgrade of the WMS is supported only from releases 2.x.x. The upgrade procedure automatically performs a back up of the required files (database, license and .smx files) and installs the current version of WMS. For more information on upgrading the WMS, see *Applying Upgrades and Patches to Avaya WLAN 8100*, NN47251-402.

  If you require to manually uninstall the previous version of the WMS, ensure that you do the following.

  Be sure to note down the paths to the location of these files on your computer.

  - Perform a database backup.
  - During the uninstall, backup the license file and `.smx` files as necessary, to a location on your computer. You will be prompted to restore the files during the install.
- Ensure that you close any open instances of an external TFTP server.

  When you install WMS, a built-in TFTP server is automatically installed and bound to the default TFTP port (port 69). So before you begin WMS install, you must close any running instances of an external TFTP server. Otherwise, the built-in WMS TFTP server does not get started.

Procedure

1. Launch the WMS installer.
   - **On Linux**:

To launch the WMS installer on a Linux platform, see Launching the WMS Installer on a Linux platform on page 114.

- **On Windows**:

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

The WMS installer launches displaying the **Introduction** window.

2. Click **Next**.

   The installer checks the system requirements. After a successful system check, the **Choose WMS Install Folder** window displays.

3. Choose the location of installation of the WMS on your computer.

   The **Choose WMS Install Folder** window displays the default path of installation of the WMS on your computer. Avaya recommends that you retain this default location.

   You can however choose a different installation path. Click **Choose...** to navigate to a location on your computer. At any time, click **Restore Default Folder** to restore the default path.

4. 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 `5.5` and the default server port is `3306`.

   - To retain the default values and proceed with the install, go to step 5.
   - 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 of MySQL Server on your computer is the same as or later than the default 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.

5. Click **Next**.
6. On the **WMS Port Configuration** window, select the ports to be used by the WMS Server for different operations or 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.
7. Click **Next**.

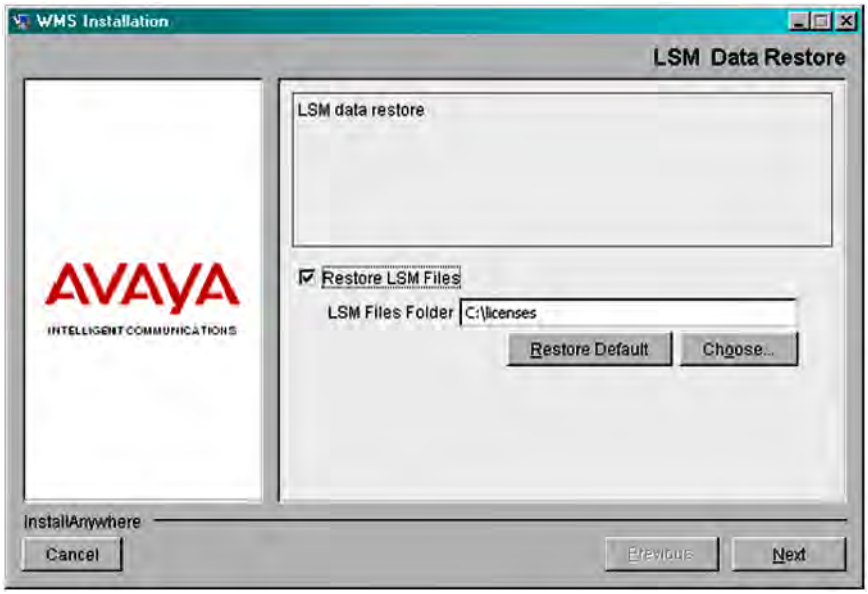
   The WMS installer displays a summary of the system requirements on the **System Requirements** window.
8. Click **Next**.

   The WMS installer displays the pre-installation summary.
9. Verify the pre-installation summary and click **Install**. The installation begins.
10. Optionally, perform the LSM (license) data restore on the **LSM Data Restore** window.

Note:

Perform this step only if you have the license file from a previous WMS version stored on your computer.

If this is first time installation of WMS, proceed to Step 11. You can download the WMS license *after* you complete the installation from the Avaya support site. See Obtaining licenses from the Avaya Data Licensing portal on page 108.



a. Select **Restore LSM Files**. Click **Choose...** to choose the location of the license file on your computer.

b. If required, click **Restore Default** to restore the path to the default location.

11. Click **Next**.

12. Optionally perform the WMS data restore on the **WMS Data Restore** window.

Note:

Again, perform this step only if you backed up the database, log and SMX files from a previous WMS install.

If this is a first time installation of WMS, proceed to step 13.

Perform the following steps to restore data:

a. Enable **Restore Database** to restore the database. Click **Choose...** to navigate to the path of the back up file.

   If required, click **Restore Default** to restore the path to the default location.

b. Enable **Restore SMX Files** to restore the backed up `.smx` files. Click **Choose...** to navigate to the path of the back up file.

   SMX files are site model files that typically capture the physical properties and layout of each floor in a building where the WLAN solution is deployed.

   If required, click **Restore Default** to restore the path to the default location.

13. Click **Next** to proceed with the install.

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

14. Click **Done**.

    You can now launch the WMS using your web browser.

15. Verify that the WMS is installed successfully.

    a. 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**.

    b. 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 Links

Launching the WMS Installer on a Linux platform on page 114
Uninstalling the WLAN Management System (WMS) software on page 115

Launching the WMS Installer on a Linux platform

Before you begin

Ensure that the latest WMS installer executable is at the location `/opt/Avaya/WMS` on your computer. For the latest software build information, refer to *Release Notes for Avaya WLAN 8100*, NN47251-400.

Procedure

1. Navigate to the location of the WMS installer executable *<latest software build>*.
2. Set execute permissions on the installer executable file. At the prompt, enter:

   ```
   chmod 777 WLAN8100_<latest software build>.bin
   ```

   To verify permissions, enter:

   ```
   ls -l WLAN8100_WMS_<latest software build>_Linux.bin
   ```

Sample output:

```
-rwxrwxrwx 1 root root 200470938 Sep 25 03:07 WLAN8100_WMS_<latest software
build>_Linux.bin
```

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

```
./WLAN8100_WMS_<latest software build>_Linux.bin
```

Sample output:

```
#./WLAN8100_WMS_<latest software build>_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...
```

Related Links

[Installing the WLAN Management System software](#) on page 110
[Variable definitions](#) on page 115

Variable definitions

Variable	Value
<latest software build>	Defines latest WMS software build number.

Related Links

[Launching the WMS Installer on a Linux platform](#) on page 114

Uninstalling the WLAN Management System (WMS) software

Use this procedure to uninstall WMS on Windows or Linux platforms.

Note:

Uninstalling the WMS removes only those features installed by the WMS installer. It does not remove the files and folders that you create after installation.

Procedure

1. Launch the WMS installer to being uninstallation.
   - **On Linux**:
     - Navigate to the uninstall folder at the location of installation of WMS on your computer.

Sample commands and output:

```
# cd opt/avaya/wms

# ls
backup  dbmigration  log    rrd    uninstall_WMS    WMS_InstallLog.log
bin     jre          lsm    smd    WLAN8100_WMS_<latest software
build>_Linux.bin
conf    lib          MySQL  smx-repository          webapps

# cd uninstall_WMS
```

- Enter the command `./Uninstall`.

  This launches the WMS installer, to begin the uninstall.

- **On Windows**

  From the **Start** menu, click **All Programs, WMS, Uninstall WMS**.

  Note:

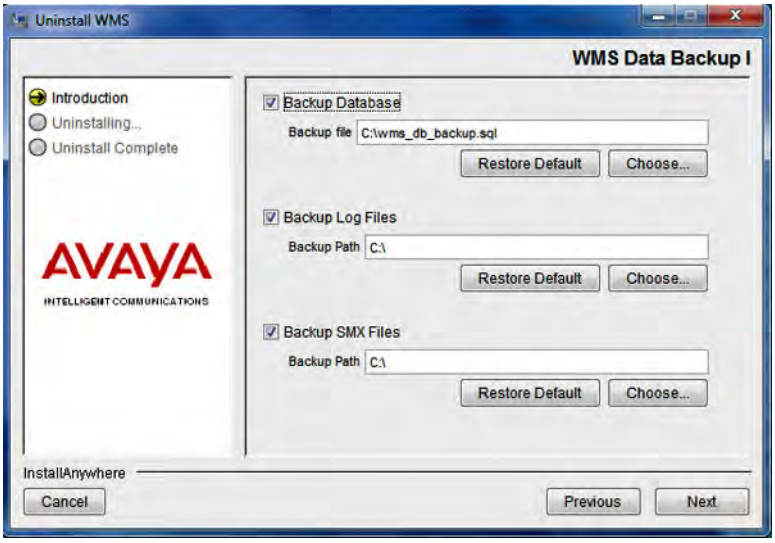
  By default, WMS is installed at a default location on the **C drive**. If you installed WMS at a location other than the default location, you must uninstall WMS from that location.

The **Uninstall WMS** window displays.

2. Click **Next**.

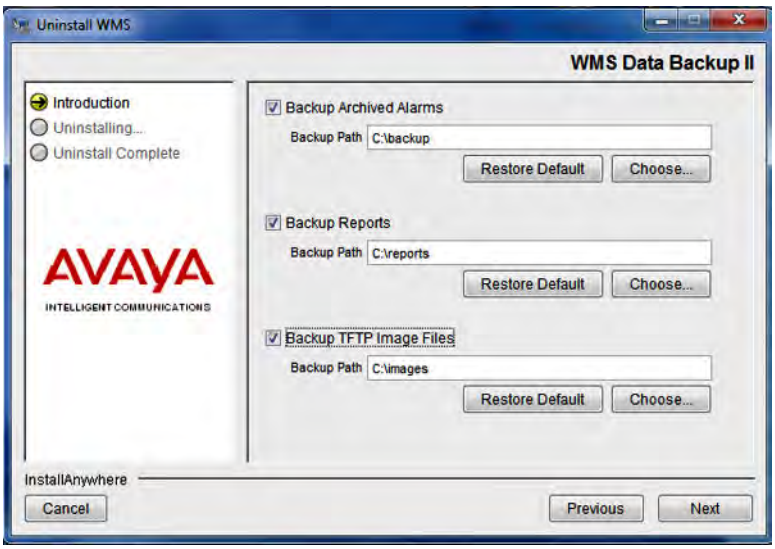
   The system displays the **WMS Data Backup 1** window displaying the fields necessary to back up the *WMS database*, *log files* and the *.smx* files. Note down the path to the location of these files, as you will be prompted for this path during the install, when you perform a restore.

   To change the location of backup of these files on your computer, click **Choose...**. At any point, to restore the default location, click **Restore Default**.



3. Click **Next**.

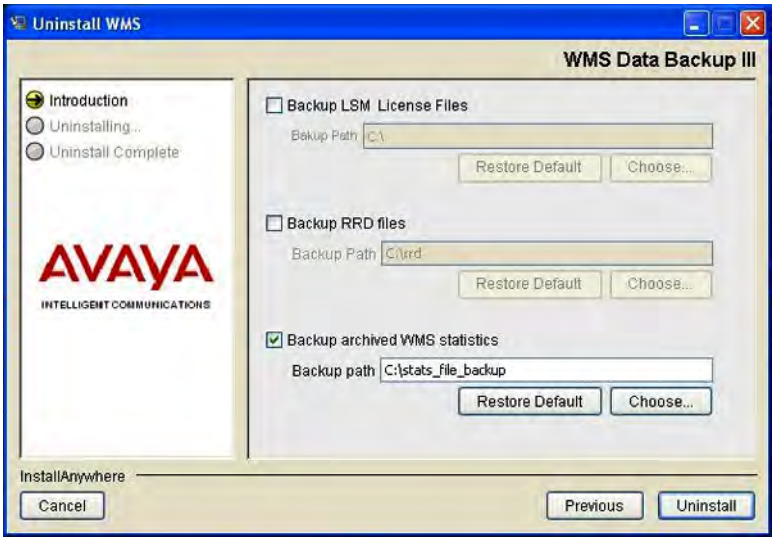
   The system displays the **WMS Data Backup 2** window displaying the fields necessary to back up the *Archived Alarms*, *Reports* and the *TFTP image* files. Note down the path to the location of these files, as you will be prompted for this path during the install, when you perform a restore.



   To change the location of backup of these files on your computer, click **Choose...**. At any point, to restore the default location, click **Restore Default**.

4. Click **Next**.

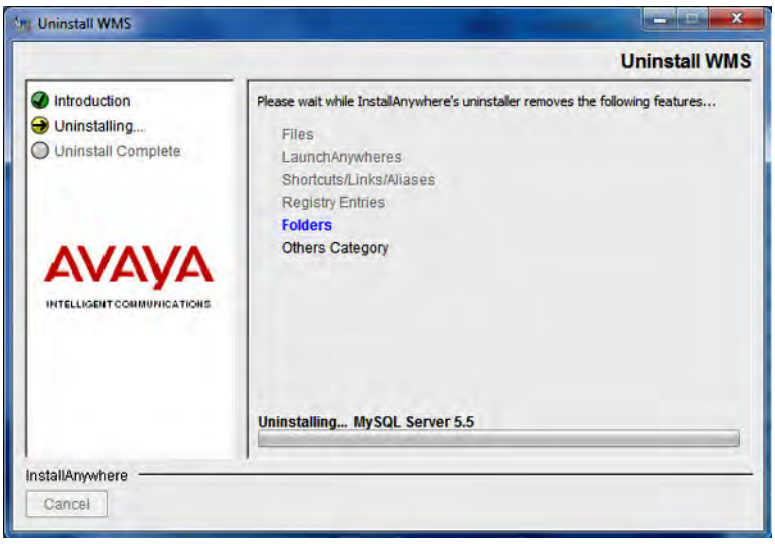
   The system displays the **WMS Data Backup 3** window displaying the fields necessary to back up the *LSM License Files*, *RRD files*, and *Archived WMS statistics*. Note down the path to the location of these files, as you will be prompted for this path during the install, when you perform a restore.



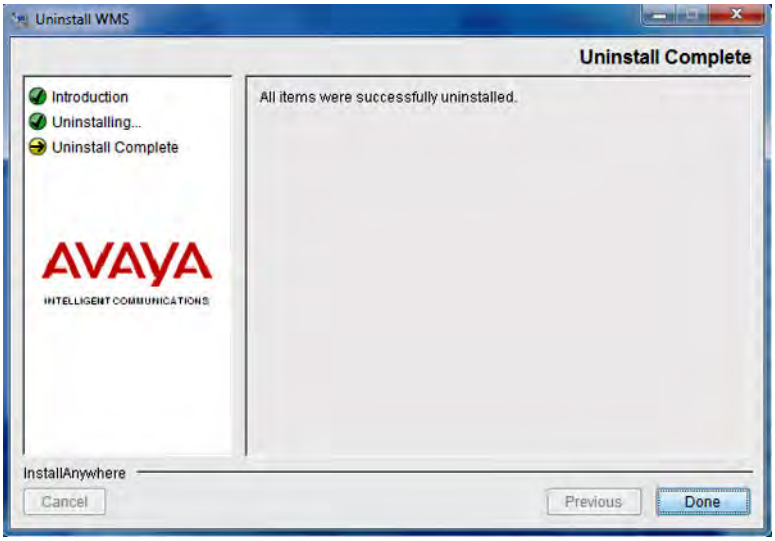
To change the location of backup of these files on your computer, click **Choose...**. At any point, to restore the default location, click **Restore Default**.

5. Click **Uninstall**.

   The **Uninstall WMS** window displays, initiating the uninstall process. This takes a few minutes.



Wait for the system to display the **Uninstall Complete** screen.



6. Click **Done** .

Related Links

Installing the WLAN Management System software on page 110