Using the Avaya Wireless Orchestration System

Release 8.0
NN47252-103
Issue 03.03
April 2017

Notices

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. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance 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, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel SoAPAPftware” 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”, or such successor site as designated by Avaya. 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 or such successor site as designated by Avaya. 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.

Table of Contents

List of Figures

Introduction

This section introduces the Wireless LAN Orchestration System (WOS), including an overview of key features and benefits. It also includes an outline of how this User's Guide is organized. Section headings for this chapter include:

The Avaya Family of WLAN Products

- **Wireless LAN Orchestration System (WOS)**

  WOS is a powerful management tool, designed to manage your wireless APs from anywhere in the network—ideal for large scale wireless deployments.

  WOS provides full monitoring and management of the Avaya wireless network via a web-based application with graphical map views. WOS scales from small to large networks and from one location to multiple locations, as well as large campus environments with thousands of wireless users.

  WOS is available for hosting on your own server:

  - **Avaya Virtual Appliance—Virtualized WOS Server Software**

    This package allows you to install and run WOS server software on your own virtual server.

- **Avaya Wireless APs**

  Multiple versions of Avaya Wireless APs with different numbers of radios support a variety of deployment applications. For more information on most APs, refer to *Using the Avaya OS for Avaya WLAN AP 9100 Series (NN47252-102).* Some smaller models, such as the WAP9112, run the

AOSLite operating system, and are managed only with the Wireless LAN Orchestration System.

WOS Product Overview

The Wireless LAN Orchestration System is a wireless network management application for managing a network of Avaya APs. WOS provides centralized monitoring, configuration, reporting, and management functions for APs—either individually, by group, or for all APs.

Extended Management Capability

WOS provides a dashboard overview of wireless network health, as well as maps and other views to monitor and manage the network. You may drill down to see detailed information about individual APs, radios, stations, and rogue devices. With its powerful discovery feature and map-based organization of your WAPs, WOS streamlines the management of AP configurations.

WOS allows IT administrators to manage configurations, schedule firmware upgrades across multiple wireless APs, and create groups of wireless APs to simplify repetitive tasks. WOS also offers different administrative levels that allow Help Desk staff to monitor their network and its client activity, and restrict network setting changes to specific staff members. All of these features allow the IT department to actively monitor and manage the health of their wireless network from anywhere using a browser.

A Scalable Solution

The Avaya centralized management technology scales from small to large networks and from one location to multiple locations, as well as large campus environments with thousands of wireless users. Together with its family of WAPs, Avaya developed WOS to facilitate faster and more cost-effective high capacity Wi-Fi rollouts across large campus environments.

WOS monitors wireless performance and gathers detailed reporting and statistical data for each AP residing in the network, or for the entire network as a whole. It also allows you to schedule firmware updates for individual WAPs or groups of APs to ensure that your firmware is up-to-date and consistent across the network.

Key Features and Benefits

- Web-based interface for complete monitoring and management of an Avaya wireless network.
- Profile networks provide automatic configuration for newly installed APs.
- Complete monitoring of wireless network status, traffic and clients.
- Complete configuration management of the wireless network.
- Graphical maps depicting wireless coverage, wireless performance, and user/rogue location.
- Comprehensive management reports on wireless performance, security, users, applications, RF, and more.
- Security monitoring, alerting and mitigation for rogues and security events.
- Troubleshooting tools to diagnose connectivity and performance issues.

This section describes some of the key product features and the benefits you can expect when deploying the WOS to configure and manage your network of APs.

Centralized Configuration and Management

Allows you to view and manage your entire wireless network at Layer 3 using your existing Ethernet infrastructure. In addition, WOS discovers, authenticates and configures new wireless APs, making large scale deployments quick and easy. Configuration templates ensure consistent configuration of APs across the network, and they are easily created by copying the configuration of a “known-good” AP.

Scalability

With its ability to support thousands of APs and many more concurrent wireless clients per WOS server, WOS allows your network to grow as your business grows.

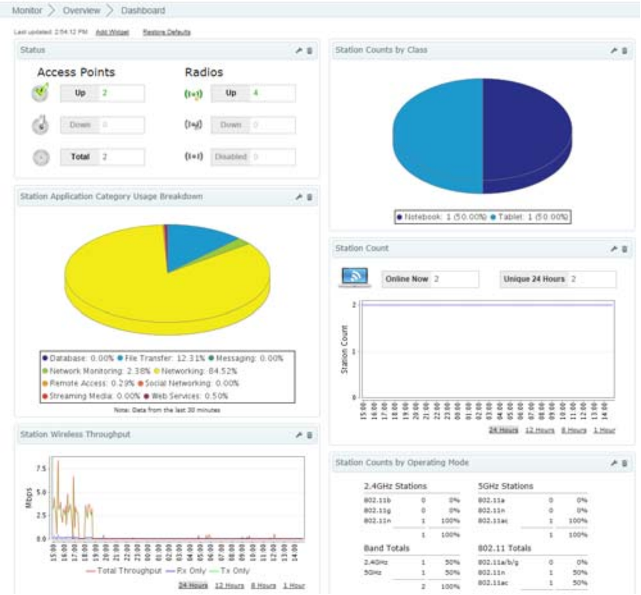
Security Management

Defines and distributes security policies for the entire AP network, and allows you to set encryption, authentication, access times, and guest user access policies for secure AP rollouts.

Powerful Graphical Interface

WOS's client interfaces provide all the tools and features that are necessary to ensure your AP network is configured and managed effectively and securely. The interfaces are easy to use and can be accessed from any location using a Web browser.

The WOS Dashboard (**Figure 1**) provides an at-a-glance overview of the security and performance of your AP network.



Last updated: 2:54:12 PM

Access Points

Up	2
Down	0
Total	2

Radios

Up	4
Down	0
Disabled	0

● Notebook: 1 (50.00%) ● Tablet: 1 (50.00%)

● Database: 0.00% ● File Transfer: 12.31% ● Messaging: 0.00%
● Network Monitoring: 2.38% ● Networking: 84.52%
● Remote Access: 0.29% ● Social Networking: 0.00%
● Streaming Media: 0.00% ● Web Services: 0.50%

Note: Data from the last 30 minutes

Online Now	2
Unique 24 Hours	2

2.4GHz Stations		
802.11b	0	0%
802.11g	0	0%
802.11n	1	100%
	1	100%

5GHz Stations		
802.11a	0	0%
802.11n	0	0%
802.11ac	1	100%
	1	100%

Band Totals		
2.4GHz	1	50%
5GHz	1	50%
	2	100%

802.11 Totals		
802.11a/b/g	0	0%
802.11n	1	50%
802.11ac	1	50%

Figure 1. WOS Dashboard

Performance Monitoring

Continuously monitors and displays wireless performance.

Centralized Upgrade Management

Allows you to schedule firmware updates for individual wireless APs or groups of APs at specific times.

Network Monitoring and Reporting

WOS displays all AP alerts and alarms to allow you to determine how to respond to faults in the AP network. It also monitors your AP network's performance and provides detailed reporting and statistical data for APs individually, by group of APs, by SSID, or by individual radios.

About this User's Guide

Detailed information and procedures have been provided in this User's Guide that will enable network administrators to install and run WOS on their own virtual environment, to understand and navigate the WOS client interface, and to successfully manage their network of wireless APs with a browser-based interface. WOS is installed on your own VMware-based platform. This Guide does not cover the installation or management of APs in isolation from WOS. For procedures that deal with APs not centrally managed by WOS, refer to *Using the Avaya OS for Avaya WLAN AP 9100 Series* (NN47252-102).

Organization

This User's Guide is organized by function under the following headings:

- **Introduction**
  Provides an overview of the product, including its key features and benefits.

- **Wireless LAN Orchestration System Products**
  This chapter provides an overview of what to expect when you install your Avaya management product for the first time, and provides instructions to help plan and complete a successful installation.

- **Getting Started with WOS**
  Describes starting, stopping, and managing the WOS server and client software. Provides procedures for initial setup of WOS, such as setting a network address and discovering the wireless network.

- **The WOS Web Client**
  Describes how to use the web client interface, including a summary of the wireless network monitoring, configuration, reporting, and WOS server management tools.
- **Monitoring the Network**
  Describes how to use the wireless network monitoring features.
- **Configuring the Network**
  Describes how to use the wireless network configuration tools.
- **Managing by Profiles**
  Describes how to organize sets of APs as profile networks to ensure the deployment of consistent software and settings across each profile.
- **Working with Maps**
  Introduces you to the location/RF heat map in the web client, and provides instructions for managing your maps and map layouts. It also shows you how to prepare map background images.
- **Managing Reports**
  WOS generates detailed performance and status reports about the wireless network, all APs within the network, individual radios contained within each AP, and their client stations. This chapter provides instructions for reviewing and managing these reports in the web client.
- **Configuring a Wireless AP**
  WOS provides a configuration window that has options that allow you to easily configure settings on an AP.
- **WOS Administration**
  Provides instructions for managing the WOS database and other administrative tasks, including how to review the current status of the database, how to schedule and create backups, and how to restore the database from the server.
- **Technical Support**
  Offers guidance to resolve technical issues, some general hints and tips to enhance your product experience, and Avaya contact information.

- **Glossary of Terms**
  Provides an explanation of terms directly related to WOS product technology, organized alphabetically.

Notes and Cautions

The following symbol is used throughout this User's Guide:

! *This symbol is used for cautions. Cautions provide critical information that may adversely affect the performance of the product.*

General notes provide useful supplemental information.

Hyperlinks

If you click on body text that appears in the color TEAL (with the exception of headings or notes) the embedded hyperlink within the text will immediately take you to the referenced destination. All cross-references, including the Table of Contents, page numbers within the List of Figures and the Index, and embedded text have associated hyperlinks. If you want to return to the reference source, you can do this by clicking on Acrobat's **previous page** button.

Wireless LAN Orchestration System Products

The Enterprise version of the Wireless LAN Orchestration System is offered as:

- **WOS**—a virtualized WOS server software application package that allows you to install and run the WOS server software on your own virtual server under VMware or Hyper-V.

WOS

The WOS server is designed to be run on a virtual platform. The application package allows you to install and run the WOS server on your own virtual machine under VMware or Hyper-V (WOS-VM or -HV). For installation instructions, see **"Installing the WOS-VM Virtual Appliance" on page 11** or **"Installing the WOS-HV Virtual Appliance" on page 20**.

Take care not to over-subscribe RAM when using either version of the Virtual WOS server - e.g., if there are three virtual instances on the system that are provisioned for 8GB each, then the total system must have no less than 3 x 8GB = 24 GB provisioned for it.

WOS-VM System Requirements

The recommended requirements for the system hosting the VMware-based WOS server are based on the scale of the Wi-Fi AP network to be managed—small, medium, or large. The WOS-VM package must be installed on a server running VMware™. The versions that are supported are:

- VMware ESXi (recommended)
- VMware vSphere
- VMware Workstation

Please see the product fact sheet for specifications and system requirements for the scale of the network to be managed.

WOS-HV System Requirements

The recommended requirements for the system hosting the Hyper-V version of the WOS server are based on the scale of the Wi-Fi AP network to be managed—small, medium, or large. The WOS-HV package must be installed on a server running Microsoft Hyper-V™. The versions that are supported are:

- Windows Server 2012 R2
- Hyper-V Server 2012 R2
- Cores—at least 2
- Memory—4 GB minimum

You can check memory use and free space available at any time when WOS is running. See **"Viewing WOS Server Status" on page 556***. That page also provides an option for reducing database size by deleting accumulated statistical data.*

Please see the product fact sheet for specifications and system requirements for the scale of the network to be managed.

If you will need more than 200 GB of disk space, you must create a disk of this size ***before the first time you start the WOS server****. Follow the instructions in* **"Installing the WOS-VM Virtual Appliance" on page 11***.*

Installing the WOS-VM Virtual Appliance

For VMware, the WOS Virtual Appliance is supplied as an .ova file (Open Virtual Appliance), for example, **WOS-vm-7.0.0-4280.ova**. It contains all the software that you need to run a WOS server on a VMware machine.

You must ensure that the BIOS on the computer running VMware has Virtualization Technology (VT) enabled. VMware requires this setting for WOS, which runs as a 64-bit guest operating system. Different BIOS versions may have a different name for this setting. Please see VMware support for more information. The knowledge base topic, "Ensuring Virtualization Technology is enabled on your VMware host" is especially useful. ***kb.vmware.com***

1. One of the following versions of VMware must already be installed on the server platform: VMware ESXi (recommended), VMware Workstation, or VMware vSphere. Please refer to documentation supplied for your VMware product for exact instructions for using the .ova file. Documentation is available online at **http://www.vmware.com/support/pubs/**.

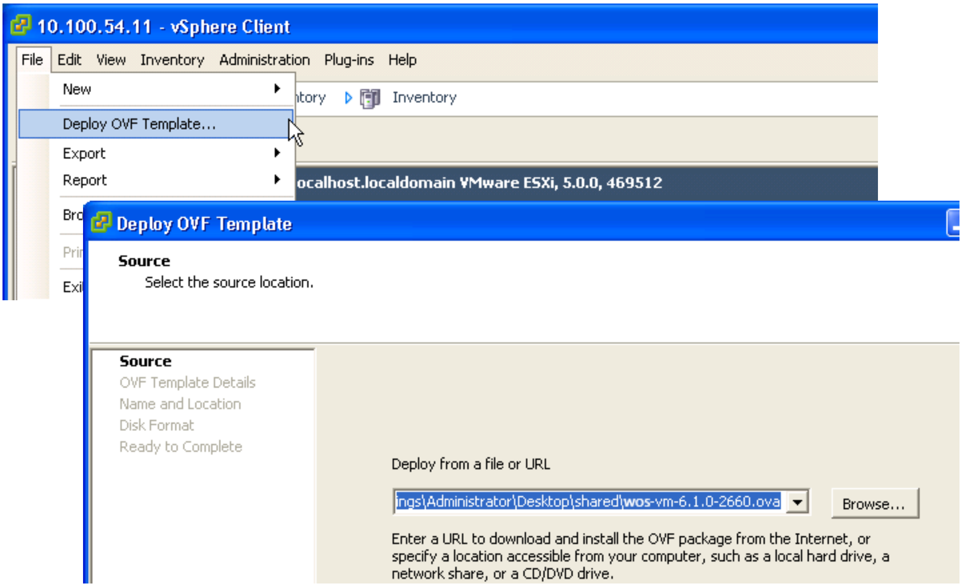
2. Determine the amount of storage (disk) space required for your deployment as recommended in the product datasheet. If more than 200 GB is recommended, you must carefully follow the steps later in this procedure to create a larger virtual disk **before** starting the WOS server for the first time.

3. Open the client for managing your VMware product. For example, open VMware vSphere.

4. Open the .ova file in your VMware product.

   a. For **VMware Workstation**: select **Open a Virtual Machine**. Browse to the .ova file. In the browse dialog, be sure to set **Files of type** so that the .ova file will be listed.

b. For **VMware ESXi Versions 4** and **5**: select **File > Deploy OVF Template**. Browse to the .ova file. In the browse dialog, be sure to set **Files of type** so that the .ova file will be listed.



Source

Select the source location.

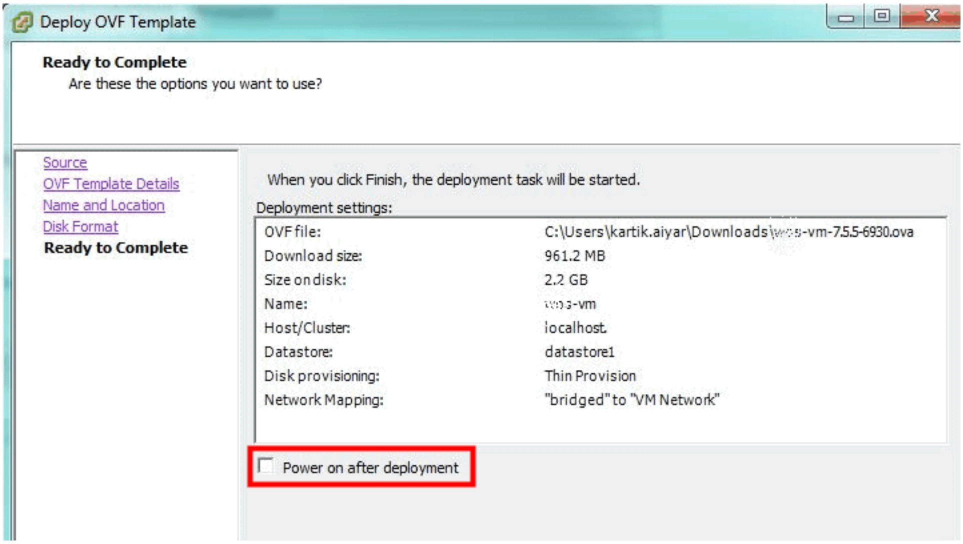
Deploy from a file or URL

ings\Administrator\Desktop\shared\wos-vm-6.1.0-2660.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

Figure 2. Opening the WOS Virtual Appliance in VMware ESXi

5. Follow the prompts to import the WOS Virtual Appliance. **IMPORTANT**: Select the WOS Virtual Appliance from the list at the left and ***make sure to disable*** the option for **Power on this virtual machine** or **Power on after deployment**, before clicking **Finish**.



Deploy OVF Template

Ready to Complete

Are these the options you want to use?

Source

OVF Template Details

Name and Location

Disk Format

Ready to Complete

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\Users\kartik.aiyar\Downloads\wos-vm-7.5.5-6930.ova
Download size:	961.2 MB
Size on disk:	2.2 GB
Name:	wos-vm
Host/Cluster:	localhost.
Datastore:	datastore1
Disk provisioning:	Thin Provision
Network Mapping:	"bridged" to "VM Network"

□ Power on after deployment

Figure 3. Don’t start the WOS Server automatically (ESXi shown)

6. Once deployment is complete, right click the WOS Virtual Appliance from the list at the left and select **Settings**. For larger wireless networks, increase the amount of **Memory** and **Processors** dedicated to the WOS Appliance as recommended in the datasheet.

7. The default disk size is 200 GB. If this is sufficient for your deployment per the WOS data sheet, skip to **Step 10**.

   Delete **Disk 2**, then display the **Add Hardware** dialog. Click **Hard Disk** then **Next**.

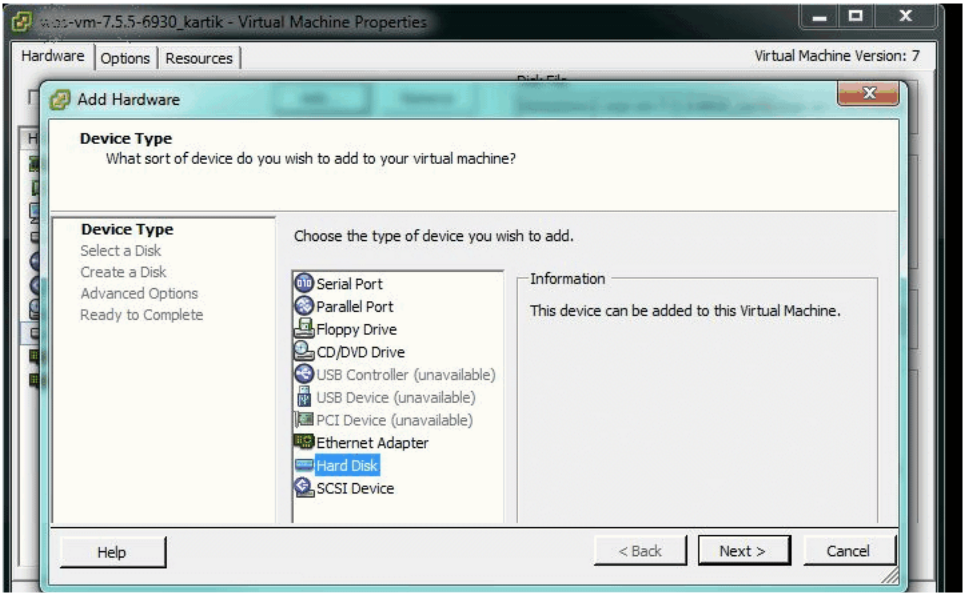
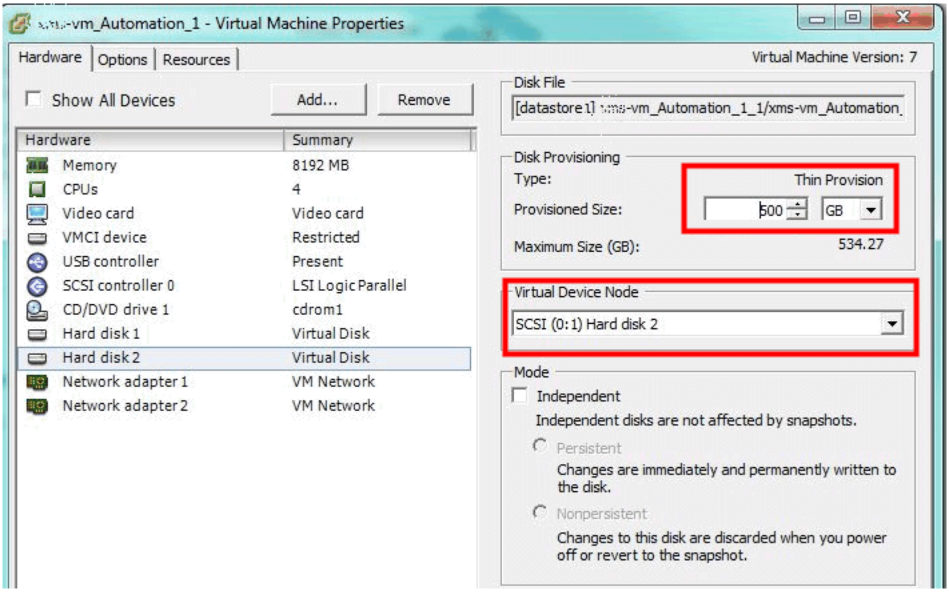


Figure 4. Creating a new, larger hard disk (ESXi shown)

8. Select **Create a new virtual disk**, then click **Next**. For **Disk Provisioning**, set the **Type to Thin Provision.** Set the **Provisioned Size** to the size recommended in the data sheet. **Virtual Device Node** should be set to **SCSI (0:1) Hard disk 2**. Click **OK** when done.



xms-vm_Automation_1 - Virtual Machine Properties

Hardware | Options | Resources — Virtual Machine Version: 7

□ Show All Devices — Add... — Remove

Hardware	Summary
Memory	8192 MB
CPUs	4
Video card	Video card
VMCI device	Restricted
USB controller	Present
SCSI controller 0	LSI Logic Parallel
CD/DVD drive 1	cdrom1
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	VM Network
Network adapter 2	VM Network

Disk File: [datastore1] xms-vm_Automation_1/xms-vm_Automation_

Disk Provisioning
Type: Thin Provision
Provisioned Size: 500 GB
Maximum Size (GB): 534.27

Virtual Device Node: SCSI (0:1) Hard disk 2

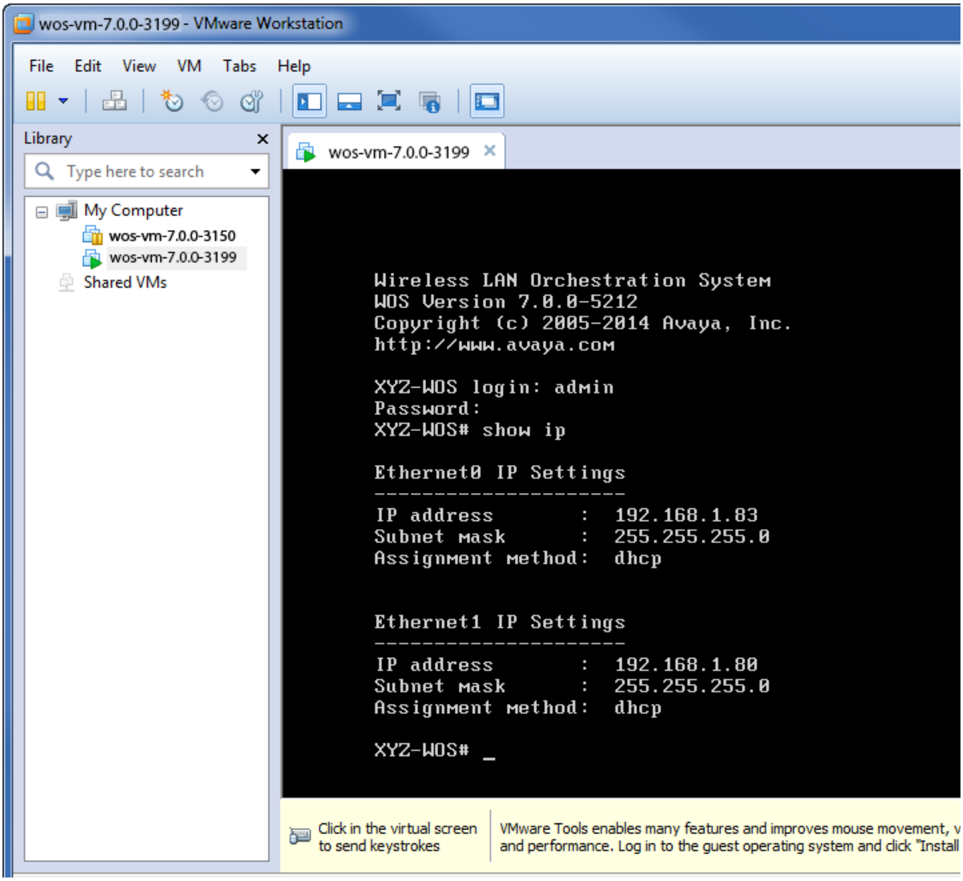
Mode
□ Independent
Independent disks are not affected by snapshots.
○ Persistent
Changes are immediately and permanently written to the disk.
○ Nonpersistent
Changes to this disk are discarded when you power off or revert to the snapshot.

Figure 5. Creating a new, larger hard disk (continued, ESXi shown)

9. Start the WOS server. Note that with a larger disk, the server will take longer to start the first time that you bring it up.

10. In VMware, type Ctrl+g to direct commands to the WOS server in the Virtual Appliance. Log in with the login/password **admin/admin**. (**Figure 6**)

    Type **show ip**, and note the IP address of the port that you are using for management.


wos-vm-7.0.0-3199 - VMware Workstation
File
Edit
View
VM
Tabs
Help
Library
Type here to search
My Computer
wos-vm-7.0.0-3150
wos-vm-7.0.0-3199
Shared VMs
wos-vm-7.0.0-3199
Click in the virtual screen to send keystrokes
VMware Tools enables many features and improves mouse movement, v
and performance. Log in to the guest operating system and click "Install

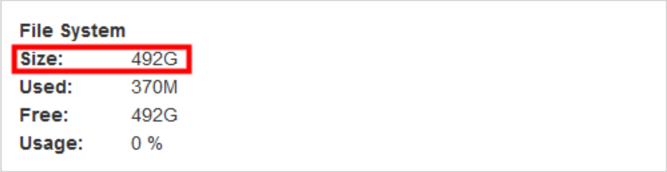
```
Wireless LAN Orchestration System
WOS Version 7.0.0-5212
Copyright (c) 2005-2014 Avaya, Inc.
http://www.avaya.com

XYZ-WOS login: admin
Password:
XYZ-WOS# show ip

Ethernet0 IP Settings
---------------------
IP address         :  192.168.1.83
Subnet mask        :  255.255.255.0
Assignment method:  dhcp


Ethernet1 IP Settings
---------------------
IP address         :  192.168.1.80
Subnet mask        :  255.255.255.0
Assignment method:  dhcp

XYZ-WOS# _
```

Figure 6. Starting the WOS Server on the Virtual Appliance

11. To access the web client, set your browser's URL to this IP address, followed by **:9090**. For example, **http://192.168.1.110:9090**. When the splash page appears, log in. The default username and password are **admin/admin**.

    For VMware Workstation, if you have problems with network connectivity, see **"Correct Network Port Problems" on page 17**.

12. To verify the disk size using the WOS server, open the **Settings** menu, and then click **Status**.



File System

Size:	492G
Used:	370M
Free:	492G
Usage:	0 %

Figure 7. Verifying disk size in the WOS server

13. Continue to **"Initial Server Setup for Virtual Appliances" on page 31** to configure and begin using the WOS server.

__Licensing__ - The WOS server requires a license for full operation. The license is entered via the client, and will automatically be requested the first time you start the client.

Correct Network Port Problems

The WOS Virtual Appliance obtains network connectivity by binding interfaces on the virtual machine with physical ports on the host computer. In some installations, VMware Workstation may associate the WOS Virtual Appliance with a physical port that is not connected to the network, and the Appliance will have no connectivity.

VMware Workstation has a separate utility, **vmnetcfg.exe**, that you may use to set the interface bindings explicitly to correct this problem. The following commands are for a Windows-based host computer. For other operating systems, modify them accordingly.

1. Current versions of VMware Workstation require you to extract **vmnetcfg.exe** from the installation file manually, using the following steps. Older versions may have made the utility accessible automatically. Search your computer's VMware installation directory (we'll call it <*VMware*> in these instructions) and subdirectories for the file **vmnetcfg.exe**. If found, skip to **Step 5**.

   If not found, continue to the next step.

2. Open an elevated command prompt (Run as Administrator). Browse to the directory that contains the VMware installation file.

3. Run the installation file with the following options to extract the contents of the installation file to the **c:\vmware** folder (create the **c:\vmware** folder first if necessary):

   <install-file.exe> **/e c:\vmware**

   For example:

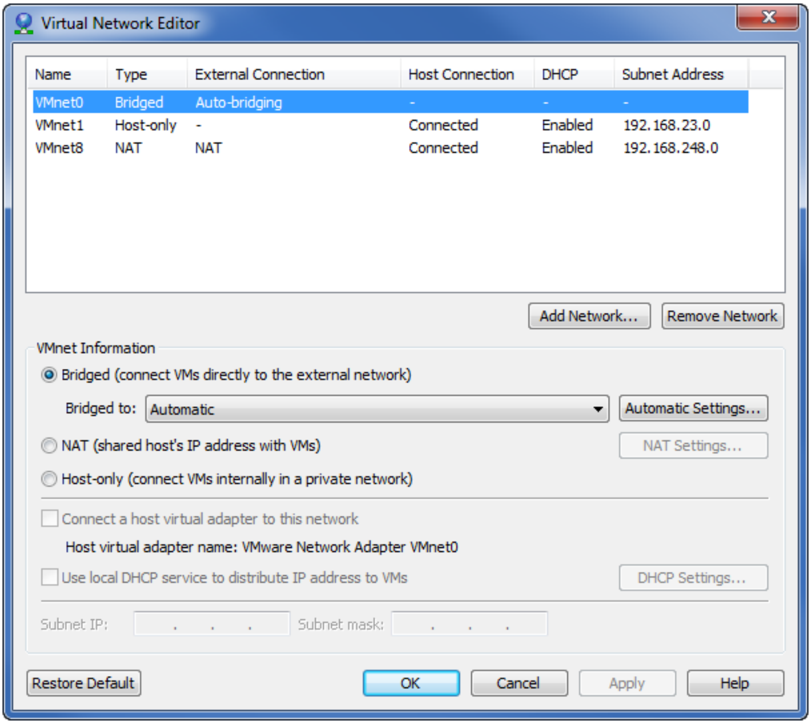
   VMware-workstation-full-8.0.1-528992.exe /e c:\vmware

   Use the actual name of the installation file supplied to you by VMware, which may be different than the names shown above.

4. Browse to **c:\vmware** and open the file **network.cab**. This is a compressed file that should open in most file compression software. Extract the contents of the cab file to the *<VMware>* directory. For example:

   C:\Program Files\VMware\VMware Workstation

5. Browse your *<VMware>* directory. Find and run **vmnetcfg.exe**.



Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.23.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.248.0

VMnet Information

● Bridged (connect VMs directly to the external network)

Bridged to: Automatic

○ NAT (shared host's IP address with VMs)

○ Host-only (connect VMs internally in a private network)

□ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet0

□ Use local DHCP service to distribute IP address to VMs

Subnet IP: . . . Subnet mask: . . .

Figure 8. Using vmnetcfg.exe

6. Highlight the **VMnet0** interface (at the top of the page).
7. Under **VMnet Information**, select **Bridged (connect VMs directly to the external network)**.
8. On the **Bridged to:** line, select the physical interface that provides network connectivity on your host computer.
9. Click **OK**.

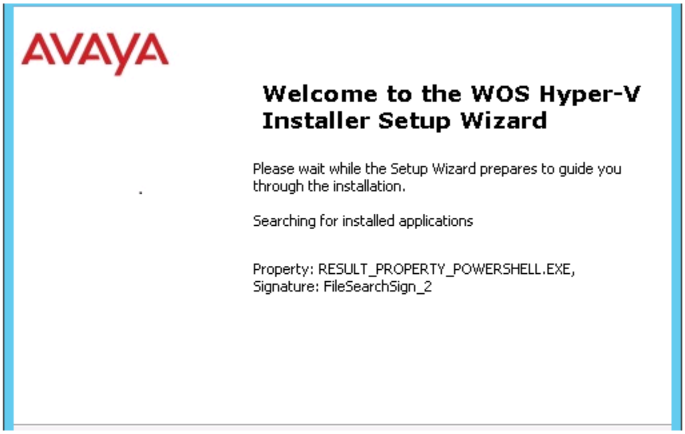
Installing the WOS-HV Virtual Appliance

The WOS Virtual Appliance for Hyper-V is supplied as an .exe file, for example, **WOS Hyper-V Installer-8.0.1-7301.exe**. It contains all the software that you need to install a WOS server on a Hyper-V based virtual machine.

You must ensure that the BIOS on the computer running Hyper-V has Virtualization Technology (VT) enabled. Hyper-V requires this setting for WOS, which runs as a 64-bit guest operating system. Different BIOS versions may have a different name for this setting. Please refer to the relevant Microsoft documentation for general Hyper-V requirements, etc.

1. You must use one of the following platforms: Windows Server 2012 R2 or Hyper-V Server 2012 R2. Please refer to documentation for your Hyper-V product for more information.
2. Run the installer executable file, for example: **WOS Hyper-V Installer-8.0.1-7301.exe**. The WOS Hyper-V Installer Setup Wizard will walk you through the installation steps.
3. WOS-HV requires Internet access via an Ethernet port on the host machine. If you have not used the Hyper-V Virtual Switch Manager to associate a virtual port with a physical port, you will be informed that you are missing prerequisites. Click **Next**, and the Prerequisites Wizard assists you in satisfying these requirements.

If the Hyper-V virtual machine has more than one active Ethernet port on the same subnet as the WOS server, be sure to specify the IP address that APs should use for contacting the server. See **“WOS Call-back Address” on page 591**.



Welcome to the WOS Hyper-V Installer Setup Wizard

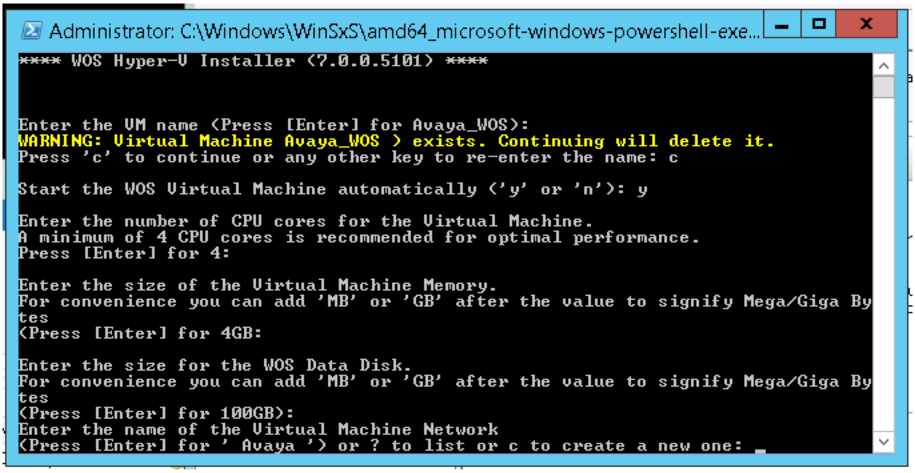
Please wait while the Setup Wizard prepares to guide you through the installation.

Searching for installed applications

Property: RESULT_PROPERTY_POWERSHELL.EXE, Signature: FileSearchSign_2

Figure 9. WOS Hyper-V Installer Setup Wizard

4. Click **Next>.** A Windows PowerShell window appears. In it, the WOS Hyper-V Installer continues to walk you through entering the remainder of the WOS server settings. (**Figure 10**)

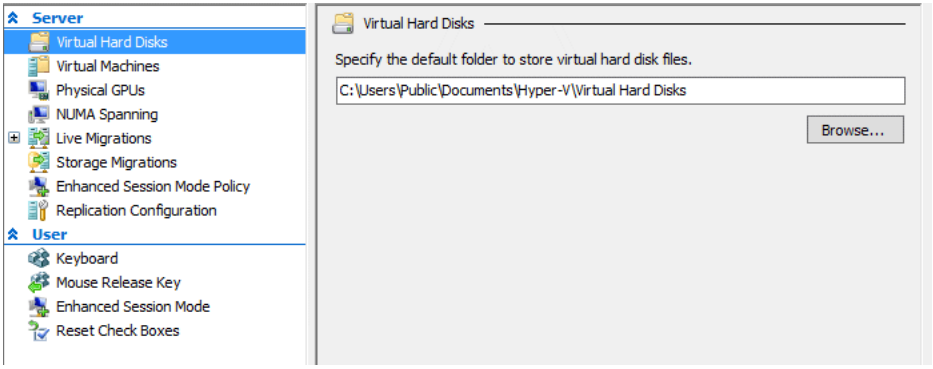


Administrator: C:\Windows\WinSxS\amd64_microsoft-windows-powershell-exe...

```
**** WOS Hyper-V Installer (7.0.0.5101) ****


Enter the VM name (Press [Enter] for Avaya_WOS):
WARNING: Virtual Machine Avaya_WOS ) exists. Continuing will delete it.
Press 'c' to continue or any other key to re-enter the name: c

Start the WOS Virtual Machine automatically ('y' or 'n'): y

Enter the number of CPU cores for the Virtual Machine.
A minimum of 4 CPU cores is recommended for optimal performance.
Press [Enter] for 4:

Enter the size of the Virtual Machine Memory.
For convenience you can add 'MB' or 'GB' after the value to signify Mega/Giga By
tes
(Press [Enter] for 4GB:

Enter the size for the WOS Data Disk.
For convenience you can add 'MB' or 'GB' after the value to signify Mega/Giga By
tes
(Press [Enter] for 100GB):
Enter the name of the Virtual Machine Network
(Press [Enter] for ' Avaya ') or ? to list or c to create a new one: _
```

Figure 10. WOS Hyper-V Installer—PowerShell

- **Enter the VM Name** (name of the WOS server): Press the **Enter** key to use the default name for the server: **Avaya-WOS**. If you use a different name, be aware that you **must** ensure that the name **Avaya-WOS** resolves to your chosen server name. Please see **“How Discovery Works” on page 160**.
- **Start the WOS Virtual Machine automatically ('y' or 'n')**: Enter **y** to have the server start automatically when the host starts.
- **Enter the number of CPU cores for the Virtual Machine**: Use of at least four CPU cores is recommended for optimal performance.
- **Enter the size of the Virtual Machine Memory**: Use MB, GB, or TB to signify megabytes, gigabytes or terabytes, respectively. Note that if you don’t use one of these suffixes to specify the units, then you get the exact number that you entered, i.e., if you enter 1 you will get 1 byte!
- **Enter the size for the WOS Data Disk**: Use MB, GB, or TB to signify megabytes, gigabytes or terabytes, as above. If you press the **Enter** key without specifying a size, the installer will assign a large portion of the available capacity of the host machine’s hardware (after allowing room for the WOS server’s system disk).



Specify the default folder to store virtual hard disk files.

C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks

Figure 11. Hyper-V—Virtual Hard Disks

5. After you have entered the settings above, the installation of the WOS server under Hyper-V proceeds. Messages will inform you of the

progress of the installation, and of the location of the WOS server Virtual Hard Disk (vhd file).

6. The installer will ask whether you wish to start the WOS server virtual machine. Type **y** to start it now, or type **n** to start it later via the Hyper-V Manager.

   Messages will inform you of the progress. After the State displays as **Running**, when prompted press the **Enter** key to continue.

7. You may use the Hyper-V Manager for ongoing management of the server.

Getting Started with WOS

This chapter describes how to get started using WOS.

Section headings for this chapter include:

WOS Port Requirements

A number of ports are used by WOS and by various AP features. These ports must not be blocked by firewalls.

The **Port Requirements table on page 27** lists ports and the features that require them.

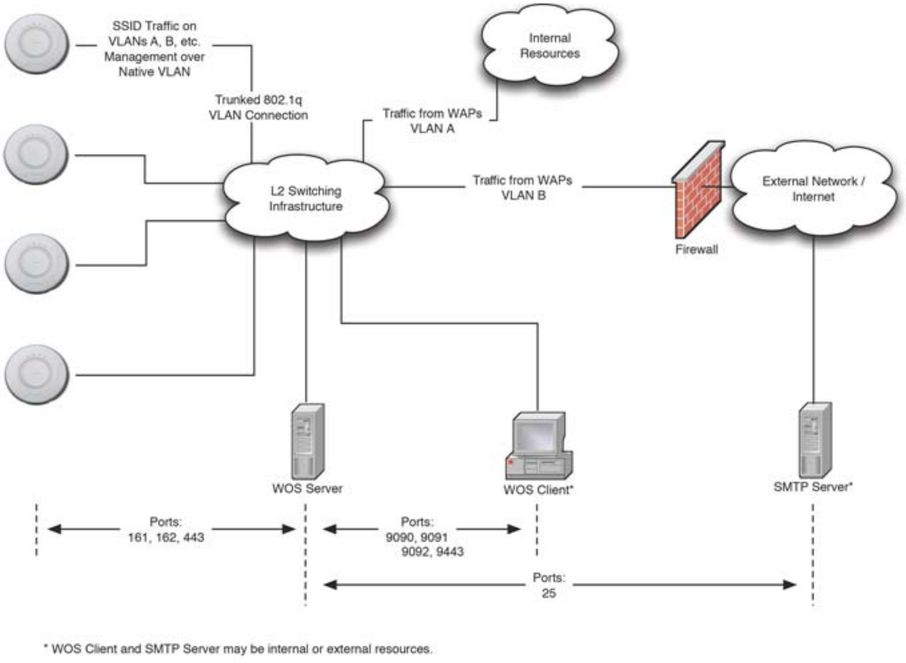

SSID Traffic on VLANs A, B, etc. Management over Native VLAN
Trunked 802.1q VLAN Connection
Internal Resources
Traffic from WAPs VLAN A
L2 Switching Infrastructure
Traffic from WAPs VLAN B
Firewall
External Network / Internet
WOS Server
WOS Client*
SMTP Server*
Ports: 161, 162, 443
Ports: 9090, 9091 9092, 9443
Ports: 25
* WOS Client and SMTP Server may be internal or external resources.

Figure 12. Sample Port Requirements for WOS

Note that AP port requirements are included in the table for your convenience—some of the AP ports shown are unrelated to communication with WOS. If you are using a feature, please make sure that the ports that it requires are not blocked by firewalls or other policies, and that they do not conflict with any other port assignments.

As an example, some WOS port requirements are illustrated in **Figure 12**. WOS requires ports 161, 162, and 443 to be passed between APs and the WOS server. Similarly, ports 9090, 9091, 9092, and 9443 are required for communication between the WOS server and WOS clients, and port 25 is typically used by the WOS server to access an SMTP server to send email notifications.

The following table lists port requirements for the AP and for WOS, how they are used, and whether they may be changed.

Port	Application	Peer	Configurable
WOS			
22 tcp	SSH	APs	Yes
25 tcp	SMTP	Mail Server	Yes
123 udp	NTP	NTP Server	No
161 udp	SNMP	APs	No
162 udp	SNMP Trap Receiver	APs	Yes
514 udp	Syslog server	APs	Via WOS config file
	Ping	APs	No
1099 tcp	RMI Registry	Internal*	No
2000 tcp	WOS Back-end Server	Internal*	No
2022 tcp	SSH	AP	Yes
3306 tcp	MySQL Database	Internal*	No
8001 tcp	Status Viewer	Internal*	No

Port	Application	Peer	Configurable
8007 tcp	Tomcat Shutdown	Internal*	During installation
8009 tcp	Web Container	Internal*	During installation
8085 tcp	Web Socket Communication	Access Points	No
9090 tcp	WOS Client Server	WOS client	Via WOS config file
9091 tcp	WOS Client Server	WOS client	Via WOS config file
9092 tcp	WOS Client Server	WOS client	Via WOS config file
9443 tcp	WOS WMI SSL	WOS web client	Yes
9444 tcp	Secure Web Socket	Access Points	No
* Internal to WOS Server, no ports need to be unblocked on other network devices			
AP			
icmp	Ping	WOS server	No
20 tcp 21 tcp	FTP	Client	Yes
22 tcp	SSH	Client	Yes
23 tcp	Telnet	Client	Yes
25 tcp	SMTP	Mail Server	Yes
69 udp	TFTP	TFTP Server	No
123 udp	NTP	NTP Server	No
161 udp	SNMP	WOS Server	No

Port	Application	Peer	Configurable
162 udp	SNMP Traphost Note: Up to four Traphosts may be configured.	WOS Server	Yes - but required by WOS
443 tcp	HTTPS (WMI,WPR)	Client	Yes
514 udp	Syslog	Syslog Server	Yes
1812, 1645 udp	RADIUS (some servers use 1645)	RADIUS Server	Yes
1813, 1646 udp	RADIUS Accounting (some servers still use 1646)	RADIUS Accounting Server	Yes
2055 udp	Netflow	Client	Yes
5000 tcp	Virtual Tunnel	VTUN Server	Yes
22610 udp	(Avaya Roaming)	APs	Yes
22612 udp	Avaya virtual console (Console Utility)	Admin Workstation	Yes

Starting and Managing the WOS Server

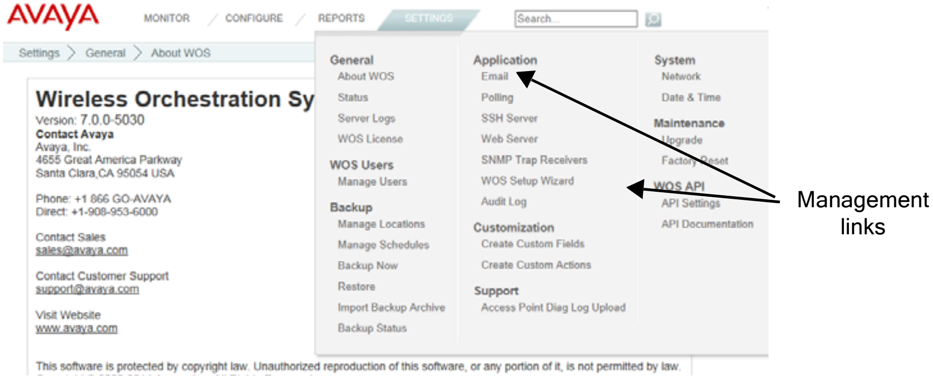
anage the WOS server using its management tools:

- **Managing WOS on a Virtual Appliance**
- **Initial Server Setup for Virtual Appliances**

NOTE: For full operation, the WOS server must have a license installed.

Managing WOS on a Virtual Appliance

On the Virtual Appliance, the WOS server is started automatically when your computer is restarted. (For other platforms, see **"Initial Server Setup for Virtual Appliances" on page 31**). Use the browser-based WOS web client (**Figure 13**) to perform mandatory initial configuration, to restart or reboot the server, and for server maintenance.



Wireless Orchestration Sy

Version: 7.0.0-5030

Contact Avaya
Avaya, Inc.
4655 Great America Parkway
Santa Clara,CA 95054 USA

Phone: +1 866 GO-AVAYA
Direct: +1-908-953-6000

Contact Sales
sales@avaya.com

Contact Customer Support
support@avaya.com

Visit Website
www.avaya.com

This software is protected by copyright law. Unauthorized reproduction of this software, or any portion of it, is not permitted by law.

Figure 13. Server Management using the Web Client

To access the web client, set your browser's URL to the WOS server machine's IP address or host/domain name, followed by **:9090**. For example, **http:// 192.168.10.40:9090**. You will be redirected to a secure connection (https://<server>:9443), and the login page will be displayed.

NOTE*: *WOS web client access to the WOS server requires access to ports 9090 and 9443. Make sure *that these ports are open in any firewalls between clients and the WOS server.*

Log in to the web client (the default for both fields is **admin**). In a few moments it will prompt you to run the **WOS Setup Wizard**. This will lead you through entering your WOS server license and setting up discovery for your network of wireless APs. Proceed to **"Initial Server Setup for Virtual Appliances" on page 31** to perform required initial setup on the server.

NOTE: *You may use the Command Line Interface (CLI) to manage the WOS server via SSH. Access it at port 2022 and log in using **admin/admin**. Do **not** use port 22 for CLI.*

If WOS is not running properly, you may click the **Restart Application** button on the lower left of the Status page to restart the WOS server software. If the server is currently running, an orderly shutdown will be performed first.

The **Reboot Appliance** button will reboot the Appliance—this will shut down WOS related processes in an orderly manner before rebooting. Rebooting and restarting will take about two minutes on a new Appliance. As WOS is used and the database grows, startup integrity checks will take longer. For shutdown, see **"Shutting Down the WOS Server" on page 31**.

Initial Server Setup for Virtual Appliances

Use the WOS web client to complete the following steps on virtual appliances in order to configure WOS for proper operation.

When you start the WOS server for the first time, you must configure basic settings by following the steps in:

- **WOS Setup Wizard**

When those steps are complete, proceed to:

- Set the WOS polling interval based on your deployment size (see **"Polling Settings" on page 589**.

About the WOS User Interface

The WOS Web Client is a very fast and efficient application for viewing the status of your AP network and performing network management tasks. The Dashboard provides an at-a-glance overview of the health of your AP network; network discovery may be fine-tuned; RF heat maps display the RF coverage provided by your APs; alarms and events are displayed; pages for APs, radios, Stations, and SSIDs show detailed information and allow configuration; rogue devices are monitored; and AP configuration policies may be configured. The web client has special features such as bulk editing, which allows you to quickly configure selected identical settings on a number of APs in one step. Reports on system performance may be created.

Shutting Down the WOS Server

There is a correct way and an incorrect way to shut down the WOS server. Shutting down the server incorrectly can cause problems the next time you start WOS. If you need to shut down the server, you must use the following procedure:

1. Terminate all clients.

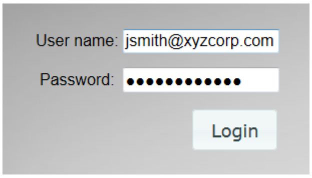
2. For the Virtual Appliance servers—in the **Status** page of the WOS web client, click the **Shutdown Appliance** button at the bottom of the window.
3. You will be notified when the server has shut down successfully. The database server will be shut down as well.
4. When the WOS server has shutdown successfully you may shut down your computer.

The WOS Web Client

The Web Client provides a fast, efficient interface for checking wireless network performance and for selected management tasks.

Starting the Web Client

Avaya supports the latest version of the following browsers: Internet Explorer, Mozilla Firefox, Chrome, or Safari. A secure web browser is required.


User name: jsmith@xyzcorp.com

Password: ●●●●●●●●●●●●

Figure 14. Login Window

To start the web client, point your workstation's browser to the IP address or hostname for the WOS server machine followed by **:9090**. For example, if the IP address is 192.168.10.40, point your browser to **http://192.168.10.40:9090**. You will automatically be redirected to an HTTPS connection (if you prefer, you may connect directly via HTTPS using port 9443, with a URL in the form **https://<ip address or hostname>:9443)**. When the WOS splash window appears, log in with your **User name** and **Password**. The default login is **admin**/**admin**.

Web Client Menus

The web client has four major menus, selected by links at the top of the window. Each menu offers a selection of pages which manage different WOS functions. The menus are described in the following sections:

- **"About Monitor Pages" on page 34**
- **"About the Configure Pages" on page 36**
- **"About Reports Pages" on page 38**
- **"About Settings Pages" on page 39**

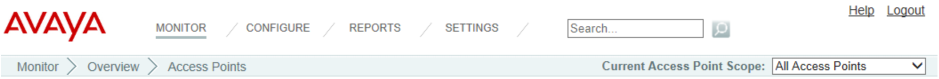


Figure 15. Mode Selection in WOS Web Client

About Monitor Pages

These pages display information about the current status of the network. Click the **Monitor** link at the top of the window to see the list of pages.

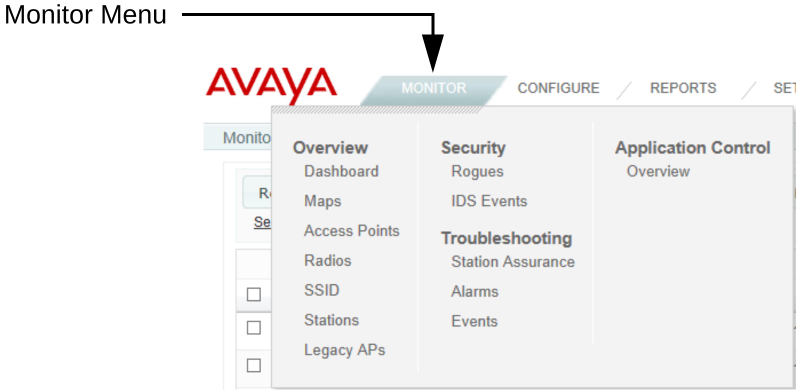


Figure 16. WOS Web Client Monitor Functions

The monitor options for WOS are shown in **Figure 16**. These are primarily read-only pages, although most of the pages have links to click to drill down for details, and allow you to export data to a file. The Monitor link always opens to the Dashboard page.

Monitor pages include the following. Click one of the links below for more information.

Overview

- **Dashboard**
- **Maps**
- **Access Points**
- **Radios**

- **SSID**
- **Stations**
- **Legacy APs**

Security

- **Rogues**
- **IDS Events**

Troubleshooting

- **Station Assurance**
- **Alarms**
- **Events**

Application Control

- **Application Control—Overview**

About the Configure Pages

Note that smaller APs that use the AOSLite system software, such as the WAP9112, have many fewer settings than more powerful APs. Some of the configuration pages will not list AOSLite devices, or are not available for those devices.

Configure Menu (requires read-write privileges)

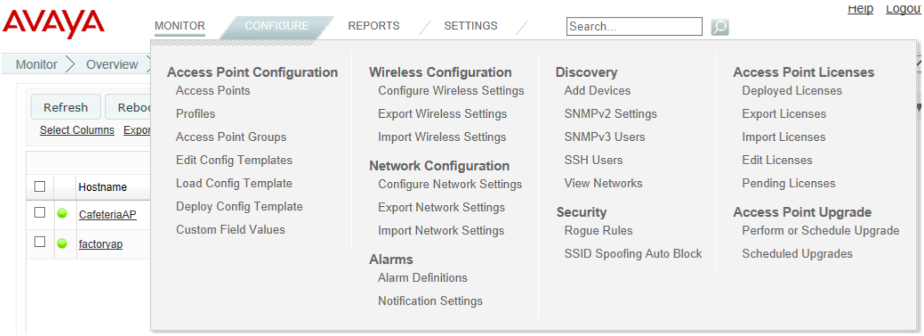


Figure 17. WOS Web Client Configure Functions

These pages perform specific wireless network configuration actions. Some of these pages are particularly powerful, allowing you to make bulk configuration changes over multiple radios and APs in one step. Click the **Configure** link at the top of the window to see the list of configure pages. The **Configure** link always opens to the APs page, which is the same as the Monitor > **Access Points** page. You must be logged in to WOS as an administrator with read-write privileges to see the **Configure** link.

Configure pages include the following. Click a link below for more information.

AP Configuration

- **Access Points (Configure)**
- **Profiles**

- AP Groups
- Edit Config Templates
- Load Config Template
- Deploy Config Template
- Custom Field Values
- Import Access Point Custom Fields

Wireless Configuration

- Configure Wireless Settings
- Export Wireless Settings
- Import Wireless Settings

Network Configuration

- Configure Network Settings
- Export Network Settings
- Import Network Settings

Alarms

- Alarm Definitions
- Notification Settings

Discovery

- Add Devices
- SNMPv2 Settings
- SNMPv3 Users
- SSH Users
- View Networks

Security

- Security—Rogue Rules
- SSID Spoofing Auto Block

Access Point Licenses

- Deployed Licenses
- Export Licenses
- Import Licenses
- Edit Licenses
- Pending Licenses

Access Point Upgrade

- Perform or Schedule Upgrade
- Scheduled Upgrades

About Reports Pages

These pages are used to generate reports on the operation of your wireless network. WOS offers an extensive suite of reports on performance and status, including such aspects as throughput, error rates, station information, availability, RF usage, and security.

All of these reports are discussed in detail in "Managing Reports" on page 259.

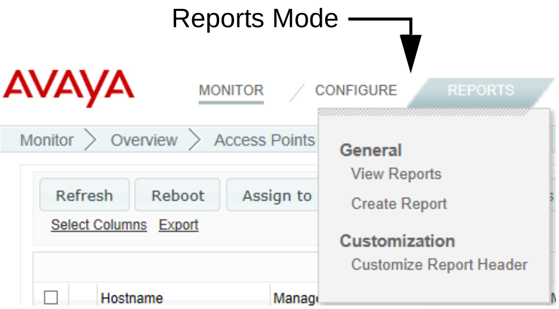


Figure 18. WOS Web Client Reports Functions

Click the **Reports** tab at the top of the window to see the list of reports pages.

General

- **“View Reports” on page 261**

  The web client’s **Reports** link opens to this page, listing the reports you have already created and allowing you to view or run these reports.

- **“Create Report” on page 267**

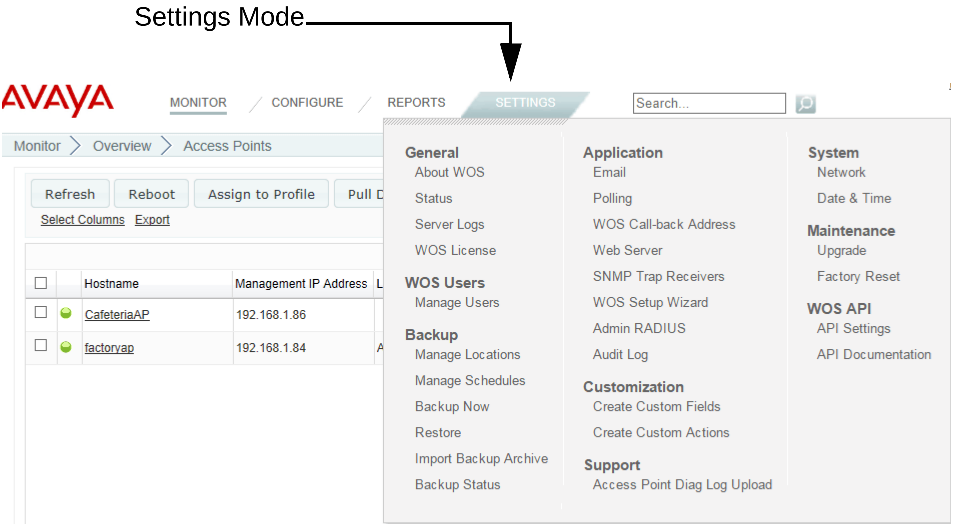
  This page lists all the types of reports available in WOS. Click on a report, and enter the desired selection criteria. You may then save the report and run it now or schedule it for later.

Customization

- **“Customize Report Header” on page 278**

  Click this link to customize the appearance of reports by changing the logo at the top of the report.

About Settings Pages



□		Hostname	Management IP Address	L
□	●	CafeteriaAP	192.168.1.86	
□	●	factoryap	192.168.1.84	A

Figure 19. Settings Menus for WOS Server Platforms

These pages are used to change WOS server settings, such as managing user accounts. Click the **Settings** tab at the top of the window to see the list of settings pages.

Settings for Virtual Platforms

General

- About WOS—Click this to display the current running WOS version as well as contact information.
- Status — Shows the running status of the WOS server. For details, see **"Viewing WOS Server Status" on page 556**.
- Server Logs—shows WOS server's operational logs. For details, see **"Viewing Server Log Files" on page 608**.
- WOS License—manages the license for the WOS software. For details, see **"Managing the WOS Server License" on page 610**.

WOS Users

- Manage Users—manages accounts for WOS users/administrators. See **"WOS Users" on page 570**.

Backup

- Backup—sets up WOS database backups. For details, see **"Database Backup Settings" on page 560**.

Application

- Email—specifies the SMTP server that WOS uses for sending emails. For details, see **"Email Settings" on page 588**.
- Polling—changes the frequency of polling APs. For details, see **"Polling Settings" on page 589**.
- WOS Call-back Address—changes the server address used by APs for some forms of communication. For details, see **"WOS Call-back Address" on page 591**.
- Web Server—changes the HTTP/HTTPS IP address used for accessing the WOS server. For details, see **"Web Server" on page 592**.

- SNMP Trap Receivers—the WOS server sends traps to supervisory software at these addresses when an alarm occurs. For details, see **“SNMP Trap Receivers” on page 593**.
- WOS Setup Wizard—initial setup steps for WOS server to enter license and discover AP network. For details, see **“WOS Setup Wizard” on page 594**.
- Admin RADIUS—specify RADIUS servers to be used for authenticating WOS logins. For details, see **“Admin RADIUS” on page 603**.
- Audit Log—shows all of the configuration changes that have occurred on managed APs. For details, see **“Audit Log” on page 607**.

Customization

- **Create Custom Fields**—defines custom columns to be displayed on APs pages. See **“Create Custom Fields” on page 574**.
- **Create Custom Actions**—defines custom actions to be offered on APs pages. See **“Create Custom Actions” on page 575**.

Support

- **AP Diag Log Upload**—uploads diagnostic information from selected APs to an FTP server.

WOS API

- **API Settings**—Controls API access to the WOS server. For details, see **“API Settings” on page 580**.
- **API Documentation**—describes the API and provides a sandbox for making sample calls. For details, see **“API Documentation” on page 582**.

Settings for Virtual Appliance

The following settings provide functions such as setting the network address and the system time for the host.

- Web Server—Configures HTTP and HTTPS access to the WOS server, including the ports used. For details, see **"Web Server" on page 592**.

Maintenance

- Upgrade—Upgrade the WOS server software. For details, see **"Performing Server Upgrades" on page 611**.
- Factory Reset—Reinitializes the WOS server and database. For details, see **"Resetting the WOS Server" on page 612**.

Monitoring the Network

About the Monitor Pages

These pages display information about the current status of the network. Click the **Monitor** link at the top of the window to see the list of pages.

The monitor options for WOSare shown in **Figure 16**. These are primarily read-only pages, although most of the pages have links to click to drill down for details, and allow you to export data to a file. The Monitor link always opens to the Dashboard page.

Monitor pages include the following. Click one of the links below for more information.

Overview

- **Dashboard**
- **Maps**
- **Access Points**
- **Radios**
- **SSID**
- **Stations**
- **Legacy APs**

Security

- **Rogues**
- **IDS Events**

Troubleshooting

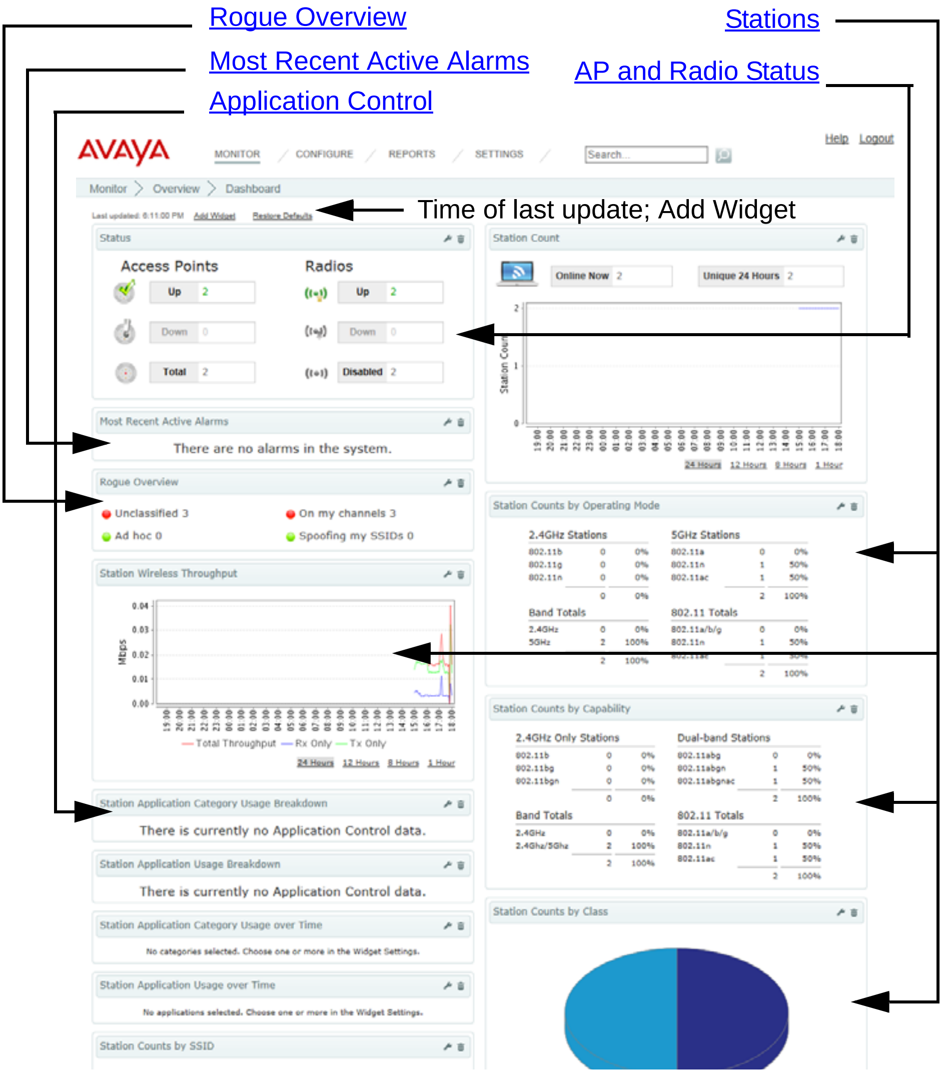
- **Station Assurance**
- **Alarms**
- **Events**

Application Control

- **Application Control—Overview**

Dashboard

The web client Dashboard gives you an at-a-glance overview of all system status and activity. Administrators can quickly assess system health and overall system usage, as well as viewing alarm status.



Status

Access Points		Radios	
Up	2	Up	2
Down	0	Down	0
Total	2	Disabled	2

Station Count

Online Now 2 Unique 24 Hours 2

Most Recent Active Alarms

There are no alarms in the system.

Rogue Overview

● Unclassified 3 ● On my channels 3
● Ad hoc 0 ● Spoofing my SSIDs 0

Station Wireless Throughput

Station Counts by Operating Mode

2.4GHz Stations			5GHz Stations		
802.11b	0	0%	802.11a	0	0%
802.11g	0	0%	802.11n	1	50%
802.11n	0	0%	802.11ac	1	50%
	0	0%		2	100%
Band Totals			**802.11 Totals**		
2.4GHz	0	0%	802.11a/b/g	0	0%
5GHz	2	100%	802.11n	1	50%
	2	100%	802.11ac	1	50%
				2	100%

Station Counts by Capability

2.4GHz Only Stations			Dual-band Stations		
802.11b	0	0%	802.11abg	0	0%
802.11bg	0	0%	802.11abgn	1	50%
802.11bgn	0	0%	802.11abgnac	1	50%
	0	0%		2	100%
Band Totals			**802.11 Totals**		
2.4GHz	0	0%	802.11a/b/g	0	0%
2.4Ghz/5Ghz	2	100%	802.11n	1	50%
	2	100%	802.11ac	1	50%
				2	100%

Station Application Category Usage Breakdown

There is currently no Application Control data.

Station Application Usage Breakdown

There is currently no Application Control data.

Station Application Category Usage over Time

No categories selected. Choose one or more in the Widget Settings.

Station Application Usage over Time

No applications selected. Choose one or more in the Widget Settings.

Station Counts by SSID

Station Counts by Class

Figure 20. Dashboard

The following sections describe the use of the Dashboard:

- **"Dashboard Overview" on page 45**
- **"About Dashboard Data" on page 46**
- **"Application Control" on page 47**
- **"AP and Radio Status" on page 51**
- **"Most Recent Active Alarms" on page 53**
- **"Stations" on page 54**
- **"Rogue Overview" on page 58**
- **"AP Software and License Versions" on page 59**

Dashboard Overview

When you start the web client, the Dashboard is initially displayed. To navigate to it when you have another page displayed, simply click the **Monitor** link at the top of the page and then select **Overview: Dashboard** (**Figure 16 on page 34**).

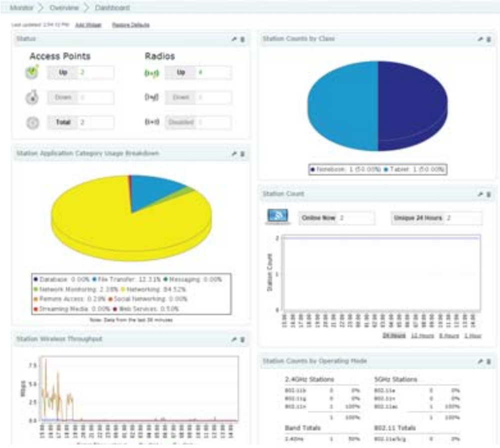
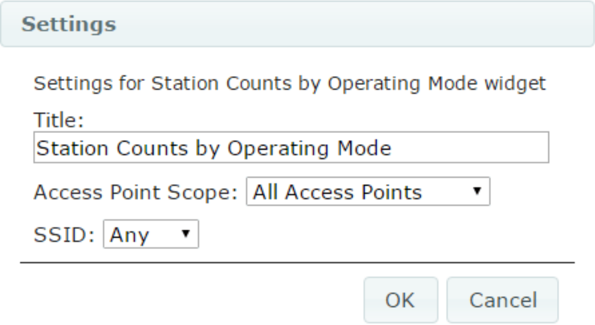

Monitor > Overview > Dashboard
Add Widget
Restore Defaults
Status
Access Points
Radios
Up 2
Up 4
Down
Total 2
Disabled
Station Counts by Class
Notebook: 1 (50.00%) Tablet: 1 (50.00%)
Station Application Category Usage Breakdown
Database: 0.00% File Transfer: 12.11% Messaging: 0.00%
Network Monitoring: 2.28% Networking: 84.52%
Remote Access: 0.21% Social Networking: 0.00%
Streaming Media: 0.00% Web Services: 0.50%
Note: Data from the last 30 minutes
Station Count
Online Now 2
Unique 24 Hours 2
Station Count
24 Hours 12 Hours 8 Hours 1 Hour
Station Wireless Throughput
Mbps
7.5
5.0
2.5
0.0
Station Counts by Operating Mode
2.4GHz Stations
5GHz Stations
802.11b
802.11g
802.11n
802.11a
802.11n
802.11ac
Band Totals
802.11 Totals

Figure 21. Three-column Arrangement of Widgets

You may customize the Dashboard to your liking. To rearrange the widgets (i.e., sections), simply click the title bar of a widget and drag and drop it to the desired location. You may even move widgets to the right to make a third or a fourth column to make a horizontal display as shown in **Figure 21**, or arrange them in two columns to make a vertical display. Click the **Restore Defaults** link near the top to return the layout to its original appearance. Changes that you make will only apply to logins by your account—other users' dashboard views will not be affected.

Click the **settings** link 🔧 in the widget's title bar to change the title of any widget and/or have it display only data from a selected **SSID** or AP **Scope** (profile network or group of APs). You may delete any widget using the **delete** link in its title bar. Use the **Add Widget** link near the top of the Dashboard to restore deleted widgets or add others. You may even add the same widget multiple times with different settings, for example, to show a different profile network in each.



Settings

Settings for Station Counts by Operating Mode widget

Title: Station Counts by Operating Mode

Access Point Scope: All Access Points

SSID: Any

Figure 22. Change Widget Settings

In general, a count is faded if its value is zero. For example, if no APs are down in the Status widget, then the count and its icon are faded. This helps present the at-a-glance health of the wireless network by eliminating the display of red symbols when there are no devices down.

About Dashboard Data

The Dashboard displays data for all APs in the WOS **managed network** by default, although you may have a widget display data for just a selected AP **Scope** or a selected SSID by changing its settings. All widgets are updated to contain only data related to the selected APs (except for Alarms, which always shows all alarms). This will not affect data display on other pages—they will continue to display data for all APs.

The Dashboard is automatically refreshed at frequent intervals—you do not have to refresh explicitly. The time of the most recent update is shown towards the upper left, as seen in **Figure 20**. Note that some values displayed in the Dashboard may lag with respect to actual current values—items in the WOS database are polled (updated) at differing intervals. When the Dashboard is refreshed, it simply picks up the current values in the database. The WOS server does not poll APs to update all status or statistics in the database specifically for a Dashboard refresh. Each data item in the database will be refreshed at whatever rate is defined for it. For more details on the polling rate and how to change it, please see **"Polling Settings" on page 589**

The Dashboard refreshes data at the following rates by default:

- Performance data is updated on the Dashboard every 30 seconds. (This is true for APs running Release 3.1 and higher software images.)
- Data for the Dashboard is updated at least every two minutes.
- Alarms occur in real time. Traps generated by APs and other events with a severity greater than informational are displayed as alarms.

Application Control

The Application Control widgets provide real-time visibility of application usage by users across the wireless network for the selected AP **Scope** (see **"About Dashboard Data" on page 46**), categorized in a number of ways. Each AP uses Deep Packet Inspection (DPI) to determine what applications are being used and by whom, and how much bandwidth they are consuming. For more information, see **"Application Control—Overview" on page 104**.

Four widgets describe Application Control:

- **Station Application Category Usage Breakdown**
- **Station Application Usage Breakdown**
- **Station Application Category Usage over Time**
- **Station Application Usage over Time**

Station Application Category Usage Breakdown

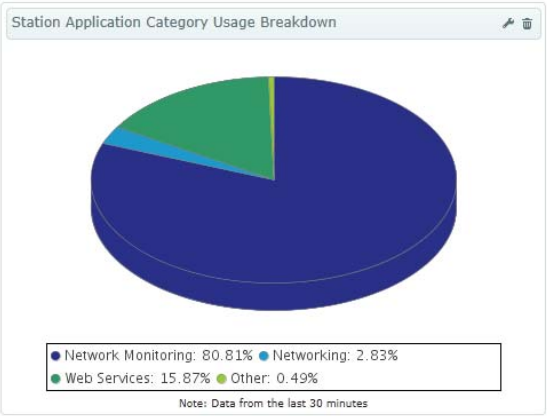

Station Application Category Usage Breakdown
● Network Monitoring: 80.81% ● Networking: 2.83%
● Web Services: 15.87% ● Other: 0.49%
Note: Data from the last 30 minutes

Figure 23. Dashboard - Station Application Category Usage Breakdown

This provides a breakdown of the categories of applications being used on the selected APs. Traffic is analyzed by what types of applications are in use, such as Games or Collaboration, rather than by specific application names. This gives you an overview of the categories of work (or not work!) for which the wireless network is being used.

Station Application Usage Breakdown

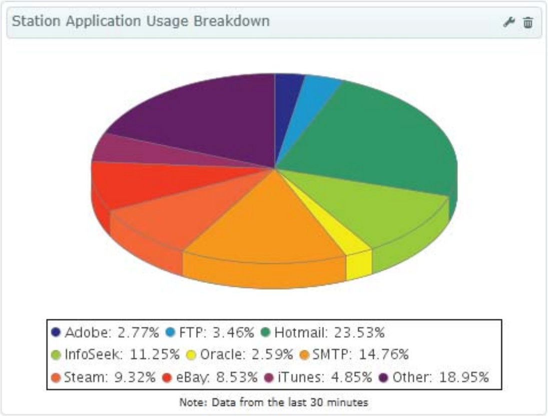
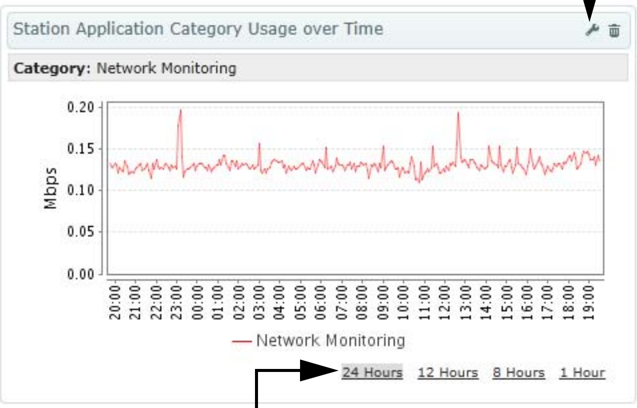

Station Application Usage Breakdown
● Adobe: 2.77% ● FTP: 3.46% ● Hotmail: 23.53%
● InfoSeek: 11.25% ● Oracle: 2.59% ● SMTP: 14.76%
● Steam: 9.32% ● eBay: 8.53% ● iTunes: 4.85% ● Other: 18.95%
Note: Data from the last 30 minutes

Figure 24. Dashboard - Station Application Usage Breakdown

This provides a breakdown of the applications being used on the selected APs. Traffic is analyzed for the applications in use, such as SNMP or Facebook.

Station Application Category Usage over Time

Click here to select a Category



Station Application Category Usage over Time

Category: Network Monitoring

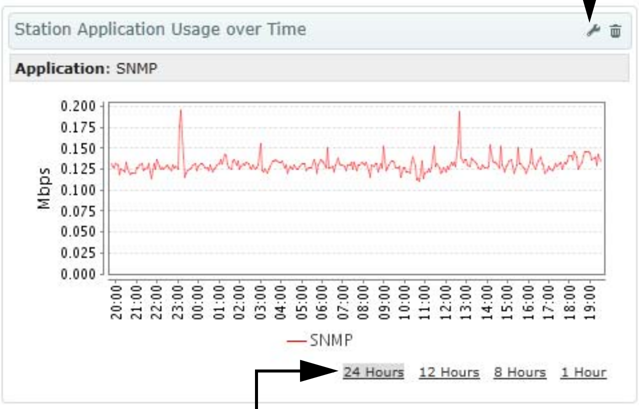
Click here to select a Time Period

Figure 25. Dashboard - Station Application Category Usage over Time

This graph shows the amount of network traffic used by a selected category of application over time, on the selected APs. Select a Category of application and a time period as shown in **Figure 25**.

Station Application Usage over Time

Click here to select an Application



Station Application Usage over Time

Application: SNMP

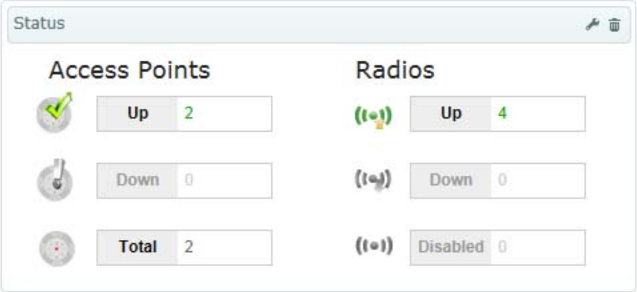
Click here to select a Time Period

Figure 26. Dashboard - Station Application Usage over Time

This graph shows the amount of network traffic used by a selected application over time, on the selected APs. Select an application and a time period as shown in **Figure 26**. When selecting an application, select a category first - this helps narrow down the final selection of application, as APs recognize hundreds of applications.

AP and Radio Status

The AP and Radio Status widget summarizes the number of each that are up or down. Use the **settings** link on the title bar if you wish to filter the results to display values for a selected AP Group only (see **"AP Groups" on page 117**).



Status

Access Points		Radios	
Up	2	Up	4
Down	0	Down	0
Total	2	Disabled	0

Figure 27. Dashboard - AP and Radio Status

AP Status Details

This is a summary of the status of the selected APs that are known to WOS. The entries show the count of APs that are up or down, and the total count. Click on a count, and the web client will display the **Access Points** or **Radios** page, filtered to show only entries that have the status that you selected.

The following status counts are shown:

- **Up (green)**—the number of APs that are **up**, in the selected group. Click this button to show only APs whose status is up in the **Access Points** page.
- **Down (red)**—the number of APs that are **down**, in the selected group. An AP is considered to be down if WOS has been unable to communicate with it for over three minutes. Click this button to show only APs that are down in the **Access Points** page.
- **Off line (blue)**—the number of APs that have been temporarily taken out of service in the selected group. See the **Take AP(s) Out of Service** option under **"More" on page 114**.

- **Total**—the **total** number of APs in the group that are known to WOS. Click this button to show all APs in the **Access Points** page, regardless of status.

Radio Status Details

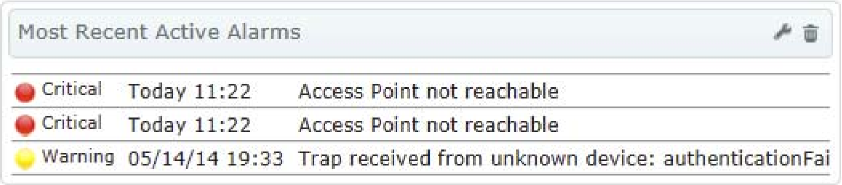
This is a summary of the status of all radios on APs that are known to WOS in the selected AP group. The entries show the count of radios at each status value. Each entry is a link—click it to display the **Radios** page, with the radio list filtered to show only those radios that have the selected status value.

The following status counts are shown:

- **Up (green)**—the number of radios that are **up**. Click this button to show only radios whose status is up in the **Radios** page.
- **Down (red)**—the number of radios that are **down**. Click this button to show only radios that are down in the **Radios** page.
- **Disabled (gray)**—the number of radios that are not enabled on APs. Click this button to show only radios that are disabled in the **Radios** page.

Most Recent Active Alarms

This table lists the most recent alarms generated by your wireless network. For each alarm, the dashboard shows the severity, the date, and the beginning of the description. To see more information for an alarm in the list, click it to view the Alarm Details. All severity levels are displayed—Critical, Major, Minor, Warning, and Clear. Alarms are shown only for APs in the selected AP Group.



Most Recent Active Alarms

● Critical	Today 11:22	Access Point not reachable
● Critical	Today 11:22	Access Point not reachable
● Warning	05/14/14 19:33	Trap received from unknown device: authenticationFai

Figure 28. Dashboard - Recent Alarms

To see a complete list of wireless network alarms, use the web client **Alarms** page (see **“Alarms” on page 98**).

- **Alarm severity classifications**
  - **Critical**—Red
  - **Major**—Orange
  - **Minor**—Gold
  - **Warning**—Yellow
  - **Clear**—Green

  Each entry is a link. Click it, and additional details are displayed.

Stations

The Stations widgets summarize the number of stations associated to APs for the selected AP Group (see **"About Dashboard Data" on page 46**), categorized in a number of ways.

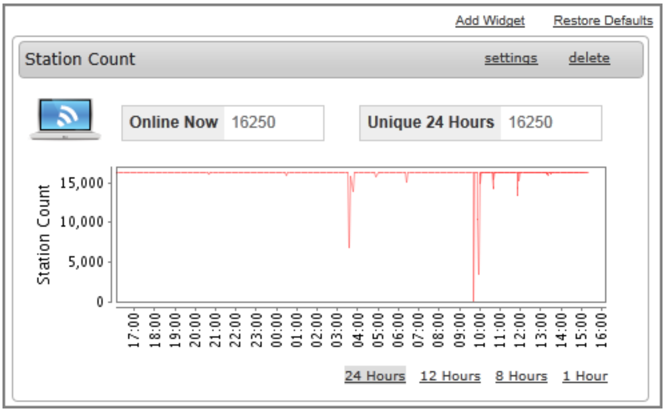


Figure 29. Dashboard - Station Count

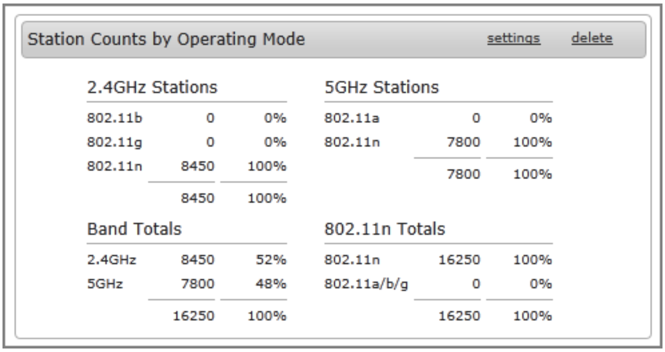
Seven widgets describe stations:

- **Station Count**
- **Station Counts by Operating Mode**
- **Station Counts by Capability**
- **Station Counts by Manufacturer**
- **Station Counts by Class**
- **Station Counts by SSID**
- **Station Throughput**

Station Count

This shows the total number of stations associated to APs known to WOS, and plots the number of stations over time. (**Figure 29**) Select the desired time period for the graph— 24 hours is the default.

Station Counts by Operating Mode



Station Counts by Operating Mode

2.4GHz Stations		
802.11b	0	0%
802.11g	0	0%
802.11n	8450	100%
	8450	100%

5GHz Stations		
802.11a	0	0%
802.11n	7800	100%
	7800	100%

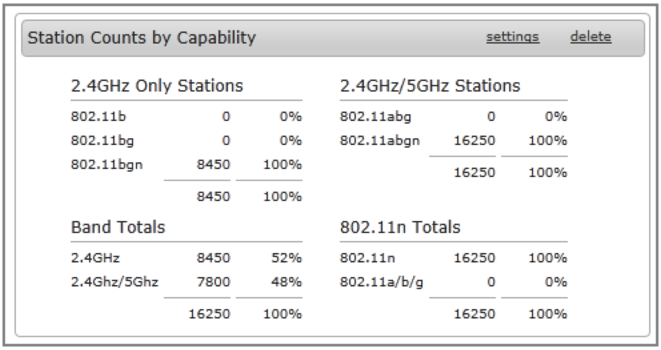
Band Totals		
2.4GHz	8450	52%
5GHz	7800	48%
	16250	100%

802.11n Totals		
802.11n	16250	100%
802.11a/b/g	0	0%
	16250	100%

Figure 30. Dashboard - Station Counts by Operating Mode

This provides a breakdown of stations by band and by Wi-Fi mode: the number of 802.11n and 802.11ac stations (in the 5GHz and 2.4 GHz bands), 802.11a, 802.11bg, and 802.11b stations that are currently associated to the selected APs.

Station Counts by Capability



Station Counts by Capability

2.4GHz Only Stations		
802.11b	0	0%
802.11bg	0	0%
802.11bgn	8450	100%
	8450	100%

2.4GHz/5GHz Stations		
802.11abg	0	0%
802.11abgn	16250	100%
	16250	100%

Band Totals		
2.4GHz	8450	52%
2.4Ghz/5Ghz	7800	48%
	16250	100%

802.11n Totals		
802.11n	16250	100%
802.11a/b/g	0	0%
	16250	100%

Figure 31. Dashboard - Station Count by Capability

This widget is similar to **Station Counts by Operating Mode**. Instead of displaying the types of station connections, this widget shows the wireless capabilities of the connected stations.

Station Counts by Class

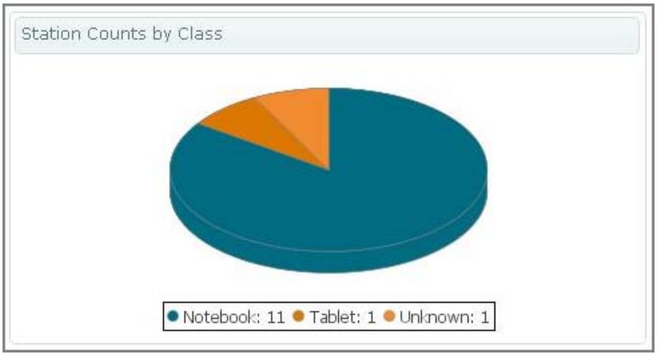
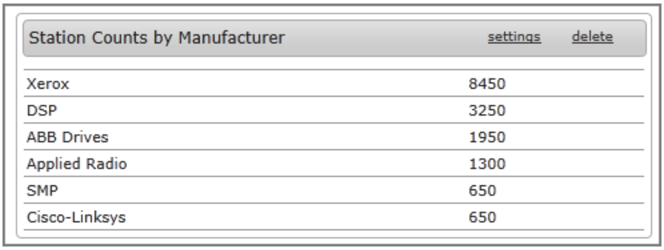


Figure 32. Dashboard - Station Count by Class

This provides a breakdown of the number of stations by class of device, for example, phone, tablet, notebook, etc. A pie chart shows the proportion of each type.

Station Counts by Manufacturer



Station Counts by Manufacturer

Xerox	8450
DSP	3250
ABB Drives	1950
Applied Radio	1300
SMP	650
Cisco-Linksys	650

Figure 33. Dashboard - Station Count by Manufacturer

This provides a breakdown by station manufacturer of the number of stations that are currently associated to the selected APs. The most common manufacturers of stations in your network environment are listed, with those having the highest number of stations listed first. Up to ten manufacturers are listed.

Station Counts by SSID

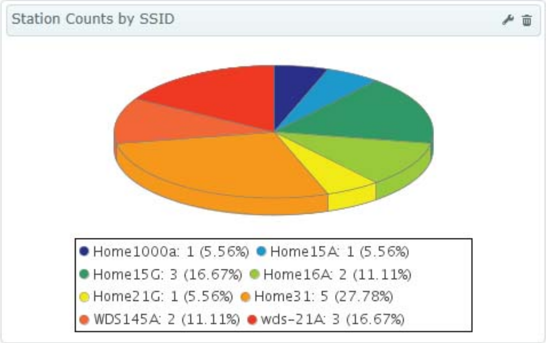


Figure 34. Dashboard - Station Counts by SSID

This provides a network breakdown of the number of stations by the SSID to which they have associated, in both tabular and graphical form. Each SSID is listed by name, along with its station count and the percentage of stations connected to it.

Station Throughput

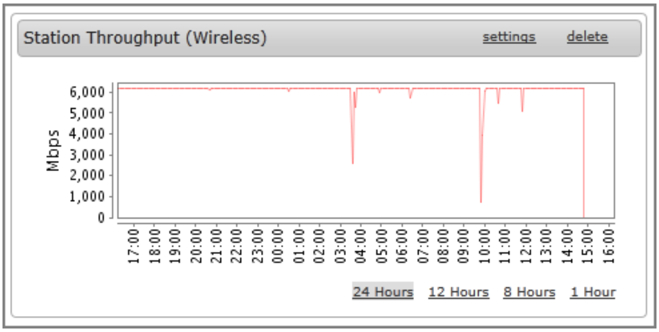
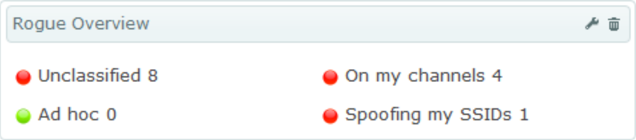


Figure 35. Dashboard - Station Throughput

This graphs the aggregate station throughput of your wireless network over time. Select the desired time period for the graph— 24 hours is the default.

Rogue Overview

This widget provides a quick snapshot of the security status of the selected AP Group in the wireless network (see **"About Dashboard Data" on page 46**), including counts of rogue APs. Each entry is a link—click it to display on the selected items on the **Rogues** page.



Rogue Overview

● Unclassified 8
● On my channels 4
● Ad hoc 0
● Spoofing my SSIDs 1

Figure 36. Dashboard - Rogue Overview

For more information about security and intrusion detection, please see **"Rogues" on page 90**.

This is a summary of the more dangerous APs that have been detected by the selected APs. Categories that have a zero count are shown with a green check mark; categories that have a non-zero count are flagged in orange. Rogues that you have already classified are not shown. The categories shown are:

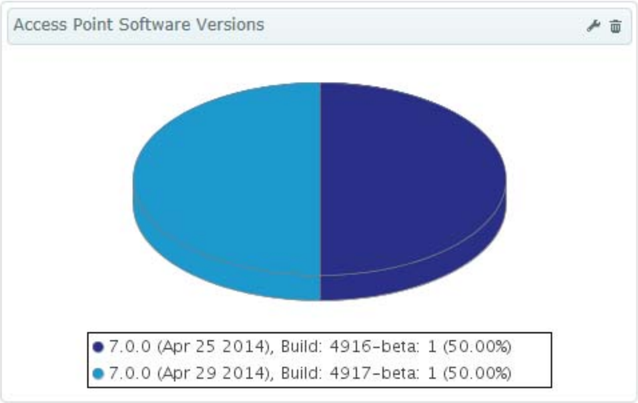
- **Unclassified**: When a device is initially detected, it is unclassified, which simply means that no one has classified it yet. To classify a device, see **"Rogues" on page 90**.
- **Ad hoc**: An ad hoc wireless network is typically a network formed between two or more stations that are communicating with each other directly without going through a normal AP. This line shows a count of ad hoc nodes detected by AP. Ad hoc networks can disrupt the performance of your wireless network by contributing additional RF interference to the environment.
- **On my channels**: This is the number of detected rogues that are on channels that are the same as or adjacent to the channels used by AP

radios that are in operation. All classes of rogues are included except for Approved and Known devices.

- **Spoofing my SSIDs**: This is the number of detected rogues that are using the same SSIDs as your wireless network. All classes of rogues are included except for Approved and Known devices.

AP Software and License Versions

These widgets summarize the software versions and license versions for APs in the selected AP Group (see **"About Dashboard Data" on page 46**).



Access Point Software Versions
● 7.0.0 (Apr 25 2014), Build: 4916-beta: 1 (50.00%)
● 7.0.0 (Apr 29 2014), Build: 4917-beta: 1 (50.00%)

Figure 37. Dashboard - AP Software Versions

Two widgets describe versions:

- **AP Software Versions**
- **AP License Versions**

AP Software Versions

This shows the total number of APs running recent Avaya OS software versions, in both tabular and graphical form. (**Figure 37**)

AP License Versions

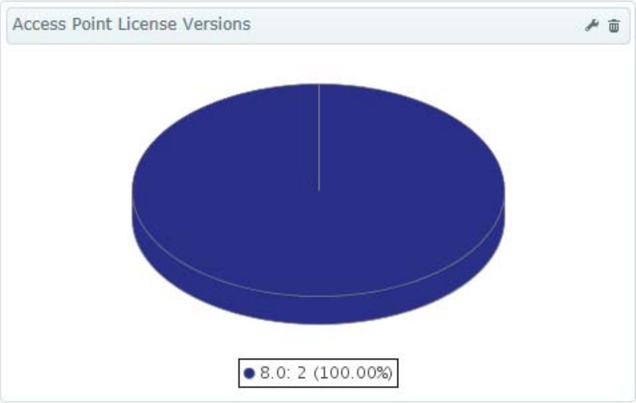


Figure 38. Dashboard - AP License Versions

This shows the total number of APs having various Avaya OS license versions, in both tabular and graphical form.

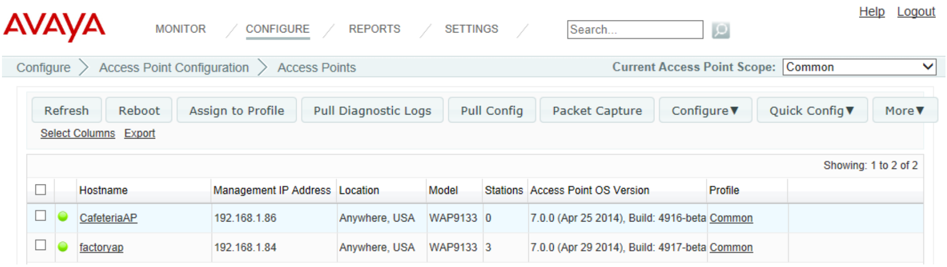
Access Points

The web client APs page lists all of the APs being managed by WOS, and allows you to perform selected management functions on them. You may reboot APs, gather diagnostic logs, or remove APs from the WOS database.

The following sections describe the APs page:

- **About Using the Access Points Page**
- **The Access Points List**
- **The Access Points Toolbar**
- **AP Details**

To perform bulk configuration on APs, please see **“Configure Network Settings” on page 141** and **“Discovery” on page 159**.



Current Access Point Scope: Common

Showing: 1 to 2 of 2

☐		Hostname	Management IP Address	Location	Model	Stations	Access Point OS Version	Profile
☐	●	CafeteriaAP	192.168.1.86	Anywhere, USA	WAP9133	0	7.0.0 (Apr 25 2014), Build: 4916-beta	Common
☐	●	factoryap	192.168.1.84	Anywhere, USA	WAP9133	3	7.0.0 (Apr 29 2014), Build: 4917-beta	Common

Figure 39. APs Page

About Using the Access Points Page

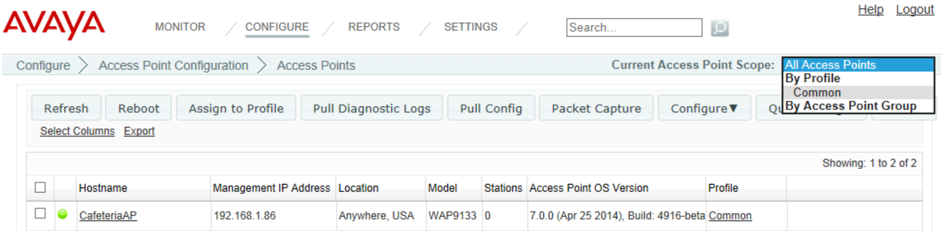
A number of basic operations are available on the APs page to allow you to customize it for your own use:

- **Current Access Point Scope**
- **Select Columns**
- **Export**
- **Select Rows**
- **Rearranging and Resizing Columns in a Table**

- Sorting
- Searching

Current Access Point Scope

In the web client, **Current AP Scope** allows you to filter the data displayed so that only information for members of the selected AP group or profile network is presented. Select the desired **AP Group** or **Profile** from the drop-down list. For example, if you select a profile network on the **The Access Points List** window, then only the APs that are members of the selected profile are displayed.



Showing: 1 to 2 of 2

□		Hostname	Management IP Address	Location	Model	Stations	Access Point OS Version	Profile
□	●	CafeteriaAP	192.168.1.86	Anywhere, USA	WAP9133	0	7.0.0 (Apr 25 2014), Build: 4916-beta	Common

This selection is persistent when you browse to other pages, until you change **Current AP Scope**. Thus, if you select a profile on the **The Access Points List** window and then open the **Radios** window, it will only list radios that belong to the selected APs.

Select Columns

The page may be customized by changing the columns that are displayed and the order of display. If you prefer to use a smaller browser window for WOS and there's not enough room for all the columns to display, you can use this feature to select your preferred columns. Click the **Select Columns** link on the upper right to display the table column chooser.

The left hand column shows the columns that will be displayed, with the number of items selected at the top. To hide a column, select it from the list and drag it to the right hand (non-selected) list. Similarly, to display a column, select it from the right hand list and drag it to the desired display order in the selected columns list.

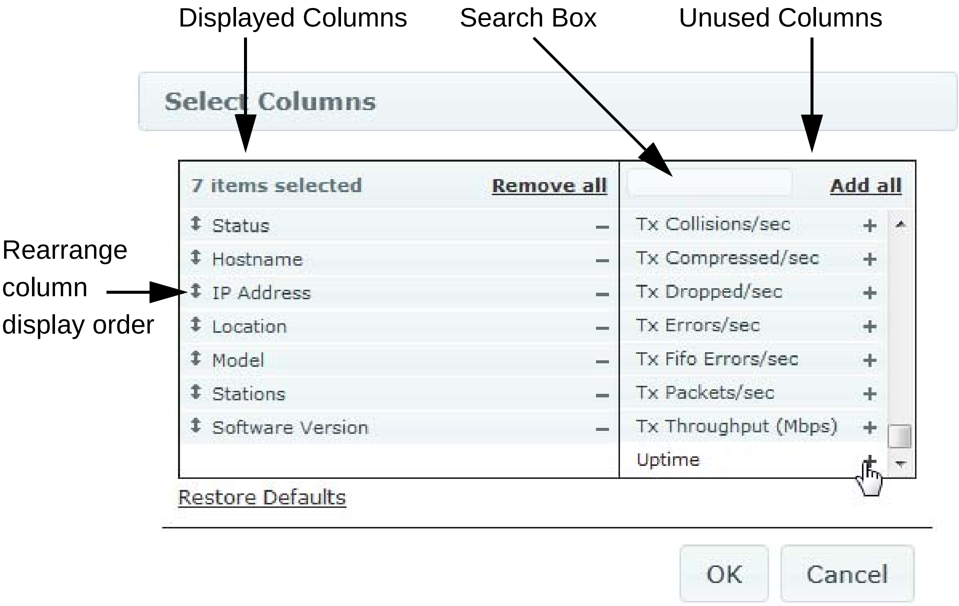


Figure 40. Table Column Chooser

You may type text into the Search Box shown above the right hand list in **Figure 40** to filter the unused columns list to show only column headers that contain the specified string. For example, type **ip** and the list will show three options: **Eth0 IP Address**, **Gig1 IP Address**, and **Gig2 IP Address**. You may drag selected items up or down to rearrange the order in which they will be displayed. There is also a button to **Restore Default** display settings. Click **OK** when done.

These changes are persistenton a per-user basis—if you log out, they will still apply the next time that you open the web client.

Export

The **Export** link above the list may be used to export rows from this page to an Excel file or to a CSV file—a set of comma-separated values that are compatible with Microsoft Excel. The exported file may be used to provide Avaya Customer Support with a snapshot of the configuration of your network, at their request. All rows will be exported, but only the displayed columns will be exported.

When you click **Export**, a dialog box allows you to select the file format. Click the **Export** button again to browse to the destination folder and specify the filename.

Select Rows

Simply click the checkboxes of the rows you wish to select. You may then click function buttons to perform operations on the selected entries. You may click the checkbox in the header row to select all rows. Click again to deselect all rows. To select a number of consecutive rows, you may click the checkbox of the first desired row. Then use Shift+Click to select the checkbox of the last desired row.

If the list contains many entries, use the scroll bar on the right to find the desired entries (or use **Searching**).

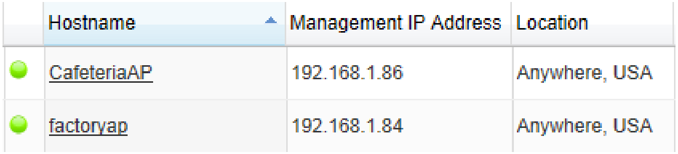
Rearranging and Resizing Columns in a Table

For easier viewing of list data, you may rearrange columns by dragging the column header and moving it to the desired position. This is helpful if you wish to view particular columns in close proximity, or to move less viewed columns to the right. The new arrangement is saved per user. The next time you log in, you will see the columns in the same order.

To resize a column, simply drag the right-side edge of the column to expand or reduce the width of the column. You may auto-size a column by double clicking on its right edge. The column will automatically expand or shrink to the correct size so that all data in the displayed rows is visible.

Sorting

To change how the table is sorted, click in any column header to define that column as the sort criteria. You may click in any column (except the checkbox column). Click the header for the status column (red or green dots on the left of the table) to sort APs by operating status. In addition, you can choose to have the results displayed in ascending order or descending order. To do this, simply click in the same header again to toggle between ascending and descending order. An arrow in the column header indicates which column was used for sorting and which order the grid is sorted in.

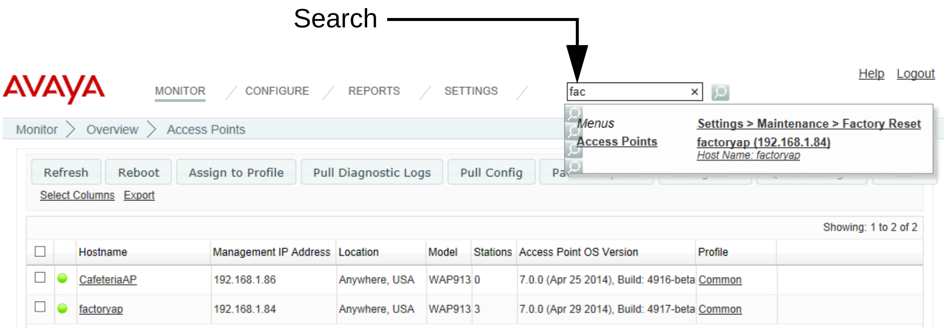


	Hostname ▲	Management IP Address	Location
●	CafeteriaAP	192.168.1.86	Anywhere, USA
●	factoryap	192.168.1.84	Anywhere, USA

Figure 41. Sorting on a Column

Searching

Enter a string in the **Search** box, and WOS will display a list of matching entries as you type. The list appears after you type a couple of characters, and is refined as you continue typing. Results are displayed as links that you may click to go to the corresponding entry. (**Figure 42**)



Showing: 1 to 2 of 2

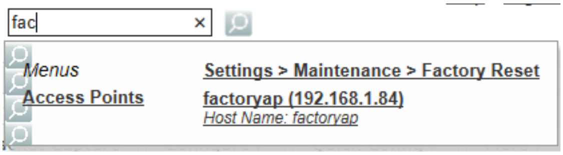
□		Hostname	Management IP Address	Location	Model	Stations	Access Point OS Version	Profile
□	●	CafeteriaAP	192.168.1.86	Anywhere, USA	WAP913	0	7.0.0 (Apr 25 2014), Build: 4916-beta	Common
□	●	factoryap	192.168.1.84	Anywhere, USA	WAP913	3	7.0.0 (Apr 29 2014), Build: 4917-beta	Common

Figure 42. Search Results

APs, Stations, Rogues, Group Names, Profile Names, and even WMI menu options are shown. (**Figure 43**) If no results are displayed, then no matching entries could be found.

The following fields are searched:

- APs—Hostname, Location, Gigabit1 IP Address, Ethernet0 IP Address, Management IP Address, Software Version, Ethernet0 MAC Address, Gigabit1 MAC Address, Gigabit2 MAC Address, Serial Number, License Key, Profile.
- Rogues—SSID, BSSID, Manufacturer.
- Stations—MAC Address, IP Address, NetBIOS, Hostname, Username, Device Type, Device Class, SSID, Manufacturer.



fac

Menus — Settings > Maintenance > Factory Reset

Access Points — factoryap (192.168.1.84)
Host Name: factoryap

Figure 43. Search Results include Web Client Menu Options

The Access Points List

The APs List (**Figure 39 on page 61**) shows APs that have been discovered by WOS. Only APs that belong to the group selected in **Current AP Scope** are displayed. To search for a particular AP, see **“Searching” on page 65**. **The Access Points Toolbar** allows you to perform a number of operations selected APs.

Click on an AP’s Hostname to access a variety of **AP Details** pages.

For each AP, the following information is shown by default:

- A green or red dot showing the current status of each AP
- The **Hostname**
- The **Management IP Address** of the AP
- The **Location** of the AP (if this information was configured on the AP)
- The **Model** of the AP
- The number of **Stations** associated to this AP
- The **AOS version** running on the AP

- The **Profile** network that the AP is a member of, if any (see **"Managing by Profiles" on page 195**)

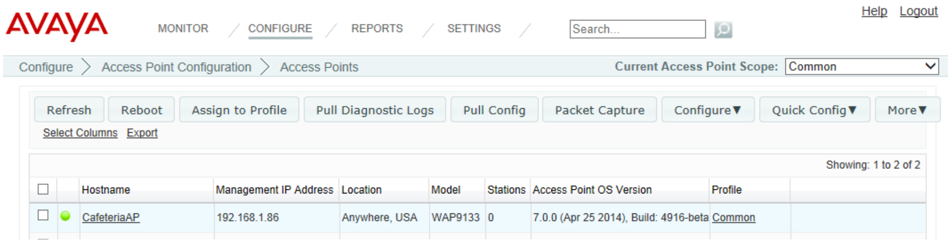
A newly discovered AP will automatically be added to the default profile network, if one has been specified. See **"Managing by Profiles" on page 195** *and the* ***Default*** *button in* **"The Profiles Toolbar" on page 199**.

You may customize the columns shown in this list—many more columns are available. For example, selecting the **Licensed Features** column is the best way to see the features supported on all of your APs. See **"Select Columns" on page 62**.

An AP's Host Name will typically be used to identify the AP throughout the WOS user interface. In places where a specific attribute such as IP address is called out, then that value will be shown.

The Access Points Toolbar

The APs toolbar offers functions for AP management, including configuration, gathering diagnostic information, rebooting selected APs, and capturing packets. This toolbar is visible to WOS users with read-write privileges. WOS users with read-only privileges will see a restricted toolbar that only includes options for **Refresh**, **Pull Diagnostic Logs**, **Pull Config**, and **Packet Capture**.



□		Hostname	Management IP Address	Location	Model	Stations	Access Point OS Version	Profile
□	●	CafeteriaAP	192.168.1.86	Anywhere, USA	WAP9133	0	7.0.0 (Apr 25 2014), Build: 4916-beta	Common

Figure 44. The Monitor—APs Page Toolbar

Select one or more APs in the list by clicking their checkboxes in the first column. You may click the checkbox in the header row to select all APs, or click again to deselect all. The operations available are very similar to those offered on the Configure APs Toolbar. See **"The Configure APs Toolbar" on page 110** for details.

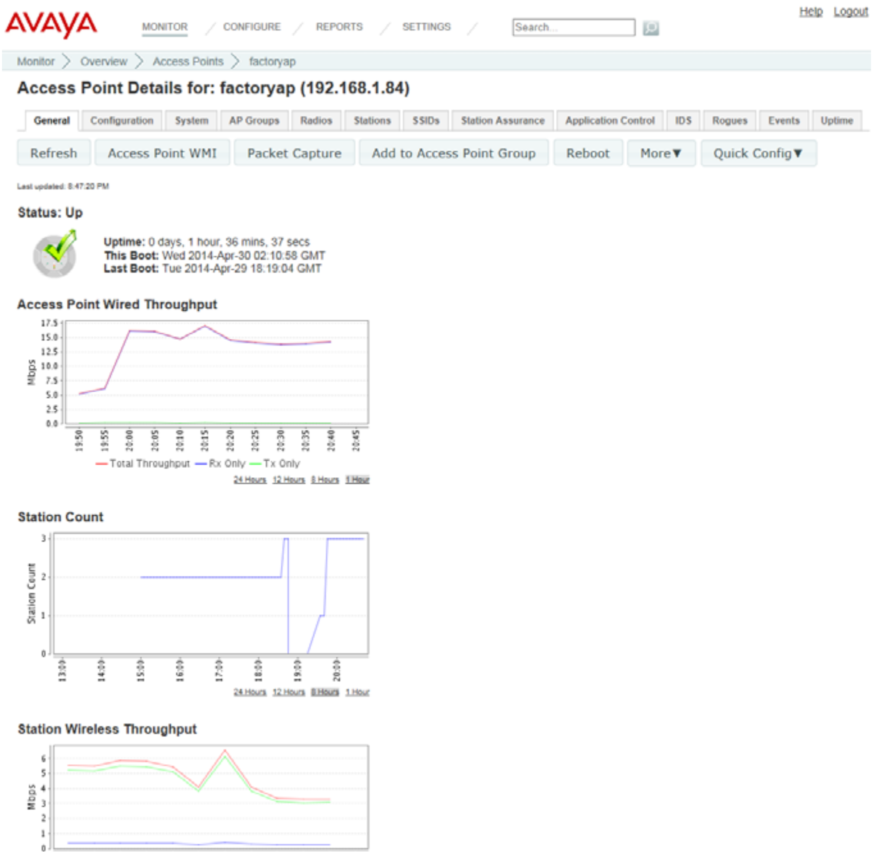
AP Details

By clicking the **Hostname** of an AP in **The Access Points List**, you may view a variety of details about the selected unit.

- **"AP Details—General" on page 69**
- **"AP Details—Configuration" on page 70**
- **"AP Details—System" on page 71**
- **"AP Details—AP Groups" on page 72**
- **"AP Details—Radios" on page 72**
- **"AP Details—Stations" on page 73**
- **"AP Details—SSIDs" on page 73**
- **"AP Details—Station Assurance" on page 74**
- **"AP Details—Application Control" on page 74**
- **"AP Details—IDS" on page 76**
- **"AP Details—Rogues" on page 77**
- **"AP Details—Events" on page 77**
- **"AP Details—Uptime" on page 78**
- **"AP Details—Fabric Attach (FA)" on page 78**

AP Details—General

This page shows the status of the AP, time of the current and previous boot, and graphs over time of wired and wireless throughput and station counts.



Access Point Details for: factoryap (192.168.1.84)

Last updated: 8:47:20 PM

Status: Up

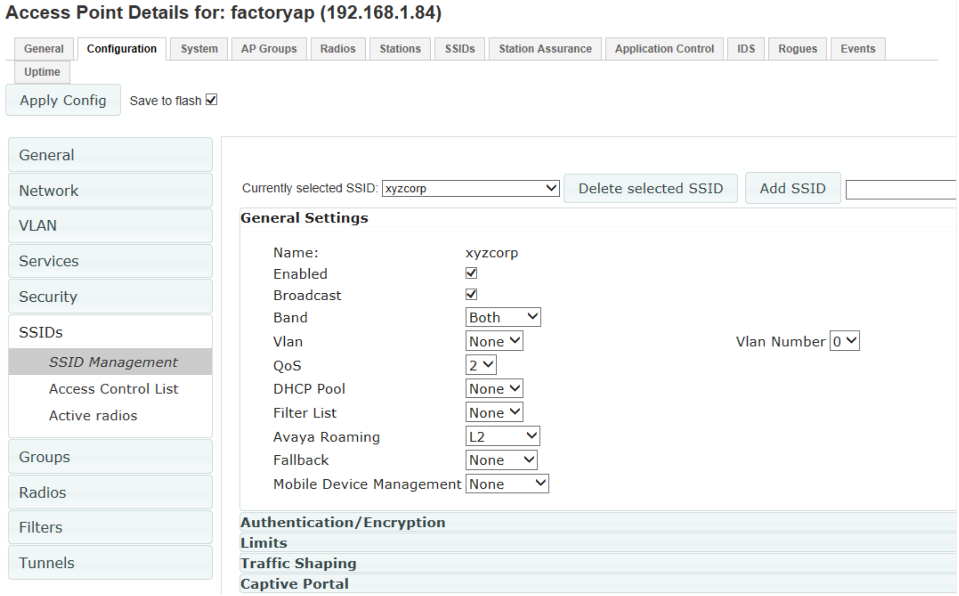
Uptime: 0 days, 1 hour, 36 mins, 37 secs
This Boot: Wed 2014-Apr-30 02:10:58 GMT
Last Boot: Tue 2014-Apr-29 18:19:04 GMT

Figure 45. AP Details: General

It also offers a number of useful AP management functions. For more information on these functions, see **“The Configure APs Toolbar” on page 110**. AP **WMI** button opens a browser window for the current AP’s Windows Management Interface.

AP Details—Configuration

This page has an extensive menu of options for changing settings on the selected AP. It is described in its own chapter. See **"Configuring a Wireless AP" on page 369**.



Access Point Details for: factoryap (192.168.1.84)

Save to flash ☑

Currently selected SSID: xyzcorp

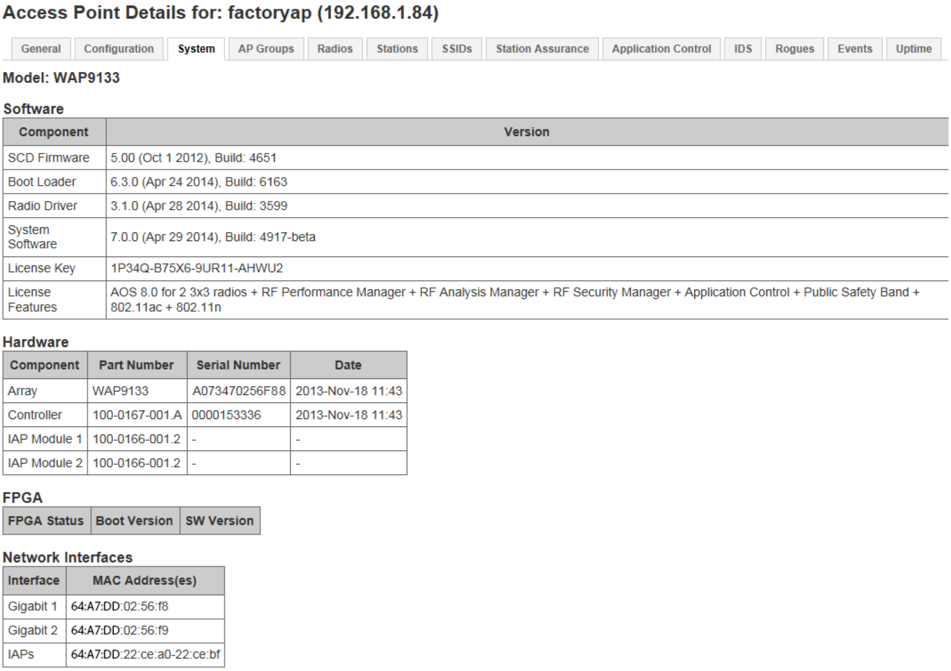
General Settings

Name: xyzcorp
Enabled ☑
Broadcast ☑
Band Both
Vlan None
Vlan Number 0
QoS 2
DHCP Pool None
Filter List None
Avaya Roaming L2
Fallback None
Mobile Device Management None

Figure 46. AP Details: Configuration

AP Details—System

This page shows system information for the AP, including serial numbers for major components, software versions and licensed features, and MAC addresses for wired and wireless interfaces. radio MAC addresses are shown as a range. For example, if an AP shows MAC addresses from 64:a7:DD:00:00:00-64:a7:DD:FF:FF:FF, addresses are assigned from this pool, starting at 64:a7:DD:00:00:00. Each radio’s SSID will have its own address assigned.



Access Point Details for: factoryap (192.168.1.84)

Model: WAP9133

Software

Component	Version
SCD Firmware	5.00 (Oct 1 2012), Build: 4651
Boot Loader	6.3.0 (Apr 24 2014), Build: 6163
Radio Driver	3.1.0 (Apr 28 2014), Build: 3599
System Software	7.0.0 (Apr 29 2014), Build: 4917-beta
License Key	1P34Q-B75X6-9UR11-AHWU2
License Features	AOS 8.0 for 2 3x3 radios + RF Performance Manager + RF Analysis Manager + RF Security Manager + Application Control + Public Safety Band + 802.11ac + 802.11n

Hardware

Component	Part Number	Serial Number	Date
Array	WAP9133	A073470256F88	2013-Nov-18 11:43
Controller	100-0167-001.A	0000153336	2013-Nov-18 11:43
IAP Module 1	100-0166-001.2	-	-
IAP Module 2	100-0166-001.2	-	-

FPGA

FPGA Status	Boot Version	SW Version

Network Interfaces

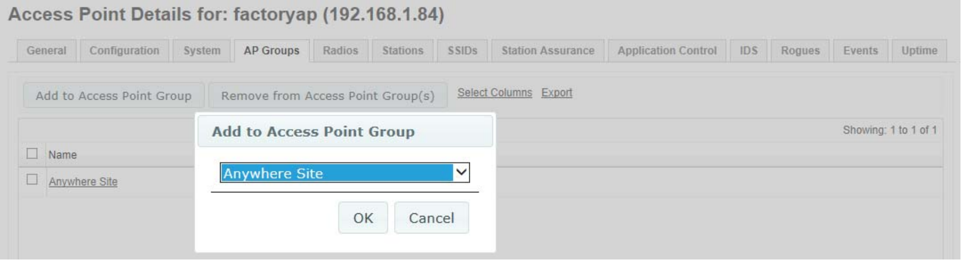
Interface	MAC Address(es)
Gigabit 1	64:A7:DD:02:56:f8
Gigabit 2	64:A7:DD:02:56:f9
IAPs	64:A7:DD:22:ce:a0-22:ce:bf

Figure 47. AP Details: System

AP Details—AP Groups

This page lists the groups to which the AP belongs, if any. An AP may belong to multiple groups. To add this AP to an additional group, click **Add to Group** and select the desired group from the drop-down list. You may also choose to **Create a new group**. Enter the name of the new group in the dialog box and click **OK**. For more details, see **“AP Groups” on page 117**.

You may also remove this AP from membership in one or more groups. Select the groups from which the AP should be removed by clicking their checkboxes in the first column in the list. Then click **Remove from Group(s)**.

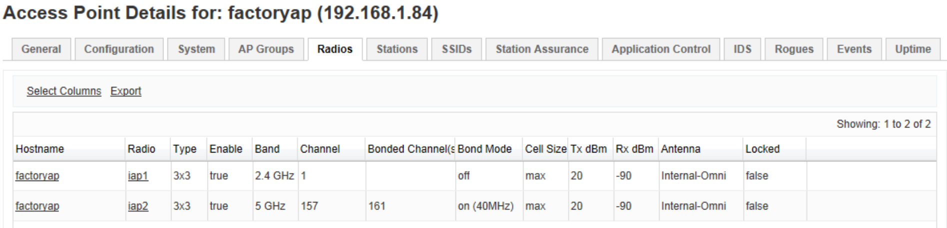


Access Point Details for: factoryap (192.168.1.84)

Figure 48. AP Details: Groups

AP Details—Radios

This page shows radio information for the AP, including band and channel assignments. Each radio is a link—click on it to see details for this radio (see **“The Radios List” on page 81**). For more information, see **“Radios” on page 80** and **“Radio Settings” on page 488**.



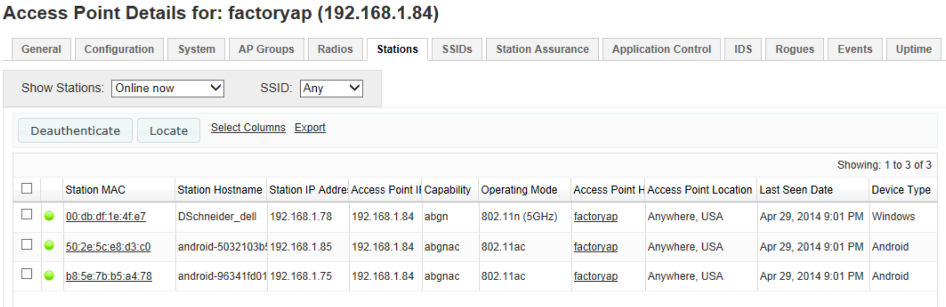
Access Point Details for: factoryap (192.168.1.84)

Hostname	Radio	Type	Enable	Band	Channel	Bonded Channel(s	Bond Mode	Cell Size	Tx dBm	Rx dBm	Antenna	Locked
factoryap	iap1	3x3	true	2.4 GHz	1		off	max	20	-90	Internal-Omni	false
factoryap	iap2	3x3	true	5 GHz	157	161	on (40MHz)	max	20	-90	Internal-Omni	false

Figure 49. AP Details: Radios

AP Details—Stations

This page lists stations associated to the AP, including station MAC and IP addresses and hostname, and the device type and class (iPod, laptop, etc.). Each Station MAC is a link—click on it to see details for this station. For more information, see **“Stations” on page 85**. Many other columns may be chosen using **“Select Columns” on page 62**.



Access Point Details for: factoryap (192.168.1.84)

Show Stations: Online now

SSID: Any

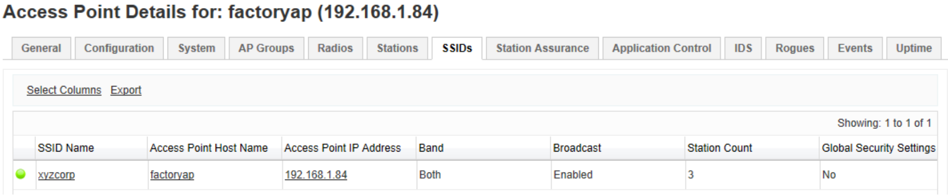
Showing: 1 to 3 of 3

☐		Station MAC	Station Hostname	Station IP Addre	Access Point I	Capability	Operating Mode	Access Point H	Access Point Location	Last Seen Date	Device Type
☐	●	00:db:df:1e:4f:e7	DSchneider_dell	192.168.1.78	192.168.1.84	abgn	802.11n (5GHz)	factoryap	Anywhere, USA	Apr 29, 2014 9:01 PM	Windows
☐	●	50:2e:5c:e8:d3:c0	android-5032103b	192.168.1.85	192.168.1.84	abgnac	802.11ac	factoryap	Anywhere, USA	Apr 29, 2014 9:01 PM	Android
☐	●	b8:5e:7b:b5:a4:78	android-96341fd01	192.168.1.75	192.168.1.84	abgnac	802.11ac	factoryap	Anywhere, USA	Apr 29, 2014 9:01 PM	Android

Figure 50. AP Details: Stations

AP Details—SSIDs

This page shows SSID information for the AP, including security settings. Each SSID Name is a link—click on it to see details for this SSID. Note that the **Captive Portal** tab displays the settings for the portal, if any, defined for this SSID on this AP. **Internal Splash** or **Internal Login** portals are shown as the client will see them. For more information, see **“SSID” on page 82**. See **“SSID Management—Captive Portal” on page 462** to create a captive portal on an AP’s SSID.



Access Point Details for: factoryap (192.168.1.84)

Showing: 1 to 1 of 1

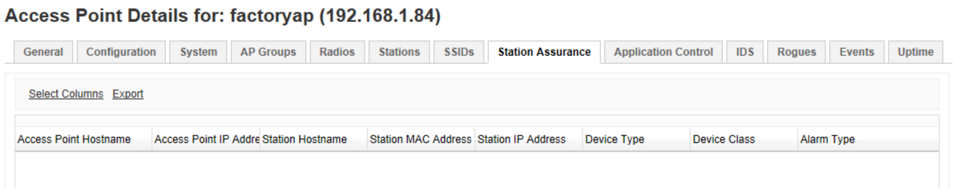
	SSID Name	Access Point Host Name	Access Point IP Address	Band	Broadcast	Station Count	Global Security Settings
●	xyzcorp	factoryap	192.168.1.84	Both	Enabled	3	No

Figure 51. AP Details: SSIDs

The circle at the beginning of each row indicates the status of the SSID—green for enabled, gray for disabled, and yellow if the SSID is enabled but inactive.

AP Details—Station Assurance

This page shows station assurance events for this AP, listing any detected connectivity issues. For descriptions of the types of problems detected, as well as the settings to fine-tune station assurance on the AP, please see **"Station Assurance" on page 96** and the *Using the AvayaOS for Avaya WLAN AP 9100 Series* (NN47252-102).



Access Point Details for: factoryap (192.168.1.84)

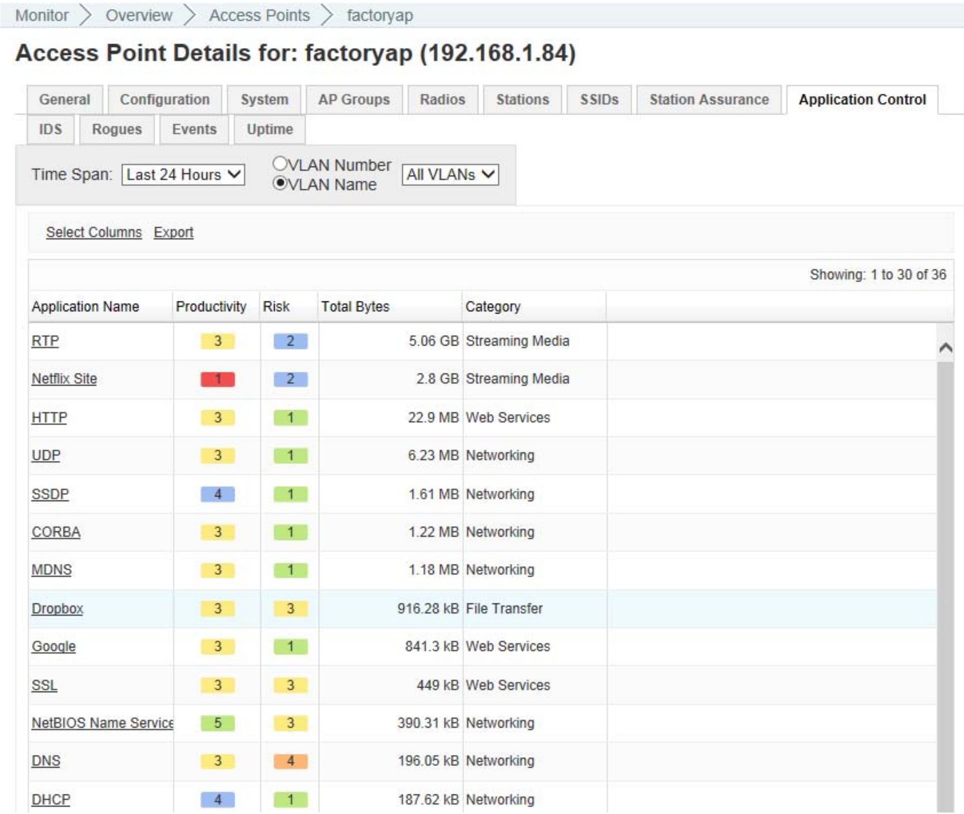
Access Point Hostname	Access Point IP Addre	Station Hostname	Station MAC Address	Station IP Address	Device Type	Device Class	Alarm Type

Figure 52. AP Details: Station Assurance

AP Details—Application Control

*This feature is only available if the AP license includes **Application Control**. See **"About Licensing and Upgrades" on page 182**.*

Application control data (**Figure 53**) provides detailed information about how your wireless bandwidth is being used on an AP, by application. The category of each application is also shown. You may select which **Time Span** to show, and which **VLAN Name** or **Number** to show (or **All VLANs**).



Access Point Details for: factoryap (192.168.1.84)

Time Span: Last 24 Hours ○VLAN Number ●VLAN Name All VLANs

Showing: 1 to 30 of 36

Application Name	Productivity	Risk	Total Bytes	Category
RTP	3	2	5.06 GB	Streaming Media
Netflix Site	1	2	2.8 GB	Streaming Media
HTTP	3	1	22.9 MB	Web Services
UDP	3	1	6.23 MB	Networking
SSDP	4	1	1.61 MB	Networking
CORBA	3	1	1.22 MB	Networking
MDNS	3	1	1.18 MB	Networking
Dropbox	3	3	916.28 kB	File Transfer
Google	3	1	841.3 kB	Web Services
SSL	3	3	449 kB	Web Services
NetBIOS Name Service	5	3	390.31 kB	Networking
DNS	3	4	196.05 kB	Networking
DHCP	4	1	187.62 kB	Networking

Figure 53. AP Details: Application Control

In addition to showing traffic statistics, there are two unique and highly useful columns. **Risk** estimates the likelihood of an application causing problems for your business, rated from 1 (low risk, e.g., Google) to 5 (high risk, e.g., BitTorrent). Risky applications (rated at 4 or 5) are flagged for your attention by highlighting the entry in red. **Productivity** estimates the value of an activity to your business, from 1 (unproductive, e.g., Y8 gaming site) to 5 (productive, e.g., Scopia). Please see **“Application Control—Overview” on page 104** for more details.

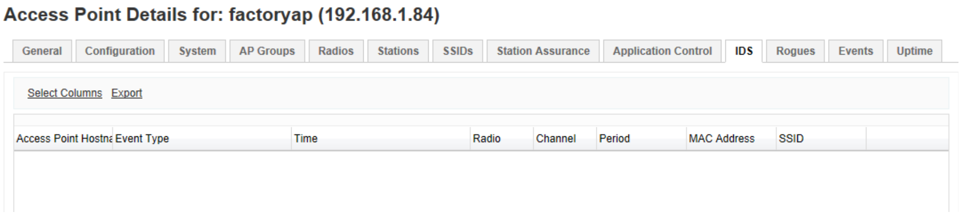
You may click the heading of any column to sort based on that column. Click again to sort in the reverse order.

Each **Application Name** in the list is a link. You may hover over it to display a tool tip with more information about the application, including a description of what it does. You may click the link to display a table listing the AP**s** on which this application has been used, and the amount of traffic that it has generated. You may specify the desired **Time Span** and/or **VLANs** to show. If you prefer, you may show the **Stations** on which this application has been used instead.

When you find risky or unproductive applications taking up bandwidth on the network, you can create filters to control them. See **"Filter Lists" on page 539**.

AP Details—IDS

This page shows Intrusion Detection System (IDS) events for this AP, listing any detected attacks. For descriptions of the types of attacks detected, as well as the settings to fine-tune IDS on the AP, please see *Using the Avaya OS for Avaya WLAN AP 9100 Series* (NN47252-102).



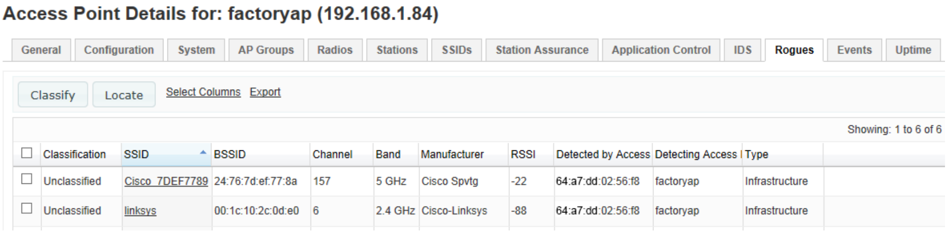
Access Point Details for: factoryap (192.168.1.84)

Access Point Hostna	Event Type	Time	Radio	Channel	Period	MAC Address	SSID

Figure 54. AP Details: IDS

AP Details—Rogues

This page shows rogue APs that have been detected by this AP, including band and channel assignments. For detailed information about a rogue, click its SSID. For more information about rogues, see **"Rogues" on page 90**. To use the Classify or Locate buttons, see **"The Rogues List" on page 91**.



Access Point Details for: factoryap (192.168.1.84)

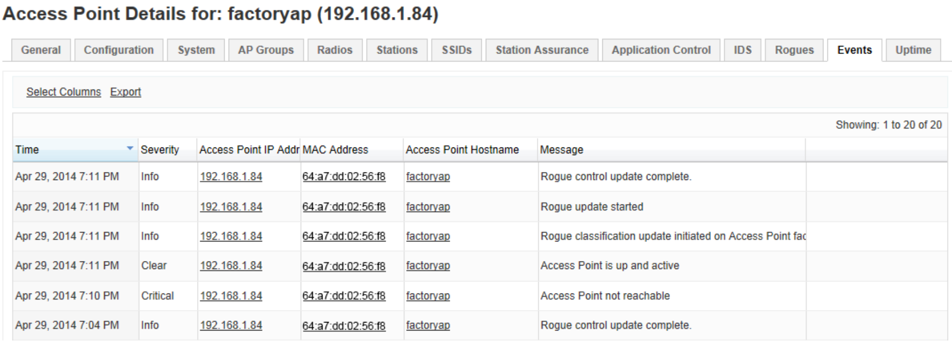
Showing: 1 to 6 of 6

☐	Classification	SSID	BSSID	Channel	Band	Manufacturer	RSSI	Detected by Access	Detecting Access	Type
☐	Unclassified	Cisco_7DEF7789	24:76:7d:ef:77:8a	157	5 GHz	Cisco Spvtg	-22	64:a7:dd:02:56:f8	factoryap	Infrastructure
☐	Unclassified	linksys	00:1c:10:2c:0d:e0	6	2.4 GHz	Cisco-Linksys	-88	64:a7:dd:02:56:f8	factoryap	Infrastructure

Figure 55. AP Details: Rogues

AP Details—Events

This page shows network events detected on this AP. The Message column on the right describes the event.



Access Point Details for: factoryap (192.168.1.84)

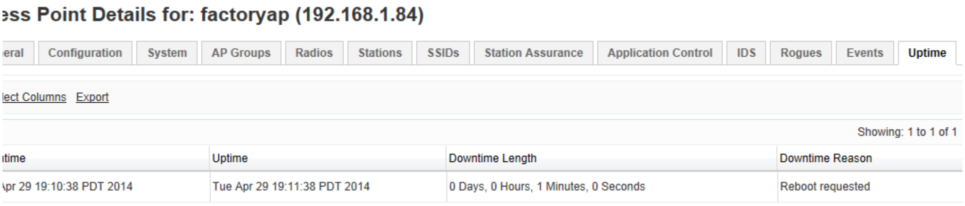
Showing: 1 to 20 of 20

Time	Severity	Access Point IP Addr	MAC Address	Access Point Hostname	Message
Apr 29, 2014 7:11 PM	Info	192.168.1.84	64:a7:dd:02:56:f8	factoryap	Rogue control update complete.
Apr 29, 2014 7:11 PM	Info	192.168.1.84	64:a7:dd:02:56:f8	factoryap	Rogue update started
Apr 29, 2014 7:11 PM	Info	192.168.1.84	64:a7:dd:02:56:f8	factoryap	Rogue classification update initiated on Access Point fac
Apr 29, 2014 7:11 PM	Clear	192.168.1.84	64:a7:dd:02:56:f8	factoryap	Access Point is up and active
Apr 29, 2014 7:10 PM	Critical	192.168.1.84	64:a7:dd:02:56:f8	factoryap	Access Point not reachable
Apr 29, 2014 7:04 PM	Info	192.168.1.84	64:a7:dd:02:56:f8	factoryap	Rogue control update complete.

Figure 56. AP Details: Events

AP Details—Uptime

This page shows down time information for the AP. For each down interval, it shows when the AP went down and came back up, and how long the AP was down.



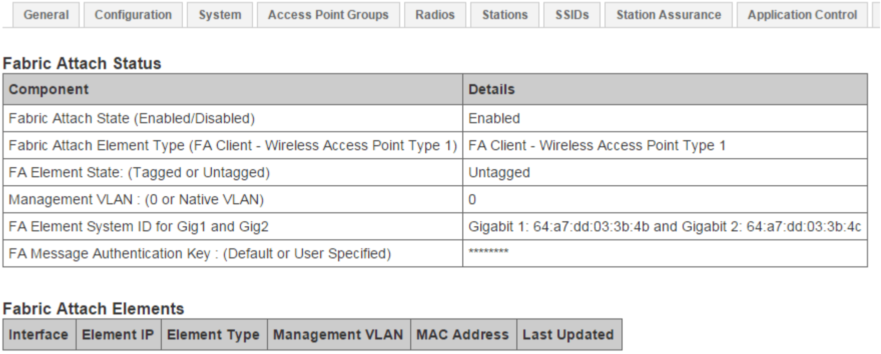
ess Point Details for: factoryap (192.168.1.84)

Showing: 1 to 1 of 1

ıtime	Uptime	Downtime Length	Downtime Reason
ıpr 29 19:10:38 PDT 2014	Tue Apr 29 19:11:38 PDT 2014	0 Days, 0 Hours, 1 Minutes, 0 Seconds	Reboot requested

Figure 57. AP Details: Uptime

AP Details—Fabric Attach (FA)



Fabric Attach Status

Component	Details
Fabric Attach State (Enabled/Disabled)	Enabled
Fabric Attach Element Type (FA Client - Wireless Access Point Type 1)	FA Client - Wireless Access Point Type 1
FA Element State: (Tagged or Untagged)	Untagged
Management VLAN : (0 or Native VLAN)	0
FA Element System ID for Gig1 and Gig2	Gigabit 1: 64:a7:dd:03:3b:4b and Gigabit 2: 64:a7:dd:03:3b:4c
FA Message Authentication Key : (Default or User Specified)	********

Fabric Attach Elements

Interface	Element IP	Element Type	Management VLAN	MAC Address	Last Updated

Figure 58. AP Details: Fabric Attach

This page shows Fabric Attach information for the AP, displayed as two tables: **Fabric Attach Status** and **Fabric Attach Elements**.

LLDP must be enabled on the AP in order to gather and display this information. For details, see **“Fabric Attach (FA) or LLDP Settings” on page 388**.

The **Fabric Attach Status** table shows the FA configuration for this WAP, including the management VLAN (this is the WAP's Native VLAN if one is defined, else 0), and whether tagging is in use.

The **Fabric Attach Elements** table shows other network elements that are known to this WAP and that play a role in Fabric attach. The types of elements included are: FA Server, FA Proxy, FA Server—No Auth, and FA Proxy—No Auth.

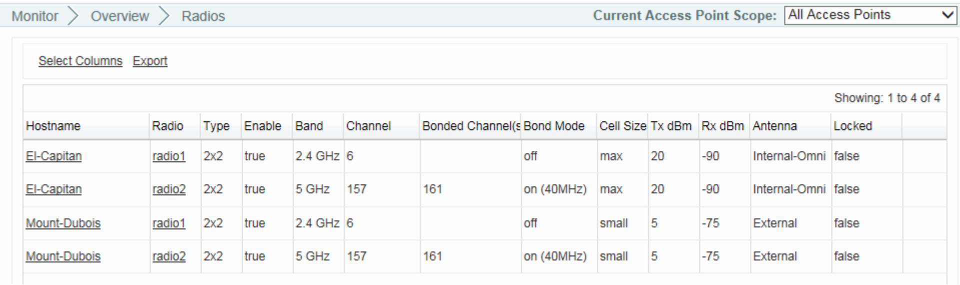
The WAP uses LLDP to perform FA discovery on the network on an ongoing basis. For each FA element, this table shows the IP and MAC Address, the device interface that is connected to the network (i.e., the port that was discovered), and the management VLAN.

Radios

The web client **Radios** page lists the radios on all of the APs being managed by WOS. This is a display-only page, but values may be exported. To change settings on radios, please see **"Configure Wireless Settings" on page 138**.

The following sections describe the radios page:

- **About Using the Radios Page**
- **The Radios List**



Monitor > Overview > Radios
Current Access Point Scope: All Access Points
Select Columns Export
Showing: 1 to 4 of 4

Hostname	Radio	Type	Enable	Band	Channel	Bonded Channel(s	Bond Mode	Cell Size	Tx dBm	Rx dBm	Antenna	Locked
El-Capitan	radio1	2x2	true	2.4 GHz	6		off	max	20	-90	Internal-Omni	false
El-Capitan	radio2	2x2	true	5 GHz	157	161	on (40MHz)	max	20	-90	Internal-Omni	false
Mount-Dubois	radio1	2x2	true	2.4 GHz	6		off	small	5	-75	External	false
Mount-Dubois	radio2	2x2	true	5 GHz	157	161	on (40MHz)	small	5	-75	External	false

Figure 59. Radios Page

About Using the Radios Page

A number of basic operations are available on the radios page to allow you to customize it for your own use:

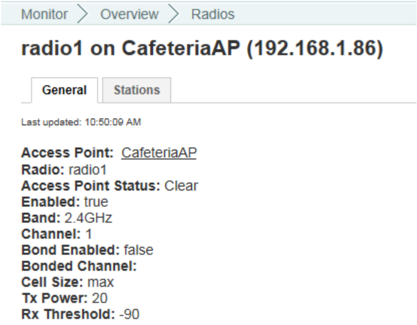
- **"Current Access Point Scope" on page 62**
- **"Select Columns" on page 62**
- **"Export" on page 63**
- **"Rearranging and Resizing Columns in a Table" on page 64**
- **"Sorting" on page 64**
- **"Searching" on page 65**

The Radios List

The Radios List (**Figure 59 on page 80**) shows all of the radios on APs that have been discovered by WOS. Only radios that belong to the **Current AP Scope** (selected on the upper right) are displayed.

For each radio, the following information is shown by default.

- The AP **Hostname**. Click on this link to show the **AP Details** page.
- The **Radio** name (e.g., radio4, abgn2, an3, etc.). Click on this link for the **Radio Details—General** page that shows the settings for this radio. Click the **Stations** tab to list the stations that are associated to this radio.



radio1 on CafeteriaAP (192.168.1.86)

Last updated: 10:50:09 AM

Access Point: CafeteriaAP
Radio: radio1
Access Point Status: Clear
Enabled: true
Band: 2.4GHz
Channel: 1
Bond Enabled: false
Bonded Channel:
Cell Size: max
Tx Power: 20
Rx Threshold: -90

Figure 60. Radio Details—General

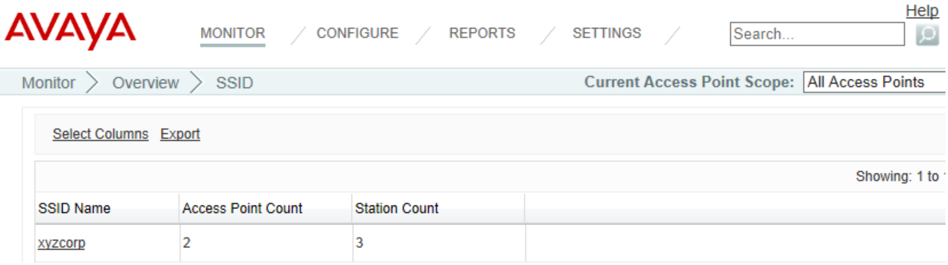
- Whether the radio is **Enabled**.
- The **Band** that the radio is using.
- The radio's current **Channel** number.
- For IEEE 802.11n or .11ac radios, the **Bonded Channel** for this radio.
- For IEEE 802.11n or .11ac radios, the **Bond Mode** that was set for this radio.
- The radio's current **Cell Size**.
- The radio's current **Tx dBm** (transmit power) setting.
- The radio's current **Rx dBm** (receive threshold) setting.
- The radio's current **Antenna** setting (internal or external).

SSID

The web client SSID page lists the SSIDs defined in your AP network. This is a display-only page, but values may be exported.

The following sections describe the SSID page:

- About Using the SSID Page
- The SSID List



SSID Name	Access Point Count	Station Count
xyzcorp	2	3

Figure 61. SSID Page

About Using the SSID Page

A number of basic operations are available on this page to allow you to customize it for your own use:

- "Current Access Point Scope" on page 62
- "Select Columns" on page 62
- "Export" on page 63
- "Rearranging and Resizing Columns in a Table" on page 64
- "Sorting" on page 64
- "Searching" on page 65

The SSID List

The SSID List (**Figure 61 on page 82**) shows all of the SSIDs defined on APs in your managed network. Only SSIDs defined on APs that belong to the **Current AP Scope** are displayed.

For each SSID, the following information is shown by default:

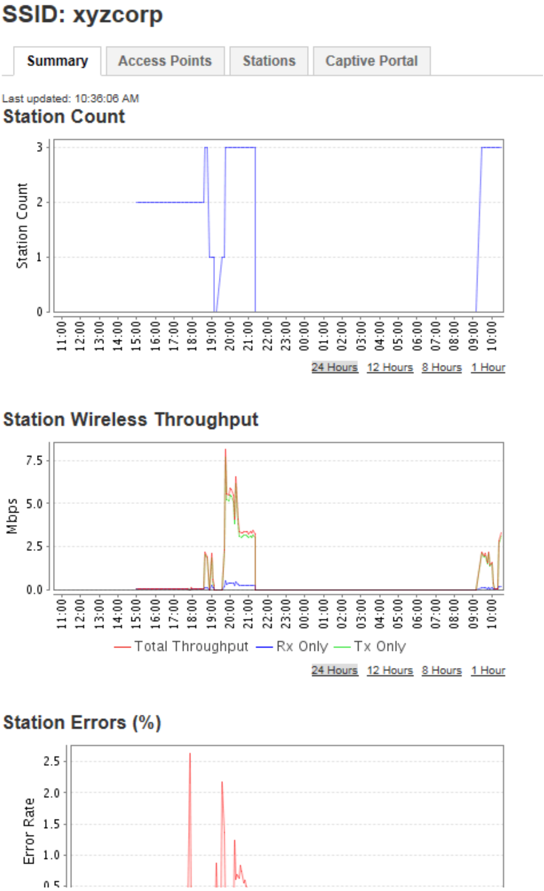
- The **SSID Name**.

  Click on this link for the **SSID Details—Summary** page that shows performance information including graphs for station count, wireless throughput and error percentage. (**Figure 62 on page 84**)

  Click the **SSID Details—APs** tab to list all of the APs on which this SSID is defined. You may click the link for any of the AP **Host Names** or **IP Addresses** to show **AP Details** for that AP.

  Click the **SSID Details—Stations** tab to list all of the stations which have associated to this SSID. You may click the link for any of the **Station MAC** Addresses to show station details for that AP.

  Click the **SSID Details—Captive Portal** tab to list all of the APs on which this SSID is defined that also have captive portals defined. Settings are listed, to make it easy to compare the portal configuration on these APs. See **“SSID Management—Captive Portal” on page 462** to create a captive portal on an AP’s SSID.
- The AP **Count** shows the number of APs on which this SSID is defined.
- The **Station Count** shows the number of stations associated to this SSID.



SSID: xyzcorp

Last updated: 10:36:06 AM

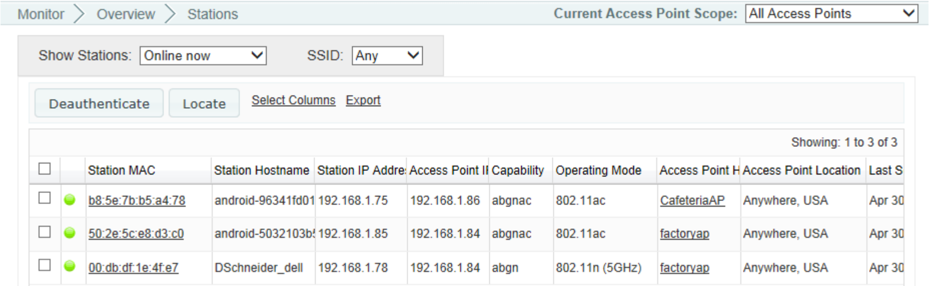
Figure 62. SSID Details—Summary

Stations

The web client Stations page lists the stations that are associated to all APs within your managed network. This is a display-only page, but values may be exported.

The following sections describe the Stations page:

- **About Using the Stations Page**
- **The Stations List**



Monitor > Overview > Stations   Current Access Point Scope: All Access Points

Show Stations: Online now   SSID: Any

Showing: 1 to 3 of 3

□		Station MAC	Station Hostname	Station IP Addre	Access Point II	Capability	Operating Mode	Access Point H	Access Point Location	Last S
□	●	b8:5e:7b:b5:a4:78	android-96341fd01	192.168.1.75	192.168.1.86	abgnac	802.11ac	CafeteriaAP	Anywhere, USA	Apr 30
□	●	50:2e:5c:e8:d3:c0	android-5032103b!	192.168.1.85	192.168.1.84	abgnac	802.11ac	factoryap	Anywhere, USA	Apr 30
□	●	00:db:df:1e:4f:e7	DSchneider_dell	192.168.1.78	192.168.1.84	abgn	802.11n (5GHz)	factoryap	Anywhere, USA	Apr 30

Figure 63. Stations Page

About Using the Stations Page

A number of basic operations are available on the Stations page to allow you to customize it for your own use:

- **"Current Access Point Scope" on page 62**
- **"Select Columns" on page 62**
- **"Export" on page 63**
- **"Rearranging and Resizing Columns in a Table" on page 64**
- **"Sorting" on page 64**
- **"Searching" on page 65**

The Stations List

The Stations List (**Figure 63 on page 85**) shows all of the stations associated to APs that have been discovered by WOS. Only APs that belong to the **Current AP Scope** are displayed.

This list shows information about each station associated to the wireless network.

You may use the **Show Stations** option to select whether to show the stations that are **Online now** (i.e., currently connected to APs), or to show historical information as well by including all stations that are currently connected or have been connected **Within 24 hours**, **Within the last week**, or **Within the last month**.

There are two actions offered for stations:

- Click the **Deauthenticate** button to send a "deauth" signal to the selected APs. This will terminate the current connections between each selected station and the AP to which it is associated.
- Select one station and click the **Locate** button to have WOS find the station's physical location and display it on a map. In order for this command to work, the selected station must be detected by APs that have been placed accurately on maps. See **"Adding APs to Maps" on page 231**.

For each station, the following information is shown by default:

- The **Station MAC** address.

  Click on this link for the **Station Details—General** page that shows information about the type of connection and performance information including graphs for session throughput and error percentage. (**Figure 64 on page 88**)

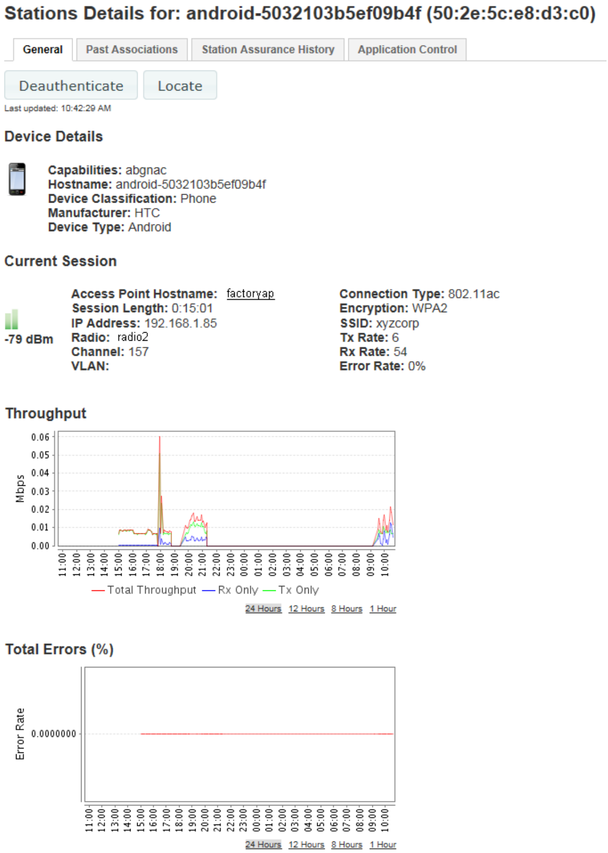
  Click the **Station Details—Past Associations** tab to show Association and Disassociation timestamps for this station, along with the SSID for the connection. If the station is having difficulty staying connected to the AP or SSID, this provides valuable details.

  Click the **Station Details—Assurance History** tab to show connection problems (if any) experienced by this station. The information shown is the same as described in **"Station Assurance" on page 96**.

Click the **Station Details—Application Control** tab to show application usage by this station. The information shown is the same as described in **"Application Control—Overview" on page 104**.

> *Application Control data is only available if the AP license includes* ***Application Control****. See* **"About Licensing and Upgrades" on page 182***. In order for an AP to produce Application Control data, you must have enabled the* ***Application Control*** *option in the* ***Configure*** *menu on the APs* ***Toolbar****. See* **"The Access Points Toolbar" on page 67***.*

- The **Station MAC Address** of the station.
- The **Station Hostname**.
- The **Station IP Address** of the station.
- The wireless **Capability** of the station: **ac** for 802.11ac, **n** for 802.11n, **a** for 802.11a, **b** for 802.11b, and **g** for 802.11g.
- The **Operating Mode** of the connection: 802.11ac (5 GHz or 2.4 GHz), 802.11n (5 GHz or 2.4 GHz), 802.11a, 802.11b, or 802.11g.
- The AP **Hostname** and AP **Location** of the AP to which the station is associated. Click the hostname to go to **AP Details**.
- The **Last Seen Date**—The last time the station was associated to the AP.
- The **User Name** under which the station was authenticated.
- The **Device Type** (for example, iPad, Android, Windows)
- The **Device Class** (Notebook, phone, tablet, etc.)
- The **Assoc Time**—How long (in days:hours:minutes) the station has been associated to the AP.
- The current **RSSI** (signal strength) of the connection as measured by the radio.



Stations Details for: android-5032103b5ef09b4f (50:2e:5c:e8:d3:c0)

Last updated: 10:42:29 AM

Device Details

Capabilities: abgnac
Hostname: android-5032103b5ef09b4f
Device Classification: Phone
Manufacturer: HTC
Device Type: Android

Current Session

-79 dBm

Access Point Hostname: factoryap
Session Length: 0:15:01
IP Address: 192.168.1.85
Radio: radio2
Channel: 157
VLAN:

Connection Type: 802.11ac
Encryption: WPA2
SSID: xyzcorp
Tx Rate: 6
Rx Rate: 54
Error Rate: 0%

Throughput

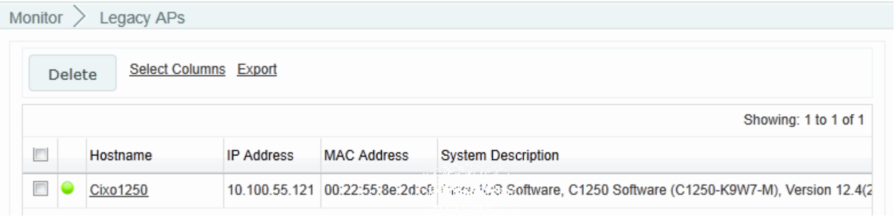
Total Errors (%)

Figure 64. Station Details—General

Legacy APs

The Legacy APs page lists the non-Avaya access points known to WOS as part of your Wi-Fi network, and shows whether the devices are up or down. To discover these devices, make sure to add their SNMP community strings to WOS. See **“Discovery” on page 159** for more information. (Note that WOS discovers legacy APs that use the standard MIB: *IEEE802dot11-MIB*. It will not discover other manufacturers’ controller-based APs.)

This is a display-only page, but values may be exported.



Monitor > Legacy APs

Delete   Select Columns   Export

Showing: 1 to 1 of 1

□		Hostname	IP Address	MAC Address	System Description
□	●	Cixo1250	10.100.55.121	00:22:55:8e:2d:c8	[illegible] Software, C1250 Software (C1250-K9W7-M), Version 12.4(2

Figure 65. Legacy APs Page

You may customize the columns shown in this list—see **“Select Columns” on page 62**.

Rogues

The web client Rogues page lists the potential rogue access points detected by APs in the network, and types of encryption in use. When you configure an individual radio on the Avaya wireless AP to be in **monitor** mode, it can detect APs in its vicinity.

In order for APs to detect rogue APs, the APs must have one radio set to ***monitor*** *as described in* **"Radio Settings" on page 488**. *Intrusion Detection Mode must be set to Standard, as described in* **"Intrusion Detection" on page 525**. *You may set a minimum signal strength threshold for considering an AP to be a rogue, in order to keep WOS from detecting too many irrelevant APs—see* **"Security—Rogue Rules" on page 176**.

If you set blocking on for one of these rogue APs, the AP's monitor radio sends out signals that will make it difficult for stations to associate to the rogue. Devices start out as **Unclassified** when first detected, and you may then *classify* them as **Blocked**, **Unknown**, **Known**, or **Approved**.

We suggest that you use the following classifications:

- Use **Approved** for devices in the operational network.
- Use **Known** for other devices not in the operational network but whose operation is known about, e.g., a neighbor or adjunct network.
- Use **Blocked** to counter rogues that you believe may be malicious.
- Use **Unknown** for other rogue or unapproved devices.

When you classify a device as known, blocked, etc., that information is sent to every AP managed by WOS as soon as possible. Also, WOS sends its latest device classifications to all managed APs daily at 3 AM.

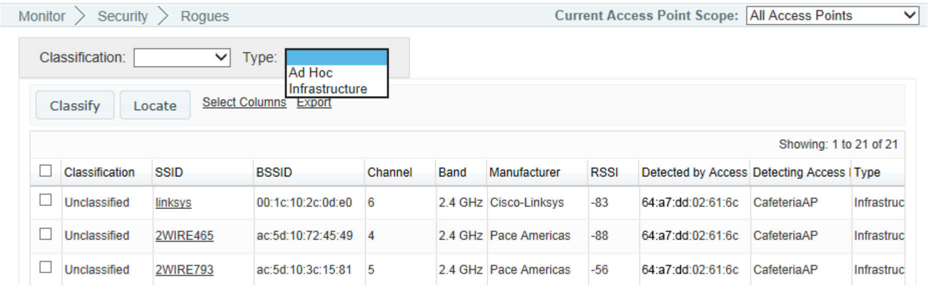
APs have an Auto Block feature, described in **"About Blocking Rogue APs" on page 528.**

The rogues list identifies the APs that detected the intruding APs. Values may be exported.

WOS adds rogues to this list as described in **“Populating the WOS Rogues and Rogue Rules Windows” on page 179**.

The following sections describe the Rogues page:

- **About Using the Rogues Page**
- **The Rogues List**



Monitor > Security > Rogues

Current Access Point Scope: All Access Points

Classification: Type:

Showing: 1 to 21 of 21

□	Classification	SSID	BSSID	Channel	Band	Manufacturer	RSSI	Detected by Access	Detecting Access	Type
□	Unclassified	linksys	00:1c:10:2c:0d:e0	6	2.4 GHz	Cisco-Linksys	-83	64:a7:dd:02:61:6c	CafeteriaAP	Infrastruc
□	Unclassified	2WIRE465	ac:5d:10:72:45:49	4	2.4 GHz	Pace Americas	-88	64:a7:dd:02:61:6c	CafeteriaAP	Infrastruc
□	Unclassified	2WIRE793	ac:5d:10:3c:15:81	5	2.4 GHz	Pace Americas	-56	64:a7:dd:02:61:6c	CafeteriaAP	Infrastruc

Figure 66. Rogues Page

About Using the Rogues Page

A number of basic operations are available on the Rogues page to allow you to customize it for your own use:

- **“Current Access Point Scope” on page 62**
- **“Select Columns” on page 62**
- **“Export” on page 63**
- **“Rearranging and Resizing Columns in a Table” on page 64**
- **“Sorting” on page 64**
- **“Searching” on page 65**

The Rogues List

The Rogues List (**Figure 66 on page 91**) shows all of the rogues that have been detected by WOS. You may **Classify** entries by selecting them and using the provided button. To search for a particular rogue, see **“Searching” on page 65**. You may use the **Classification** drop-down list to select only rogues of one class to display. You may use the **Type** drop-down list to display only **Ad Hoc** rogues, or only those that are part of network **Infrastructure**. An ad hoc wireless network is typically a network formed between two stations that are communicating with each other directly without going through a normal AP.

You may use the **Locate** button to display the location of one selected rogue on a map. There are some prerequisites for this feature to operate properly—the rogue must be detected by more than one AP, and a number of detecting APs must be members of the same map. See **“Locating Devices” on page 236** for details.

This list shows information about each rogue and the AP that detected it. For each rogue, the following information is shown by default:

- The rogue’s **Classification (Unclassified, Approved, Known, Blocked,** or **Unknown)**.
  - **Approved:** These are rogues that you have designated as Approved.
  - **Known:** These are rogues that you have designated as Known. All Avaya WAPs are automatically known. Their MAC addresses include any of the following: 64:a7:dd:*, b0-ad-aa:*, cc:f9:54:*, f8-15-47:*, 00:1b:4f:*, 2c:f4:c5:*, 5c:e2:86:*, 58:16:26:*, 70:52:c5:*, or 70:38:ee:*.
  - **Unclassified**: When a device is initially detected, it is unclassified, which simply means that no one has classified it yet.
  - **Unknown/Rogue:** These are rogues that you have designated as Unknown.
  - **Blocked**: These are rogues that you have designated as Blocked. If you classify a rogue AP as **blocked**, then the AP will take measures to prevent stations from staying associated to the rogue. When the monitor radio is scanning, any time it hears a beacon from a blocked rogue the monitor sends out a broadcast “deauth” signal using the rogue's BSSID and source address. This has the effect of disconnecting all of a rogue AP’s clients approximately every 5 to 10 seconds, which is enough to make the rogue frustratingly unusable.

  To set or modify the classification of rogues, select the desired entries using the checkbox to the left of the entries and click the **Classify** button.

In the dialog box, select the desired **Classification** value from the drop-down list and click **OK**. This value will be set for all selected rogues.

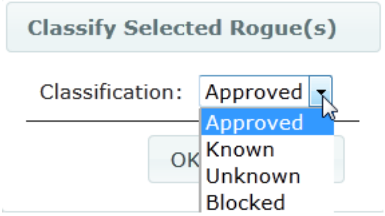


Figure 67. Classifying Rogues

To set up rules to automatically classify groups of rogues (for example, by SSID, MAC address, or manufacturer), see **“Security—Rogue Rules” on page 176**.

- The rogue’s **SSID**. Click the SSID to display the **Rogue Details—General** tab, showing additional details about this device. Click the **Detecting APs** tab for a list of APs that have detected this device. Click the **Channel/ SSID History** tab for a list of the channels and SSIDs that have been used by this device.
- The rogue’s **BSSID** (MAC address).
- The **Channel** being used for the connection.
- The **Band** (5 GHz or 2.4 GHz) being used for the connection.
- The **Manufacturer** of the rogue device.
- The current **RSSI** (signal strength) of the rogue’s signal as measured by the AP that detected it.
- The MAC Address of the AP that detected the rogue.
- The host name of the AP that detected the rogue. If the same rogue device is detected by a number of APs, it will only be listed once in this table.
- The **Type** of the rogue's wireless network—Ad Hoc or Infrastructure.

IDS Events

This page displays the Intrusion Detection System (IDS) Event log, listing any attacks detected on your network for your **Current Access Point Scope**. For descriptions of the types of attacks detected, as well as the settings to fine-tune IDS on the AP, please *refer to Avaya WLAN AP 9100 Series (NN47252-102)*.

Note that IDS Event polling is not enabled by default. If you wish to use the IDS Event log, you must enable the optional polling for IDS Events as described in **“Polling Settings” on page 589**.

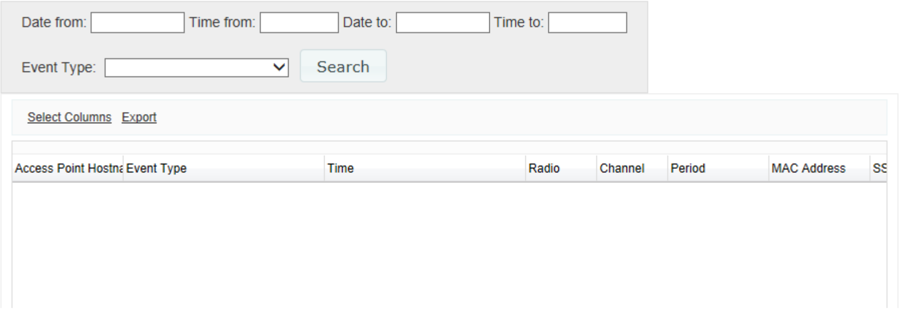


Figure 68. IDS Events

The IDS Events page has a number of search fields that allow you to filter the log messages to be displayed. This is a very useful feature, since the list may contain a large number of messages. To search for the desired messages, use any or all of the following fields, then click **Search**:

- Specify a time period (optional)—enter the **Date from/Time from** and/or **Date to/Time to** fields. The Dates are entered by clicking in the field and selecting the desired date from the popup calendar, or by typing the date in **mm/dd/yyyy** format. Times are specified by clicking in the field and using the drag bars to select the **Hour** and **Minute**.
- Enter **Event Type** (optional)—WOS will search for entries of this type.

If you wish to see information for a particular AP, click its **Hostname** and select the tab for the **AP Details—IDS** page.

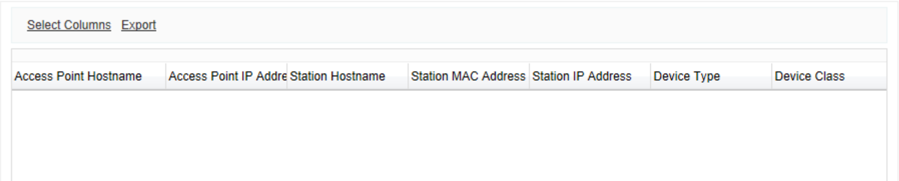
The following fields are displayed on the IDS Events page by default:

- **AP Hostname** of the AP on which the event occurred.
- **Event Type**—the type of attack, as described in **“Intrusion Detection” on page 525**.
- **Time**—the time that the event occurred.
- **Radio**—the affected radio.
- **Channel**—the affected channel.
- **Period**—the length of the window used to determine whether the count of this type of event exceeded the threshold.
- **MAC Address**—the MAC address of the attacker.
- **SSID**—the SSID that was attacked.

Station Assurance

Station assurance monitors the connection quality that users are experiencing on the wireless network. This window shows client stations for your **Current Access Point Scope** that have had connectivity issues, such as excessive packet retry or packet error rates, or stations that are unable to stay associated to the AP. When the AP detects that a station has reached the threshold value for one or more of the problems that it checks, it adds the station to this page. In addition, an event is triggered and a Syslog message is logged. If you wish to see information for a particular AP, click its **Hostname** and select the tab for the **AP Details—Station Assurance** page. Similarly, if you wish to see information for a particular station, click its **Station MAC Address** and select the tab for **Station Assurance History**.

Note that Station Assurance event polling is not enabled by default. If you wish to use the Station Assurance event log, you must enable the optional polling for it as described in **“Polling Settings” on page 589**.



Access Point Hostname	Access Point IP Addre	Station Hostname	Station MAC Address	Station IP Address	Device Type	Device Class

Figure 69. Station Assurance History

For each station, the following information is shown by default:

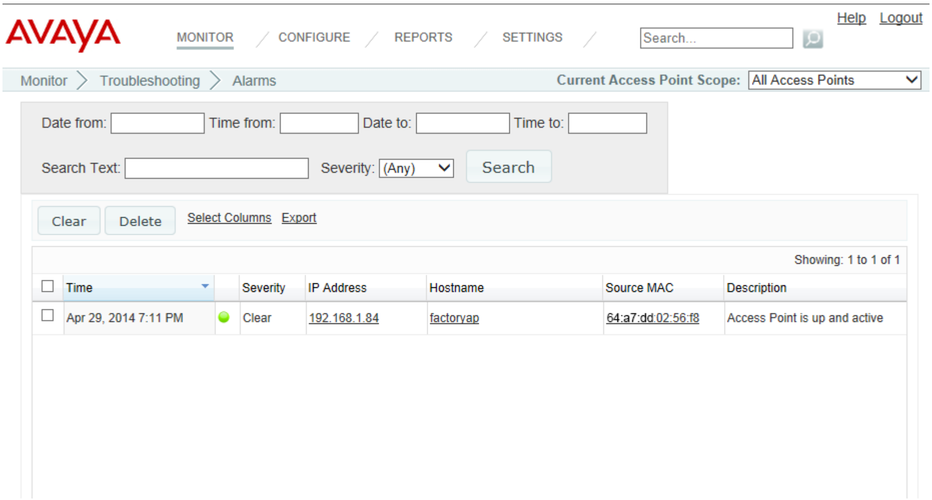
- The AP **Hostname** of the AP to which the station is associated.
- The AP **IP Address**.
- The **Station Hostname**.
- The **Station MAC** address.
- The **IP Address** of the station.
- The **Device Type** (for example, iPad, Android, Windows)
- The **Device Class** (Notebook, phone, tablet, etc.)
- The **Alarm Type**—the connection criterion that was not within acceptable thresholds.

- The **Start Time** of the session (i.e., when the client associated to the AP).
- The **End Time** of the session. This will be blank if the session is still active.

Alarms

The web client Alarms page lists the alarms received by WOS for your **Current Access Point Scope**. All alarm levels are displayed—Critical, Major, Minor, Warning, and Clear. Values may be exported.

WOS allows you to define your own custom alarms. See **“Alarm Definitions” on page 154**. You may also send email notifications when alarms of a particular severity occur, as described in **“Notification Settings” on page 157**.



Showing: 1 to 1 of 1

□	Time		Severity	IP Address	Hostname	Source MAC	Description
□	Apr 29, 2014 7:11 PM	●	Clear	192.168.1.84	factoryap	64:a7:dd:02:56:f8	Access Point is up and active

Figure 70. Alarms Page

The following sections describe the Alarms page:

- **About Using the Alarms Page**
- **The Alarms List**

About Using the Alarms Page

A number of basic operations are available on the Alarms page to allow you to customize it for your own use:

- **"Current Access Point Scope" on page 62**
- **"Select Columns" on page 62**
- **"Export" on page 63**
- **"Rearranging and Resizing Columns in a Table" on page 64**
- **"Sorting" on page 64**

The Alarms page has a number of tailored search fields that allow you to filter the items to be displayed. This is a very useful feature, since the list may contain a large number of alarms. To search for the desired messages, use any or all of the following fields, then click **Search**:

- Specify a time period (optional)—enter the **Date from/Time from** and/or **Date to/Time to** fields. The Dates are entered by clicking in the field and selecting the desired date from the popup calendar, or by typing the date in **mm/dd/yyyy** format. Times are specified by clicking in the field and using the drag bars to select the **Hour** and **Minute**.
- Enter **Search Text** (optional)—WOS will search for entries that contain this text in any position in any field.
- Select the desired **Severity**. If you select a particular severity level, *only* messages at that level will be displayed (rather than displaying messages at that level and above). The default value is **Any**, which shows all alarms.

The Alarms List

The Alarms List (**Figure 70**) shows the alarms that have been received by WOS. Only alarms on APs that belong to the **Current AP Scope** are displayed. Only the current (most recent) alarm with a given description for each device will be shown in this list.

You may **Clear** or **Delete** alarms by selecting the check box to the left of each desired entry and clicking the appropriate button on the upper left. Use **Clear** to change the severity of selected alarms to **Clear**, without removing the alarm from the list. For example, you can use this to indicate that an alarm condition has been remedied while still keeping a record of the alarm. Use **Delete** to remove the selected alarms from the database (and consequently, from the list of alarms).

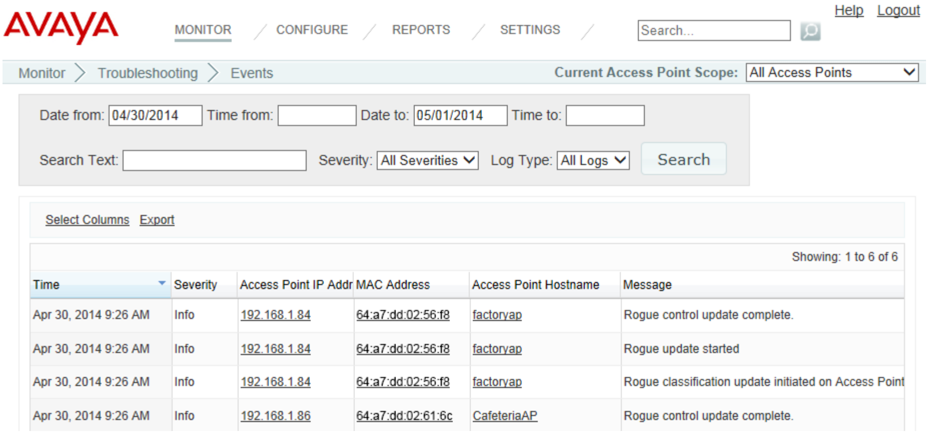
This list shows information about each alarm and the AP that generated it. For each alarm, the following information is shown by default:

- The alarm's **Severity (Critical, Major, Minor, Warning**, or **Clear)**, preceded by a color indicator of the severity.
  - **Red—Critical**: A critical failure has occurred within the network and the problem must be resolved immediately.
  - **Orange—Major**: A major problem exists. If this problem is ignored there is a likelihood that the problem will escalate to a critical condition.
  - **Gold—Minor**: A minor problem exists and should be investigated.
  - **Yellow—Warning**: This informs you that some action needs to be taken to avoid an alarm (an alarm has not yet been invoked, but probably will be if the warning is ignored).
  - **Green—Clear**: This state is reported when any problem that previously caused a critical (red) alarm has been resolved.
- The **Time** and date of the alarm.
- The **IP Address** of the AP that generated the alarm.
- The **Hostname** of the AP that generated the alarm.
- The **Source MAC** address of the AP that generated the alarm.
- A text **Description** of the alarm.

Events

The web client Events page lists the log and syslog messages received by WOS for your **Current Access Point Scope**. Syslog is a protocol that allows a machine to send event notification messages across IP networks to event message collectors, known as syslog servers. Syslog messages are based on the User Datagram Protocol (UDP). They are received on UDP port 514 and cannot exceed 1,024 bytes in length (they have no minimum length). For more information about configuring APs to send syslog messages to WOS, refer to **"System Log" on page 401**.

WOS reconciles syslog activity on all wireless APs in the network. Syslog reporting is time-stamped, and to ensure that all syslog time-stamping is maintained by a universal clock for all APs, an NTP (Network Time Protocol) server should be used for the WOS server and for all managed APs. Without an NTP server assigned (no universal clock), each AP will use its own internal clock and stamp syslog event times accordingly, which may result in discrepancies. For more information about using an NTP server, refer to **"Time Settings (NTP)" on page 396**.



Current Access Point Scope: All Access Points

Date from: 04/30/2014 Time from: Date to: 05/01/2014 Time to:

Search Text: Severity: All Severities Log Type: All Logs

Showing: 1 to 6 of 6

Time	Severity	Access Point IP Addr	MAC Address	Access Point Hostname	Message
Apr 30, 2014 9:26 AM	Info	192.168.1.84	64:a7:dd:02:56:f8	factoryap	Rogue control update complete.
Apr 30, 2014 9:26 AM	Info	192.168.1.84	64:a7:dd:02:56:f8	factoryap	Rogue update started
Apr 30, 2014 9:26 AM	Info	192.168.1.84	64:a7:dd:02:56:f8	factoryap	Rogue classification update initiated on Access Point
Apr 30, 2014 9:26 AM	Info	192.168.1.86	64:a7:dd:02:61:6c	CafeteriaAP	Rogue control update complete.

Figure 71. Events Page

Only events on APs that belong to the **Current AP Scope** are displayed. All severity levels at or above the informational level are shown by default. Values may be exported. A set of search fields above the list allow you to select the messages to be displayed. If you wish to see information for a particular AP, click its **Hostname** and select the tab for the **AP Details—Events** page.

The Events page has a special search feature for finding particular log messages. This is described in **“About Using the Events Page” on page 102**.

The following sections describe the Events page:

- **About Using the Events Page**
- **The Events List**

About Using the Events Page

A number of basic operations are available on the Events page to allow you to customize it for your own use:

- **“Current Access Point Scope” on page 62**
- **“Select Columns” on page 62**
- **“Export” on page 63**
- **“Rearranging and Resizing Columns in a Table” on page 64**
- **“Sorting” on page 64**

The Events page has a number of tailored search fields that allow you to filter the log messages to be displayed. This is a very useful feature, since the list may contain a large number of messages. To search for the desired messages, use any or all of the following fields, then click **Search**:

- Specify a time period (optional)—enter the **Date from/Time from** and/or **Date to/Time to** fields. The Dates are entered by clicking in the field and selecting the desired date from the popup calendar, or by typing the date in **mm/dd/yyyy** format. Times are specified by clicking in the field and using the drag bars to select the **Hour** and **Minute**.
- Enter **Search Text** (optional)—WOS will search for entries that contain this text in any position in any field.
- Select the desired **Severity**. If you select a particular severity level, *only* messages at that level will be displayed (rather than displaying messages

at that level and above). The default value is **All Severities**, which shows all messages at the informational level and above.

- Select the **Log Type**. The default is All Logs, which displays all WOS log files including syslog messages.

The Events List

The Events List (**Figure 70**) shows the events that have been received by WOS. Only events on APs that belong to the **Current AP Scope** are displayed. Events that trigger alarms are also shown in the **Alarms** window. This list shows information about each event and the AP that generated it. For each event, the following information is shown by default:

- The **Time** and date of the event.
- The event's **Severity**. All syslog messages are categorized by their levels of severity, which include:
  - Emergency
  - Alerts
  - Critical
  - Error
  - Warning
  - Notice
  - Information (default)
  - Debug (not to be used for routine syslog monitoring)
- The AP **IP Address** of the AP that generated the event.
- The **MAC Address** of the AP that generated the event.
- The AP **Hostname** of the AP that generated the event.
- The **Message**—a text description of the event.

Application Control—Overview

This page analyzes application usage over your entire Avaya wireless network, or for your **Current Access Point Scope**. If you wish to see information for just one particular AP, please see **"AP Details—Application Control" on page 74.**

About Application Control

APs use Deep Packet Inspection (DPI) to determine what applications are being used and by whom, and how much bandwidth they are consuming. These applications are rated by their degree of risk and productivity. Filters may then be put in place to implement per-application policies that keep network usage focused on productive uses.

Application Control can track application usage over time to monitor trends. Many hundreds of applications are recognized and grouped into a number of categories. The distributed architecture of Avaya APs allows Application Control to scale naturally as you grow the network.

For more information about Application Control and using Filters to prioritize mission-critical application and reduce/eliminate traffic from undesirable applications, see the *refer to Avaya WLAN AP 9100 Series (NN47252-102).*

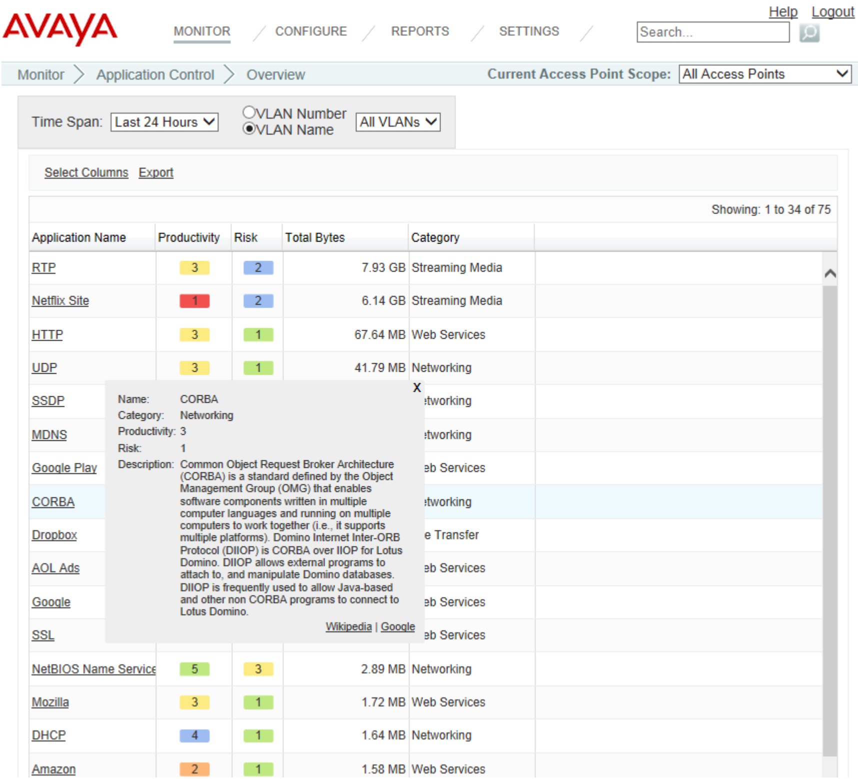
About Risk and Productivity

Application Control ranks applications in terms of their levels of risk and productivity. **Productivity** indicates how appropriate an application is for business purposes. The higher the rating number, the more business-oriented an application is. **Risk** indicates how likely an application is to pose a threat to the security of your network. The higher the rating number, the more risky an application is.

This feature is only available on APs whose licenses include ***Application Control****. See* **"About Licensing and Upgrades" on page 182***.*

In order for an AP to produce Application Control data, you must enable the ***Application Control*** *option in the* ***Configure*** *menu on the APs* ***Toolbar****. See* **"The Access Points Toolbar" on page 67***.*

The Application Control—Overview Page



AVAYA
MONITOR / CONFIGURE / REPORTS / SETTINGS /
Help Logout
Search...
Monitor > Application Control > Overview

Current Access Point Scope: All Access Points

Time Span: Last 24 Hours

○ VLAN Number
● VLAN Name

All VLANs

Showing: 1 to 34 of 75

Application Name	Productivity	Risk	Total Bytes	Category
RTP	3	2	7.93 GB	Streaming Media
Netflix Site	1	2	6.14 GB	Streaming Media
HTTP	3	1	67.64 MB	Web Services
UDP	3	1	41.79 MB	Networking
SSDP				etworking
MDNS				etworking
Google Play				eb Services
CORBA				etworking
Dropbox				e Transfer
AOL Ads				eb Services
Google				eb Services
SSL				eb Services
NetBIOS Name Service	5	3	2.89 MB	Networking
Mozilla	3	1	1.72 MB	Web Services
DHCP	4	1	1.64 MB	Networking
Amazon	2	1	1.58 MB	Web Services

X

Name: CORBA
Category: Networking
Productivity: 3
Risk: 1
Description: Common Object Request Broker Architecture (CORBA) is a standard defined by the Object Management Group (OMG) that enables software components written in multiple computer languages and running on multiple computers to work together (i.e., it supports multiple platforms). Domino Internet Inter-ORB Protocol (DIIOP) is CORBA over IIOP for Lotus Domino. DIIOP allows external programs to attach to, and manipulate Domino databases. DIIOP is frequently used to allow Java-based and other non CORBA programs to connect to Lotus Domino.

Wikipedia | Google

Figure 72. Application Control—Overview

This table provides detailed information about how your wireless bandwidth is being used on the selected AP Group, by application. The category of each application is also shown. You may select which **Time Span** to show, and which **VLAN Name** or **Number** to show (or **All VLANs**).

In addition to showing traffic statistics, there are two unique and highly useful columns. **Risk** estimates the likelihood of an application causing problems for your business, rated from 1 (low risk, e.g., Google) to 5 (high risk, e.g., BitTorrent). Risky applications (rated at 4 or 5) are flagged for your attention by highlighting the entry in red. **Productivity** estimates the value of an activity to your business, from 1 (unproductive, e.g., Y8 gaming site) to 5 (productive, e.g., Scopia).

You may click the heading of any column to sort based on that column. Click again to sort in the reverse order.

Each **Application Name** in the list is a link. You may hover over it to display a tool tip with more information about the application, including a description of what it does. You may click the link to display a table listing the AP**s** on which this application has been used, and the amount of traffic that it has generated. You may specify the desired **Time Span** and/or **VLANs** to show. If you wish to drill down further, you may show the **Stations** on which this application has been used instead. This information is available on the Station Details—Application Control page. See **"The Stations List" on page 86**.

When you find risky or unproductive applications taking up bandwidth on the network, you can create filters to control them. See **"Filter Lists" on page 539**.

Configuring the Network

About the Configure Pages

Note that smaller APs that use the AOSLite system software, such as the WAP9112, have many fewer settings than more powerful APs. Some of the configuration pages will not list AOSLite devices, or are not available for those devices.

These pages perform specific wireless network configuration actions. Click the **Configure** link at the top of the window to see the list of configure pages. The **Configure** link always opens to the Access Points page, which is the same as the Monitor > Access Points page. You must be logged in to WOS as an administrator with read-write privileges to see the **Configure** link.

Configure pages include the following. Click a link below for more information.

Access Point Configuration

- Access Points (Configure)
- Profiles
- AP Groups
- Edit Config Templates
- Load Config Template
- Deploy Config Template
- Custom Field Values
- Import Access Point Custom Fields

Wireless Configuration

- Configure Wireless Settings
- Export Wireless Settings
- Import Wireless Settings

Network Configuration

- Configure Network Settings

- Export Network Settings
- Import Network Settings

Alarms

- Alarm Definitions
- Notification Settings

Discovery

- Add Devices
- SNMPv2 Settings
- SNMPv3 Users
- SSH Users
- View Networks

Security

- Security—Rogue Rules
- SSID Spoofing Auto Block

Access Point Licenses

- Deployed Licenses
- Export Licenses
- Import Licenses
- Edit Licenses
- Pending Licenses

Access Point Upgrade

- Perform or Schedule Upgrade
- Scheduled Upgrades

Access Point Configuration

This section includes the following pages:

- **Access Points (Configure)**
- **The Configure APs Toolbar**
- **Profiles**
- **AP Groups**
- **Edit Config Templates**
- **Load Config Template**
- **Deploy Config Template**
- **Custom Field Values**
- **Import Access Point Custom Fields**

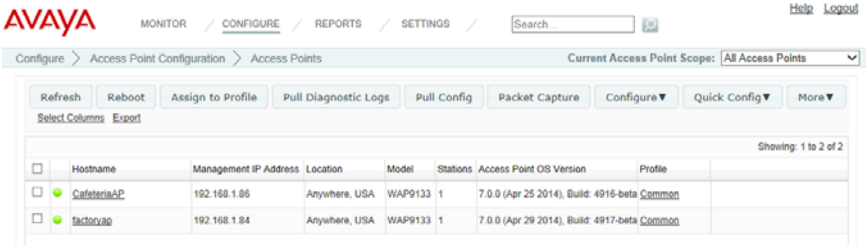
Access Points (Configure)

This page lists the APs in the WOS database and offers a number of operations on the selected APs. To display this page, click the AP**s** link in the AP **Configuration** section under **Configure** at the top of the page. This page is identical to the Monitor—APs page (see **"Access Points" on page 61**).

The Access Points List shows APs that have been discovered by WOS. When you click on an AP's **Hostname**, you can access a variety of AP Details pages. These pages offer some very powerful features, including the **Configuration** page, which allows you configure most settings on that AP. See **"AP Details" on page 68** and **"Configuring a Wireless AP" on page 369** for more information.

The Configure APs Toolbar

The Configure APs toolbar offers several functions for AP management, including gathering diagnostic information, rebooting selected APs, and capturing packets. The diagnostic logs and packet capture functions are also available on the **The Access Points Toolbar** on the Monitor—APs page.



□		Hostname	Management IP Address	Location	Model	Stations	Access Point OS Version	Profile
□	●	CafeteriaAP	192.168.1.86	Anywhere, USA	WAP9133	1	7.0.0 (Apr 25 2014), Build: 4916-beta	Common
□	●	factoryap	192.168.1.84	Anywhere, USA	WAP9133	1	7.0.0 (Apr 29 2014), Build: 4917-beta	Common

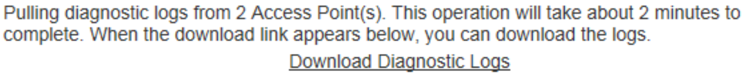
Figure 73. The Configure APs Toolbar

Note that smaller APs that use the AOSLite system software, such as the WAP9112, have fewer options and settings than more powerful APs. Options and settings that are not available on a particular AP are not displayed, or will be grayed out.

Select one or more APs in the list by clicking their checkboxes in the first column. You may click the checkbox in the header row to select all APs, or click again to deselect all. The following operations are available:

- **Refresh**—this option refreshes discovery on the selected APs.
- **Reboot**—this option reboots the selected APs. You will be asked to confirm the operation.
- **Assign to Profile**—this option assigns the selected APs to the profile that you specify. Since an AP may not be a member of more than one profile, the selected APs will be removed from any other profiles to which they belong. APs may also be assigned to profiles using the **Add** button on **The Profiles Toolbar**.
- **Pull Diagnostic Logs**—this option initiates a task that instructs the selected APs to create a diagnostic log file. When the diagnostic log is

complete, a link will appear. Click it to download the requested diagnostic results as a zip file. (**Figure 74**)



Pulling diagnostic logs from 2 Access Point(s). This operation will take about 2 minutes to complete. When the download link appears below, you can download the logs.

Download Diagnostic Logs

Figure 74. Pull Diagnostic Logs

- **Pull Config**—this option pulls configuration files from the selected APs, containing each AP's current configuration. When the files are available, a link will appear. Click it to download the requested files as a zip file.
- **Packet Capture**—this option initiates packet capture on one or more selected APs. See **"About Packet Capture" on page 115**.
- **Configure—**select an option from this drop-down list to perform configuration on the selected APs. The following options are available:
  - **Network Settings** on the selected APs. See **"Import Wireless Settings" on page 140**.
  - **Radio Settings** on the selected APs. See **"Configure Wireless Settings" on page 138**.
  - **Optimize Channels**—this option starts auto channel, which computes the best channel assignments for the selected APs in the local RF environment. You will be asked to confirm the operation. Note that the best way to run auto channel is from a map. See the **Auto Configure Channels** option (in the **Configure** drop-down menu) in **"Managing APs Within Maps" on page 241**. See also, **"RF Spectrum Management (Auto Channel Configuration)" on page 522**.

*Note that Auto Channel normally assigns individual channels. However, if you select **Auto bond 5GHz channels** on the **Global Settings .11n** page, and have 40MHz channels set up prior to running Auto Channel, those bonds will be preserved. 80MHz bonds will not be preserved.*

  - **Optimize Band**s—this option starts automatic band configuration, the recommended method for assigning bands to the abgn radios. It runs only on command, assigning radios to the 2.4GHz or 5GHz band. The AP uses its radios to listen for other APs on the same channel, and it assigns bands based on where it finds the least interference.

- **Optimize Cells**—this option starts autocell configuration, an automatic, self-tuning mechanism that adjusts radio power to balance cell size between the selected Access Points to optimize coverage while limiting channel interference between neighboring APs. Autocell uses communication between Access Points to set radio power so that coverage is provided to all areas at the minimum power level required. This reduces potential interference with neighboring networks.

This operation will temporarily drop stations from the selected APs, so we advise against performing this on a production network.

Any configuration changes made through the profile for cell sizes will overwrite the values set by this operation.

The **Multi Channel** autocell option determines how autocell is performed. If the multi channel option is off (i.e., single channel autocell), a radio's cell size is adjusted when nearby APs have radios on the same ***channel*** within earshot of each other, so that the two radios minimize interference. If the multi channel option is on, then autocell will adjust the cell size for a radio when nearby APs have radios on the same ***band***, even if they are using different channels. This will result in smaller cell sizes and improves performance in dense environments.

Figure 75 illustrates autocell operation with four APs in four adjoining rooms, where the aim is to reduce channel interference and have clients connect to the AP that is in the same room with them. Figure A shows the result of running single channel autocell. Each radio's signal strength is reduced such that its cell size does not overlap the radio in the next room. In Figure B, after running single channel autocell, the cells will overlap because the radios all use different channels. In Figure C, multi channel autocell reduces cell size so that even radios on different channels in the same band do not overlap.

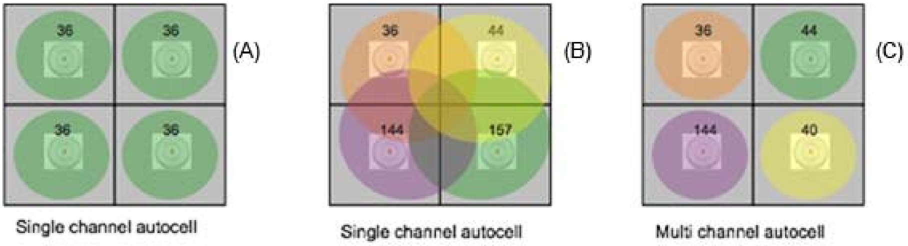


Figure 75. Autocell—Single Channel vs. Multi Channel

Select **Save configuration on successful completion** to automatically save the results of autocell if there are no problems.

For more information on the auto configuration of cells, or to have autocell run on a regularly scheduled basis, see **"Global Settings .11a" on page 507** or **"Global Settings .11bg" on page 510**.

    - **Enable Application Control**—this option enables deep packet inspection for traffic on the selected APs. See **"Application Control—Overview" on page 104**.

    - **Disable Application Control**—this option disables deep packet inspection for traffic on the selected APs. No data is collected, and you will not be able to display Application Control analysis for those APs.

- **Quick Config—**select an option from this drop-down list to apply a predefined configuration that uses best practices on the selected APs. The following options are available: **Classroom** or **High Density**. Select **Classroom** to configure the Access Point for use in classroom settings such as K-12 schools, higher education, etc. Select **High Density** to configure the Access Point for use in high density settings such as lecture halls, convention centers, stadiums, etc.

- **More**
  - Choose the **Add to AP Group** option to add the selected APs to a group. (**Figure 76**) A dialog box allows you to select an existing group or **Create a new group**.

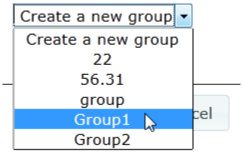


Figure 76. Adding APs to a Group

  - Choose the **Create Profile** option from the **More** drop-down list to create a new profile network containing the selected APs. See **“Managing by Profiles” on page 195**.
  - **Access Point WMI**connects to the Windows Management Interface for the selected AP (only one AP may be selected when using this command). After logging in to the AP, if you make any configuration changes, they apply only to that AP. They will not be propagated to other APs being managed by WOS. For detailed information about configuring an AP, refer to the *Using the Avaya OS for Avaya WLAN AP 9100 Series (NN47252-102)*. Note that you may also use WOS to configure an individual AP. See **“Configuring a Wireless AP” on page 369**.
  - Choose the **Delete** option from the **More** drop-down list to delete the selected APs from the WOS database.
  - Choose the **Take AP(s) Out of Service** option from the **More** drop-down list to mark the selected APs as being out of service, so that they are no longer polled for status or data. This allows maintenance to be performed without having to delete the APs from the WOS database. These units will be displayed with a blue dot in the list of APs. Use the **Return AP(s) to Service** option to restore normal WOS operation for these APs.

- **Custom**—If you have created any Custom Actions, the **Custom** button will be displayed. Your Custom Actions will appear in this drop-down list. Click on the desired action to apply it to the selected APs. See **"Create Custom Actions" on page 575** for more information.

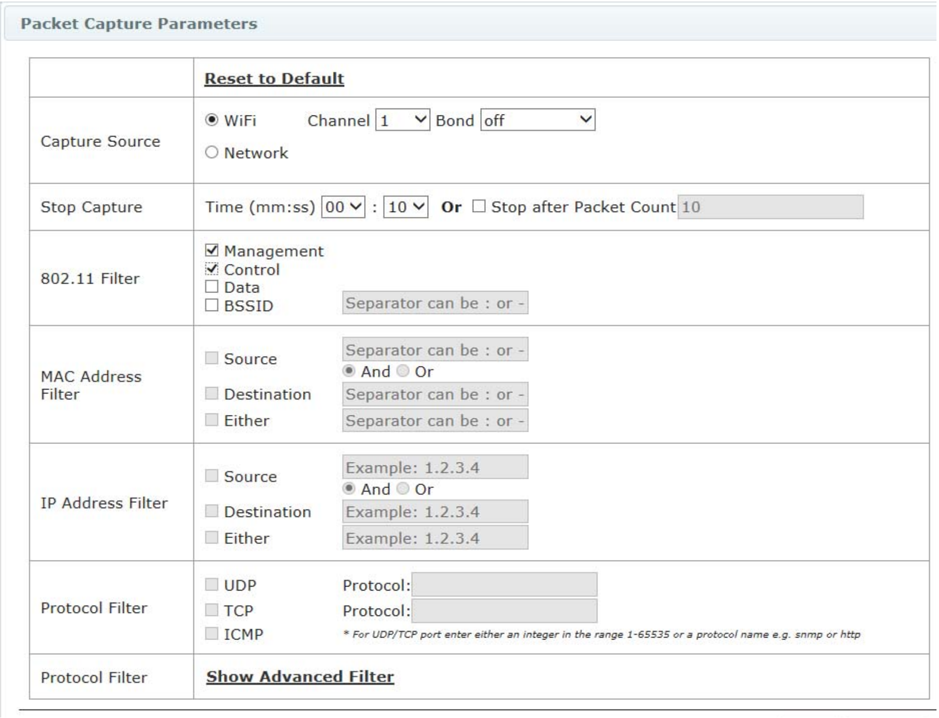
About Packet Capture

Capture is performed on the selected APs according to your specified filter settings. (**Figure 77**) The capture includes 802.11 header information (for APs running Avaya OS version 7.0 or higher). The capture is performed in promiscuous mode, which means that it can include all of the packets that are transmitted on the selected channel regardless of the origin or destination.

When the capture is complete, a download link will appear. Click it to download the requested capture as a zip file. You can also have the option to download an individual file for each AP in the list.

In the Packet Capture Parameters dialog, specify the following:

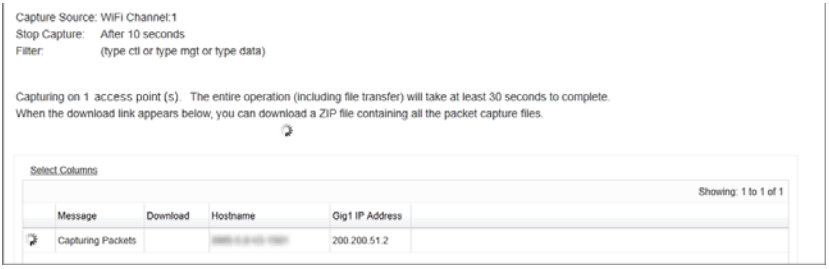
- **Capture Source**—the Ethernet port or Wi-Fi channel (with optional bonded channel) for the capture.
- **Stop Capture**—stop capturing after the specified number of seconds or packet count.
- **802.11 Filter**—capture a selected combination of types of traffic: control, management, data, or BSSID (specified by MAC address).
- **MAC Address Filter**—(optional) capture only packets with a source or destination of the specified MAC address (or both).
- **IP Address Filter**—(optional) capture only packets with a source or destination of the specified IP address (or both).
- **Protocol Filter**—(optional) capture only packets with the specified protocol.
- **Advanced Filter**—(optional) This uses the same syntax as tcpdump.



Packet Capture Parameters

	Reset to Default
Capture Source	● WiFi Channel 1 Bond off ○ Network
Stop Capture	Time (mm:ss) 00 : 10 **Or** □ Stop after Packet Count 10
802.11 Filter	☑ Management ☑ Control □ Data □ BSSID Separator can be : or -
MAC Address Filter	□ Source Separator can be : or - ● And ○ Or □ Destination Separator can be : or - □ Either Separator can be : or -
IP Address Filter	□ Source Example: 1.2.3.4 ● And ○ Or □ Destination Example: 1.2.3.4 □ Either Example: 1.2.3.4
Protocol Filter	□ UDP Protocol: □ TCP Protocol: □ ICMP ** For UDP/TCP port enter either an integer in the range 1-65535 or a protocol name e.g. snmp or http*
Protocol Filter	Show Advanced Filter

Figure 77. Packet Capture Dialog



Capture Source: WiFi Channel:1
Stop Capture: After 10 seconds
Filter: (type ctl or type mgt or type data)

Capturing on 1 access point (s). The entire operation (including file transfer) will take at least 30 seconds to complete.
When the download link appears below, you can download a ZIP file containing all the packet capture files.

Select Columns

Showing: 1 to 1 of 1

	Message	Download	Hostname	Gig1 IP Address
	Capturing Packets		[redacted]	200.200.51.2

Figure 78. Packet Capture in Progress

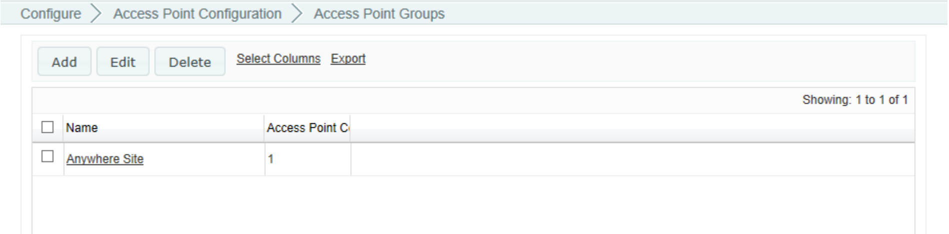
Profiles

Please see **"Managing by Profiles" on page 195**.

AP Groups

In WOS, you can create AP groups and assign the desired APs to be members of a group. In the web client, AP groups allow you to filter the data displayed so that only information for members of the selected AP group is presented.

The AP Groups page lists all of the AP groups that have been defined in WOS. It allows you to **Add**, **Edit**, or **Delete** groups. To display this page, click the **AP Groups** link in the **AP Configuration** section under **Configure** at the top of the page. Note that you may also create new groups in the web client from the **Access Points (Configure)** page, using the **More > Add to Group** option on the **The Configure APs Toolbar**. Similarly, you may use the same link on the **Access Points (Configure)** to add an AP to a group.



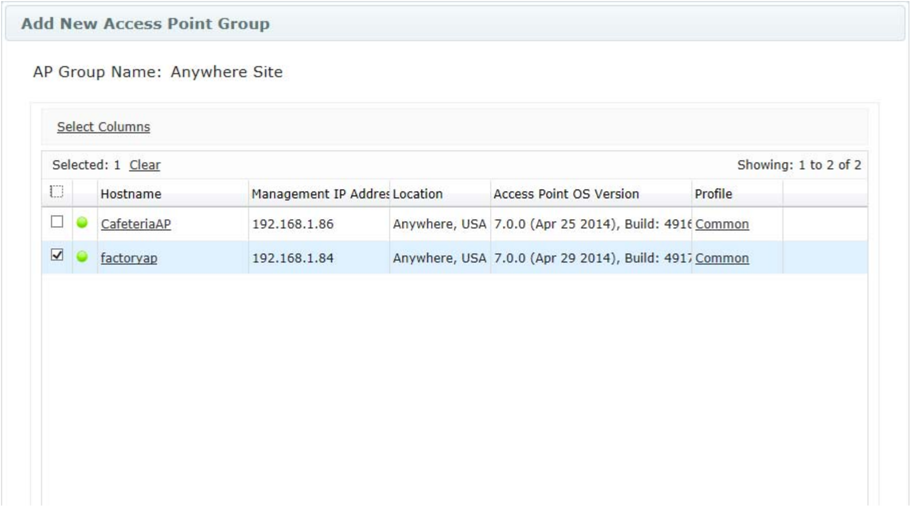
□	Name	Access Point C
□	Anywhere Site	1

Figure 79. AP Group Page

To modify an existing group, click **Edit**. The web client displays a list of all APs, with check marks in front of those that belong to the group. (**Figure 80**) You may check additional APs to add them to the group, or uncheck them to remove them from the group. Click **OK** when done.

To add a new group, click **Add**. Enter the new **Group Name**. The web client displays a list of all APs. Check the APs that you wish to add to the group. Click **OK** when done.

Click the **Delete** button if you wish to remove a group.



Add New Access Point Group

AP Group Name: Anywhere Site

Select Columns

Selected: 1 Clear

Showing: 1 to 2 of 2

□		Hostname	Management IP Addres	Location	Access Point OS Version	Profile
□	●	CafeteriaAP	192.168.1.86	Anywhere, USA	7.0.0 (Apr 25 2014), Build: 4916	Common
☑	●	factoryap	192.168.1.84	Anywhere, USA	7.0.0 (Apr 29 2014), Build: 4917	Common

Figure 80. Add or Edit Group

Config Templates

The Config Template pages allow you to apply a file containing a complete or partial configuration to an AP. Using config templates is described in the following topics:

- **"About Config Template Files" on page 118**
- **"Edit Config Templates" on page 119**
- **"Load Config Template" on page 122**
- **"Deploy Config Template" on page 124**

About Config Template Files

A config template (or config file) is a set of CLI commands to configure an AP. It may consist of:

- A complete set of commands to define every setting on the AP,
- an almost complete set that just omits a few items, like leaving out the IP address commands in order to leave the AP address as is,
- or a partial set of commands that just deal with particular aspects of the AP's configuration.

The file may be copied from the existing configuration of an AP that you select as a model, or may be entirely typed in. For example, if Avaya Customer Support sends you a config template, you may copy that file and paste it in to the config template editor to create your file.

If you start with a config template copied from the existing configuration of an AP, you may edit the file to contain only the settings that you wish to copy to other APs. The file makes incremental changes to the settings on an AP when it is deployed. Thus, ***settings not defined in the config template will be left unchanged***.

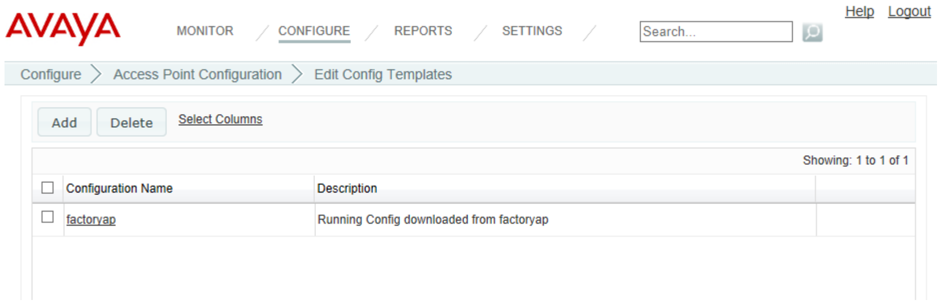
Config templates are useful in a number of situations. In particular, they are the *only* way to apply new features to APs before those features have been incorporated in WOS.

Edit Config Templates

*This feature is intended for **advanced users** who are familiar with use of the Avaya Wireless AP CLI and configuration files. Only **expert users** should use the option to create the entire configuration file.*

Use this page to type in the entire config template from beginning to end (i.e., “from scratch”), to modify an existing file, and to manage your config templates. Only expert users should create a config template from scratch. As an alternative, we strongly recommend that you use the **Load Config Template** page to download a config template from an AP. It may then be managed with this page.

Open this page by clicking the **Configure** link near the top of the window, then select **Edit Config Template** from the AP **Configuration** section.



Showing: 1 to 1 of 1

□	Configuration Name	Description
□	factoryap	Running Config downloaded from factoryap

Figure 81. Edit Config Template Page

To create a config template from beginning to end ("from scratch")

This procedure opens the config template editor so that you can type in the CLI command lines of the config template, or cut and paste commands from an existing config template into the editor.

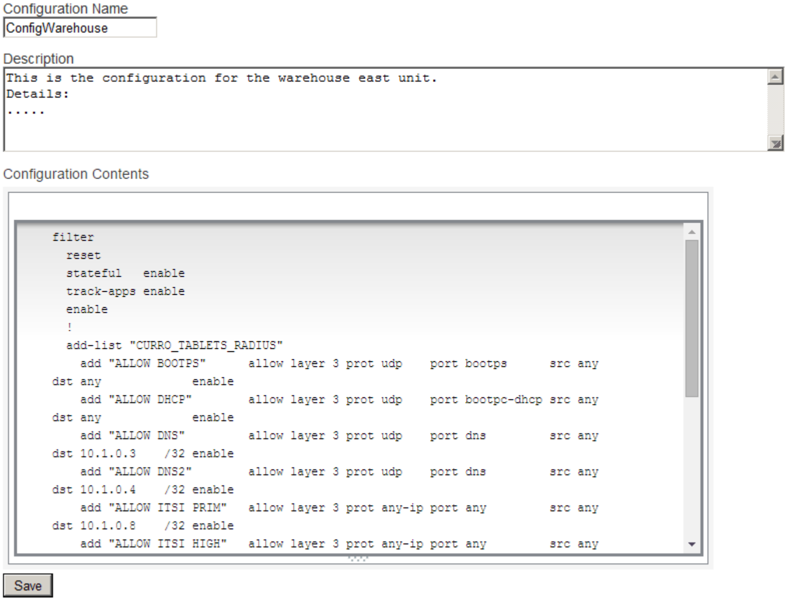
Click the **Add** button on the upper left of the **Edit Config Template** page. The config template editor appears. (**Figure 82**)

Enter **Configuration Name**, a name for this config template. Then enter an optional **Description**. You may type, paste text, or edit your commands in the large gray box at the bottom of the page. It is especially useful to copy large sections of text from a configuration file that has been quality-tested elsewhere, and paste the text into the editor box.

Editing the Configuration Template

You may type text to enter it in the box, and use the **Backspace** and **Delete** keys. You may use common selection and cut and paste keys:

- Ctrl+a: select all
- Ctrl+c: copy selected text
- Ctrl+x: cut selected text
- Ctrl+v: paste text (may be from an application other than WOS)
- Shift+Click: select contiguous text up to clicked location
- Shift+Arrow: select contiguous text in direction of arrow
- Use your browser's search functions if you want to search for text



Configuration Name

ConfigWarehouse

Description

```
This is the configuration for the warehouse east unit.
Details:
.....
```

Configuration Contents

```
filter
  reset
  stateful   enable
  track-apps enable
  enable
  !
  add-list "CURRO_TABLETS_RADIUS"
    add "ALLOW BOOTPS"      allow layer 3 prot udp    port bootps      src any
dst any             enable
    add "ALLOW DHCP"        allow layer 3 prot udp    port bootpc-dhcp src any
dst any             enable
    add "ALLOW DNS"         allow layer 3 prot udp    port dns         src any
dst 10.1.0.3    /32 enable
    add "ALLOW DNS2"        allow layer 3 prot udp    port dns         src any
dst 10.1.0.4    /32 enable
    add "ALLOW ITSI PRIM"   allow layer 3 prot any-ip port any         src any
dst 10.1.0.8    /32 enable
    add "ALLOW ITSI HIGH"   allow layer 3 prot any-ip port any         src any
```

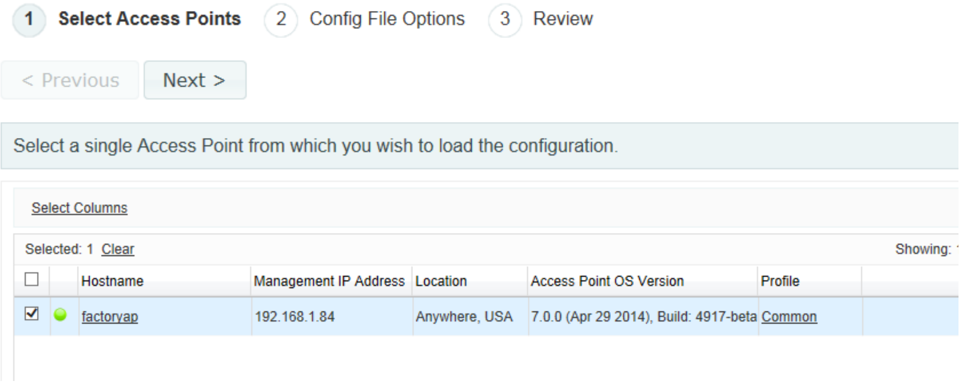
Figure 82. Config Template Editor

Click **Save** when done. The editor closes, and your new file appears in the list of config templates. (**Figure 81**) Each **Configuration Name** in this list is a link. To edit a file, simply click the link. If you wish to remove a config template, select the checkbox to the left of it and click the **Delete** button.

Load Config Template

Use this page to create a config template by downloading the configuration of an AP that you wish to use as a model. This method of creating a config template is highly recommended for most users. Only *expert* users should type in the entire file as described in **"Edit Config Templates" on page 119**!

Open this page by clicking the **Configure** link near the top of the window, then select **Load Config Template** from the AP **Configuration** section.



Select a single Access Point from which you wish to load the configuration.

☐		Hostname	Management IP Address	Location	Access Point OS Version	Profile
☑	●	factoryap	192.168.1.84	Anywhere, USA	7.0.0 (Apr 29 2014), Build: 4917-beta	Common

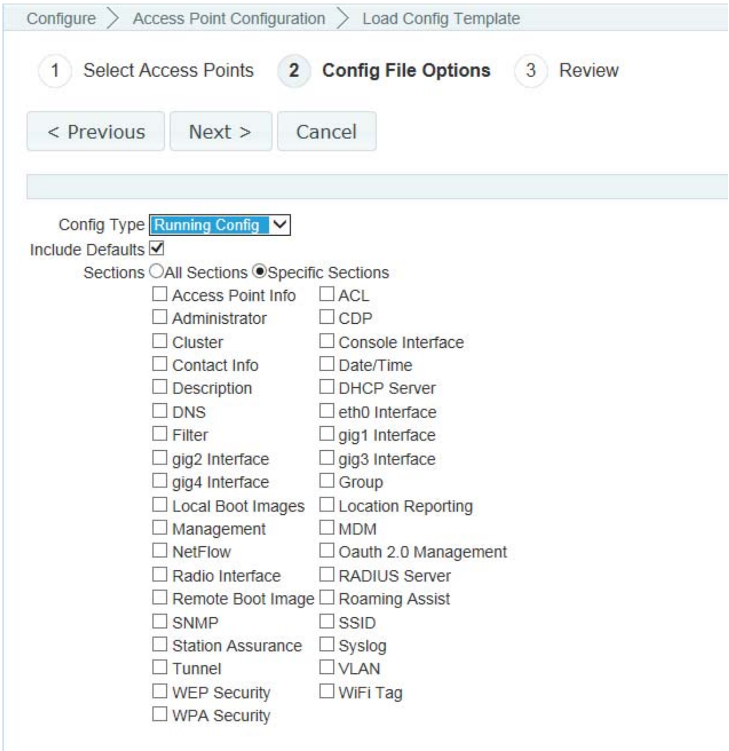
Figure 83. Load from AP

1. **Step 1 - Select APs:** The web client displays a list of the APs in the WOS database (for your **Current Access Point Scope**). Select the checkbox to the left of the "model" AP in the list, then click **Next**. The web client displays a **Loading** message while the download proceeds.
2. **Step 2 - Config File Options:** (**Figure 84**) Set **Config Type** according to the type of usage for this file.
   - factory.conf: The factory default settings.
   - lastboot.conf: The setting values from just before the last reboot.
   - saved.conf: The last settings that were explicitly saved using the Save changes to flash button at the top of each window.

Click the **Include Defaults** checkbox if you wish settings that are at their default value to be explicitly included in the file as well.

Select **All Sections** if you wish to keep the entire config file. Select **Specific Sections** to choose only specific settings for inclusion in the file.

Click **Next** when done.



Config Type Running Config

Include Defaults ☑

Sections ○ All Sections ● Specific Sections

☐ Access Point Info
☐ Administrator
☐ Cluster
☐ Contact Info
☐ Description
☐ DNS
☐ Filter
☐ gig2 Interface
☐ gig4 Interface
☐ Local Boot Images
☐ Management
☐ NetFlow
☐ Radio Interface
☐ Remote Boot Image
☐ SNMP
☐ Station Assurance
☐ Tunnel
☐ WEP Security
☐ WPA Security

☐ ACL
☐ CDP
☐ Console Interface
☐ Date/Time
☐ DHCP Server
☐ eth0 Interface
☐ gig1 Interface
☐ gig3 Interface
☐ Group
☐ Location Reporting
☐ MDM
☐ Oauth 2.0 Management
☐ RADIUS Server
☐ Roaming Assist
☐ SSID
☐ Syslog
☐ VLAN
☐ WiFi Tag

Figure 84. Load from AP - Config File Options

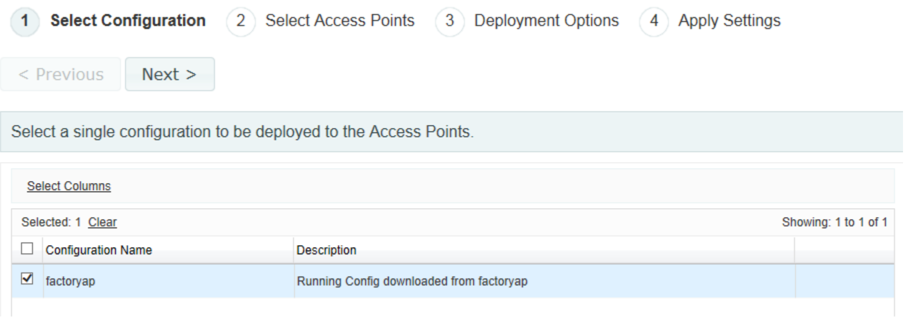
3. **Step 3 - Review:** When the download is complete, you are returned to the **Edit Config Template Page** and may review the file and make any desired changes as described in **"Edit Config Templates" on page 119**. The new template will appear on the **Edit Config Template Page**. The new file's name is the same as the host name of the AP from which it was downloaded.

When you download a config template from an AP, the file represents the entire configuration of the AP, except that WOS makes certain modifications to the file for your convenience:

- CLI commands are added to reset all the radios and then bring them back up. Similarly, other settings such as SSID, User Group, DHCP Server, and VLAN will be reset and brought back up. This guarantees that when the config template is deployed to another AP, all of these settings will be applied to an AP starting from a known baseline, due to the resets.
- All other radio settings are commented out, so that no radio settings will change. Certain other settings, such as Host Name, Location, and Avaya OS primary and backup software images will be commented out as well in order to prevent these device-specific settings from being applied to multiple APs.
- The entire VLAN section, VTUN section, and the IP address are commented out. Since these settings can vary from one AP to another, it would be easy to create problems if they were copied to other APs.

Deploy Config Template

Use this page to apply one of the config template files that you have already created to one or more APs.



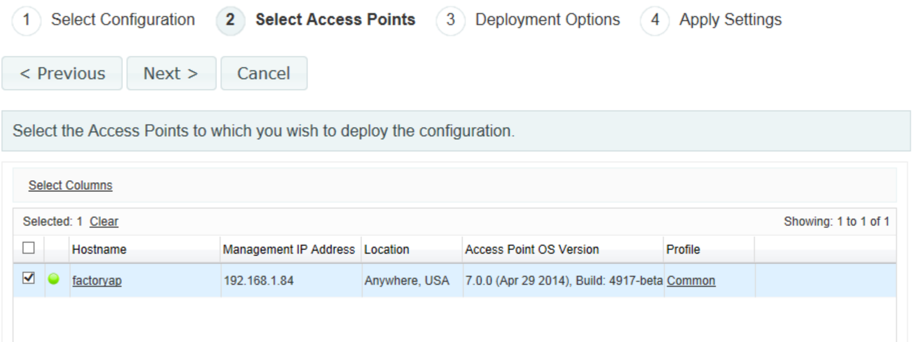
Select a single configuration to be deployed to the Access Points.

□	Configuration Name	Description
☑	factoryap	Running Config downloaded from factoryap

Figure 85. Select Config Template File to Deploy

Open this page by clicking the **Configure** link near the top of the window, then select **Deploy Config Template** from the AP **Configuration** section. The web client displays a list of the available config templates. (**Figure 85**)

Select the checkbox to the left of the desired config template, then click **Next**. The web client displays a list of the APs in the WOS database (for your **Current Access Point Scope**). (**Figure 86**)



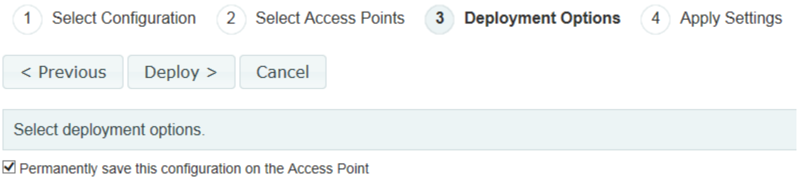
Select the Access Points to which you wish to deploy the configuration.

Selected: 1 Clear — Showing: 1 to 1 of 1

☐		Hostname	Management IP Address	Location	Access Point OS Version	Profile
☑	●	factoryap	192.168.1.84	Anywhere, USA	7.0.0 (Apr 29 2014), Build: 4917-beta	Common

Figure 86. Select APs for Deployment

Select the checkbox of one or more APs in the list to which the config template is to be deployed, then click **Next**. The web client displays deployment options. (**Figure 87**)

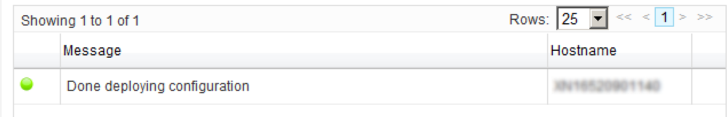


Select deployment options.

☑ Permanently save this configuration on the Access Point

Figure 87. Select Deployment Options

Select the checkbox to **Permanently save this configuration on the AP**. If you do not check this box, the commands in the config template will be deployed on the selected APs, but they will not be saved. Thus, they will not be reapplied if you reboot the AP. Click **Deploy** to apply the config template to the selected APs. The web client displays deployment results. (**Figure 88**)



Showing 1 to 1 of 1 Rows: 25

	Message	Hostname
●	Done deploying configuration	[redacted]

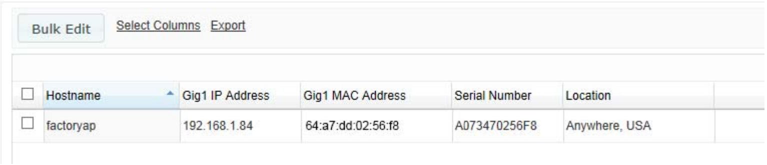
Figure 88. Deployment Results

The **Message** list indicates when the deployment is in progress for each of the selected APs, and then shows whether the deployment has been completed.

Custom Field Values

This page populates a new column (created with **"Create Custom Fields" on page 574**) with data values. The page includes a **Bulk Edit** option that allows you to enter identical data for multiple APs in one step, in the same way that you can use Bulk Edit for the **Configure Network Settings** and **Configure Wireless Settings** pages. To import custom field values (and even define custom fields) for many APs from a file, see **"Import Access Point Custom Fields" on page 128**.

Open this page by clicking the **Configure** link near the top of the window, then select **Custom Field Values** from the AP **Configuration** section. You may filter the APs displayed using **Current Access Point Scope**.



□	Hostname	Gig1 IP Address	Gig1 MAC Address	Serial Number	Location
□	factoryap	192.168.1.84	64:a7:dd:02:56:f8	A073470256F8	Anywhere, USA

Figure 89. Custom Field Values—Adding a single value

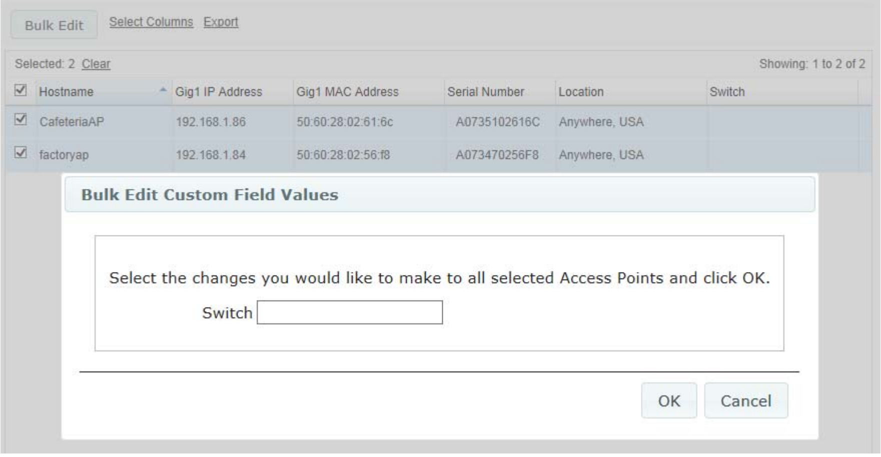
Before you add values, you must make sure that the desired custom column is displayed. If you have scrolled all the way to the right of the APs list and the new column is not visible, use the **Select Columns** link to add it to your display. You may also wish to change the custom column's position to be further to the left. See

“Select Columns” on page 62 if you need more details. Note that you can also change the new column’s position by simply dragging its column header in the AP list (see **“Rearranging and Resizing Columns in a Table” on page 64**).

To enter a value for an individual AP, simply click a cell in the custom column. (**Figure 89**) You may need to click at the beginning of the cell (i.e., towards the left-hand side of the cell). A dialog box is displayed where you can type the desired string, up to 255 characters long. Click **OK** when done to save the value, or click **Cancel** to abort.

Use **Bulk Edit** to quickly configure multiple APs to have the same value. Select the checkbox at the beginning of each row that is to contain this value. To select all rows, click the checkbox in the header row. Click again to deselect all rows.

Click **Bulk Edit** when the desired rows are selected. The Bulk Edit Custom Field Values dialog box appears. Enter the desired string, up to 255 characters, and click **OK**. (**Figure 90**)



Selected: 2 Clear

Showing: 1 to 2 of 2

☑	Hostname	Gig1 IP Address	Gig1 MAC Address	Serial Number	Location	Switch
☑	CafeteriaAP	192.168.1.86	50:60:28:02:61:6c	A0735102616C	Anywhere, USA	
☑	factoryap	192.168.1.84	50:60:28:02:56:f8	A073470256F8	Anywhere, USA	

Bulk Edit Custom Field Values

Select the changes you would like to make to all selected Access Points and click OK.

Switch

Figure 90. Bulk Configuration (Custom Field Values)

The value that you entered will be displayed in the APs list for the selected APs.

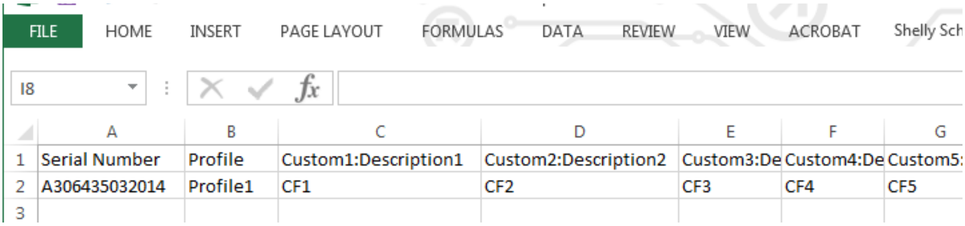
Import Access Point Custom Fields

This feature imports a Comma-Separated Values (.csv) file to populate a number of AP profile assignments and custom fields in one step. The file contains a list of APs, and you can specify the following information for each:

- **Profile**—for AOS profiles only, if this field is populated (not blank), the AP is assigned to this profile. See **"Profiles" on page 196**.
- **Custom Fields**—these are extra fields that you can define for any sort of data or notes that you want to keep with each of your APs, as described in **Customization**. Each field is a column that can be displayed on the **Monitor—Access Points** page and the **Access Points (Configure)** page. For example, you might add an asset tag column, or a column for notes regarding support actions for this AP. You may add up to five new columns.

To set custom field values for just a few APs manually, see **"Custom Field Values" on page 126**.

Format of the CSV File



	A	B	C	D	E	F	G
1	Serial Number	Profile	Custom1:Description1	Custom2:Description2	Custom3:De	Custom4:De	Custom5:
2	A306435032014	Profile1	CF1	CF2	CF3	CF4	CF5
3							

1. The first row must have the names of the desired fields (column headers), as shown above.

    - The first column must be called **Serial Number**. The capitalization and punctuation must match this exactly.
    - The second column must be called **Profile**. The capitalization and punctuation must match this exactly.
    - The remaining columns (from zero up to five additional columns) are the names of the custom fields whose values you will be entering from this file. The names can be any alphanumeric strings of up to

255 characters. If a custom field with a column name has already been defined, then the data in that column for the rest of the file will apply to that existing custom field. If this is a new custom field name, then it will define a new custom field. Note that if you misspell the name of an existing custom field, a new custom field will be created with the misspelled name.

2. Each of the second and successive rows contain information for a single AP. The fields in each row must match the column headers in the first row. The steps below describe these fields.

3. The first field specifies the AP by its **Serial Number**. There should be only one entry (i.e., row) per AP. If there are multiple rows for the same AP, its last occurrence (bottom-most) in the file is used—it over-writes any previous values in the WOS database.

4. The second field in a row specifies the profile to which this AP is assigned. If the field is blank, this entry in the csv file will be skipped. If the profile name entered matches an existing profile, then the AP is placed into that profile. If the profile field string does not match an existing profile, then a new profile is created with that name, and the AP is added to it. The profile name is not case-sensitive and cannot be longer than 50 characters (no spaces allowed). Note that if you misspell the profile name, a new profile will be created with the misspelled name.

5. All the data in columns 3 to 7 of the remaining rows will be used to populate the custom fields with data.

6. Profile configuration will not be automatically applied (pushed) to APs after the file import is complete. You should review the new **Profiles** and enter their configuration and software version settings. Then push each profile to its member APs manually, either by using the **Sync APs** button on the **The Profiles Toolbar**, or using the **Apply Config** button on the **Profile Details—Configuration** page.

The profile assignments and custom field values in the file become the current values, replacing any previous values, and they may later be edited as well. If there are multiple entries in the file for the same AP, then the later entries will override the previous ones.

Access Point Upgrade

The AP Upgrade pages allow you to specify a software upgrade to apply to selected APs immediately or at a scheduled time, and then view pending and in-progress upgrades, and the results of finished operations.

This is described on the following pages:

- **"Perform or Schedule Upgrade" on page 131**
- **"Scheduled Upgrades" on page 136**

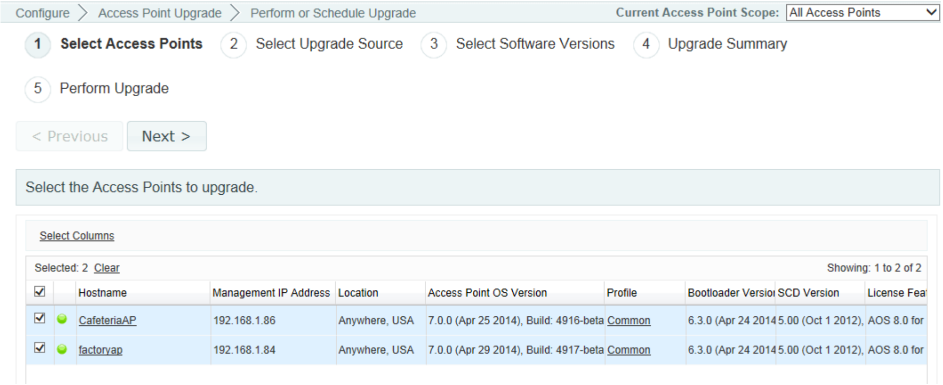
Perform or Schedule Upgrade

This page allows you to upgrade one or more APs to a new software release. To display this page, click the **Perform or Schedule Upgrade** link in the AP **Upgrade** section under **Configure** at the top of the page. You may perform the upgrades immediately, or schedule them for a later time.

If you are upgrading an AP to add new features that are not supported by your existing license, the AP must have the new license key that includes the upgraded features before upgrading. Similarly, if you are upgrading an AP for a new software release, the AP must have the new license key that enables the operation of that release before upgrading.

License updates are performed **automatically** as part of the WOS upgrade process. For each selected AP, WOS will check if the requested upgrade requires a new license. If so, it will send a command to the AP to activate the license update process, and then wait to allow the license update to proceed. F

Major *and* minor releases will need a new license key, but patch releases will not. For example, to upgrade from Avaya OS Release 7.0.5 to Release 7.1 requires a new license. To upgrade from Avaya OS Release 7.0.1 to Release 7.0.2, use the existing license.



Configure > Access Point Upgrade > Perform or Schedule Upgrade   Current Access Point Scope: All Access Points

Select the Access Points to upgrade.

Select Columns

Selected: 2 Clear   Showing: 1 to 2 of 2

☑		Hostname	Management IP Address	Location	Access Point OS Version	Profile	Bootloader Versio	SCD Version	License Fea
☑	●	CafeteriaAP	192.168.1.86	Anywhere, USA	7.0.0 (Apr 25 2014), Build: 4916-beta	Common	6.3.0 (Apr 24 2014	5.00 (Oct 1 2012),	AOS 8.0 for
☑	●	factoryap	192.168.1.84	Anywhere, USA	7.0.0 (Apr 29 2014), Build: 4917-beta	Common	6.3.0 (Apr 24 2014	5.00 (Oct 1 2012),	AOS 8.0 for

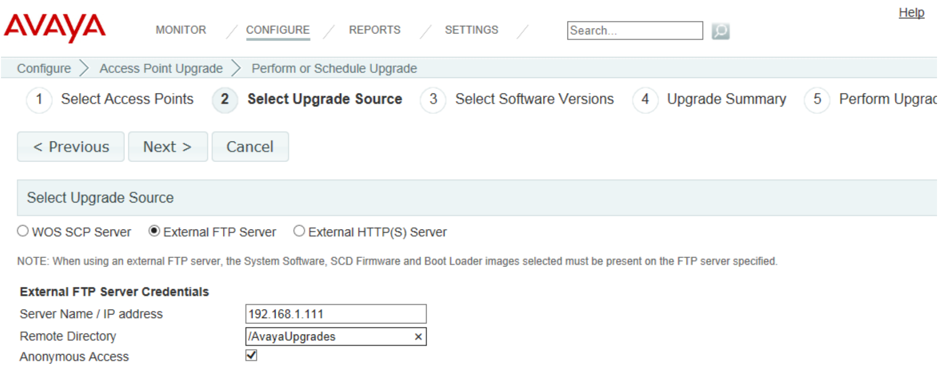
Figure 91. AP Upgrade

1. **Step 1 - Select APs:** Select all of the APs that are to be updated with the new software image. (**Figure 91**) Check that they all have licenses installed that will support the new release (see **"Deployed Licenses" on page 185**). Note that only APs in the selected **Current AP Scope** are listed. Click **Next**.

2. **Step 2 - Select Upgrade Source:** (**Figure 92**)

   a. **WOS SCP Server**: By default, the upload uses Secure Channel Protocol (SCP) to upload files (specified in the next step) to each AP.

   b. **External FTP Server**: If you select FTP instead, fields will appear where you must specify **Server Name** or **IP Address**, **Remote Directory**, and login details. When using an external FTP server, any System Software, SCD Firmware and Boot Loader images selected in the next step must be present on the FTP server specified.



Select Upgrade Source

○ WOS SCP Server ● External FTP Server ○ External HTTP(S) Server

NOTE: When using an external FTP server, the System Software, SCD Firmware and Boot Loader images selected must be present on the FTP server specified.

External FTP Server Credentials

Server Name / IP address	192.168.1.111
Remote Directory	/AvayaUpgrades
Anonymous Access	☑

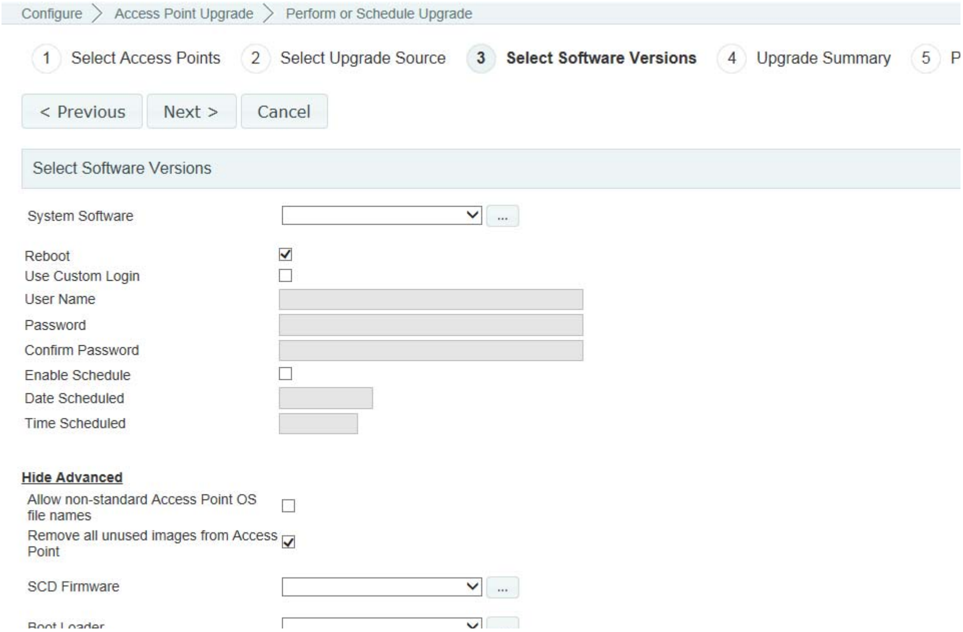
Figure 92. Select Upgrade Source

c. **External HTTP(S) Server**: If you select HTTP, you will specify the URL of the new software and other details in the next step.

Click **Next>** when done to proceed to the next step.

3. **Step 3 - Select Software Versions:** (Figure 93)

   a. **System Software / URL**:
   If the Upgrade Source is **HTTP—**Enter the URL of the new System Software file.
   If the Upgrade Source is **SCP** or **FTP—**If you have already uploaded this software image to WOS, then select it from the drop-down list in this field. Otherwise, make sure that you have the software image file in a location that you can access from your file system. Click ... and then click **Choose File**, and browse to the software image file. Next, click the **Upload** button, then click **Close** when the upload is complete. Make sure that the desired file is selected in the **System Software** field.



System Software

☑ Reboot

□ Use Custom Login

User Name

Password

Confirm Password

□ Enable Schedule

Date Scheduled

Time Scheduled

□ Allow non-standard Access Point OS file names

☑ Remove all unused images from Access Point

SCD Firmware

Boot Loader

Figure 93. Select Software Versions

b. **Reboot**: Check this if you want the APs to be rebooted when the upgrade is complete. This will cause the selected APs to run the new image. If this is left unchecked, then the new images will be uploaded to the selected APs but they will not be run until the APs are rebooted at a later time.

c. **Use Custom Login**: Use these fields to specify an administrator login for the upgrade. Custom Login is optional if SNMP is enabled on the AP. Check this box and set up the login parameters required for uploading the image to APs. These values must match an admin account that is configured on the AP, else the upload to the AP will fail. By default, the upload uses Secure Channel Protocol (SCP) to authenticate access to each AP. The AP will accept logins that match any of its Admin accounts with write privileges. These accounts may be entered either directly on the AP or using WOS. Also, this process will use any AP Shell Authentication information defined in the discovery dialog (see **"SSH Users" on page 172**). Note that APs are shipped with the factory default login admin/admin.

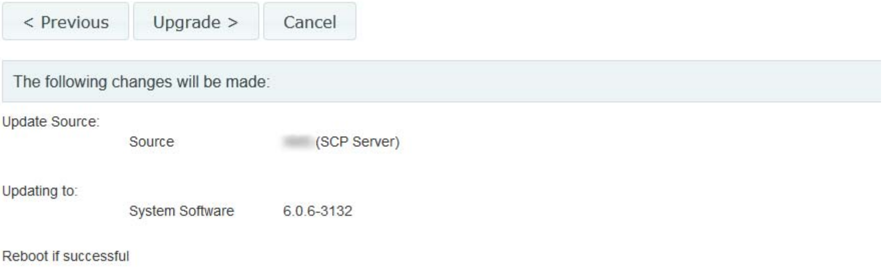
d. **Enable Schedule**: If you want to perform this upgrade at a later time, rather than immediately, check this box and set the time for the upgrade. Click in the **Date Scheduled** field, and select the date. Click in the **Time Scheduled** field, and use the **Hour** and **Minute** sliders to select the time (on a 24 hour clock).

e. **Show Advanced:** Click this link for certain advanced features on the advice of Avaya Customer Support personnel, and enter the following fields as needed.

- **Allow non-standard Avaya OS file names:** If Avaya advises you that your files will have non-standard names, check this box.
- **Remove all unused images from AP:** If you wish to clean up old images from the AP, check this box. Only the active and backup images are kept—all others are removed.
- **Ignore certificate warnings** (for **HTTP** upgrade only): If you wish to ignore any SSL certificate warnings on the URL that you entered as the Upgrade Source, check this box.
- **SCD Firmware** (for **SCP** and **FTP** upgrade only): This is the software on the AP that controls low-level hardware functions such as the fan, the environment controller, and the watchdog timer. If you have been advised to upgrade your SCD Firmware, then upload it and select it here, as described in **Step 3**. For Avaya OS Release 7.0 and above, this file is part of the system software and is automatically updated along with it.
- **Boot Loader** (for **SCP** and **FTP** upgrade only): If you have been advised to upgrade your Boot Loader, then upload it and select it here, as described in **Step 3**. For Avaya OS Release 7.0 and above, this file is part of the system software and is automatically updated along with it.

4. **Step 4 - Upgrade Summary:** This page shows the details that you specified for the upgrade. (**Figure 94**) Review these values carefully. Click the **Previous** button if you need to change anything.

Click the **Upgrade** button when you are done making changes.



The following changes will be made:

Update Source:

Source [redacted] (SCP Server)

Updating to:

System Software 6.0.6-3132

Reboot if successful

Figure 94. Upgrade Summary

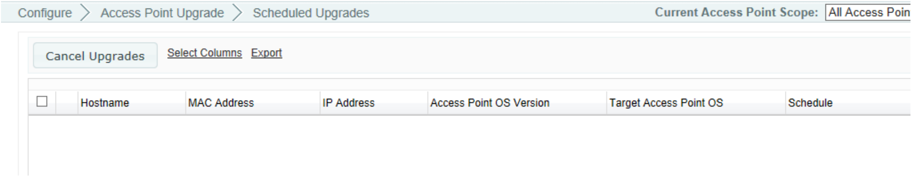
The web client will apply the upgrades you entered, and display the success or failure of the operation on the selected APs.

Scheduled Upgrades

Use this page to view or cancel pending upgrades that you have scheduled. To display this page, click the **Scheduled Upgrades** link in the AP **Upgrade** section under **Configure** at the top of the page.

Only APs in the selected **Current AP Scope** are listed. If you wish to see all of the scheduled/performed operations, set **Current AP Scope** to **All APs**.

To delete scheduled upgrades, select the desired APs and click the **Cancel Upgrades** button. You may only cancel upgrades that have not yet begun.



Current Access Point Scope: All Access Poin

□	Hostname	MAC Address	IP Address	Access Point OS Version	Target Access Point OS	Schedule

Figure 95. Scheduled Upgrades

The following information is show for each AP, by default:

- **Hostname, MAC Address, IP Address**—these identify the AP to upgrade.
- **AOS Version**—the software version that was running on the AP before the upgrade.
- **Target AOS**—the new software version to which the AP is to be upgraded.
- **Schedule**—the date and time for which the upgrade is scheduled.
- **Message**—the status of the pending, in-progress, or scheduled upgrade.

Wireless Configuration

This section includes the following pages:

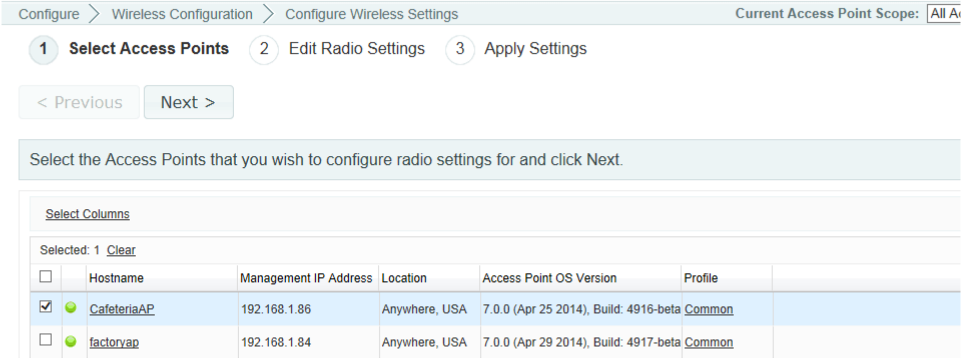
- **Configure Wireless Settings**
- **Export Wireless Settings**
- **Import Wireless Settings**

Configure Wireless Settings

Note that this feature is not available for smaller APs that use the AOSLite system software, such as the WAP9112.

The Configure Wireless Settings page provides very convenient options for configuring settings on a per-radio basis. Bulk radio configuration and the ability to set different values on multiple radios easily at one time are available only from this web client window. Bulk configuration is a particularly valuable feature, allowing you to apply the same settings to multiple radios in one step. Individual and bulk editing are used in the same way as on the **"Configure Network Settings" on page 141** page. See **"Individual vs. Bulk Edits" on page 142** for usage instructions.

Open the Configure Wireless Settings page by clicking the **Configure** link near the top of the window. In the **Wireless Configuration** section, select **Configure Wireless Settings**.


Configure > Wireless Configuration > Configure Wireless Settings
Current Access Point Scope: All A
1 Select Access Points
2 Edit Radio Settings
3 Apply Settings
< Previous
Next >
Select Columns

Select the Access Points that you wish to configure radio settings for and click Next.

Selected: 1 Clear

☐		Hostname	Management IP Address	Location	Access Point OS Version	Profile
☑	●	CafeteriaAP	192.168.1.86	Anywhere, USA	7.0.0 (Apr 25 2014), Build: 4916-beta	Common
☐	●	factoryap	192.168.1.84	Anywhere, USA	7.0.0 (Apr 29 2014), Build: 4917-beta	Common

Figure 96. Configure Wireless Settings Page

Pages that **Export Wireless Settings** and **Import Wireless Settings** are also available.

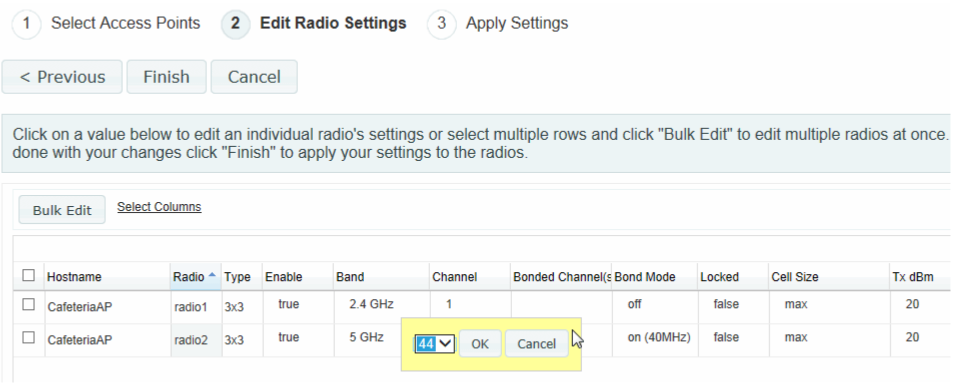
To Modify Wireless Settings

1. **Select APs:** For each radio that you wish to modify, select the checkbox at the beginning of the row. You may click the checkbox in the header row to select or deselect all rows. Note that only APs in the selected **Current AP Scope** are listed. Click **Next>** when the desired rows are selected.

2. **Edit Radio Settings:** You may edit the values in the following columns: **Enable**, **Band**, **Channel**, **Bond Mode**, **Locked**, **Cell Size**, **Tx dBm**, **Rx dBm**, **Antenna**, and **Wi-Fi Mode**. See **"Radio Settings" on page 488** for descriptions of these settings.

   Simply click a table cell that you wish to modify. A text box will be displayed where you may type the desired value, then click **OK**. (**Figure 97**) You may change as many cells in as many rows as you wish. There is no need to click the check boxes on modified rows. Modifications will be highlighted on the page. To set a field to the same value in multiple APs, use the **Bulk Edit** button. See **"To modify multiple rows at once with Bulk Edit" on page 143**.

   Click **Finish** when done. WOS applies the changes to the selected APs.



Click on a value below to edit an individual radio's settings or select multiple rows and click "Bulk Edit" to edit multiple radios at once. done with your changes click "Finish" to apply your settings to the radios.

□	Hostname	Radio	Type	Enable	Band	Channel	Bonded Channel(s	Bond Mode	Locked	Cell Size	Tx dBm
□	CafeteriaAP	radio1	3x3	true	2.4 GHz	1		off	false	max	20
□	CafeteriaAP	radio2	3x3	true	5 GHz	44		on (40MHz)	false	max	20

Figure 97. Editing the Radio Settings Page

3. **Apply Settings:** The web client will display the success or failure of the configuration operation on the selected APs.

Export Wireless Settings

This option exports channel and other radio settings on selected APs to an Excel file or to a CSV file—a set of comma-separated values that are compatible with Microsoft Excel. This file is useful in a number of ways:

- As a backup of the current configuration, especially since the settings in the file may be imported to restore this configuration.
- To provide Avaya Customer Support with a snapshot of the configuration of your network, at their request.
- You may edit the settings in this file and then import the changed values. Take care only to modify the fields that are editable on the Bulk Configuration page.

This feature is used in exactly the same way as the export feature for network settings. Please see **“Export Network Settings” on page 149** for instructions. To import a file that was exported from the Wireless Settings page, see **“Import Wireless Settings” on page 140**.

Note that Import and Export Wireless Settings are not available for smaller APs that use the AOSLite system software, such as the WAP9112.

Import Wireless Settings

This option allows you to change settings on radios by importing a file that was exported from the Wireless Settings page. (See **“Export Wireless Settings” on page 140** for details). This feature is used in exactly the same way as the import feature for network settings. Please see **“Import Network Settings” on page 152** for instructions.

Network Configuration

This section includes the following pages:

- **Configure Network Settings**
- **Export Network Settings**
- **Import Network Settings**

Configure Network Settings

The Configure Network Settings page provides very convenient options for configuring AP network settings for the Ethernet ports. Some of these functions are also available from the **Configure** menu on **The Access Points Toolbar**. Bulk configuration is a particularly valuable feature, allowing you to change network settings on a number of APs in one step. **"Individual vs. Bulk Edits" on page 142** describes usage of the two methods for changing settings on this page.

Open the Network Settings page by clicking the **Configure** link near the top of the page. In the **Network Configuration** section, select **Configure Network Settings**. Note that only APs in the selected **Current AP Scope** are listed.

You have two major options for network settings—**Modify Network Settings (Basic)** or **Modify Network Settings (Advanced)**. The Basic option mainly changes IP settings. The Advanced option adds management of settings for DNS, Ethernet, and Gigabit port bonding.

Pages that **Export Network Settings**, and **Import Network Settings** are also available.

The following topics describe configuring network settings:

- **"About Using the Network Settings Page" on page 142**
- **"Individual vs. Bulk Edits" on page 142**
- **"Modify Network Settings (Basic)" on page 145**
- **"Modify Network Settings (Advanced)" on page 146**

About Using the Network Settings Page

A number of basic operations are available on this page to allow you to customize it for your own use:

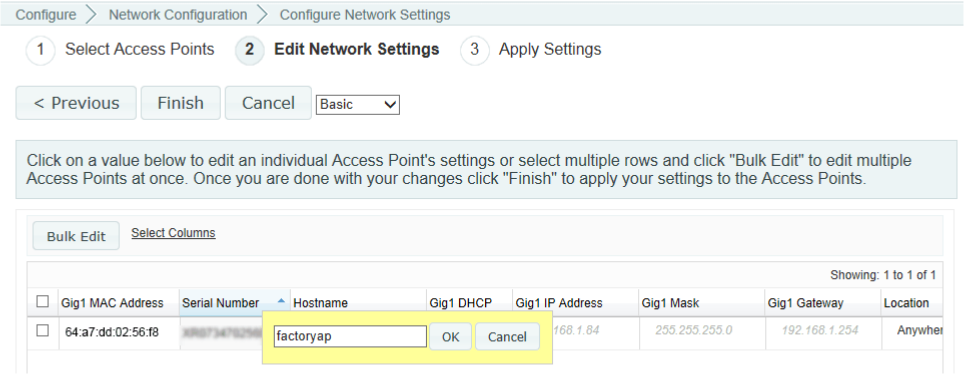
- **"Current Access Point Scope" on page 62**
- **"Select Columns" on page 62**
- **"Rearranging and Resizing Columns in a Table" on page 64**
- **"Sorting" on page 64**

Individual vs. Bulk Edits

Network settings pages offer the option of modifying rows individually, or modifying multiple rows with bulk configuration. The bulk option is a very useful shortcut that applies identical settings to the selected APs. In some cases, bulk configuration has an additional intelligent capability—for example, when setting the IP Address, the value you enter is used as a starting point for a range of addresses, since you cannot assign the same IP address to multiple APs. (**Figure 100**)

To modify rows individually

Simply click a table cell that you wish to modify. A text box will be displayed where you may type the desired value. (**Figure 98**) Click **OK** when done. You may change as many cells in as many rows as you wish. There is no need to click the check boxes on modified rows. Modifications will be highlighted on the page. All changes will be accumulated, but will not be applied until you complete the **Apply Settings** step.



Configure > Network Configuration > Configure Network Settings

1 Select Access Points 2 **Edit Network Settings** 3 Apply Settings

< Previous Finish Cancel Basic

Click on a value below to edit an individual Access Point's settings or select multiple rows and click "Bulk Edit" to edit multiple Access Points at once. Once you are done with your changes click "Finish" to apply your settings to the Access Points.

Bulk Edit Select Columns

Showing: 1 to 1 of 1

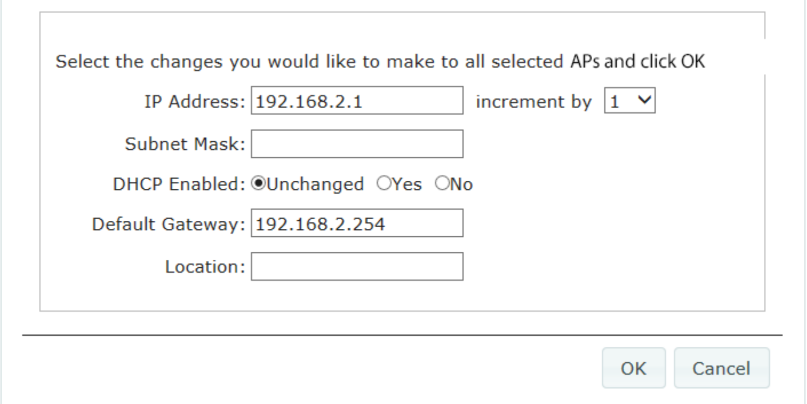
□	Gig1 MAC Address	Serial Number	Hostname	Gig1 DHCP	Gig1 IP Address	Gig1 Mask	Gig1 Gateway	Location
□	64:a7:dd:02:56:f8	[redacted]	factoryap OK Cancel		168.1.84	255.255.255.0	192.168.1.254	Anywher

Figure 98. Editing Individual Rows

To modify multiple rows at once with Bulk Edit

Select the APs that you wish to edit by clicking their check boxes. Then click the **Bulk Edit** button. This displays blank fields for all of the settings that are modifiable in bulk on this page. For example, **Figure 99** shows the Bulk Edit dialog for the **Edit Network Settings** step in Basic mode. Enter the values that you want applied to all of the APs that you selected.

For the **IP Address** field, enter the starting value for a range of addresses. Then select an **Increment by** value for the range. Note that AP **Host Names** cannot be bulk configured. Bulk edit fields that are left blank will be unchanged on APs.



Select the changes you would like to make to all selected APs and click OK

IP Address: 192.168.2.1 increment by 1

Subnet Mask:

DHCP Enabled: ● Unchanged ○ Yes ○ No

Default Gateway: 192.168.2.254

Location:

Figure 99. Bulk Configuration (Network Settings)

Click **OK** when done. The Bulk Edit dialog closes, and your desired changes will be displayed in the network settings table. Note that the new values have not yet been sent to the APs. Take a moment to review your changes. In particular, make sure that the IP addresses that were assigned are correct. You may individually edit any incorrect settings.

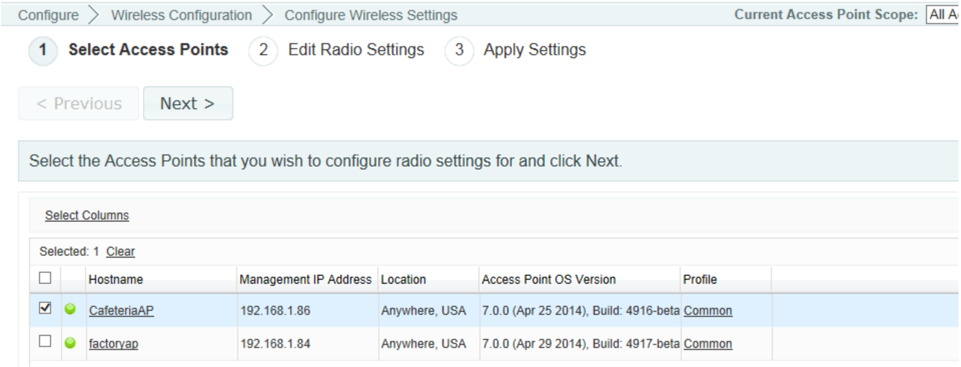
Click **Finish** when satisfied with the changes.

Modify Network Settings (Basic)

1. **Select APs:** Ensure that the **Basic** option is selected (to the right of the **Next>** button).

   For each row that you wish to modify, select the checkbox at the beginning of the row. Click the checkbox in the header row to select all rows. Click again to deselect all rows.

   Click **Next>** when the desired rows are selected.



Configure > Wireless Configuration > Configure Wireless Settings — Current Access Point Scope: All A

1 Select Access Points — 2 Edit Radio Settings — 3 Apply Settings

< Previous | Next >

Select the Access Points that you wish to configure radio settings for and click Next.

Select Columns

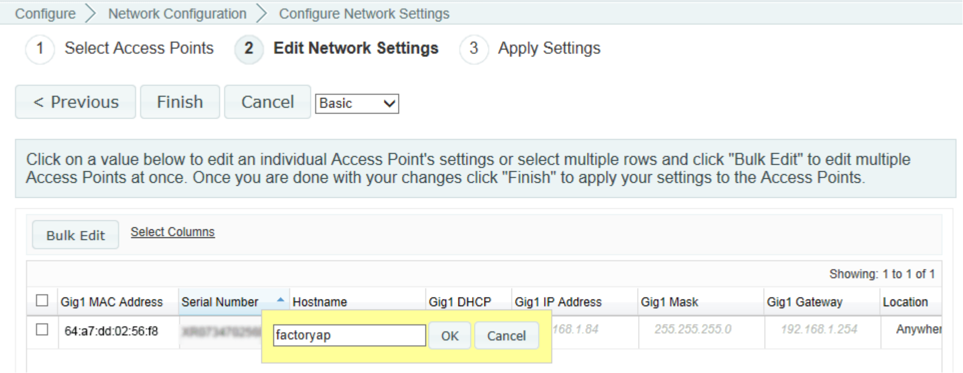
Selected: 1 Clear

□		Hostname	Management IP Address	Location	Access Point OS Version	Profile
☑	●	CafeteriaAP	192.168.1.86	Anywhere, USA	7.0.0 (Apr 25 2014), Build: 4916-beta	Common
□	●	factoryap	192.168.1.84	Anywhere, USA	7.0.0 (Apr 29 2014), Build: 4917-beta	Common

Figure 100. Configure Network Settings Page (Basic)

2. **Edit Network Settings:** You may edit the values in the following columns individually: **Hostname**, **Gig1 DHCP**, **Gig1 IP Address**, **Gig1 Mask**, **Gig1 Gateway**, **Location**. Simply click a table cell that you wish to modify. A text box will be displayed where you may type the desired value. (**Figure 101**) You may change as many cells in as many rows as you wish. There is no need to click the check boxes on modified rows. Modifications will be highlighted on the page. To set a field to the same value in multiple APs, use the **Bulk Edit** button. See **“To modify multiple rows at once with Bulk Edit” on page 143**.

   Click **Finish** when done. WOS applies the changes to the selected APs.



Configure > Network Configuration > Configure Network Settings

1 Select Access Points 2 **Edit Network Settings** 3 Apply Settings

Click on a value below to edit an individual Access Point's settings or select multiple rows and click "Bulk Edit" to edit multiple Access Points at once. Once you are done with your changes click "Finish" to apply your settings to the Access Points.

Showing: 1 to 1 of 1

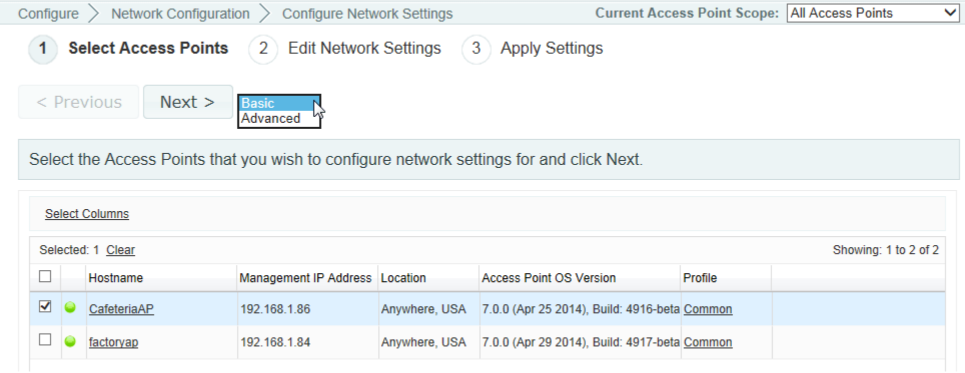
☐	Gig1 MAC Address	Serial Number	Hostname	Gig1 DHCP	Gig1 IP Address	Gig1 Mask	Gig1 Gateway	Location
☐	64:a7:dd:02:56:f8	[redacted]	factoryap OK Cancel		168.1.84	255.255.255.0	192.168.1.254	Anywher

Figure 101. Editing the Network Settings Page (Basic)

3. **Apply Settings:** The web client will display the success or failure of the configuration operation on the selected APs.

Modify Network Settings (Advanced)

1. **Select APs:** Select the **Advanced** option (to the right of the **Next>** button). Select the checkbox to the left of each AP row that you wish to modify. You may click the checkbox in the header row to select or deselect all rows. Click **Next>** when the desired rows are selected.



Configure > Network Configuration > Configure Network Settings   Current Access Point Scope: All Access Points

1 **Select Access Points** 2 Edit Network Settings 3 Apply Settings

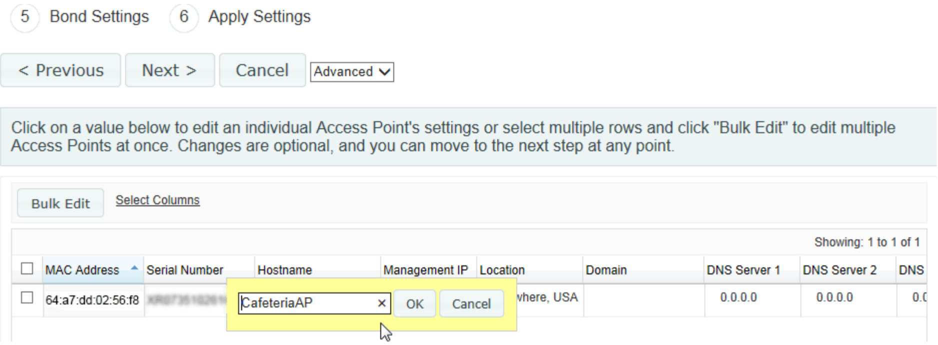
Select the Access Points that you wish to configure network settings for and click Next.

Selected: 1 Clear   Showing: 1 to 2 of 2

☐		Hostname	Management IP Address	Location	Access Point OS Version	Profile
☑	●	CafeteriaAP	192.168.1.86	Anywhere, USA	7.0.0 (Apr 25 2014), Build: 4916-beta	Common
☐	●	factoryap	192.168.1.84	Anywhere, USA	7.0.0 (Apr 29 2014), Build: 4917-beta	Common

Figure 102. Configure Network Settings Page (Advanced)

2. **AP Network Settings:** You may edit the values in the following columns individually: **Hostname**, **Location**, **Domain**, **DNS Server 1**, **DNS Server 2**, **DNS Server 3**. Simply click a table cell that you wish to modify. (Figure 103) A text box will be displayed where you may type the desired value. You may change as many cells in as many rows as you wish. There is no need to click the check boxes on modified rows. Modifications will be highlighted on the page. To set a field to the same value in multiple APs, use the **Bulk Edit** button. See **"To modify multiple rows at once with Bulk Edit" on page 143**.



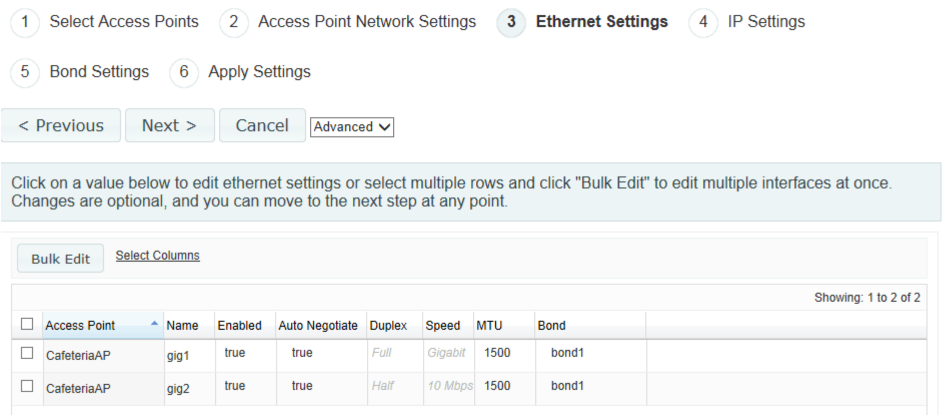
Click on a value below to edit an individual Access Point's settings or select multiple rows and click "Bulk Edit" to edit multiple Access Points at once. Changes are optional, and you can move to the next step at any point.

□	MAC Address	Serial Number	Hostname	Management IP	Location	Domain	DNS Server 1	DNS Server 2	DNS
□	64:a7:dd:02:56:f8	[redacted]	CafeteriaAP		vhere, USA		0.0.0.0	0.0.0.0	0.(

Figure 103. Editing the AP Network Settings Page (Advanced)

Click **Next>** when done.

3. **Ethernet Settings:** You may edit the values in the following columns (individually or using the Bulk Edit button, as described above): **Enabled**, **Auto Negotiate**, and **MTU**. If **Auto Negotiate** is disabled, then you may also modify **Duplex** and **Speed**.



Click on a value below to edit ethernet settings or select multiple rows and click "Bulk Edit" to edit multiple interfaces at once. Changes are optional, and you can move to the next step at any point.

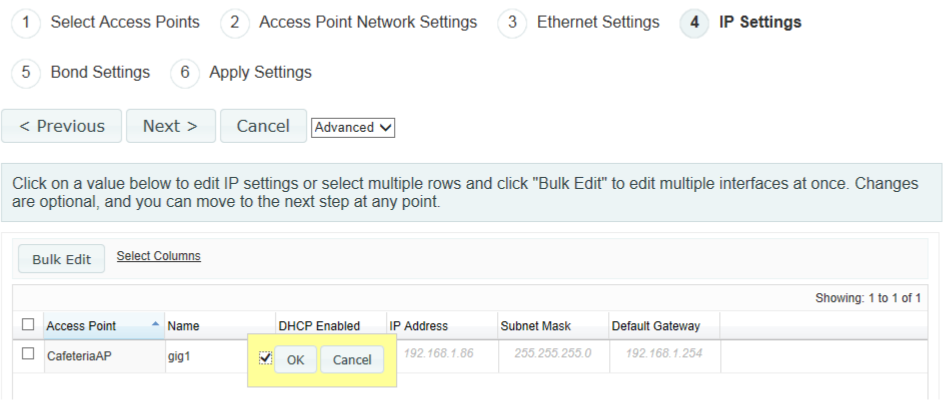
Showing: 1 to 2 of 2

□	Access Point	Name	Enabled	Auto Negotiate	Duplex	Speed	MTU	Bond
□	CafeteriaAP	gig1	true	true	Full	Gigabit	1500	bond1
□	CafeteriaAP	gig2	true	true	Half	10 Mbps	1500	bond1

Figure 104. Editing the AP Network Settings Page (Ethernet)

Click **Next>** when done.

4. **IP Settings:** You may edit the values in the following columns (individually or using the Bulk Edit button, as described above): **DHCP Enabled**, **IP Address**, **Subnet Mask**, **Default Gateway**. Note that **DHCP Enabled** must be **false** in order to edit any of the other three columns.



Click on a value below to edit IP settings or select multiple rows and click "Bulk Edit" to edit multiple interfaces at once. Changes are optional, and you can move to the next step at any point.

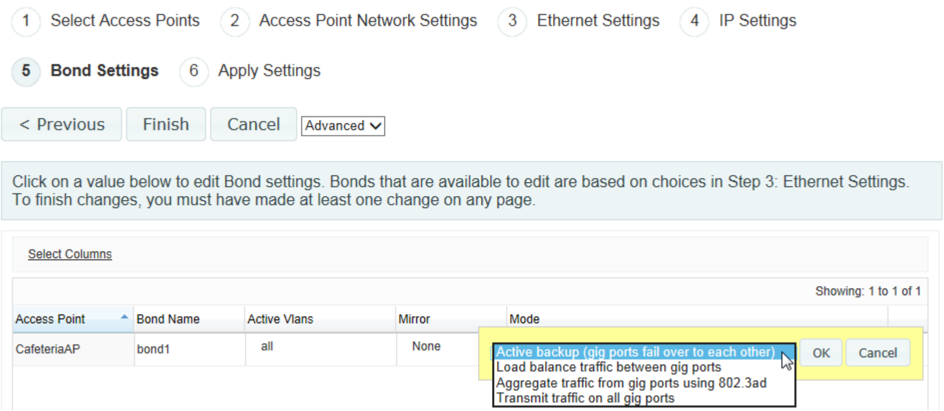
Showing: 1 to 1 of 1

□	Access Point	Name	DHCP Enabled	IP Address	Subnet Mask	Default Gateway
□	CafeteriaAP	gig1	☑	192.168.1.86	255.255.255.0	192.168.1.254

Figure 105. Editing the AP Network Settings Page (IP)

Click **Next>** when done.

5. **Bond Settings:** You may edit the values in the following columns (individually or using the Bulk Edit button, as described above): **Mode**. See **“Bonds and Bridging” on page 379** for an explanation of the **Port Mode** options.


1 Select Access Points
2 Access Point Network Settings
3 Ethernet Settings
4 IP Settings
5 Bond Settings
6 Apply Settings
< Previous
Finish
Cancel
Advanced
Select Columns
Showing: 1 to 1 of 1
OK
Cancel
Active backup (gig ports fail over to each other)
Load balance traffic between gig ports
Aggregate traffic from gig ports using 802.3ad
Transmit traffic on all gig ports

Click on a value below to edit Bond settings. Bonds that are available to edit are based on choices in Step 3: Ethernet Settings. To finish changes, you must have made at least one change on any page.

Access Point	Bond Name	Active Vlans	Mirror	Mode
CafeteriaAP	bond1	all	None	Active backup (gig ports fail over to each other)

Figure 106. Editing the AP Network Settings Page (Bond)

Click **Finish** when done. WOS applies the changes to the selected APs.

6. **Apply Settings:** The web client will display the success or failure of the configuration operation on the selected APs.

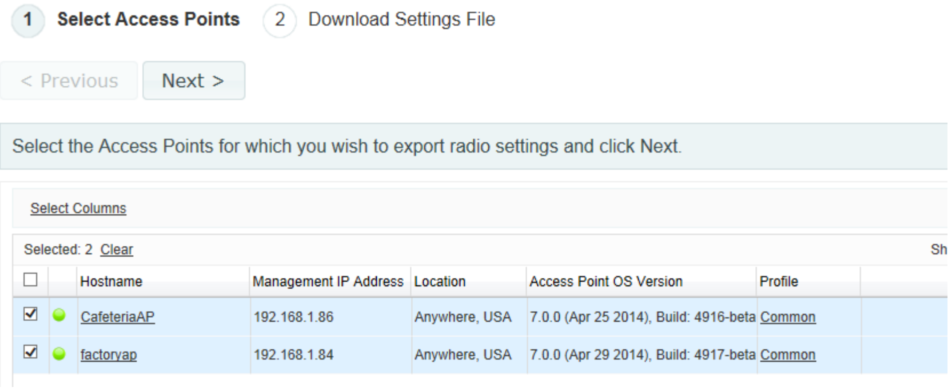
Export Network Settings

This option exports IP and other network settings on selected APs to an Excel file or to a CSV file—a set of comma-separated values that are compatible with Microsoft Excel. This file is useful in a number of ways:

- As a backup of the current configuration, especially since the settings in the file may be imported to restore this configuration.
- To provide Avaya Customer Support with a snapshot of the configuration of your network, at their request.
- You may edit the settings in this file and then import the changed values. Take care only to modify the fields that are editable on the Bulk Configuration page.

To import a file that was exported from the Export Network Settings page, see **"Import Network Settings" on page 152**.

1. **Step 1 - Select APs:** Open the Export Network Settings page by clicking the **Configure** link near the top of the window, then click the **Export Network Settings** link that appears under **Network Configuration**. Note that only APs in the selected **Current AP Scope** are listed.



Select the Access Points for which you wish to export radio settings and click Next.

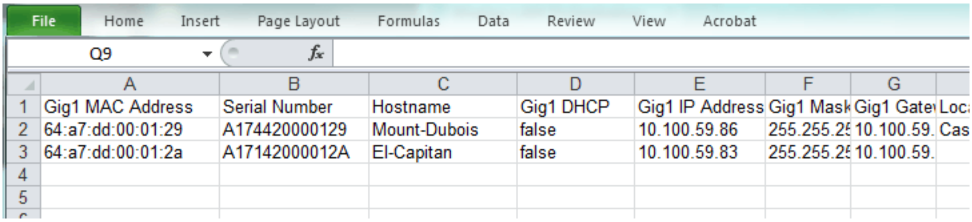
Selected: 2 Clear

□		Hostname	Management IP Address	Location	Access Point OS Version	Profile
☑	●	CafeteriaAP	192.168.1.86	Anywhere, USA	7.0.0 (Apr 25 2014), Build: 4916-beta	Common
☑	●	factoryap	192.168.1.84	Anywhere, USA	7.0.0 (Apr 29 2014), Build: 4917-beta	Common

Figure 107. Export Network Settings

For each row that you wish to export, select the checkbox at the beginning of the row. To select all rows, click the checkbox in the header row. Click again to deselect all rows. (**Figure 107**) Click **Next>** when the desired rows are selected. Only the "Basic" Network Settings columns are exported.

2. **Step 2 - Download Settings File:** Select the desired output file format: **Excel** or **CSV**, and change the **File name** for the download as desired. Click the **Export** button again to browse to the destination folder and filename.



	A	B	C	D	E	F	G	
1	Gig1 MAC Address	Serial Number	Hostname	Gig1 DHCP	Gig1 IP Address	Gig1 Mask	Gig1 Gatev	Loc:
2	64:a7:dd:00:01:29	A174420000129	Mount-Dubois	false	10.100.59.86	255.255.25	10.100.59.	Cas
3	64:a7:dd:00:01:2a	A17142000012A	El-Capitan	false	10.100.59.83	255.255.25	10.100.59.	
4								
5								

Figure 108. Exported Network Settings File

3. You may choose to save the results in a file or open them in Excel. Click **Cancel** when done to close the Export dialog.

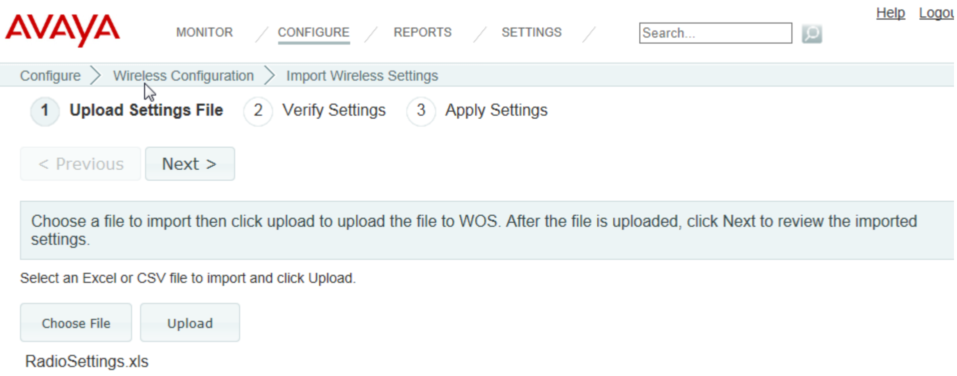
Import Network Settings

This option allows you to change IP and other network settings on APs by importing a file that was exported from the Export Network Settings page. See "Export Network Settings" on page 149 for instructions on exporting settings to a file.

1. **Step 1 - Upload Settings File:** Open the Import Network Settings page by clicking the **Configure** link near the top of the window, then click the **Import Network Settings** link that appears under Network Configuration.

   Click **Choose File**, and browse to the desired .xls or .csv file. (Figure 109) Next, click the **Upload** button.

   Click **Next>** when the **Upload Complete** message appears.



Choose a file to import then click upload to upload the file to WOS. After the file is uploaded, click Next to review the imported settings.

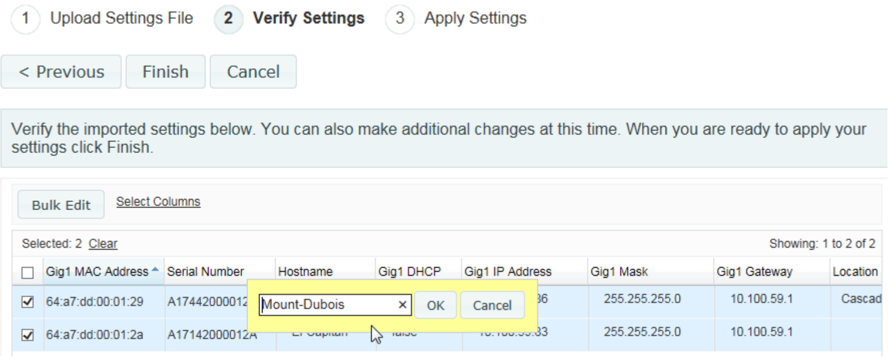
Select an Excel or CSV file to import and click Upload.

RadioSettings.xls

Figure 109. Import Network Settings

2. **Step 2 - Verify Settings:** This page lists network settings for all of the APs that were included in the imported file. (Figure 110) Review these values carefully. Click a setting to change it. An edit field will appear if the setting is modifiable. There is also a **Bulk Edit** option which may be used as described in "To modify multiple rows at once with Bulk Edit" on page 143. Note that you don't need to click the checkboxes at the front of the rows to be changed unless you are using the Bulk Edit option.

   Click the **Finish** button when you are done making changes.



Verify the imported settings below. You can also make additional changes at this time. When you are ready to apply your settings click Finish.

Selected: 2 Clear

Showing: 1 to 2 of 2

□	Gig1 MAC Address	Serial Number	Hostname	Gig1 DHCP	Gig1 IP Address	Gig1 Mask	Gig1 Gateway	Location
☑	64:a7:dd:00:01:29	A17442000012	Mount-Dubois		36	255.255.255.0	10.100.59.1	Cascad
☑	64:a7:dd:00:01:2a	A17142000012A	El Capitan	false	10.100.59.33	255.255.255.0	10.100.59.1	

Figure 110. Verify Imported Network Setting Values

3. **Step 3 - Apply Settings:** The web client will apply the changes you entered, and display the success or failure of the configuration operation on the selected APs.

Alarms

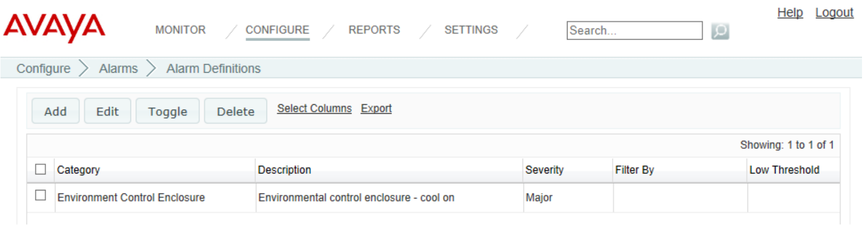
This section includes the following pages:

- Alarm Definitions
- Notification Settings

Alarm Definitions

The Custom Alarms page allows you to define your own alarms. You can instruct WOS to monitor a specified operating condition on all APs and issue an alarm if your stated criteria are met on any AP. For example, you may set application traffic alarms to send a notification when usage of an application or application category exceeds the defined threshold, either system-wide or per-AP.

Open this configuration page by clicking the **Configure** link near the top of the window, then select **Alarm Definitions** from the **Alarms** section. (**Figure 111**) This page lists all of the alarms that you have created.

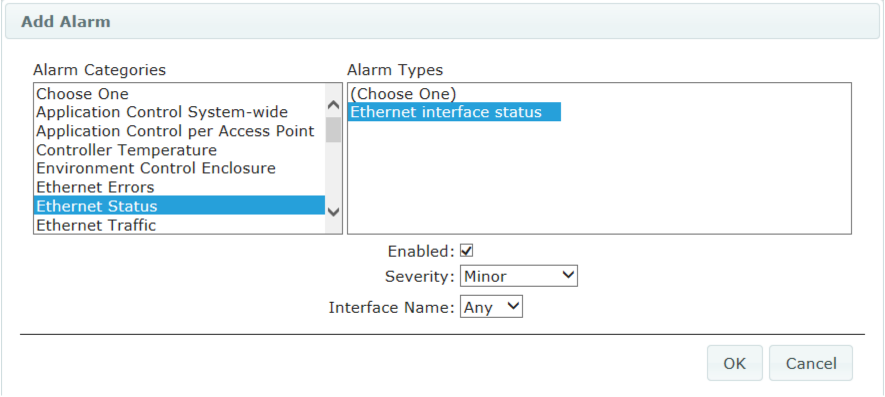


Showing: 1 to 1 of 1

□	Category	Description	Severity	Filter By	Low Threshold
□	Environment Control Enclosure	Environmental control enclosure - cool on	Major		

Figure 111. Custom Alarms Page

Click the **Add** button to display the **Add Alarm** dialog and create a new custom alarm. Select an **Alarm Category** from the list, and one or more **Alarm Types** will be shown based on your selection. (**Figure 112**)



Add Alarm

Alarm Categories

- Choose One
- Application Control System-wide
- Application Control per Access Point
- Controller Temperature
- Environment Control Enclosure
- Ethernet Errors
- Ethernet Status
- Ethernet Traffic

Alarm Types

- (Choose One)
- Ethernet interface status

Enabled: ☑

Severity: Minor

Interface Name: Any

Figure 112. Add a Discrete Alarm

Choose an **Alarm Type**, and additional fields will be displayed based on your choice. There are two kinds of alarms:

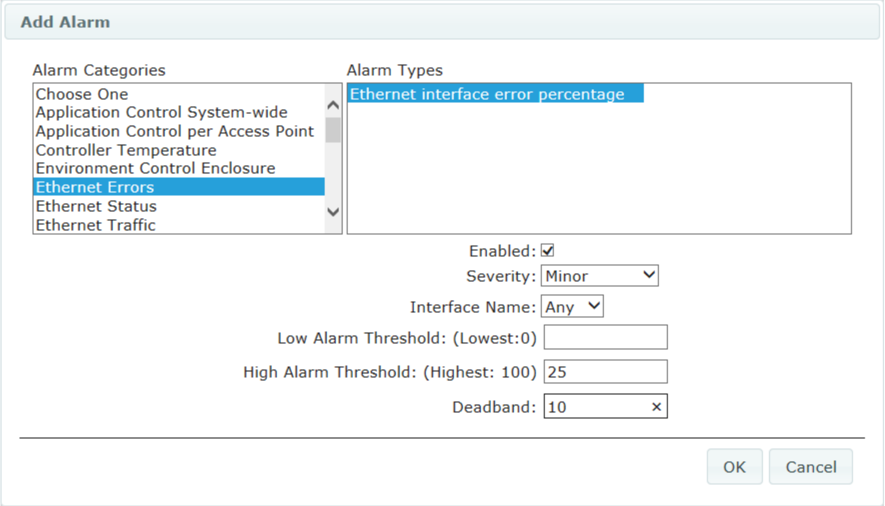
- **Discrete Alarm—**a discrete alarm is issued if the condition described in **Alarm Type** becomes true. For example, in Figure 112, the selected **Alarm Category** is **Radio Status**. If you select **Radio Disabled** as the alarm type, fields will be displayed allowing you to select a specific **Radio Name** to monitor and specify the **Severity** of the resulting alarm. In this example, an alarm will be issued if the specified radio on any managed AP goes down. Note that the radio must transition from enabled to disabled to trigger the alarm, and another alarm will not be triggered for that radio until the radio cycles through the enabled state first. Click the **Enabled** check box to activate your new alarm. Note that you may enter additional custom alarms of the same type to monitor additional named radios.

- **Analog Alarm—**an analog alarm is triggered any time its value is not within the specified range (subject to the deadband restrictions described below). You must specify additional parameters to define a **Low Alarm Threshold** and/or a **High Alarm Threshold**.

  The alarm is triggered when the value is greater than or equal to the upper threshold, or less than or equal to the lower threshold. To clear the alarm, the value must be less than the upper limit minus the deadband, or greater than the lower limit plus the deadband.

For an analog alarm, you may also set a **Deadband** value. This value keeps the alarm from being reissued multiple times by the same event. The default value is 0. The alarm will not be cleared until the value from the AP recovers into the non-alarm range by the amount set in deadband.

For example, in **Figure 113**, the selected **Alarm Category** is **Ethernet Errors**. If you select **Ethernet Interface retry percentage** as the **Alarm Type**, fields will be displayed allowing you to select a specific Ethernet **Interface Name** to monitor, and specify the **Severity** of the resulting alarm. In this example, an alarm will be issued if retry percentage on the specified interface on any managed AP equals or exceeds the **High Alarm Threshold**. If you had also specified a **Low Alarm Threshold**, then reaching or going below that value would also trigger the alarm. The **Deadband** value of 10 ensures that the alarm will not be cleared until the retry percentage recovers an additional 10% back into the non-alarm value range.



Add Alarm

Alarm Categories
- Choose One
- Application Control System-wide
- Application Control per Access Point
- Controller Temperature
- Environment Control Enclosure
- Ethernet Errors
- Ethernet Status
- Ethernet Traffic

Alarm Types
- Ethernet interface error percentage

Enabled: ☑

Severity: Minor

Interface Name: Any

Low Alarm Threshold: (Lowest:0)

High Alarm Threshold: (Highest: 100) 25

Deadband: 10

Figure 113. Add an Analog Alarm

Click the **Enabled** check box to activate your new alarm, and click **OK** when done to save it. Alarm conditions are checked every time the corresponding data is polled. (See **“Polling Settings” on page 589**.)

Looking for Something?

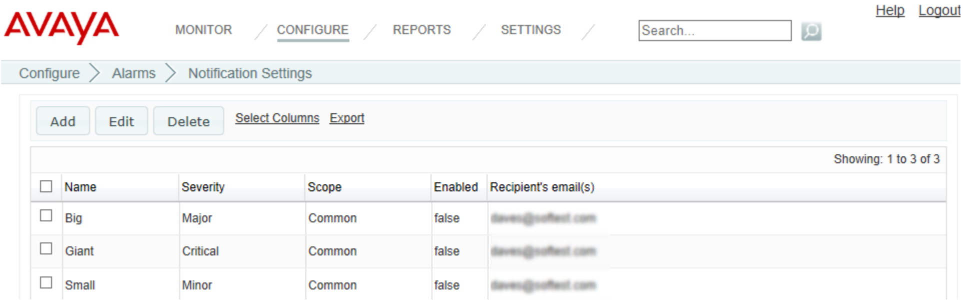
One interesting alarm type may be used to help find iPads and other devices that have gone missing. Under **Alarm Category** select **Station Status**. Then set **Alarm Type** to **Alarm when a particular station is associated to an AP**. Enter the **MAC address** of the missing device. WOS will issue an alarm of the specified **Severity** if the device associates to an AP in the managed network.

Notification Settings

You can set up email notifications to be sent when alarms occur. The email will identify the notifying AP by host name, IP address, and MAC address.

Notifications may be restricted to apply only to a selected AP scope—a set of APs belonging to a selected profile or AP group. For example, say WOS is managing multiple AP networks at sites in different cities, and that you have defined a profile network for each city. When an alarm occurs for an AP, you may wish to notify only the IT personnel managing that AP's site. You may accomplish this by setting up a separate notification for each profile.

Open this configuration page by clicking the **Configure** link near the top of the window, then select **Notification Settings** from the **Alarms** section. (**Figure 114**) This page lists all of the notifications that you have created.



Showing: 1 to 3 of 3

□	Name	Severity	Scope	Enabled	Recipient's email(s)
□	Big	Major	Common	false	[redacted]
□	Giant	Critical	Common	false	[redacted]
□	Small	Minor	Common	false	[redacted]

Figure 114. Alarm Notification Settings

Click the **Add** button to display the **Add Notification** dialog and create a new entry. (**Figure 115**) Enter a meaningful **Notification Name**. Select an alarm

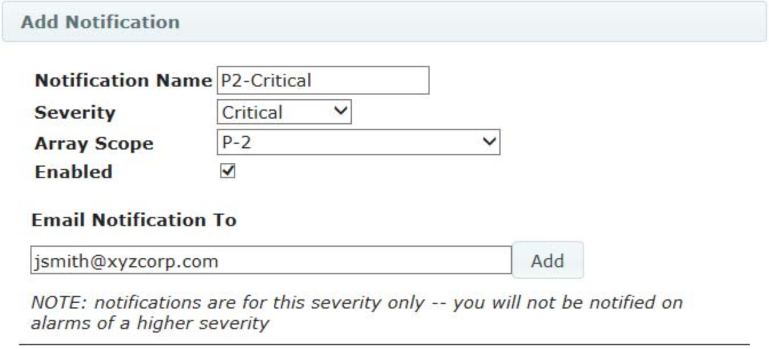
Severity from the list. An *exact match* of this severity level will trigger the notification.

Select the AP **Scope** for this notification. Only alarms on APs that are members of the selected group or profile will trigger this notification. Select **ALL** to allow an alarm of the selected severity on *any* WOS-managed device to send this notification. If you wish to notify one set of personnel about a critical alarm on Profile A, and notify a different set of personnel about a critical alarm on Profile B, then you may simply create a separate notification for each profile by setting the AP **Scope** field appropriately.

Check the **Enabled** checkbox to enable this email notification to be sent when the selected condition occurs. You can use the **Edit** button later to disable and re-enable this notification if desired, without having to delete and re-enter it.

In the **Email Notification To** field, enter a recipient's email address, then click **Add**. You may repeat this step to add additional recipient email addresses. The email addresses will be listed as you add them. To remove an address, click the **X** in front of it. Click **OK** when you are done, and the new notification is complete.

You must specify the SMTP server that WOS will use for sending email notifications, along with the email account to use and the name of the sender. See **"Email Settings" on page 588**.



Notification Name	P2-Critical
Severity	Critical
Array Scope	P-2
Enabled	☑

Email Notification To

jsmith@xyzcorp.com

NOTE: notifications are for this severity only -- you will not be notified on alarms of a higher severity

Figure 115. Add a Notification

You may select an existing entry and modify or delete it using the **Edit** or **Delete** buttons.

Discovery

Use the Discovery configuration pages to enter all the settings necessary to have WOS find the Avaya APs on your wireless network and add them to its database of managed devices. When a device has been discovered, it will appear on the **Access Points** list. You can enter SNMP settings, add devices and networks, and enter AP SSH user information.

For an overview of how discovery adds devices and how SNMP must be configured on APs and on WOS to support it, please see:

- **How Discovery Works**

For a summary of the steps for starting discovery of your network, please see:

- **How to Perform Discovery**

Each of the discovery pages is separately discussed in the following topics:

- **“Add Devices” on page 163**

  Adds a specific device, range of devices, list of devices, or subnetwork to WOS.

- **“SNMPv2 Settings” on page 168**

  Adds or deletes SNMPv2 community names.

- **“SNMPv3 Users” on page 170**

  Adds or deletes SNMPv3 users.

- **“SSH Users” on page 172**

  Add user accounts that WOS can use when it must log in to APs for some management functions.

- **“View Networks” on page 172**

  Adds a subnetwork for WOS to scan for Avaya devices.

- **“What If My Device Is Not Discovered?” on page 174**

  What to do if WOS has not discovered a device that you expected to find on the **Access Points** list.

How Discovery Works

To allow WOS to find an Avaya device, the device must have SNMP enabled and its community string must match one of the strings listed in the Discovery window. See **"SNMPv2 Settings" on page 168**. *The default SNMPv2 community string in WOS matches the AP default value.*

When an AP boots up, it sends an SNMP trap to the WOS server's default hostname, ***Avaya-WOS****. WOS can then add it to its managed devices list. This Phone Home feature requires DNS to resolve the hostname* ***Avaya-WOS*** *correctly. Thus, if you change the host name of the WOS server, you must configure DNS to resolve* ***Avaya-WOS*** *to the actual name of the WOS server host.*

NOTE: *To use SNMPv3 successfully, system time must be set using an NTP server on both the WOS server host machine and all APs using SNMPv3. This is because SNMPv3 requires synchronization between the WOS server and the APs so that the system time difference between them never exceeds more than 150 seconds. If the time difference exceeds 150 seconds, SNMPv3 suspects a security breach and removes the SNMPv3 credentials for affected APs from the database. This means that the AP will appear to be down and statistics will not be polled until the AP is re-discovered. A manual refresh of the AP should remedy the situation. See* **"Add Devices" on page 163**.

WOS has two main ways of getting devices added to its database: the **Phone Home** feature that relies on an AP sending an SNMP trap to the WOS server's hostname, and the **Discovery** tool that uses SNMP.

Phone Home

Any time an AP boots up or its IP address changes, it announces its presence on the network. It does this by sending an SNMP trap to the WOS server's default hostname, **Avaya-WOS** (this name is not case-sensitive). WOS can then communicate with the device, and add it to the **Access Points** window. The Phone Home feature requires DNS to be properly configured in the network, so that the hostname **Avaya-WOS** can be resolved to the IP address of the WOS server.

As soon as a new device is plugged in, it “adds itself” to WOS without waiting for the next time discovery is run on the network. This reduces network overhead by greatly reducing the need for discovery and the traffic overhead that accompanies the process. Any devices that phone home to WOS are added to the **Access Points** window and become part of the WOS **managed network**.

Discovery

WOS’s discovery feature uses SNMP to find networks and devices that are reachable from the server’s network. Despite the advantages of the Phone Home feature, discovery is still needed when you first start using WOS. Discovery will find your current network of Avaya devices, without waiting for them to announce themselves as a result of being booted up. In some networks, discovery must be used because DNS is not configured to allow devices to resolve the hostname **Avaya-WOS**.

If you do not have a valid license for the WOS server, you are limited to managing one AP. when WOS has discovered the maximum permitted number of APs, no additional APs will be discovered.

APDevices that do not have SNMP enabled will **not** be discovered by WOS—in this case, go to **“Single Device (Figure 117)” on page 163**.

Once a discovered network or device is included in the list of managed items, you can then modify (edit) or delete the item, as needed. Only devices that are included in the list of manageable items on the **Access Points** list can be managed by WOS. Only APs that are listed can be added to maps that you create.

How to Perform Discovery

This section provides a quick summary of the steps required to start adding devices to WOS.

Once started, this process uses SNMP to automatically find Avaya APs in the subnets that you specify. (**Figure 116**) No networks are discovered by default, so you must add the subnets containing your APs.

1. To add **SNMPv2 Community Names** or **SNMPv3 Users** to match the strings being used by your devices, click **SNMPv2 Settings** or **SNMPv3**

Users. For WOS to discover and manage a device, the device must have SNMP v2 and/or v3 enabled. The device's SNMPv2 community string or SNMPv3 read-write authentication settings must match one of those defined here for discovery.

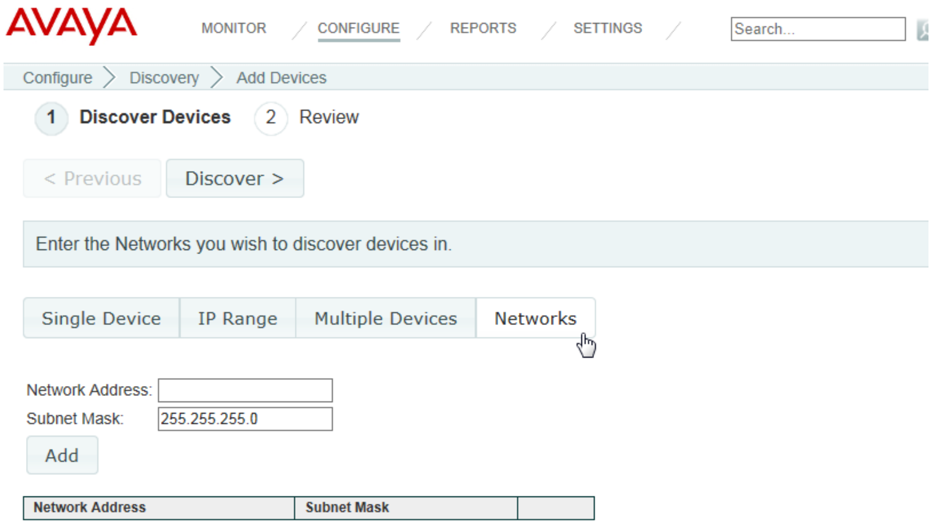
The default SNMPv2 community name (**private**) allows WOS to discover new APs that still have default SNMP settings (SNMPv2 is enabled by default with its **Read Write Community String** set to **private**).

Enter the appropriate SNMP settings. For more details, see **"SNMPv2 Settings" on page 168**.

2. To add networks to be discovered, click the **Add Devices** link under **Discovery**. (**Figure 116**) When the page appears, click the **Networks** button as shown. In the **Network Address** field, enter the subnet's **Network Address** and **Subnet Mask** and click **Add**. Use the subnet mask to define the addresses for discovery as narrowly as possible, to avoid creating excess traffic by discovering a needlessly large network. Add additional subnets as required. Note that the newly entered networks are displayed in the list of networks for discovery. Click **Discover>** so that the discovery process will be initiated.

   Discovery begins soon after adding a network.

   To add individual APs or power supplies, use the **Single Device** or **Multiple Devices** link instead.



Enter the Networks you wish to discover devices in.

Network Address:

Subnet Mask: 255.255.255.0

Network Address	Subnet Mask	

Figure 116. Discovering Networks

Add Devices

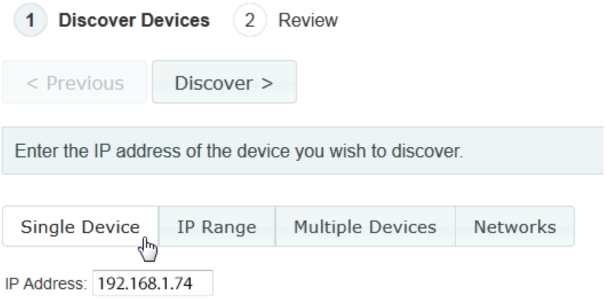
This page is used to add subnetworks or devices to WOS. It allows a great deal of flexibility in adding devices. You may individually add one or more devices to WOS, rather than specifying a network and having WOS discover them. You may enter a single device IP address, a range of addresses, or a list of addresses. The list option is especially useful if you have an Excel spreadsheet with a list of APs and their addresses. Simply copy and paste the single column that has the device IP addresses. You may also add subnetworks for discovery.

Open this configuration page by clicking the **Configure** link near the top of the window, then select **Add Devices** from the **Discovery section**.

Select whether to add a **Single Device**, an **IP Range**, **Multiple Devices,** or **Networks** by clicking the appropriate tab.

- **Single Device (Figure 117)**

  Enter the **IP Address** of the single device to be added to WOS. Click the **Discover** button.

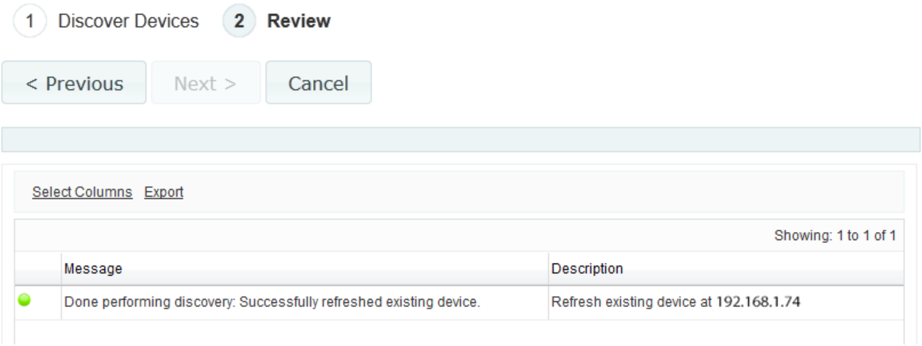


Enter the IP address of the device you wish to discover.

IP Address: 192.168.1.74

Figure 117. Discover a Single Device

WOS will display the results of discovery for the device. (**Figure 118**)



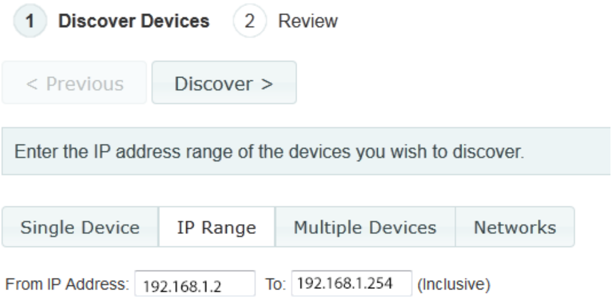
Showing: 1 to 1 of 1

	Message	Description
●	Done performing discovery: Successfully refreshed existing device.	Refresh existing device at 192.168.1.74

Figure 118. Discovery Results—Single Device

- **IP Range (Figure 119)**

  Enter the start of the range in the **From IP Address** field. Enter the end of the range in the **To** field. WOS will check every address in the range, up to and including the **To** address. Click the **Discover** button. At each address, if it finds an Avaya AP, WOS will add the device to its list of discovered devices.



Enter the IP address range of the devices you wish to discover.

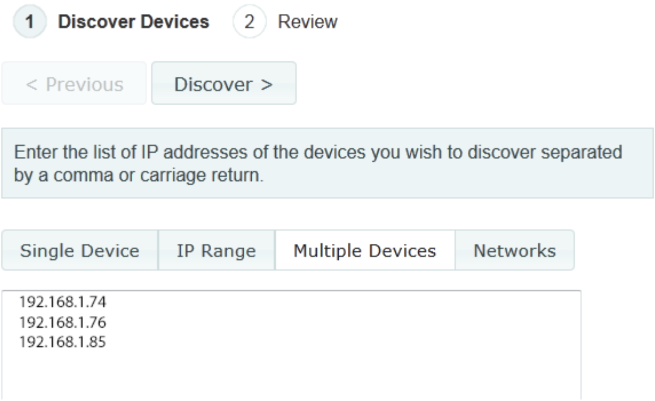
From IP Address: 192.168.1.2 To: 192.168.1.254 (Inclusive)

Figure 119. Discover a Range of IP Addresses

WOS will display the results of discovery for the IP range. You may click the **Cancel** button to stop discovery. (Figure 118) Canceling will not remove devices that have already been discovered for this range.

- **Multiple Devices (Figure 120)**

  Type or paste a list of as many IP addresses as you like in the box, separated by commas or carriage returns. You may paste a list of IP addresses obtained from an Excel .csv (comma-separated values) file. Click the **Discover** button. WOS will check every address in the list. At each address, if it finds an Avaya AP, WOS will add the device to its list of discovered devices.



Enter the list of IP addresses of the devices you wish to discover separated by a comma or carriage return.

192.168.1.74
192.168.1.76
192.168.1.85

Figure 120. Discover a List of IP Addresses

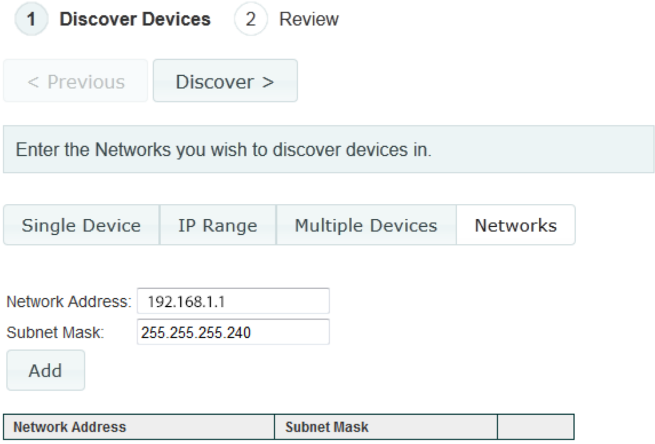
WOS displays the results of discovery, listing whether it succeeded or failed at each address. If discovery fails at an address, WOS will still try all the rest of the addresses that you entered. Note that if you enter a device that is already in the WOS database, WOS will attempt to "refresh" the device by obtaining up-to-date information about it.

You may use the **Cancel** button if you wish to abort discovery while still in progress. This will stop WOS from finding any additional devices, but will not remove any devices that have just been discovered.

- **Networks (Figure 121)**

  Enter the subnet's **Network Address** and **Subnet Mask**, then click **Add**. Continue adding subnetworks as required. Click **Discover** to initiate the discovery process. The newly entered network will be displayed in the list of networks for discovery.

  Be careful to specify the smallest subnet that includes the devices, to avoid creating excess traffic by discovering a needlessly large network. Take care not to accidentally specify a Class A network.



Enter the Networks you wish to discover devices in.

Network Address: 192.168.1.1

Subnet Mask: 255.255.255.240

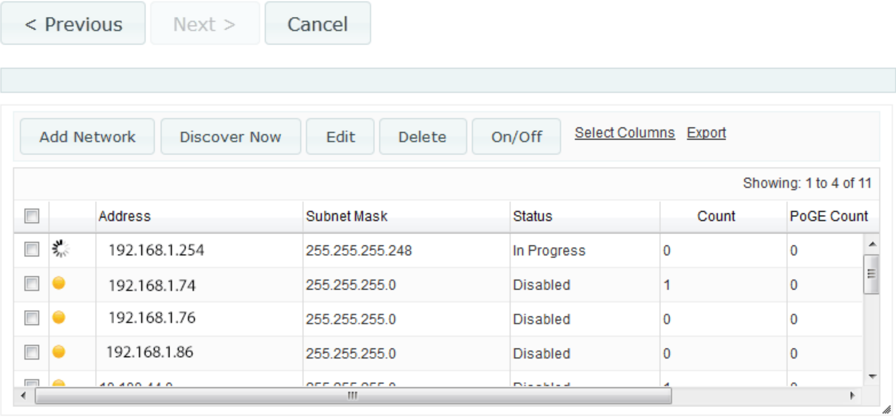
Network Address	Subnet Mask	

Figure 121. Discover Networks

After you click the **Discover** button, WOS will attempt to discover an Avaya AP or managed power supply at all of the IP addresses in the specified subnetworks. It will display the results for each network, listing whether discovery is **In Progress**, **Completed**, **Disabled**, or **Failed**. **(Figure 122)**

You may use the **Cancel** button if you wish to abort discovery while still in progress. This will stop WOS from finding any additional devices, but will not remove any devices that have just been discovered.

If WOS has not discovered a device that you expected to find on the **Access Points** list, see **"What If My Device Is Not Discovered?" on page 174**.



Showing: 1 to 4 of 11

□		Address	Subnet Mask	Status	Count	PoGE Count
□		192.168.1.254	255.255.255.248	In Progress	0	0
□	●	192.168.1.74	255.255.255.0	Disabled	1	0
□	●	192.168.1.76	255.255.255.0	Disabled	0	0
□	●	192.168.1.86	255.255.255.0	Disabled	0	0

Figure 122. Review Results of Adding Devices

From the discovery results window, you may click the **Add** button to add more networks. **Discover Now** will restart discovery on all listed networks. You may check the checkboxes for the desired rows and then do any of the following:

- Click **Edit** to modify the specification of a subnetwork.
- Click **Delete** to remove a subnetwork from discovery from this point onwards.
- Click **On/Off** to enable or disable the discovery of a subnetwork, without deleting the entry. Discovery occurs on a daily basis if the network discovery is enabled here.

SNMPv2 Settings

For a device to successfully ***Phone Home*** *(announce its presence to WOS) or be discovered, SNMPv2 must be enabled on the device. For SNMPv2, the read-write community string (i.e., community name) must match one of the strings listed in the Discovery window.*

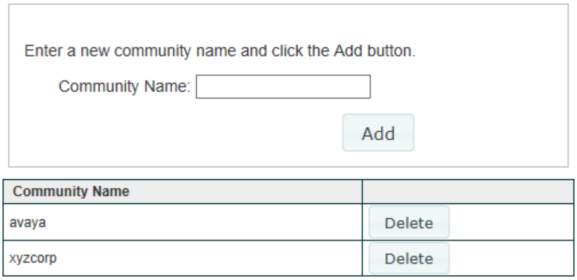
This page is used to add or delete SNMPv2 community names.

The WOS discovery process searches networks using both SNMPv2 and SNMPv3. Discovery will search for devices using SNMPv3 first. See **"SNMPv3 Users" on page 170** for more information. When an AP is discovered using SNMPv3, then WOS uses that version for communication with the AP from then on. When an AP is discovered via SNMPv2, then WOS uses SNMPv2 to communicate with the device.

WOS discovery has default SNMPv2 entries which match the factory default SNMP v2 settings in APs. However, for proper security on your Avaya devices, we recommend that you improve security on Avaya devices by entering your own SNMPv2 community strings and/or SNMPv3 user names and passwords. Thus, you must add those community strings or user names/passwords to WOS for discovery to find those devices.

To add an **SNMPv2 Community Name**, click the **Configure** link near the top of the window, then click the **SNMPv2 Settings** link in the **Discovery** section. (**Figure 123**)

Enter the new **Community Name** and click **Add**. The new **Community Name** will be added to the list, located under the dialog box.



Enter a new community name and click the Add button.

Community Name:

Community Name	
avaya	Delete
xyzcorp	Delete

Figure 123. SNMPv2 Settings

The next time that the discovery process runs after adding a new SNMP v2 entry, WOS will use all of the Community Names listed. Adding or deleting a name on a list will not trigger discovery to run immediately. The new name will be used by the next discovery process (but will not be used now, if discovery is currently running). To trigger a discovery process using the new entry, use the **Discover Now button** described in **“View Networks” on page 172**.

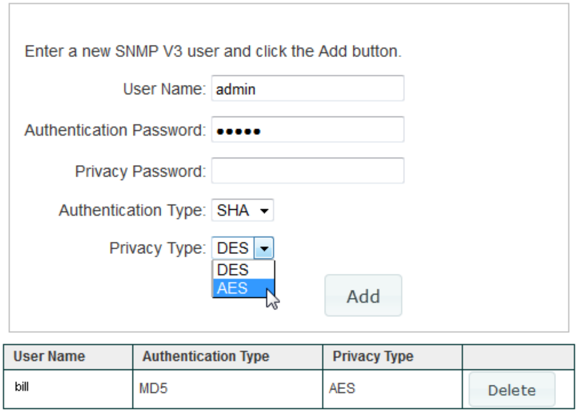
To delete an entry from the list, click the **Delete** button to its right. You will be asked to confirm the deletion. The next time that the discovery process runs, it will use the Community and User Names listed at that time. Note that discovery will not remove devices from its device list if they have a community name that was deleted. Once a device is discovered, it stays on the device list even if you remove the community or user name or disable discovery. The device remains until you delete it manually. You cannot modify an entry in the Community Names list, but you may delete it and then add the new value. The next time that the discovery process runs, it will use the new value. WOS will continue to manage the device using the original community name as long as the device is still configured to use it.

SNMPv3 Users

This page is used to add or delete SNMPv3 users. The WOS discovery process searches networks using both SNMPv2 and SNMPv3. Since SNMPv3 offers improved security, this version is recommended if you need an added layer of security. Note that SNMPv3 has an overhead for encryption, so it will have an impact on larger systems.

WOS discovery searches for devices using SNMPv3 first. If an AP is discovered using SNMPv3, then WOS uses that version for communication with the AP from then on.

WOS discovery has default SNMPv2 entries which match the factory default SNMPv2 settings in APs. However, for proper security on your Avaya devices, we recommend that you improve security on Avaya devices by entering your own SNMPv2 community strings and/or SNMPv3 user names and passwords. Thus, you must add those community strings or user names/passwords to WOS for discovery to find those devices.



Enter a new SNMP V3 user and click the Add button.

User Name:	admin
Authentication Password:	●●●●●
Privacy Password:	
Authentication Type:	SHA
Privacy Type:	DES

User Name	Authentication Type	Privacy Type	
bill	MD5	AES	Delete

Figure 124. SNMPv3 Users

NOTE: *Both WOS and Avaya APs have matching default SNMPv3 usernames and passwords. The default read-write username and password are* ***avaya-private****; the default read-only username and password are* ***avaya-public****.*

To add an **SNMPv3 User**, open this configuration page by clicking the **Configure** link near the top of the window, then select **SNMPv3 Users** from the **Discovery section**. (**Figure 124**)

Enter the new **User Name,** and **Authentication** and **Privacy Passwords**. Set the **Authentication Type** to match your APs. Select the **Privacy Type**: **DES** or **AES**. Click **Add** when done. The new user will be added to the list, located under the dialog box.

The next time that the discovery process runs after adding a new SNMP v2 or v3 entry, WOS will use all of the Community Names and Users listed. Adding or deleting a name on a list will not trigger discovery to run immediately. The new name will be used by the next discovery process (but will not be used now, if discovery is currently running). To trigger a discovery process using the new entry, use the **Discover Now** button described in **"View Networks" on page 172**.

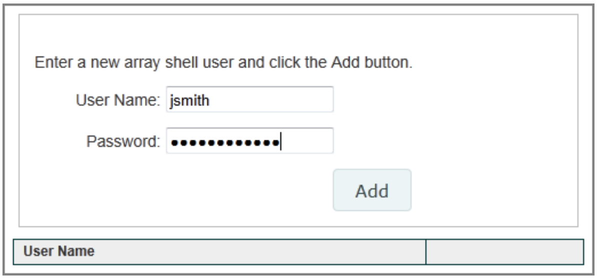
To delete an entry from the list, click the **Delete** button to its right. You will be asked to confirm the deletion. The next time that the discovery process runs, it will use the User Names listed at that time. Note that discovery will not remove devices from its device list if they have a user name that was deleted. Once a device is discovered, it stays on the device list even if you remove the user name or disable discovery. The device remains until you delete it manually. You cannot modify an entry in the User Names list, but you may delete it and then add the new value. The next time that the discovery process runs, it will use the new value. WOS will continue to manage the device using the original user name as long as the device is still configured to use it.

SSH Users

Some setting changes, such as **Perform or Schedule Upgrade**, require APs to download files. When it instructs an AP to fetch a file from the server, WOS must log in to the AP shell. Depending on the configuration of the AP, authentication may use the AP's local accounts or may use a RADIUS server. In either case, the WOS server needs to know a **Username** and **Password** to gain access to the AP shell.

To define this AP login information, use the **SSH Users** page. Click the **Configure** link near the top of the window, then click the **SSH Users** link under **Discovery**. (**Figure 125**)

Enter an AP's **User Name** and **Password**, and click **Add**. The new entry will appear in the AP Shell Authentication list, located under the dialog box. You may use the **Delete** button to remove a selected entry, if necessary.



Enter a new array shell user and click the Add button.

User Name: jsmith

Password: ••••••••••••

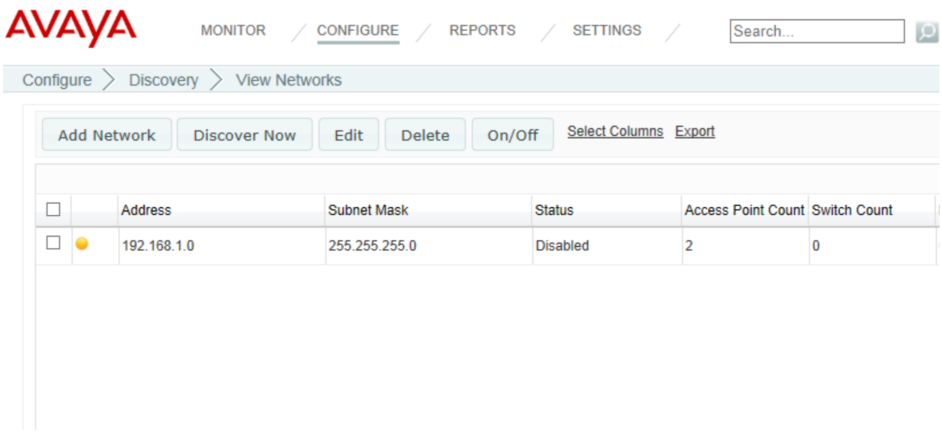
Figure 125. Adding SSH Users

These authentication entries are not used by the discovery process itself, but are managed on this page for convenience. When WOS needs to log in to an AP's shell, it tries entries from the list until it finds one that works. Then it will remember to use this login for this AP. On future login attempts to the same AP, it will try the remembered login first.

View Networks

To view discovered networks, click the **Configure** link near the top of the window, then click **View Networks** from the **Discovery** section. (**Figure 126**)

This page is very similar to the page shown in **Figure 122 on page 167**.



□		Address	Subnet Mask	Status	Access Point Count	Switch Count
□	●	192.168.1.0	255.255.255.0	Disabled	2	0

Figure 126. View Discovered Networks

The list of networks for discovery shows the following information.

- **Address—**the **Network Address** that you entered. The icon to the left of the address is green if you enabled **Start Discovery**, and yellow if you have disabled discovery for this network. Note that you may use the **Edit** button to toggle **Start Discovery**.
- **Subnet Mask—**the mask that you entered.
- **Status—**the status of the discovery process. The status may be **Finished** (discovery complete), **Disabled** (Start Discovery not enabled for this network), or **In Progress** (discovery is still in progress for this network).
- **AP Count—**the number of APs discovered on this network so far.
- **Legacy AP Count—**the number of non-Avaya APs discovered on this network so far. (Devices will only be discovered if they use a standard MIB.)

The toolbar above the list of networks provides a number of functions:

- **Add Network—**add a network for discovery (enter **Network Address**, **Subnet Mask**, and whether **Start Discovery** is enabled).

- **Discover Now—**click this button to start discovery immediately. This will start discovery on the selected networks only. You may use this to rediscover a network.
- **Edit—**to change a network (**Network Address**, **Subnet Mask**, and whether **Start Discovery** is enabled), select the network and click **Edit**.
- **Delete—**to remove networks, select the desired networks and click **Delete**. You will be asked to confirm the deletion.
- **On/Off—**this button toggles whether **Start Discovery** is enabled on the selected networks. If you use this button to enable **Start Discovery**, then the discovery process will be started immediately on the selected networks.

Note that discovery will not remove devices from the WOS database if you delete their network, if they are on a network where discovery has been disabled, or if you have edited the IP address so that their original network is no longer listed for discovery. Devices remain on the list until you delete them manually.

What If My Device Is Not Discovered?

If you do not have a valid license for the WOS server, you are limited to managing one AP. Valid WOS licenses are typically for a particular number of AP radios. In either case, when WOS has discovered the maximum permitted number of radios, no additional APs will be discovered. See **"Managing the WOS Server License" on page 610***.*

WOS Discovery will find devices that are reachable from the WOS server's network if their SNMP settings match those configured on the WOS server. If your AP has not been discovered, check the following.

1. Have you discovered the maximum number of APs allowed by your WOS license?
2. Is the device powered up and fully booted?
3. For an AP—is SNMP enabled?
4. Does the WOS server have connectivity to the device (i.e., is the device connected and can you ping it?).

5. In the **SNMPv2 Community Names** and **SNMPv3 Users** sections, verify that one of the listed entries matches the SNMP values configured on the device. If not, click **Add** under the appropriate list if you need to create a new entry. It is ***crucial*** that the values used by the device and by WOS match.

6. In the Search Networks section, verify that the subnetwork containing the device is listed, and that it is enabled. If not, click **Add** to enter it. After a few seconds the system generates a message informing you that discovery has started on the newly added network.

7. To launch discovery immediately on a network, see **“Add Devices” on page 163**.

8. You may add a device explicitly, using its IP address. See **“Discover a Single Device” on page 164**. If the device is detected by WOS it is added, otherwise an error message is displayed. In this case, check the IP address that you entered.

Security

This section includes the following pages:

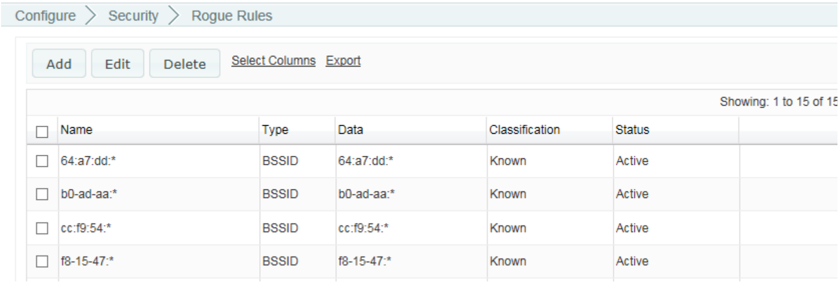
- **Security—Rogue Rules**
- **SSID Spoofing Auto Block**

Security—Rogue Rules

This page sets the signal strength (RSSI) threshold for considering APs to be rogues, and allows you to set up and manage rules to automatically classify rogue APs (see **"Rogues" on page 90**), based on SSID, BSSID, or manufacturer. You may classify rogues as **Blocked**, so that the AP will take steps to prevent stations from associating with the blocked AP. To open this page, click the **Configure** link at the top of the page. Then select **Rogue Rules** from the **Security** section.

To classify current rogues individually rather than using rules as they are discovered, please see **"Rogues" on page 90**. *Note that if a rogue is classified by a rule, it cannot be individually overridden.*

Rogues may be automatically blocked, as described in **"SSID Spoofing Auto Block" on page 180**, *and* **"Intrusion Detection" on page 525**.



Showing: 1 to 15 of 15

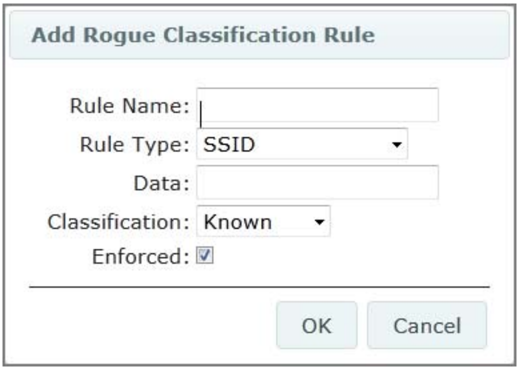
□	Name	Type	Data	Classification	Status
□	64:a7:dd:*	BSSID	64:a7:dd:*	Known	Active
□	b0-ad-aa:*	BSSID	b0-ad-aa:*	Known	Active
□	cc:f9:54:*	BSSID	cc:f9:54:*	Known	Active
□	f8-15-47:*	BSSID	f8-15-47:*	Known	Active

Figure 127. Rogue Rules

To set a threshold signal strength for detection of rogue APs, click the checkbox for **Ignore Rogue APs with RSSI less than:**, then set the desired minimum signal strength. Unknown APs whose RSSI is less than this value will be ignored and will not be added to the Rogues list. This keeps WOS from identifying too many rogues and impacting performance. This feature is enabled by default, with threshold of -80 dBm. Note that if you have upgraded from an earlier release than 7.4, then this feature is off by default, and existing rogues are unaffected regardless of this setting.

Rogue rules allow you to classify groups of devices, rather than classifying each selected device individually. Rules may be enforced (pushed out to all APs) or unenforced, as described later in this section. Rules may be created as described below, or may appear as a result of being read from APs (see **"Populating the WOS Rogues and Rogue Rules Windows" on page 179**). You may edit existing rules, if you wish.

To create a rogue rule, click the **Add** button on the upper left. (**Figure 127**) In the Add Rogue Classification Rule dialog box (**Figure 128**), enter a unique **Rule Name** for your new rule.


Add Rogue Classification Rule

Rule Name:

Rule Type: SSID

Data:

Classification: Known

Enforced: ☑

Figure 128. Adding a Rogue Rule

The **Rule Type** field specifies the characteristic of the rogue to be matched, which determines what to enter in the **Data** field as described below. The wild card character (*) may be used in the Data field for any of the types. **Rule Type** options are:

- **BSSID**—set **Data** to a MAC address (typically including * for a wild card) that describes the devices to be matched. When entering a MAC address, the string often specifies the OUI of a manufacturer—the first three octets of the device MAC address are a unique identifier for the manufacturer. For example, 64:a7:dd, b0-ad-aa, cc:f9:54, f8-15-47, 00:1b:4f, 2c:f4:c5, 5c:e2:86, 58:16:26, 70:52:c5, and 70:38:ee:* are the OUIs of Avaya, so the strings 64:a7:dd:*, b0-ad-aa:*, cc:f9:54:*, f8-15-47:*, 00:1b:4f:*, 2c:f4:c5:*, 5c:e2:86:*, 58:16:26:*, 70:52:c5:*, and 70:38:ee:* will uniquely match all Avaya APs

  To match a device individually (i.e., a specific rogue, rather than a set of rogues specified with a wild card), enter the BSSID (MAC address) of the device, and specify its classification.

- **SSID**—set **Data** to any legal SSID name to be matched. For example, to match the SSIDs named **company-student** or **company-staff**, enter the string **company***.
- **BSSID_OR_SSID**—set **Data** to either of the types above. This type is provided for backwards compatibility with rules that are read from some older APs. Note that rules created on newer APs have a **Match Only** setting that will specify either a BSSID or an SSID, although these APs will still process the old-style rules. On older APs, rules with type set to SSID, BSSID/SSID, or BSSID will all be processed on the AP as though they were BSSID/SSID rules. Rules with type set to Manufacturer will be dropped on older APs. (Manufacturer is supported on Avaya OS 4.0.6 or higher, and on Avaya OS Release 3 builds of 3.5.1 or higher.)
- **Manufacturer**—enter the manufacturer name as an ASCII string.

From the **Classification** drop-down list, select the classification to be applied to these devices. For example, you might set all Avaya APs to **Known**. See **“The Rogues List” on page 91** for an explanation of rogue classifications.

Leave the **Enforced** checkbox checked if you wish to have the rule pushed to all managed APs, otherwise clear the checkbox.

- **Enforced** rules are pushed (sent) to all managed APs to become part of the APs’ Rogue Control Lists. If the AP has a conflicting rule (for the same wildcard pattern, but with a different classification), the WOS rule will replace the AP rule.

- **Unenforced** rules are not pushed to managed APs. This way, if an AP already has a rule for the same BSSID, SSID, or manufacturer, it will not be overridden.

  Keeping unenforced rules in the database provides a single place where you can see a global view of all rules in the managed network, without necessarily applying all the rules universally. You may change a rule to Enforced if you wish.

Click **OK** when done.

To change an existing rule, select it in the list and click **Edit**, or to delete the rule click **Delete**.

Populating the WOS Rogues and Rogue Rules Windows

When the WOS server is first started, the Rogues list is empty (see **"Rogues" on page 90**), and there are only two default rules: all Avaya APs (BSSID 64:a7:dd:*, b0-ad-aa:*, cc:f9:54:*, f8-15-47:*, 00:1b:4f:*, 2c:f4:c5:*, 5c:e2:86:*, 58:16:26:*, 70:52:c5:*, or 70:38:ee:*.) are Known. This rule is Enforced—it is sent out to all APs.

In order to populate the **Rogues** list, WOS fetches the rogue devices and Rogue Control List entries from each discovered AP. Thereafter during operation of WOS, APs are polled for new entries. Also during operation, when a new AP is discovered, WOS fetches its rogue devices and Rogue Control List entries and adds them to its database.

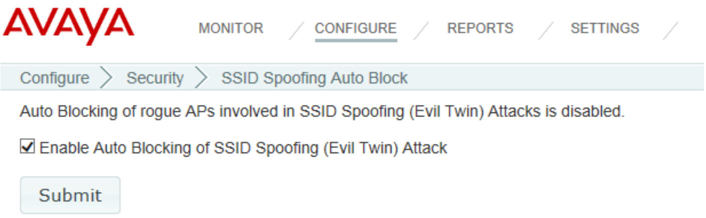
When a classification of an *individual device* is read from an AP and added to the WOS database it is marked as **Enforced**, and thus it will be "pushed" to all managed APs. On the other hand, when a *rule* is read from an AP and added to the WOS database, it is marked as **Unenforced**. This prevents the rule from being sent out to all managed APs, possibly overriding existing rules that were explicitly configured in APs. Once a rule has been added to the WOS database, if additional rules for the same BSSID/SSID are later read from other APs, they are ignored.

If you set a rule to Enforced, it will be sent out to each managed AP and become part of its Rogue Control List.

SSID Spoofing Auto Block

WOS can automatically block rogue APs that launch spoofing (evil twin) attacks on your SSIDs—that is, rogues that impersonate one of your SSIDs. This blocking is performed on a system-wide basis, for all managed APs rather than for a particular AP or Profile network. To enable auto blocking of rogue APs that spoof your SSIDs, check the box for **Enable Auto Blocking of SSID Spoofing (Evil Twin) Attack**. ***Be sure to abide by applicable regulations when using this feature—see the* Caution on page 530.** Clearing the checkbox will disable this feature.

Spoofing is detected by APs managed by WOS. In order to be able to detect this type of attack, APs must have **Intrusion Detection Mode** set to **Standard**, and have detection of **Evil Twin Attacks** enabled. These settings may be made by WOS for individual APs or for Profile networks. See **"Intrusion Detection" on page 525** and **"Profile Details—Configuration" on page 207**.



Auto Blocking of rogue APs involved in SSID Spoofing (Evil Twin) Attacks is disabled.

☑ Enable Auto Blocking of SSID Spoofing (Evil Twin) Attack

Figure 129. Auto Blocking SSID Spoofing Attacks

Suppose you add a new SSID to your AP network and a previously identified rogue AP already has that SSID. If SSID Spoofing Auto Block is enabled, then it will block that SSID on the rogue AP.

For more information about Rogue APs and Auto Blocking, you may also wish to see:

- **"Rogues" on page 90**

- **"Security—Rogue Rules" on page 176**
- **"About Blocking Rogue APs" on page 528**

Access Point Licenses

These pages display and manage the licenses for APs in your Avaya network. You may view the license of each AP and deploy new or upgraded licenses. Working with licenses is described in the following topics:

- **About Licensing and Upgrades**
- **Deployed Licenses**
- **Export Licenses**
- **Import Licenses**
- **Edit Licenses**
- **Pending Licenses**

This section describes using WOS to manage AP licenses. If you are looking for information regarding the WOS server's license, please see **Managing the WOS Server License**.

About Licensing and Upgrades

WOS manages the licenses for large numbers of APs. You can easily view licensing information for your APs and manage individual licenses. The license utility can apply bulk licenses in one step, by simply importing the .csv license file issued by Avaya. Similarly, when it's time to upgrade all of your APs with new features, the required licenses may all be installed in one step.

An AP's license determines many of the features that are available on the AP. For example, Application Control and use of 802.11ac are licensed features. To check the features supported by your license, see the next section—**Deployed Licenses**. For more information on the features that require a license, please see **Licensing** in *Using the Avaya OS for Avaya WLAN AP 9100 Series (NN47252-102)*.

If you are upgrading an AP to add new features that are not supported by your existing license, **the AP must have the new license key that includes the upgraded features before upgrading**.

Optional Licenses

11N to 11AC Upgrade License—WAP9122 and WAP9123 provide customers investment protection with the option to enable 802.11ac capability on the 802.11a/b/g/n radios via optional license purchase. The WAO9122 Access Point does not support the 11AC Upgrade License.

Application Control License—Avaya Application Control functionality can be enabled on all Avaya WAP91XX/WAO91XX Access Points via an optional license purchase.

License Certificate and License Activation Code

Upon fulfillment of the Purchase Order for the optional licenses, you will receive the License Certificate that entitles you to optional licenses on the specified number of Access Points. The License Certificate includes the License Activation Code that is required to generate the licenses on the Avaya WLAN Licensing Portal http://licenses.wifi.avaya.com.

Important: Keep the License Certificate safely for future reference.

Obtaining Software License Keys

To enable the optional licensed capability on the Access Points, you must first obtain software license keys from Avaya and apply them to the Access Points, as described below.

Instructions for Wireless Orchestration System Customers

1. Connect to WOS using a web browser and navigate to **Configure, Access Point Licenses, Export Licenses**.

2. Select the Access Points to which you wish to apply the new 802.11ac Upgrade or Application Control Licenses and click **Next**.

3. Review the **File Name**. Select **Export as CSV** and click the **Export** button. Note the name and location where the CSV file is saved.

4. Connect to Avaya's WLAN 9100 Licensing portal at http://licenses.wifi.avaya.com using a web browser.

5. Fill out the required customer contact details on the Licensing Page and select **Create/Generate Licenses for your 9100 series APs**.

6. Enter the **License Activation Code** listed in the lower right box of the License Certificate and choose **Upload a CSV File that you exported from your WOS-E**.

7. Choose the CSV file exported from WOS in Step 3, and click **Upload**. Then click **Submit** at the bottom of the page.

8. The license file will be sent to the email address entered in the request.

Applying Software Licenses to Access Points

The license keys received via email must be applied to the Access Points to enable the optional capabilities/features.

Instructions for Customers with Wireless Orchestration System

1. Download the License File received to your personal computer. Note down the file name and location.

2. Connect to WOS using a web browser and navigate to **Configure, Access Point Licenses, Import Licenses**.

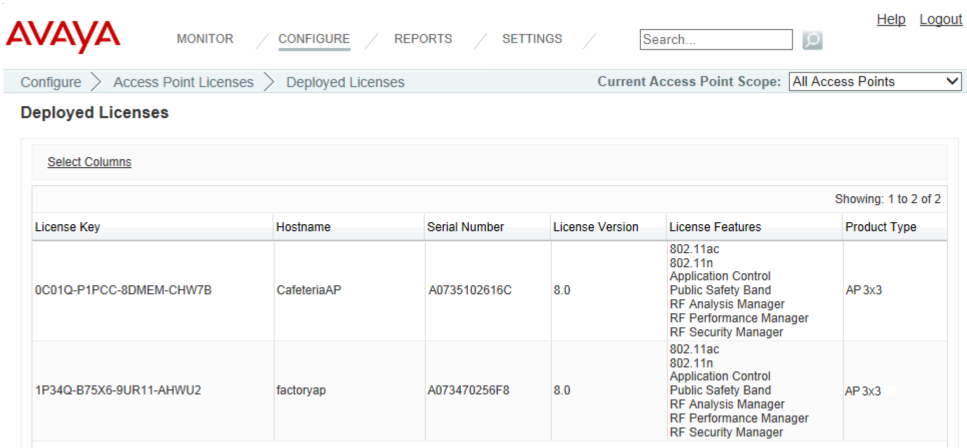
3. Choose the License File saved in Step 1 and click **Upload**. Click **Next** when the upload is complete.

4. Verify that the optional license feature is now included in the License Feature List. Click **Finish**.

5. Navigate to **Configure, Access Points, Deployed Licenses**. Confirm that the Access Points to which the license keys have been applied show that the optional feature is included.

Deployed Licenses

This window is displayed by your browser when you select **Configure** on the top of the window, and then select the **Deployed Licenses** page from the **Licenses** section. Note that only APs in the selected **Current AP Scope** are listed.



Deployed Licenses

Showing: 1 to 2 of 2

License Key	Hostname	Serial Number	License Version	License Features	Product Type
0C01Q-P1PCC-8DMEM-CHW7B	CafeteriaAP	A0735102616C	8.0	802.11ac 802.11n Application Control Public Safety Band RF Analysis Manager RF Performance Manager RF Security Manager	AP 3x3
1P34Q-B75X6-9UR11-AHWU2	factoryap	A073470256F8	8.0	802.11ac 802.11n Application Control Public Safety Band RF Analysis Manager RF Performance Manager RF Security Manager	AP 3x3

Figure 130. AP License Management - Deployed Licenses

Initially, this page displays a list of all *deployed* AP licenses being managed by WOS. This is a list of all discovered APs and their licenses. By default the following is shown for each AP: the **License Key**, the **Hostname** along with the **AP Serial Number**; the **License Version**, **License Features, Product Type**, and **Max Radios** supported by the license, and the license **Expiration** date. You may use the **Select Columns** option to choose which information you wish to display.

The **License Features** column shows the advanced features that are enabled by this license, such as the RF Performance Manager (RPM), RF Security Manager (RSM), RF Analysis Manager (RAM), or IEEE 802.11n or 802.11ac operation.

The following main operations are available for managing licenses:

- Viewing deployed licenses on discovered APs, described above.
- **Export Licenses**
- **Import Licenses**

- **Edit Licenses**
- **Pending Licenses**

If you change a license directly using the CLI or WMI on an AP whose license status is ***Deployed****, WOS will detect the change and display the changed license in the list of deployed licenses.*

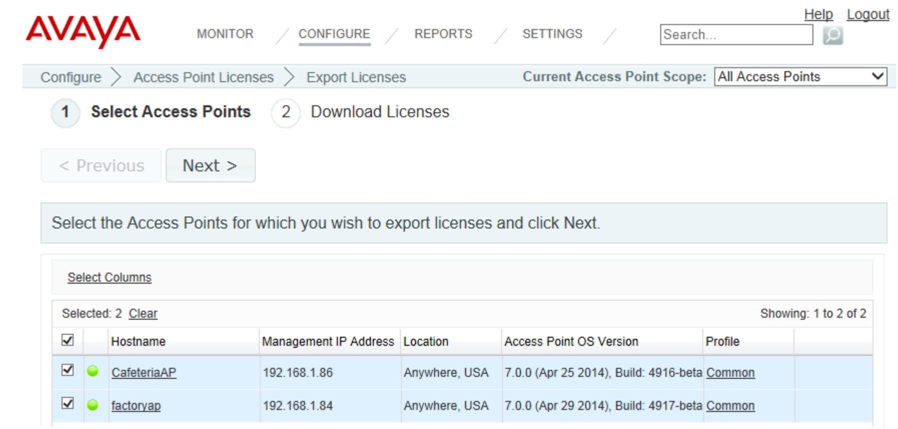
However, if WOS has a license pending for that AP, that license will be deployed as soon as WOS is able to do so, replacing the license in the AP.

Export Licenses

At times, you may wish to export AP licenses to a file. For example, you may want a consolidated record of some or all of your licenses, or Avaya Customer Service may request this information to issue upgraded licenses or resolve a support issue. This feature exports the selected licenses shown on the Deployed Licenses window into a file that can be imported by Excel—either a .csv file or an .xls file. This file may also be used to **Import Licenses**. To export Pending licenses, see **"Pending Licenses" on page 192**.

To export deployed licenses from the web client, select the **Export Licenses** page from the **Licenses** section of the **Configure** menu. Note that only APs in the selected **Current AP Scope** are listed.

To proceed, select the desired licenses by checking them off in the first column. Click the **Next >** button at the top of the page. (**Figure 131**)

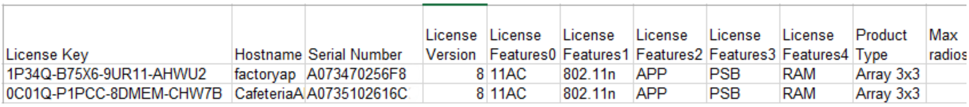


Select the Access Points for which you wish to export licenses and click Next.

☑		Hostname	Management IP Address	Location	Access Point OS Version	Profile
☑	●	CafeteriaAP	192.168.1.86	Anywhere, USA	7.0.0 (Apr 25 2014), Build: 4916-beta	Common
☑	●	factoryap	192.168.1.84	Anywhere, USA	7.0.0 (Apr 29 2014), Build: 4917-beta	Common

Figure 131. Exporting AP Licenses

To export an .xls file, click the **Excel** radio button. To export a file of comma-separated values (.csv), click the **Csv** radio button. Then click **Export**. The File Download dialog box will allow you to open the file, or save it to the location you select.



License Key	Hostname	Serial Number	License Version	License Features0	License Features1	License Features2	License Features3	License Features4	Product Type	Max radios
1P34Q-B75X6-9UR11-AHWU2	factoryap	A073470256F8	8	11AC	802.11n	APP	PSB	RAM	Array 3x3	
0C01Q-P1PCC-8DMEM-CHW7B	CafeteriaA	A0735102616C	8	11AC	802.11n	APP	PSB	RAM	Array 3x3	

Figure 132. Sample Export File

This exports the selected deployed licenses into a file of the selected format. A sample export file is shown in **Figure 132**.

Import Licenses

Use this feature to import a .csv or .xls file with licensing information for any number of APs. For example, to upgrade your entire Avaya wireless network for Application Control, you must first deploy licenses for that feature. Avaya will furnish these licenses to you in the form of an Excel (.csv) file. Simply click to import the file and click **Finish** to deploy the licenses to the appropriate APs.

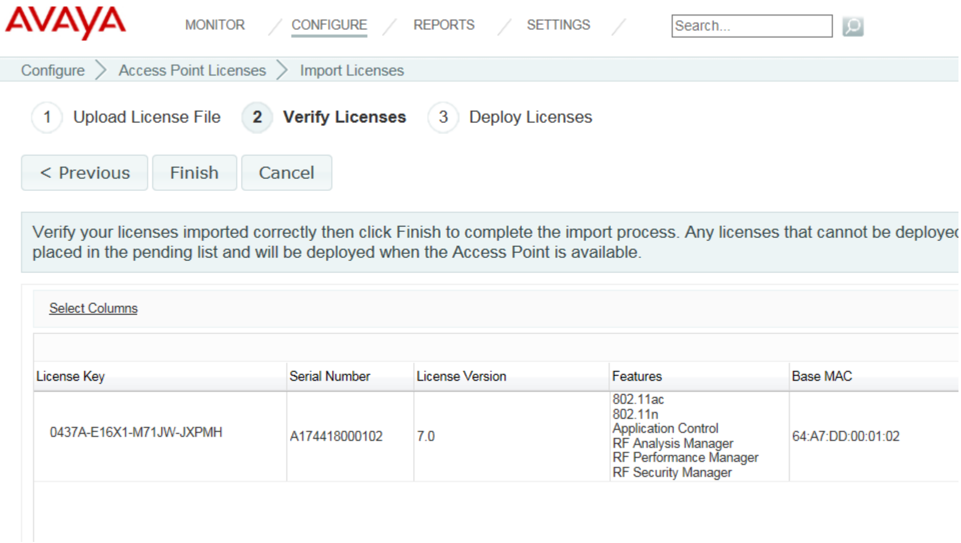
After your license file has been imported, any licenses that are for WOS managed APs (i.e., those that have been discovered) will be deployed to those APs. The AP is not rebooted but the radios will go down and up, so that station associations will be disrupted briefly. The AP will start using the new license, and will support the capabilities shown in the **Features** column.

A license for an AP that is not yet under WOS management will be deployed as soon as the target AP is discovered. Similarly, a license for a managed AP that is down will be deployed shortly after it comes back on line.

To import licenses using the web client, select the **Import Licenses** page from the **Licenses** section of the **Configure** menu. Fields are displayed to allow you to specify the license file.

Click the **Choose file** button to browse to the license file. It must be either an .xls or a .csv (comma-separated values) file. To see an example of the format, you may export a sample license file (see **"Export Licenses" on page 186**). The File Download dialog box will allow you to open the file, or save it to the location you select. Click the **Upload** button. When the upload is complete, click **Next >** at the top of the page.

The imported licenses will be displayed on the Verify Licenses page. Check that the licenses imported correctly. If necessary, you may edit any **License Key** by clicking on it.



Verify your licenses imported correctly then click Finish to complete the import process. Any licenses that cannot be deployec placed in the pending list and will be deployed when the Access Point is available.

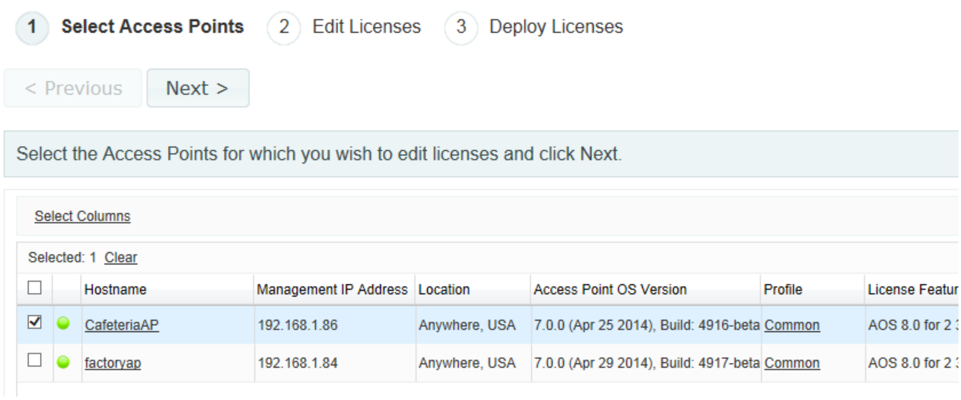
License Key	Serial Number	License Version	Features	Base MAC
0437A-E16X1-M71JW-JXPMH	A174418000102	7.0	802.11ac 802.11n Application Control RF Analysis Manager RF Performance Manager RF Security Manager	64:A7:DD:00:01:02

Figure 133. Importing AP Licenses

Click **Finish** to complete the import process. Any license that cannot be deployed now either because the AP has not yet been discovered by WOS or because the AP is off line will be placed in the pending list and will be deployed when the AP is available. The **Status** field will show the results for each AP.

Edit Licenses

To modify deployed licenses from the web client, select the **Edit Licenses** page from the **Licenses** section of the **Configure** menu to display all deployed licenses. (**Figure 134**) Note that only APs in the selected **Current AP Scope** are listed.



Select the Access Points for which you wish to edit licenses and click Next.

Selected: 1 Clear

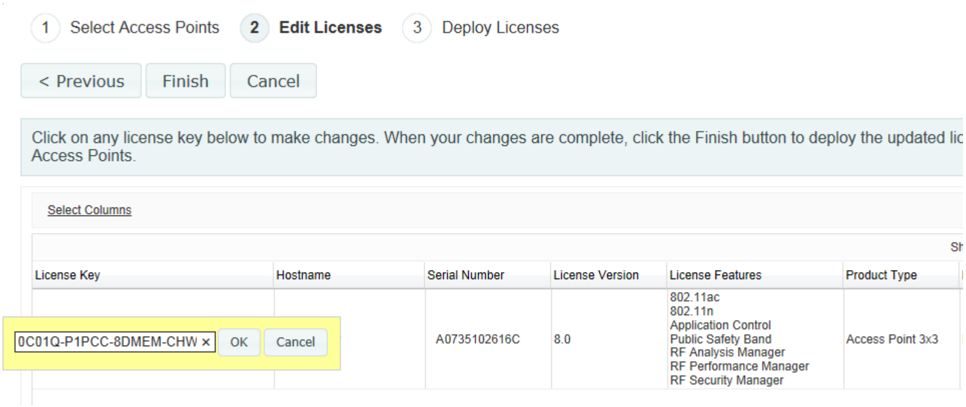
□		Hostname	Management IP Address	Location	Access Point OS Version	Profile	License Featur
☑	●	CafeteriaAP	192.168.1.86	Anywhere, USA	7.0.0 (Apr 25 2014), Build: 4916-beta	Common	AOS 8.0 for 2 :
□	●	factoryap	192.168.1.84	Anywhere, USA	7.0.0 (Apr 29 2014), Build: 4917-beta	Common	AOS 8.0 for 2 :

Figure 134. Select AP Licenses to Edit

Select the licenses to be edited by checking the box to the left of each desired row. To select all entries at once, click the checkbox in the header row. To deselect all entries, click the checkbox in the header row again. When the desired entries are selected, click the **Next >** button at the top of the page. The Edit Licenses page appears. (**Figure 135**)

To modify a license, click the AP's **License Key** field and edit it or type the new license into the field. This is the only field that may be edited. Repeat for as many entries as you need to change.

When you are done editing, click the **Finish** button. The license modifications will be deployed to the selected APs, and the status of the operation will be displayed for each AP.



Click on any license key below to make changes. When your changes are complete, click the Finish button to deploy the updated lic
Access Points.

License Key	Hostname	Serial Number	License Version	License Features	Product Type
0C01Q-P1PCC-8DMEM-CHW		A0735102616C	8.0	802.11ac 802.11n Application Control Public Safety Band RF Analysis Manager RF Performance Manager RF Security Manager	Access Point 3x3

Figure 135. Editing AP Licenses

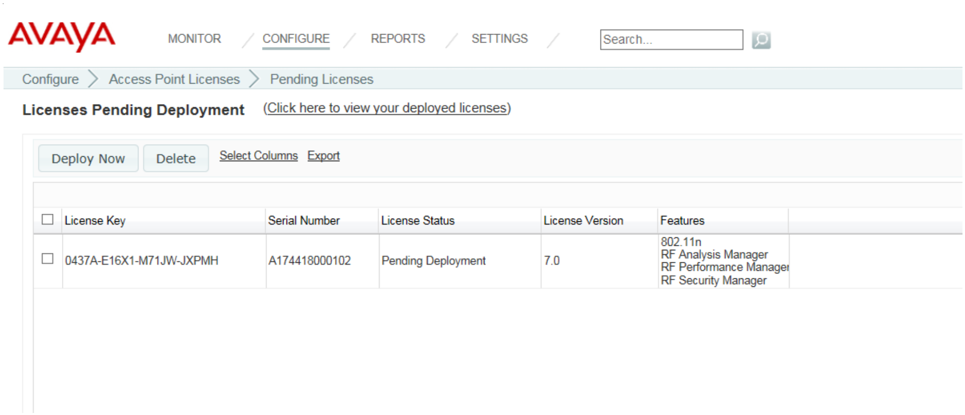
You may not delete deployed licenses, but you may delete those that have not yet been deployed. See **“Pending Licenses” on page 192**.

Also note that you may not enter new licenses “by hand”. To add a new license, please see **“Import Licenses” on page 188** and **“Pending Licenses” on page 192**.

Pending Licenses

Pending licenses are those that WOS has imported but has not yet been able to deploy. Select the **Pending Licenses** page from the **Licenses** section of the **Configure** menu to display all non-deployed licenses that have been imported. (Figure 136)

Note that if an AP is running with a valid license, but a new license was imported for it, it will be listed on both the Deployed Licenses page and the Licenses Pending Deployment page until the new license has been deployed.



Licenses Pending Deployment (Click here to view your deployed licenses)

□	License Key	Serial Number	License Status	License Version	Features
□	0437A-E16X1-M71JW-JXPMH	A174418000102	Pending Deployment	7.0	802.11n RF Analysis Manager RF Performance Manager RF Security Manager

Figure 136. AP Licenses Pending Deployment

License Status may have the following values:

- **AP Not Discovered**—a new license that has not been installed because the designated AP has not been discovered yet (i.e., the AP is not listed in the Access Points page). This does not mean that WOS cannot find the AP in your network, but rather that the discovery process has not yet added it. To add the AP to WOS using the web client, see “Add Devices” on page 163 or “View Networks” on page 172. When the AP is discovered, WOS will automatically check whether there is a license pending for it and if so, will attempt to deploy it.
- **Invalid License Key**—the license is not valid. You may edit the License Key as described in “Edit Licenses” on page 190. Use the **Deploy Now** button to “push” the corrected license to the AP.

- **Pending Deployment**—a previously discovered AP is currently unreachable or down, and WOS cannot deploy the license.

You may use the **Deploy Now** or **Delete** buttons to manage licenses. Select the desired licenses by checking the box to the left of each desired row. To select all entries at once, click the checkbox in the header row. To deselect all entries, click the checkbox in the header row again.

Click the **Deploy Now** button at the top of the page to have WOS immediately attempt to deploy the selected licenses on their target APs. You will be informed of the results of the operation. The **License Status** field will show the results quickly, typically well within a few minutes. If successful, the entry will be moved to the list of deployed licenses. The AP is not rebooted but the radios will go down and up, so that station associations will be disrupted briefly. The AP will start using the new license, and will support the capabilities shown in the **Features** column.

Click the **Delete** button to remove the selected pending licenses. (Deployed licenses may **not** be deleted.)

You may click the Export link at the top of the page to export all pending licenses. It is not necessary to select any entries first—all pending licenses will be exported. To export an .xls file, click the Excel radio button. To export a file of comma-separated values (.csv), click the Csv radio button. Then click Export. The File Download dialog box will allow you to open the file, or save it to the location you select.

Managing by Profiles

WOS provides profiles for ease of management. A profile allows you to specify a set of APs and manage them as a group. After creating a profile, you then define a uniform configuration and Avaya OS software release to be applied to all of the member APs. This “manage by network” feature eliminates the time-consuming and error-prone task of configuring and managing APs individually, and ensures the deployment of consistent software and settings across each profile. You can add APs to the profile at any time, before or after entering its configuration and software version settings.

There are two different kinds of profiles:

- **AOSLite Profiles** are for small APs that run AOSLite software, such as the WAP9112. AOSLite profiles have a small number of settings, consistent with the simple configuration of these APs.
- **AOS Profiles** are for the rest of the Avaya AP models, which run Avaya OS software. AOS profiles have a rich set of configuration options, just as Avaya OS does.

If you have both types of APs, you should create one or more AOS and AOSLite profiles and set a default profile for each type. When WOS discovers an Avaya AP, it automatically places it into the correct default profile based on whether the AP runs AOS or AOSLite.

To guarantee the uniformity of a profile, member APs should not be configured individually directly via their CLI or WMI. This usually results in temporary inconsistencies between the AP configuration and the WOS database. Note that member APs can be configured individually via WOS, but this is not recommended either—with the exception of changing settings that cannot be managed as part of the profile, such as individual **Radio Settings**.

If you do configure an AP manually via its WMI or CLI, or by using its **AP Details—Configuration** *tab in WOS, you must then use the* ***Refresh*** *button for this AP (on the* **AP Details** *page or on the* **The Access Points List** *page). When you refresh the AP, WOS will update its database with the current configuration of the AP. When a profile change is applied to the AP, WOS pushes out configuration changes to the AP based on the AP's current configuration as shown in the WOS database. After making a "manual" change, you must use the Refresh button, or risk having subsequent profile changes fail because WOS is unaware of the AP's current settings.*

Settings that must be unique per AP are automatically excluded from management by the profile. For example, the AP IP address and hostname must be different for each AP, and are thus not changed by updates to the profile. Individual radio settings (channel, cell size, etc.) are also not changed, since these are tailored to the environment of each AP.

Profiles

The web client Profiles page lists all of the profiles being managed by WOS, and allows you define new profiles and perform selected functions on them. To display this page, click the **Profiles** link in the AP **Configuration** section under **Configure** at the top of the page.

To start using profiles, follow these basic steps:

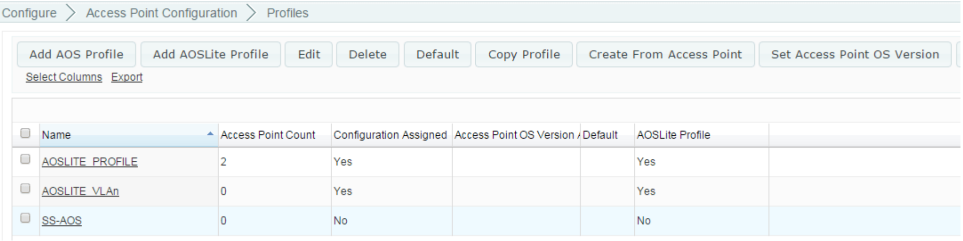
1. **Create a profile** and assign APs to it. See **Add AOS Profile** and **Add AOSLite Profile** in the **"The Profiles Toolbar" on page 199**. Alternatively, for AOS profiles only, you may import a .csv file that contains assignments to profiles for many APs and will create those profiles if needed, as described in **"Import Access Point Custom Fields" on page 128**.

2. **Specify the software release** to be run on the profile network. See **Set AP OS Version** in the **"The Profiles Toolbar" on page 199**.

3. **Specify the configuration to be enforced on members**—click the profile to go to its detail pages and enter configuration settings. See **“Profile Details—Configuration” on page 207**.

The following sections describe the Profiles page:

- **About Using the Profiles Page**
- **The Profiles List**
- **The Profiles Toolbar**
- **Profile Details**
  - **Profile Details—APs**
  - **Profile Details—Configuration**
  - **Profile Details—Job Status**



□	Name	Access Point Count	Configuration Assigned	Access Point OS Version	Default	AOSLite Profile
□	AOSLITE_PROFILE	2	Yes			Yes
□	AOSLITE_VLAn	0	Yes			Yes
□	SS-AOS	0	No			No

Figure 137. Profiles Page

About Using the Profiles Page

A number of basic operations are available on the APs page to allow you to customize it for your own use:

- **“Select Columns” on page 62**
- **“Export” on page 63**
- **“Select Rows” on page 64**
- **“Rearranging and Resizing Columns in a Table” on page 64**
- **“Sorting” on page 64**
- **“Searching” on page 65**

The Profiles List

The Profiles List (**Figure 137 on page 197**) shows the profiles (for AOS and AOSLite) that you have already created. **The Profiles Toolbar** allows you to add new profiles, define the software version for member APs, and perform a number of other operations on the profiles that you select.

Click on a profile's **Name** to access **Profile Details** pages that manage the configuration of member APs and show the status of the operations performed on them.

For each profile, the following information is shown by default:

- The **Name**
- The AP **Count** of member APs
- Whether or not there is a **Configuration Assigned** to the profile
- Whether or not there is an **AP OS Version Assigned** to the profile
- Whether this is the **Default** profile. When new APs are first discovered, they will be assigned automatically to the default profile, if one has been selected.
- Whether or not this is an AOSLite type of profile

The Profiles Toolbar

This toolbar offers functions for profile management, including creating profiles, editing their membership, and specifying their software version.

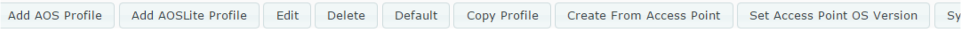
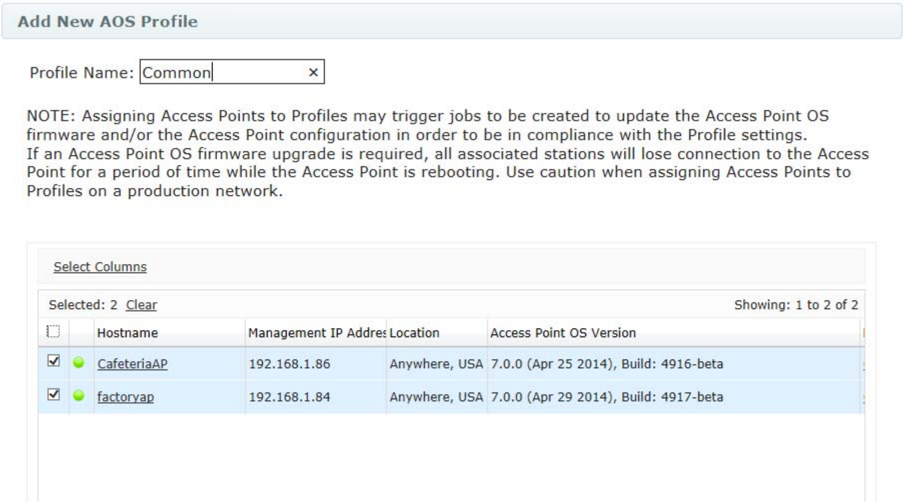


Figure 138. The Monitor—APs Page Toolbar

Select one or more profiles in the list for operations such as Delete by clicking their checkboxes in the first column, and then click one of the toolbar buttons. You may click the checkbox in the header row to select all profiles, or click again to deselect all.

The operations available are:

- **Add AOS Profile** or **Add AOSLite Profile—**Create a new profile using the selected APs. You may also create a new profile from **The Access Points List**, using the **Create Profile** option under the **More** drop-down in **The Configure APs Toolbar**. Alternatively, for AOS profiles only, you may import a .csv file that contains assignments to profiles for many APs and will create those profiles if needed, as described in **Import Access Point Custom Fields**.



Add New AOS Profile

Profile Name: Common ×

NOTE: Assigning Access Points to Profiles may trigger jobs to be created to update the Access Point OS firmware and/or the Access Point configuration in order to be in compliance with the Profile settings.
If an Access Point OS firmware upgrade is required, all associated stations will lose connection to the Access Point for a period of time while the Access Point is rebooting. Use caution when assigning Access Points to Profiles on a production network.

Select Columns

Selected: 2 Clear Showing: 1 to 2 of 2

□		Hostname	Management IP Addres	Location	Access Point OS Version
☑	●	CafeteriaAP	192.168.1.86	Anywhere, USA	7.0.0 (Apr 25 2014), Build: 4916-beta
☑	●	factoryap	192.168.1.84	Anywhere, USA	7.0.0 (Apr 29 2014), Build: 4917-beta

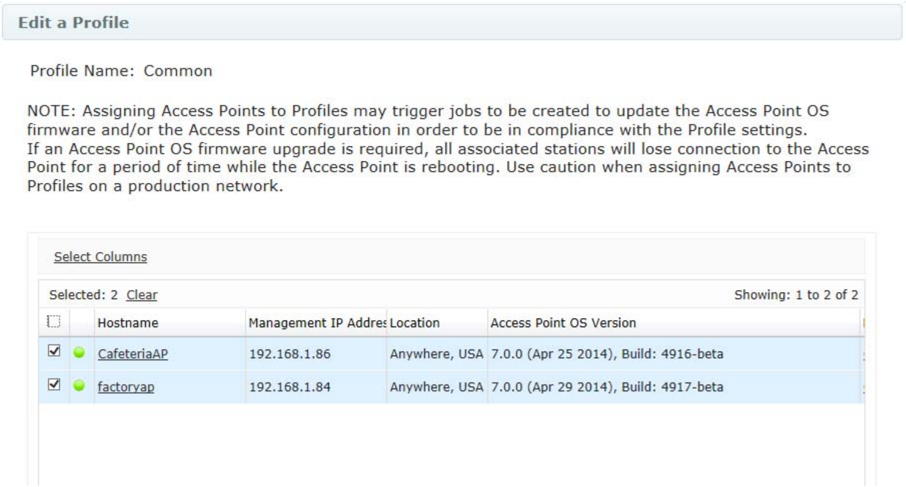
Figure 139. Add a Profile

Enter the new **Profile Name**, then select the APs that are to be members of this profile. Only APs that are not already assigned to another profile and of the appropriate type (AOS or AOSLite) will be listed. For your convenience, the current software version running on each AP is shown. Click **OK** when done.

Note that you may also add APs to a profile from **The Access Points List**, using the **Assign to Profile** button in **The Configure APs Toolbar**.

An AP may not be a member of more than one profile. If you wish to move an AP from another profile to this one, it must be removed from the old profile first. The easiest way to do this is by using the **Assign to Profile** button in **The Configure APs Toolbar**. The **Assign to Profile** button will remove each selected AP from its old profile assignment (if any) and add it to the specified profile in one step. See **"The Configure APs Toolbar" on page 110**.

- **Edit**—this option allows you to change which APs are members of the profile. The APs listed include both the profile's current members, and APs that are not already assigned to another profile.



Edit a Profile

Profile Name: Common

NOTE: Assigning Access Points to Profiles may trigger jobs to be created to update the Access Point OS firmware and/or the Access Point configuration in order to be in compliance with the Profile settings.
If an Access Point OS firmware upgrade is required, all associated stations will lose connection to the Access Point for a period of time while the Access Point is rebooting. Use caution when assigning Access Points to Profiles on a production network.

Select Columns

Selected: 2 Clear

Showing: 1 to 2 of 2

□		Hostname	Management IP Addres	Location	Access Point OS Version
☑	●	CafeteriaAP	192.168.1.86	Anywhere, USA	7.0.0 (Apr 25 2014), Build: 4916-beta
☑	●	factoryap	192.168.1.84	Anywhere, USA	7.0.0 (Apr 29 2014), Build: 4917-beta

Figure 140. Edit a Profile

You may check APs to add them to the profile, or uncheck them to remove them from the profile. Click **OK** when done. This does not delete the unchecked APs from the WOS database - they just cease to be assigned to a profile, and their configuration and software version are untouched by this action.

Alternatively, you may import a .csv file that contains assignments to profiles for many APs as described in **“Import Access Point Custom Fields” on page 128**. These assignments will replace any current assignments of APs to profiles, and they may then be edited as well.

When you add an AP to an existing profile that has a software version and or configuration defined, the new member is checked for compliance with this profile. If needed, jobs are triggered to upgrade the software version and/or update the configuration. Note that if both are needed, the software upgrade is always performed first. Then, if the configuration update involves new settings that are only implemented in the new software version, they will be handled properly.

If a software upgrade is required, all associated stations will lose connection to the AP for a period of time while the AP is rebooting. Use caution when assigning APs to profiles on a production network.

- **Delete—**this option deletes the selected profiles. It does not delete the member APs from the WOS database - they just cease to be assigned to a profile. The configuration and software version of these APs are untouched by this deletion. You will be asked to confirm the operation.
- **Default**—this option sets one selected profile as the default. When APs are discovered, they are automatically added as members of the default profile. These APs are automatically checked for compliance with the profile and updated as described above for the **Edit** button.
- **Copy Profile—**this option creates a duplicate of one selected profile.

  This feature is handy if you have already configured some profile and then you want to define another profile whose configuration is just slightly different. Select the checkbox of the profile to be duplicated and click this button. Enter the name of the new profile.

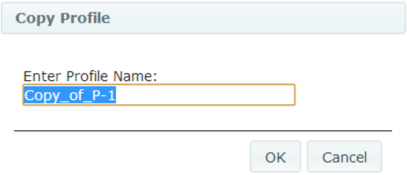
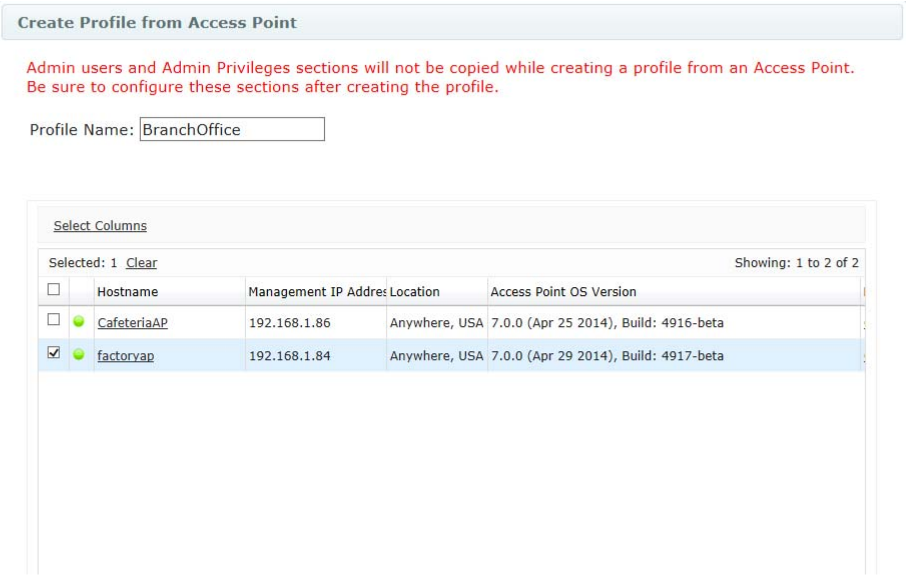


Figure 141. Copy a Profile

  The new profile is created with no member APs. Use the **Edit** button to add the desired APs to it. The new profile's Configuration and AOS Version are identical to those of the original profile until you change them.

- **Create From AP—**this option creates a new profile with an initial configuration that is copied from the selected AP. This is useful if you already have an Avaya network deployed and wish to create profiles to mirror the existing settings, or if you prefer to perform configuration directly on an AP and then create a profile based on it.



Create Profile from Access Point

Admin users and Admin Privileges sections will not be copied while creating a profile from an Access Point. Be sure to configure these sections after creating the profile.

Profile Name: BranchOffice

Selected: 1 Clear

Showing: 1 to 2 of 2

□		Hostname	Management IP Addres	Location	Access Point OS Version
□	●	CafeteriaAP	192.168.1.86	Anywhere, USA	7.0.0 (Apr 25 2014), Build: 4916-beta
☑	●	factoryap	192.168.1.84	Anywhere, USA	7.0.0 (Apr 29 2014), Build: 4917-beta

Figure 142. Create a Profile from an AP

You may also create a profile from a selected AP in **The Access Points List** or from an **AP Details** page, by selecting **More > Create Profile** from **The Configure APs Toolbar**.

The new profile is created with no member APs and no AOS Version. Use the **Edit** button to add the desired APs to it. The new profile's Configuration settings are identical to those of the prototype AP until you change them, except as noted below.

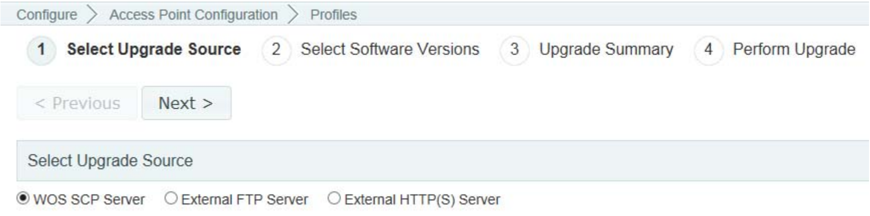
- The rules listed in **"Settings that are omitted from profile configuration" on page 209** are observed.
- VLANs are copied, and **Enable VLAN Management For This Profile** is enabled.
- Profiles may have lower limits for the number of entries allowed for certain settings than some APs do. For example, if the prototype AP has more than 8 SSIDs configured, you will see an error message.

  - **Admin Management** accounts and **Admin Privileges** are not copied from the prototype AP. Only the default **admin** account will be created. Configure other accounts or privileges separately in the profile. Also, the settings shown in **"Settings that are omitted from profile configuration" on page 209** are not included in the profile.
  - The profile is created using the configuration data for the AP that is already in the WOS database, rather than reading the configuration directly from AP. If you wish, you may refresh the AP prior to creating the profile, using the **Refresh** button on **The Access Points List** page—this will update WOS with the latest configuration.

- **Set AP Access Point OS Version**

  Click this button to set up the desired Avaya OS or AOSLite software version for this profile network. You can specify the software version regardless of whether or not the profile contains any member APs. It is also possible to use this to roll back the profile network to an earlier software version, although the downgrade will fail for APs that don't support the older software.

  Follow the same steps described in **"Perform or Schedule Upgrade" on page 131**, except that you will not be asked to specify the APs to be upgraded since the software version selected here will be enforced on all members of the profile network. Similarly, you do not specify a scheduled time for the upgrade. Note that AP licenses will be updated if necessary prior to the upgrade, also as described in **"Perform or Schedule Upgrade" on page 131**.



● WOS SCP Server ○ External FTP Server ○ External HTTP(S) Server

Figure 143. Set Profile's Software Image

Member APs will be checked for the correct software version when:

- You enter a different software version in **Set AP OS Version**.
- An AP is added to the profile network either via discovery, or by using the **Edit** button.
- You click the **Sync APs** button.

To reset the AOS version back to “none”, choose the blank entry in the **System Software** drop-down list (in **Step 2 - Select Software Versions**). In this case, the profile network will not require member APs to run a specific software version.

- **Sync APs**—Click this button to check that **all** member APs comply with the profile. Software and then configuration are updated if needed, as described above for the **Edit** button. Any configuration changes performed can be seen in the job status tab. Use this feature if you have used WOS to make configuration changes to individual member APs and wish to revert to the standard profile configuration.

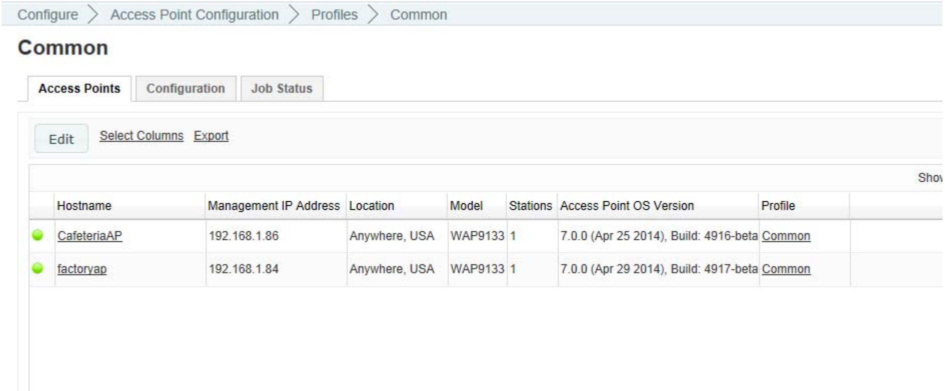
Profile Details

By clicking the **Name** of a profile in **The Profiles List**, you may view a variety of details about the selected profile network.

- **“Profile Details—APs” on page 206**—a list of member APs.
- **“Profile Details—Configuration” on page 207**—this tab allows you to define the configuration settings for all member APs.
- **“Profile Details—Job Status” on page 211**—this tab shows all the configuration/software upgrade jobs for member APs, along with their status.

Profile Details—APs

This page lists the member APs of this profile network. By default, it shows the **Hostname**, **Management IP Address**, **Location**, **Model**, count of associated **Stations**, and current running **AP OS Version** for each. The **Edit** button allows you to change which APs are members of this profile, as described for the **Edit** button in **“The Profiles Toolbar” on page 199**.



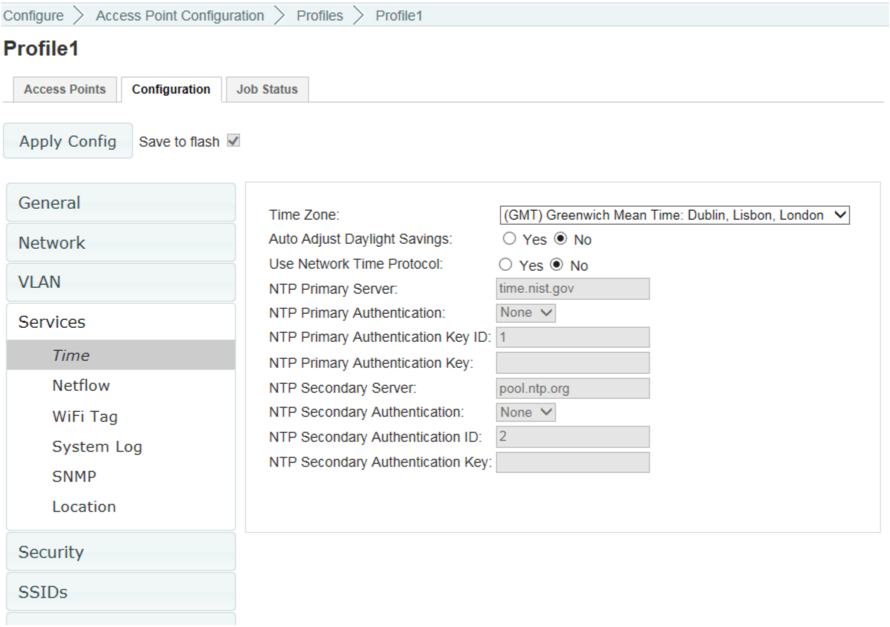
	Hostname	Management IP Address	Location	Model	Stations	Access Point OS Version	Profile
●	CafeteriaAP	192.168.1.86	Anywhere, USA	WAP9133	1	7.0.0 (Apr 25 2014), Build: 4916-beta	Common
●	factoryap	192.168.1.84	Anywhere, USA	WAP9133	1	7.0.0 (Apr 29 2014), Build: 4917-beta	Common

Figure 144. Profile Details: General

Click the **Configuration** tab to define the AP settings for this network.

Profile Details—Configuration

This page has an extensive menu of options for defining the configuration profile on the member APs. Almost all of the settings that are available in the AP Windows Management Interface (WMI, for non-AOSLite devices only) are also available here.



Save to flash ☑

Time Zone: (GMT) Greenwich Mean Time: Dublin, Lisbon, London
Auto Adjust Daylight Savings: ○ Yes ● No
Use Network Time Protocol: ○ Yes ● No
NTP Primary Server: time.nist.gov
NTP Primary Authentication: None
NTP Primary Authentication Key ID: 1
NTP Primary Authentication Key:
NTP Secondary Server: pool.ntp.org
NTP Secondary Authentication: None
NTP Secondary Authentication ID: 2
NTP Secondary Authentication Key:

Figure 145. Profile Details: Configuration (AOS Profile Type Shown)

The configuration profile is a complete configuration rather than an incremental one. This means that the profile entirely replaces all settings on each member AP, rather than simply updating a few settings that you entered. Any settings that you haven’t specified are set to the default value, shown on this Configuration tab, except for **“Settings that are omitted from profile configuration” on page 209**.

Note that smaller APs that use the AOSLite system software, such as the WAP9112, have many fewer settings than more powerful APs. Some of the configuration pages will not list AOSLite devices, or are not available for those devices.

For an explanation of all of the settings available on the Configuration tab, see **"Configuring a Wireless AP" on page 369**. When you create a new profile, it will have the default configuration setting values shown in **Default Profile Configuration**, below.

*If you plan to define a required Avaya OS version for this profile network, we strongly recommend that you do that first using the **Set AP AOS Version** button, as described in **The Profiles Toolbar**. The profile performs the required software upgrades before updating configuration on member APs. This ensures that settings for new features in the specified software version are handled correctly.*

Default Profile Configuration

All configuration setting values for new AOS Profiles will be the default AP values, except for those in the following table. Note that the defaults below apply *only* to AOS profiles, except as noted.

Tab	Setting	Value
Security> Admin Management	User Name/ Password	admin/admin
Network>DNS	Hostname DNS Servers	Not displayed 0.0.0.0
Services> SNMP	Context Engine ID	Not displayed
Services> Location	Location Support	Disabled
SSIDs> SSID Management	Name	avaya (same for AOSLite devices)

Tab	Setting	Value
Radios> Global Settings	Country	AOSLite—United States; AOS—Not set. See **"Settings with special handling in profile configuration" on page 210**.
Filters> Filter Lists	Filter List Name	global
Tunnels> Tunnel Management	Local Endpoint	Not displayed

Settings that are omitted from profile configuration

Some settings cannot be configured as part of a profile. Settings such as the AP IP address must be unique, and the assigned address must not be changed when the profile configuration is "pushed" to the AP. For this reason, such settings are not shown anywhere on this Configuration tab at all. Individual radio settings (channel, cell size, etc.) are also not changed, since these are tailored to the environment of each AP.

The following settings are not part of the profile configuration and are left unchanged (i.e., not included) in the profile.

- **General**: **Location, License Key**
- **Network> Interfaces: IP Address, Subnet Mask, Default Gateway**
- **Network> DNS: Hostname**
- **Network Bonds**: all settings (i.e, this page is not present for profiles)
- **Services> SNMP: Context Engine ID**
- **Security> External RADIUS: NAS Identifier**
- **SSIDs > Active Radios**: all settings (i.e, this page is not present for profiles)
- **Radios > Radio Settings**: Individual radio settings are not changed, but you may enable or disable all radios at the same time.
- **Tunnel Management: Local Endpoint**

If you need to modify settings listed above, you may do this using other WOS configuration options. For example, for radio settings, see **Configure Wireless**

Settings. For IP settings, see **Configure Network Settings**. (Note that many of these settings above are not present on AOSLite devices.)

Settings that are only present in profile configuration

Some settings are only used as part of a profile, and you will not see them in **"Configuring a Wireless AP" on page 369**. These are special settings that deal with the differences in the range of AP models. Currently, there is only one such setting, and it is only for AOS Profiles.

- **Radios > Advanced RF Settings**: **Enable Timeshare for 2-Radio APs**— By default, the **RF Monitor Mode** on profile-member APs is **Dedicated**, which means that the radio that is set as the monitor radio observes the RF-environment full-time for problems. This is very good for larger APs, but it is inefficient usage of radio resources for APs that only have two radios.

  If **RF Monitor Mode** is set to **Dedicated** for the profile, then you may set **Enable Timeshare for 2-Radio APs** to **Yes**. Then APs that are members of the profile and that have only two radios will use **Timeshare** mode for the monitor radio. This allows that radio to spend part of its time as a monitor radio, and function as a normal radio providing wireless service to stations the rest of the time. See **"RF Monitor" on page 520** for other settings that control timeshared use of the monitor radio. This setting defaults to **Yes** when **RF Monitor Mode** is set to **Dedicated**.

Settings with special handling in profile configuration

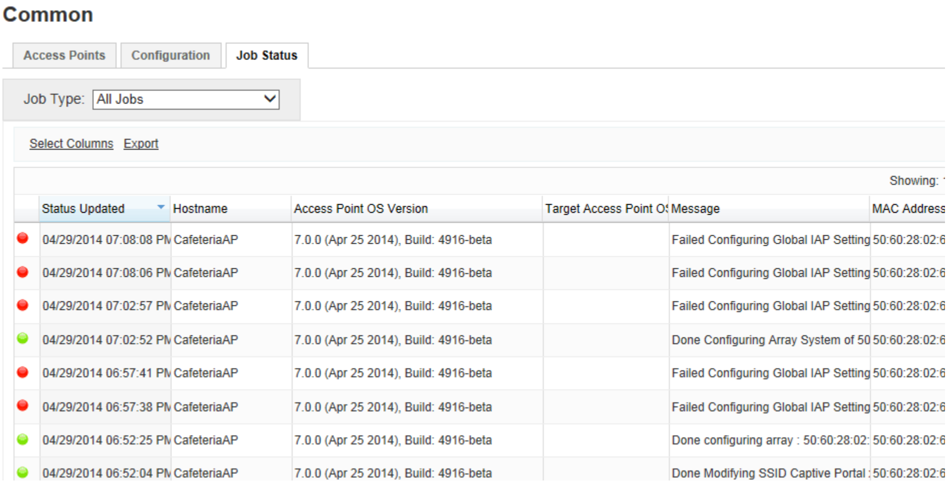
The behavior of some settings need additional explanation. These settings typically deal with the differences in the capabilities of AP models.

- **Radios> Global Settings: Country**—You may configure a country in the profile. This setting will not override an existing country code, but it will set the country on APs where it isn't already set.
- **VLANs > VLAN Management**—You may define up to 64 VLANs in a profile. Some APs support 64 VLANs, but smaller APs may support as few as 32. AOSLite devices support 53 VLANs. Application of a profile

will fail on an AP that doesn't support as many VLANs as you have defined.

Profile Details—Job Status

This page shows jobs launched for member APs by the profile. You may select whether to show **AOS Upgrades**, AP **Config** updates, **Discovery**, or **All Jobs**. Note that if **AOS Upgrades** and AP **Config** updates need to be performed for the same AP, the software upgrade is performed first. This ensures that any configuration settings related to new features in the upgraded software will be handled properly.



Common

Job Type: All Jobs

	Status Updated	Hostname	Access Point OS Version	Target Access Point O	Message	MAC Address
🔴	04/29/2014 07:08:08 PM	CafeteriaAP	7.0.0 (Apr 25 2014), Build: 4916-beta		Failed Configuring Global IAP Setting	50:60:28:02:6
🔴	04/29/2014 07:08:06 PM	CafeteriaAP	7.0.0 (Apr 25 2014), Build: 4916-beta		Failed Configuring Global IAP Setting	50:60:28:02:6
🔴	04/29/2014 07:02:57 PM	CafeteriaAP	7.0.0 (Apr 25 2014), Build: 4916-beta		Failed Configuring Global IAP Setting	50:60:28:02:6
🟢	04/29/2014 07:02:52 PM	CafeteriaAP	7.0.0 (Apr 25 2014), Build: 4916-beta		Done Configuring Array System of 50	50:60:28:02:6
🔴	04/29/2014 06:57:41 PM	CafeteriaAP	7.0.0 (Apr 25 2014), Build: 4916-beta		Failed Configuring Global IAP Setting	50:60:28:02:6
🔴	04/29/2014 06:57:38 PM	CafeteriaAP	7.0.0 (Apr 25 2014), Build: 4916-beta		Failed Configuring Global IAP Setting	50:60:28:02:6
🟢	04/29/2014 06:52:25 PM	CafeteriaAP	7.0.0 (Apr 25 2014), Build: 4916-beta		Done configuring array : 50:60:28:02:	50:60:28:02:6
🟢	04/29/2014 06:52:04 PM	CafeteriaAP	7.0.0 (Apr 25 2014), Build: 4916-beta		Done Modifying SSID Captive Portal :	50:60:28:02:6

Figure 146. Profile Details: Job Status

By default, this page shows the following columns:

- **Status Indicator**—green for success, red for failure.
- **Status Updated**—the last time this status was updated.
- **Hostname**—the host name of the member AP that is being updated by this job.
- **Management IP Address**—the IP address of the member AP that is being updated by this job.

- **Job Type**—the type of update that this job is performing—**AOS Upgrade** or AP **Config**.
- **AOS Version**—the current Avaya OS version running on the member AP that is being updated by this job.
- **Target AOS**—the Avaya OS version defined for this profile network, if any.
- **Message**—information about the job performed on the AP, if successful; or the type of failure, otherwise.

Working with Maps

This chapter takes you on a tour of the web client's map window and its features. It walks you through creating a map, and shows you how to display a heat map of your RF coverage. Section headings for this chapter include:

Note that smaller APs that use the AOSLite system software, such as the WAP9112, are not included on heat maps.

About Maps

Maps offer a topographical view of your wireless network and the RF coverage it provides. From a map you may view a variety of information about each AP, its radios and associated stations. AP management functions may also be applied from the map.

A heat map shows wireless coverage at your site, and is based on measurements observed by APs. It visualizes the RF environment provided by your wireless network. The map incorporates directional antenna coverage on a per radio basis, and readings are enhanced by means of inter-AP correction. By leveraging the RF analysis capabilities available on the AP, WOS makes it easy to view the changing RF environment.

A performance plan shows the predicted throughput of the wireless network under various types of usage, for network planning and troubleshooting.

The WOS Location capability displays the position of a station or rogue device on the map for you, facilitating asset tracking and security policy enforcement.

Getting Started with Maps

This overview describes how to get started using maps, and points you to topics that describe each step in detail.

- **“The Map Window and Heat Contour Map” on page 216**—provides an overview of the map window.
- **“Migrating Maps from Earlier Releases” on page 224**—WOS is furnished without any default maps. However, if you have already created maps in pre-6.2 releases of WOS, they will automatically be migrated to the current release.

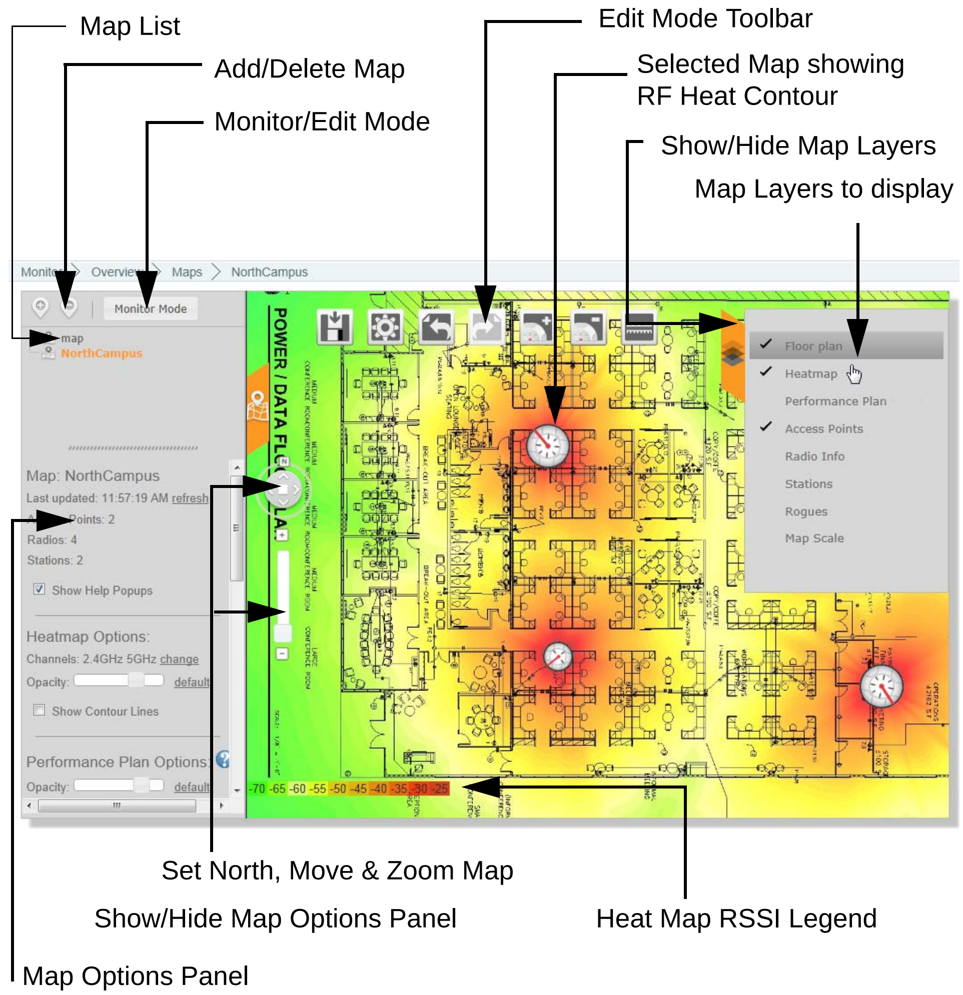
- To add a new map (and modify existing ones):
    - **“Preparing Background Images for New Maps” on page 224**—you must supply a background image for your map, such as a floor plan or a site layout of buildings.
    - **“Adding a New Map” on page 226**—follow these instructions to create a new map.

    - **“Setting the Map Scale and North Direction” on page 228**—set the distance scale for the map, so that RF contours will display accurately.

- Select the APs that belong on the map. Rotate each AP on the map so that the monitor radio has the correct orientation (Note that many APs can automatically detect North, and WOS places these on the map in the correct orientation). See **“Adding APs to Maps” on page 231**.
- After completing the steps above, you may use the **RF Heat Contour Map** to present a live display of RF coverage by AP. To manage APs, see **“Managing APs Within Maps” on page 241**.
- After completing the steps above, you may use the **Performance Plan** to predict the performance of the network under different usage scenarios.
- You may customize your display. See **“Map Options Panel” on page 247** and **“Map Layers Panel” on page 255**.

The Map Window and Heat Contour Map

To display the map window, click the **Maps** link in the **Overview** section under **Monitor** at the top of the page. Select the desired map from the Map List.



map
NorthCampus

Map: NorthCampus
Last updated: 11:57:19 AM refresh
Access Points: 2
Radios: 4
Stations: 2
☑ Show Help Popups

Heatmap Options:
Channels: 2.4GHz 5GHz change
Opacity: default
□ Show Contour Lines

Performance Plan Options:
Opacity: default

Figure 147. Main Map with RF Heat Contours Enabled

No default maps are provided. If you have created maps in a previous release of WOS, they will be present after you upgrade. When you upgrade to a new release of WOS, maps created in earlier releases will be automatically migrated. See **“Migrating Maps from Earlier Releases” on page 224**. You may create new maps as described in **“Adding a New Map” on page 226**.

The map window has the following parts:

- **The Map List**
- **RF Heat Contour Map**
- **Performance Plan**
- **Map Options Panel**
- **Map Layers Panel**
- **AP Management Panel**

The Map List

This list shows all of the maps in the WOS database. If the Map List is not visible at the left of the map, click the Map Options tab as shown in **Figure 148**.

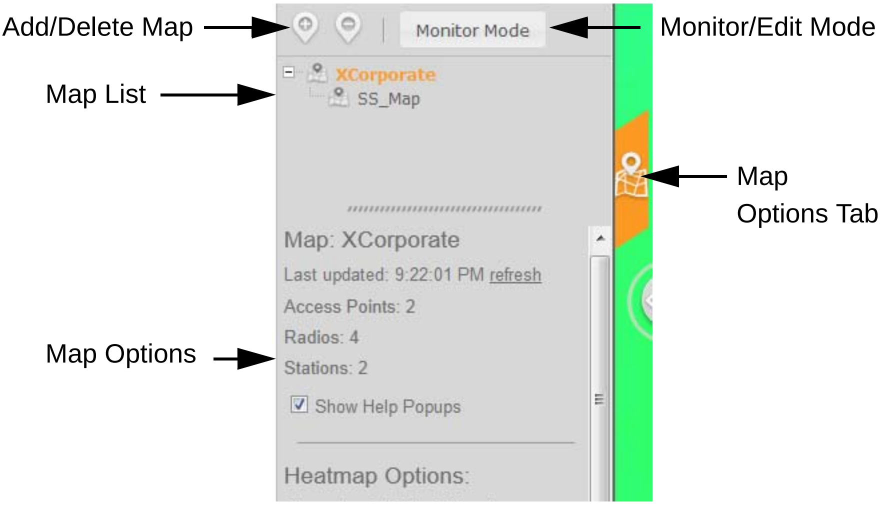


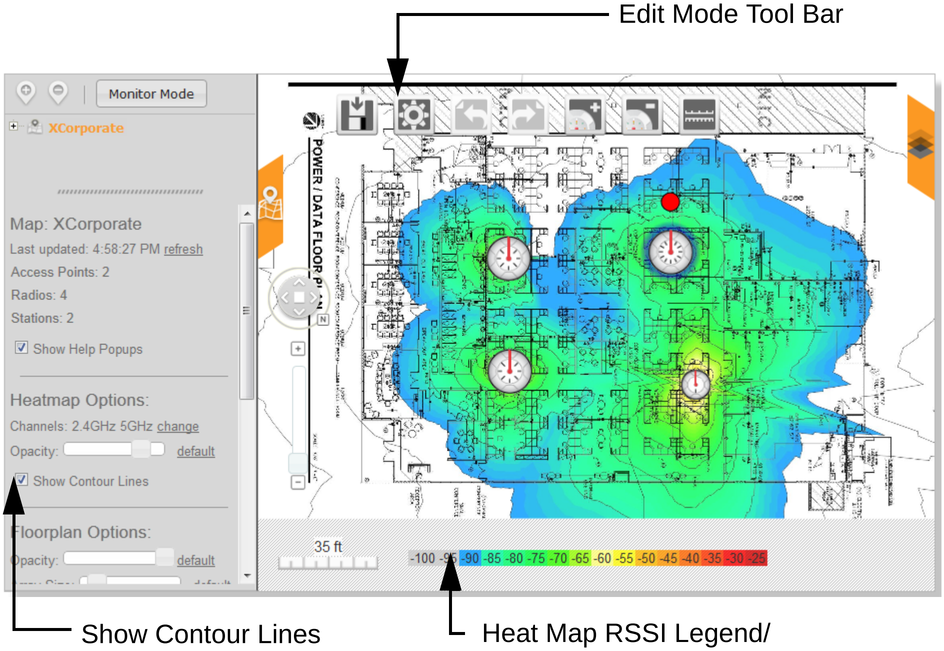
Figure 148. The Map List and Map Options Panel

The Map List has a tree structure, with child maps displayed under parent maps. If the desired map name is not visible, click the **+** sign to the left of its parent to expand the parent entry.

Click on a map to display it. If the currently displayed map has unsaved changes, you will be asked whether to save the changes before displaying the new map.

RF Heat Contour Map

The heat map gives an at-a-glance representation of the APs in an area, their locations, and the RF coverage that they provide. Areas of low coverage are immediately visible. In order to display this view, enable **Heatmap** in the **Map Layers Panel**. You may hover over an AP to display a popup identifying the AP, or double-click an AP to show more information about it. See **"Viewing AP, Station, or Rogue Details" on page 233**.



Map: XCorporate
Last updated: 4:58:27 PM refresh
Access Points: 2
Radios: 4
Stations: 2
☑ Show Help Popups

Heatmap Options:
Channels: 2.4GHz 5GHz change
Opacity: default
☑ Show Contour Lines

Floorplan Options:
Opacity: default

Edit Mode Tool Bar

Show Contour Lines

Heat Map RSSI Legend/
Minimum Acceptable RSSI

Figure 149. Main Map Showing RF Heat Contours

When enabled, RF contour lines are displayed on this map to show the strength of RF signals broadcast by each AP. To display contours, enable **Show Contour Lines** in **Heatmap Options** in the Map Options panel (see **"Map Options Panel"**

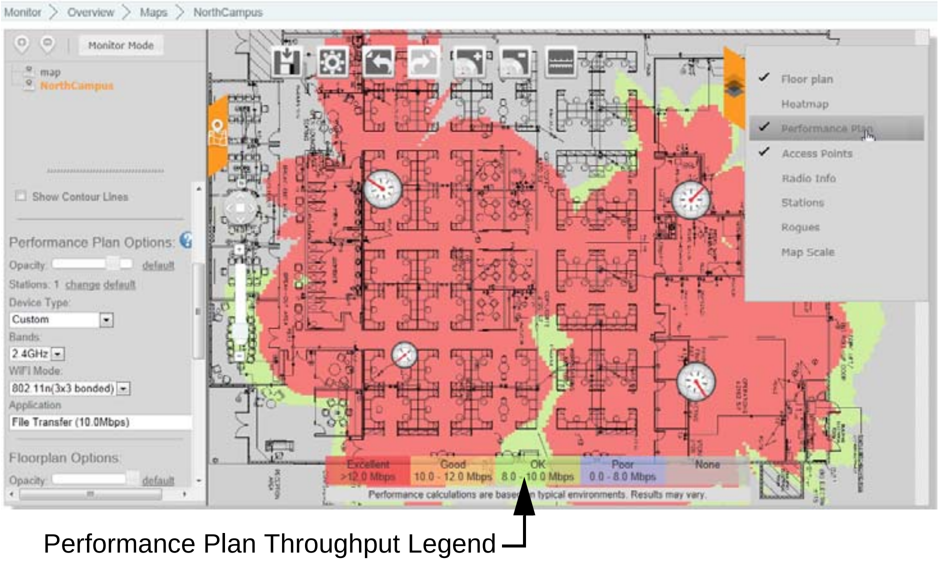
on page 247). If an AP’s radios are disabled, no contours are displayed for that AP. Signal strength is displayed using the colors shown in the Heat Map RSSI Values legend under the map.

The bottom of the map also has a heat map RSSI legend, which defines the signal strength indicated by each color. You may define a minimum acceptable signal strength by clicking that value on the legend. The map will only display RSSI levels above that value in color. Areas with unacceptable signal strength are obvious, as they have no color, as shown in **Figure 149**.

You may add any model of Avaya APs to a map (see **“Adding APs to Maps” on page 231***). However, units that use external antennas (such as WAO9122) will not display heat contours.*

Performance Plan

The performance plan offers a visual representation of the predicted throughput of the wireless network over your site for different station/user profiles. Use this as a resource to plan for network expansion and troubleshoot network performance issues. In order to display this view, enable **Performance Plan** in the **Map Layers Panel**.



Monitor > Overview > Maps > NorthCampus

Performance Plan Options:

Opacity: default

Stations: 1 change default

Device Type: Custom

Bands: 2.4GHz

WiFI Mode: 802.11n(3x3 bonded)

Application: File Transfer (10.0Mbps)

Floorplan Options:

Opacity: default

Excellent	Good	OK	Poor	None
>12.0 Mbps	10.0 - 12.0 Mbps	8.0 - 10.0 Mbps	0.0 - 8.0 Mbps	

Performance calculations are based on typical environments. Results may vary.

Performance Plan Throughput Legend

Figure 150. Performance Plan Map

The Performance Plan shows expected performance of your network, using color to indicate whether the level of throughput in an area will be excellent, good, okay, poor, or non-existent. The prediction is calculated based on selectable station characteristics including: number of stations on the map, station device type, band, WiFi mode, and typical application. Expected throughput is computed using these characteristics and observed performance of the network. See **"Performance Plan Options" on page 250** to set the characteristics of your network.

In addition, settings on the AP radios can also impact the plan, including: band, channel, bond mode, WiFi mode, cell size, Tx dBm, Rx dBm, and status (enabled/

disabled). Predicted throughput is computed based on the current settings of your radios, rather than their maximum settings. For example, any of the following settings will result in computed throughput that is less than the maximum that the APs can support: having radios disabled, setting reduced transmit/receive power, reduced cell size, etc.

The bottom of the map has a performance legend that defines the throughput and user satisfaction level indicated by each color.

Map Modes of Operation and User Privileges

WOS maps have two modes of operation:

- **Edit Mode**—this mode displays the **Edit Mode Toolbar** (**Figure 149**) and allows you to make basic changes to a map, such as adding, moving, orienting, and deleting APs, changing map settings like the RF environment, and setting the map scale. In edit mode, you may use the **Map Options Panel** and **Map Layers Panel** to customize the map display.
- **Monitor Mode**—this mode does not allow you to make basic changes such as adding and deleting APs. In monitor mode, you may use the **Map Options Panel** and **Map Layers Panel** to customize the map display. You may also use the **AP Management Panel** to manage the map's APs with functions such as rebooting or configuring settings on APs. See **"Managing APs Within Maps" on page 241**. The AP Management panel is not available in edit mode.

WOS users with read-write privileges may use edit mode and monitor mode. Users with read-only privileges may only use monitor mode; also, these users have access to a restricted set of functions on the AP Management Panel.

Use the button shown below to change modes. (**Figure 151**) The **Monitor Mode** button appears when you are in Edit Mode. Use it to switch to Monitor Mode. Similarly, the **Edit Mode** button appears when you are in Monitor Mode. Use it to switch to Edit Mode.

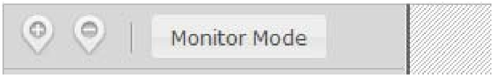


Figure 151. Add/Delete a Map and Edit/Monitor Mode Buttons

Overview of Map Features

The operations available in the map window depend on your WOS account privileges and the selected map mode, as discussed above in **Map Modes of Operation and User Privileges**.

WOS offers the following map functions:

- **Add** or **Delete Map** (edit mode and monitor mode)—the plus and minus buttons provide these functions. (**Figure 151**) See **"Adding a New Map" on page 226**.
- **Edit** or **Monitor Mode**—map modes determine the operations that are available. (**Figure 151**) See **"Map Modes of Operation and User Privileges" on page 221**.
- **Map List** (edit mode and monitor mode)—select the desired map from this tree structured list. (**Figure 148**) See **"The Map List" on page 217**.
- **AP, Station**, or **Rogue Info**—double-click an AP on the map (single click a station or rogue) to show detailed information about the item. See **"Viewing AP, Station, or Rogue Details" on page 233**.
- **Map Options Panel** (edit mode and monitor mode)—these options affect a number of aspects of the map display. (**Figure 148**) Some of the options include:
    - **Heatmap Options** select the bands displayed (2.4 GHz/5 GHz), the transparency of the heat map, and whether to show contour lines.
    - **Floorplan Options** select the transparency of the background floor map, the size of AP icons, and how much information to display for individual AP radios.
    - **Rogue Location** shows rogues that have been detected.
    - **Station Location** shows stations that are associated to APs.
    - **Channel Configuration** performs an automatic channel configuration on APs.

  See **"Map Options Panel" on page 247** for a detailed discussion of the Map Options panel.

- **Map Layers Panel** (edit mode and monitor mode)—there are options to select whether or not to show the following items on the map display: (**Figure 147**)
  - **Floorplan**
  - **Heatmap**
  - **Performance Plan**
  - **APs**
  - **Radio Info**
  - **Stations**
  - **Rogues**
  - **Map Scale**

  See **"Map Layers Panel" on page 255** for a detailed discussion of the Map Layers panel.
- **AP Management Panel** (monitor mode only)—allows you to perform the following operations on the selected APs:
  - **Refresh**
  - **Reboot**
  - **Assign to Profile**
  - **Pull Diagnostic Logs**
  - **Pull Config**
  - **Packet Capture**
  - **Configure** allows changes to Network Settings, Radio Settings, Channel and Band Autoconfigure, and enabling Application Control.
  - **Quick Config** allows some preset configurations to be applied.
  - **More** offers Add to Group and Delete operations, and allows access to the AP's WMI.

  See **"Managing APs Within Maps" on page 241** for a detailed discussion of this panel.

- **Zoom/Move** map—You may perform operations which change your view of the map, such as zooming in and dragging the map to view different regions. See **“Zooming or Moving the Map” on page 245**.

Migrating Maps from Earlier Releases

When you upgrade your WOS server, any maps that you have already created are automatically migrated to new maps that are compatible with the current WOS release. They are immediately available for use with the new software. Migrated maps will be listed in the **Map List** under the same names that they previously had.

Note that the old map information is kept in the WOS database. If you should wish to revert to an older release of the server, the old-style maps will still be available. If you have maps that are from a release prior to 6.0, please call Customer Support.

Before you begin using a migrated map be sure to perform these steps so that the map will accurately represent your environment:

- **“Setting the Map Scale and North Direction” on page 228**
- **Environment Settings**

Preparing Background Images for New Maps

You will typically want to present maps with a background image such as a floor plan or a site layout of buildings, a geographic area, a functional domain within your corporation, or any combination of map designs—whichever suits your needs.

WOS will accept most graphic file formats (including .bmp files) for your background images, though we recommend using either GIF, PNG, or JPG since these formats are the most suitable for online use. In particular, whenever possible, optimize your image files and try to keep the file size between 50KB and 100KB. Files in this size range will load into the client quickly, give reasonable image resolution, and will perform well when zooming in.

Preferred Image Formats

- **Graphics Interchange Format (GIF)**
  This is the file format most commonly used to display indexed-color graphics and images in HTML documents over the Web and other online services. Simple graphics (for example, floor plans) with or without spot colors are considered most suitable for the GIF file format, which is designed to minimize the image file size and electronic transfer time.
- **Portable Network Graphics (PNG)**
  This format is an alternative to the GIF format but supports 24-bit images with “no loss” compression and produces background transparency without jagged edges. However, some older Web browsers do not support this format.
- **Joint Photographic Experts Group (JPEG)**
  This format is commonly used to display photographs and other continuous-tone images. Unlike GIF images, the JPEG format retains all color information in an RGB graphic, but compresses the file size by selectively discarding data without serious degradation to the quality of the original image.

Physical Size

The physical size of the image is not critical because WOS scales the image automatically. However, the more scaling that is required the greater the loss in quality. We recommend a physical size of between 10 inches and 14 inches wide, while maintaining the aspect ratio of the original image (when scaled, the vertical axis will retain the correct proportion with the horizontal axis).

Resolution

The preferred resolution for your map background images is 72 dpi (standard for online viewing). A higher resolution will generate a smoother image, but the file size will be increased relative to the resolution you choose.

Adding a New Map

WOS allows you to add maps. Existing maps are displayed in the Maps list. Note that the currently selected map is highlighted in orange.

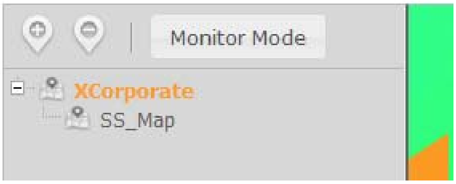
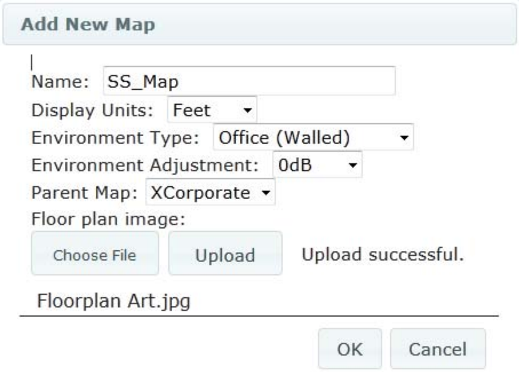


Figure 152. Maps List

To add a new map, use the following procedure:

1. The background image file for your map should be optimized for the smallest size possible. For more information about creating background images, go to **"Preparing Background Images for New Maps" on page 224**.

2. Click the **Add Map** button above the Maps List. (You do not need to be in edit mode to add a map. WOS will automatically switch you to edit mode once you click OK at the end of the Add New Map dialog.) The Add New Map window is displayed.



Add New Map

Name: SS_Map
Display Units: Feet
Environment Type: Office (Walled)
Environment Adjustment: 0dB
Parent Map: XCorporate
Floor plan image:
Upload successful.
Floorplan Art.jpg

Figure 153. Add New Map Window

3. Enter the **Name** for the new map.

4. Select the desired **Display Units** (feet or meters).

5. Environment settings customize your map for the type of construction in the area represented by the map. WOS uses these values to determine the degree of RF signal attenuation at your site. This increases the accuracy of RF heat map contours. See the discussion of “Planning your Installation - General Deployment Considerations” in Chapter 2 of *Using the Avaya WLAN AP 9100 Series (NN47252-102)*.

   Select the typical **Environment Type** for your type of construction, for example, **Office (Cubicles)**, **Office (Walled)**, **School**, or **Warehouse**.

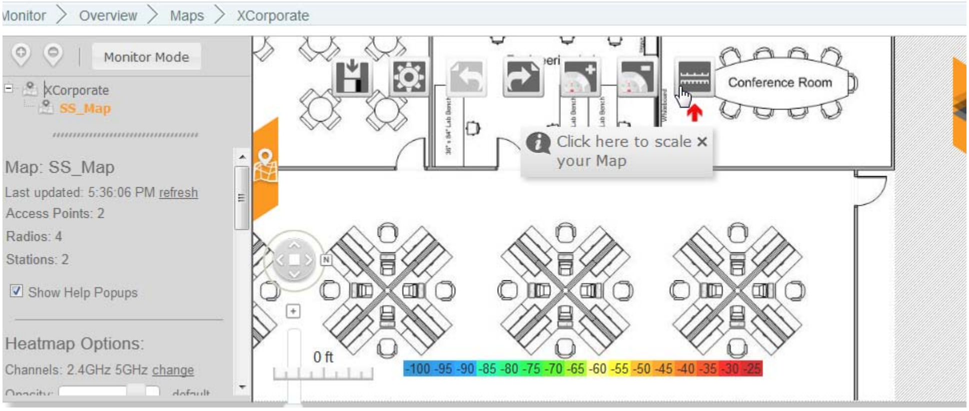
6. Now, use **Environment Adjustment** to tune the environment settings for the area included in the map. To set the adjustment properly, you should take a few data points and compare them to the values on the heat map without any adjustment. If the heat map shows -75dB at a particular spot but your reading is -70dB, then you should set an adjustment of +5dB. Likewise, if the map shows -50dB, but your measurement is -55dB, then set an adjustment of -5dB.

7. Select the desired **Parent Map** from the drop-down list. The Maps List has a tree structure that allows you to organize related maps. If you want this map to be at the top level, select **None**.

8. Under **Floor Plan image**, click the **Choose File** button and browse to select the image file. Note that the file should be located on your file system (accessible from the computer where you are running the WOS client). Click **Upload**.

9. Click **OK** to create the new map. If you were not already in edit mode, WOS will switch you to edit mode automatically once you click **OK**.

10. The new map will be displayed. Prompting messages will walk you through a series of additional steps to prepare the map for use.



Monitor > Overview > Maps > XCorporate

Monitor Mode

XCorporate
SS_Map

Map: SS_Map
Last updated: 5:36:06 PM refresh
Access Points: 2
Radios: 4
Stations: 2

☑ Show Help Popups

Heatmap Options:
Channels: 2.4GHz 5GHz change

Click here to scale ✕ your Map

Figure 154. New Map (showing prompt for scaling the map)

11. You may modify the map later. Click the **Map Settings** button on the **Edit Mode Toolbar**. You may change the **Environment Type** and **Adjustment**, **Display Units**, or even the **Name**.

You can now start to build your map by performing these steps, as the prompts from WOS direct you.

- **"Setting the Map Scale and North Direction" on page 228**
- **"Adding APs to Maps" on page 231**

To work with the APs that you have placed on the map, see **"Managing APs Within Maps" on page 241**.

Setting the Map Scale and North Direction

It is important to set the scale of each map in order for the RF heat map contours to display accurately and for location information to be as precise as possible.

You should also adjust the orientation of North on your map. APs contain hardware capable of sensing their orientation and are automatically placed on the map with the correct orientation. This feature requires North to be set correctly on the map.

It is very easy to set the scale. Before you start, measure the actual length of a wall or other feature represented on the map. The longer the object being measured is, the more accurate the scale will be.

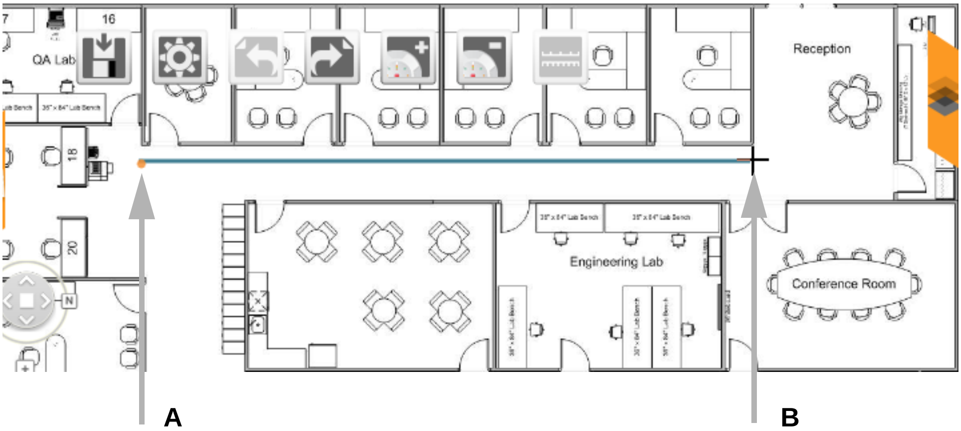


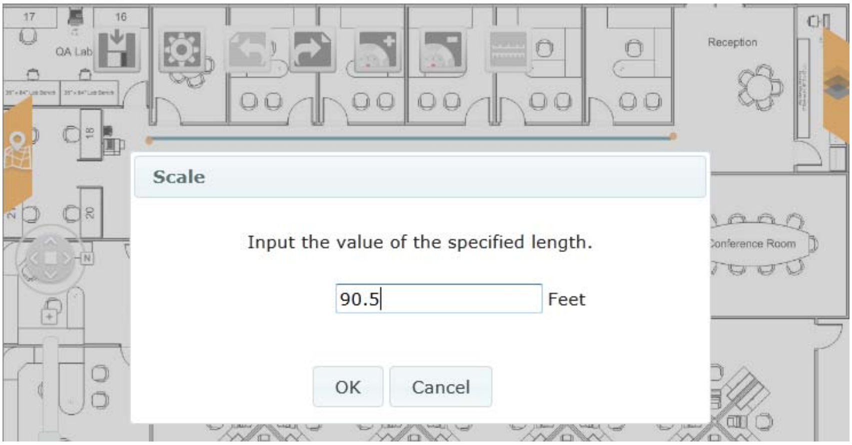
Figure 155. Calibrating the Map Scale

1. Measure a wall or other feature that is represented accurately on the map. **Figure 155** shows both ends (A and B) of a wall being measured.

2. Click the **Scale Map** button. The mouse pointer will change to a cross-hair tool in the next step.

3. On the map, move the cursor to one end of the wall or other feature that you measured (A) and click the mouse. Now click at the other end of the feature (B). A line will be drawn between the endpoints.

   The Scale dialog box appears.



Scale

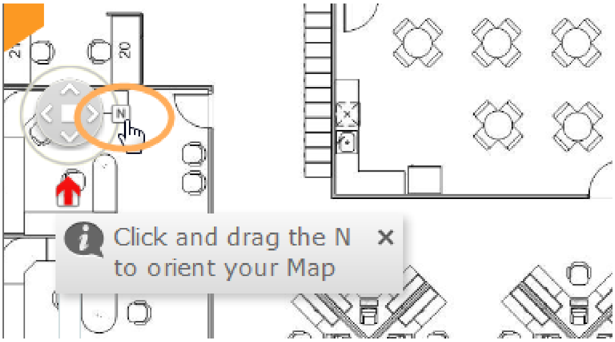
Input the value of the specified length.

90.5 Feet

Figure 156. Edit Map Scale

4. Enter the measured length of the wall. Click **OK**.

5. Now WOS prompts you to set North on the map.



Click and drag the N to orient your Map

Click and drag "N" until it points to the direction of North at your site.

Figure 157. WOS Prompts You to Set North on the Map

6. Determine the direction of north at the site represented by the floor map. Click and drag the "N" symbol on the map until it points in that direction.

WOS will now prompt you to add APs to the map.

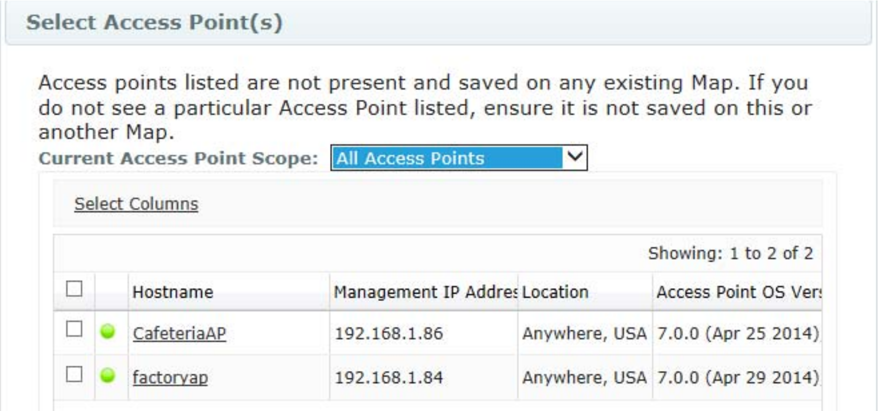
Adding APs to Maps

After you create a map and set its scale and set its north, the next step is to add APs to the map, locating them to match their physical locations as closely as possible. Each AP may only belong to one map at a time.

The procedure below describes how to add an AP to the map, move it, or delete it.

To add an AP to the map, use the following procedure.

1. Click the **Add APs** button. WOS displays the **Select APs** list.
2. Check the desired APs in the **Select APs** list as shown in Figure 158. If an AP already belongs to another map, it will not be shown on this list. If you need to add such an AP to this map, you will need to explicitly delete it from its current map first.
3. Click to select APs from the list.



Select Access Point(s)

Access points listed are not present and saved on any existing Map. If you do not see a particular Access Point listed, ensure it is not saved on this or another Map.

Current Access Point Scope: All Access Points

Select Columns

Showing: 1 to 2 of 2

☐		Hostname	Management IP Addres	Location	Access Point OS Ver
☐	●	CafeteriaAP	192.168.1.86	Anywhere, USA	7.0.0 (Apr 25 2014)
☐	●	factoryap	192.168.1.84	Anywhere, USA	7.0.0 (Apr 29 2014)

Figure 158. Adding APs to a Map

4. Click the **OK** button when done.

   The APs will appear on the map, and WOS prompts you to orient the APs. You must rotate each AP on the map to match the actual orientation of its monitor radio. This is critical for accurately calculating and displaying locations of stations and rogues. This also allows the heat contours to be correctly displayed on the map.

5. Move the APs to the proper location on the map. Click each AP and drag it to the desired position.
6. To remove one or more APs from the current map, select them and click the **Remove APs** button. You will be ask to verify the deletions. This will remove APs from the map without deleting them from the WOS database.
7. Remember to click the **Save Map** button to save your work.

Saving a Map

Always remember to save your map after making changes, since some map features may not be up to date until you save the map.

To save a map after making changes, click the **Save Map** button. Saving your map makes it available to all users of the WOS server.

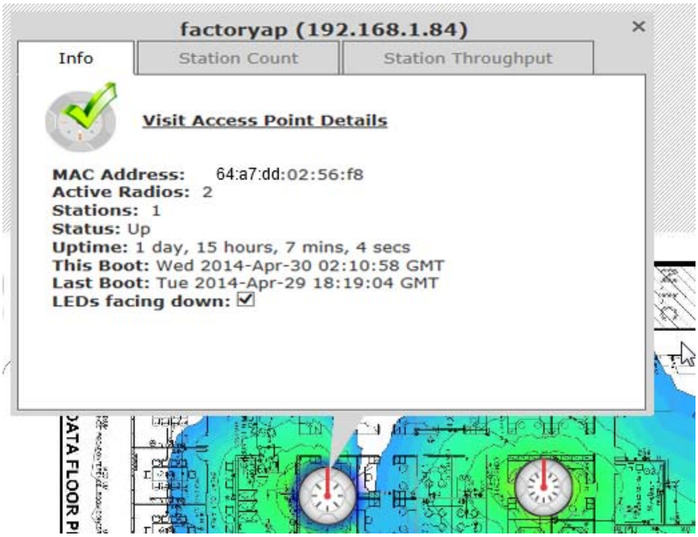
WOS will prompt you to save the map before it will allow you to switch to another web client page.

Viewing AP, Station, or Rogue Details

If you hover the mouse over an item on the map (AP, station, or rogue), WOS will show the hostname of the device and its IP address (or MAC address for rogue devices). To see additional information about an AP, double-click it (single click a station or rogue). The details shown differ according to the type of device.

AP Details

Double-clicking on an AP allows you to select from three tabs showing general AP **Info**, **Station Count**, or **Station Throughput**. (Figure 159) This is an abbreviated presentation of the same information that is shown on the **AP Details** page that you reach when you click on an entry on the **Access Points** page. In fact, you can go to that page by clicking the **Visit AP Details** link on the **Info** tab. For a description of any of the information presented on these tabs, please see **"AP Details" on page 68**.

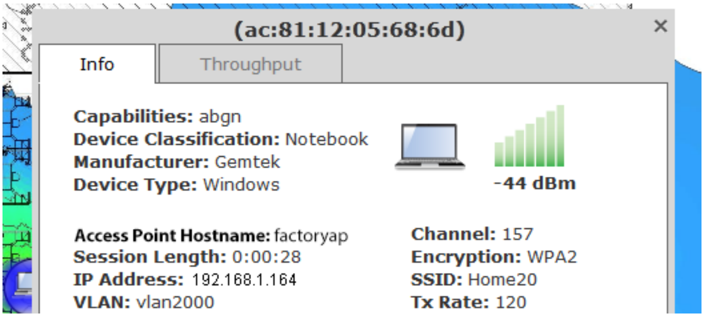


MAC Address: 64:a7:dd:02:56:f8
Active Radios: 2
Stations: 1
Status: Up
Uptime: 1 day, 15 hours, 7 mins, 4 secs
This Boot: Wed 2014-Apr-30 02:10:58 GMT
Last Boot: Tue 2014-Apr-29 18:19:04 GMT
LEDs facing down: ☑

Figure 159. Map AP Details

Station Details

Clicking on a station allows you to select from two tabs showing general **Info** or **Throughput**. (**Figure 160**) This is an abbreviated presentation of the same information that is shown on the Station Details page that you reach when you click on an entry on the **Stations** page. For a description of the information presented on these tabs, please see **"Stations" on page 85**.



Capabilities: abgn
Device Classification: Notebook
Manufacturer: Gemtek
Device Type: Windows

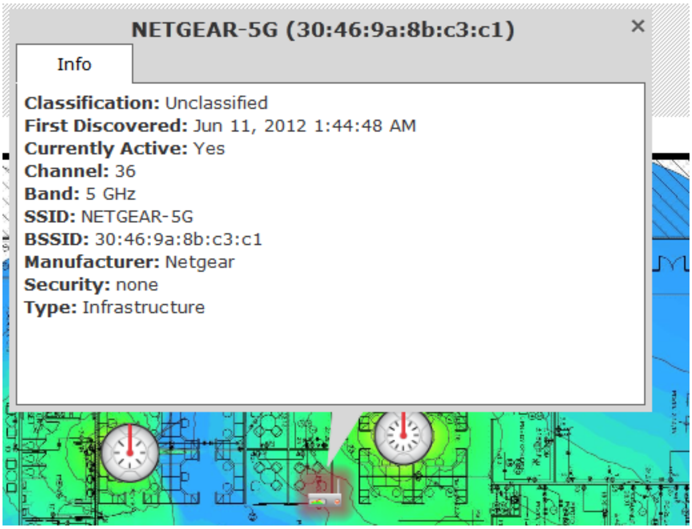
Access Point Hostname: factoryap
Session Length: 0:00:28
IP Address: 192.168.1.164
VLAN: vlan2000

Channel: 157
Encryption: WPA2
SSID: Home20
Tx Rate: 120

Figure 160. Map Station Details

Rogue Details

Clicking on a rogue shows general **Info** about the rogue. (**Figure 161**) This is an abbreviated presentation of the same information that is shown on the Rogue Details page that you reach when you click on an entry on the **Rogues** page. For a description of the information presented, please see **"The Rogues List" on page 91**.



Classification: Unclassified
First Discovered: Jun 11, 2012 1:44:48 AM
Currently Active: Yes
Channel: 36
Band: 5 GHz
SSID: NETGEAR-5G
BSSID: 30:46:9a:8b:c3:c1
Manufacturer: Netgear
Security: none
Type: Infrastructure

Figure 161. Map Rogue Details

Locating Devices

The WOS Location feature leverages the RF capability of the wireless AP to determine the position of a device to within a few meters and display it on the map. With this capability, you can track stations or rogues using your existing wireless infrastructure. WOS Location is available for stations that are associated to an AP that is a member of a map. For accuracy, this feature requires at least three APs, and the station or rogue should be located inside the region formed by the APs.

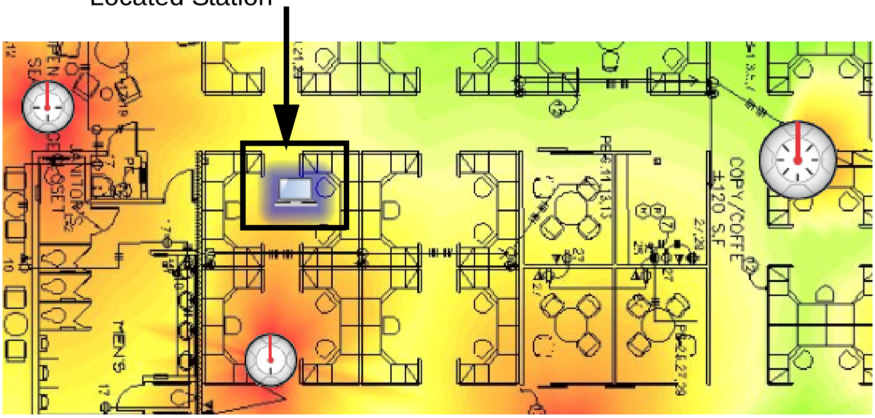

Located Station

Figure 162. Using the Location Feature

The location feature is described in the following sections:

- **Understanding Locationing**
- **Preparing to Use WOS Location**
- **Using WOS Location**

Understanding Locationing

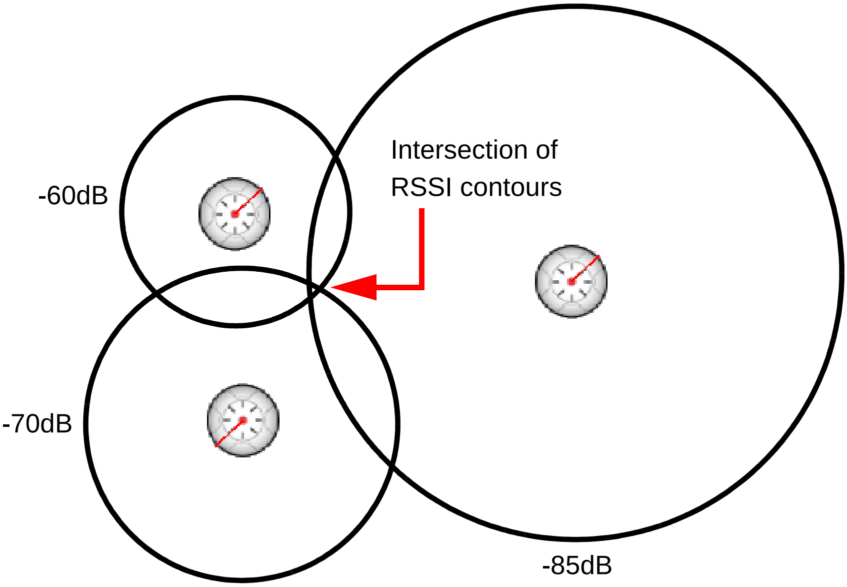


Figure 163. Determining Position

WOS uses a technique called trilateration based on received signal strength to determine the location of stations or rogues. When you request the location of stations, each AP that can hear a station's signal reports back, giving the received signal strength. The signal strength indicates the approximate distance of each station from the AP. A simplified representation of this is illustrated in **Figure 163**, showing the RF contour of the observed signal strength as a circle around the AP. Each circle shows possible locations of a station, based on that AP's signal strength observation. In the diagram, if there were only two APs reporting, the circles would intersect at two points, giving two possible locations for that station. When you add additional AP observations, the intersection of the circles defines the station's most likely location. Actually, WOS has much more information than a simple radius (circle) to work with, due to the advanced design of the WiFi AP. The AP's multiple directional radios also give information on the direction of the station. Rather than modeling the location of the station as a circle, the RF contour map is used. This map incorporates directional antenna coverage on a per radio basis, and readings are enhanced by means of inter-AP correction and take RF attenuation due to building construction into account.

Preparing to Use WOS Location

You must complete the following steps before locating a device to get the best results.

- **Planning**—WOS is able to locate a device most accurately when APs are located around the perimeter of the area to be monitored, as shown in **Figure 162 on page 236**. This is in contrast to placement of APs for greatest Wi-Fi coverage, where we recommend that you place APs away from exterior walls.
- **Adding a New Map**—Create a WOS map, using the most accurate graphic representation possible.
- **Environment Settings**—Set this according to the type of construction at your deployment site.
- **Setting the Map Scale and North Direction**—It is very important to set the scale accurately, as the placement of a located device depends critically on the scale of the map.
- **Adding APs to Maps**—As you place your APs on the map, be certain to get their locations as precise as possible. WOS will only locate stations that are associated to an AP that is a member of a map. The orientation of the APs must also be as accurate as possible.

Using WOS Location

There are two ways to use the Location feature:

- locate one specific station or rogue
- display all stations and/or rogues

Locate one specific station or rogue

The WOS location algorithm will locate a selected station that is associated to an AP on a map or a selected rogue that has been detected by an AP on a map.

1. Go to the **Monitor** > **Stations** window or the **Monitor** > **Rogues** window in the web client.
2. Select only one station or rogue that you wish to locate. Click the **Locate** button above the list.
3. WOS determines which map contains the AP to which the station is associated (for a rogue, it finds a map that has an AP that detected the rogue). That map window will be displayed, and the location of the station or rogue is displayed. See **Figure 162 on page 236**. You may click the station or rogue to see detailed information about it, as described in **“Viewing AP, Station, or Rogue Details” on page 233**.
4. If the associated AP is not a member of any map, an error message will inform you of this problem. You must add the AP to a map in order to locate the stations that are associated to it.

Only one station or rogue location may be displayed at a time using this method.

Display all stations and/or rogues

The WOS location algorithm will locate all stations and/or all rogues on a map. This method uses the Map Options panel.

1. Open the Map Options panel. See **“Map Options Panel” on page 247**.
2. To display stations, see **“Station Location” on page 253**.
3. To display rogues, see **“Rogue Location” on page 252**.

Deleting a Map

If you delete a map, the map is permanently removed from the database. Make sure you want to permanently delete the map before doing so.

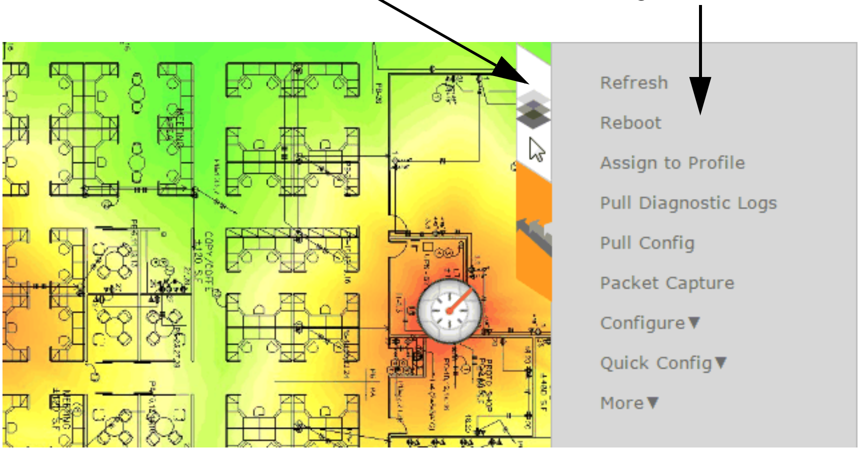
1. Select the map that you want to delete. Click the **Delete Map** button above the Maps List. You do not need to be in edit mode to delete a map. WOS will ask you to verify that you wish to delete the map.

If the selected map has any child maps, they will also be deleted.

Managing APs Within Maps

The map offers management functions for the APs shown on the map. These are the same actions that may be performed from the **Access Points (Configure)** window. Use the following procedure to manage APs from the map.

1. The map must be in Monitor Mode to perform AP management. Click the **Monitor Mode** button if necessary to switch to this mode. See **"Map Modes of Operation and User Privileges" on page 221**.
2. Select the APs that you wish to manage. You may use Ctrl + click to select multiple APs.
3. Click the tab as shown in **Figure 164** to display the AP Management Panel, which lists all of the available AP operations.


Click to Show or Hide Panel

AP Management Panel

Figure 164. AP Management Panel

4. Select the desired operation from the AP Management Panel. The results of the operation will be displayed. Some operations may take you to a different web client page so that you may enter additional information. For example, if you select **Configure > Radio Settings...**, you will be taken to the **Configure Wireless Settings** page to complete the operation.

In this example, the new page will list all radios that belong to the APs that you selected on the map.

The AP operations are summarized below. Please see **"The Configure APs Toolbar" on page 110** for detailed usage information.

- **Refresh**—this option refreshes discovery on the selected APs.
- **Reboot**—this option reboots the selected APs. You will be asked to confirm the operation.
- **Assign to Profile**—this option adds the selected APs to a profile.
- **Pull Diagnostic Logs**—this option initiates a task that instructs the selected APs to create a diagnostic log file. When the diagnostic log is complete, a link will appear. Click it to download the requested diagnostic results as a zip file.
- **Pull config**—this option pulls configuration files from the selected APs, containing each AP's current configuration. When the files are available, a link will appear. Click it to download the requested files as a zip file.
- **Packet Capture**—this option initiates packet capture on one or more selected APs. See **"About Packet Capture" on page 115**.
- **Configure** — select an option from this drop-down list to configure the selected APs.
  - You may modify **Network Settings** as described in **"Configure Network Settings" on page 141**.
  - You may modify **Radio Settings** as described in **"Configure Wireless Settings" on page 138**.
  - The **Optimize Channels** option computes the best channel assignments for the selected APs in the local RF environment. See **"RF Spectrum Management (Auto Channel Configuration)" on page 522**. The map is actually the best place to perform an auto channel. Since the map has information locating where the APs are in relationship to each other, auto channel is performed on the APs in the correct order to yield the best results. The options for auto channel are described in **"Channel Configuration" on page 253**.

Note that Auto Channel normally assigns individual channels. However, if you select ***Auto bond 5GHz channels*** *on the* **Global Settings .11n** *page, and have 40MHz channels set up prior to running Auto Channel, those bonds will be preserved. 80MHz bonds will not be preserved.*

  - **Optimize Bands** configuration is the recommended method for assigning bands to the abgn radios. It runs only on command, assigning radios to the 2.4GHz or 5GHz band when you click this link. The AP uses its radios to listen for other APs on the same channel, and it assigns bands based on where it finds the least interference. Auto band assigns as many radios to the 5 GHz band as possible when there are other APs within earshot. It does this by determining how many APs are in range and then picking the number of radios to place in the 2.4 GHz band. Auto band runs separately from auto channel configuration. If the band is changed for a particular radio, associated stations will be disconnected and will then reconnect.
  - **Optimize Cells** configuration is an automatic, self-tuning mechanism that adjusts radio power to balance cell size between the selected Access Points to optimize coverage while limiting the RF energy that could extend beyond the organizational boundary. For more information, see **"The Configure APs Toolbar" on page 110**.
  - **Enable/Disable Application Control**—this feature analyzes the application usage on your AP. Use these links to turn this feature on or off. See **"Application Control—Overview" on page 104** for more information. Application Control is only available on an AP if its license supports this feature.

- **Quick Config**—this offers predefined configuration options such as **Classroom** and **High-Density** that capture best practices from years of field experience. If one of the options in the drop-down list is appropriate to your deployment, select it. For example, the **High-Density** option uses best practices to configure the AP for high density settings such as lecture halls, convention centers, stadiums, etc.

- **More**
  - Choose the **Add to Access Point Group** option to add the selected APs to a group. A dialog box allows you to select an existing group or **Create a new group**.
  - Choose **Create Profile** to create a new profile that initially contains the selected Access Points. See **"Managing by Profiles" on page 195**.
  - Choose **AP WMI** to open a WMI session with the AP in a new browser window.
  - Choose the **Delete** option from the **More** drop-down list to delete the selected APs from the WOS database.
  - Choose the **Take AP(s) Out of Service** option from the **More** drop-down list to mark the selected APs as being out of service, so that they are no longer polled for status or data. This allows maintenance to be performed without having to remove the APs from the WOS database. These units will be displayed with a blue dot in the list of APs. Use the **Return AP(s) to Service** option to restore normal WOS operation for these APs.
- **Custom**—Any Custom Actions that you have created will appear in this drop-down list. Click on the desired action to apply it to the selected APs. See **"Create Custom Actions" on page 575** for more information.

Zooming or Moving the Map

The zoom and move controls (**Figure 165**) are located at the lower left of the map window.

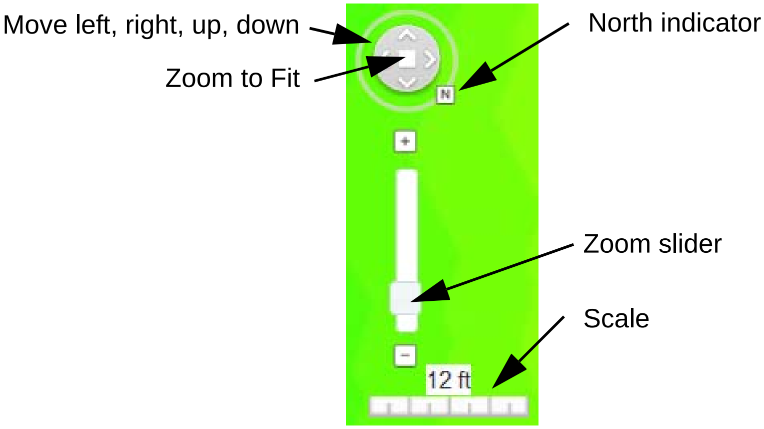


Figure 165. Map Zoom and Move Controls

Moving the Map

There are two ways to move the map:

- Click the arrow controls shown in **Figure 165** to move the map left, right, up, or down.
- Simply use the mouse to drag the map in the desired direction.

Zooming the Map

There are three ways to zoom the map:

- Click and drag the zoom slider shown in **Figure 165** to zoom in or out.
- Use the mouse wheel to expand or shrink map size.
- Click the Zoom to Fit square shown in **Figure 165** to resize the map so that the entire floorplan image fits in the current browser window.

The current scale of the map is indicated below the zoom slider.

Edit Mode Toolbar

This toolbar appears above the map when you click the Edit Mode button to switch to Edit Mode, as described in **“Map Modes of Operation and User Privileges” on page 221**.

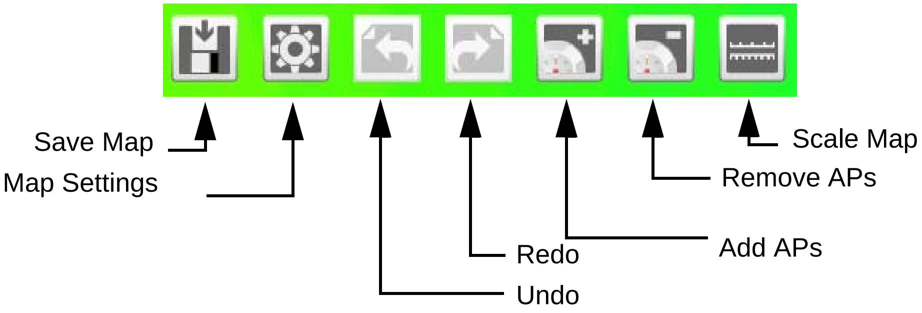


Figure 166. Map Edit Mode Toolbar

The following buttons are available, from left to right:

Save Map
Click to save changes to a map, as described in **“Saving a Map” on page 232**.

Edit Map Settings
Click here to change the **Environment Type** and **Adjustment**, **Display Units**, or even the **Name**. See **“Adding a New Map” on page 226**.

Undo
Click to undo the last change to a map, for example to undo the removal of an AP. This button is grayed out if there is nothing to undo.

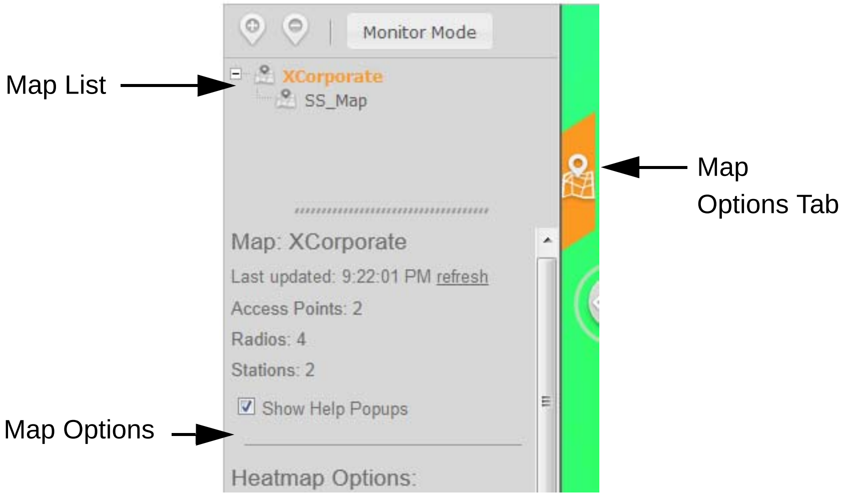
Redo
Click to redo the undo that was just performed. This button is grayed out if there is nothing to redo.

Add AP
Click to add APs to a map, as described in **"Adding APs to Maps" on page 231**.

Remove APs
Click to remove the selected APs (one or more) from a map. Note that the APs are only removed from the map. They are not deleted from the database.

Scale Map
Click to set the scale of the floor plan of the map, as described in **"Setting the Map Scale and North Direction" on page 228**.

Map Options Panel



Map: XCorporate
Last updated: 9:22:01 PM refresh
Access Points: 2
Radios: 4
Stations: 2
☑ Show Help Popups
Heatmap Options:

Figure 167. Map Options Panel

This panel is located to the left of the map. It may be accessed from both Edit Mode and Monitor Mode (see **"Map Modes of Operation and User Privileges" on page 221**). Click the Map Options tab to show or hide the panel. (**Figure 167**)

Its options affect a number of aspects of the map display. The types of options include:

- **Map Options** select whether to show help pop-ups and summarize the number of APs and stations shown on the map.
- **Heatmap Options** select the bands displayed (2.4 GHz/5 GHz) or channels displayed, the transparency of the heat map, and whether to show contour lines.
- **Performance Plan Options** specify the target usage for this plan. Select the number of stations, the bands in use (2.4 GHz/5 GHz/both), station device types (laptops, tablets, etc.), WiFi mode (802.11b, 802.11n 2x2, etc.), and the application in use (Browsing, VoIP, video HD, etc.).
- **Floorplan Options** select the transparency of the background floor map, the size of AP icons, and how much information to display for individual AP radios.
- **Rogue Location** shows rogues that have been detected.
- **Station Location** shows stations that are associated to APs.
- **Channel Configuration** performs an automated channel allocation procedure.

Map Options

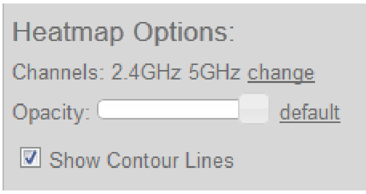
See **Figure 167**.

- Map Information—shows the name of the map and the time it was last refreshed. If you wish to update the map immediately, click the **refresh** link. This section also lists the number of APs, radios, and stations included on this map.

If you have made any changes to the map, it is a good idea to save them using **"Save Map" on page 246** *before clicking the refresh link.*

- Check the **Show Help Popups** box if you wish to see the helpful, red arrows that walk you step-by-step through setting up a new map (set north, scale, add APs, etc.).

Heatmap Options



Heatmap Options:

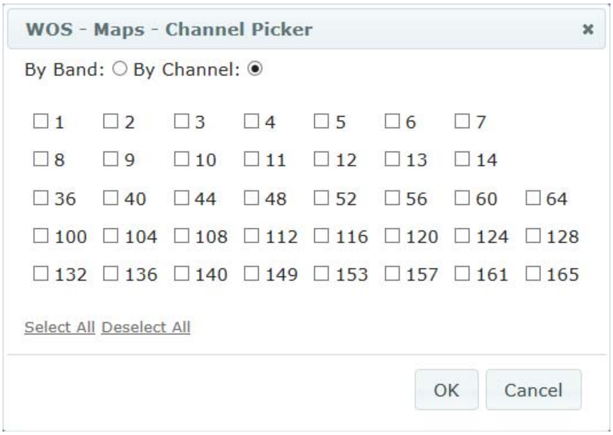
Channels: 2.4GHz 5GHz change

Opacity: default

☑ Show Contour Lines

Figure 168. Heatmap Options

- **Channels—**shows the Bands or Channels included on the map. If you wish to filter the heat map to include signal strength for only a selected band or only particular channels, click the **change** link.



WOS - Maps - Channel Picker ×

By Band: ○ By Channel: ●

□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

□ 8 □ 9 □ 10 □ 11 □ 12 □ 13 □ 14

□ 36 □ 40 □ 44 □ 48 □ 52 □ 56 □ 60 □ 64

□ 100 □ 104 □ 108 □ 112 □ 116 □ 120 □ 124 □ 128

□ 132 □ 136 □ 140 □ 149 □ 153 □ 157 □ 161 □ 165

Select All Deselect All

OK Cancel

Figure 169. Map Channel Selection

You may click the **By Band** radio button to select the 2.4GHz or 5GHz band. By default, both of these are shown on the map.

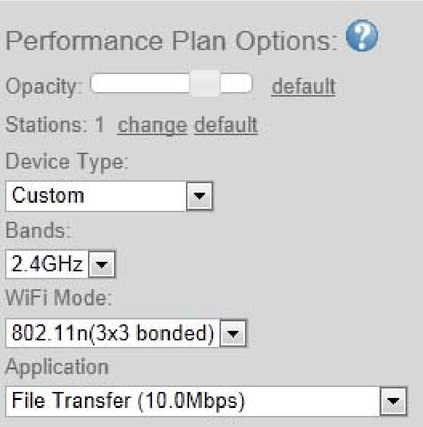
To show only selected channels, click the **By Channel** radio button and check off the desired channels. (**Figure 169**)

- The **Opacity** slider adjusts the transparency of the heat map colors. Slide it to the left to make the colors more transparent, or to the right to make them more opaque (darker). To restore the map to the default level of color display, click the **default** link.

- Check the **Show Contour Lines** box if you wish to see lines separating the regions of different signal strength gradation on the heat map.

Performance Plan Options

Expected throughput is computed using the following characteristics. Note that observed performance of the network and current settings on AP radios are also used as inputs to the predictive analysis.



Performance Plan Options:

Opacity: default

Stations: 1 change default

Device Type: Custom

Bands: 2.4GHz

WiFi Mode: 802.11n(3x3 bonded)

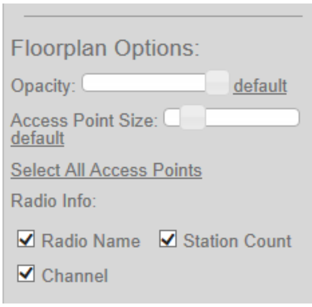
Application File Transfer (10.0Mbps)

Figure 170. Performance Plan Options

- **Stations**—number of stations on the map. This starts out as the actual number of stations currently associated to APs on the map (or one, if there are no stations). To increase the number of stations to observe the predicted decrease in performance or to experiment with how far you should decrease the station count to improve performance, click the **change** link. To restore the number of stations to the default value, click the **default** link. The maximum number of stations that you can enter is 240 times the number of radios on the map.
- **Device Type**—select the type of device that you wish to analyze, e.g., smartphone, tablet, business computer. Note that devices have preset parameters. For example, the smart phone’s band is set to 2.4GHz. If you change any of these preset values, the device type automatically changes to **Custom**.

- **Bands**—select the wireless band that you wish to analyze, 2.4 GHz, 5 GHz, or both.
- **WiFi Mode**—select the Wi-Fi mode that you wish to analyze, e.g., 802.11b. Then select the type of device that you wish to analyze, e.g., 802.11n (3x3 bonded), etc. Your choices will vary based on the **Bands** setting. For example, 802.11b and 802.11g will not be offered if you selected 5 GHz only. For 802.11n or .11ac, select the number of antennas assumed for all of the radios (1x1, 2x2, or 3x3). Bonded and unbonded channel choices are offered.
- **Application**—select the type of usage that you wish to model for this plan. The various options are listed together with the assumed load that they put on the network. For example, VoIP is 0.5 Mbps, while file transfer is 10 Mbps.
- **Opacity**—this slider simply adjusts the transparency of the plan colors. Slide it to the left to make the colors more transparent, or to the right to make them more opaque (darker). To restore the plan to the default level of color display, click the **default** link.

Floorplan Options



Floorplan Options:

Opacity: default

Access Point Size: default

Select All Access Points

Radio Info:

☑ Radio Name ☑ Station Count

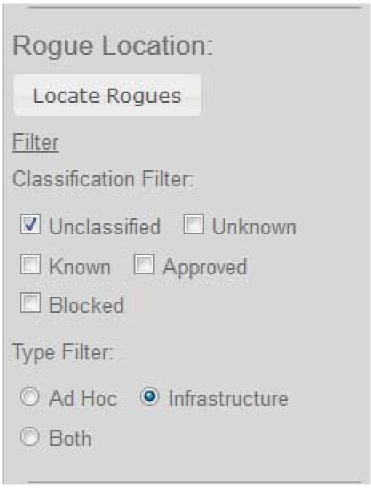
☑ Channel

Figure 171. Map Floorplan Options

- The **Opacity** slider adjusts the transparency of the background floorplan image. Slide it to the left to make the image more transparent, or to the right to make it more opaque (darker). To restore the map to the default display, click the **default** link.

- The AP **Size** slider adjusts the display size of the AP icons. To restore APs to the default display size, click the **default** link.
- Check the **Radio Info** boxes to customize the information shown if you enable display of the radio Info layer (see **"Radio Info" on page 256**). You may show or hide display of **Radio Name**, **Station Count**, and **Channel** on the radios.

Rogue Location



Classification Filter:

☑ Unclassified ☐ Unknown

☐ Known ☐ Approved

☐ Blocked

Type Filter:

○ Ad Hoc ● Infrastructure

○ Both

Figure 172. Map Rogue Location Options

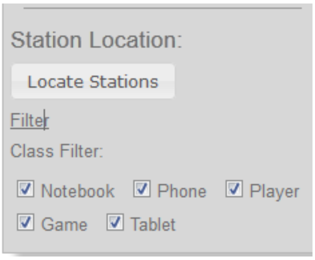
- Click **Locate Rogues** to show rogues that have been detected by APs on this map. Rogues will not be shown until you click this button. WOS will also enable the **Rogues** in order to display rogues on the map. Up to 100 rogues will be shown.
- Click the **Filter** link if you wish to display only rogues that meet certain criteria. You may filter by **Classification**, **Type**, or both.

  The **Classification Filter** allows you to select rogues that match the selected classifications: **Unclassified**, **Unknown**, **Known**, **Approved**, or **Blocked**. See **"Rogues" on page 90** for more information.

The **Type Filter** allows you to select rogues that have the selected types of wireless network: **Ad Hoc**, **Infrastructure**, or **Both**.

If the monitor radios of some APs on this map are set to Timeshare mode, rogue location information from these APs may not be sufficient to identify and locate rogues. See **"RF Monitor" on page 520**.

Station Location



Class Filter:

☑ Notebook ☑ Phone ☑ Player
☑ Game ☑ Tablet

Figure 173. Map Station Location Options

- Click **Locate Stations** to show stations that are associated to APs on this map. Stations will not be shown until you click this button. WOS will also enable the **Stations** in order to display stations on the map. Up to 100 stations will be shown.
- Click the **Filter** link if you wish to display only stations that meet certain criteria. You may filter by **Type**. Select as many of the following as you wish: **Notebook**, **Phone**, **Player**, **Game**, or **Tablet**.

Channel Configuration

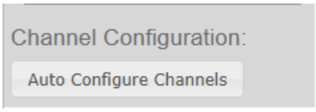
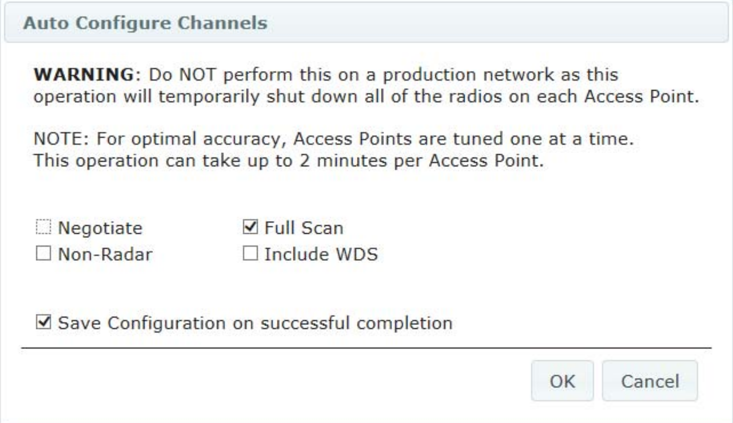


Figure 174. Auto Channel Configuration

- Click **Channel Configuration**—Automatic channel configuration is the recommended method for channel allocation, and the map is the best place to perform this process. Since the map has information locating where the APs are in relationship to each other, auto channel is performed on all of the APs on the map (regardless of which are selected) in the correct order to yield the best results. Each AP determines the best channel allocation settings for each enabled radio and selects the channel automatically, based on changes in the environment. A dialog allows you to specify the following options. (**Figure 175**)

- **Negotiate**: negotiate air-time with other APs before performing a full scan. Negotiating is slower, but if multiple APs are configuring channels at the same time the Negotiate option ensures that multiple APs don't select the same channels. Turning off the Negotiate option allows the **Auto Configure** button to manually perform auto channel without waiting, and may be used when you know that no other nearby APs are configuring their channels.
- **Full Scan**: perform a full traffic scan on all channels on all radios to determine the best channel allocation.
- **Non-Radar**: give preference to channels without radar-detect. See table in **"Procedure for Configuring Global 802.11a Radio Settings" on page 507**.
- **Include WDS**: automatically assign 5GHz to WDS client links.



Auto Configure Channels

WARNING: Do NOT perform this on a production network as this operation will temporarily shut down all of the radios on each Access Point.

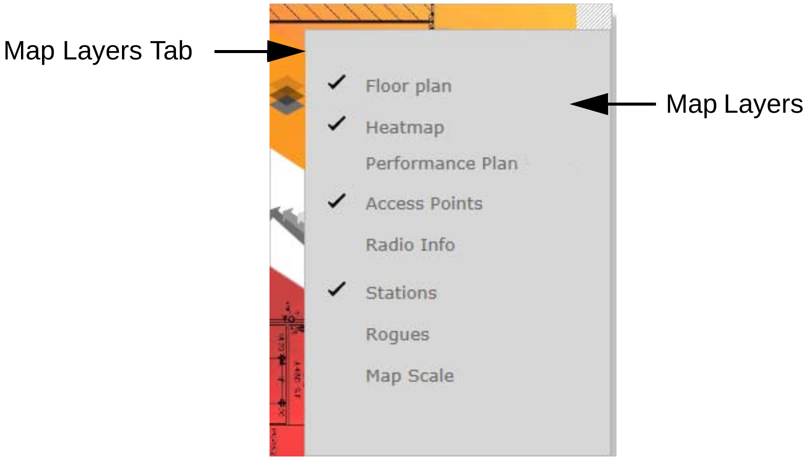
NOTE: For optimal accuracy, Access Points are tuned one at a time. This operation can take up to 2 minutes per Access Point.

□ Negotiate ☑ Full Scan
□ Non-Radar □ Include WDS

☑ Save Configuration on successful completion

Figure 175. Map Auto Channel Options

Map Layers Panel



✓ Floor plan

✓ Heatmap

Performance Plan

✓ Access Points

Radio Info

✓ Stations

Rogues

Map Scale

Figure 176. Map Layers Panel

This panel is located to the right of the map. It may be accessed from both Edit Mode and Monitor Mode (see **"Map Modes of Operation and User Privileges" on page 221**). Click the Map Layers tab to show or hide the panel. (**Figure 176**) Its options enable or disable the display of a number of types of information on the map. The types of layers include:

- **Floorplan**
- **Heatmap**
- **Performance Plan**
- **APs**
- **Radio Info**
- **Stations**
- **Rogues**
- **Map Scale**

Floorplan

When enabled, this layer shows your floorplan image in the background. Note that you can modify the transparency of this image. See **"Floorplan Options" on page 251**.

Heatmap

When enabled, this layer indicates RF signal strength with a color heat map. Note that you can modify the transparency of the color display and enable or disable the display of contour lines. See **"Heatmap Options" on page 249**.

Performance Plan

When enabled, this layer shows predicted throughput over the map based on the type of usage you select.

APs

When enabled, this layer shows the location of APs on the map.

Radio Info

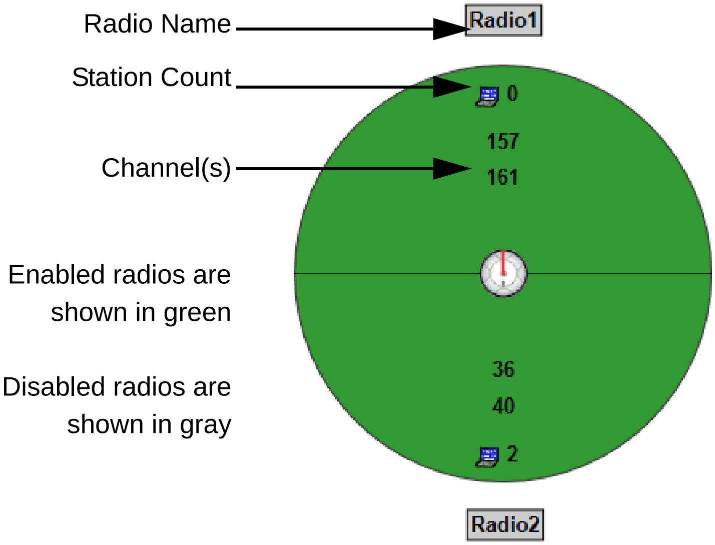

Radio Name
Radio1
Station Count
0
Channel(s)
157
161
Enabled radios are shown in green
Disabled radios are shown in gray
36
40
2
Radio2

Figure 177. Radio Info Layer

When enabled, this layer shows each AP's radios on the map. Active radios are green, disabled radios are gray, and radio failure is shown in red. (**Figure 177**) By default, each radio is labeled with its name, its station count (the number of stations associated to it), and the channel that it is using. Note that IEEE 802.11n or .11ac radios may use a bonded set of channels, and may show all channel numbers included in this bond.

You may customize the information shown. See **Radio Info** **"Floorplan Options" on page 251**.

Stations

This enables and disables the display of stations on the map. After you enable this layer, you must take one more action to display stations:

- To view all stations, you must also use the **Locate Stations** button once so that WOS will locate all the stations on the map. If you have selected any **Filters**, then only the stations meeting the criteria will be shown. See **"Display all stations and/or rogues" on page 239**.
- To view only one selected station, you must also select that station on the Monitor > **Stations** window, and use the **Locate** button. See **"Locate one specific station or rogue" on page 239**.

Rogues

This enables and disables the display of rogues on the map. After you enable this layer, you must take one more action to display rogues:

- To view all rogues, you must also use the **Locate Rogues** button once so that WOS will locate all the rogues on the map. If you have selected any **Filters**, then only the rogues meeting the criteria will be shown. See **"Display all stations and/or rogues" on page 239**.
- To view only one selected rogue, you must also select that rogue on the Monitor > **Rogues** window, and use the **Locate** button. See **"Locate one specific station or rogue" on page 239**.

Map Scale

If you wish to show the map scale, you must enable this.

Managing Reports

WOS generates performance reports about the network, all wireless APs within the network, the individual radios contained within each AP, and wireless data (channels, throughput, signal strength, etc.). Selection criteria allow you to focus your reports on just the data that is of interest.

Click the **Reports** link in the main menu at the top of the page to access the reports pages.

This chapter provides instructions for managing and reviewing these reports via the web client. Section headings for this chapter include:

- **"About Reports" on page 259**
- **"Application Control Reports" on page 279**
- **"Traffic Reports" on page 292**
- **"Station Reports" on page 322**
- **"Access Point Reports" on page 350**
- **"RF Reports" on page 357**
- **"Security Reports" on page 360**

Note that smaller APs that use the AOSLite system software, such as the WAP9112 and WAP9114, do not contribute data to all reports. In particular, they do not generate any radio (wireless) statistics.

About Reports

Reports provide information about the content, performance and usage of your network(s) and APs. Most reports display a combination of graphs and text-based information organized in tabular form.

There are three main reports pages:

- **View Reports**—The web client's **Reports** button opens to the **View Reports** page, listing all of the reports you have already created and allowing you to view or run these reports.

- **Create Report**—Click this link to list all the types of reports that you can create. Click on a report, and a form allows you to enter all the selection criteria for your report. You may then save the report setup, and run it now or schedule it for later.
- **Customize Report Header**—Click this link to customize the appearance of reports by changing the logo at the top of the report.

Selection Criteria differ according to the type of report, but most reports use similar criteria such as defining the group of APs and time period to consider for the report.

Reports are not to be confused with events and alarms, which provide alerts when the system encounters problems. For information about events and alarms, go to **"Alarms" on page 98** and **"Events" on page 101**.

Sample reports shown in this chapter may show multiple APs managed by WOS. In some cases you may see examples where only one AP is under management. The results are the same regardless of how many APs are being addressed.

Topics for this section include:

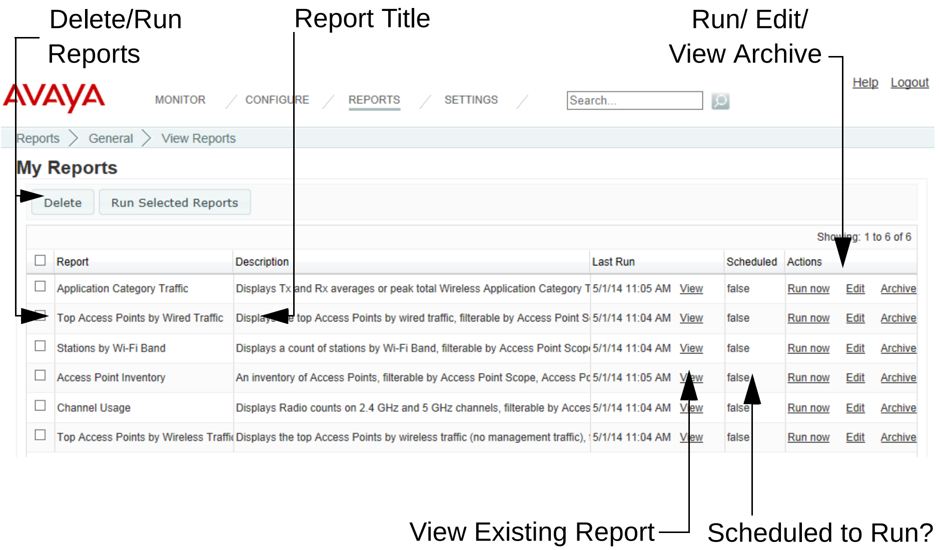
- **"View Reports" on page 261**
- **"Viewing a Report" on page 263**
- **"Create Report" on page 267**
- **"Selection Criteria" on page 274**
- **"Customize Report Header" on page 278**

The data in most reports is delayed by 30 minutes. Exceptions are AP Inventory, AP Availability, Station Assurance, and IDS Events, which show current data. If a report is based on delayed data, it will state that fact.

View Reports

To access reports, click the **Reports** button at the top of the web client window. The initial window always defaults to the **View Reports** page. If you are on one of the other Reports pages, click the **View Reports** link to return to this page.

This page lists all of the reports that you have already created using the **Create Report** link. You may view latest or archived report results, run the report, or edit report parameters from this page. The list of reports may be sorted by clicking on the column header for the **Report**, **Last Run**, or **Scheduled** columns. Click again to reverse the sort order.



My Reports

Showing: 1 to 6 of 6

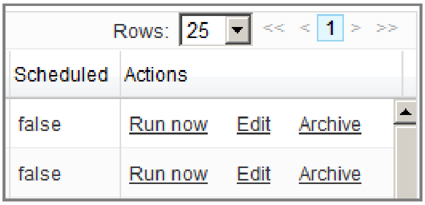
□	Report	Description	Last Run		Scheduled	Actions		
□	Application Category Traffic	Displays Tx and Rx averages or peak total Wireless Application Category T	5/1/14 11:05 AM	View	false	Run now	Edit	Archive
□	Top Access Points by Wired Traffic	Displays the top Access Points by wired traffic, filterable by Access Point S	5/1/14 11:04 AM	View	false	Run now	Edit	Archive
□	Stations by Wi-Fi Band	Displays a count of stations by Wi-Fi Band, filterable by Access Point Scop	5/1/14 11:04 AM	View	false	Run now	Edit	Archive
□	Access Point Inventory	An inventory of Access Points, filterable by Access Point Scope, Access Pc	5/1/14 11:05 AM	View	false	Run now	Edit	Archive
□	Channel Usage	Displays Radio counts on 2.4 GHz and 5 GHz channels, filterable by Acces	5/1/14 11:04 AM	View	false	Run now	Edit	Archive
□	Top Access Points by Wireless Traffi	Displays the top Access Points by wireless traffic (no management traffic),	5/1/14 11:04 AM	View	false	Run now	Edit	Archive

Figure 178. View Reports Window

The following information is displayed for each report:

- **Report—**this is the **Name** that you assigned when you created the report. To delete a report, select the checkbox to the left of it, then click the **Delete** button at the top left. Select as many reports as you wish for deletion. You may click the checkbox in the header row to select or deselect all reports.

- **Description—**this is a general description of this type of report.
- **Last Run—**this column lists the time that the report was most recently run, if any. Click the **View** link to see that report. For a description of the options available, see **"Viewing a Report" on page 263**).
- **Scheduled—true** indicates that the report has been scheduled to run at some time in the future.



Rows: 25 << < 1 > >>

Scheduled	Actions
false	Run now Edit Archive
false	Run now Edit Archive

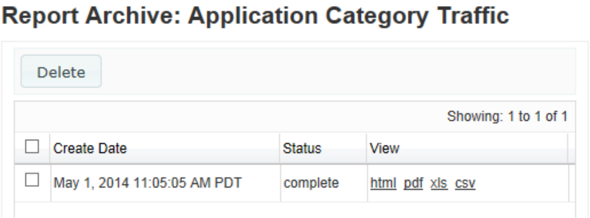
Figure 179. Actions for Reports

- **Actions (Figure 179)—**this column allows you run or edit this report, or see all of its saved runs.

  Click **Run Now** to start a report immediately. The **Report Queue** page will be displayed, showing the status of the report. You may go to other web client pages to perform tasks while the report is generated. Generating reports may take some time on large AP networks.

  Click **Edit** to change the selection criteria for the report. This displays the same fields you entered when you originally used **Create Report** to create the report, as described in **"Selection Criteria" on page 274**. You may change any field, including the report's **Name**. Note that this report will *replace* the edited report, even if you change the name (i.e., you will not have entries listed on the View Reports page for the old name and the edited name—the Archive entries that were created with the old name will still be there under the new name).

  Click **Archive** to list all of the saved copies of this report. (**Figure 180**) Each time a report is run, it is automatically saved with a date/time stamp. The archive lists these reports in the order that they were run. Click the desired format for a report: **html**, **Excel**, **pdf**, or **csv**. You may choose to save the resulting file to your file system, or display it immediately (the appropriate software is automatically used). For example, a CSV file is displayed by Excel. See **“Viewing a Report” on page 263** for more details. You may click the **Delete** link in front of a report if you wish to remove it.



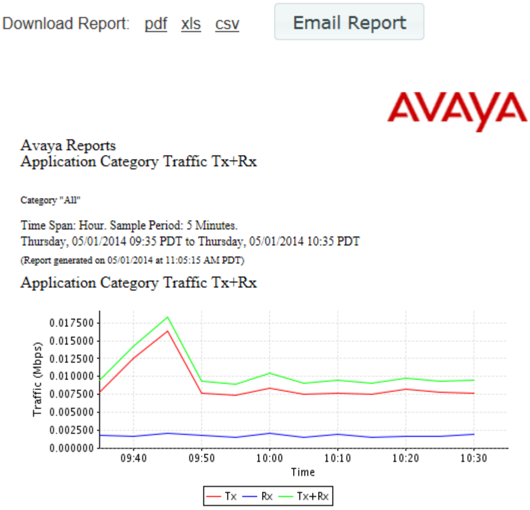
Report Archive: Application Category Traffic

Showing: 1 to 1 of 1

□	Create Date	Status	View
□	May 1, 2014 11:05:05 AM PDT	complete	html pdf xls csv

Figure 180. Archived Reports List

Viewing a Report



Download Report: pdf xls csv

Avaya Reports
Application Category Traffic Tx+Rx

Category "All"

Time Span: Hour. Sample Period: 5 Minutes.
Thursday, 05/01/2014 09:35 PDT to Thursday, 05/01/2014 10:35 PDT
(Report generated on 05/01/2014 at 11:05:15 AM PDT)

Application Category Traffic Tx+Rx

Figure 181. Viewing a Report

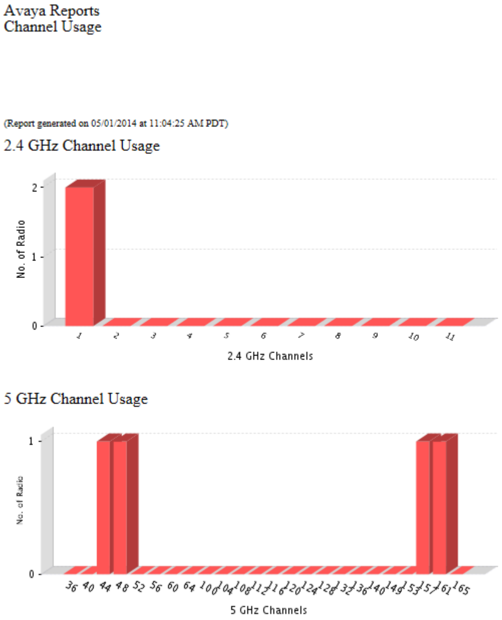
You may select a report for viewing from two places on the **View Reports** page:

- Click the desired report’s **View** link in the **Last Run** column. (**Figure 181**)

- Click the desired report's **Archive** link in the **Actions** column to choose the report with the desired time stamp. Click the **html** link to view the report as shown in **Figure 180**.

When you create and run a report from the **Create Report** page, it is automatically displayed when it is complete. To view the report again at a later time, go to the **View Reports** page to view the report in one of the two ways just described.

The selected report is displayed in the web client. Some types of report only have text (**Figure 181**), while others may include charts (**Figure 182**). Information included in the report is determined by the **Selection Criteria** that you set up when creating the report.



Avaya Reports
Channel Usage

(Report generated on 05/01/2014 at 11:04:25 AM PDT)

2.4 GHz Channel Usage

5 GHz Channel Usage

Figure 182. Report Including Charts

If the report had a time span setting, then the **Time Span** that you selected is shown underneath the title. It also identifies the data collection **Sample Period** used for the report. The sample period is automatically determined based on the

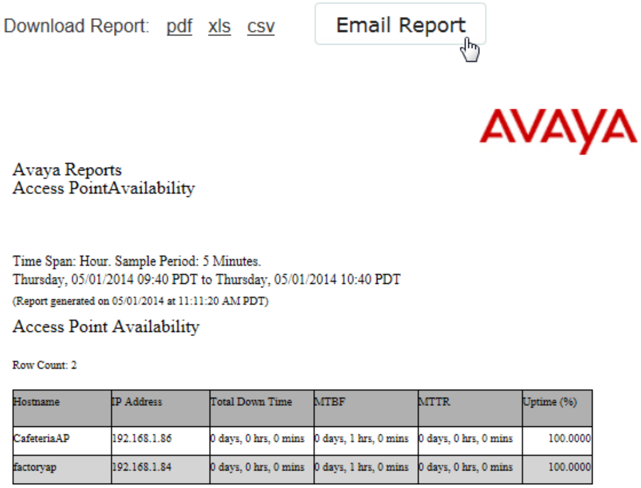
Time Span. For long time spans, such as a year, the period will be longer (e.g., one day). Short reporting periods, such as an hour, will be more granular and may have a period of 5 minutes.

The report may only be viewed as presented. You cannot sort columns or resize their width. Note that for very long reports, the HTML version is truncated to three pages so it will be able to be loaded in a browser. To view the full report, download it in PDF format as described below.

To download or view the report in a format other than HTML, select **pdf**, **xls**, or **csv** from the top of the page. The **File Download** dialog box will ask whether you wish to **Open** or **Save** the file. Select **Save** to specify where to save the file in your file system. Select **Open** to view the file using the appropriate software. By default, Acrobat is used to open PDFs and Excel is used for .csv and .xls files (unless you have changed the settings on your computer to open these files with a different application).

To print the report, we recommend that you download it as a PDF and print it from Acrobat.

To email the report, click the **Email Report** button at the top. (**Figure 183**) (Note that this button may not be displayed if you have not specified a mail server that WOS can use to send emails, as described in **“Email Settings” on page 588**.)



Avaya Reports
Access PointAvailability

Time Span: Hour. Sample Period: 5 Minutes.
Thursday, 05/01/2014 09:40 PDT to Thursday, 05/01/2014 10:40 PDT
(Report generated on 05/01/2014 at 11:11:20 AM PDT)

Access Point Availability

Row Count: 2

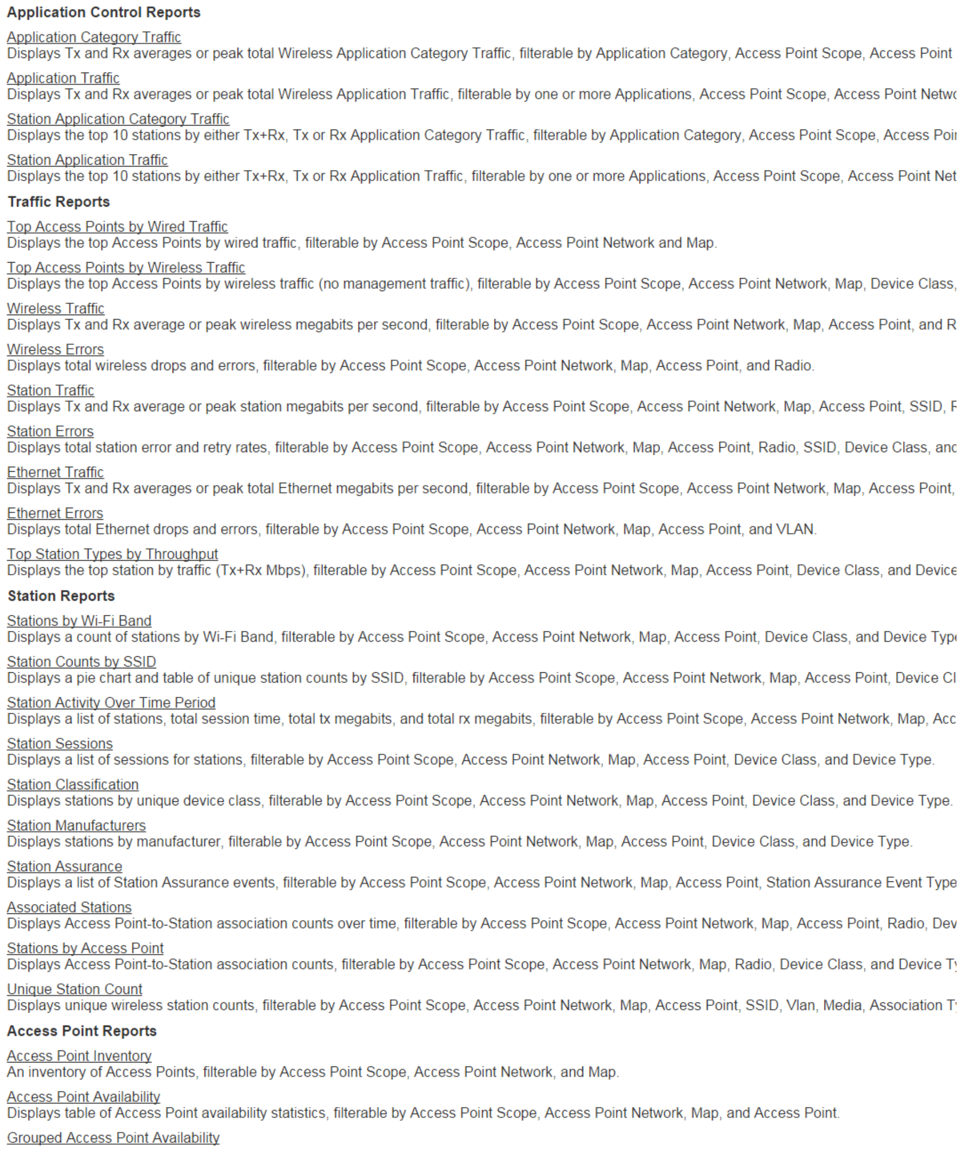
Hostname	IP Address	Total Down Time	MTBF	MTTR	Uptime (%)
CafeteriaAP	192.168.1.86	0 days, 0 hrs, 0 mins	0 days, 1 hrs, 0 mins	0 days, 0 hrs, 0 mins	100.0000
factoryap	192.168.1.84	0 days, 0 hrs, 0 mins	0 days, 1 hrs, 0 mins	0 days, 0 hrs, 0 mins	100.0000

Figure 183. Emailing a Report

The web client will prompt you to enter the email address, then click **OK**. A message will appear near the top of the page when the email has been successfully sent. The email displays the report in the same format shown on the web client page (i.e., HTML format), and there will be three attachments, one for each other format (PDF, .xls, .csv). Be aware that for large reports, the email size may be quite large.

Create Report

To create a new report, click the **Reports** button at the top of the web client window, then click the **Create Report** link.



Application Control Reports

Application Category Traffic
Displays Tx and Rx averages or peak total Wireless Application Category Traffic, filterable by Application Category, Access Point Scope, Access Point

Application Traffic
Displays Tx and Rx averages or peak total Wireless Application Traffic, filterable by one or more Applications, Access Point Scope, Access Point Netwo

Station Application Category Traffic
Displays the top 10 stations by either Tx+Rx, Tx or Rx Application Category Traffic, filterable by Application Category, Access Point Scope, Access Poi

Station Application Traffic
Displays the top 10 stations by either Tx+Rx, Tx or Rx Application Traffic, filterable by one or more Applications, Access Point Scope, Access Point Net

Traffic Reports

Top Access Points by Wired Traffic
Displays the top Access Points by wired traffic, filterable by Access Point Scope, Access Point Network and Map.

Top Access Points by Wireless Traffic
Displays the top Access Points by wireless traffic (no management traffic), filterable by Access Point Scope, Access Point Network, Map, Device Class,

Wireless Traffic
Displays Tx and Rx average or peak wireless megabits per second, filterable by Access Point Scope, Access Point Network, Map, Access Point, and R

Wireless Errors
Displays total wireless drops and errors, filterable by Access Point Scope, Access Point Network, Map, Access Point, and Radio.

Station Traffic
Displays Tx and Rx average or peak station megabits per second, filterable by Access Point Scope, Access Point Network, Map, Access Point, SSID, F

Station Errors
Displays total station error and retry rates, filterable by Access Point Scope, Access Point Network, Map, Access Point, Radio, SSID, Device Class, anc

Ethernet Traffic
Displays Tx and Rx averages or peak total Ethernet megabits per second, filterable by Access Point Scope, Access Point Network, Map, Access Point,

Ethernet Errors
Displays total Ethernet drops and errors, filterable by Access Point Scope, Access Point Network, Map, Access Point, and VLAN.

Top Station Types by Throughput
Displays the top station by traffic (Tx+Rx Mbps), filterable by Access Point Scope, Access Point Network, Map, Access Point, Device Class, and Device

Station Reports

Stations by Wi-Fi Band
Displays a count of stations by Wi-Fi Band, filterable by Access Point Scope, Access Point Network, Map, Access Point, Device Class, and Device Typ

Station Counts by SSID
Displays a pie chart and table of unique station counts by SSID, filterable by Access Point Scope, Access Point Network, Map, Access Point, Device Cl

Station Activity Over Time Period
Displays a list of stations, total session time, total tx megabits, and total rx megabits, filterable by Access Point Scope, Access Point Network, Map, Acc

Station Sessions
Displays a list of sessions for stations, filterable by Access Point Scope, Access Point Network, Map, Access Point, Device Class, and Device Type.

Station Classification
Displays stations by unique device class, filterable by Access Point Scope, Access Point Network, Map, Access Point, Device Class, and Device Type.

Station Manufacturers
Displays stations by manufacturer, filterable by Access Point Scope, Access Point Network, Map, Access Point, Device Class, and Device Type.

Station Assurance
Displays a list of Station Assurance events, filterable by Access Point Scope, Access Point Network, Map, Access Point, Station Assurance Event Type

Associated Stations
Displays Access Point-to-Station association counts over time, filterable by Access Point Scope, Access Point Network, Map, Access Point, Radio, Dev

Stations by Access Point
Displays Access Point-to-Station association counts, filterable by Access Point Scope, Access Point Network, Map, Radio, Device Class, and Device T

Unique Station Count
Displays unique wireless station counts, filterable by Access Point Scope, Access Point Network, Map, Access Point, SSID, Vlan, Media, Association T

Access Point Reports

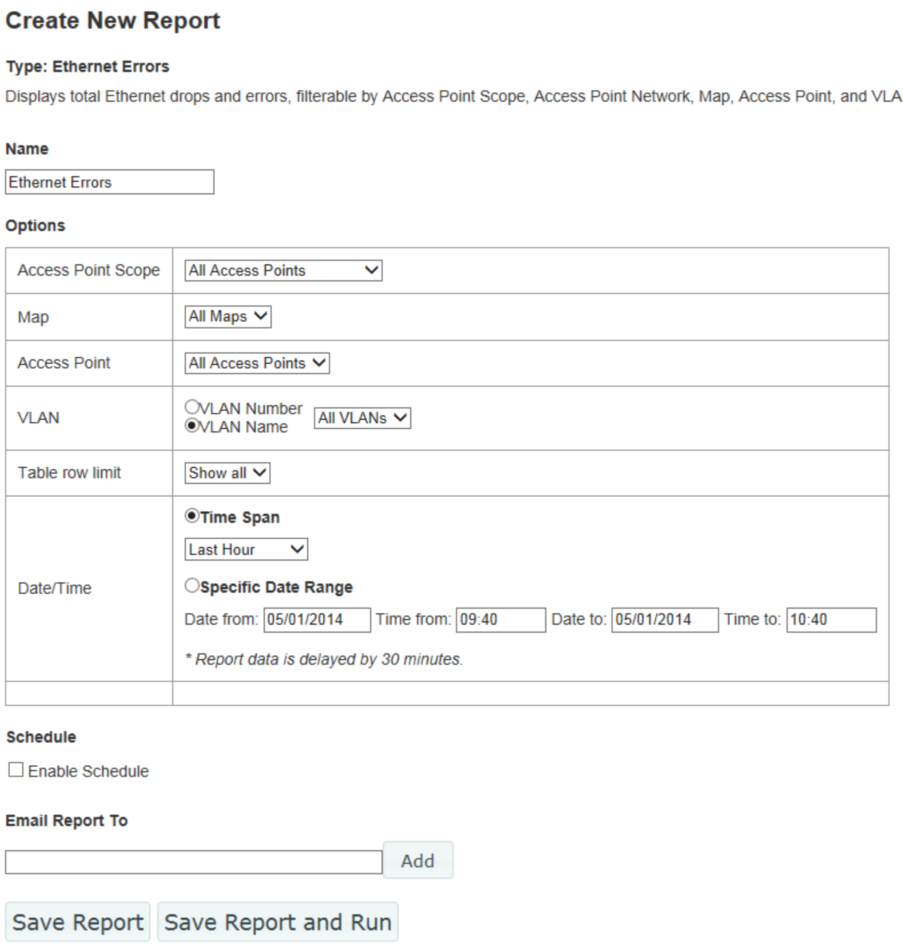
Access Point Inventory
An inventory of Access Points, filterable by Access Point Scope, Access Point Network, and Map.

Access Point Availability
Displays table of Access Point availability statistics, filterable by Access Point Scope, Access Point Network, Map, and Access Point.

Grouped Access Point Availability

Figure 184. List of Create Report Types

This page lists all of the report types offered by the web client. Click the desired report type, and the **Create Report** page for the chosen report type is displayed. (**Figure 185**)



Create New Report

Type: Ethernet Errors

Displays total Ethernet drops and errors, filterable by Access Point Scope, Access Point Network, Map, Access Point, and VLAN.

Name

Ethernet Errors

Options

Access Point Scope	All Access Points
Map	All Maps
Access Point	All Access Points
VLAN	○ VLAN Number ● VLAN Name All VLANs
Table row limit	Show all
Date/Time	● **Time Span** Last Hour ○ **Specific Date Range** Date from: 05/01/2014 Time from: 09:40 Date to: 05/01/2014 Time to: 10:40 ** Report data is delayed by 30 minutes.*

Schedule

□ Enable Schedule

Email Report To

Figure 185. Create Report Page

The **Create Report** page sets up the name and parameters for a report, especially the selection criteria use to filter the data included in the report. You may choose to run the report immediately after creating it, schedule it to run later at a specific time, or just save it without running it. Regardless, the report setup is always saved to the **View Reports** list, where you may run it or view previous results at any time. You may also choose to email the report after it runs.

The following topics are discussed for the Create Reports page:

- **"Types of Reports" on page 269**
- **"To create a report" on page 271**
- **"Report Queue" on page 273**

Types of Reports

There are five categories of reports, listed below. Each report type may be filtered to select only the desired data. For example, you may select only certain APs or AP groups to include in the report. For details, see **"Selection Criteria" on page 274**. The available selection criteria vary for each report. They are listed in the detailed description of each report.

Application Control Reports

These reports display wireless traffic statistics for selected applications or categories of applications.

- **Application Category Traffic**—shows Tx and Rx averages or peak total wireless traffic for a category of applications.
- **Application Traffic**—shows Tx and Rx averages or peak total wireless traffic for selected applications.
- **Station Application Category Traffic**—shows the top 10 stations by either Total, Tx or RX Application Category Traffic.
- **Station Application Traffic**—shows the top 10 stations by either Total, Tx or RX Application Traffic.

Traffic Reports

These reports display wireless traffic and error statistics for radios, Ethernet ports, and stations.

- **Top APs by Wired Traffic**—shows the ten APs with the highest level of wired traffic.
- **Top APs by Wireless Traffic**—shows the ten APs with the highest level of wireless traffic (not including management traffic).
- **Wireless Traffic**—Tx and Rx average or peak megabits per second. The wireless reports include all the data from the station reports (below) plus Wi-Fi management traffic such as beacons, probe requests, etc.
- **Wireless Errors**—total wireless drops and errors.
- **Station Traffic**—Tx and Rx average or peak megabits per second for traffic that flows to or from all associated stations.
- **Station Errors**—total station drops and errors.
- **Ethernet Traffic**—Tx and Rx averages or peak total megabits per second for the AP gigabit Ethernet ports.
- **Ethernet Errors**—total drops and errors for the AP gigabit Ethernet ports.
- **Top Station Types by Throughput**—the types of stations generating the highest traffic demand (Tx+Rx Mbps).

Station Reports

These reports display statistics related to station counts and AP-to-Station associations.

- **Stations by Wi-Fi Band**—a count of stations by Wi-Fi Band.
- **Station Counts by SSID**—a pie chart and table of unique station counts by SSID.
- **Station Activity Over Time Period**—a list of stations that had active sessions, along with the total time that the station was connected and traffic usage statistics.
- **Station Sessions**—a list of active sessions along with station information for each.

- **Station Classification**—a list of stations by unique device class and type.
- **Station Manufacturers**—a list of stations by manufacturer.
- **Station Assurance**—a list of Station Assurance events, showing stations experiencing poor connectivity.
- **Associated Stations**—a list of stations associated to the wireless network.
- **Stations By AP**—AP-to-Station association counts.
- **Unique Station Count**—wireless station counts.

Access Point Reports

These reports display information about managed APs and their reliability statistics.

- **Access Point Inventory**—an inventory of APs.
- **Access Point Availability**—table of AP availability statistics.
- **Grouped Access Point Availability**—table of uptime percentage by profile or AP group.

RF Reports

This report displays information about channel usage.

- **Channel Usage**—radio counts on 2.4 GHz and 5 GHz channels.

Security Reports

This report displays information about intrusion attacks and detected rogue APs.

- **IDS Events**—list of intrusion attacks detected by the wireless network.
- **Rogue List**—list of rogue access points detected by the wireless network.

To create a report

Enter the following information to set up the report.

- **Name**

  This is a unique name that will identify this report on the **View Reports** page. You may create different reports of the same report type, with different options defined for each. Each report must have its own name.

WOS will not allow you to create a new report using a name that is already in the View Reports list.

- **Options**

  These settings define the selection criteria for the report. The types of criteria shown will differ by report type. They typically select criteria such as the APs and time period to be included in the report. For details on setting up these options for the report, please see **“Selection Criteria” on page 274**.

- **Schedule**

  You may schedule the report to be automatically run on a recurring schedule. Click **Enable Schedule** to display time settings. Select one of the following options:

  Hourly—Select the **minutes after the hour** when the report is to be run every hour. For example, to run the report on the hour, every hour, select **00**.

  Daily—Enter the **Time of Day** when the report is to be run every day, based on a 24-hour time notation. For example, midnight is 00:00, half past noon is 12:30 and 4 PM is 16:00.

  Weekly—Select the day of the week when the report is to be run, and then enter the **Time of Day** when the report is to be run, as described above.

  Monthly—Select the day of the month when the report is to run, and then enter the **Time of Day** for the run, as described above.

You should use the Time Span option when scheduling reports, because the Specific Date Range option will just generate the same report over and over again.

- **Email Report To**

  If you wish to have this report emailed to yourself or other recipients each time it runs, enter an email address and click the **Add** button. You may add multiple addresses. To remove an address from the email list, click the **X** in front of the entry. The email will display the report in the same format that is used to display it on the web client page (i.e., HTML format), and there will also be three attachments, one for each other format (PDF, .xls, .csv). Be aware that for large reports, the email size may be quite large.

You must specify the email server that WOS will use to send the email. Please see **"Email Settings" on page 588**.

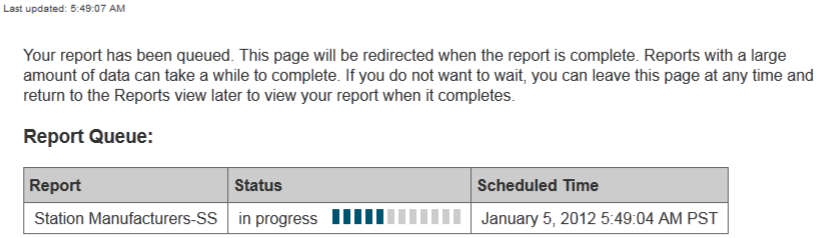
- Save Report / Save and Run

  When the settings for the report are complete, click **Save Report** to simply add it to the **View Reports** list without running it. Click **Save & Run** to add it to the **View Reports** list and run it immediately. The **Report Queue** page will be displayed, showing the status of the report. You may navigate to another page while the report is being generated. Use the **View Reports** page to view the report later on.

Report Queue

When you run a new or saved report, or when the time comes to run a scheduled report, it is added to the Report Queue. Reports are run one at a time, in the order in which they are added to the queue. The queue displays the status of each report that is waiting to be run—**Pending** or **In progress**.

The report queue page is displayed only when you run a new or saved report immediately, but not when you schedule a report. On the report queue page, you may wait for an in progress report to complete, at which time the report will automatically be displayed. Or you may navigate away from the report queue page to perform other tasks with the web client. In this case, you may view the report later after it completes by using its entry on the **View Reports** page.



Last updated: 5:49:07 AM

Your report has been queued. This page will be redirected when the report is complete. Reports with a large amount of data can take a while to complete. If you do not want to wait, you can leave this page at any time and return to the Reports view later to view your report when it completes.

Report Queue:

Report	Status	Scheduled Time
Station Manufacturers-SS	in progress	January 5, 2012 5:49:04 AM PST

Figure 186. Report Queue

Selection Criteria

The web client presents you with a set of options for filtering (restricting) the data that it includes in a report. Different selection criteria are appropriate for different report types, thus the settings that you may specify are tailored for each type of report. This section will describe how to use selection criteria. The detailed description of each report type later in this chapter will list the selection criteria that are available for that report.

Open the **Create Report Page** for the desired type of report as described in **"Create Report" on page 267**. Choose your selection criteria in the **Options** section. You may select no options, or one or more options. Remember that each type of report will use its own subset of these settings. In all cases, you may select only one entry from each drop-down list.

When you choose values for a number of different selection criteria, the report will use only data that satisfies of all of them—in other words, the report is based on the intersection of the conditions that you set. For example, if you select an **AP Group** and a particular radio, the report will show results for just the selected radio on all APs in that group. Take some care so that you don't choose criteria that will yield no results.

The following criteria are used in most report types.

- **AP Scope**—the drop-down list shows all of the profile networks and AP groups that you have defined in WOS. Select an entry to report on just the

APs that are members of the group or profile, or select **All APs**. For more information, see “AP Groups” on page 117 or “Profiles” on page 116.

- **Map**—the drop-down list shows all of the maps that you have defined in WOS. Each map may have multiple APs located on it, and an AP may only belong to one map. Select a map to report on just the APs that are assigned to the map, or select **All Maps**. For more information, see “Working with Maps” on page 213.
- **AP**—the drop-down list shows all of the APs being managed in WOS. Select an AP to report on just that one AP, or select **All APs**. You cannot make more than one choice from the drop-down list. If you have selected a Group, then this list will only contain APs that are members of the group.
- **Detail on**—this setting specifies how you would like to break out report results. It is used by the **Unique Station Count** report. Select **Total** to show the total station count only, or you may break out detailed counts by AP **Name, VLAN Name**, **VLAN Number**, **SSID**, **Media Type**, **Radio**, or **Association Type**. The drop-down list allows you to select one of these parameters for detailing. For example, if you select detail on **VLAN**, the chart and the table will each will show one line for each VLAN.
- **Display traffic by**—the drop-down list allows you to select **Tx+Rx** to display transmit, receive, and total traffic broken out separately into three lines, or select **Total** to display only the totals. **Total** will show two lines: the average value of Tx+Rx, and the peak value of Tx+Rx.
- **Order table by**—the drop-down list allows you to select the column to use for sorting results: AP **Name** (the default), **MAC Address, IP Address, Map,** or **Serial Number**.
- **Order direction**—select **Ascending** or **Descending** sort order from the drop-down list.
- **Table row limit**—select the total number of rows to display in the report from the drop-down list: **10**, **20**, **50**, or **Show all**.
- **Date/Time**—this defines the time interval covered by the report, specified in terms of **Time Span** or **Specific Date Range**. In either case,

the report will state the start time and end time of the period that it covers.

Select **Time Span** to specify a period ending at the report's run time. For example, if you select **Last Hour**, then the report will include data from the 60 minutes prior to the time when the report runs. You may select any entry in the drop-down list, for example **Last 24 Hours** or **Last 30 Days**. You should use the **Time Span** option when scheduling reports, because the **Specific Date Range** option will just generate the same report over and over again.

Select **Specific Date Range** to specify a start time and end time for the data to be included in the report. Click in the **Date From** field and then click the desired starting date using the drop-down calendar. Click in the **Time From** field and the **Choose Time** drop-down appears. Set the desired starting time by dragging the sliders for **Hour** and **Minute**. Set the **Date to** and **Time to** fields in the same way.

The remainder of the criteria are shown in alphabetical order.

- **Association**—select **Authenticated** from the drop-down list to show only stations that have been authenticated, or select **Any** to show all stations.
- **Classification**—the drop-down list allows you to select whether to report only on rogue radios whose classification matches your selection (select one of **Approved, Known, Unknown, Unclassified, Blocked,** or **Ad Hoc**) or select **All** to display rogues of any classification.
- **Device Class**—the drop-down list shows general classes of stations, for example **Notebook**, **Tablet**, **Phone**, etc. If you are using WDS (Wireless Distributed System) links to carry traffic between APs wirelessly, then the client device class is AP.

  Select a class to report on just that one class, or select **All Device Classes**. You cannot make more than one choice from the drop-down list.
- **Device Type**—the drop-down list shows more detailed types of stations. For example, if the Device Class is **Notebook**, then the Device Type might be Mac or Windows. If you are using WDS, then the client type is **WDS Link**.

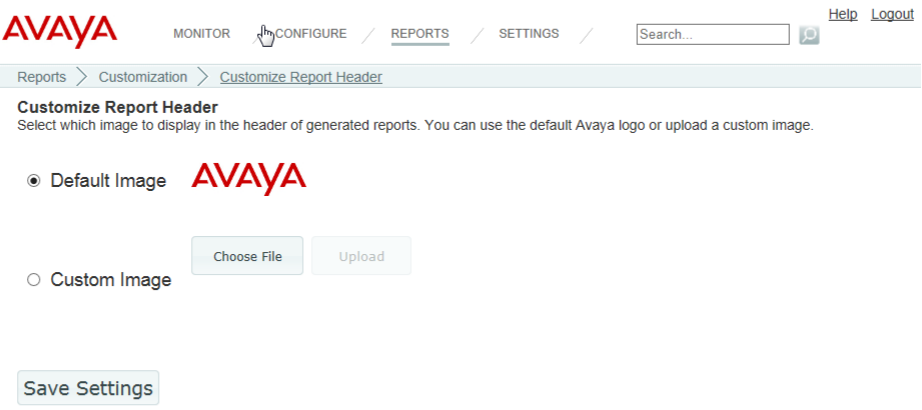
Select a type to report on just that one type, or select **All Device Types**. You cannot make more than one choice from the drop-down list.

- **IDS Event Type**—the drop-down list allows you to select whether to report only on intrusion detection events of the selected type (for example, **Beacon Flood** or **Authentication Flood**) or select **All IDS Event Types** to display all events.
- **Media Type**—the drop-down list shows the radio modes that are available on APs: **802.11b, 802.11n**, etc. Select a mode to report on just data for AP radios operating in that mode, or select **All Modes**.
- **Radio**—Select an individual radio if you wish to report on just data for that one radio, or select **All Radios**. For more information, see **"Radios" on page 80**.
- **SSID**—the drop-down list shows all of the SSIDs that you have defined in WOS. Select an SSID to report on just data for that one SSID, or select **All SSIDs**. For more information, see **"SSID" on page 82**.
- **Station Assurance Event Type**—the drop-down list allows you to select whether to report only on station assurance events of the selected type (for example, **Authentication Failures** or **Error Rate**) or select **All Station Assurance Event Types** to display all events.
- **VLAN**—the drop-down list shows all of the VLANs that you have defined in WOS. You may choose to display them by **VLAN Number** or by **VLAN Name**. Select a VLAN to report on just data for that one VLAN, or select **All VLANs**. For more information, see **"VLAN" on page 391**.

Customize Report Header

This page allows you to change the appearance of the report by modifying its header. Use this page to add your custom logo to the header.

To create a new report, click the **Reports** button at the top of the web client window, then click the **Customize Report Header** link. The **Customize Report Header** page appears. (Figure 187)n



Customize Report Header
Select which image to display in the header of generated reports. You can use the default Avaya logo or upload a custom image.

● Default Image

○ Custom Image

Figure 187. Customize Report Header Page

Select **Default Image** to use the default Avaya logo at the top of all reports. Select **Custom Image** to upload your own logo to be used at the top of all reports. Click **Choose File** to browse to the desired image file. It must be one of the following types: .bmp, .jpg, .png. Then click the **Upload** button. Click **Save Settings** when done. Note that WOS does not impose a particular size limit on the image file, but the Avaya logo is approximately 200 x 50 pixels, if you wish to use it as a guide.

The currently selected image will apply to all subsequent report runs (from either **Create Report** or **View Reports**). It will not affect any previously run reports—they will use the customization settings that were current at the time they were run.

Application Control Reports

Application Control reports analyze the amount of traffic generated on APs by the selected applications. Each AP uses Deep Packet Inspection (DPI) to determine what applications are being used, and how much bandwidth they are consuming. For more information, see **“Application Control—Overview” on page 104**.

The results returned for all reports in this section are dependent on the reporting period you specify. Application Control reports include:

- **Application Category Traffic**

  Shows Tx and Rx averages or peak total wireless traffic for a category of applications.
- **Application Traffic**

  Shows Tx and Rx averages or peak total wireless traffic for selected applications.
- **Station Application Category Traffic**

  Shows the ten stations with the highest wireless traffic for a category of applications.
- **Station Application Traffic**

  Shows the ten stations with the highest wireless traffic for selected applications.

Application Control data is only available from APs whose licenses include Application Control. See **“About Licensing and Upgrades” on page 182**.

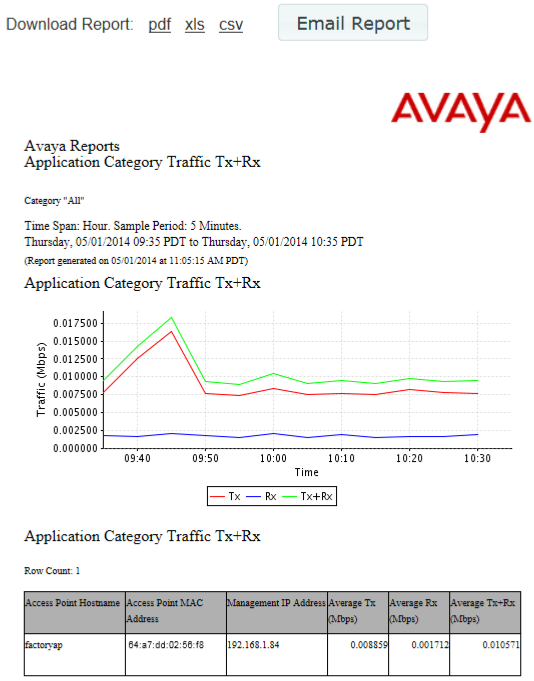
Application Category Traffic

This report provides statistical data for wireless traffic flow generated by a selected category of applications. (**Figure 188**) The graph at the top of the window displays wireless traffic for that category, summed over the selected APs for the selected time range.

A table shows traffic generated by this application category on each AP. The information displayed in this window and in the graph is dependent on the selection criteria you specify, summarized below. Note that the report includes only APs capable of generating application control data.

Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
Category	Include only traffic for the selected category of applications, such as File Transfer or Social Networking.
AP Scope	Include only APs that are members of the selected AP group or profile.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
VLAN	Include only the selected VLAN.
Display Traffic by	Break out transmit and receive traffic separately, or show only totals.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **"Schedule" on page 272**.
Email Report To	After running, email the report. See **"Email Report To" on page 272**.

If you have a large network, the results returned in this report may span many pages. The browser display of the report will truncate to three pages to give you a preview—to see the entire report open the PDF version.



Avaya Reports
Application Category Traffic Tx+Rx

Category "All"

Time Span: Hour. Sample Period: 5 Minutes.
Thursday, 05/01/2014 09:35 PDT to Thursday, 05/01/2014 10:35 PDT
(Report generated on 05/01/2014 at 11:05:15 AM PDT)

Application Category Traffic Tx+Rx

Application Category Traffic Tx+Rx

Row Count: 1

Access Point Hostname	Access Point MAC Address	Management IP Address	Average Tx (Mbps)	Average Rx (Mbps)	Average Tx+Rx (Mbps)
factoryap	64:a7:dd:02:56:f8	192.168.1.84	0.008859	0.001712	0.010571

Figure 188. Application Category Traffic Report

Table Details for the Application Category Traffic Report

The table portion of the report shows traffic statistics for each selected AP, organized by the following column headers:

- **AP Hostname**
  The host name assigned to the AP. Only APs that meet your selection criteria are included.
- **AP MAC Address**
  This is the AP's MAC address.

- **Management IP Address**
  This is the AP's IP address.

Throughput data shown in the table depends on your **Selection Criteria**. If you set **Display Traffic by** to **Tx+Rx**, these columns are shown:

- **Average Tx (Mbps)**
  Shows the average traffic transmitted (in megabits per second) by the application category for the time period you specified.
- **Average Rx (Mbps)**
  Shows the average traffic received (in megabits per second) by the application category for the time period you specified.
- **Average Tx+Rx (Mbps)**
  Shows the average total throughput (in megabits per second) achieved by the application category for the time period you specified.

If you set **Display Traffic by** to **Total**, these columns are shown:

- **Average Tx/Rx (Mbps)**
  Shows the average total throughput (in megabits per second) achieved by the application category for the time period you specified.
- **Peak Tx/Rx (Mbps)**
  Shows the maximum total throughput (in megabits per second) achieved by the application category for the time period you specified.

Application Traffic

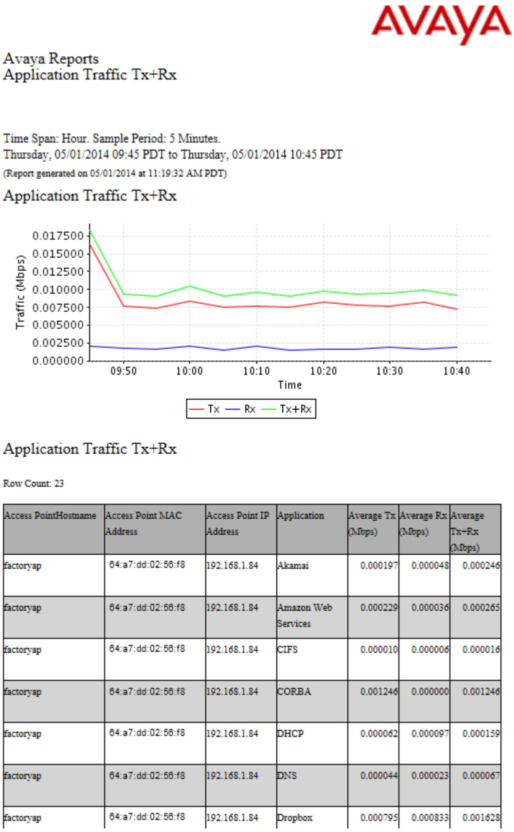
This report provides statistical data for wireless traffic flow generated by a selected set of applications. The graph at the top of the window displays wireless traffic for those applications, summed over the selected APs for the selected time range (**Figure 189**).

A table shows traffic generated by each application on each AP. The information displayed in this window and in the graph is dependent on the selection criteria you specify, summarized below. Note that the report includes only APs capable of generating application control data.

Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
Applications	Include only traffic for the selected applications, for example, Facebook and FTP. For each desired application, first select its **Category**, then select the **Application** and click **Add**. For example, for Facebook, first select the category **Social Networking** and then select **Facebook** from the application list. You may unselect an application with the **Delete** button. Click **Reset** to delete all applications from your selected list.
AP Scope	Include only APs that are members of the selected AP group or profile.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
VLAN	Include only the selected VLAN.
Display Traffic by	Break out transmit and receive traffic separately, or show only totals.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.

Selection Criterion	Description (see **“Selection Criteria” on page 274** for details)
Schedule	Run the report at this time. See **“Schedule” on page 272**.
Email Report To	After running, email the report. See **“Email Report To” on page 272**.

If you have a large network, the results returned in this report may span many pages. The browser display of the report will truncate to three pages to give you a preview—to see the entire report open the PDF version.



Avaya Reports
Application Traffic Tx+Rx

Time Span: Hour. Sample Period: 5 Minutes.
Thursday, 05/01/2014 09:45 PDT to Thursday, 05/01/2014 10:45 PDT
(Report generated on 05/01/2014 at 11:19:32 AM PDT)

Application Traffic Tx+Rx

Application Traffic Tx+Rx

Row Count: 23

Access PointHostname	Access Point MAC Address	Access Point IP Address	Application	Average Tx (Mbps)	Average Rx (Mbps)	Average Tx+Rx (Mbps)
factoryap	64:a7:dd:02:56:f8	192.168.1.84	Akamai	0.000197	0.000048	0.000246
factoryap	64:a7:dd:02:56:f8	192.168.1.84	Amazon Web Services	0.000229	0.000036	0.000265
factoryap	64:a7:dd:02:56:f8	192.168.1.84	CIFS	0.000010	0.000006	0.000016
factoryap	64:a7:dd:02:56:f8	192.168.1.84	CORBA	0.001246	0.000000	0.001246
factoryap	64:a7:dd:02:56:f8	192.168.1.84	DHCP	0.000062	0.000097	0.000159
factoryap	64:a7:dd:02:56:f8	192.168.1.84	DNS	0.000044	0.000023	0.000067
factoryap	64:a7:dd:02:56:f8	192.168.1.84	Dropbox	0.000795	0.000833	0.001628

Figure 189. Application Traffic Report

Table Details for the Application Traffic Report

The table portion of the report shows traffic averages or peak values for each selected application on each selected AP, organized by the following column headers:

- **AP Hostname**
  The host name assigned to the AP. Only APs that meet your selection criteria are included.
- **AP MAC Address**
  This is the AP's MAC address.
- **AP IP Address**
  This is the AP's IP address.
- **Application**
  This table row shows traffic for this selected application.

Throughput data shown in the table depends on your **Selection Criteria**. If you set **Display Traffic by** to **Tx+Rx**, these columns are shown:

- **Average Tx (Mbps)**
  Shows the average traffic transmitted (in megabits per second) by the application for the time period you specified.
- **Average Rx (Mbps)**
  Shows the average traffic received (in megabits per second) by the application for the time period you specified.
- **Average Tx+Rx (Mbps)**
  Shows the average total throughput (in megabits per second) achieved by the application for the time period you specified.

If you set **Display Traffic by** to **Total**, these columns are shown:

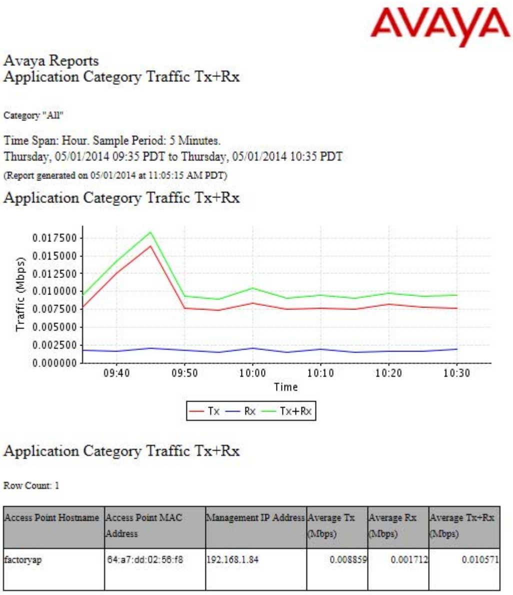
- **Average Tx/Rx (Mbps)**
  Shows the average total throughput (in megabits per second) achieved by the application for the time period you specified.
- **Peak Tx/Rx (Mbps)**
  Shows the maximum total throughput (in megabits per second) achieved by the application for the time period you specified.

Station Application Category Traffic

This report shows the ten stations with the highest level of wireless traffic for the selected category of applications. (Figure 190) The graph at the top of the window displays wireless traffic for that category for those stations over the specified time period. You may select the APs to consider. If no category is specified, then all categories are included.

A table shows average traffic generated by this application category on each station. The information displayed in this window and in the graph is dependent on the selection criteria you specify, summarized below.

Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
Category	Include only traffic for the selected category of applications, such as File Transfer or Social Networking, or select **All**.
AP Scope	Include only APs that are members of the selected AP group or profile.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
Display Traffic by	Break out transmit and receive traffic separately, or show only totals.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **"Schedule" on page 272**.
Email Report To	After running, email the report. See **"Email Report To" on page 272**.



Avaya Reports
Application Category Traffic Tx+Rx

Category "All"

Time Span: Hour. Sample Period: 5 Minutes.
Thursday, 05/01/2014 09:35 PDT to Thursday, 05/01/2014 10:35 PDT
(Report generated on 05/01/2014 at 11:05:15 AM PDT)

Application Category Traffic Tx+Rx

Application Category Traffic Tx+Rx

Row Count: 1

Access Point Hostname	Access Point MAC Address	Management IP Address	Average Tx (Mbps)	Average Rx (Mbps)	Average Tx+Rx (Mbps)
factoryap	64:a7:dd:02:56:f8	192.168.1.84	0.008859	0.001712	0.010571

Figure 190. Station Application Category Traffic Report (All Categories)

Table Details for the Station Application Category Traffic Report

The table portion of the report shows average traffic statistics for each of the top ten stations, organized by the following column headers:

- **Station MAC Address**
  This is the station's MAC address.
- **Station Hostname**
  The host name of the station. Only stations associated to APs that meet your selection criteria are included.
- **Station Device Type/Class**
  The type and class of station device, e.g., Notebook/Mac. For a WDS Link session, **WDS Link/AP** are shown here.
- **Manufacturer**
  The manufacturer of the station device, e.g., Apple, Motorola, etc.

Throughput data shown in the table depends on your **Selection Criteria**, and may be one of:

- **Average Tx (Mbps)**
  Shows the average traffic transmitted (in megabits per second) by the application category for the time period you specified.
- **Average Rx (Mbps)**
  Shows the average traffic received (in megabits per second) by the application category for the time period you specified.
- **Average Tx+Rx (Mbps)**
  Shows the average total throughput (in megabits per second) achieved by the application category for the time period you specified.

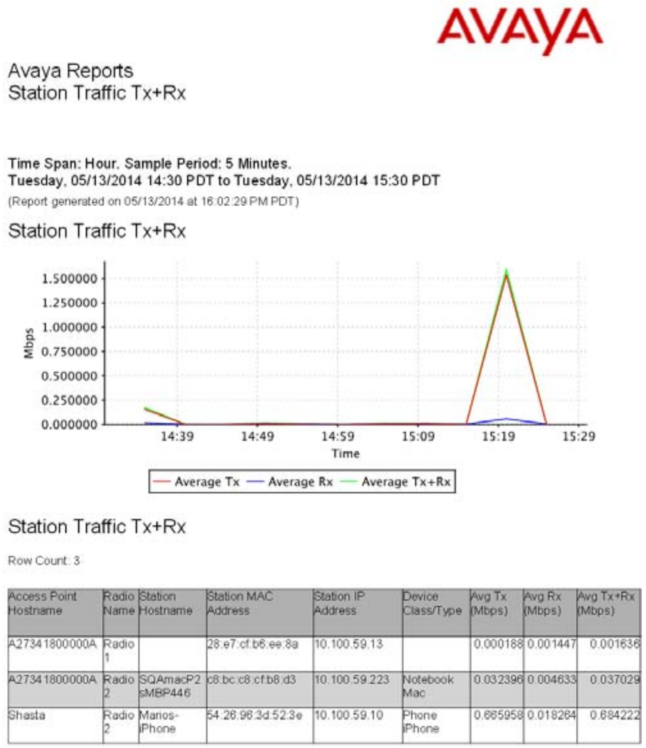
Station Application Traffic

This report shows the ten stations with the highest level of wireless traffic for the selected applications. (**Figure 191**) The graph at the top of the window displays wireless traffic for those applications for those stations over the specified time period. You may select the APs to consider. If no applications are specified, then all applications are included.

A table shows average traffic generated by each selected application on each of the ten stations, in decreasing order of the amount of traffic. The information displayed in this window and in the graph is dependent on the selection criteria you specify, summarized below.

Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
Applications	Include only traffic for the selected applications, for example, Facebook and FTP. For each desired application, first select its **Category**, then select the **Application** and click **Add**. For example, for Facebook, first select the category **Social Networking** and then select **Facebook** from the application list. If no applications are listed, then all applications will be included. You may unselect an application with the **Delete** button. Click **Reset** to delete all applications from your selected list.
AP Scope	Include only APs that are members of the selected AP group or profile.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
Display Traffic by	Break out transmit and receive traffic separately, or show only totals.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.

Selection Criterion	Description (see **“Selection Criteria” on page 274** for details)
Schedule	Run the report at this time. See **“Schedule” on page 272**.
Email Report To	After running, email the report. See **“Email Report To” on page 272**.



Avaya Reports
Station Traffic Tx+Rx

Time Span: Hour. Sample Period: 5 Minutes.
Tuesday, 05/13/2014 14:30 PDT to Tuesday, 05/13/2014 15:30 PDT
(Report generated on 05/13/2014 at 16:02:29 PM PDT)

Station Traffic Tx+Rx

Station Traffic Tx+Rx

Row Count: 3

Access Point Hostname	Radio Name	Station Hostname	Station MAC Address	Station IP Address	Device Class/Type	Avg Tx (Mbps)	Avg Rx (Mbps)	Avg Tx+Rx (Mbps)
A27341800000A	Radio 1		28:e7:cf:b6:ee:8a	10.100.59.13		0.000188	0.001447	0.001636
A27341800000A	Radio 2	SQAmacP2sMBP446	c8:bc:c8:cf:b8:d3	10.100.59.223	Notebook Mac	0.032396	0.004633	0.037029
Shasta	Radio 2	Marios-iPhone	54:26:96:3d:52:3e	10.100.59.10	Phone iPhone	0.665958	0.018264	0.684222

Figure 191. Station Application Traffic Report (All Applications)

Table Details for the Station Application Traffic Report

The table portion of the report shows traffic averages for each of the top ten stations for each of the selected applications that generated any traffic, organized by the following column headers:

- **Station MAC Address**
  This is the station's MAC address.
- **Station Hostname**
  The host name of the station. Only stations associated to APs that meet your selection criteria are included.
- **Station Device Type/Class**
  The type and class of station device, e.g., Notebook/Mac. For a WDS Link session, **WDS Link/AP** are shown here.
- **Manufacturer**
  The manufacturer of the station device, e.g., Apple, Motorola, etc.
- **Application**
  The name of the application generating this traffic.

Throughput data shown in the table depends on your **Selection Criteria**, and may be one of:

- **Average Tx (Mbps)**
  Shows the average traffic transmitted (in megabits per second) by the application for the time period you specified.
- **Average Rx (Mbps)**
  Shows the average traffic received (in megabits per second) by the application for the time period you specified.
- **Average Tx+Rx (Mbps)**
  Shows the average total throughput (in megabits per second) achieved by the application for the time period you specified.

Traffic Reports

Throughput is a measure of the amount of data that is transmitted in a given amount of time, expressed in bits per second (bps). Wireless APs are designed to handle Gigabit Ethernet speeds.

With their high-speed capability, your APs can easily handle time-sensitive traffic, such as voice and video.

Note that smaller APs that use the AOSLite system software, such as the WAP9112 and WAP9114, do not contribute data to all reports. In particular, they do not generate any radio (wireless) statistics.

The results returned for all reports in this section are dependent on the reporting period you specify. Throughput reports include:

- **Top APs by Wired Traffic**
  Shows the ten APs with the highest level of wired traffic.
- **Top APs by Wireless Traffic**

  Shows the ten APs with the highest level of wireless traffic (not including management traffic).
- **Wireless Traffic**

  Shows wireless throughput statistics for APs.
- **Wireless Errors**
  Shows wireless error statistics for APs.
- **Station Traffic**

  Tx and Rx average or peak megabits per second for traffic that flows to or from all associated stations.
- **Station Errors**
  Provides wireless error statistics for stations.
- **Ethernet Traffic**
  Shows Ethernet throughput statistics for APs.
- **Ethernet Errors**
  Shows Ethernet error statistics for APs.

- **Top Station Types by Throughput**
  Shows station types generating the highest traffic demand (Tx+Rx Mbps).

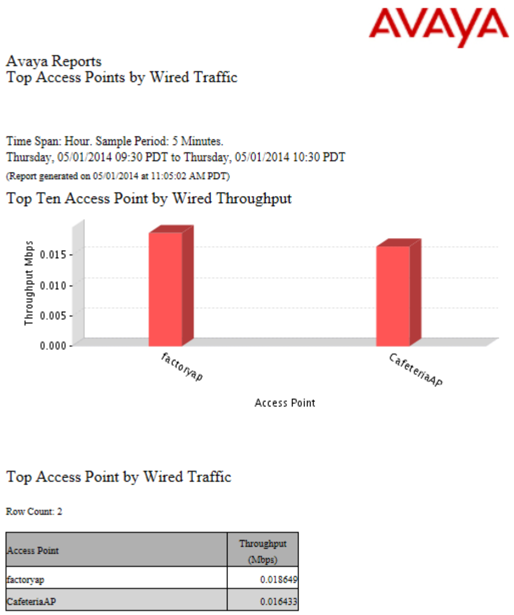
Top APs by Wired Traffic

This report displays the ten APs with the highest level of wired traffic, based on the traffic flow through the Gigabit ports on each wireless AP for the selected time period. (Figure 192) The bar chart at the top of the window identifies the APs (among the set you selected) with the highest throughput on the wired ports for the selected time range. If you selected less than ten APs, then all of them will be shown.

A table shows throughput on the wired ports for each AP managed by WOS (not just the selected APs). The information displayed in this window and in the graph is dependent on the selection criteria you specify, summarized below.

Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
AP Scope	Include only APs that are members of the selected AP group or profile.
Map	Include only APs that are members of the selected map.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **"Schedule" on page 272**.
Email Report To	After running, email the report. See **"Email Report To" on page 272**.

If you have a large network, the results returned in this report may span many pages. The browser display of the report will truncate to three pages to give you a preview—to see the entire report open the PDF version.



Avaya Reports
Top Access Points by Wired Traffic

Time Span: Hour. Sample Period: 5 Minutes.
Thursday, 05/01/2014 09:30 PDT to Thursday, 05/01/2014 10:30 PDT
(Report generated on 05/01/2014 at 11:05:02 AM PDT)

Top Ten Access Point by Wired Throughput

Top Access Point by Wired Traffic

Row Count: 2

Access Point	Throughput (Mbps)
factoryap	0.018649
CafeteriaAP	0.016433

Figure 192. Top APs by Wired Traffic Report

Table Details for the Top APs by Wired Traffic Report

The table portion of the report shows throughput for all managed APs (not just the selected APs), organized by the following column headers:

- **AP Hostname**
  The host name assigned to the AP. Only APs that meet your selection criteria are included.
- **Throughput (Mbps)**
  Shows the throughput (in megabits per second) achieved by the AP's wired ports for the time period you specified.

Top APs by Wireless Traffic

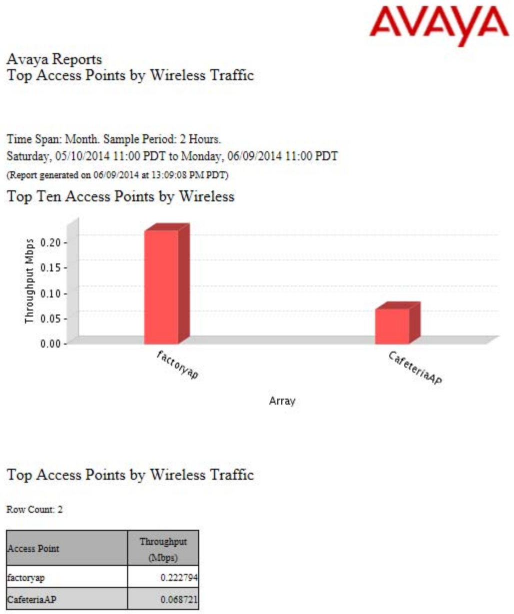
Note that smaller APs that use the AOSLite system software, such as the WAP9112 and WAP9114, do not contribute data to all reports. In particular, they do not generate any radio (wireless) statistics.

This report shows the ten APs with the highest level of wireless traffic for the selected APs and devices (not including management traffic). The bar chart at the top of the window identifies the APs (among the set you selected) with the highest wireless throughput for the selected time range. If you selected less than ten APs, then all of them will be shown (**Figure 193**).

A table shows wireless throughput for each AP. The information displayed in this window and in the graph is dependent on the selection criteria you specify, summarized below.

Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
AP Scope	Include only APs that are members of the selected AP group or profile.
Map	Include only APs that are members of the selected map.
Device Class	Include only this class of station device, e.g., Notebook, Phone, etc.
Device Type	Include only this type of station device, e.g., Windows, Mac, etc.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **"Schedule" on page 272**.
Email Report To	After running, email the report. See **"Email Report To" on page 272**.

If you have a large network, the results returned in this report may span many pages. The browser display of the report will truncate to three pages to give you a preview—to see the entire report open the PDF version.



Avaya Reports
Top Access Points by Wireless Traffic

Time Span: Month. Sample Period: 2 Hours.
Saturday, 05/10/2014 11:00 PDT to Monday, 06/09/2014 11:00 PDT
(Report generated on 06/09/2014 at 13:09:08 PM PDT)

Top Ten Access Points by Wireless

Top Access Points by Wireless Traffic

Row Count: 2

Access Point	Throughput (Mbps)
factoryap	0.222794
CafeteriaAP	0.068721

Figure 193. Top APs by Wireless Traffic Report

Table Details for the Top APs by Wireless Traffic Report

The table portion of the report shows throughput for the selected APs, organized by the following column headers:

- **AP Hostname**
  The host name assigned to the AP. Only APs that meet your selection criteria are included.

- **Throughput (Mbps)**
  Shows the wireless throughput (in megabits per second) achieved by the AP for the devices and time period you specified.

Wireless Traffic

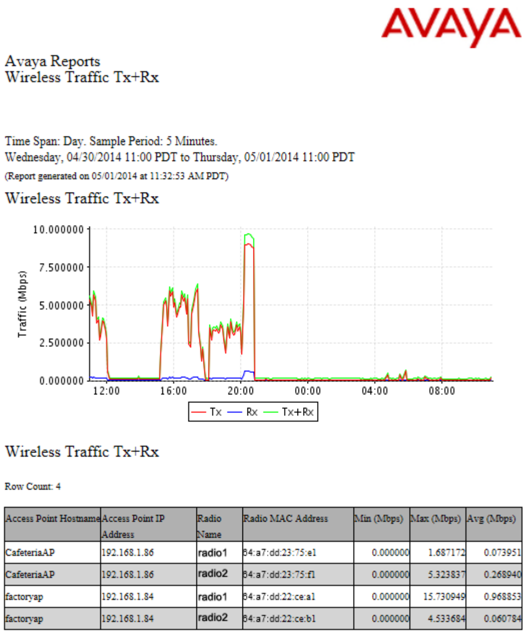
Note that smaller APs that use the AOSLite system software, such as the WAP9112 and WAP9114, do not contribute data to all reports. In particular, they do not generate any radio (wireless) statistics.

This report provides statistical data for wireless throughput, based on the traffic flow achieved by each wireless AP. (**Figure 194**) The graph at the top of the window displays wireless data summed over the selected APs for the selected time range.

A table shows throughput for each AP, broken out by individual radios. The information displayed in this window and in the graph is dependent on the selection criteria you specify, summarized below.

Selection Criterion	Description (see **“Selection Criteria” on page 274** for details)
AP Scope	Include only APs that are members of the selected AP group or profile.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
Radio	Include only the selected radio.
Display Traffic by	Break out transmit and receive traffic separately, or show only totals.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **“Schedule” on page 272**.
Email Report To	After running, email the report. See **“Email Report To” on page 272**.

If you have a large network, the results returned in this report may span many pages. The browser display of the report will truncate to three pages to give you a preview—to see the entire report open the PDF version.



Avaya Reports
Wireless Traffic Tx+Rx

Time Span: Day. Sample Period: 5 Minutes.
Wednesday, 04/30/2014 11:00 PDT to Thursday, 05/01/2014 11:00 PDT
(Report generated on 05/01/2014 at 11:32:53 AM PDT)

Wireless Traffic Tx+Rx

Wireless Traffic Tx+Rx

Row Count: 4

Access Point Hostname	Access Point IP Address	Radio Name	Radio MAC Address	Min (Mbps)	Max (Mbps)	Avg (Mbps)
CafeteriaAP	192.168.1.86	radio1	84:a7:dd:23:75:e1	0.000000	1.687172	0.073951
CafeteriaAP	192.168.1.86	radio2	84:a7:dd:23:75:f1	0.000000	5.323837	0.268940
factoryap	192.168.1.84	radio1	84:a7:dd:22:ce:a1	0.000000	15.730949	0.968853
factoryap	192.168.1.84	radio2	84:a7:dd:22:ce:b1	0.000000	4.533684	0.060784

Figure 194. Wireless Traffic Report

Table Details for the Wireless Traffic Report

The table portion of the report shows traffic statistics for each radio1 on the selected APs, organized by the following column headers:

- **AP Hostname**
  The host name assigned to the AP. Only APs that meet your selection criteria are included.
- **AP IP Address**
  This is the AP's IP address.
- **Radio Name**
  Each radio in each AP is listed.

- **Radio MAC Address**
  This is the radio's MAC address.

Throughput data shown in the table depends on your **Selection Criteria**. If you set **Display Traffic by** to **Tx+Rx**, these columns are shown:

- **Min. (Mbps)**
  Shows the minimum throughput (in megabits per second) achieved by the radio for the time period you specified.
- **Max. (Mbps)**
  Shows the maximum throughput (in megabits per second) achieved by the radio for the time period you specified.
- **Avg. (Mbps)**
  Shows the average throughput (in megabits per second) achieved by the radio for the time period you specified.

If you set **Display Traffic by** to **Total**, these columns are shown:

- **Average Tx/Rx (Mbps)**
  Shows the average total throughput (in megabits per second) achieved by the radio for the time period you specified.
- **Peak Tx/Rx (Mbps)**
  Shows the maximum total throughput (in megabits per second) achieved by the radio for the time period you specified.

Wireless Errors

Note that smaller APs that use the AOSLite system software, such as the WAP9112 and WAP9114, do not contribute data to all reports. In particular, they do not generate any radio (wireless) statistics.

This report shows wireless communication error statistics for AP radios in the WOS managed network, based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
AP Scope	Include only APs that are members of the selected AP group or profile.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
Radio	Include only errors for the selected radio.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **"Schedule" on page 272**.
Email Report To	After running, email the report. See **"Email Report To" on page 272**.

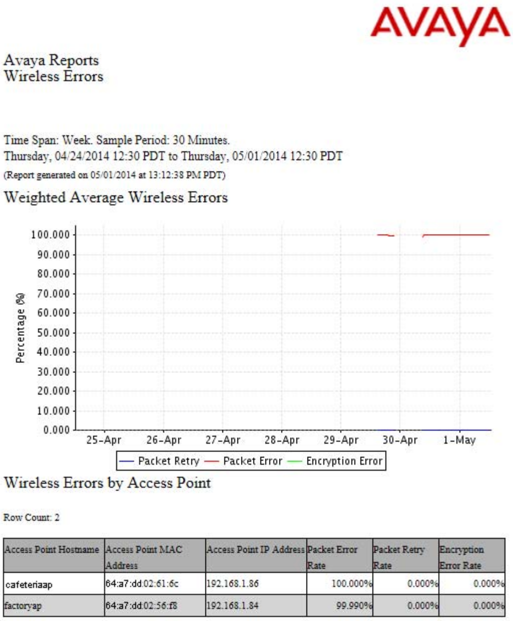
AP errors reported are packet error rate, packet retry rate, and encryption retry rate, shown as a percentage of the total number of packets. (**Figure 195**) The graph shows the weighted average wireless error percentages for all APs, using this formula:

Errors / (Retries + Errors + Encryption Errors)

Table Details for the Wireless Errors Report

The results shown in this report are organized by the following column headers, which can be sorted to best suit your viewing needs:

- **AP Hostname**
  The host name assigned to the AP.
- **AP MAC Address**
  This is the AP's MAC address.
- **AP IP Address**
  The IP address assigned to the AP.
- **Packet Error Rate**
  The packet error rate shown in this window reflects the bit errors detected by the system during the time period that you specified. The percentage shown is the number of bit errored packets divided by the total number of packets.



Avaya Reports
Wireless Errors

Time Span: Week. Sample Period: 30 Minutes.
Thursday, 04/24/2014 12:30 PDT to Thursday, 05/01/2014 12:30 PDT
(Report generated on 05/01/2014 at 13:12:38 PM PDT)

Weighted Average Wireless Errors

Wireless Errors by Access Point

Row Count: 2

Access Point Hostname	Access Point MAC Address	Access Point IP Address	Packet Error Rate	Packet Retry Rate	Encryption Error Rate
cafeteriaap	64:a7:dd:02:61:6c	192.168.1.86	100.000%	0.000%	0.000%
factoryap	64:a7:dd:02:56:f8	192.168.1.84	99.990%	0.000%	0.000%

Figure 195. Wireless Errors Report

- **Packet Retry Rate**
  Shows how many attempts were made to re-send dropped packets during the time period you specified. The percentage shown is the number of packet retries divided by the total number of packets.
- **Encryption Error Rate**
  Shows how many attempts were made to reconcile security issues. The percentage shown is the number of received encryption errors divided by the total number of received packets.

Station Traffic

Note that smaller APs that use the AOSLite system software, such as the WAP9112 and WAP9114, do not contribute data to all reports. In particular, they do not generate any radio (wireless) statistics.

This report provides statistical data for throughput for the selected time period, based on the traffic flow achieved by each client station associated to the selected APs. Throughput summed over all stations is represented in a graph at the top of the window (**Figure 196**). Throughput broken out by station is detailed in a table underneath.

The information displayed in this window is dependent on your **Selection Criteria**. There are two types of throughput data displayed, based on your choice for **Display Traffic by**:

- If you select **Tx+Rx**, both graph and table display average transmit, receive, and total traffic broken out separately into three lines. Transmit throughput is shown in red (**Tx**), receive throughput is shown in blue (**Rx**), and total throughput is shown in green (**Tx+Rx**).
- Select **Total** to display two lines: the average value of Tx+Rx in green, and the peak value of Tx+Rx in magenta.

Selection Criterion	Description (see **“Selection Criteria” on page 274** for details)
AP Scope	Include only APs that are members of the selected AP group or profile.
Map	Include only member APs of the selected map.
AP	Include only the selected AP.
SSID	Include only the selected SSID.
Radio	Include only the selected radio.
Device Class	Include only this class of station device, e.g., Notebook, Phone, etc.

Selection Criterion	Description (see **“Selection Criteria” on page 274** for details)
Device Type	Include only this type of station device, e.g., Windows, Mac, etc.
Display Traffic by	Break out transmit and receive traffic separately, or show only totals.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **“Schedule” on page 272**.
Email Report To	After running, email the report. See **“Email Report To” on page 272**.

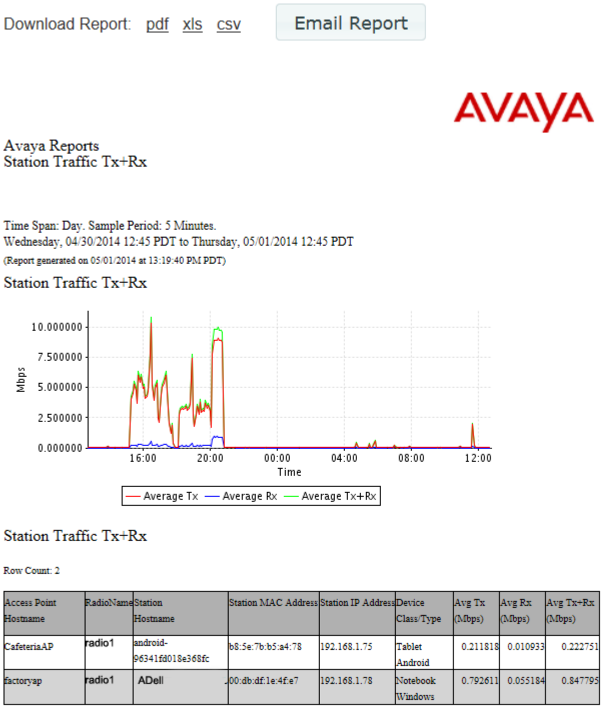
If you have a large network the results returned in this report may span many pages. The browser display of the report will truncate to three pages to give you a preview—to see the entire report open the PDF version.

Table Details for the Station Traffic Report

The results shown in this report are organized by the following column headers:

- **AP Hostname**
  The host name of the AP to which the station is associated.
- **Radio Name**
  The radio to which the station is associated.
- **Station Hostname**
  This column shows the host name for each client station listed in the report. The Station Hostname is specified for a device (in this case, a client station) when its networking is installed and configured. In order to connect to a computer running the TCP/IP protocol via its hostname (or Windows NetBIOS name), the name must be resolved to an IP address.
- **Station MAC Address**
  This is the station’s MAC address.

- **Station IP Address**
  This is the station's IP address.
- **Device Class/Type**
  The class and type of station device, e.g., Notebook/Mac. For a WDS Link session, AP/**WDS Link** are shown here.



Avaya Reports
Station Traffic Tx+Rx

Time Span: Day. Sample Period: 5 Minutes.
Wednesday, 04/30/2014 12:45 PDT to Thursday, 05/01/2014 12:45 PDT
(Report generated on 05/01/2014 at 13:19:40 PM PDT)

Station Traffic Tx+Rx

Station Traffic Tx+Rx

Row Count: 2

Access Point Hostname	RadioName	Station Hostname	Station MAC Address	Station IP Address	Device Class/Type	Avg Tx (Mbps)	Avg Rx (Mbps)	Avg Tx+Rx (Mbps)
CafeteriaAP	radio1	android-96341fd018e368fc	b8:5e:7b:b5:a4:78	192.168.1.75	Tablet Android	0.211818	0.010933	0.222751
factoryap	radio1	ADell	00:db:df:1e:4f:e7	192.168.1.78	Notebook Windows	0.792611	0.055184	0.847795

Figure 196. Station Traffic Report (Tx+Rx)

Throughput data shown in the table depends on your **Selection Criteria**. If you set **Display Traffic by** to **Tx+Rx**, these columns are shown:

- **Average Tx (Mbps)**
  Shows the average transmit throughput (in megabits per second) achieved by the station for the time period you specified.

- **Average Rx (Mbps)**
  Shows the average receive throughput (in megabits per second) achieved by the station for the time period you specified.
- **Average Tx+Rx (Mbps)**
  Shows the average total throughput (in megabits per second) achieved by the station for the time period you specified.

If you set **Display Traffic by** to **Total**, these columns are shown:

- **Average Tx/Rx (Mbps)**
  Shows the average total throughput (in megabits per second) achieved by the station for the time period you specified.
- **Peak Tx/Rx (Mbps)**
  Shows the maximum total throughput (in megabits per second) achieved by the station for the time period you specified.

Station Errors

Note that smaller APs that use the AOSLite system software, such as the WAP9112 and WAP9114, do not contribute data to all reports. In particular, they do not generate any radio (wireless) statistics.

This report lists all stations with errors that were detected by WOS, based on your **Selection Criteria**.

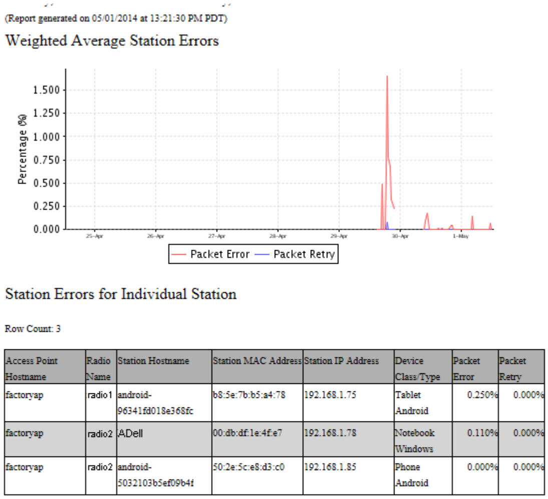
Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
AP Scope	Include only APs that are members of the selected AP group or profile.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
Radio	Include only the selected radio.
Device Class	Include only this class of station device, e.g., Notebook, Phone, etc.
Device Type	Include only this type of station device, e.g., Windows, Mac, etc.
SSID	Include only the selected SSID.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **"Schedule" on page 272**.
Email Report To	After running, email the report. See **"Email Report To" on page 272**.

Station errors reported in this window include weighted averages for the packet error rate and packet retry rate, where both categories are based on a percentage of the total number of these events detected by the system. **Figure 197** shows an example of the error report for stations. The graph shows the packet error and packet dropped error percentages for all APs.

Table Details for the Station Errors Report

The results shown in this report are organized by the following column headers:

- **AP Hostname**
  The host name of the AP that the station is associated with.
- **Radio Name**
  The radio that the station is associated with.
- **Station Hostname**
  This column shows the host name of each client station in the report.
- **Station MAC Address**
  This is the station's MAC address.



(Report generated on 05/01/2014 at 13:21:30 PM PDT)

Weighted Average Station Errors

Station Errors for Individual Station

Row Count: 3

Access Point Hostname	Radio Name	Station Hostname	Station MAC Address	Station IP Address	Device Class/Type	Packet Error	Packet Retry
factoryap	radio1	android-96341fd018e368fc	b8:5e:7b:b5:a4:78	192.168.1.75	Tablet Android	0.250%	0.000%
factoryap	radio2	ADell	00:db:df:1e:4f:e7	192.168.1.78	Notebook Windows	0.110%	0.000%
factoryap	radio2	android-5032103b5ef09b4f	50:2e:5c:e8:d3:c0	192.168.1.85	Phone Android	0.000%	0.000%

Figure 197. Station Errors Report

- **Station IP Address**
  The IP address assigned to the station.
- **Device Class/Type**
  The class and type of station device, e.g., Notebook/Mac. For a WDS Link session, AP/**WDS Link** are shown here.
- **Packet Error Rate%**
  The packet error rate shown in this window reflects the bit errors detected by the system during the time period you specified. The percentage shown is the number of packet errors divided by the total number of packets.

- **Packet Retry Rate%**
  Shows how many attempts were made to re-send failed packets during the time period you specified. The percentage shown is the number of packet retries divided by the total number of packets.

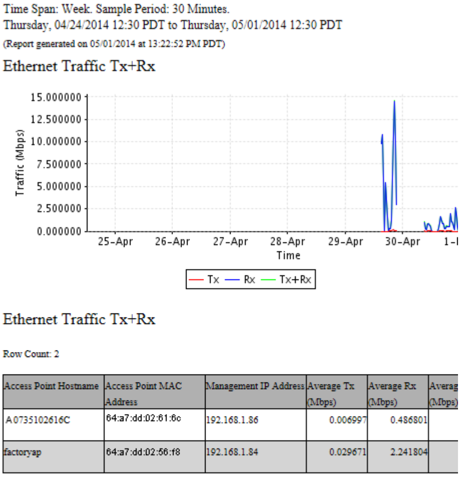
Ethernet Traffic

This report provides statistical data for Ethernet throughput, based on the speeds achieved by the Gigabit1 Ethernet port on wireless APs. (**Figure 198**) The graph at the top of the window displays aggregate data throughput across all APs for the selected time range.

A table shows average and peak Ethernet rates for each AP. The information displayed in this window and in the graph is dependent on the selection criteria you specify, summarized below.

Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
AP Scope	Include only APs that are members of the selected AP group or profile.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
VLAN	Include only the selected VLAN (specified by name or number)
Display Traffic by	Break out transmit and receive traffic separately, or show only totals.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **"Schedule" on page 272**.
Email Report To	After running, email the report. See **"Email Report To" on page 272**.

If you have a large network, the results returned in this report may span many pages. The browser display of the report will truncate to three pages to give you a preview—to see the entire report open the PDF version.



Time Span: Week. Sample Period: 30 Minutes.
Thursday, 04/24/2014 12:30 PDT to Thursday, 05/01/2014 12:30 PDT
(Report generated on 05/01/2014 at 13:22:52 PM PDT)

Ethernet Traffic Tx+Rx

Ethernet Traffic Tx+Rx

Row Count: 2

Access Point Hostname	Access Point MAC Address	Management IP Address	Average Tx (Mbps)	Average Rx (Mbps)	Averag (Mbps)
A0735102616C	64:a7:dd:02:61:6c	192.168.1.86	0.006997	0.486801	
factoryap	64:a7:dd:02:56:f8	192.168.1.84	0.029671	2.241804	

Figure 198. Ethernet Traffic Report

Table Details for the Ethernet Traffic Report

The table portion of the report shows traffic statistics for the Gigabit1 port on selected APs, organized by the following column headers:

- **AP Hostname**
  The host name assigned to the AP. Only APs that meet your selection criteria are included.
- **AP MAC Address**
  This is the AP’s MAC address.
- **Management IP Address**
  This is the AP’s management IP address.

Throughput data shown in the table depends on your **Selection Criteria**. If you set **Display Traffic by** to **Tx+Rx**, these columns are shown:

- **Average Tx (Mbps)**
  Shows the average transmit throughput (in megabits per second) achieved by the AP for the time period you specified.
- **Average Rx (Mbps)**
  Shows the average receive throughput (in megabits per second) achieved by the AP for the time period you specified.
- **Average Tx+Rx (Mbps)**
  Shows the average total throughput (in megabits per second) achieved by the AP for the time period you specified.

If you set **Display Traffic by** to **Total**, these columns are shown:

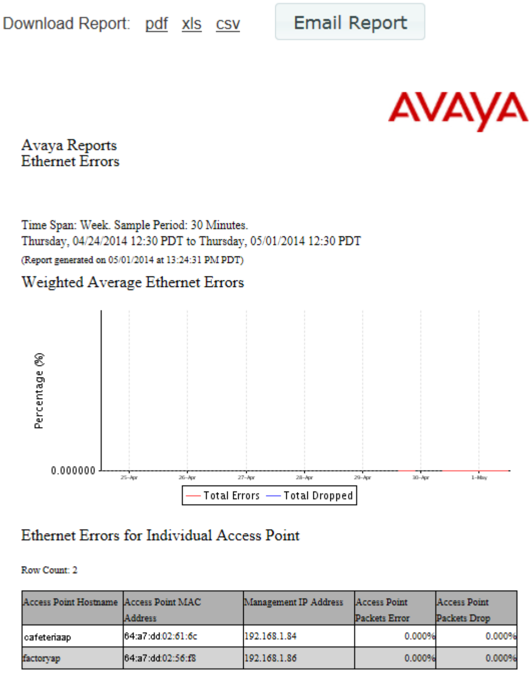
- **Average Tx/Rx (Mbps)**
  Shows the average total throughput (in megabits per second) achieved by the AP for the time period you specified.
- **Peak Tx/Rx (Mbps)**
  Shows the maximum total throughput (in megabits per second) achieved by the AP for the time period you specified.

Ethernet Errors

This report shows Ethernet communication errors for the Gigabit ports for APs in the WOS managed network, based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
AP Scope	Include only APs that are members of the selected AP group or profile.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
VLAN	Include only the selected VLAN (specified by name or number)
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **"Schedule" on page 272**.
Email Report To	After running, email the report. See **"Email Report To" on page 272**.

Ethernet errors reported include packet error rate and packet retry rate, where both categories are based on a percentage of the total number of packets. **(Figure 199)**



Avaya Reports
Ethernet Errors

Time Span: Week. Sample Period: 30 Minutes.
Thursday, 04/24/2014 12:30 PDT to Thursday, 05/01/2014 12:30 PDT
(Report generated on 05/01/2014 at 13:24:31 PM PDT)

Weighted Average Ethernet Errors

Ethernet Errors for Individual Access Point

Row Count: 2

Access Point Hostname	Access Point MAC Address	Management IP Address	Access Point Packets Error	Access Point Packets Drop
cafeteriaap	64:a7:dd:02:61:6c	192.168.1.84	0.000%	0.000%
factoryap	64:a7:dd:02:56:f8	192.168.1.86	0.000%	0.000%

Figure 199. Ethernet Errors Report

Table Details for the Ethernet Errors Report

The results shown in this report are organized by the following column headers:

- **AP Hostname**
  The host name assigned to the AP.
- **AP MAC Address**
  This is the AP’s MAC address.
- **Management IP Address**
  The IP address assigned to the AP.

- **AP Packets Error Rate**
  The packet error rate reflects the bit errors detected by the system during the time period you specified. The percentage shown is the number of bit errors divided by the total number of packets.
- **AP Packets Drop Rate**
  Shows how many packets failed due to being dropped during the time period you specified. The percentage shown is the number of packets dropped divided by the total number of packets.

Top Station Types by Throughput

Note that smaller APs that use the AOSLite system software, such as the WAP9112 and WAP9114, do not contribute data to all reports. In particular, they do not generate any radio (wireless) statistics.

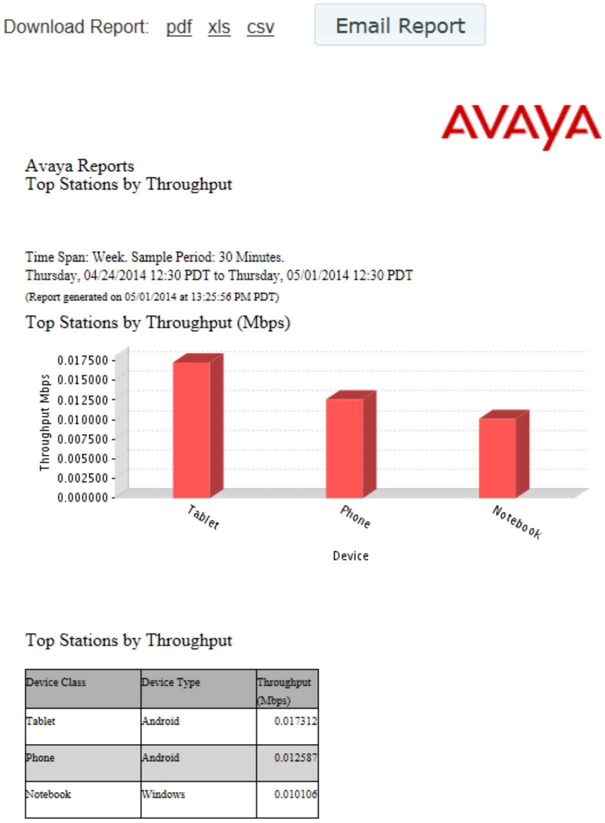
This report shows the types of stations generating the highest traffic demand (both transmitted and received). The bar chart summarizes throughput of connected stations by their **Device Class** and **Type**. It includes all stations matching the selected device classes and types that were associated to the selected APs at any time during the specified time period.

Note that if you are using Wireless Distributed System (WDS) links to carry traffic between APs wirelessly, client link stations will be included. These stations can be recognized by their **Device Class** and **Type**—AP and **WDS Link**.

The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
AP Scope	Include only member APs of the selected AP group.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
Device Class	Include only this class of station device, e.g., Notebook, Phone, etc.
Device Type	Include only this type of station device, e.g., Windows, Mac, etc.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **"Schedule" on page 272**.
Email Report To	After running, email the report. See **"Email Report To" on page 272**.

Use the bar chart for an at-a-glance overview of the station devices generating the most traffic in your wireless network.



Avaya Reports
Top Stations by Throughput

Time Span: Week. Sample Period: 30 Minutes.
Thursday, 04/24/2014 12:30 PDT to Thursday, 05/01/2014 12:30 PDT
(Report generated on 05/01/2014 at 13:25:56 PM PDT)

Top Stations by Throughput (Mbps)

Top Stations by Throughput

Device Class	Device Type	Throughput (Mbps)
Tablet	Android	0.017312
Phone	Android	0.012587
Notebook	Windows	0.010106

Figure 200. Top Station Types by Throughput Report

Table Details for the Station Types by Throughput Report

The table below the graph shows the overall throughput for each combination of device type and class for the stations included in the selection criteria.

- **Device Class**
  The class of station device, e.g., Notebook, Tablet, Phone, etc. For a WDS Link session, AP is shown here.

- **Device Type**
  The type of station device, e.g., Blackberry, Android, Windows, Mac, etc. For a WDS Link session, **WDS Link** is shown here.
- **Through put**
  The combined throughput of stations with this combination of device class and type.

Station Reports

A basic wireless network consists of an Access Point (AP) and client stations that are associated to the network via the AP. Each wireless AP includes a number of radios, with each radio capable of associating up to 96 client stations.

The following reports are available in this section:

- **Stations by Wi-Fi Band**
  Displays a count of stations by Wi-Fi Band.
- **Station Counts by SSID**

  Displays a pie chart and table of unique station counts by SSID.
- **Station Activity Over Time Period**

  Displays a table of stations with the total time that the stations were connected and traffic usage statistics.
- **Station Sessions**

  Displays information about current sessions and their duration.
- **Station Classification**

  Displays stations by unique device class and type.
- **Station Assurance**

  Displays Station Assurance events, showing stations that are having problems with connection quality.
- **Associated Stations**

  Provides station association data for the selected APs.
- **Stations By AP**
  Allows you to review station association data based on selected APs, including how many stations were associated at the busiest (peak) time.
- **Unique Station Count**
  This report displays a line graph showing station counts over time, broken out into categories by your choice of categories such as SSID and VLAN.

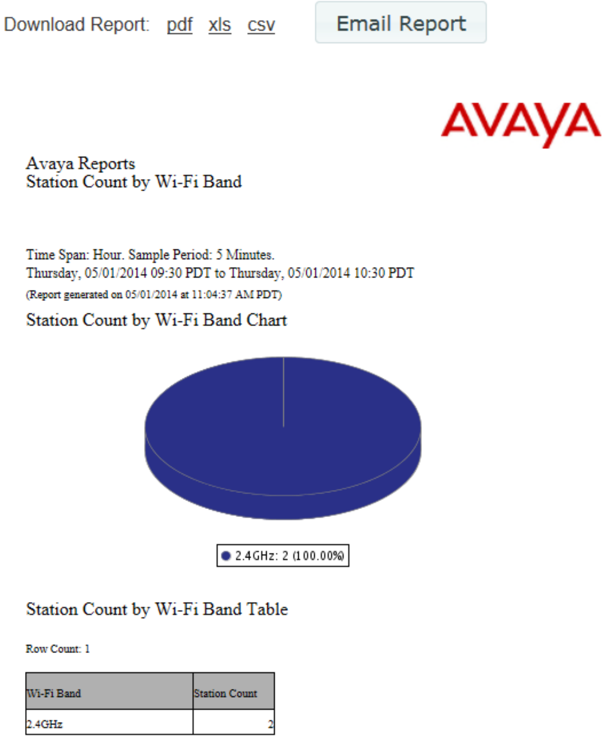
Stations by Wi-Fi Band

This report summarizes connected stations by their wireless band—2.4GHz or 5 GHz. It includes all stations of the selected **Device Class** and **Type** that were associated to the selected APs at any time during the specified time period. A pie chart shows the distribution of stations by band. (**Figure 201**)

The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
AP Scope	Include only member APs of the selected AP group.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
Device Class	Include only this class of station device, e.g., Notebook, Phone, etc.
Device Type	Include only this type of station device, e.g., Windows, Mac, etc.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **"Schedule" on page 272**.
Email Report To	After running, email the report. See **"Email Report To" on page 272**.

Use the pie chart for an at-a-glance overview of the proportion of stations connected at 2.4GHz or 5GHz in your wireless network.



Avaya Reports
Station Count by Wi-Fi Band

Time Span: Hour. Sample Period: 5 Minutes.
Thursday, 05/01/2014 09:30 PDT to Thursday, 05/01/2014 10:30 PDT
(Report generated on 05/01/2014 at 11:04:37 AM PDT)

Station Count by Wi-Fi Band Chart

Station Count by Wi-Fi Band Table

Row Count: 1

Wi-Fi Band	Station Count
2.4GHz	2

Figure 201. Stations by Wi-Fi Band Report

Table Details for the Stations by Wi-Fi Band Report

The table below the graph shows the station count for each Wi-Fi band for the stations included in the selection criteria.

- **Wi-Fi Band**
  The wireless band used by the stations—2.4GHz or 5 GHz.
- **Station Count**
  The number of stations using this band.

Station Counts by SSID

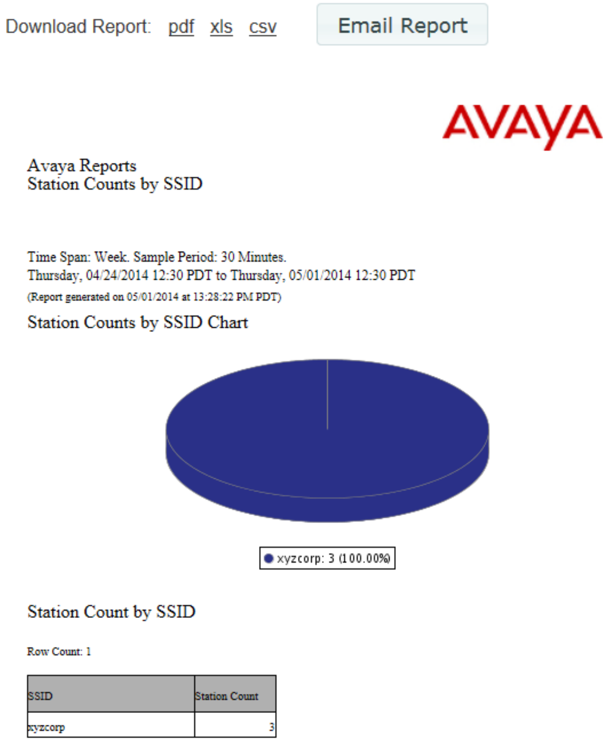
This report summarizes stations by the SSID to which they are connected. It includes all stations of the chosen **Device Class** and **Type** that were associated to the selected APs at any time during the specified time period. A pie chart shows the distribution of SSID usage. (**Figure 202**)

If you are using WDS links to carry traffic between APs wirelessly, client link stations will be included. The **Device Class** and **Type** of these stations are AP and **WDS Link**, respectively.

The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
AP Scope	Include only member APs of the selected AP group.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
Device Class	Include only this class of station device, e.g., Notebook, Phone, etc.
Device Type	Include only this type of station device, e.g., Windows, Mac, etc.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **"Schedule" on page 272**.
Email Report To	After running, email the report. See **"Email Report To" on page 272**.

Use the pie chart for an at-a-glance overview of the proportion of stations using each SSID.



Avaya Reports
Station Counts by SSID

Time Span: Week. Sample Period: 30 Minutes.
Thursday, 04/24/2014 12:30 PDT to Thursday, 05/01/2014 12:30 PDT
(Report generated on 05/01/2014 at 13:28:22 PM PDT)

Station Counts by SSID Chart

Station Count by SSID

Row Count: 1

SSID	Station Count
xyzcorp	3

Figure 202. Station Counts by SSID Report

Table Details for the Stations by SSID Report

The table below the graph shows the station count for each SSID, for the stations included in the selection criteria.

- **SSID**
  The SSIDs available on the selected APs are listed.
- **Station Count**
  The number of stations connected using this SSID.

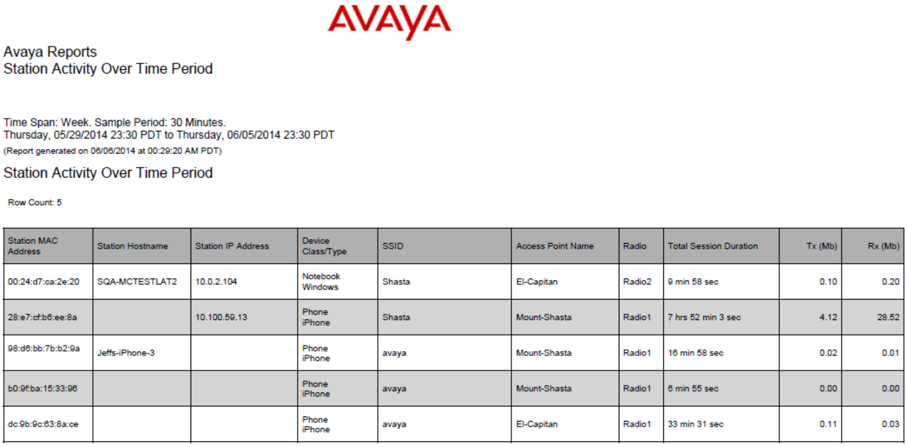
Station Activity Over Time Period

This report lists stations that had active sessions during the specified time period, along with the time that the session was active and traffic usage statistics.

Note that if you are using WDS links to carry traffic between APs wirelessly, client link sessions will be displayed. These sessions can be recognized by their **Device Class** and **Type—AP** and **WDS Link**.

The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **“Selection Criteria” on page 274** for details)
AP Scope	Include only member APs of the selected AP group.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
SSID	Include only the selected SSID.
Device Class	Include only this class of station device, e.g., Notebook, Phone, etc.
Device Type	Include only this type of station device, e.g., Windows, Mac, etc.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **“Schedule” on page 272**.
Email Report To	After running, email the report. See **“Email Report To” on page 272**.



Avaya Reports
Station Activity Over Time Period

Time Span: Week. Sample Period: 30 Minutes.
Thursday, 05/29/2014 23:30 PDT to Thursday, 06/05/2014 23:30 PDT
(Report generated on 06/06/2014 at 00:29:20 AM PDT)

Station Activity Over Time Period

Row Count: 5

Station MAC Address	Station Hostname	Station IP Address	Device Class/Type	SSID	Access Point Name	Radio	Total Session Duration	Tx (Mb)	Rx (Mb)
00:24:d7:ca:2e:20	SQA-MCTESTLAT2	10.0.2.104	Notebook Windows	Shasta	El-Capitan	Radio2	9 min 58 sec	0.10	0.20
28:e7:cf:b6:ee:8a		10.100.59.13	Phone iPhone	Shasta	Mount-Shasta	Radio1	7 hrs 52 min 3 sec	4.12	28.52
98:d6:bb:7b:b2:9a	Jeffs-iPhone-3		Phone iPhone	avaya	Mount-Shasta	Radio1	16 min 58 sec	0.02	0.01
b0:9f:ba:15:33:96			Phone iPhone	avaya	Mount-Shasta	Radio1	6 min 55 sec	0.00	0.00
dc:9b:9c:63:8a:ce			Phone iPhone	avaya	El-Capitan	Radio1	33 min 31 sec	0.11	0.03

Figure 203. Station Activity Over Time Period Report

Table Details for the Station Activity Over Time Period Report

The table shows the total session length and traffic statistics for each station included in the selection criteria.

- **Station MAC Address**
  This column shows the MAC address for each client station included in the report.
- **Station Hostname**
  This column shows the name for each client station.
- **Device Class/Type**
  The class and type of station device, e.g., Notebook/Mac. For a WDS Link session, AP/**WDS Link** are shown here.
- **SSID**
  The SSID to which each station was associated.
- **Total Session Duration**
  The total length of time that each station was associated. If the station connected multiple times during the selected time range, then all such sessions are totaled in this number. The entire length of each session that occurred during the time period is included. For example, say you specify

a time period of one hour. If a station was associated during that hour and the total length of that session was ten hours, then all ten hours of that session will be included in the **Total Session Duration** statistic.

- **Tx (Mb)**
  Shows the total amount of traffic transmitted by this station (in megabits) for the time period you specified.
- **Rx (Mb)**
  Shows the total amount of traffic received by this station (in megabits) for the time period you specified.

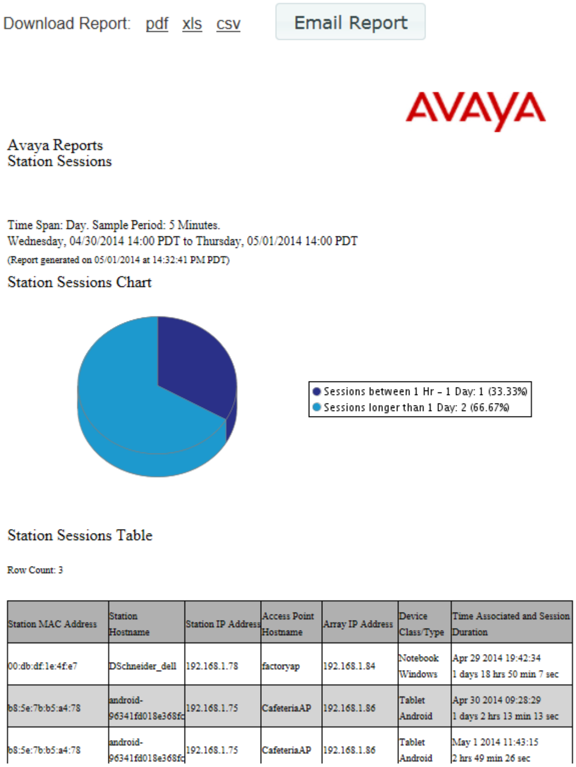
Station Sessions

This report lists stations that have currently active sessions, along with the time that the session has been active. A pie chart shows the distribution of session lengths.

Note that if you are using Wireless Distributed System (WDS) links to carry traffic between APs wirelessly, client link sessions will be displayed. These sessions can be recognized by their **Device Class** and **Type**—AP and **WDS Link**.

The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
AP Scope	Include only member APs of the selected AP group.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
Device Class	Include only this class of station device, e.g., Notebook, Phone, etc.
Device Type	Include only this type of station device, e.g., Windows, Mac, etc.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **"Schedule" on page 272**.
Email Report To	After running, email the report. See **"Email Report To" on page 272**.


Download Report: pdf xls csv
Email Report
AVAYA
Sessions between 1 Hr – 1 Day: 1 (33.33%)
Sessions longer than 1 Day: 2 (66.67%)

Avaya Reports
Station Sessions

Time Span: Day. Sample Period: 5 Minutes.
Wednesday, 04/30/2014 14:00 PDT to Thursday, 05/01/2014 14:00 PDT
(Report generated on 05/01/2014 at 14:32:41 PM PDT)

Station Sessions Chart

Station Sessions Table

Row Count: 3

Station MAC Address	Station Hostname	Station IP Address	Access Point Hostname	Array IP Address	Device Class/Type	Time Associated and Session Duration
00:db:df:1e:4f:e7	DSchneider_dell	192.168.1.78	factoryap	192.168.1.84	Notebook Windows	Apr 29 2014 19:42:34 1 days 18 hrs 50 min 7 sec
b8:5e:7b:b5:a4:78	android-96341fd018e368fc	192.168.1.75	CafeteriaAP	192.168.1.86	Tablet Android	Apr 30 2014 09:28:29 1 days 2 hrs 13 min 13 sec
b8:5e:7b:b5:a4:78	android-96341fd018e368fc	192.168.1.75	CafeteriaAP	192.168.1.86	Tablet Android	May 1 2014 11:43:15 2 hrs 49 min 26 sec

Figure 204. Station Sessions Report

Use the pie chart for an at-a-glance overview of session lengths for Wi-Fi clients.

Table Details for the Station Sessions Report

The table below the graph shows the session start time and length for each station included in the selection criteria.

- **Station MAC Address**
  This column shows the MAC address for each client station included in the report.
- **Station Hostname**
  This column shows the name for each client station.

- **Station IP Address**
  The IP address assigned to the station.
- **AP Hostname**
  The host name of the AP to which the station is associated.
- **AP IP Address**
  The IP address of the AP to which the station is associated.
- **Device Class/Type**
  The class and type of station device, e.g., Notebook/Mac. For a WDS Link session, AP/**WDS Link** are shown here.
- **Time Associated and Session Duration**
  The time that the session started (i.e., when the client associated to the AP), and the current length of the session.

Station Classification

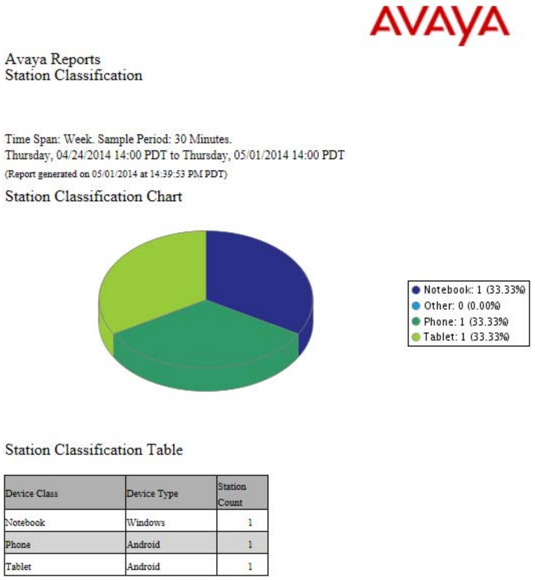
This report summarizes connected stations by their Device Class and Device Type. It includes all stations that were associated to the selected APs at any time during the specified time period. A pie chart shows the distribution of device classes.

Note that if you are using WDS (Wireless Distributed System) links to carry traffic between APs wirelessly, client link stations will be included. These stations can be recognized by their **Device Class** and **Type**—AP and **WDS Link**.

The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
AP Scope	Include only member APs of the selected AP group.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
Device Class	Include only this class of station device, e.g., Notebook, Phone, etc.
Device Type	Include only this type of station device, e.g., Windows, Mac, etc.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **"Schedule" on page 272**.
Email Report To	After running, email the report. See **"Email Report To" on page 272**.

Use the pie chart for an at-a-glance overview of the proportion of station device classes in your wireless network.



Avaya Reports
Station Classification

Time Span: Week. Sample Period: 30 Minutes.
Thursday, 04/24/2014 14:00 PDT to Thursday, 05/01/2014 14:00 PDT
(Report generated on 05/01/2014 at 14:39:53 PM PDT)

Station Classification Chart

Station Classification Table

Device Class	Device Type	Station Count
Notebook	Windows	1
Phone	Android	1
Tablet	Android	1

Figure 205. Station Classification Report

Table Details for the Station Classification Report

The table below the graph shows the station count for each combination of device type and class for the stations included in the selection criteria.

- **Device Class**
  The class of station device, e.g., Notebook, Tablet, Phone, etc. For a WDS Link session, AP is shown here.
- **Device Type**
  The type of station device, e.g., Blackberry, Android, Windows, Mac, etc. For a WDS Link session, **WDS Link** is shown here.

- **Station Count**
  The number of stations with this combination of device class and type. For example, Phone/Blackberry and Phone/Android will each have a separate row with their own count.

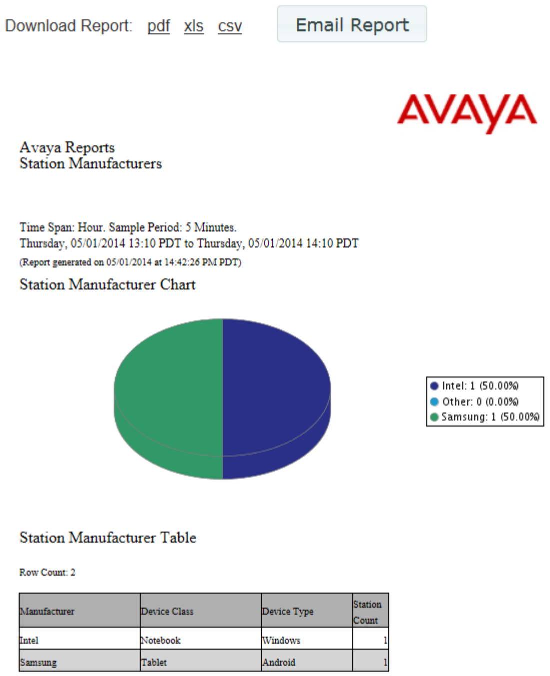
Station Manufacturers

This report summarizes connected stations by their manufacturer. It includes all stations that were associated to the selected APs at any time during the specified time period. A pie chart shows the distribution of device manufacturers.

The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **“Selection Criteria” on page 274** for details)
AP Scope	Include only member APs of the selected AP group.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
Device Class	Include only this class of station device, e.g., Notebook, Phone, etc.
Device Type	Include only this type of station device, e.g., Windows, Mac, etc.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **“Schedule” on page 272**.
Email Report To	After running, email the report. See **“Email Report To” on page 272**.

Use the pie chart for an at-a-glance overview of the proportion of manufacturers in your wireless network.



Download Report: pdf xls csv

Email Report

Avaya Reports
Station Manufacturers

Time Span: Hour. Sample Period: 5 Minutes.
Thursday, 05/01/2014 13:10 PDT to Thursday, 05/01/2014 14:10 PDT
(Report generated on 05/01/2014 at 14:42:26 PM PDT)

Station Manufacturer Chart

Station Manufacturer Table

Row Count: 2

Manufacturer	Device Class	Device Type	Station Count
Intel	Notebook	Windows	1
Samsung	Tablet	Android	1

Figure 206. Station Manufacturers Report

Table Details for the Station Manufacturers Report

The table below the graph shows the station count for each combination of device type and class for the stations included in the selection criteria.

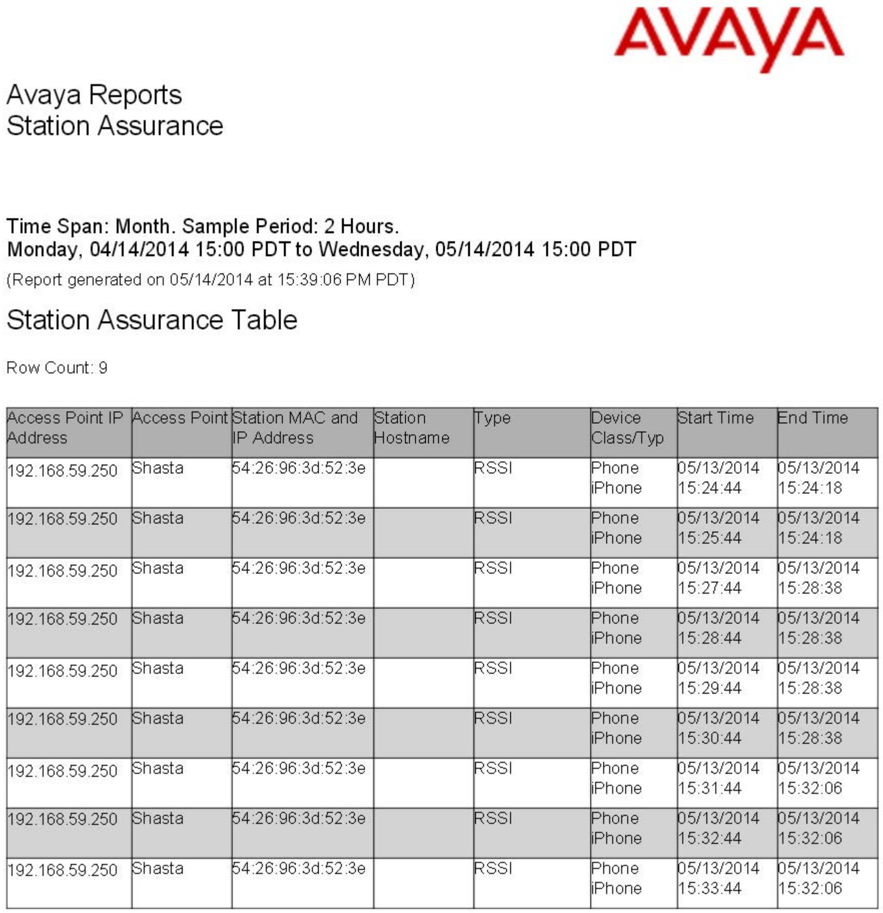
- **Manufacturer**
  The manufacturer of the station device, e.g., Apple, Motorola, etc.
- **Device Class**
  The class of station device, e.g., Notebook, Tablet, Phone, etc.
- **Device Type**
  The type of station device, e.g., Blackberry, Android, Windows, Mac, etc.
- **Station Count**
  The number of stations with this manufacturer.

Station Assurance

This report displays a list of Station Assurance events that have been detected in the wireless network. Station assurance monitors the connection quality that users are experiencing. The report shows client stations that have had connectivity issues, such as excessive packet retry or packet error rates, or stations that are unable to stay associated to the AP. When an AP detects that a station has reached the threshold value for one or more of the problems that it checks, an event is triggered. Please see **“Station Assurance” on page 96** in *Using the AvayaOS for Avaya WLAN AP 9100 Series (NN47252- 102)* for more information.

The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **“Selection Criteria” on page 274** for details)
AP Scope	Include only member APs of the selected AP group.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
Station Assurance Event Type	Include only this type of station connectivity problem.
Device Class	Include only this class of station device, e.g., Notebook, Phone, etc.
Device Type	Include only this type of station device, e.g., Windows, Mac, etc.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **“Schedule” on page 272**.
Email Report To	After running, email the report. See **“Email Report To” on page 272**.



Avaya Reports
Station Assurance

Time Span: Month. Sample Period: 2 Hours.
Monday, 04/14/2014 15:00 PDT to Wednesday, 05/14/2014 15:00 PDT

(Report generated on 05/14/2014 at 15:39:06 PM PDT)

Station Assurance Table

Row Count: 9

Access Point IP Address	Access Point	Station MAC and IP Address	Station Hostname	Type	Device Class/Typ	Start Time	End Time
192.168.59.250	Shasta	54:26:96:3d:52:3e		RSSI	Phone iPhone	05/13/2014 15:24:44	05/13/2014 15:24:18
192.168.59.250	Shasta	54:26:96:3d:52:3e		RSSI	Phone iPhone	05/13/2014 15:25:44	05/13/2014 15:24:18
192.168.59.250	Shasta	54:26:96:3d:52:3e		RSSI	Phone iPhone	05/13/2014 15:27:44	05/13/2014 15:28:38
192.168.59.250	Shasta	54:26:96:3d:52:3e		RSSI	Phone iPhone	05/13/2014 15:28:44	05/13/2014 15:28:38
192.168.59.250	Shasta	54:26:96:3d:52:3e		RSSI	Phone iPhone	05/13/2014 15:29:44	05/13/2014 15:28:38
192.168.59.250	Shasta	54:26:96:3d:52:3e		RSSI	Phone iPhone	05/13/2014 15:30:44	05/13/2014 15:28:38
192.168.59.250	Shasta	54:26:96:3d:52:3e		RSSI	Phone iPhone	05/13/2014 15:31:44	05/13/2014 15:32:06
192.168.59.250	Shasta	54:26:96:3d:52:3e		RSSI	Phone iPhone	05/13/2014 15:32:44	05/13/2014 15:32:06
192.168.59.250	Shasta	54:26:96:3d:52:3e		RSSI	Phone iPhone	05/13/2014 15:33:44	05/13/2014 15:32:06

Figure 207. Station Assurance Report

Table Details for the Station Assurance Report

For each station assurance event included in the selection criteria, the table shows the station and its device information, the AP to which it is associated, the type of connectivity problem, and the session start and end time.

- **AP Hostname**
  The host name of the AP to which the station is associated.

- **AP IP Address**
  The IP address of the AP to which the station is associated.
- **Station MAC and IP Address**
  This column shows the MAC and IP address for each station included in the report.
- **Station Hostname**
  This column shows the name of the station.
- **Type**

  The connection criterion that was not within acceptable thresholds.
- **Device Class/Type**
  The class and type of station device, e.g., Notebook/Mac. For a WDS Link session, AP/**WDS Link** are shown here.
- **Start Time**

  When the problem started.
- **End Time**

  When the affected session ended. This will show **Currently Active** if the session is still active.

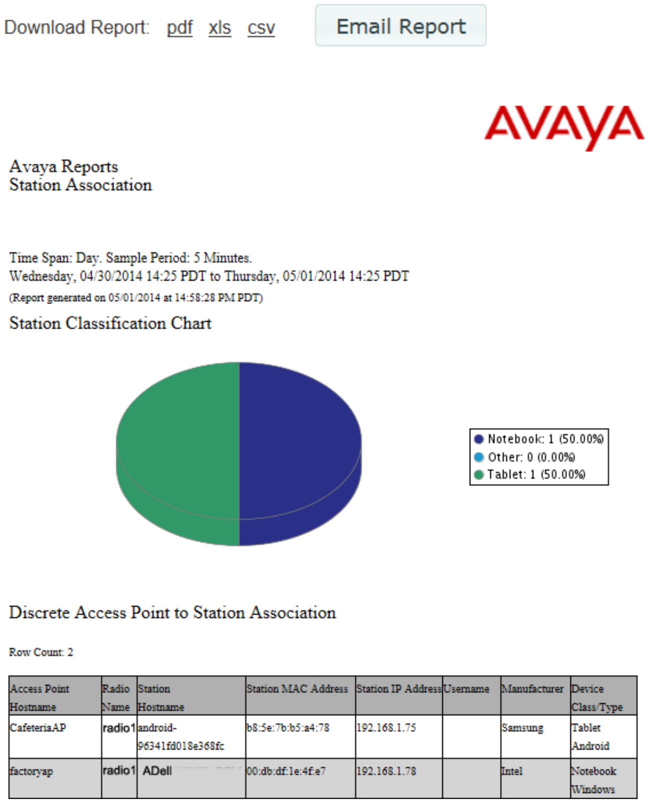
Associated Stations

This report consists of a table listing stations that are associated to your wireless network (**Figure 208**). The information displayed in this window is based on your **Selection Criteria**. You may use the criteria to report on just those stations that are associated to the selected APs, selected radios, and/or selected device type/class.

Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
AP Scope	Include only APs that are members of the selected AP group or profile.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
Radio	Include only the selected radio.
Device Class	Include only this class of station device, e.g., Notebook, Phone, etc.
Device Type	Include only this type of station device, e.g., Windows, Mac, etc.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **"Schedule" on page 272**.
Email Report To	After running, email the report. See **"Email Report To" on page 272**.

Station Classification Chart

This pie chart provides a quick overview of Wi-Fi clients, showing the proportions of different device classes.



Download Report: pdf xls csv Email Report

Avaya Reports
Station Association

Time Span: Day. Sample Period: 5 Minutes.
Wednesday, 04/30/2014 14:25 PDT to Thursday, 05/01/2014 14:25 PDT
(Report generated on 05/01/2014 at 14:58:28 PM PDT)

Station Classification Chart

Discrete Access Point to Station Association

Row Count: 2

Access Point Hostname	Radio Name	Station Hostname	Station MAC Address	Station IP Address	Username	Manufacturer	Device Class/Type
CafeteriaAP	radio1	android-96341fd018e368fc	b8:5e:7b:b5:a4:78	192.168.1.75		Samsung	Tablet Android
factoryap	radio1	ADell	00:db:df:1e:4f:e7	192.168.1.78		Intel	Notebook Windows

Figure 208. Station Association

Discrete AP to Station Association

This table presents a list of all stations associated to the selected APs/radios/devices based on the time period you specify. The results shown in this window are organized by the following column headers:

- **AP Hostname**
  The host name of the AP that the station is associated with.
- **Radio Name**
  The radio that the station is associated with.

- **Station Hostname**
  This column shows the name for each client station listed in the report.
- **Station MAC Address**
  This is the station's MAC address.
- **Station IP Address**
  The IP address assigned to the station.
- **Username**
  The session was authenticated under this user name.
- **Manufacturer**
  The manufacturer of the station device.
- **Device Class/Type**
  The class and type of station device, e.g., Notebook/Mac. For a WDS Link session, AP**/WDS Link** are shown here.

Stations By AP

This report displays a bar chart showing the number of stations associated to those APs that have the highest station count (**Figure 209**). The table below gives minimum and maximum counts of clients per AP. The information displayed in this window is based on your **Selection Criteria**.

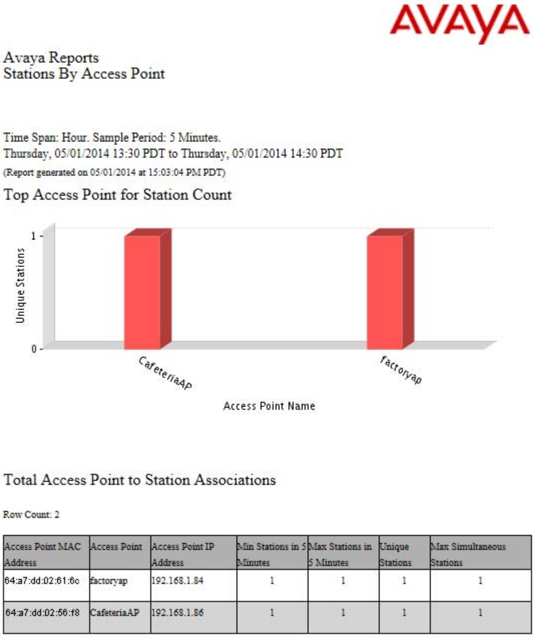
Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
AP Scope	Include only APs that are members of the selected AP group or profile.
Map	Include only APs that are members of the selected map.
Radio	Include only the selected radio.
Device Class	Include only this class of station device, e.g., Notebook, Phone, etc.
Device Type	Include only this type of station device, e.g., Windows, Mac, etc.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **"Schedule" on page 272**.
Email Report To	After running, email the report. See **"Email Report To" on page 272**.

Total AP to Station Associations

This table shows the minimum and maximum number of stations that have been associated to each AP, with the following information:

- **AP Name**
  The host name assigned to the AP.
- **AP MAC Address**
  This is the AP's MAC address.

- **AP IP Address**
  The IP address assigned to the AP.
- **Min Stations in 5 Minutes**
  Shows the lowest number of stations concurrently associated to each AP over any five minute interval during the time period.
- **Max Stations in 5 Minutes**
  Shows the number of stations that were concurrently associated to each AP at the busiest (peak) five minute interval during the time period.
- **Unique Stations**
  Shows the total number of different stations that have associated to each AP over the time period. "Unique" means that if the same station disconnects and then reconnects, it will not be counted more than once.
- **Max Simultaneous Stations**
  Shows the maximum number of stations that were concurrently associated to each AP during the time period.



Avaya Reports
Stations By Access Point

Time Span: Hour. Sample Period: 5 Minutes.
Thursday, 05/01/2014 13:30 PDT to Thursday, 05/01/2014 14:30 PDT
(Report generated on 05/01/2014 at 15:03:04 PM PDT)

Top Access Point for Station Count

Total Access Point to Station Associations

Row Count: 2

Access Point MAC Address	Access Point	Access Point IP Address	Min Stations in 5 Minutes	Max Stations in 5 Minutes	Unique Stations	Max Simultaneous Stations
64:a7:dd:02:61:6c	factoryap	192.168.1.84	1	1	1	1
64:a7:dd:02:56:f8	CafeteriaAP	192.168.1.86	1	1	1	1

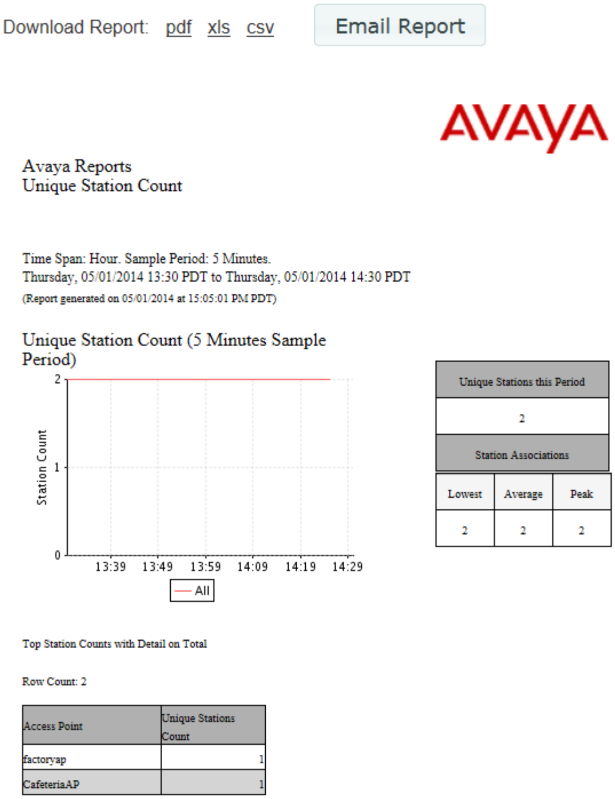
Figure 209. Station Association (By AP) Report

Unique Station Count

This report displays a line graph showing unique station counts over time. “Unique” means that if the same station disconnects and then reconnects, it will not be counted more than once in any sum displayed.

The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **“Selection Criteria” on page 274** for details)
AP Scope	Include only member APs of the selected AP group.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
SSID	Include only the selected SSID.
VLAN	Include only the selected VLAN (specified by name or number)
Media Type	Include only radios operating in the selected mode (802.11b, 802.11n, etc.)
Device Class	Include only this class of station device, e.g., Notebook, Phone, etc.
Device Type	Include only this type of station device, e.g., Windows, Mac, etc.
Association	Include only authenticated stations, or all stations.
Detail on	Break out counts by the selected category, or show only totals.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **“Schedule” on page 272**.
Email Report To	After running, email the report. See **“Email Report To” on page 272**.



Download Report: pdf xls csv

Email Report

Avaya Reports
Unique Station Count

Time Span: Hour. Sample Period: 5 Minutes.
Thursday, 05/01/2014 13:30 PDT to Thursday, 05/01/2014 14:30 PDT
(Report generated on 05/01/2014 at 15:05:01 PM PDT)

Unique Station Count (5 Minutes Sample Period)

Unique Stations this Period		
2		
Station Associations		
Lowest	Average	Peak
2	2	2

Top Station Counts with Detail on Total

Row Count: 2

Access Point	Unique Stations Count
factoryap	1
CafeteriaAP	1

Figure 210. Unique Station Count Report

The graph is detailed on (i.e., broken out into categories by) your choice of category:

- Total—show totals only.
- AP Name—show station count by AP.
- VLAN (by name or number)—show station count by VLAN.
- SSID—show station count by SSID.
- Media Type—show station count by radio mode: 802.11n, 802.11a, etc.
- Radio—show station count by radio: radio1, an1, abgn1, etc.

- Association Type—show station count according to whether the connection is authenticated.

The graph has a separate line for each member of the detailing category. For example, if you detail on radio as shown in **Figure 210**, then there will be a separate line graph for each radio: an1, an2, and so on. This report also shows you how many stations are currently online, and includes minimum (Lowest) and maximum (Peak) activity. A table at the bottom lists peak station counts broken out by your requested category.

Table Details for the Station Count Report

The table below the graph simply shows the peak station count for each member of the **Detail on** category.

Access Point Reports

AP status reports provide utility functions, such as listing all APs for you and showing reliability statistics.

The following reports are available in this section:

- **Access Point Inventory**
  Provides a list of all APs in your managed wireless network, including serial numbers.
- **Access Point Availability**
  This report shows reliability statistics for your managed wireless network, including MTBF and MTTR figures.
- **Grouped Access Point Availability**
  This report shows average percentage of time that the APs in each profile or AP group have been up.

Access Point Inventory

This report creates an inventory list for your use (**Figure 211**). The result is a list of all your managed wireless APs for your reference. You may find it very useful to save this report as a .csv or .xls file as a starting point for working with Excel. The report is based on your **Selection Criteria**.

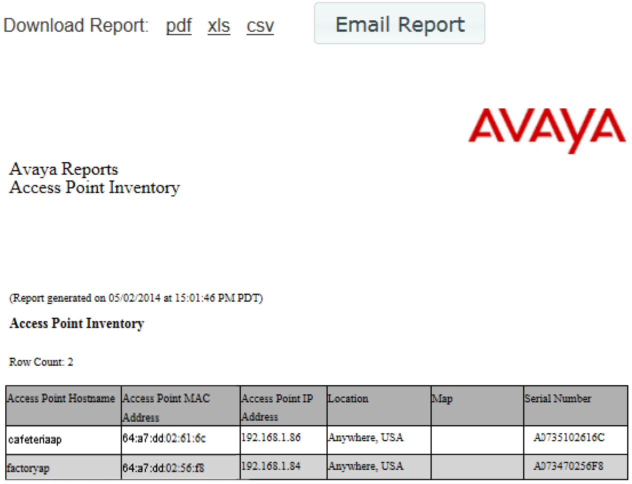
Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
AP Scope	Include only APs that are members of the selected AP group or profile.
Map	Include only APs that are members of the selected map.
Order table by	Sort table by selected column.
Order Direction	Sort in ascending or descending order.

Selection Criterion	Description (see **“Selection Criteria” on page 274** for details)
Schedule	Run the report at this time. See **“Schedule” on page 272**.
Email Report To	After running, email the report. See **“Email Report To” on page 272**.

Table Details for the AP Inventory Report

The table portion of the report shows the name, addresses, and serial number of the selected APs, organized by the following column headers:

- **AP Hostname**
  The host name assigned to the AP. Only APs that meet your selection criteria are included.
- **AP MAC Address**
  This is the AP’s MAC address.
- **IP Address**
  This is the AP’s IP address.
- **Location**
  The physical location information that you entered for this AP, if any.
- **Serial Number**
  This is the AP’s serial number.



Avaya Reports
Access Point Inventory

(Report generated on 05/02/2014 at 15:01:46 PM PDT)

Access Point Inventory

Row Count: 2

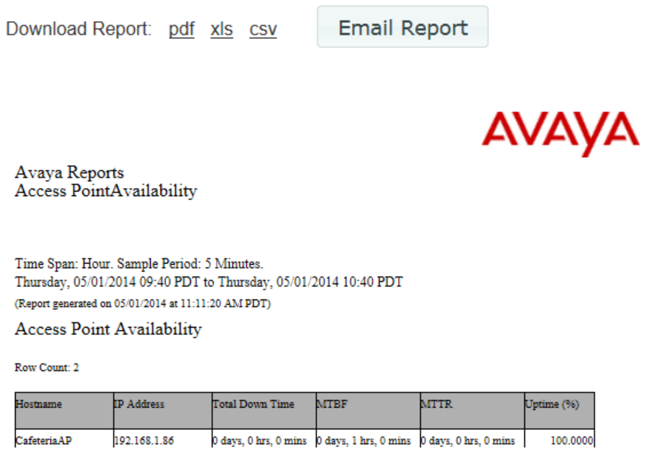
Access Point Hostname	Access Point MAC Address	Access Point IP Address	Location	Map	Serial Number
cafeteriaap	64:a7:dd:02:61:6c	192.168.1.86	Anywhere, USA		A0735102616C
factoryap	64:a7:dd:02:56:f8	192.168.1.84	Anywhere, USA		A073470256F8

Figure 211. AP Inventory Report

Access Point Availability

This report shows system reliability statistics for the wireless network, based on **Selection Criteria**. **Figure 212** shows an example of the AP Availability report.

Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
AP Scope	Include only APs that are members of the selected AP group or profile.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **"Schedule" on page 272**.
Email Report To	After running, email the report. See **"Email Report To" on page 272**.



Avaya Reports
Access PointAvailability

Time Span: Hour. Sample Period: 5 Minutes.
Thursday, 05/01/2014 09:40 PDT to Thursday, 05/01/2014 10:40 PDT
(Report generated on 05/01/2014 at 11:11:20 AM PDT)

Access Point Availability

Row Count: 2

Hostname	IP Address	Total Down Time	MTBF	MTTR	Uptime (%)
CafeteriaAP	192.168.1.86	0 days, 0 hrs, 0 mins	0 days, 1 hrs, 0 mins	0 days, 0 hrs, 0 mins	100.0000

Figure 212. AP Availability Report

Table Details for the AP Availability Report

The AP Availability report is generated as a table. The results are organized by the following column headers:

- **Hostname**
  The host name assigned to the AP.
- **IP Address**
  The IP address assigned to the AP.
- **Total Down Time**
  Shows the total time (in minutes) that this AP has been down within the time range specified for this report.
- **Mean Time Between Failures (MTBF)**
  Shows the average length of time that elapsed between failures of the AP within the time range specified for this report—shown in days/hours/minutes.
- **Mean Time To Repair (MTTR)**
  Shows the average length of time that elapsed before functionality to the AP was restored following a failure within the time range specified for this report—shown in days/hours/minutes.
- **Up Time%**
  This is the time that the AP has been up and running successfully, based on a percentage of the total time for the time period specified for this report.

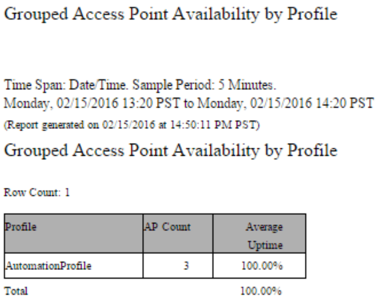
If WOS is non-operational for a period of time, AP availability information for this report is extrapolated from the last known state of the AP prior to WOS going off-line.

Grouped Access Point Availability

This report shows system reliability statistics for your wireless network grouped by **Profiles** or by **AP Groups**, based on your **Selection Criteria**. **Figure 213** shows an example of this report.

Availability is calculated per AP, as for the **Access Point Availability** report. Then Average Uptime over the period of the report is calculated as the average percentage of time that the members of each group or profile were up. The report includes a row for each group or profile in the network, depending on the display type you selected.

Selection Criterion	Description (see **“Selection Criteria” on page 274** for details)
Display Availability by	Show average AP availability for AP groups or for profiles.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **“Schedule” on page 272**.
Email Report To	After running, email the report. See **“Email Report To” on page 272**.



Grouped Access Point Availability by Profile

Time Span: Date/Time. Sample Period: 5 Minutes.
Monday, 02/15/2016 13:20 PST to Monday, 02/15/2016 14:20 PST
(Report generated on 02/15/2016 at 14:50:11 PM PST)

Grouped Access Point Availability by Profile

Row Count: 1

Profile	AP Count	Average Uptime
AutomationProfile	3	100.00%
Total		100.00%

Figure 213. Grouped Access Point Availability Report

Table Details for the Grouped Access Point Availability Report

The AP Availability report is generated as a table. The results are organized by the following column headers:

- **Profile** or **AP Group**
  The profile or AP group name for each row.
- **AP Count**
  The number of APs in this profile or AP group.
- **Average Uptime**
  Shows the average percentage of time that the APs in this profile or AP group have been up within the time range specified for this report.

RF Reports

RF reports provide information on RF (channel) usage in your network. For more information about assigning channels, see **"Radios" on page 487**. The following RF report is available:

- **Channel Usage**
  Shows which channels each radio is using.

Channel Usage

This report generates a table of current channel assignments for each radio and for all media types (2.4 and 5 GHz channels), based on your **Selection Criteria**.

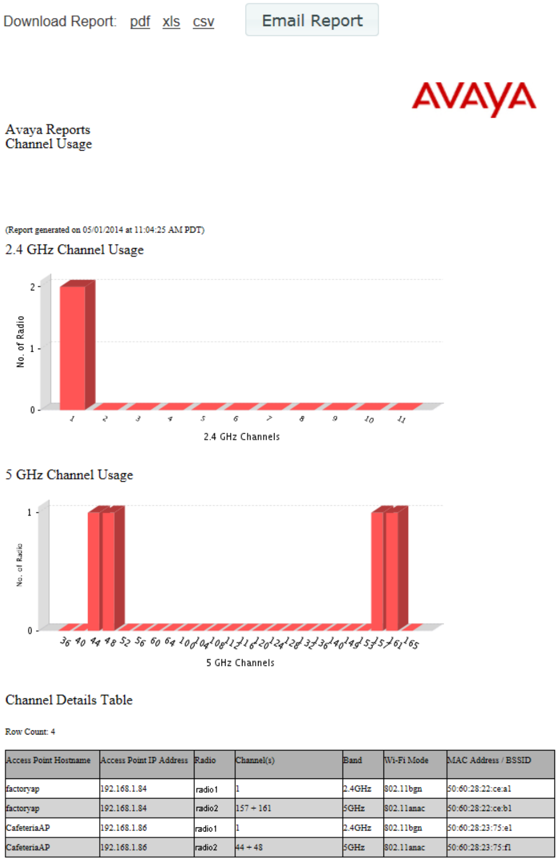
Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
AP Scope	Include only APs that are members of the selected AP group or profile.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
Table Row Limit	Total number of rows.
Schedule	Run the report at this time. See **"Schedule" on page 272**.
Email Report To	After running, email the report. See **"Email Report To" on page 272**.

The Channel Usage report also provides separate bar charts for the 2.4 GHz and 5 GHz bands, highlighting at a glance the number of radios using each channel.

Table Details for the Channel Usage Report

The results shown in this report are organized by the following column headers:

- **AP Hostname**
  The host name assigned to the AP that the radio belongs to.



Avaya Reports
Channel Usage

(Report generated on 05/01/2014 at 11:04:25 AM PDT)

2.4 GHz Channel Usage

5 GHz Channel Usage

Channel Details Table

Row Count: 4

Access Point Hostname	Access Point IP Address	Radio	Channel(s)	Band	Wi-Fi Mode	MAC Address / BSSID
factoryap	192.168.1.84	radio1	1	2.4GHz	802.11bgn	50:60:28:22:ce:a1
factoryap	192.168.1.84	radio2	157 + 161	5GHz	802.11anac	50:60:28:22:ce:b1
CafeteriaAP	192.168.1.86	radio1	1	2.4GHz	802.11bgn	50:60:28:23:75:e1
CafeteriaAP	192.168.1.86	radio2	44 + 48	5GHz	802.11anac	50:60:28:23:75:f1

Figure 214. Channel Usage Report

- **AP IP Address**
  The IP address assigned to the host AP.
- **Radio**
  The name of the radio (for example, radio1, radio3, abg4, an3, a7, etc.).
- **Channel(s)**
  This column shows the channel(s) used by the radio. IEEE 802.11n and .11ac radios may use adjacent bonded channels for improved

performance, so those radios will show additional channels if they have bonding in operation.

- **Wi-Fi Mode**
  This shows the IEEE 802.11 media in use by the radio. Note that client stations cannot associate with the monitor radio.
- **MAC Address / BSSID**
  This is the radio's MAC address.

Security Reports

The level of security you introduce into your network depends on the requirements of your deployment, though we strongly recommend that you do not configure your APs as Open Systems (no authentication required and no data encryption). An Access Control List (ACL) and/or Wired Equivalent Privacy (WEP) should be your minimum requirement for security. WPA and WPA2 offer even stronger security. The wireless AP's line rate encryption ensures high performance when encryption is in use. For more information about security, go to **"Rogues" on page 90** and **"IDS Events" on page 94**.

Security reports provide data based on the security parameters defined for your network of APs, including authentication and data encryption. The following security reports are available:

- **IDS Events**
  Displays a list of intrusion detection events.

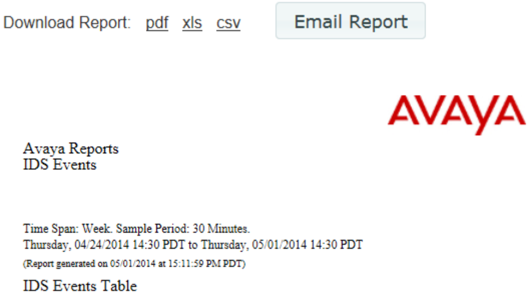
- **Rogue List**
  Shows all rogue APs that are visible on your network and provides charts that distinguish between **Unclassified**, **Approved**, **Known** or **Unknown** rogue devices.

IDS Events

This report displays a list of Intrusion Detection System (IDS) events, such as flood attacks, that have been detected in the wireless network. For descriptions of the types of attacks detected, as well as the settings to fine-tune IDS on APs, please see *Using AvayaOS for Avaya WLAN AP 9100 Series (NN47252-102)*.

The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **“Selection Criteria” on page 274** for details)
AP Scope	Include only member APs of the selected AP group.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
IDS Event Type	Include only this type of intrusion detection problem.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **“Schedule” on page 272**.
Email Report To	After running, email the report. See **“Email Report To” on page 272**.



Avaya Reports
IDS Events

Time Span: Week. Sample Period: 30 Minutes.
Thursday, 04/24/2014 14:30 PDT to Thursday, 05/01/2014 14:30 PDT
(Report generated on 05/01/2014 at 15:11:59 PM PDT)

IDS Events Table

Figure 215. IDS Events Report

Table Details for the IDS Events Report

For each IDS event included in the selection criteria, the table shows the detecting AP, the time and channel on which the attack occurred, and the SSID and MAC address of the attacker, if appropriate.

- **AP MAC Address**
  The MAC address of the detecting AP.
- **AP Hostname**
  The host name of the detecting AP.
- **Type**
  The type of attack detected.
- **Channel**
  The channel on which the attack occurred.
- **Event MAC Address**
  This column shows the MAC address of the attacker.

- **Event SSID**
  The SSID that was attacked.
- **Event Time**

  The date and time that the attack occurred.

Rogue List

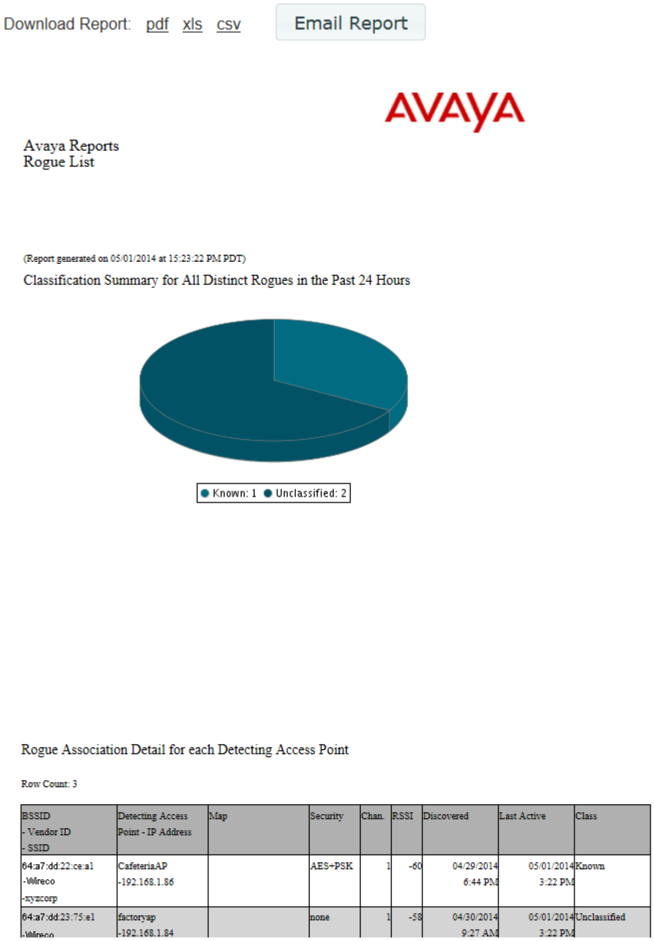
A rogue is any wireless device that is visible on your network but not recognized as being an integral part of the network. Rogue detection is performed automatically and constantly by the built-in threat-sensing monitor radio in each AP (if monitoring is enabled). WOS collects this information from the APs in its managed network. As access points are switched off and on, the list of detected rogues changes. Please see **"Rogues" on page 90** for more information about rogues and their classifications and handling.

This report displays a color-coded pie chart representation of all rogue devices that have been detected by the portions of your network that you selected.

Selection Criterion	Description (see **"Selection Criteria" on page 274** for details)
AP Scope	Include only APs that are members of the selected AP group or profile.
Map	Include only APs that are members of the selected map.
AP	Include only the selected AP.
SSID	Include only the selected SSID.
Classification	Include only rogue radios whose classification is **Approved, Known, Unknown, Unclassified, Blocked,** or **Ad Hoc**.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See **"Schedule" on page 272**.
Email Report To	After running, email the report. See **"Email Report To" on page 272**.

The chart (**Figure 216**) shows the percentages of rogue devices based on their classifications.

- **Unclassified**
  These rogues have not yet been classified.



Avaya Reports
Rogue List

(Report generated on 05/01/2014 at 15:23:22 PM PDT)

Classification Summary for All Distinct Rogues in the Past 24 Hours

Rogue Association Detail for each Detecting Access Point

Row Count: 3

BSSID - Vendor ID - SSID	Detecting Access Point - IP Address	Map	Security	Chan.	RSSI	Discovered	Last Active	Class
64:a7:dd:22:ce:a1 -Wireco -xyzcorp	CafeteriaAP -192.168.1.86		AES+PSK	1	-60	04/29/2014 6:44 PM	05/01/2014 3:22 PM	Known
64:a7:dd:23:75:e1 -Wireco	factoryap -192.168.1.84		none	1	-58	04/30/2014 9:27 AM	05/01/2014 3:22 PM	Unclassified

Figure 216. Rogue List Report

- **Approved**
  When a rogue is designated as Approved the system stops reporting on it and no longer displays it in the rogue list.

- **Known**
  When a rogue is designated as Known the system stops reporting on this rogue, but still displays it in the rogue list.
- **Unknown**
  These rogues are always displayed in the rogue list.
- **Blocked**
  These rogues have been designated as blocked. An AP can block this AP by preventing stations from staying associated to the rogue.

Table Details for the Security Report (Rogue List)

Below the pie chart is a table identifying all of the rogues included in the pie chart. The results are sorted by the **Last Active** time column, in descending order.

- **BSSID—Vendor ID—SSID**
  This shows the BSSID of the rogue (typically its MAC address), the name of its equipment manufacturer, and the SSID (network name) that it is broadcasting. If the rogue's SSID is set to default and is being broadcast, then the entry in this field will be **default**. If the rogue is configured not to broadcast its SSID, then the entry in this field will be **(empty)**.
- **Detecting AP—IP Address**
  Shows the host name and IP address of the AP that is detecting the rogue device.
- **Security**
  Shows the authentication and encryption security levels detected on the rogue device (for example, AES+TKIP+EAP). If the rogue is running an open system—no security—the entry in this field is **none**.
- **Channel**
  This is the channel that the rogue is detected on.
- **RSSI** (Received Signal Strength Indicator)
  Shows the strength of the signal being observed from the rogue device by the detecting AP.
- **Discovered**
  This is the date and time that the rogue was discovered by the detecting AP.

- **Last Active**
  This is the date and time that the rogue was last seen by the detecting AP, or **Active** if the rogue is still active.
- **Class**
  The classification of the rogue, as defined above.

Configuring a Wireless AP

The following topics describe how to configure a selected AP using the **Configuration** tab on the **AP Details** window. This tab provides a menu with an extensive set of convenient options for changing AP settings.

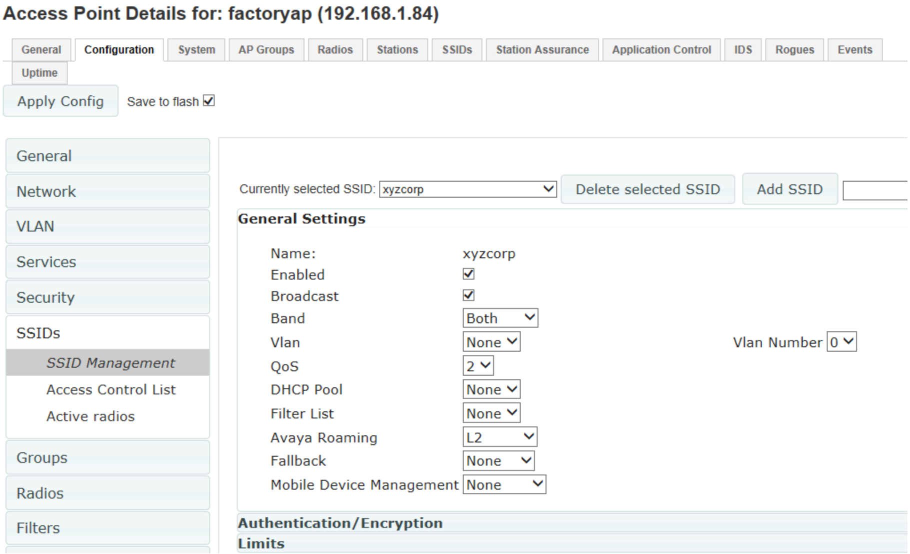
The following WMI windows allow you to establish configuration parameters for your AP, and include:

Note that smaller APs that use the AOSLite system software, such as the WAP9112, have many fewer settings than more powerful APs. Settings that are not available on a particular AP are not displayed, or will be grayed out.

- **"General" on page 371**
- **"Network" on page 372**
- **"VLAN" on page 391**
- **"Services" on page 396**
- **"Security" on page 413**
- **"SSIDs" on page 446**
- **"Groups" on page 480**
- **"Radios" on page 487**
- **"Filters" on page 538**
- **"Tunnels" on page 545**

The Configuration Tab

To reach this window, select the APs link in the AP **Configuration** section under **Configure** at the top of the window. You may also arrive at this window by selecting the APs link in the **Overview** section under **Monitor** at the top of the window. Locate the desired AP in the list. Its **Hostname** field is a link—click it to go to the AP Details window, and then select the **Configuration** tab (Figure 217).



Access Point Details for: factoryap (192.168.1.84)

Save to flash ☑

Currently selected SSID: xyzcorp

Name: xyzcorp
Enabled ☑
Broadcast ☑
Band Both
Vlan None Vlan Number 0
QoS 2
DHCP Pool None
Filter List None
Avaya Roaming L2
Fallback None
Mobile Device Management None

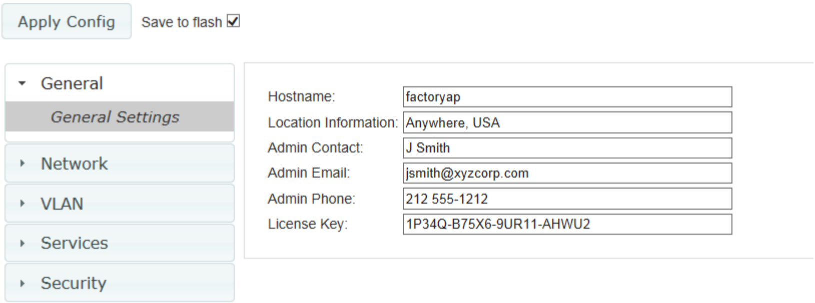
Figure 217. Opening the Configuration Window

Use the menu at the left of this window to go to the desired configuration page.

Note that as long as you remain on the Configuration tab, you may go from window to window to configure different groups of settings on the AP, and all of your changes will be accumulated. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP's running configuration. If you wish to make these changes permanent, check **Save to flash** before you click **Apply Config**, otherwise the changes you made will not be applied the next time the AP is rebooted. If you leave the Configuration tab without saving, your changes will be lost.

General

This window allows you to set general information about this AP, including changing its host name and license, and setting administrator contact information.



Hostname: factoryap
Location Information: Anywhere, USA
Admin Contact: J Smith
Admin Email: jsmith@xyzcorp.com
Admin Phone: 212 555-1212
License Key: 1P34Q-B75X6-9UR11-AHWU2

Figure 218. General Information

Procedure for Configuring General Information

1. **Hostname:** Specify a unique host name for this AP. The host name is used to identify the AP on the network. Use a name that will be meaningful within your network environment, up to 64 alphanumeric characters. The default is the AP's serial number.
2. **Location Information**: Enter a brief but meaningful description that accurately defines the physical location of the AP. In an environment where multiple units are installed, clear definitions for their locations are important if you want to identify a specific unit.
3. **Admin Contact**: Enter the name and contact information of the person who is responsible for administering the AP at the designated location.
4. **Admin Email**: Enter the email address of the admin contact you entered in Step 3.
5. **Admin Phone**: Enter the telephone number of the admin contact you entered in Step 3.

6. **License Key**: If Avaya issued you a license that differs from the current value shown, enter it now.

Network

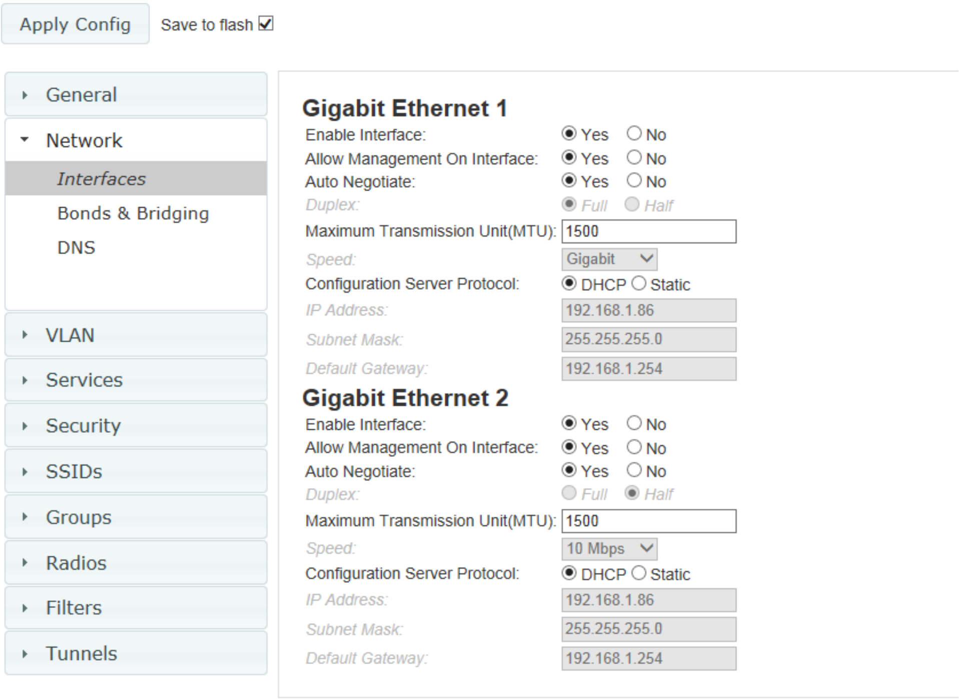
Windows that allow you to change or view a settings associated with the network interfaces include:

- **“Interfaces” on page 373**
- **“AP Switch” on page 376**
- **“Bonds and Bridging” on page 379**
- **“DNS Settings” on page 387**
- **“Fabric Attach (FA) or LLDP Settings” on page 388**

Interfaces

Note that smaller APs that use the AOSLite system software, such as the WAP9112 and the WAP9114, have many fewer settings than more powerful APs. The Gigabit port only supports Auto-negotiate mode. Settings that are not available on a particular AP are not displayed, or will be grayed out.

This window allows you to view or change network interface settings. It shows only the interfaces that are actually on this AP.



Gigabit Ethernet 1

Enable Interface: ● Yes ○ No
Allow Management On Interface: ● Yes ○ No
Auto Negotiate: ● Yes ○ No
Duplex: ● Full ○ Half
Maximum Transmission Unit(MTU): 1500
Speed: Gigabit
Configuration Server Protocol: ● DHCP ○ Static
IP Address: 192.168.1.86
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.254

Gigabit Ethernet 2

Enable Interface: ● Yes ○ No
Allow Management On Interface: ● Yes ○ No
Auto Negotiate: ● Yes ○ No
Duplex: ○ Full ● Half
Maximum Transmission Unit(MTU): 1500
Speed: 10 Mbps
Configuration Server Protocol: ● DHCP ○ Static
IP Address: 192.168.1.86
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.254

Figure 219. Network Interface Settings

Procedure for Configuring the Network Interfaces

1. **Enable Interface:** Choose **Yes** to enable this network interface, or choose No to disable the interface.

2. **Allow Management on Interface**: Choose **Yes** to allow management of this AP via the selected network interface, or choose **No** to deny all management privileges for this interface.

3. **Auto Negotiate**: This feature allows the AP to negotiate the best transmission rates automatically. Choose **Yes** to enable this feature, or choose **No** to disable this feature—the default is enabled. If you disable the Auto Negotiate feature, you must define the Duplex and Speed options manually (otherwise these options are not available).

   a. **Duplex**: Full-duplex mode transmits data in two directions simultaneously (for example, a telephone is a full-duplex device because both parties can talk and be heard at the same time). Half-duplex allows data transmission in one direction at a time only (for example, a walkie-talkie is a half-duplex device). If the Auto-Negotiate feature is disabled, you can manually choose **Half** or **Full** duplex for your data transmission preference.

   b. **MTU**: the Maximum Transmission Unit size. This is the largest packet size (in bytes) that the interface can pass along.

   c. **Speed**: If the Auto-Negotiate feature is disabled, you must manually choose the desired data transmission speed from the drop-down list. If configuring the Fast Ethernet interface, the options are **10 Megabit** or **100 Megabit**. For configuring the Gigabit interfaces the options are **10 Megabit** or **100 Megabit**. Note that the 1000 Megabit speed and the 2.5 Gigabit speed (on models that support it) can only be set by Auto-Negotiation. There are no manual settings for these rates.

4. **Configuration Server Protocol / IP Settings**: Choose **DHCP** to instruct the AP to use DHCP when assigning IP addresses to the AP, or choose **Static IP** if you intend to enter IP addresses manually. If you select the Static IP option you must specify the IP address, IP subnet mask and default gateway.

   a. **IP Address**: If you selected the Static IP option, enter a valid IP address for the AP. To use any of the remote connections (Web, SNMP, or SSH), a valid IP address must be established.

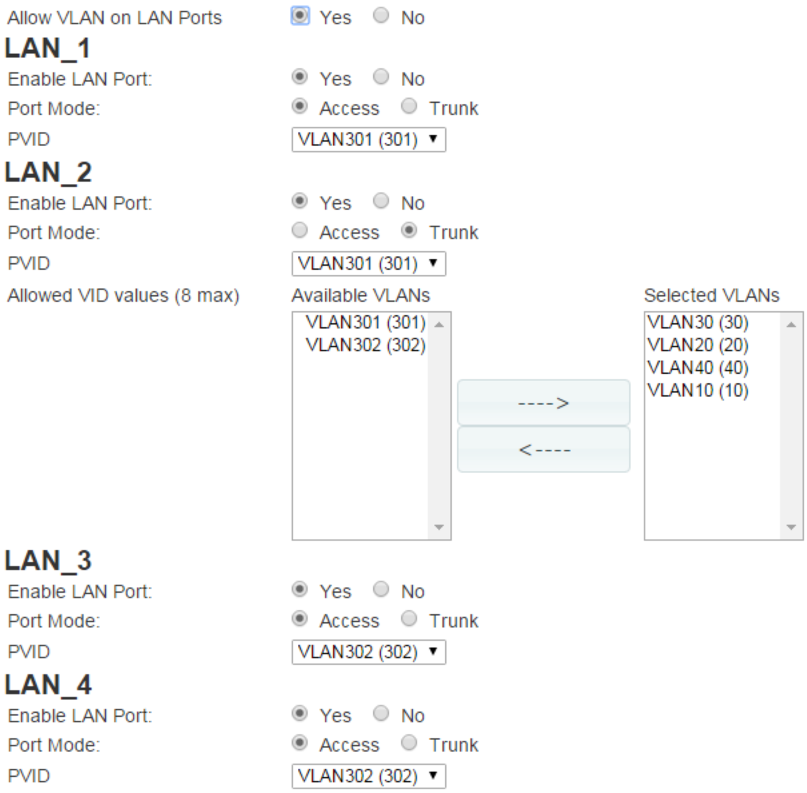
b. **Subnet Mask**: If you selected the Static IP option, enter the subnet mask (the default for Class C is 255.255.255.0). The subnet mask defines the range of IP addresses that are available on the routed subnet where the AP is located.

c. **Default Gateway**: If you selected the Static IP option, enter a valid IP address for the default gateway. This is the IP address of the router that the AP uses to transmit data to other networks.

Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

AP Switch

This window is only available for the WAP9112, because it is the only AP model that has switch ports available for use as downlinks. These four Ethernet ports are named **Lan1** to **Lan4**. If you are connecting devices to any of these ports on the WAP9112, enable them and configure them on this window.



Allow VLAN on LAN Ports ● Yes ○ No

LAN_1

Enable LAN Port: ● Yes ○ No

Port Mode: ● Access ○ Trunk

PVID VLAN301 (301) ▾

LAN_2

Enable LAN Port: ● Yes ○ No

Port Mode: ○ Access ● Trunk

PVID VLAN301 (301) ▾

Allowed VID values (8 max)

Available VLANs: VLAN301 (301), VLAN302 (302)

Selected VLANs: VLAN30 (30), VLAN20 (20), VLAN40 (40), VLAN10 (10)

LAN_3

Enable LAN Port: ● Yes ○ No

Port Mode: ● Access ○ Trunk

PVID VLAN302 (302) ▾

LAN_4

Enable LAN Port: ● Yes ○ No

Port Mode: ● Access ○ Trunk

PVID VLAN302 (302) ▾

Figure 220. Network Interface Settings

Procedure for Configuring AP Switch Ports (for WAP9112 only)

1. **Allow VLAN on LAN ports:** Choose **Yes** to allow configuration of the LAN ports as trunk or access ports with the VLAN settings below. The LAN ports (**Lan1** - **Lan4**, also called switch ports or downlinks) are the four Ethernet ports on the bottom of the wall AP. You should configure VLANs before proceeding with the steps below.

   If you choose **No**, the AP will simply pass all traffic between the LAN ports and the Gigabit Ethernet (uplink), without any inspection or modification. This is the default behavior.

   Configure each LAN port as follows.

   a. **Enable LAN Port**: Choose **Yes** to enable use of this port, or **No** to disable it (the port will not pass traffic).

   b. **Port Mode**: Select **Access** or **Trunk**.

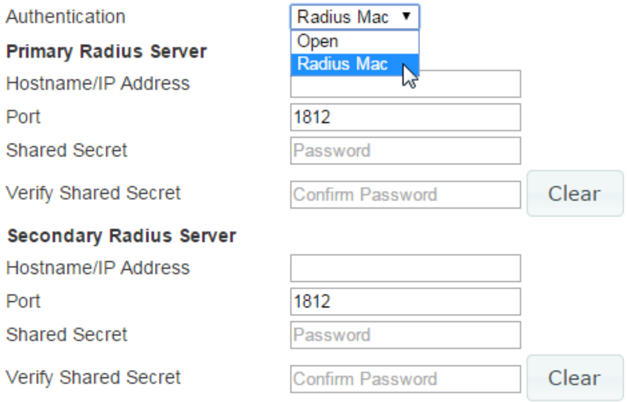
      An *access* port carries traffic for only one VLAN, and has only one VLAN configured on the interface.

      A *trunk* port carries traffic for several VLANs at the same time. You may have multiple VLANs configured on the interface (up to **8** plus one for the **PVID**, see below).

   c. **PVID** (Port VLAN ID): Select a VLAN from the drop down list. The VLAN must have been previously defined (see **“VLAN” on page 391**). All untagged ingress (entering) packets to this port will be tagged with the PVID for forwarding to other ports. Conversely, egress (exiting this port) packets are only sent out if they are tagged with this PVID (for trunk ports, packets are also sent out if they are tagged with any of that port’s Selected VLANs). Packets not meeting these conditions are dropped.

   d. **Allowed VID values (8 max) / Selected VLANs**: This setting is only used for trunk ports. Specify the VLANs to be handled on this trunk port. The VLANs must all have been previously defined (see **“VLAN” on page 391**). Use the right arrow to move the VLANS to be included to the **Selected VLANS** list.

2. **Authentication**:



Authentication: Radius Mac ▼ (Open / Radius Mac)

Primary Radius Server

Hostname/IP Address:

Port: 1812

Shared Secret: Password

Verify Shared Secret: Confirm Password [Clear]

Secondary Radius Server

Hostname/IP Address:

Port: 1812

Shared Secret: Password

Verify Shared Secret: Confirm Password [Clear]

Figure 221. AP Switch Authentication (WAP9112)

For devices connecting to the AP switch ports, the following authentication options are available. This setting applies globally to all four switch ports.

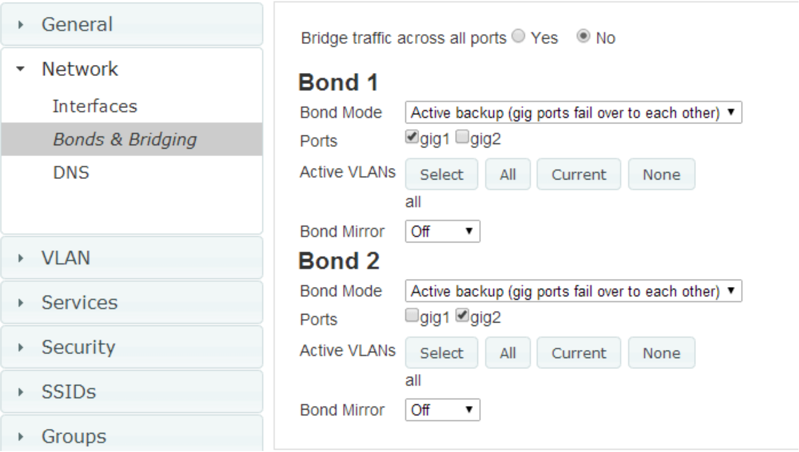
- **Open:** This option provides no authentication.
- **RADIUS MAC:** Uses an external RADIUS server to authenticate devices onto the wired network, based on the connecting device's MAC address. If you select this option, specify a primary and optional secondary RADIUS server. You may specify each server using a host name or IP address. Change the port if needed, and enter the shared secret needed to access each server.

3. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Bonds and Bridging

On models with more than one Gigabit port these ports may be bonded, i.e. configured to work together in sets. For example, one port may provide active backup or load balancing for another, or other options as described in this section.

A special option lets you configure bridging between the gigabit ports on an AP that has two of these ports.



Bridge traffic across all ports ○ Yes ● No

Bond 1

Bond Mode Active backup (gig ports fail over to each other)

Ports ☑gig1 □gig2

Active VLANs all

Bond Mirror Off

Bond 2

Bond Mode Active backup (gig ports fail over to each other)

Ports □gig1 ☑gig2

Active VLANs all

Bond Mirror Off

Figure 222. Network Bonds and Bridging

You may use the mirror option to have all the traffic that is ingressing and egressing one bond be transmitted by the bond you are configuring. For example, if you configure Bond2 to mirror Bond1, then all traffic going in and out of Bond1's Gigabit ports will be transmitted out of Bond2's Gigabit ports. This way of duplicating one bond's traffic to another bond is very useful for troubleshooting with a network analyzer.

If a set of Gigabit ports have been bonded, the IP address, IP mask, IP gateway, IP DHCP, and Management settings are shared between bonded ports. Any changes you make to these settings on one member will be reflected in the settings of the other members. Other settings may be configured individually.

Procedure for Configuring Network Bonds and Bridging

1. **Bridge traffic across all ports:** Click **Yes** for Layer 2 bridging between two Gigabit ports (Figure 223).

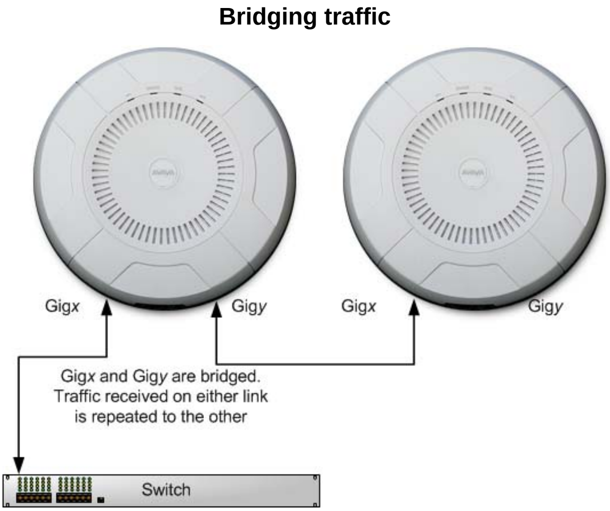


Figure 223. Bridging Traffic

This option is only available on APs that have exactly two Gigabit ports. Traffic received on Gig*x* is transmitted by Gig*y*; similarly, traffic received on Gig*y* is transmitted by Gig*x*. The AP acts as a wired bridge—this allows APs to be chained and still maintain wired connectivity.

Each AP in a chain must have power supplied to its PoE port from a compatible power injector or powered switch port. ***An AP does not supply power to another AP.***

When bridging is enabled, it configures the following bond settings for each bond and you will not be able to make any changes to bond settings.

- **Bond Mode is** set to **Active Backup** (the default value).
- Each port is in its own bond, by itself.

- **Bond Mirror** is **Off**. You will also need to enable use of Spanning Tree A message will appear that allows you to enable Spanning Tree.
- **Active VLANs** is set to **All**.

A bridge between ports **Gig1** and **Gig2** sets **Bond1** to contain only **Gig1**. **Bond2** contains only **Gig2**.

If you are bridging a chain of more than two APs, the endpoint AP is not actually bridging. It can be left with the default settings—**Bond1** is set to **Active Backup**, and will contain **Gig1** and **Gig2**.

Skip to Step 7 on page 386.

2. If you are not enabling bridging, configure the bonding behavior of the **Gigabit** network interfaces as described in the following steps. The fields for each of these bonds are the same.

3. **Bond Mode**: Select the desired behavior for a set of bonded Gigabit Ethernet ports from the following options.

   The modes below describe the relationship between a set of Gigabit ports—for example, load balancing or active backup. Use the **Ports** field to select the ports that are bonded (set in Step 4). Two or more ports may be bonded. You may also include just one single port in a bond—this is useful for mirroring one Gigabit port to another port (Step 6 on page 385). In APs that have four Gigabit ports, you have the option of bonding three or four ports together. In this discussion, we call two ports that are bonded **Gig*x*** and **Gig*y***.

   a. **Active Backup (gig ports fail over to each other)**—This mode provides fault tolerance and is the default mode. Gig*x* acts as the primary link. Gig*y* is the backup link and is passive. Gig*y* assumes the IP properties of Gig*x*. If Gig*x* fails, the AP automatically fails over to Gig*y*. When a failover occurs in this mode, Gig*y* issues gratuitous ARPs to allow it to substitute for Gig*x* at Layer 3 as well as Layer 2. See Figure 224 (a). You may include more than two ports in the bond with Active Backup to provide additional fault tolerance. For example, if you have three Gigabit ports configured in a bond, if the first two ports in the bond were to go down, the AP would fail over traffic to the third Gigabit port.

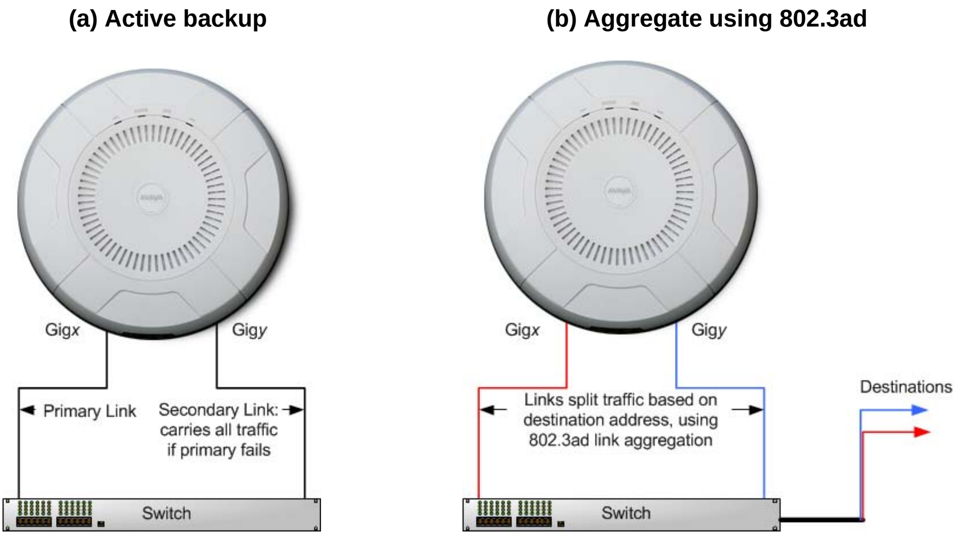

(a) Active backup
(b) Aggregate using 802.3ad
Gigx
Gigy
Primary Link
Secondary Link: carries all traffic if primary fails
Switch
Gigx
Gigy
Links split traffic based on destination address, using 802.3ad link aggregation
Destinations
Switch

Figure 224. Port Modes (a, b)

b. **Aggregate Traffic from gig ports using 802.3ad**—The AP sends network traffic across all member Gigabit ports to increase link speed to the network. These ports act as a single logical interface (trunk), using a load balancing algorithm to balance traffic across the ports. For non-IP traffic (such as ARP), the last byte of the destination MAC address is used to do the calculation. If the packet is a fragment or not TCP or UDP, the source and destination IP addresses are used to do the calculation. If the packet is TCP or UDP over IP then the source IP address, destination IP address, source port number and destination port number are all used to do the calculation. The network switch must also support 802.3ad. If a port fails, the trunk degrades gracefully—the other port still transmits. See Figure 224 (b).

c. **Transmit Traffic on all gig ports**—Transmits incoming traffic on all Gigabit ports. Any traffic received on Gigabit ports is sent to the onboard processor. This mode provides fault tolerance. See Figure 225 (c).

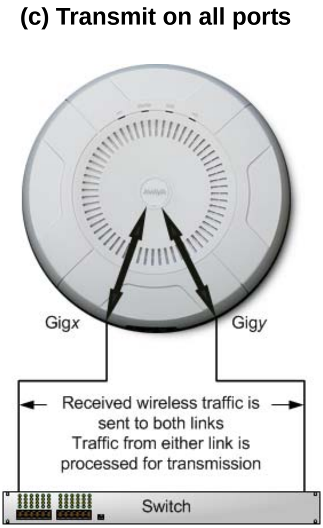

(c) Transmit on all ports
Gigx
Gigy
Received wireless traffic is sent to both links
Traffic from either link is processed for transmission
Switch

Figure 225. Port Modes (c)

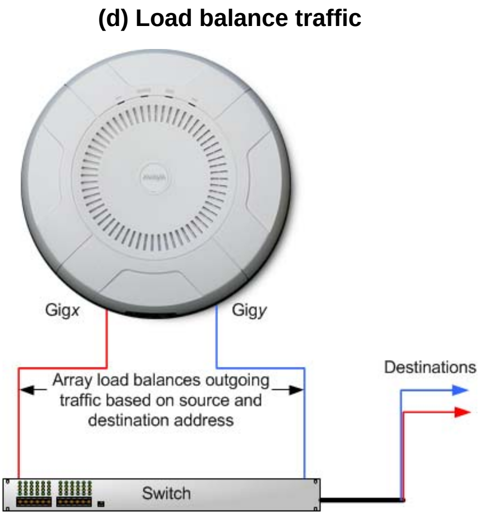

(d) Load balance traffic
Gigx
Gigy
Array load balances outgoing traffic based on source and destination address
Destinations
Switch

Figure 226. Port Modes (d)

d. **Load balance traffic between gig ports**—This option provides trunking, similar to option (b)—**Aggregate Traffic from gig1 & gig2 using 802.3ad**, but it does not use 802.3ad and it uses a different load balancing algorithm to determine the outgoing Gigabit port. The outgoing port used is based on an exclusive OR of the source and destination MAC address. Like option (b), this mode also provides load balancing and fault tolerance. See Figure 226 (d).

4. **Ports**: Select the ports to be members of this bond for the behavior specified by **Bond Mode**. By default, Bond1 contains Gig1 and Gig2. You may also set up a bond with a single port, for example, if you wish to mirror one Gigabit port to another. In APs that have four Gigabit ports, you also have the option of bonding three or four ports together.

   When you check off a port to be a member of a bond, that port is automatically removed from any other bonds that contain it.

5. **Active VLANs**: Create and manage the list of VLANs that are allowed to be passed through this port. Traffic will be dropped for VLANs that are not in this list. The default setting is to pass All VLANs.

a. To view or modify the list of allowed VLANs, click **Select**. The currently selected (i.e., active) VLANs are listed. Click the minus sign to remove a VLAN from the list, or the plus sign to add it. There are also links to **Remove all** or **Add al**l. A link near the bottom allows you to **Display by VLAN name** rather than by number.

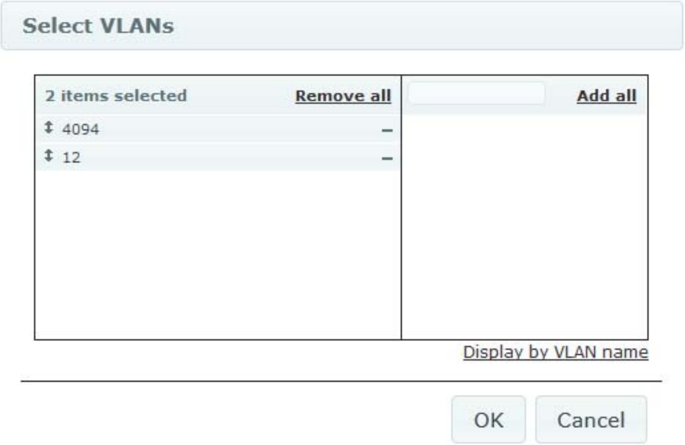


Figure 227. Select Active VLANs for this Bond

b. To allow all VLANs (current or future) to be passed, click the **All** button. To allow no VLANs (current or future) to be passed, click the **None** button.

c. To allow only the set of currently defined VLANs (see **“VLAN” on page 391**) to be passed, click the **Current** button. Essentially, this “fixes” the Active VLANs list to contain the AP’s currently defined VLANs, and only this set, until you make explicit changes to the Active VLANs list. If you create new VLANs, they will not be passed unless you take action to add them to the list.

6. **Bond Mirror**—Specify one of the active bonds (Bond*x*) that is to be mirrored by this bond (Bond*y*), or select **Off** to disable mirroring. (Figure 228) All wireless traffic received on the AP is transmitted out both Bond*x* and Bond*y*. All traffic received on Bond*x* is passed on to the

onboard processor as well as out Bond*y*. All traffic received on Bond*y* is passed on to the onboard processor as well as out Bond*x*. This allows a network analyzer to be plugged into Bond*y* to capture traffic for troubleshooting, while the bonded ports provide network connectivity for data traffic.

If each bond contains just one port, then you have the simple case of one port mirroring another.

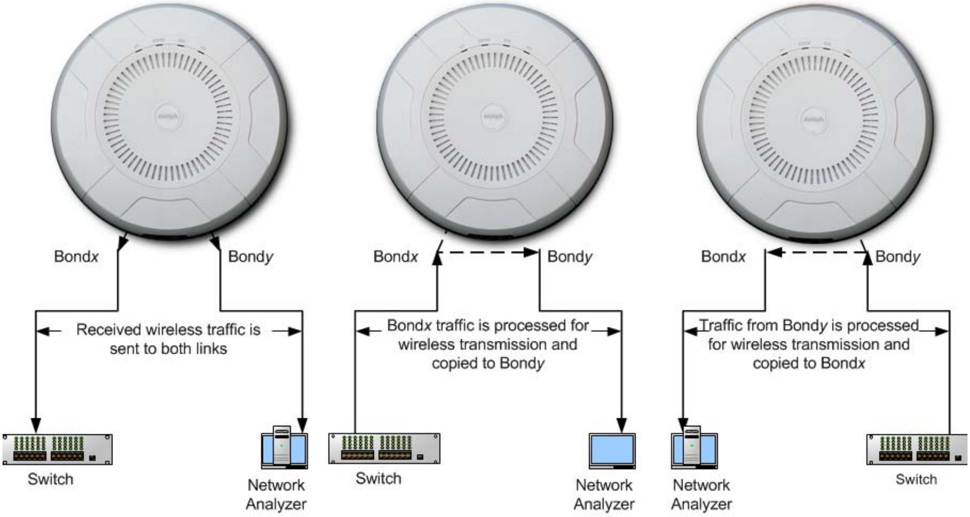

Bond*x*
Bond*y*
Received wireless traffic is sent to both links
Switch
Network Analyzer
Bond*x*
Bond*y*
Bond*x* traffic is processed for wireless transmission and copied to Bond*y*
Switch
Network Analyzer
Bond*x*
Bond*y*
Traffic from Bond*y* is processed for wireless transmission and copied to Bond*x*
Network Analyzer
Switch

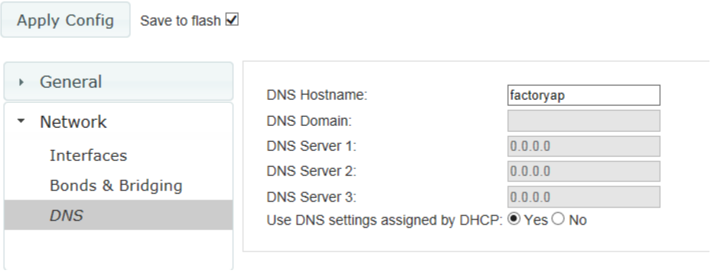
Figure 228. Mirroring Traffic

7. When done configuring bonds as desired, click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

DNS Settings

This window allows you to establish your DNS (Domain Name System) settings. The AP uses these DNS servers to resolve host names into IP addresses. The AP also registers its own Host Name with these DNS servers, so that others may address the AP using its name rather than its IP address. An option allows you to specify that the AP's DNS servers will be assigned via a DHCP server on the wired network.

Note that the DNS servers defined here are **not** used by wireless clients—servers for stations associated to the AP are defined along with DHCP pools. See **"DHCP Server" on page 408**. At least one DNS server must be set up if you want to offer clients associating with the AP the ability to use meaningful host names instead of numerical IP addresses.



DNS Hostname: factoryap
DNS Domain:
DNS Server 1: 0.0.0.0
DNS Server 2: 0.0.0.0
DNS Server 3: 0.0.0.0
Use DNS settings assigned by DHCP: ● Yes ○ No

Figure 229. DNS Settings

Procedure for Configuring DNS Servers

1. **DNS Host Name:** Enter a valid DNS host name.
2. **DNS Domain**: Enter the DNS domain name.
3. **DNS Server 1**: Enter the IP address of the primary DNS server.
4. **DNS Server 2** and **DNS Server 3**: Enter the IP address of the secondary and tertiary DNS servers (if required).

5. **Use DNS settings assigned by DHCP**: If you are using DHCP to assign the AP's IP address, click **Yes**. The AP will then obtain its DNS domain and server settings from the network DHCP server that assigns an IP address to the AP, rather than using the DNS Server fields above. You may also configure that DHCP server to assign a host name to the AP.

6. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Note that smaller APs that use the AOSLite system software, such as the WAP9112 and the WAP9114, have many fewer settings than more powerful APs. CDP is not supported. Settings that are not available on a particular AP are not displayed, or will be grayed out.

Fabric Attach (FA) or LLDP Settings

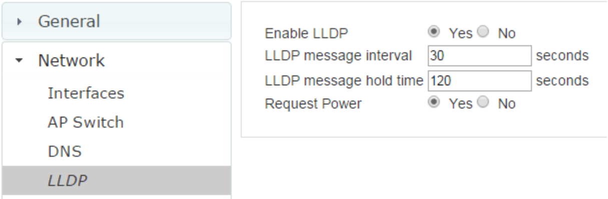
Link Layer Discovery Protocol (LLDP) is a Layer 2 network protocol used to share information (such as the device manufacturer and model, network capabilities, and IP address) with other directly connected network devices. APs can both advertise their presence by sending LLDP announcements, and gather and display information sent by neighbors. LLDP is used by Fabric Attach for discovery and communication.

There are two versions of this page:

- For AOSLite devices (WAP9112 and WAP9114) and AOSLite profiles, LLDP settings are displayed. See Procedure for Configuring LLDP Settings, below.
- For AOS APs, Fabric Attach settings are displayed. See Procedure for Configuring Fabric Attach Settings.

Procedure for Configuring LLDP Settings

This page controls LLDP settings for AOSLite devices. The Request Power feature allows you to ask for extra power for the WAP9112 so that it can power its PoE AP Switch port (LAN4).



Enable LLDP ● Yes ○ No
LLDP message interval 30 seconds
LLDP message hold time 120 seconds
Request Power ● Yes ○ No

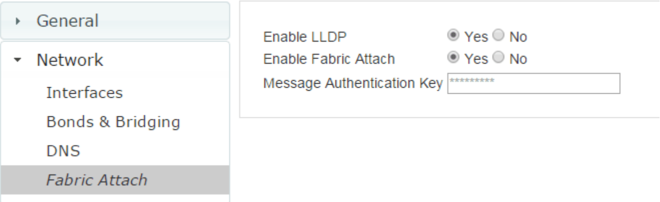
Figure 230. AOSLite LLDP Settings

1. **Enable LLDP:** When LLDP is enabled, the AP sends out LLDP announcements of the AP's presence, and gathers LLDP data sent by neighbors. When disabled, it does neither. LLDP is enabled by default.
2. **LLDP message interval**: The AP sends out LLDP announcements advertising its presence at this interval. The default is 30 seconds.
3. **LLDP message hold time**: LLDP information received from neighbors is retained for this period of time before aging out of the AP's neighbor list. Thus, if a neighbor stops sending announcements, it will no longer appear in an AP's LLDP List after LLDP Hold Time seconds from its last announcement. The default is 120 seconds.
4. **Request Power**: LLDP must be enabled before enabling this feature. If Request Power is set to **Yes** and LLDP discovers a device port that supplies power to this AP (on a powered switch, for example), the AP checks that the port is able to supply the peak power that is required by this AP model. The Request Power feature does this by requesting this peak power (in watts) from the PoE source, and it expects the PoE source to reply with the amount of power allocated. If the AP does not receive a response confirming that the power allocated by the PoE source is equal to or greater than the power requested, then the AP issues a Syslog message and keeps the radios down for ten minutes. The radios may be enabled manually after this.

   Using this feature provides a more graceful way of handling an underpowered situation on a Wi-Fi device. When the radios are turned off, WOS can notify you, rather than having to hunt down an intermittent problem. This feature is disabled by default.

Procedure for Configuring Fabric Attach Settings

This page controls Avaya Fabric Attach settings and LLDP settings for AOS devices.



Enable LLDP ● Yes ○ No
Enable Fabric Attach ● Yes ○ No
Message Authentication Key *********

Figure 231. Fabric Attach Settings

1. **Enable LLDP:** When LLDP is enabled, the AP sends out LLDP announcements of the AP's presence, and gathers LLDP data sent by neighbors. When disabled, it does neither. LLDP is enabled by default.
2. **Enable Fabric Attach**: Access Points support the Avaya Fabric Attach feature to simplify network deployment. Click **Yes** to enable the WAP as a Fabric Attach client device. This feature is enabled by default. Fabric Attach uses LLDP packets for communication, and requires LLDP to be enabled.
3. **Message Authentication Key**: This is the message authentication key used by Fabric Attach. This can be used to enter a key of length 1 to 32 octets.

VLAN

A Virtual LAN (VLAN) is comprised of a group of devices that communicate as a single network, even though they are physically located on different LAN segments. Because VLANs are based on logical rather than physical connections, they are extremely flexible. A device that is moved to another location can remain on the same VLAN without any hardware reconfiguration.

Understanding Virtual Tunnels

Avaya APs support Layer 2 tunneling with Virtual Tunnels. This allows an AP to use tunnels to transport traffic for one or more SSID-VLAN pairs onto a single destination network through the Layer 3 core network.

The AP has low overhead and latency for virtual tunnel connections, with high resilience. The AP performs all encryption and decryption in hardware, maintaining wire-rate encryption performance on the tunnel.

Virtual Tunnel Server (VTS)

Tunneling capability is provided by a Virtual Tunnel Server. You supply the server and deploy it in your network using open-source VTun software, available from vtun.sourceforge.net. To enable the AP to use tunneling for a VLAN, simply enter the IP address, port and secret for the tunnel server as described in Step 13 on page 395.

VTun may be configured for a number of different tunnel types, protocols, and encryption types. For use with APs, we recommend the following configuration choices:

- Tunnel Type: Ether (Ethernet tunnel)
- Protocol: UDP
- Encryption Type: select one of the encryption types supported by VTun (AES and Blowfish options are available)
- Keepalive: yes

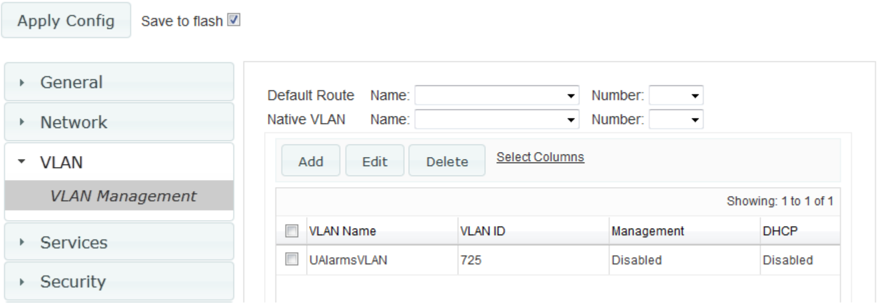
Client-Server Interaction

The AP is a client of the Virtual Tunnel Server. When you specify a VTS for an active VLAN-SSID pair, the AP contacts the VTS. The server then creates a tunnel session to the AP. VTun encapsulated packets will cross the Layer 3 network from the AP to the VTS. When packets arrive at the VTS, they will be de-encapsulated and the resultant packets will be passed to your switch with 802.1q VLAN tags for final Layer 2 processing. The process occurs in reverse for packets traveling in the other direction.

We recommend that you enable the VTun keep-alive option. This will send a keep-alive packet once per second to ensure that the tunnel remains active. Tunnels can be configured to come up on demand but this is a poor choice for wireless, since tunnel setup can take roughly 5-20 seconds and present a problem for authentication.

VLAN Management

This window allows you to assign and configure VLANs. After creating a new VLAN (added to the list of VLANs), you can modify the configuration parameters of an existing VLAN or delete a selected VLAN.



Default Route Name: Number:
Native VLAN Name: Number:

Showing: 1 to 1 of 1

□	VLAN Name	VLAN ID	Management	DHCP
□	UAlarmsVLAN	725	Disabled	Disabled

Figure 232. VLAN Management

The Wireless AP supports dynamic VLAN assignments specified by RADIUS policy settings. When RADIUS sends these assignments, the AP dynamically assigns wireless stations to VLANs as requested. VLAN tags on traffic are passed through the AP (i.e., VLAN tags are not stripped).

It is critical to configure all VLANs to be used on the AP, even those that will be dynamically assigned.

The maximum number of VLANs that you may create is determined by the limit for this AP. It depends on the type of AP, and the release version of Avaya OS that it is running.

Procedure for Managing VLANs

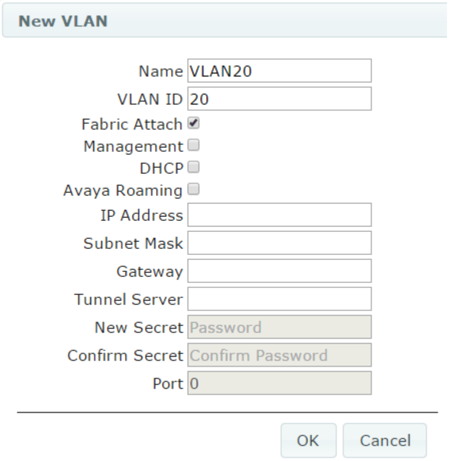
1. **Default Route:** This option sets a default route from the AP. The AP supports a default route on native and tagged interfaces. Once the default route is configured the AP will attempt to use Address Resolution Protocol (ARP) to find the default router. ARP finds the MAC address of a device with a given IP address by sending out a broadcast message requesting this information. This option allows you to choose a default VLAN route from the drop-down list. The IP Gateway must be established for this function to work. After changing the **Default Route**, you *must* check **Save to flash**, click **Apply Config**, *and then reboot*.

2. **Native VLAN**: This option sets whether the AP management is tagged or untagged. If you select a Native VLAN, then that VLAN will use an untagged (Native) link. Otherwise, the AP will use 802.1Q tagging and a specific VLAN ID with management enabled for management of the AP.

3. To **Edit** or **Delete** a VLAN, select it in the list and click the desired button.

To create a new VLAN:

4. Click the **Add** button and enter the following fields, as needed.



New VLAN

Name	VLAN20
VLAN ID	20
Fabric Attach	☑
Management	□
DHCP	□
Avaya Roaming	□
IP Address	
Subnet Mask	
Gateway	
Tunnel Server	
New Secret	Password
Confirm Secret	Confirm Password
Port	0

Figure 233. Creating a VLAN

5. **Name/VLAN ID**: Enter a name and number for the new VLAN (1-4094).

6. **Fabric Attach**: Check this box to allow this VLAN to participate in Fabric Attach. This feature is enabled by default, and should normally be used for VLANs.

   If Fabric Attach is in use on the network, it should only be disabled for a VLAN in special situations. For example, in order to support the Honeypot feature which requires a local VLAN to drop client traffic, you should disable Fabric Attach for the VLAN associated with the Honeypot SSID. This VLAN will be local to the AP and the service request for this VLAN should not be sent to the Fabric Attach switch. See also, **“High Density 2.4G Enhancement—Honeypot SSID” on page 448** and **“Fabric Attach (FA) or LLDP Settings” on page 388**.

7. **Management**: Check this box to allow management over this VLAN.

8. **DHCP**: Check this box if you want the DHCP server to assign the IP address, subnet mask and gateway address to the VLAN automatically, otherwise you must go to the next step and assign these parameters manually.

9. **Avaya Roaming**: Check this box to allow roaming over this VLAN.

10. **IP Address**: If the DHCP option is disabled, enter a valid IP address for this VLAN association.

11. **Subnet Mask**: If the DHCP option is disabled, enter the subnet mask IP address for this VLAN association.

12. **Gateway**: If the DHCP option is disabled, enter the IP gateway address for this VLAN association.

13. **Tunnel Server**: If this VLAN is to be tunneled, enter the IP address or host name of the tunnel server that will perform the tunneling. For more information on virtual tunnels, please see **"Understanding Virtual Tunnels" on page 391**.

14. **New Secret/Confirm Secret**: Enter the password expected by the tunnel server.

15. **Port**: If this VLAN is to be tunneled, enter the port number of the tunnel server.

16. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Services

Services on the AP include DHCP, SNMP, Syslog, Netflow, WiFi Tag, and Network Time Protocol (NTP) services.

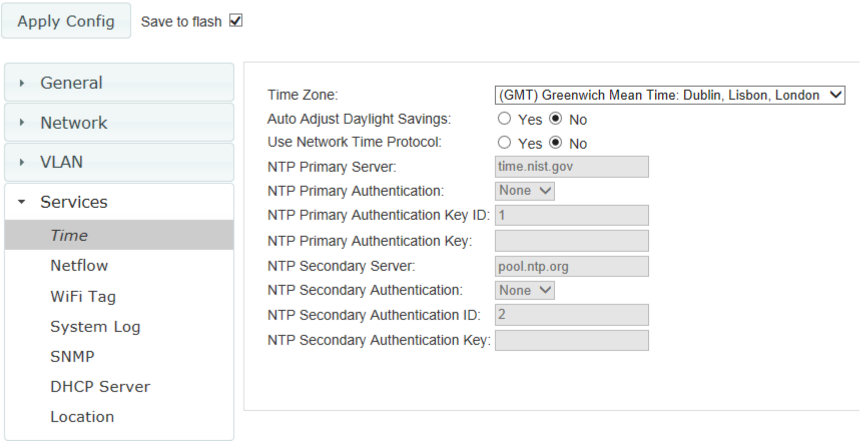
The following sections discuss configuring services on the AP:

- **"Time Settings (NTP)" on page 396**
- **"NetFlow" on page 398**
- **"Wi-Fi Tag" on page 399**
- **"System Log" on page 401**
- **"SNMP" on page 405**
- **"DHCP Server" on page 408**
- **"Location" on page 411**

Time Settings (NTP)

This window allows you to manage the AP's time settings, including synchronizing the AP's clock with a universal clock from an NTP server. We recommend that you use NTP for proper operation of SNMP in WOS, since a lack of synchronization will cause errors to be detected. Synchronizing the AP's clock with an NTP server also ensures that Syslog time-stamping is maintained across all units.

It is possible to use authentication with NTP to ensure that you are receiving synchronization from a known source. For example, the instructions for requesting a key for the NIST Authenticated NTP server are available at http://www.nist.gov/pml/div688/grp00/upload/ntp_instructions.pdf.
The AP allows you to enter optional authentication information.



Time Zone: (GMT) Greenwich Mean Time: Dublin, Lisbon, London
Auto Adjust Daylight Savings: ○ Yes ● No
Use Network Time Protocol: ○ Yes ● No
NTP Primary Server: time.nist.gov
NTP Primary Authentication: None
NTP Primary Authentication Key ID: 1
NTP Primary Authentication Key:
NTP Secondary Server: pool.ntp.org
NTP Secondary Authentication: None
NTP Secondary Authentication ID: 2
NTP Secondary Authentication Key:

Figure 234. Time Settings (Using NTP)

Procedure for Managing the Time Settings

1. **Time Zone:** Select the time zone you want to use (normally your local time zone) from the drop-down list.

2. **Auto Adjust Daylight Savings**: Check this box if you want the system to adjust for daylight savings automatically, otherwise leave this box unchecked (default).

3. **Use Network Time Protocol:** You must use NTP, since WOS works best when synced to a time server. APs managed by WOS should also use NTP.

4. **Using an NTP Server**

   a. **NTP Primary Server**: To use NTP, enter the IP address or domain name of the NTP server.

   b. **NTP Primary Authentication**: (optional) If you are using authentication with NTP, select the type of key: **MD5** or **SHA1**. Select **None** if you are not using authentication (this is the default).

   c. **NTP Primary Authentication Key ID**: Enter the key ID, which is a decimal integer.

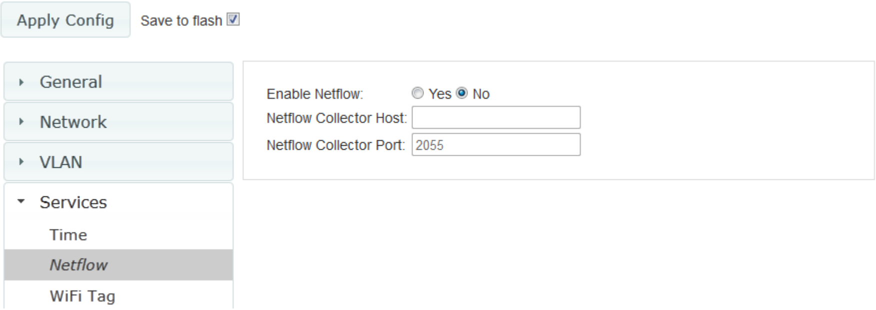
d. **NTP Primary Authentication Key**: Enter your key, which is a string of characters.

e. **NTP Secondary Server**: Enter the IP address or domain name of an optional secondary NTP server to be used in case the AP is unable to contact the primary server. You may use the authentication fields as described above if you wish to set up authentication for the secondary server.

NetFlow

This window allows you to enable or disable the sending of NetFlow information to a designated collector. When NetFlow is enabled, the AP will send IP flow information (traffic statistics) to the designated collector.

NetFlow sends per-flow network traffic information from the AP. Network managers can use a NetFlow collector to view the statistics on a per-flow basis and use this information to make key decisions. Knowing how many packets and bytes are sent to and from certain IP addresses or across specific network interfaces allows administrators to track usage by various areas. Traffic flow information may be used to engineer networks for better performance.



Enable Netflow: ○ Yes ● No

Netflow Collector Host:

Netflow Collector Port: 2055

Figure 235. NetFlow

Procedure for Configuring NetFlow

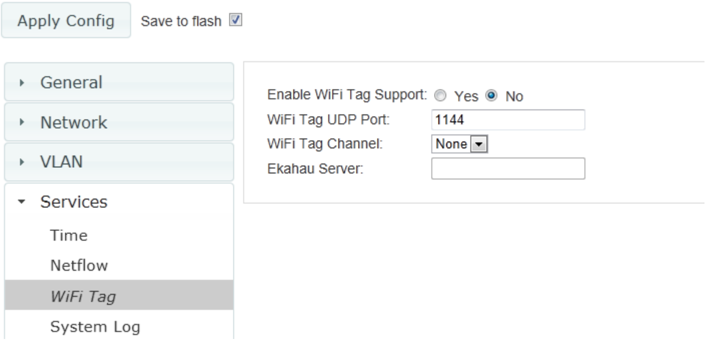
1. **Enable NetFlow:** Select one of the Netflow versions to enable NetFlow functionality: **v5**, **v9**, or **IPFIX**. Internet Protocol Flow Information Export (IPFIX) is an IETF protocol (www.ietf.org) performing many of the same functions as Netflow. Choose **Disable** if you wish to disable this feature. If you select IPFIX, 64 bit counters are supported starting with Avaya OS Release 7.1. IPFIX uses IF-MIB, whose ifXTables support 64 bit counters.

2. **NetFlow Collector Host (Domain or IP)**: If you enabled NetFlow, enter the domain name or IP address of the collector.

3. **NetFlow Collector Port**: If you enabled NetFlow, enter the port on the collector host to which to send data.

Wi-Fi Tag

This window allows you to enable or disable Wi-Fi tag capabilities. When enabled, the AP listens for and collects information about Wi-Fi RFID tags sent on the designated channel. These tags are transmitted by specialized tag devices (for example, AeroScout or Ekahau tags). A Wi-Fi tagging server then queries the AP for a report on the tags that it has received. The Wi-Fi tagging server uses proprietary algorithms to determine locations for devices sending tag signals.



Enable WiFi Tag Support: ○ Yes ● No

WiFi Tag UDP Port: 1144

WiFi Tag Channel: None

Ekahau Server:

Figure 236. Wi-Fi Tag

Procedure for Configuring Wi-Fi Tag

1. **Enable Wi-Fi Tag:** Choose **Yes** to enable Wi-Fi tag functionality, or choose **No** to disable this feature.

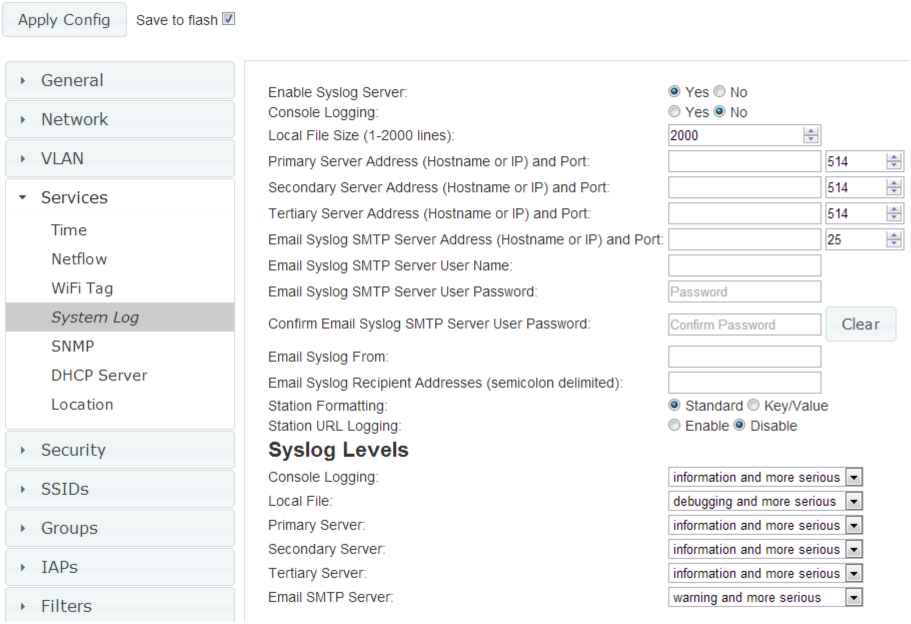
2. **Wi-Fi Tag UDP Port**: If you enabled Wi-Fi tagging, enter the port on the AP which the Wi-Fi tagging server will use to query the AP for tagging data. When queried, the AP will send back information on the tags it has observed. For each, the AP sends information such as the MAC address of the tag transmitting device, and the RSSI and noise floor observed.

3. **Wi-Fi Tag Channel**: If you enabled Wi-Fi tagging, enter the 802.11 channel on which the AP will listen for tags. The tag devices must be set up to transmit on this channel. Only one channel may be configured, and it must be an 802.11b/g channel in the range of Channel 1 to 11.

4. Ekahau Server: If you enabled Wi-Fi tagging and you are using an Ekahau server, enter its IP address or hostname. Ekahau Wi-Fi Tag packets received by the AP will be encapsulated as expected by Ekahau, and forwarded to the server.

System Log

This window allows you to enable or disable the Syslog server, define primary, secondary, and tertiary servers, set up email notification, and set the level for Syslog reporting for each of the servers and for email notification—the Syslog service will send Syslog messages that are at the selected severity or above to the defined Syslog servers and email address. An option allows you to use a Splunk application to analyze AP events.



Save to flash ☑

Enable Syslog Server:	● Yes ○ No
Console Logging:	○ Yes ● No
Local File Size (1-2000 lines):	2000
Primary Server Address (Hostname or IP) and Port:	514
Secondary Server Address (Hostname or IP) and Port:	514
Tertiary Server Address (Hostname or IP) and Port:	514
Email Syslog SMTP Server Address (Hostname or IP) and Port:	25
Email Syslog SMTP Server User Name:	
Email Syslog SMTP Server User Password:	Password
Confirm Email Syslog SMTP Server User Password:	Confirm Password
Email Syslog From:	
Email Syslog Recipient Addresses (semicolon delimited):	
Station Formatting:	● Standard ○ Key/Value
Station URL Logging:	○ Enable ● Disable

Syslog Levels

Console Logging:	information and more serious
Local File:	debugging and more serious
Primary Server:	information and more serious
Secondary Server:	information and more serious
Tertiary Server:	information and more serious
Email SMTP Server:	warning and more serious

Figure 237. System Log

Procedure for Configuring Syslog

1. **Enable Syslog Server:** Choose **Yes** to enable Syslog functionality, or choose **No** to disable this feature.

2. **Console Logging**: If you enabled Syslog, select whether or not to echo Syslog messages to the console as they occur. If you enable console logging, be sure to set the Console Logging level (see Step 9 below).

3. **Local File Size** (1-2000 lines): Enter a value in this field to define how many Syslog records are retained locally on the AP's internal Syslog file. The default is 2000.

4. **Primary Server Address (Hostname or IP) and Port**: If you enabled Syslog, enter the hostname or IP address of the primary Syslog server. You may also change the port used on the server if you do not wish to use 514, the default port.

5. **Secondary/Tertiary Server Address (Hostname or IP) and Port**: (Optional) If you enabled Syslog, you may enter the hostname or IP address of one or two additional Syslog servers to which messages will also be sent. You may also change the port used on each server if you do not wish to use 514, the default port. You may set one of the server addresses to the address of a server for Splunk.

6. **Email Notification**: (Optional) The following parameters allow you to send an email to a designated address each time a Syslog message is generated. The email will include the text of the Syslog message.

   a. **Email Syslog SMTP Server Address (Hostname or IP) and Port**: The hostname or the IP address of the SMTP server to be used for sending the email. Note that this specifies the mail server, **not** the email recipient. You may also change the port used on the server if you do not wish to use 25, the default SMTP port.

   b. **Email Syslog SMTP User Name**: Specify a user name for logging in to an account on the mail server designated in Step a.

   c. **Email Syslog SMTP User Password**: Specify a password for logging in to an account on the mail server designated in Step a.

   d. **Email Syslog SMTP From**: Specify the "From" email address to be displayed in the email.

   e. **Email Syslog SMTP Recipient Addresses**: Specify the entire email address of the recipient of the email notification. You may specify additional recipients by separating the email addresses with semicolons (;).

7. **Station Formatting**: If you are sending event information to a Splunk server, select **Key/Value** to send data in Splunk's expected format, otherwise leave this at the default value of **Standard**.

8. **Station URL Logging**: When enabled, Syslog messages are sent for each URL that each station visits. Only HTTP destinations (port 80) are logged; HTTPS destinations (port 443) are not logged. All URLs in a domain are logged, so for example, if an HTTP request to yahoo.com generates requests to 57 other URLs, all are logged. Furthermore, each visit to the same URL generates an additional log message. No deep packet inspection is performed by the URL logging, so no Application Control information is included in the Syslog message.

   The following information is included in the syslog message:

   - Date / Time
   - Source Device MAC and IP address
   - Destination Port
   - Destination Site address (e.g., 20.20.20.1)
   - The specific URL (e.g., http://20.20.20.1.24online/images/img2.jpg)

   Station URL Logging is disabled by default.

9. **Syslog Levels**: For each of the Syslog destinations, choose your preferred level of Syslog reporting from the drop-down list. Messages with criticality at the selected level and above will be shown. The default level varies depending on the destination.

   a. **Console Logging**: For messages to be echoed to the console, the default level is **Information and more serious**.

   b. **Local File**: For records to be stored on the AP's internal Syslog file, choose your preferred level of Syslog reporting from the drop-down list. The default level is **Debugging and more serious**.

   c. **Primary Server**: Choose the preferred level of Syslog reporting for the primary server. The default level is **Warning and more serious**. Note that sending too many messages to the server may degrade performance. WOS will warn you if you try to set this level lower.

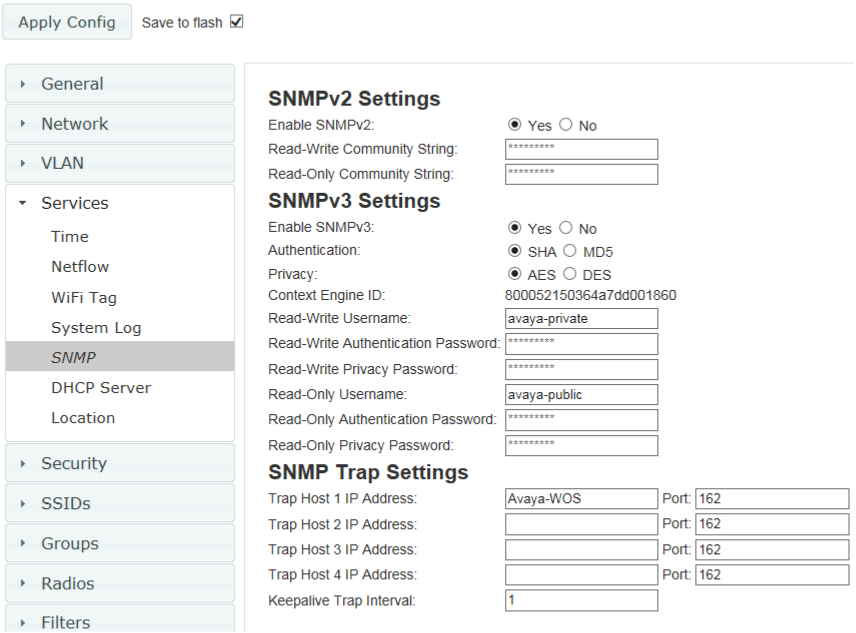
d. **Secondary/Tertiary Server**: Choose the preferred level of reporting for the secondary/tertiary server. The default level is **Warning and more serious**. (Optional) Note that sending too many messages to the server may degrade performance. WOS will warn you if you try to set this level lower.

e. **Email SMTP Server**: Choose the preferred level of Syslog reporting for the email notifications. The default level is **Warning and more serious**. This prevents your mailbox from being filled up with a large number of less severe messages such as informational messages.

10. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

SNMP

This window allows you to enable or disable SNMP v2 and SNMP v3 and define the SNMP parameters. SNMP allows remote management of the AP by the Wireless LAN Orchestration System (WOS) and other SNMP management tools. SNMP v3 was designed to offer much stronger security. You may enable either SNMP version, or both.



SNMPv2 Settings

Enable SNMPv2: ● Yes ○ No

Read-Write Community String: *********

Read-Only Community String: *********

SNMPv3 Settings

Enable SNMPv3: ● Yes ○ No

Authentication: ● SHA ○ MD5

Privacy: ● AES ○ DES

Context Engine ID: 800052150364a7dd001860

Read-Write Username: avaya-private

Read-Write Authentication Password: *********

Read-Write Privacy Password: *********

Read-Only Username: avaya-public

Read-Only Authentication Password: *********

Read-Only Privacy Password: *********

SNMP Trap Settings

Trap Host 1 IP Address: Avaya-WOS Port: 162

Trap Host 2 IP Address: Port: 162

Trap Host 3 IP Address: Port: 162

Trap Host 4 IP Address: Port: 162

Keepalive Trap Interval: 1

Figure 238. SNMP

For a summary of traps sent by the AP, see the section about traps in Appendix B of *Using the Avaya OS for Avaya WLAN AP 9100 Series*. ***NOTE:*** *If you are managing your APs with WOS, it is very important to make sure that your SNMP settings match those that you have configured for WOS. WOS uses both SNMP v2 and v3, with v3 given preference.*

Procedure for Configuring SNMP

SNMPv2 Settings

1. **Enable SNMPv2:** Choose **Yes** to enable SNMP v2 functionality, or choose No to disable this feature. When used in conjunction with the Wireless LAN Orchestration System, SNMP v2 (**not** SNMP v3) must be enabled on each AP to be managed with WOS. The default for this feature is Yes (enabled).

2. **Read-Write Community String**: Enter the read-write community string. The default is **private**.

3. **Read-Only Community String**: Enter the read-only community string. The default is **public**.

SNMPv3 Settings

4. **Enable SNMPv3**: Choose **Yes** to enable SNMP v3 functionality, or choose No to disable this feature. The default for this feature is Yes (enabled).

5. **Authentication**: Select the desired method for authenticating SNMPv3 packets: **SHA** (Secure Hash Algorithm) or **MD5** (Message Digest Algorithm 5).

6. **Privacy**: Select the desired method for encrypting data: **DES** (Data Encryption Standard) or the stronger **AES** (Advanced Encryption Standard).

7. **Context Engine ID**: The unique identifier for this SNMP server. This value may not be changed from this window. The Context Engine ID must be set if data collection is to be done via a proxy agent. This ID helps the proxy agent to identify the target agent from which data is to be collected.

8. **Read-Write Username**: Enter the read-write user name. This username and password allow configuration changes to be made on the AP. The default is **avaya-private**.

9. **Read-Write Authentication Password**: Enter the read-write password for authentication (i.e., logging in). The default is **avaya-private**.

10. **Read-Write Privacy Password**: Enter the read-write password for privacy (i.e., a key for encryption). The default is **avaya-private**.

11. **Read-Only Username**: Enter the read-only user name. This username and password do not allow configuration changes to be made on the AP. The default is **avaya-public**.

12. **Read-Only Authentication Password**: Enter the read-only password for authentication (i.e., logging in). The default is **avaya-public**.

13. **Read-Only Privacy Password**: Enter the read-only password for privacy (i.e., a key for encryption). The default is **avaya-public**.

SNMP Trap Settings

14. **Trap Host IP Address**: Enter the **IP Address** or hostname, as well as the **Port** number, of an SNMP management station that is to receive SNMP traps. You may specify up to four hosts that are to receive traps. Note that by default, **Trap Host 1** sends traps to **Avaya-WOS**. Thus, the AP will automatically communicate its presence to WOS (as long as the network is configured correctly to allow this host name to be resolved—note that DNS is not normally case-sensitive).

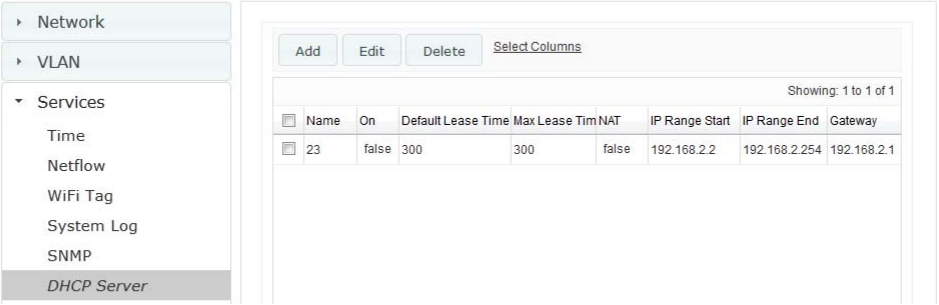
15. **Keepalive Trap Interval** (minutes): Traps are sent out at this interval to indicate the presence of the AP on the network. Keepalive traps are required for proper operation with WOS. To disable keepalive traps, set the value to **0**.

16. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

DHCP Server

This window allows you to create, enable, modify and delete DHCP (Dynamic Host Configuration Protocol) address pools. DHCP allows the AP to provide wireless clients with IP addresses and other networking information. The DHCP server will not provide DHCP services to the wired side of the network. If you do not use the DHCP server on the AP, then your wired network must be configured to supply DHCP addresses and gateway and DNS server addresses to wireless clients.

When you create a DHCP pool, you must define the DHCP lease time (default and maximum), the IP address ranges (pools) that the DHCP server can assign, and the gateway address and DNS servers to be used by clients.



Showing: 1 to 1 of 1

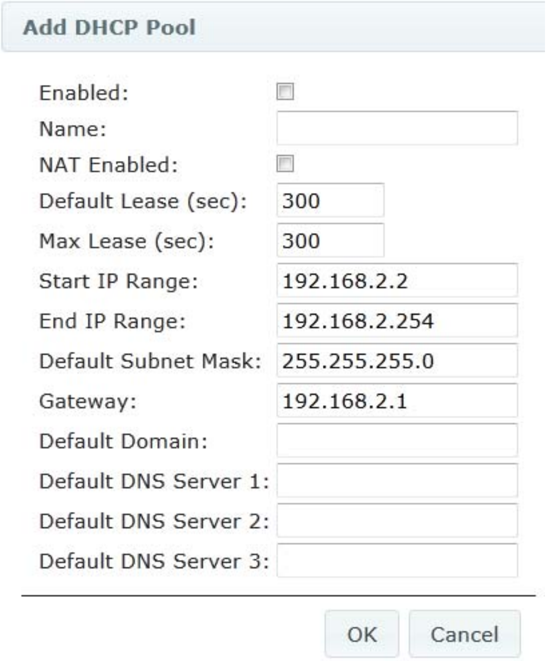
☐	Name	On	Default Lease Time	Max Lease Tim	NAT	IP Range Start	IP Range End	Gateway
☐	23	false	300	300	false	192.168.2.2	192.168.2.254	192.168.2.1

Figure 239. DHCP Management

DHCP usage is determined in several windows—see SSID Management, Group Management, and VLAN Management.

Procedure for Configuring the DHCP Server

1. Click the **Add** button to create a new DHCP pool.
2. **Enabled**: Click this checkbox to make this pool of addresses available, or clear it to disable the pool.
3. **Name**: Enter a name for the new DHCP pool. The new pool ID is added to the list of available DHCP pools.



Add DHCP Pool

Enabled:	□
Name:	
NAT Enabled:	□
Default Lease (sec):	300
Max Lease (sec):	300
Start IP Range:	192.168.2.2
End IP Range:	192.168.2.254
Default Subnet Mask:	255.255.255.0
Gateway:	192.168.2.1
Default Domain:	
Default DNS Server 1:	
Default DNS Server 2:	
Default DNS Server 3:	

Figure 240. Adding a DHCP Pool

4. **NAT Enabled** (Network Address Translation): Check this box to enable the Network Address Translation feature.

5. **Default Lease (sec)**: This field defines the default DHCP Lease time (in seconds). The factory default is 300 seconds, but you can change the default at any time.

6. **Max Lease**: Enter a value (in seconds) to define the maximum allowable DHCP lease time. The default is 300 seconds.

7. **Start IP Range**: Enter an IP address to define the start of the IP range that will be used by the DHCP server. The default is 192.168.2.2.

8. **End IP Range**: Enter an IP address to define the end of the IP range that will be used by the DHCP server. The DHCP server will only use IP addresses that fall between the start and end range that you define on this page. The default is 192.168.2.254.

9. **Default Subnet Mask**: Enter the subnet mask for this IP range for the DHCP server. The default is 255.255.255.0.

10. **Gateway**: If necessary, enter the IP address of the gateway.

11. **Default Domain**: Enter the DNS domain name. See **"DNS Settings" on page 387**.

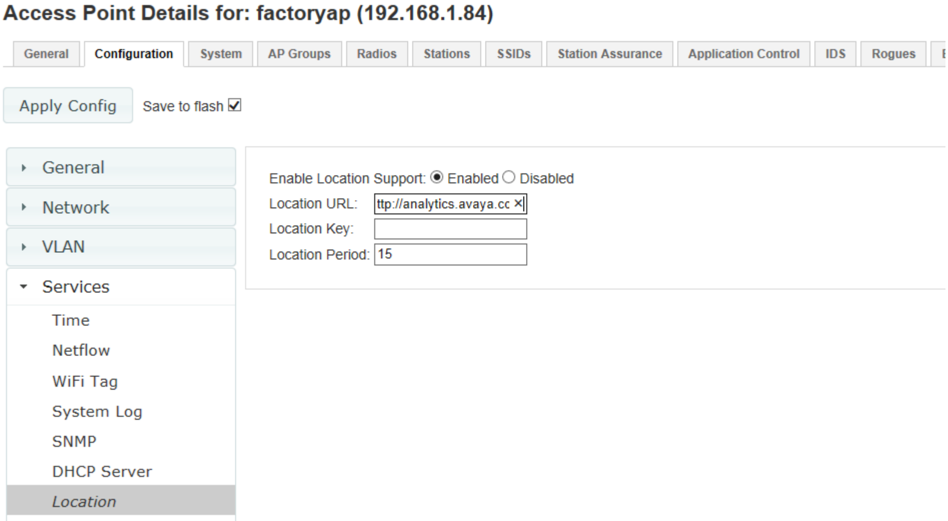
12. **Default DNS Servers** (**1** to **3**): Enter the IP address of the primary DNS server, secondary DNS server and tertiary DNS server. These DNS server addresses will be passed to stations when they associate, along with the assigned IP address. Note that if you leave these blank, no DNS information is sent to the stations. DHCP will **not** default to sending the DNS servers that are configured in DNS Settings. See also, **"DNS Settings" on page 387**.

13. Click **OK** to add this entry to the list.

14. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Location

Avaya APs offer an integrated capability for capturing and uploading visitor location data, eliminating the need to install a standalone sensor network. This data can be used to characterize information such as guest or customer traffic and location, visit duration, and frequency. Use this Location window to configure the AP to send collected data to a location analytics server, such as Euclid. Note that APs that run AOSLite do not provide location data.



Enable Location Support: ● Enabled ○ Disabled
Location URL: ttp://analytics.avaya.cc
Location Key:
Location Period: 15

Figure 241. Location

When Location Support is enabled, the AP collects information about stations, including the station ID and manufacturer, time and length of the visit and related time interval statistics, and signal strength and its related statistics. Data collected from stations comprises only basic device information that is broadcast by Wi-Fi enabled devices. Devices that are only detected are included, as well as those that actually connect to the AP. Multiple data points may be sent for a station—for Access Points running Avaya OS Release 7.1 or later, data is sent for each radio that sees a probe request from the station. The AP sending the data also sends its own ID so that the server knows where the visitors were detected. All data messages are encrypted, and they are uploaded via HTTPS. The message format used is described in **"Location Service Data Formats" on page 619**.

Procedure for Configuring Location

1. **Enable Location Support:** Choose **Enabled** to enable the collection and upload of visitor analytic data, or choose **Disabled** to disable this feature.

2. **Location URL**: If Location Support is enabled, enter the URL of the location/analytics server. If this URL contains the string **euclid**, then the AP knows that data is destined for a Euclid location server.

   For a Euclid analytics server, use the URL that was assigned to you as a customer by Euclid. The AP will send JSON-formatted messages in the form required by Euclid via HTTPS.

   For any other location analytics server, enter its URL. The AP will send JSON-formatted messages in the form described in **"Location Service Data Formats" on page 619**.

3. **Location Key**: Enter your customer ID for the location/analytics server.

4. **Location Period**: If you enabled Location Support, specify how often data is to be sent to the server, in seconds.

5. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Security

AP security settings include administration accounts, Access Control List (ACL), management settings, encryption and authentication protocol settings, and RADIUS configuration settings. For additional information about wireless network security, refer to **"Understanding Security" on page 414**.

For information about secure use of the WMI on the AP, refer to:

- **"About Creating Admin Accounts on the RADIUS Server" on page 420**
- **"About Creating User Accounts on the RADIUS Server" on page 434**

The security setting windows that are available are different for APs that run AOSLite (WAP9112 and WAP9114) and those that run AOS.

Security Settings for AOS Devices and Profiles

Security settings are configured with the following windows on all WOS versions:

- **"Admin Management" on page 417**
- **"Admin Privileges" on page 418**
- **"Admin RADIUS" on page 420**
- **"Management Control" on page 423**

Security settings are configured with the following windows on all WOS versions:

- **"Global Settings" on page 428**
- **"Access Control List" on page 431**
- **"External Radius" on page 433**
- **"Internal Radius" on page 439**
- **"Airwatch" on page 441**

Security Settings for AOSLite Devices and Profiles

- **"Admin Management" on page 417** (Only available in profiles)
- **"Global Settings" on page 428**
- **"Radius (for AOSLite Only)" on page 438**

Understanding Security

The Avaya Wireless AP incorporates many configurable security features. After initially installing an AP, always change the default administrator password (the default is admin), and choose a strong replacement password (containing letters, numbers and special characters). When appropriate, issue read-only administrator accounts.

Other security considerations include:

- **SSH versus Telnet**: Be aware that Telnet is not secure over network connections and should be used only with a direct serial port connection. When connecting to the unit’s Command Line Interface over a network connection, you must use a Secure SHell version 2 (SSH-2) utility. SSH-2 provides stronger security than SSH-1. The most commonly used freeware providing SSH tools is PuTTY.
- **Configuration auditing**: The optional WOS offers powerful management features for small or large Avaya wireless deployments, and can audit your configuration settings automatically. In addition, using the WOS eliminates the need for an FTP server.
- **Choosing an encryption method**: Wireless data encryption prevents eavesdropping on data being transmitted or received over the airwaves. The AP allows you to establish the following data encryption configuration options:
    - **Open**—this option offers no data encryption and is not recommended, though you might choose this option if clients are required to use a VPN connection through a secure SSH utility, like PuTTy.
    - **Wired Equivalent Privacy (WEP)**—this option provides minimal protection (though much better than using an open network). An early standard for wireless data encryption and supported by all Wi-Fi certified equipment, WEP is vulnerable to hacking and is therefore not recommended for use by Enterprise networks.
    - **Wi-Fi Protected Access) (WPA) and WPA2**—these are much stronger encryption modes than WEP, using TKIP (Temporal Key

Integrity Protocol) or AES (Advanced Encryption Standard) to encrypt data.

WPA solves security issues with WEP. It also allows you to establish encryption keys on a per-user-basis, with key rotation for added security. In addition, TKIP provides Message Integrity Check (MIC) functionality and prevents active attacks on the wireless network.

AES is the strongest encryption standard and is used by government agencies; however, old legacy hardware may not be capable of supporting the AES mode (it probably won't work on older wireless clients). Because AES is the strongest encryption standard currently available, WPA2 with AES is highly recommended for Enterprise networks.

Any of the above encryption methods can be used and an AP can support multiple encryption methods simultaneously, but only one method may be selected per SSID (except that selecting **WPA-Both** allows WPA and WPA2 to be used at the same time on the same SSID). Otherwise, if multiple security methods are needed, you must define multiple SSIDs.

The encryption mode (WEP, WPA, etc.) is selected in the **SSIDs >SSID Management** window (see **"SSID Management" on page 454**). The encryption standard used with WPA or WPA2 (AES or TKIP) is selected in the **Security>Global Settings** window under **WPA Settings** (see **"Global Settings" on page 428**).

- **Choosing an authentication method**: User authentication ensures that users are who they say they are. For this purpose, the AP allows you to choose between the following user authentication methods:
    - **Pre-Shared Key**—users must manually enter a key (passphrase) on the client side of the wireless network that matches the key stored by the administrator in the AP.

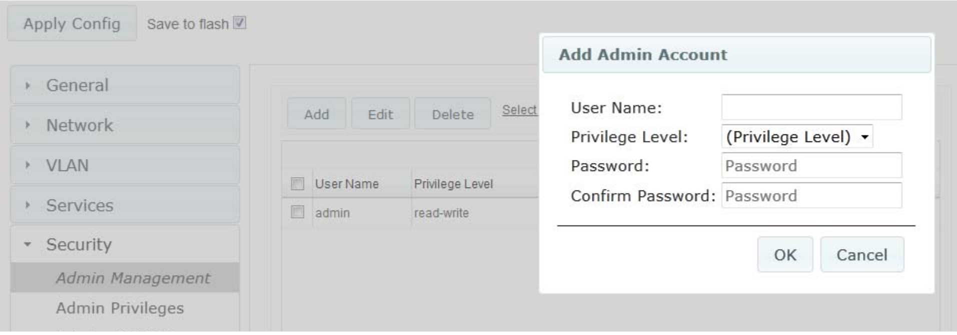
      This method should be used only for smaller networks when a RADIUS server is unavailable. If PSK must be used, choose a strong passphrase containing between 8 and 63 characters (20 is preferred). Always use a combination of letters, numbers and special characters. Never use English words separated by spaces.

- **RADIUS 802.1x with EAP**—802.1x uses a RADIUS server to authenticate large numbers of clients, and can handle different Extensible Authentication Protocol (EAP) authentication methods, including EAP-TLS, EAP-TTLS, EAP-PEAP, and LEAP-Passthrough. The RADIUS server can be internal (provided by the wireless AP) or external. An external RADIUS server offers more functionality and security, and is recommended for large deployments. When using this method, user names and passwords must be entered into the RADIUS server for user authentication.
- **MAC Address ACLs**—MAC address ACLs provide a list of client adapter MAC addresses that are allowed or denied access to the wireless network. Access Control Lists work well when there are a limited number of users—in this case, enter the MAC address of each user in the Allow list. In the event of a lost or stolen MAC adapter, enter the affected MAC address in the Deny list.

  The wireless AP will accept up to 1,000 ACL entries.

Admin Management

This window allows you to manage network administrator accounts (create, modify and delete). It also allows you to limit account access to a read only status.



□	User Name	Privilege Level
□	admin	read-write

User Name:

Privilege Level: (Privilege Level)

Password: Password

Confirm Password: Password

Figure 242. Admin Management

Procedure for Creating or Modifying Network Administrator Accounts

1. To create a new account, click the **Add** button and enter the **User Name** for a new network administrator ID. The length of the ID must be between 5 and 50 characters, inclusive.

2. **Privilege Level**: Choose **read-write** if you want to give this administrator ID full read/write privileges, or choose **read-only** to restrict this user to read only status. In the read only mode, administrators cannot save changes to configurations. Or you may select one of your custom-defined privilege levels (see **“Admin Privileges” on page 418**).

3. **Password**: Enter a password for this ID. The length of the password must be between 5 and 50 characters, inclusive.

4. **Confirm Password**: Re-enter the password in this field to verify that you typed the password correctly. If you do not re-enter the correct password, an error message is displayed.

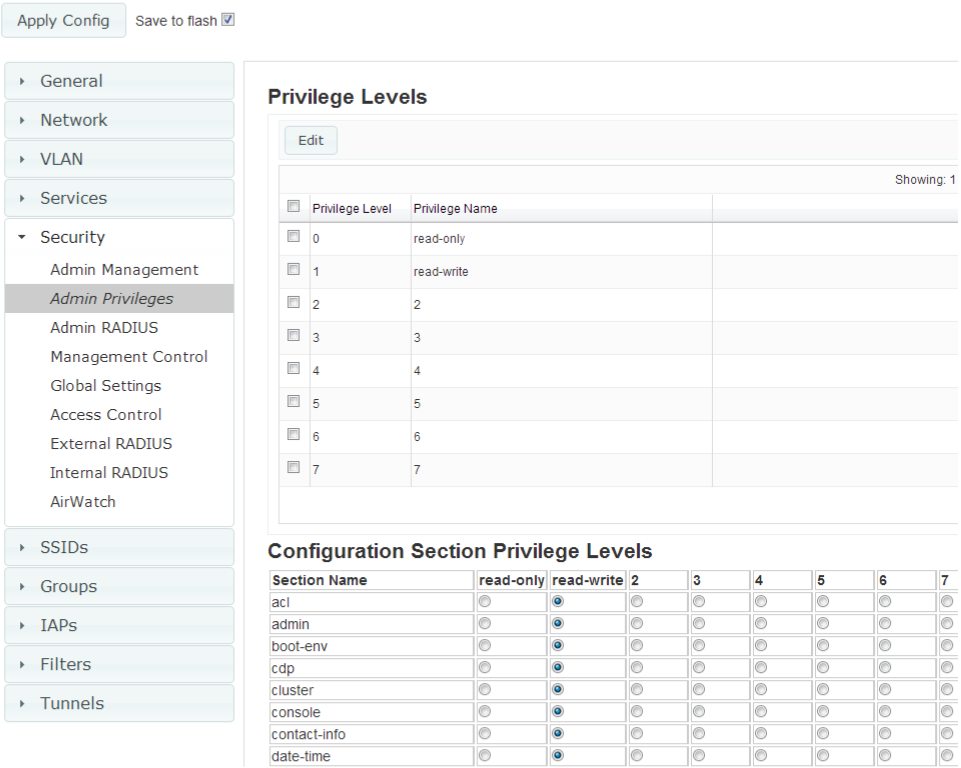
5. Click **OK** to add this administrator ID to the list.

6. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Admin Privileges

This window provides a detailed level of control over the privileges of AP administrators. Administrators may be assigned one of eight **Privilege Levels**. You may define the privilege level of each major feature (**Configuration Section**) that may be configured on the AP. For example, say that you set the privilege level to 4 for Reboot AP, Security, Radius Server, and SNMP, and you leave all other configuration sections at the default privilege level of 1. In this case, any administrator with a privilege level of 4 or higher may perform any operation on the AP, while an administrator with a privilege level lower than 4 but at least 1 may perform any operation except those whose level was set to 4. An error message will be displayed if an operation is attempted without a sufficient privilege level.

Privilege level 0 is **read-only**. As a minimum, all administrators have permission for read access to all areas of AP configuration. Higher privilege levels may be used to define additional privileges for specific configuration sections.



Save to flash ☑

Privilege Levels

□	Privilege Level	Privilege Name
□	0	read-only
□	1	read-write
□	2	2
□	3	3
□	4	4
□	5	5
□	6	6
□	7	7

Configuration Section Privilege Levels

Section Name	read-only	read-write	2	3	4	5	6	7
acl	○	●	○	○	○	○	○	○
admin	○	●	○	○	○	○	○	○
boot-env	○	●	○	○	○	○	○	○
cdp	○	●	○	○	○	○	○	○
cluster	○	●	○	○	○	○	○	○
console	○	●	○	○	○	○	○	○
contact-info	○	●	○	○	○	○	○	○
date-time	○	●	○	○	○	○	○	○

Figure 243. Admin Privileges

Procedure for Configuring Admin Privileges

1. **Privilege Levels** (optional): You may assign a **Name** to a Privilege Level by selecting it and clicking the **Edit** button. The name may be used to describe the access granted by this level. By default, levels **0** and **1** are named **read-only** and **read-write**, respectively, and levels **2** through **7** have the same name as their level number.

2. **Configuration Section Privilege Levels**: Use this section to assign a **Privilege Level** to **Section Names** as desired. By default, all sections are assigned level 1. When you select a higher privilege level for a

configuration section, then only administrators who have at least that privilege level will be able to make configuration changes to that section.

3. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Admin RADIUS

This window allows you to set up authentication of network administrators via RADIUS. Using RADIUS to control administrator accounts for logging in to APs has these benefits:

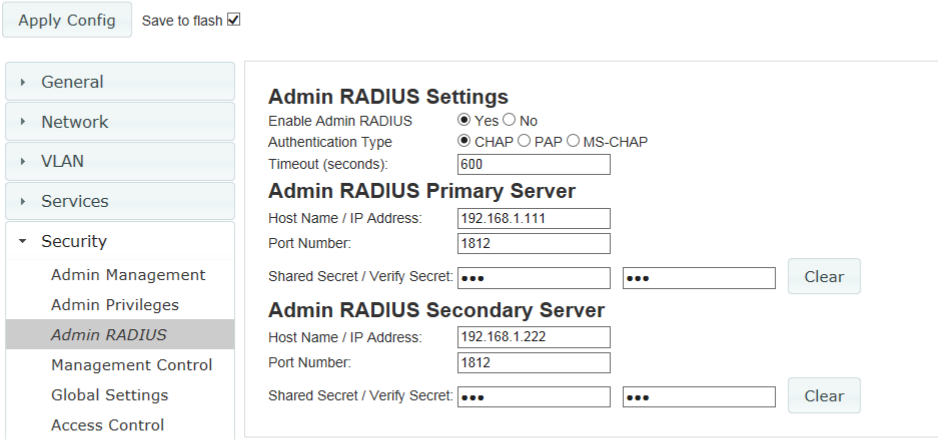
- Centralized control of administrator accounts.
- Less effort—you don't have to set up user names and passwords on each AP; just enter them once on the RADIUS server and then all of the APs can pull from the RADIUS server.
- Enforced policies—you may set password rules (e.g., passwords must contain at least one number and be at least 12 characters in length), and you may set expiration times for passwords.

Admin RADIUS settings override any local administrator accounts configured on the Admin Management window. If you have Admin RADIUS enabled, all administrator authentication is done via the configured RADIUS servers. The only exception to this is when you are connected via the Console port (using CLI). If you are using the Console port, the AP will authenticate administrators using accounts configured on the Admin Management window first, and then use the RADIUS servers. This provides a safety net to ensure that you are not completely locked out of an AP if the RADIUS server is down.

About Creating Admin Accounts on the RADIUS Server

Permissions for RADIUS administrator accounts are controlled by the RADIUS **Avaya-Admin-Role** attribute. This is a Vendor Specific Attribute (VSA). To define the privileges permitted to an administrator account, set the value of its Avaya-Admin-Role attribute to the desired **Privilege Level Name** string, as defined in **“Admin Privileges” on page 418**. For more information about the RADIUS VSAs used by Avaya, see "RADIUS Vendor Specific Attribute (VSA) for Avaya" in the Technical Support Appendix of the *Avaya WLAN AP 9100 Series (NN47252-102)*.

When configuring administrator accounts on the RADIUS server, you must observe the same restrictions for length and legal characters as when creating these accounts on the AP using the Admin Management window: the user name and password must be between 5 and 50 characters, inclusive.



Admin RADIUS Settings

Enable Admin RADIUS ● Yes ○ No

Authentication Type ● CHAP ○ PAP ○ MS-CHAP

Timeout (seconds): 600

Admin RADIUS Primary Server

Host Name / IP Address: 192.168.1.111

Port Number: 1812

Shared Secret / Verify Secret: ••• •••

Admin RADIUS Secondary Server

Host Name / IP Address: 192.168.1.222

Port Number: 1812

Shared Secret / Verify Secret: ••• •••

Figure 244. Admin RADIUS

Procedure for Configuring Admin RADIUS

Use this window to enable/disable administrator authentication via RADIUS, and to set up primary and secondary servers to use for authentication of administrators attempting to log in to the AP.

1. **Admin RADIUS Settings:**

   a. **Enable Admin RADIUS**: Click **Yes** to enable the use of RADIUS to authenticate administrators logging in to the AP. You will need to specify the RADIUS server(s) to be used.

   b. **Authentication Type**: Select the protocol used for authentication of administrators, **CHAP** or **PAP** (the default).

- **Password Authentication Protocol (PAP)**, is a simple protocol. PAP transmits ASCII passwords over the network "in the clear" (unencrypted) and is therefore considered insecure.
- **Challenge-Handshake Authentication Protocol (CHAP)** is a more secure protocol. The login request is sent using a one-way hash function.
- **Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP)**

c. **Timeout (seconds)**: Define the maximum idle time (in seconds) before the RADIUS server's session times out. The default is 600 seconds.

2. **Admin RADIUS Primary Server**: This is the RADIUS server that you intend to use as your primary server.

a. **Host Name / IP Address**: Enter the IP address or domain name of this external RADIUS server.

b. **Port Number**: Enter the port number of this RADIUS server. The default is 1812.

c. **Shared Secret / Verify Secret**: Enter the shared secret that this RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.

The shared secret that you define must match the secret used by the RADIUS server.

3. **Admin RADIUS Secondary Server** (optional): If desired, enter an alternative external RADIUS server. If the primary RADIUS server becomes unreachable, the AP will "failover" to the secondary RADIUS server (defined here).

a. **Host Name / IP Address**: Enter the IP address or domain name of this RADIUS server.

b. **Port Number**: Enter the port number of this RADIUS server. The default is 1812.

c. **Shared Secret / Verify Secret**: Enter the shared secret that this RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.

Management Control

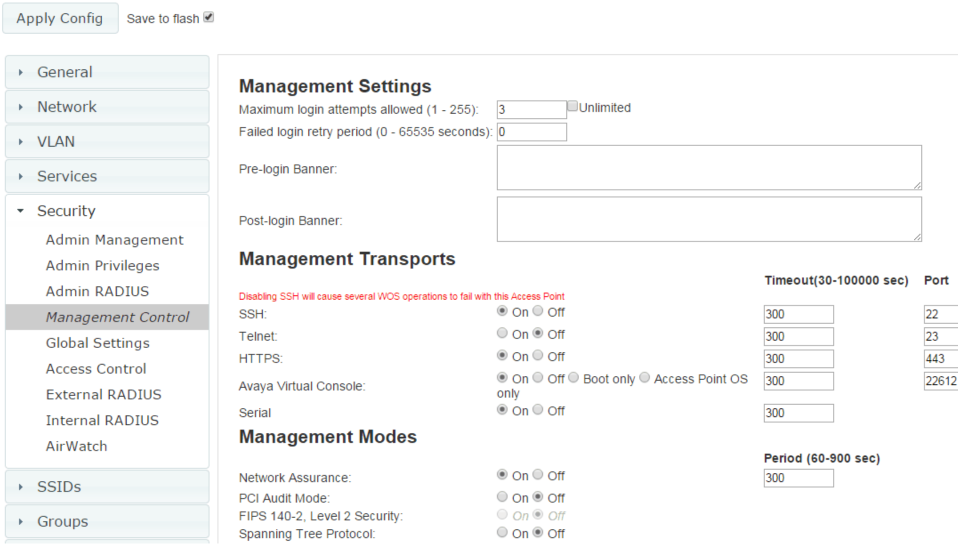
This window allows you to enable or disable the AP management interfaces and set their inactivity time-outs. The supported range is 300 (default) to 100,000 seconds. (Figure 245)

Procedure for Configuring Management Control

1. **Management Settings:**

   a. **Maximum login attempts allowed (1-255)**: After this number of consecutive failing administrator login attempts via ssh or telnet, the **Failed login retry period** is enforced. The default is 3.

   b. **Failed login retry period (0-65535 seconds)**: After the maximum number (defined above) of consecutive failing administrator login attempts via ssh or telnet, the administrator's IP address is denied access to the AP for the specified period of time (in seconds). The default is 0.



Management Settings

Maximum login attempts allowed (1 - 255): 3 □ Unlimited

Failed login retry period (0 - 65535 seconds): 0

Pre-login Banner:

Post-login Banner:

Management Transports

Disabling SSH will cause several WOS operations to fail with this Access Point

		Timeout(30-100000 sec)	Port
SSH:	● On ○ Off	300	22
Telnet:	○ On ● Off	300	23
HTTPS:	● On ○ Off	300	443
Avaya Virtual Console:	● On ○ Off ○ Boot only ○ Access Point OS only	300	22612
Serial	● On ○ Off	300	

Management Modes

		Period (60-900 sec)
Network Assurance:	● On ○ Off	300
PCI Audit Mode:	○ On ● Off	
FIPS 140-2, Level 2 Security:	○ On ● Off	
Spanning Tree Protocol:	○ On ● Off	

Figure 245. Management Control

c. **Pre-login Banner**: Text that you enter here will be displayed above the WMI login prompt.

d. **Post-login Banner**: Text that you enter here will be displayed in a message box after a user logs in to the WMI.

2. **SSH**

a. **On/Off**: Choose **On** to enable management of the AP over a Secure Shell (SSH-2) connection, or **Off** to disable this feature. Be aware that only SSH-2 connections are supported by the AP. SSH clients used for connecting to the AP must be configured to use SSH-2.

b. **Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your SSH connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.

   c. **Port**: Enter a value in this field to define the port used by SSH. The default port is 22.

3. **Telnet:**

   a. **On/Off**: Choose **On** to enable AP management over a Telnet connection, or **Off** to disable this feature. SSH offers a more secure connection than Telnet, and is recommended over Telnet.

   b. **Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your Telnet connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.

   c. **Port**: Enter a value in this field to define the port used by Telnet. The default port is 23.

4. **HTTPS**

   a. **Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your HTTPS connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds. Management via HTTPS (i.e., the Windows Management Interface) cannot be disabled on this window. To disable management over HTTPS, you must use the Command Line Interface.

   b. **Port**: Enter a value in this field to define the port used by SSH. The default port is 443.

5. **Avaya virtual console**

   The Avaya virtual console utility connects to APs that are not reachable via the normal access methods (such as SSH or WMI) and that do not have a physical console port, or whose console port is not accessible. You can enable or disable Avaya virtual console access to the AP as instructed below.

! ***Warning**: If you disable Avaya virtual console access completely on models with no console port, you **must** ensure that you do not lose track of the username and password to log in to CLI/WMI! There is no way to recover from a lost password, other than returning the AP to Avaya.*

a. **On/Off**: Choose **On** to enable Avaya virtual console access to the AP at the Avaya OS (CLI) and Avaya Boot Loader (boot loader) levels, or **Off** to disable access at both levels. On models that have no console port, Avaya virtual console access is **On** by default. On all other AP models, Avaya virtual console access is **Off** by default.

b. **Avaya OS only**: Choose this radio button to enable Avaya virtual console access at the Avaya OS level only (i.e., Avaya virtual console can access CLI only). Access to the AP at the Avaya Boot Loader (boot loader) level is disabled.

c. **Boot only**: Choose this radio button to enable Avaya virtual console access at the Avaya Boot Loader (boot loader) level only. Avaya OS level (CLI) access to the AP is disabled.

d. **Connection Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your Avaya virtual console connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.

e. **Port**: Enter a value in this field to define the port used by Avaya virtual console. The default port is 22612.

6. **Serial**

This setting is only available for APs that have a Console (serial) port.

a. **On/Off**: Choose **On** to enable management of the AP via a serial connection, or choose **Off** to disable this feature.

b. **Connection Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your serial connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.

7. **Management Modes**

    a. **Network Assurance**: Click the **On** button to enable this mode. Network assurance is on by default, and checks network connectivity to each server that you configure, such as the NTP server, RADIUS servers, SNMP trap hosts, etc. By proactively identifying network resources that are unavailable, the network manager can be alerted of problems potentially before end-users notice an issue. The distributed intelligence of APs provides this monitoring at multiple points across the network, adding to the ability to isolate the problem and expedite the resolution.

       Connectivity is checked when you configure a server. If a newly configured server is unreachable, you will be notified directly and a Syslog entry is created. Configured servers are checked once per **Period** which by default is 300 seconds (five minutes). Servers are checked regardless of whether they are configured as IP addresses or host names.

       If a server becomes unreachable, a Syslog message is generated. When the server again becomes reachable, another Syslog message is generated.

    b. **PCI Audit Mode**: Click **On** if you wish to configure this AP for auditing PCI-DSS restrictions. See the *Using the Avaya OS for Avaya WLAN AP 9100 Series (NN47252-102)* for more information.

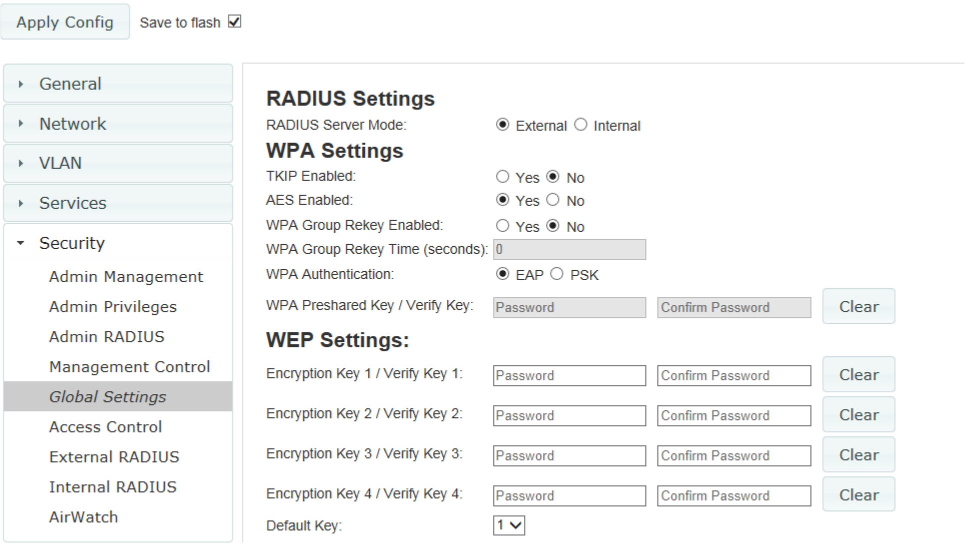
    c. **FIPS 140-2, Level 2 Security**: Click **On** if you wish this AP to enforce FIPS 140-2, Level 2 Security restrictions. See the *Using the Avaya OS for Avaya WLAN AP 9100 Series (NN47252-102)* for more information.

8. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Global Settings

This window allows you to establish the security parameters for your wireless network, including WEP, WPA, WPA2 and RADIUS authentication.

For additional information about wireless network security, refer to **"Understanding Security" on page 414**.



RADIUS Settings

RADIUS Server Mode: ● External ○ Internal

WPA Settings

TKIP Enabled: ○ Yes ● No

AES Enabled: ● Yes ○ No

WPA Group Rekey Enabled: ○ Yes ● No

WPA Group Rekey Time (seconds): 0

WPA Authentication: ● EAP ○ PSK

WPA Preshared Key / Verify Key: Password | Confirm Password

WEP Settings:

Encryption Key 1 / Verify Key 1: Password | Confirm Password

Encryption Key 2 / Verify Key 2: Password | Confirm Password

Encryption Key 3 / Verify Key 3: Password | Confirm Password

Encryption Key 4 / Verify Key 4: Password | Confirm Password

Default Key: 1

Figure 246. Global Settings (Security)

Procedure for Configuring Network Security

1. **RADIUS Server Mode**: Choose the RADIUS server mode you want to use, either **Internal** or **External**. Parameters for these modes are configured in **“External Radius” on page 433** and **“Internal Radius” on page 439**.

WPA Settings

These settings are used if the **WPA** or **WPA2** encryption type is selected on the **SSIDs >SSID Management** window or the **Express Setup** window (on this window, encryption type is set in the **SSID Settings: Wireless Security** field).

2. **TKIP Enabled**: Choose **Yes** to enable Temporal Key Integrity Protocol (TKIP), or choose **No** to disable TKIP.

TKIP encryption does not support high throughput rates, per the IEEE 802.11n specification.

TKIP should never be used for WDS links on APs.

3. **AES Enabled**: Choose **Yes** to enable Advanced Encryption Standard (AES), or choose **No** to disable AES. If both AES and TKIP are enabled, the station determines which will be used.
4. **WPA Group Rekey Enabled**: The Group Key (Group Transient Key) is a shared key among all stations connected to the same radio, and is used to secure multicast/broadcast traffic. It is not used for normal unicast traffic. **Group Key Rekey Time** (below) controls how often this key is changed. The default is **No**.
5. **WPA Group Rekey Time (seconds)**: Enter a value to specify the group rekey time (in seconds). The default is **100** (if enabled).
6. **WPA Authentication**: Select the type of authentication to be used, **PSK** or **EAP**.
7. **WPA Preshared Key / Verify Key**: If you enabled PSK, enter a passphrase here, then re-enter the passphrase to verify that you typed it correctly.

WEP Settings

These settings are used if the **WEP** encryption type is selected on the **SSIDs > SSID Management** window or the AP’s **Express Setup** window (on this window, encryption type is set in the **SSID Settings: Wireless Security** field).

WEP encryption does not support high throughput rates or features like frame aggregation or block acknowledgments, per the IEEE 802.11n specification.

WEP should never be used for WDS links on APs.

8. **Encryption Key 1 / Verify Key 1:**

   Key length is automatically computed based on the Encryption Key that you enter.

   - 5 ASCII characters (10 hex) for 40 bits (WEP-64)
   - 13 ASCII characters for (26 hex) 104 bits (WEP-128)

   Encryption Key 1 / Verify Key 1: Enter an encryption key in ASCII or hexadecimal.

   Re-enter the key to verify that you typed it correctly. You may include special ASCII characters, except for the double quote symbol (“).

9. **Encryption Key 2 to 4/ Verify Key 2 to 4/ Key Mode/Length** (optional): If desired, enter up to four encryption keys, in the same way that you entered the first key.

10. **Default Key**: Choose which key you want to assign as the default key. Make your selection from the drop-down list.

11. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

    After configuring network security, the configuration must be applied to an SSID on the AP for the new functionality to take effect.

Access Control List

This window allows you to enable or disable the use of the global Access Control List (ACL), which controls whether a station with a particular MAC address may associate to the AP. You may create station access control list entries and delete existing entries, and control the type of list.

There is only one global ACL, and you may select whether its type is an Allow List or a Deny List, or whether use of the list is disabled.

There is also a per-SSID ACL (see **"Per-SSID Access Control List" on page 477**). If the same MAC address is listed in both the global ACL and in an SSID's ACL, and if either ACL would deny that station access to that SSID, then access will be denied.

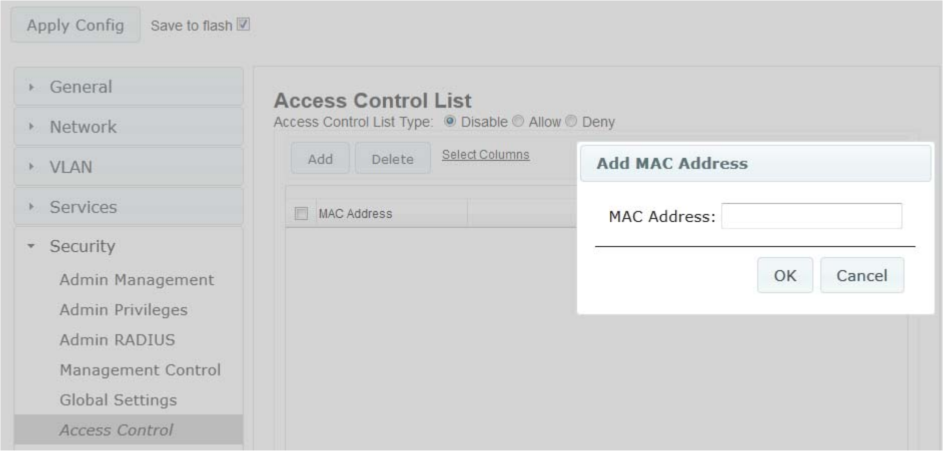


Figure 247. Access Control List

Procedure for Configuring Access Control Lists

1. **Access Control List Type:** Select **Disable** to disable use of the Access Control List, or select the ACL type—either **Allow** or **Deny**.
    - **Allow**: Only allows the listed MAC addresses to associate to the AP. All others are denied.

- **Deny**: Denies the listed MAC addresses permission to associate to the AP. All others are allowed.

  In addition to these lists, other authentication methods (for example, RADIUS) are still enforced for users.

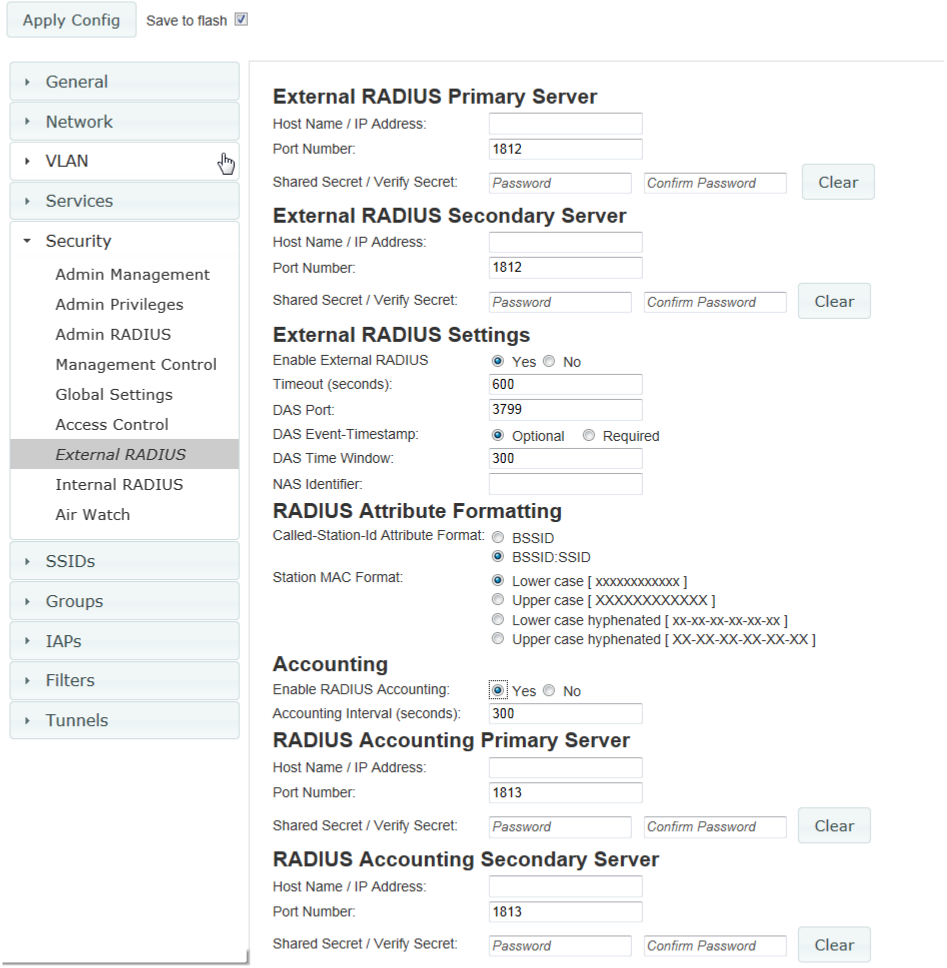
2. **MAC Address**: If you want to add a MAC address to the ACL, click the **Add** button and enter the new MAC address in the dialog box, then click **OK**. The MAC address is added to the ACL. You may use a wildcard (*) for one or more digits to match a range of addresses. You may create up to 1000 entries.

3. **Delete**: You can delete the selected MAC addresses from this list by clicking the **Delete** button.

4. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

External Radius

This window allows you to define the parameters of an external RADIUS server for user authentication. To set up an external RADIUS server, you must choose **External** as the RADIUS server mode in Global Settings. Refer to **"Global Settings" on page 428**.



External RADIUS Primary Server

Host Name / IP Address:

Port Number: 1812

Shared Secret / Verify Secret: Password Confirm Password

External RADIUS Secondary Server

Host Name / IP Address:

Port Number: 1812

Shared Secret / Verify Secret: Password Confirm Password

External RADIUS Settings

Enable External RADIUS ● Yes ○ No

Timeout (seconds): 600

DAS Port: 3799

DAS Event-Timestamp: ● Optional ○ Required

DAS Time Window: 300

NAS Identifier:

RADIUS Attribute Formatting

Called-Station-Id Attribute Format: ○ BSSID
● BSSID:SSID

Station MAC Format: ● Lower case [xxxxxxxxxxxx]
○ Upper case [XXXXXXXXXXXX]
○ Lower case hyphenated [xx-xx-xx-xx-xx-xx]
○ Upper case hyphenated [XX-XX-XX-XX-XX-XX]

Accounting

Enable RADIUS Accounting: ● Yes ○ No

Accounting Interval (seconds): 300

RADIUS Accounting Primary Server

Host Name / IP Address:

Port Number: 1813

Shared Secret / Verify Secret: Password Confirm Password

RADIUS Accounting Secondary Server

Host Name / IP Address:

Port Number: 1813

Shared Secret / Verify Secret: Password Confirm Password

Figure 248. External RADIUS Server

If you want to include user group membership in the RADIUS account information for users, see **“Understanding Groups” on page 480**. User groups allow you to easily apply a uniform configuration to a user on the AP.

About Creating User Accounts on the RADIUS Server

A number of attributes of user (wireless client) accounts are controlled by RADIUS Vendor Specific Attributes defined by Avaya. For example, you would use the VSA named **Avaya-User-VLAN** if you wish to set the VLAN for a user account in RADIUS. For more information about the RADIUS VSAs used by Avaya, see “RADIUS Vendor Specific Attribute (VSA) for Avaya” in the Technical Support Appendix of the *Avaya WLAN AP 9100 Series (NN47252-102)*.

Procedure for Configuring an External RADIUS Server

1. **External RADIUS Primary Server:** This is the external RADIUS server that you intend to use as your primary server.

    a. **Host Name / IP Address**: Enter the IP address or domain name of this external RADIUS server.

    b. **Port Number**: Enter the port number of this external RADIUS server. The default is 1812.

    c. **Shared Secret / Verify Secret**: Enter the shared secret that this external RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.

    The shared secret that you define must match the secret used by the external RADIUS server.

2. **External RADIUS Secondary Server** (optional): If desired, enter an alternative external RADIUS server. If the primary RADIUS server becomes unreachable, the AP will “failover” to the secondary RADIUS server (defined here).

    a. **Host Name / IP Address**: Enter the IP address or domain name of this external RADIUS server.

   b. **Port Number**: Enter the port number of this external RADIUS server. The default is 1812.

   c. **Shared Secret / Verify Secret**: Enter the shared secret that this external RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.

3. **External RADIUS Settings**: Define the settings used for RADIUS Dynamic Authorization.

   a. **Enable External RADIUS**: Enable or disable use of external RADIUS.

   b. **Timeout (seconds)**: Define the maximum idle time (in seconds) before the external RADIUS server's session times out. The default is 600 seconds.

   c. **DAS Port**: RADIUS Dynamic Authorization port. Some RADIUS servers have the ability to contact the AP (referred to as an NAS, see below) to terminate a user with a Disconnect Message (DM). Or RADIUS may send a Change-of-Authorization (CoA) Message to the AP to change a user's privileges due to dynamically changing session authorizations. RADIUS will use the DAS port on the AP for this purpose. The default is port **3799**.

   d. **DAS Event-Timestamp**: The Event-Timestamp Attribute provides a form of protection against replay attacks. If you select **Required**, both the RADIUS server and the AP will use the Event-Timestamp Attribute and check that it is current within the **DAS Time Window**. If the Event-Timestamp is not current, then the DM or CoA Message will be silently discarded.

   e. **DAS Time Window**: This is the time window used with the **DAS Event-Timestamp**, above.

   f. **NAS Identifier**: From the point of view of a RADIUS server, the AP is a client, also called a network access server (NAS). Enter the NAS Identifier (IP address) that the RADIUS servers expect the AP to use—this is normally the IP address of the AP's Gigabit1 port.

4. **RADIUS Attribute Formatting Settings**: Some RADIUS servers, especially older versions, expect information to be sent to them in a legacy format. These settings are provided for the unusual situation that requires special formatting of specific types of information sent to the RADIUS server. Most users will not need to change these settings.

   a. **Called-Station-Id Attribute Format**: Define the format of the **Called-Station-Id** RADIUS attribute sent from the AP—**BSSID:SSID** (default) or **BSSID**.

   b. **Station MAC Format**: Define the format of the **Station MAC** RADIUS attribute sent from the AP—lower-case or upper-case, hyphenated or not. The default is lower-case, not hyphenated.

5. **Accounting**:

   Note that RADIUS accounting start packets sent by the AP will include the client station's Framed-IP-Address attribute. The RADIUS attribute Type-50 Acct-Multi-Session-Id is included in all RADIUS accounting messages generated by Avaya OS Release 7.1 and up. This attribute is used, for example, by some applications to facilitate functions such as onboarding and guest access when stations are roaming between Access Points.

   a. **Enable RADIUS Accounting:** If you would like the AP to send RADIUS Start, Stop, and Interim records to a RADIUS accounting server, click the **Yes** button. The account settings appear, and must be configured.

   b. **Accounting Interval (seconds)**: Specify how often Interim records are to be sent to the server. The default is 300 seconds.

   c. **RADIUS Accounting Primary Server Host Name / IP Address**: Enter the IP address or domain name of the primary RADIUS accounting server that you intend to use.

   d. **Port Number**: Enter the port number of the primary RADIUS accounting server. The default is 1813.

e. **Primary Shared Secret / Verify Secret**: Enter the shared secret that the primary RADIUS accounting server will be using, then re-enter the shared secret to verify that you typed it correctly.

f. **RADIUS Accounting Secondary Server Host Name / IP Address** (optional): If desired, enter an IP address or domain name for an alternative RADIUS accounting server. If the primary server becomes unreachable, the AP will "failover" to this secondary server (defined here).

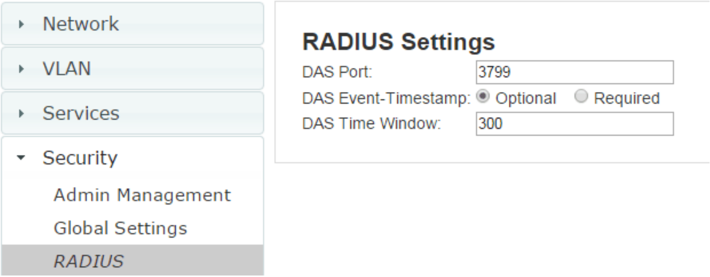
g. **Port Number**: If using a secondary accounting server, enter its port number. The default is 1813.

h. **Shared Secret / Verify Secret**: If using a secondary accounting server, enter the shared secret that it will be using, then re-enter the shared secret to verify that you typed it correctly.

6. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Radius (for AOSLite Only)

Some RADIUS servers are able to contact the AP (referred to as a NAS—Network Access Server, or as a DAS—Dynamic Authorization Server) to terminate a user with a Disconnect Message (DM). Or RADIUS may send a Change-of-Authorization (CoA) Message to the AP to change a user's privileges due to dynamically changing session authorizations.



RADIUS Settings

DAS Port: 3799

DAS Event-Timestamp: ● Optional ○ Required

DAS Time Window: 300

Figure 249. RADIUS Settings for CoA (AOSLite)

If your network will use these capabilities, enter the following settings.

1. **DAS Port:** RADIUS Dynamic Authorization port. RADIUS will use the DAS port on the AP for this purpose. The default is port **3799**.
2. **DAS Event-Timestamp**: The Event-Timestamp Attribute provides a form of protection against replay attacks. If you select **Required**, both the RADIUS server and the AP will use the Event-Timestamp Attribute and check that it is current within the **DAS Time Window**. If the Event-Timestamp is not current, then the DM or CoA Message will be silently discarded.
3. **DAS Time Window**: This is the time window used with the **DAS Event-Timestamp**, above.

Internal Radius

This window allows you to define the parameters for the AP’s internal RADIUS server for user authentication. However, the internal RADIUS server will only authenticate wireless clients that want to associate to the AP. This can be useful if an external RADIUS server is not available. To set up the internal RADIUS server, you must choose **Internal** as the RADIUS server mode in Global Settings. Refer to **“Global Settings” on page 428**.

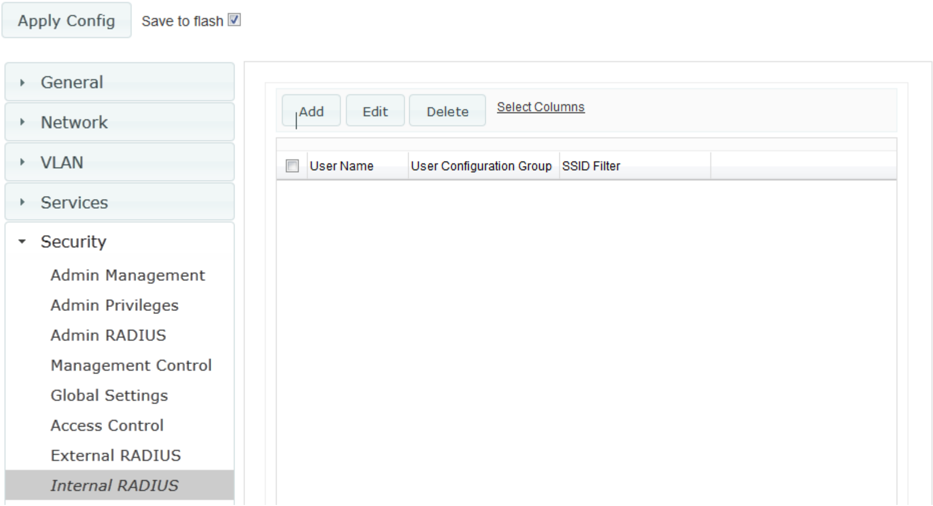
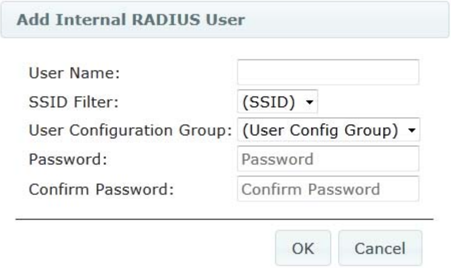


Figure 250. Internal RADIUS Server

Clients using PEAP may have difficulty authenticating to the AP using the Internal RADIUS server due to invalid security certificate errors. To prevent this problem, the user may disable the ***Validate Server Certificate*** *option on the station. Do this by displaying the station’s wireless devices and then displaying the properties of the desired wireless interface. In the security properties, disable* ***Validate server certificate****. In some systems, this may be found by setting the authentication method to PEAP and changing the associated settings.*

Procedure for Creating a New User

1. Click the **Add** button to create a new user entry. The **Add Internal RADIUS User** dialog appears.



Add Internal RADIUS User

User Name:

SSID Filter: (SSID)

User Configuration Group: (User Config Group)

Password: Password

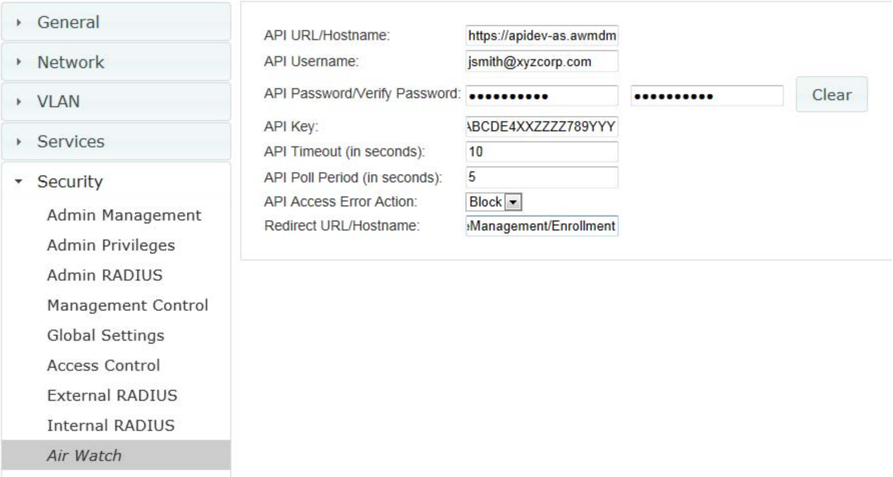
Confirm Password: Confirm Password

Figure 251. Add an Internal RADIUS User

2. **User Name**: Enter the name of the user that you want to authenticate to the internal RADIUS server.
3. **SSID Filter**: (Optional) If you want to restrict this user to associating to a particular SSID, choose an SSID from the drop-down list.
4. **User Configuration Group**: (Optional) If you want to make this user a member of a previously defined user group, choose a group from the drop-down list. This will apply all of the user group's settings to the user. See **"Understanding Groups" on page 480**.
5. **Password**: (Optional) Enter a password for the user.
6. **Confirm Password**: (Optional) Retype the user password to verify that you typed it correctly.
7. Click on the **OK** button to add the new user to the list.
8. If you want to delete a user, select it and click **Delete**.
9. If you want to modify a user entry, select it and click **Edit**.
10. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Airwatch

Mobile Device Management (MDM) servers such as Airwatch enable you to manage large-scale deployments of mobile devices. They may include capabilities to handle tasks such as enrolling devices in your environment, configuring and updating device settings over-the-air, enforcing security policies and compliance, securing mobile access to your resources, and remotely locking and wiping managed devices.



API URL/Hostname: https://apidev-as.awmdm
API Username: jsmith@xyzcorp.com
API Password/Verify Password: •••••••••• •••••••••••
API Key: \BCDE4XXZZZZ789YYY
API Timeout (in seconds): 10
API Poll Period (in seconds): 5
API Access Error Action: Block
Redirect URL/Hostname: :Management/Enrollment

Figure 252. AirWatch Settings

APs support the AirWatch MDM, using an AirWatch API call to determine the status of a user's device and allow access to the wireless network only if the device is enrolled and compliant with the policies of the service.

Individual SSIDs may be configured to require AirWatch enrollment and compliance before a mobile device such as a smartphone or tablet is admitted to the wireless network. The AP uses the AirWatch API with the settings below to request that AirWatch check whether the mobile device is enrolled and compliant with your wireless policies.

Before configuring AirWatch settings on the AP, you must have an AirWatch account, already set up with your organization's compliance policies and other configuration as required by AirWatch.

The AP settings entered on this page are mostly taken from AirWatch. Once you have entered these settings, your users will be constrained to follow a set of steps to access the wireless network, as described in **"User Procedure for Wireless Access" on page 443**.

Procedure for Managing AirWatch

If you have configured the **Mobile Device Management** setting on one or more SSIDs to use **AirWatch**, then the API specified below will be used to determine the admissibility of a mobile device requesting a connection to the wireless network.

1. **API URL/Hostname**: Obtain this from your AirWatch server's **System / Advanced / Site URLs** page. Copy the **REST API URL** string into this field. This specifies the AirWatch API that the AP will call to determine the enrollment and compliance status of a mobile device attempting to connect to the AP. The steps that the user will need to take are described in **"User Procedure for Wireless Access" on page 443**.

2. **API Username**: Enter the user name for your account on the AirWatch server.

3. **API Password**/Verify Password: Enter the password for your account on the AirWatch server.

4. **API Key**: Obtain this from your AirWatch server. Go to the **System / Advanced / API / REST** page, **General** tab, and copy the **API Key** string into this field. The key is required for access to the API.

5. **API Timeout**: (seconds) If AirWatch does not respond within this many seconds, the request fails.

6. **API Poll Period**: (seconds) Mobile device enrollment and compliance status will be checked via polling at this interval. Note that there may thus be a delay before the mobile device will be admitted.

7. **API Access Error Action**: Specify whether or not to allow access if AirWatch fails to respond. The default is to **Block** access.

8. **Redirect URL**: Obtain this from your AirWatch server. Go to the **System / Advanced / Site URLs** page, and copy the **Enrollment URL** string into this field. When a mobile device that is not currently enrolled with AirWatch attempts to connect to the AP, the device displays a page directing the user to install the AirWatch agent and go to the AirWatch enrollment page. Note that Android devices will need another form of network access (i.e. cellular) to download the agent, since un-enrolled devices will not have access to download it via the AP. See **"User Procedure for Wireless Access" on page 443** for more details.

9. You must configure the **Mobile Device Management** setting on one or more SSIDs to use **AirWatch**, as described in Procedure for Managing General Settings (Step 14 on page 457).

User Procedure for Wireless Access

1. A user attempts to connect a mobile device to an SSID that uses AirWatch.

2. The device will authenticate according to the SSID's authentication settings (Open, RADIUS MAC, 802.1x).

3. The user browses to any destination on the Internet.

   The AP asks the user to wait while it checks device enrollment and compliance status by querying the AirWatch API with the device MAC address.

Device enrollment and compliance status will be checked via polling so there may be a delay before the device will be allowed in. That delay will depend on the API Polling Period setting.

4. If AirWatch responds that the device is enrolled and compliant, the device will be allowed into the network. The device will be considered compliant if AirWatch finds that the device does not violate any applicable policies for that device. (If no policies are assigned to the device in AirWatch, then the device is compliant by default.)

5. If the device is not enrolled, all user traffic will be blocked, except that HTTP traffic is redirected to an intermediate page on the AP that tells the user to download and install the AirWatch agent. The page displays a link to the AirWatch-provided device enrollment URL. This link is a pass-though that allows the user to go through the enrollment process. The user will need to enter your organization's AirWatch Group ID and individual account credentials when requested.

   Once the agent is installed, the user must start again at Step 1.

Android devices must go to the PlayStore to install the agent BEFORE they can go through the enrollment process. This means un-enrolled devices need another form of network access (i.e., cellular or an unrestricted SSID) to download this agent, as they are not permitted access to the PlayStore.

Once the agent is installed, the user must start again at Step 1.

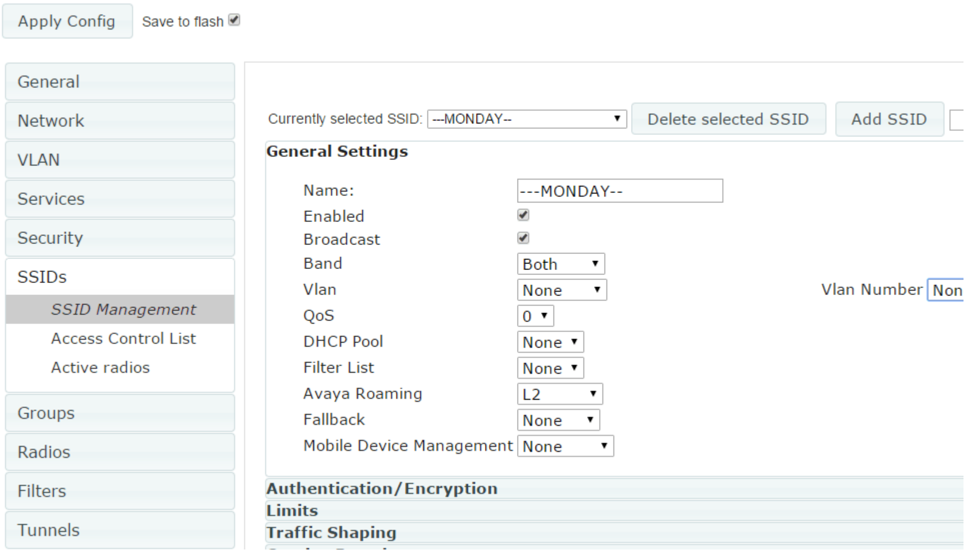
6. If the device is enrolled with AirWatch but not compliant with applicable policies, all traffic will be blocked as in Step 5 above, and the HTTP traffic will be redirected to an intermediate page on the AP that tells the user which policies are out of compliance.

   This page contains a button for the user to click when the compliance issues have been corrected. This button causes AirWatch to again check device compliance. The user's browser is redirected to a "wait" page until the AP has confirmed compliance with AirWatch. The user's browser is then redirected to a page announcing that the device is now allowed network access.

7. If the AP is unable to access AirWatch to obtain enrollment and compliance status (for example, due to bad credentials, timeout, etc.), device access to the network will be granted according to the **API Access Error** setting (**Allow** or **Block**). If this field is set to **Block**, traffic will be blocked as in Step 5 above and HTTP traffic will be redirected to an informational page that informs the user that AirWatch cannot be contacted at this time and advises the user to contact the network administrator. If this field is set to **Allow**, then the device will be allowed network access.

SSIDs

This window allows you to manage SSID (Service Set IDentifier) assignments. You may add or delete SSIDs. Choose the **Currently selected SSID** to view or change an entry's settings.



Save to flash ☑

Currently selected SSID: ---MONDAY--

Name: ---MONDAY--
Enabled ☑
Broadcast ☑
Band Both
Vlan None
Vlan Number Non
QoS 0
DHCP Pool None
Filter List None
Avaya Roaming L2
Fallback None
Mobile Device Management None

Figure 253. SSIDs

Settings are organized into five sections, and you can expand one section at a time to manage that group of settings:

- SSID Management—General Settings—includes whether or not an SSID is enabled and visible on the network, which bands it is available on, which wired VLAN it is associated with, DHCP pools defined per SSID, and other settings.
- SSID Management—Authentication/Encryption—specifies the type of authentication and encryption, and whether to use global security settings or specify individual settings for the SSID here.
- SSID Management—Limits—specifies station limits and operating periods for the SSID.

- SSID Management—Traffic Shaping—specifies how much traffic is allowed, per SSID and station.
- SSID Management—Captive Portal—specifies settings for a portal for guest logins.

For information to help you understand SSIDs and how multiple SSIDs are managed by the wireless AP, go to **“Understanding SSIDs” on page 447**. For a description of how QoS operates on the AP, see **“Understanding QoS Priority on the Wireless AP” on page 450**.

SSIDs are managed with the following windows:

- **“SSID Management” on page 454**
- **“Per-SSID Access Control List” on page 477**
- **“Active Radios” on page 479**

SSIDs are discussed in the following topics:

- **“Understanding SSIDs” on page 447**
- **“High Density 2.4G Enhancement—Honeypot SSID” on page 448**
- **“Understanding QoS Priority on the Wireless AP” on page 450**

Understanding SSIDs

The SSID (Service Set Identifier) is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSIDs. SSIDs are case-sensitive and can contain up to 32 alphanumeric characters (do not include spaces when defining SSIDs).

Multiple SSIDs

A BSSID (Basic SSID) refers to an individual access point radio and its associated clients. The identifier is the MAC address of the access point radio that forms the BSS. A group of BSSs can be formed to allow stations in one BSS to communicate to stations in another BSS via a backbone that interconnects each access point.

The Extended Service Set (ESS) refers to the group of BSSIDs that are grouped together to form one ESS. The ESSID (often referred to as SSID or “wireless network name") identifies the Extended Service Set. Clients must associate to a single ESS at any given time. Clients ignore traffic from other Extended Service Sets that do not have the same SSID.

Legacy access points typically support one SSID per access point. Wireless APs support the ability to define and use multiple SSIDs simultaneously.

Using SSIDs

The creation of different wireless network names allows system administrators to separate types of users with different requirements. The following policies can be tied to an SSID:

- The wireless security mode needed to join this SSID.
- The wireless Quality of Service (QoS) desired for this SSID.
- The wired VLAN associated with this SSID.

As an example, one SSID named **accounting** might require the highest level of security, while another named **guests** might have low security requirements.

Another example may define an SSID named **voice** that supports voice over Wireless LAN phones with the highest Quality of Service (QoS) definition. This SSID might also forward traffic to specific VLANs on the wired network.

High Density 2.4G Enhancement—Honeypot SSID

Note that smaller APs that use the AOSLite system software, such as the WAP9112 and the WAP9114, have many fewer settings than more powerful APs. Honeypot options are not supported. Settings that are not available on a particular AP are not displayed, or will be grayed out.

Some situations pose problems for all wireless APs. For example, iPhones will remember every SSID and flood the airwaves with probes, even when the user doesn't request or desire this behavior. In very high density deployments, these probes can consume a significant amount of the available wireless bandwidth.

The AP offers a feature targeting this problem—a "honeypot" SSID. Simply create an SSID named **honeypot** (lower-case) on the AP, with no encryption or authentication (select **None/Open**). Once this SSID is created and enabled, it will respond to any station probe looking for a named open SSID (unencrypted and unauthenticated) that is *not* configured on the AP. It will make the station go through its natural authentication and association process.

The following SSIDs are excluded from being honeypotted:

- Explicitly whitelisted SSIDs. See **"SSID Management—Honeypot Service Whitelist" on page 476**.
- SSIDs that are encrypted and/or authenticated.
- SSIDs that are configured on this AP, whether or not they are enabled.

Traffic for a station connected to the honeypot SSID may be handled in various ways using other AP features:

- it may be directed to a captive portal to display a splash page or offer the user the opportunity to sign in to your service (see **"SSID Management—Captive Portal" on page 462**);
- it may be filtered (see **"Filters" on page 538**);
- or it may be dead-ended by defining a specific dead-end VLAN on the honeypot SSID to "trap" stations (see **"VLAN" on page 391**).

Use the honeypot feature carefully as it could interfere with legitimate SSIDs and prevent clients from associating to another available network. You may define a whitelist of allowed SSIDs which are not to be honeypotted. See **"SSID Management—Honeypot Service Whitelist" on page 476**.

Understanding QoS Priority on the Wireless AP

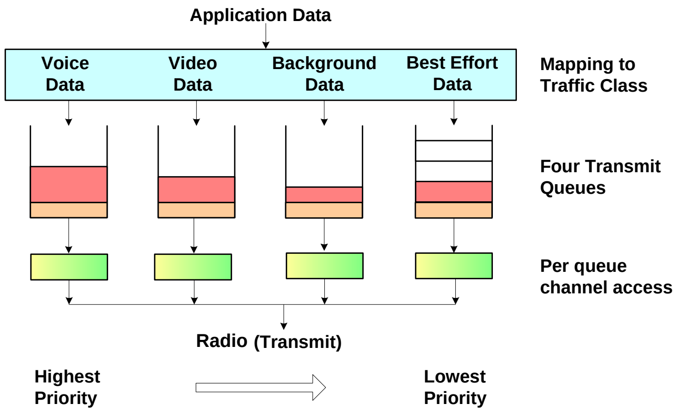


Figure 254. Four Traffic Classes

The wireless AP's Quality of Service Priority feature (preamble) allows traffic to be prioritized according to your requirements. For example, you typically assign the highest priority to voice traffic, since this type of traffic requires delay to be under 10 ms. The AP has four separate queues for handling wireless traffic at different priorities, and thus it supports four traffic classes (QoS levels).

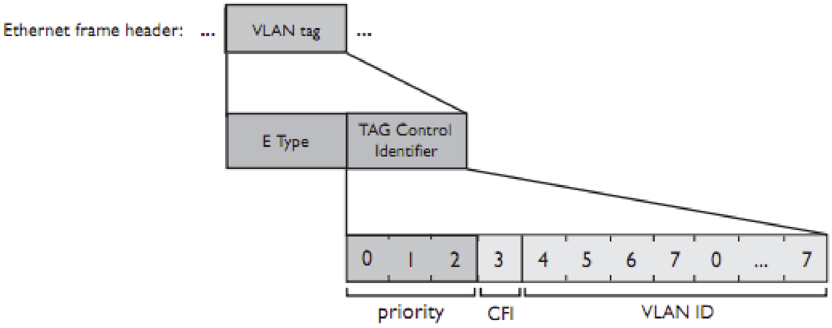


Figure 255. Priority Level—IEEE 802.1p (Layer 2)

IEEE802.1p uses three bits in an Ethernet frame header to define eight priority levels at the MAC level (Layer 2) for wired networks. Each data packet may be tagged with a priority level, i.e., a **user priority** tag. Since there are eight possible user priority levels and the AP implements four wireless QoS levels, user priorities are mapped to QoS as described below.

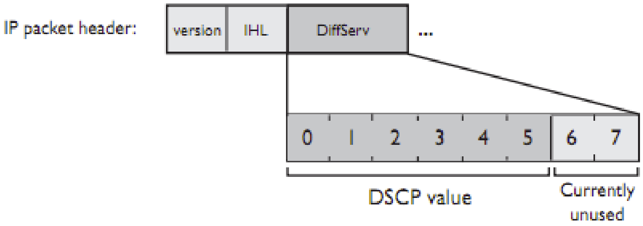


Figure 256. Priority Level—DSCP (DiffServ - Layer 3)

DSCP (Differentiated Services Code Point or DiffServ) uses 6 bits in the IPv4 or IPv6 packet header, defined in RFC2474 and RFC2475. The DSCP value classifies a Layer 3 packet to determine the Quality of Service (QoS) required. DSCP replaces the outdated Type of Service (TOS) field.

The description below describes how both of these priority levels are mapped to the AP's four traffic classes.

End-to-End QoS Handling

- Wired QoS - Ethernet Port:

  Ingress: Incoming wired packets are assigned QoS priority based on their SSID and 802.1p tag (if any), as shown in the table below. This table follows the mapping recommended by IEEE802.11e.

FROM Priority Tag 802.1p (Wired)	**TO** AP QoS (Wireless)	Typical Use
0	0	Best Effort
1	1 (Lowest priority)	Background—explicitly designated as low-priority and non-delay sensitive
2	1	Spare

FROM Priority Tag 802.1p (Wired)	**TO** AP QoS (Wireless)	Typical Use
3	0	Excellent Effort
4	2	Controlled Load
5	2	Video
6	3	Voice - requires delay <10ms
7 (Highest priority)	3 (Highest priority)	Network control

- Egress: Outgoing wired packets are IEEE 802.1p tagged at the Ethernet port for upstream traffic, thus enabling QoS at the edge of the network.

FROM AP QoS (Wireless)	**TO** Priority Tag 802.1p (Wired)
1 (Lowest priority)	1
0	0
2 (Default)	5
3 (Highest priority)	6

Wireless QoS - Radios:

- Each SSID can be assigned a separate QoS priority (i.e., traffic class) from 0 to 3, where 3 is highest priority and 2 is the default. See **“SSID Management” on page 454**. If multiple SSIDs are used, packets from the SSID with higher priority are transmitted first.
- The AP supports IEEE802.11e Wireless QoS for downstream traffic. Higher priority packets wait a shorter time before gaining access to the air and contend less with all other 802.11 devices on a channel.
- How QoS is set for a packet in case of conflicting values:

a. If an SSID has a QoS setting, and an incoming wired packet's user priority tag is mapped to a higher QoS value, then the higher QoS value is used.

b. If a group or filter has a QoS setting, this overrides the QoS value above. See **"Groups" on page 480**, and **"Filters" on page 538**.

c. Voice packets have the highest priority (see Voice Support, below).

d. If **DSCP to QoS Mapping Mode** is enabled, the IP packet is mapped to QoS level 0 to 3 as specified in the DSCP Mappings table. This value overrides any of the settings in cases a to c above.

   In particular, by default:

   - DSCP 8 is set to QoS level 1.
   - DSCP 40 is typically used for video traffic and is set to QoS level 2.
   - DSCP 48 is typically used for voice traffic and is set to QoS level 3—the highest level
   - All other DSCP values are set to QoS level 0 (the lowest level—Best Effort).

Packet Filtering QoS classification

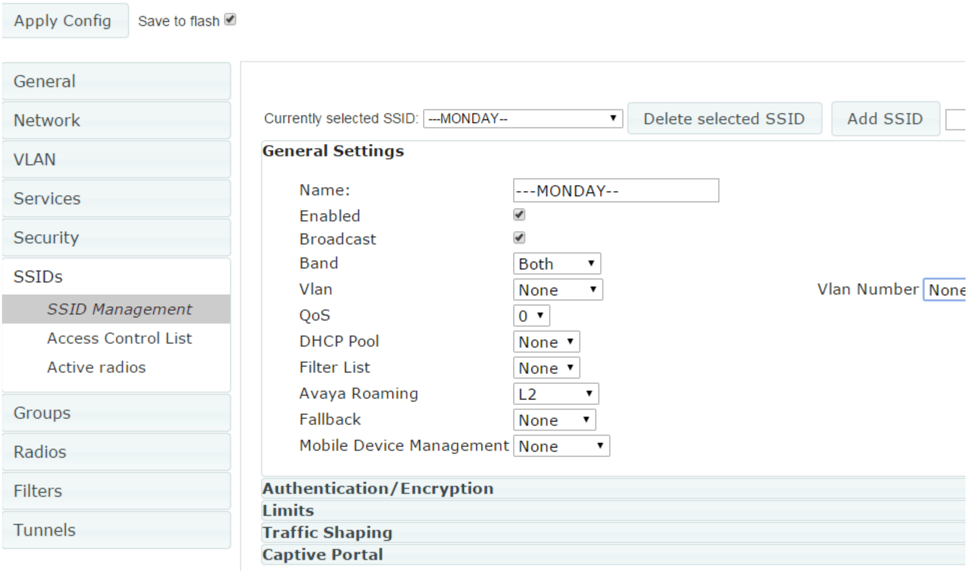
- Filter rules can be used to redefine the QoS priority level to override defaults. See **"Filter Management" on page 541**. This allows the QoS priority level to be assigned based on protocol, source, or destination.

Voice Support

- The QoS priority implementation on the AP give voice packets the highest priority to support voice applications.

SSID Management

This window manages SSIDs (create, edit and delete), assigns security parameters and VLANs on a per SSID basis, and configures the Captive Portal functionality.



Currently selected SSID: ---MONDAY--

General Settings

Name: ---MONDAY--
Enabled ☑
Broadcast ☑
Band Both
Vlan None
Vlan Number None
QoS 0
DHCP Pool None
Filter List None
Avaya Roaming L2
Fallback None
Mobile Device Management None

Figure 257. SSID Management

This page has the following sections. Click a section heading to expand that section.

- **“SSID Management—General Settings” on page 455**
- **“SSID Management—Authentication/Encryption” on page 458**
- **“SSID Management—Limits” on page 460**
- **“SSID Management—Traffic Shaping” on page 461**
- **“SSID Management—Captive Portal” on page 462**
- **“SSID Management—Honeypot Service Whitelist” on page 476**

When done, click the **Apply Config** button near the top of the window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

SSID Management—General Settings

This section manages all SSID settings other than those related to security, station limits, traffic shaping, and captive portal setup.

Procedure for Managing General Settings

1. To create a new SSID, enter its name to the right of the **Add SSID** button, and click the button. (Figure 257)) The SSID **Name** may only consist of the characters A-Z, a-z, 0-9, dash, and underscore. You may create up to 16 SSIDs. (On the WAO9122, you may only create up to six SSIDs).

2. **Currently selected SSID**: The drop-down list shows all currently defined SSIDs. Click any SSID in the list to select it. All the rest of the settings shown and modified on this page will apply to that SSID. When you create a new SSID, the SSID name is added to the list.

   If you wish to delete the currently selected SSID, click **Delete selected SSID**.

3. **Name**: If you wish, you may change the name of the SSID. All other settings will remain unchanged, including whether the SSID is enabled or broadcast. Clients currently connected to the SSID will lose their connection and need to connect to the new name. Renaming an SSID may be very useful in certain situations, such as when a convention center wants to rename an SSID for a new exposition.

4. **Enabled**: Check this box to activate this SSID or clear it to deactivate it.

5. **Broadcast**: Check this box to make the selected SSID visible to all clients on the network. Although the wireless AP will not broadcast SSIDs that are hidden, clients can still associate to a hidden SSID if they know the SSID name to connect to it. Clear this box if you do not want this SSID to be visible on the network.

6. **Band**: Choose which wireless band the SSID will be beaconed on. Select either **5 GHz**, **2.4 GHz**, or **Both**.

7. **VLAN Number**: (Optional) From the drop-down list, select a VLAN that you want this traffic to be forwarded to on the wired network.

8. **QoS**: (Optional) Select a value in this field for QoS (Quality of Service) priority filtering. The QoS value must be one of the following:

   - 0—The lowest QoS priority setting, where QoS makes its best effort at filtering and prioritizing data, video and voice traffic without compromising the performance of the network. Use this setting in environments where traffic prioritization is not a concern.
   - 1—Medium, with QoS prioritization aggregated across all traffic types.
   - 2—High, normally used to give priority to video traffic.
   - 3—The highest QoS priority setting, normally used to give priority to voice traffic.

   The QoS setting you define here will prioritize wireless traffic for this SSID over other SSID traffic, as described in **"Understanding QoS Priority on the Wireless AP" on page 450**. The default value for this field is 2.

9. **DHCP Pool**: If you want to associate an internal DHCP pool to this SSID, choose the pool from the pull--down list. An internal DHCP pool must be created before it can be assigned. To create an internal DHCP pool, go to **"DHCP Server" on page 408**.

10. **Filter List**: If you wish to apply a set a filters to this SSID's traffic, select the desired Filter List. See **"Filters" on page 538**.

11. **802.11r Support**: Check this box to allow Fast Transitions while roaming on this SSID, by having stations pre-authenticated to neighbor APs. For more information and other settings, see **"Fast Transition Configuration" on page 496**. Note that this feature is currently available only on APs that run AOS Lite (WAP9112/WAP9114), and they must be running Release 8.0 or above.

12. **Avaya Roaming**: For this SSID, select whether to enable fast roaming between radios or APs at **L2** (Layer 2 only), or disable roaming (**Off**). See **"Understanding Fast Roaming" on page 487**.

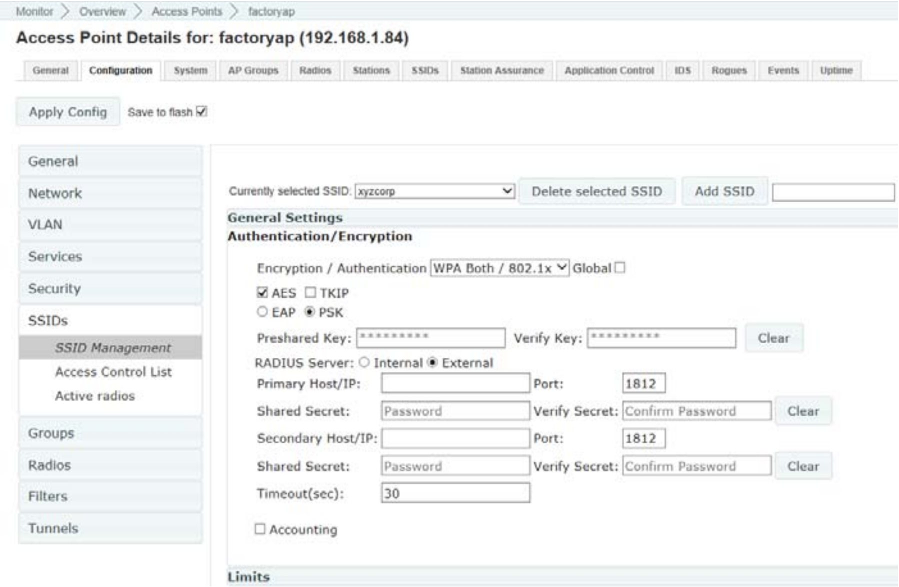
13. **Fallback**: Network Assurance checks network connectivity for the AP. When Network Assurance detects a failure, perhaps due to a bad link or WDS failure, if Fallback is set to **Disable** the AP will automatically disable this SSID. This will disassociate current clients, and prevent new clients from associating. Since the AP's network connectivity has failed, this gives clients a chance to connect to other, operational parts of the wireless network. No changes are made to WDS configuration. See Step a on page 427 for more information on Network Assurance.

14. **Mobile Device Management** (MDM): If you are an AirWatch customer and wish to have AirWatch manage mobile device access to the wireless network on this SSID, select **AirWatch** from the drop-down list. Before selecting this option, you must configure your Airwatch settings. See **"Airwatch" on page 441**.

Note that you cannot use MDM and Captive Portal on the same SSID.

SSID Management—Authentication/Encryption

This section manages all SSID settings related to security.



Access Point Details for: factoryap (192.168.1.84)

Save to flash ☑

Currently selected SSID: xyzcorp

General Settings

Authentication/Encryption

Encryption / Authentication WPA Both / 802.1x Global □

☑ AES □ TKIP

○ EAP ● PSK

Preshared Key: ********* Verify Key: *********

RADIUS Server: ○ Internal ● External

Primary Host/IP: Port: 1812

Shared Secret: Password Verify Secret: Confirm Password

Secondary Host/IP: Port: 1812

Shared Secret: Password Verify Secret: Confirm Password

Timeout(sec): 30

□ Accounting

Figure 258. SSID Management: Authentication/Encryption

Procedure for Managing Authentication/Encryption

1. **Encryption/Authentication: only valid combinations are listed.**

   The following authentication options are available:

   - **Open:** This option provides no authentication and is not recommended.
   - **RADIUS MAC:** Uses an external RADIUS server to authenticate stations onto the wireless network, based on the station's MAC address. Accounting for these stations is performed according to the

accounting options that you have configured specifically for this SSID or globally (see Step 2 below).

If this SSID is on a VLAN, the VLAN must have management turned on in order to pass CHAP authentication challenges from the client station to the RADIUS server.

- **802.1x:** Authenticates stations onto the wireless network via a RADIUS server using 802.1x with EAP. The RADIUS server can be internal (provided by the wireless AP) or external.

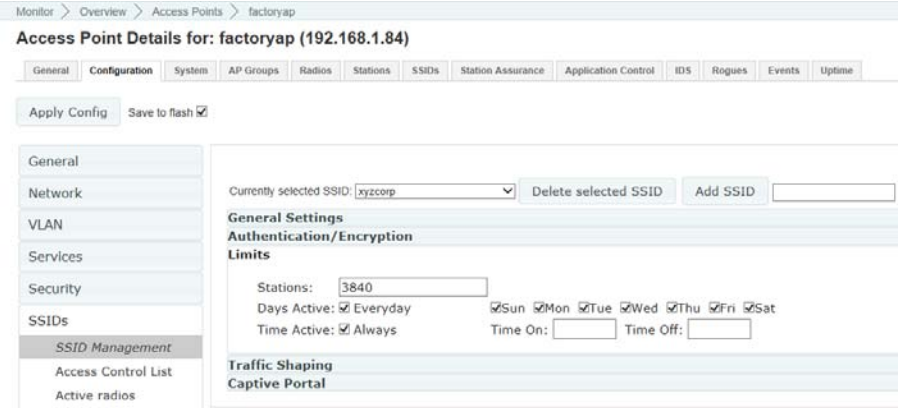
From the drop-down list, choose the encryption that will be required—specific to this SSID—either **None, WEP, WPA, WPA2** or **WPA-Both**. The **None** option provides no security and is not recommended; WPA2 provides the best practice Wi-Fi security.

Each SSID supports only one encryption type at a time (except that WPA and WPA2 are both supported on an SSID if you select WPA-Both). If you need to support other encryption types, you must define additional SSIDs. The encryption standard used with WPA or WPA2 is selected in the Security>Global Settings window (page 428). For an overview of the security options, see **"Understanding Security" on page 414**.

2. **Global**: Check the checkbox if you want this SSID to use the security settings established at the global level (refer to **"Global Settings" on page 428**). Clear the checkbox if you want the settings established here to take precedence. Additional sections will be displayed to allow you to configure encryption, RADIUS, and RADIUS accounting settings. The **WPA Configuration** encryption settings have the same parameters as those described in **"Procedure for Configuring Network Security" on page 429**. The external RADIUS and accounting settings are configured in the same way as for an external RADIUS server (see **"Procedure for Configuring an External RADIUS Server" on page 434**). External RADIUS servers may be specified using IP addresses or domain names.

SSID Management—Limits

This section manages station limits for this SSID. See **“Group Limits” on page 485** for a discussion of the interaction of SSID limits and group limits. To eliminate confusion, we recommend that you configure one set of limits or the other, but not both.



Save to flash ☑

Currently selected SSID: xyzcorp

Stations: 3840

Days Active: ☑ Everyday ☑Sun ☑Mon ☑Tue ☑Wed ☑Thu ☑Fri ☑Sat

Time Active: ☑ Always Time On: Time Off:

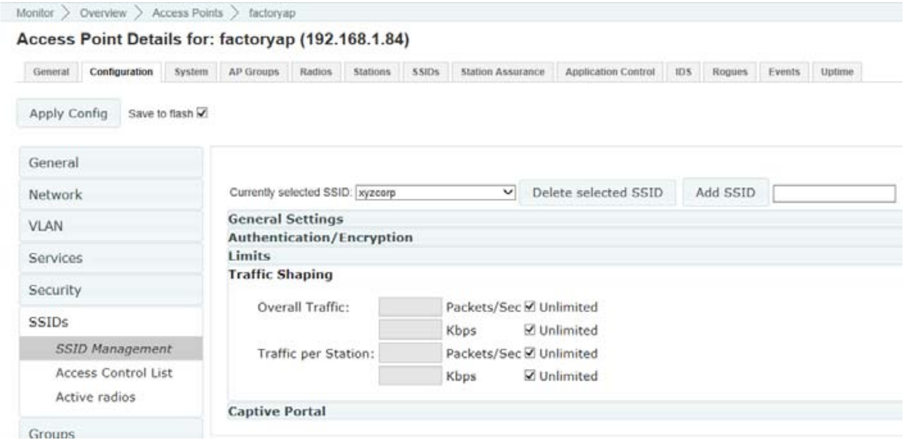
Figure 259. SSID Management: Limits

Procedure for Managing Limits

1. **Stations:** Enter the maximum number of stations allowed on this SSID. This step is optional. Note that station limits may be set in several places—see Step 15 on page 497 in Global Settings (Radio) for details. If multiple limits are set, all will be enforced. As soon as any limit is reached, no new stations can associate until some other station has terminated its association.
2. **Days Active**: Choose **Everyday** if you want this SSID to be active every day of the week, or select only the specific days that you want this SSID to be active. Days that are not checked are considered to be the inactive days.
3. **Time Active**: Choose **Always** if you want this SSID active without interruption, or enter values in the **Time On** and **Time Off** fields to limit the time that this SSID is active.

SSID Management—Traffic Shaping

This section manages traffic limits for this SSID.



Access Point Details for: factoryap (192.168.1.84)

Save to flash ☑

Currently selected SSID: xyzcorp

Overall Traffic:		Packets/Sec	☑ Unlimited
		Kbps	☑ Unlimited
Traffic per Station:		Packets/Sec	☑ Unlimited
		Kbps	☑ Unlimited

Figure 260. SSID Management: Traffic Shaping

Procedure for Managing Traffic Shaping

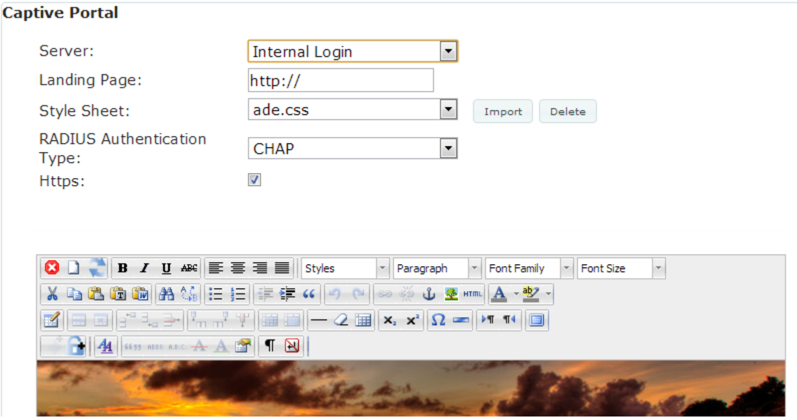
1. **Overall Traffic**: Choose **Unlimited** if you do not want to place a restriction on the traffic for this SSID, or enter a value in the **Packets/Sec** field or the **Kbps** field to force a traffic restriction. If you set both values, the AP will enforce the limit it reaches first.

2. **Traffic per Station**: Choose **Unlimited** if you do not want to place a restriction on the traffic per station for this SSID, or enter a value in the **Packets/Sec** field or the **Kbps** field to force a traffic restriction. If you set both values, the AP will enforce the limit it reaches first.

SSID Management—Captive Portal

Note that smaller APs that use the AOSLite system software, such as the WAP9112 and the WAP9114, have many fewer settings than more powerful APs. Settings that are not available on a particular AP are not displayed, or will be grayed out.

This section manages captive portal settings for this SSID, and includes a WYSIWYG (What You See Is What You Get) HTML editor for creating a splash page or login page for the portal.



Captive Portal

Server:	Internal Login
Landing Page:	http://
Style Sheet:	ade.css Import Delete
RADIUS Authentication Type:	CHAP
Https:	☑

Figure 261. SSID Management: Captive Portal (Internal Login page)

Procedure for Managing Captive Portal Settings

The Access Point-based Captive Portal (also called WPR—Web Page Redirect) may be used to provide a portal for an alternate mode of authentication, or to simply display a splash screen when a user first associates to the wireless network. After that, it can optionally redirect the user to a landing page at an alternate URL. Example applications are:

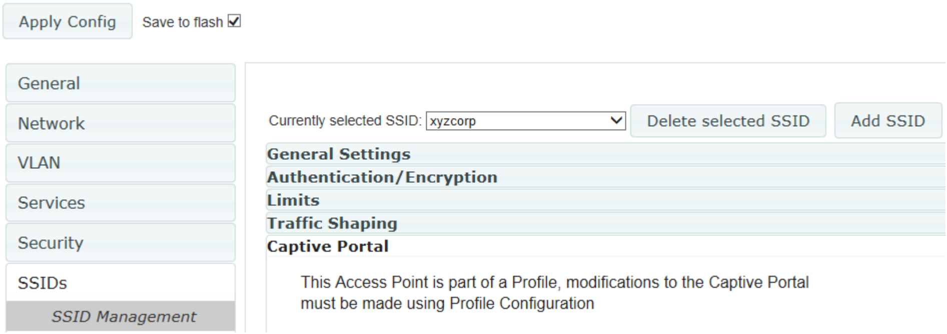
- As an authentication device requiring a user to enter a username and password (and possibly, a method of payment) before accessing network resources.

- To inform the user about the Terms and Conditions of using the network before allowing access.
- To intercept a web page request by the client device and redirect to a specific web page before accessing the network.

You may specify a white list—a list of Internet destinations that stations can access without having to pass the captive portal first. For example, you may make your organization's public web site accessible without redirection to the captive portal. See **“White List Configuration for Captive Portal” on page 475**.

*When using a captive portal, it is particularly important to adhere to the SSID naming restrictions detailed in **Step 1 on page 455**.*

Enable a captive portal by setting the **Server** type to any choice other than **Disabled**. The SSID Management window displays additional fields to be configured, based on your selection. The captive portal HTML editor is displayed, when needed, to create a splash or login page with a WYSIWYG editor.



Currently selected SSID: xyzcorp

This Access Point is part of a Profile, modifications to the Captive Portal must be made using Profile Configuration

Figure 262. Captive Portal Server Types

If enabled, the captive portal displays a splash or login page when a user associates to the wireless network and opens a browser to any URL (provided the URL does not point to a resource directly on the user’s machine). The user-requested URL is captured, the user’s browser is redirected to the specified splash or login page, and then the browser is redirected either to your specified landing page, if any, or else back to the captured URL. The landing page may be specified for a user group as well. See **“Group Management” on page 482**. Note that if you change the management HTTPS port, captive portal uses that port, too. See **“HTTPS” on page 425**.

When users roam between APs, their captive portal authentication will follow them so that re-authentication is not required.

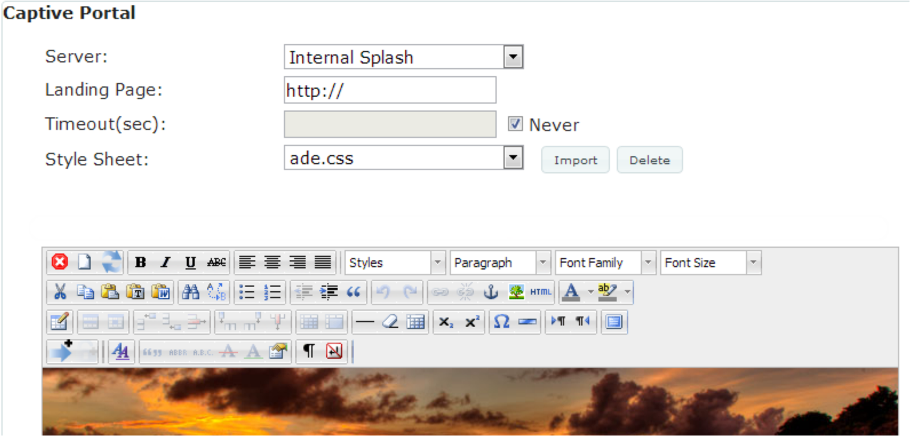
When you are done making changes to captive portal settings, save the changes to the AP by clicking **Apply Config** with **Save to flash** enabled.

You may select among five different modes for use of the Captive Portal feature, each displaying a different set of parameters that must be entered.

- **“Internal Splash page” on page 465**
- **“Internal Login page” on page 466**
- **“External Login page” on page 468**
- **“External Splash page” on page 469**
- **“Landing Page Only” on page 470**

After you specify the captive portal, you may specify a white list of Internet destinations that may be accessed without passing through the captive portal flow—see **“White List Configuration for Captive Portal” on page 475**.

- Internal Splash page



Captive Portal

Server: Internal Splash

Landing Page: http://

Timeout(sec): ☑ Never

Style Sheet: ade.css

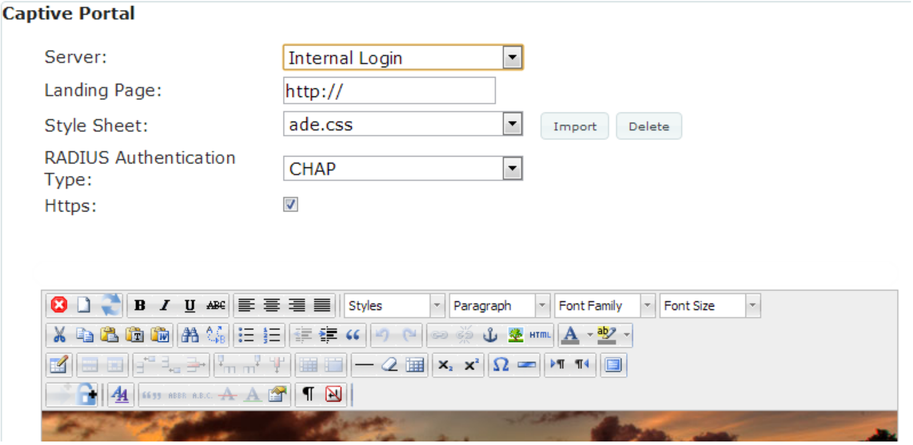
Figure 263. Captive Portal—Internal Splash Page

This option displays a splash page instead of the first user-requested URL. The splash page files reside on the AP. Create the splash page using the captive portal editor. The HTML editor can add text and images and insert a **Proceed** button. See **"Editing an Internal Login or Internal Splash Page" on page 470**.

To use an internal splash page, set **Server** to **Internal Splash**. Enter a value in the **Timeout** field to define how many seconds the splash screen is displayed before timing out, or select **Never** to prevent the page from timing out automatically (be sure to add a **Proceed** button in this case—Figure 269 on page 472). After the splash page, the user is redirected to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page**.

If you have a CSS file defining the styles for the splash page, use the **Style Sheet** field to specify it. Select one of the previously uploaded CSS files from the drop-down list, or click the **Import** button to select the desired CSS file and upload it to the WOS server. You may remove files from the list with the **Delete** button. Only one CSS file may be applied to each captive portal, and the same file may be used by different portals. The file must end in a .css extension and be under 1 MB. The HTML files uploaded to an AP for the captive portal will include the CSS file.

- Internal Login page



Captive Portal

Server: Internal Login

Landing Page: http://

Style Sheet: ade.css

RADIUS Authentication Type: CHAP

Https: ☑

Figure 264. Captive Portal—Internal Login Page

This option displays a login page instead of the first user-requested URL. Create the login page (which resides on the AP) using the captive portal editor. The HTML editor can add text and images and insert a section containing fields to capture user credentials, or you may insert a default login page and customize it. See **“Editing an Internal Login or Internal Splash Page” on page 470**.

To set up internal login, set **Server** to **Internal Login**. If you have a CSS file defining the styles for the login page, use the **Style Sheet** field to specify it. Select one of the previously uploaded CSS files from the drop-down list, or click the **Import** button to select the desired CSS file and upload it to the WOS server. You may remove a CSS file from the list by using the **Delete** button. Only one CSS file may be applied to each captive portal, and the same file may be used by different portals. The file must end in a .css extension and be under 1 MB. The HTML files uploaded to an AP for the captive portal will include the CSS file.

Check the **HTTPS** checkbox for a secure login, or uncheck it to use HTTP. Select the **RADIUS Authentication Type** to use for the client. This is the protocol used for authentication of users, **CHAP** (the default), **MS-CHAP**, or **PAP**.

- **Password Authentication Protocol (PAP)**, is a simple protocol. PAP transmits ASCII passwords over the network "in the clear" (unencrypted) and is therefore considered insecure.
- **Challenge-Handshake Authentication Protocol (CHAP)** is a more secure Protocol. The login request is sent using a one-way hash function.
- **MS-CHAP** is the Microsoft version of Challenge-Handshake Authentication Protocol.

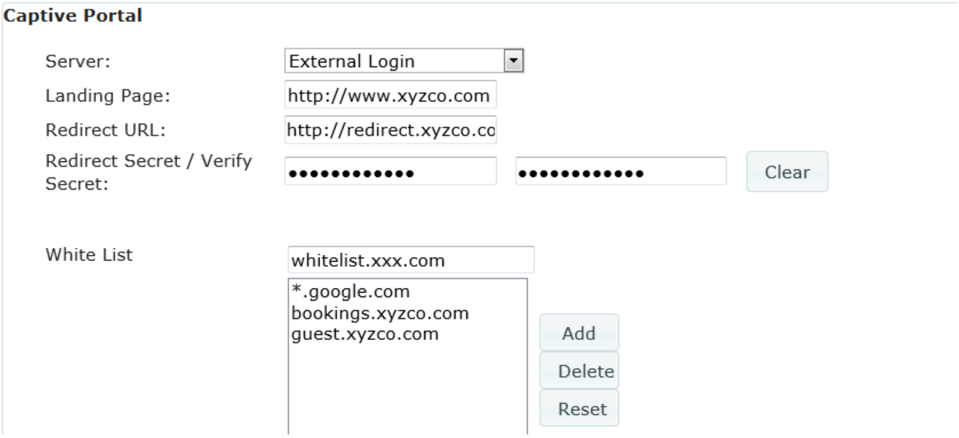
The user name and password are obtained by the login page, and authentication occurs according to your configured authentication information (see **"SSID Management—Authentication/Encryption" on page 458**).

After authentication, the browser is redirected back to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page**.

Both the Internal Login and External Login options of Captive Portal perform authentication using your configured RADIUS servers.

- External Login page

  This option redirects the user to a login page on an external web server for authentication, instead of the first user-requested URL. Login information (user name and password) must be obtained by that page, and returned to the AP for authentication.



Captive Portal

Server:	External Login
Landing Page:	http://www.xyzco.com
Redirect URL:	http://redirect.xyzco.co
Redirect Secret / Verify Secret:	●●●●●●●●●●●● ●●●●●●●●●●●●
White List	whitelist.xxx.com *.google.com bookings.xyzco.com guest.xyzco.com

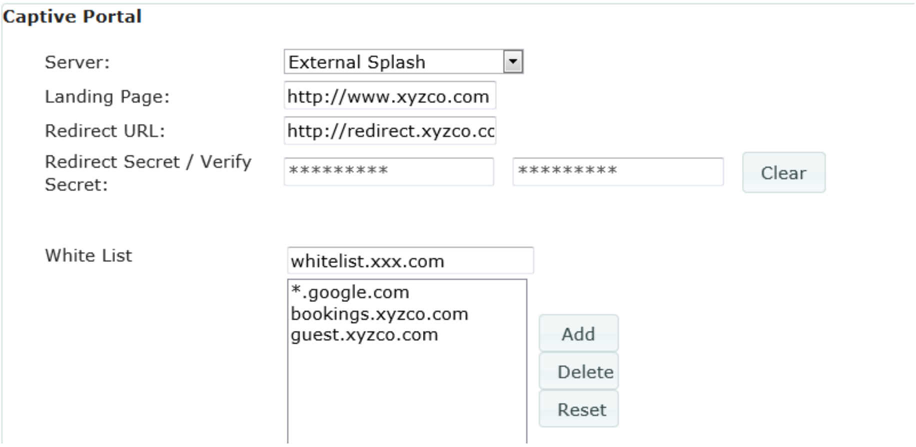
Figure 265. Captive Portal—External Login Page

Authentication occurs according to your configured authentication information (see **“SSID Management—Authentication/Encryption” on page 458**). After authentication, the browser is redirected back to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page**.

To set up external login page usage, set **Server** to **External Login**. Enter the URL of the external web server in **Redirect URL**, and enter that server’s shared secret in **Redirect Secret**.

- External Splash page

  This option displays a splash page instead of the first user-requested URL. The splash page files reside on an external web server.



Captive Portal

Server: External Splash

Landing Page: http://www.xyzco.com

Redirect URL: http://redirect.xyzco.cc

Redirect Secret / Verify Secret: ********* *********

White List: whitelist.xxx.com

*.google.com
bookings.xyzco.com
guest.xyzco.com

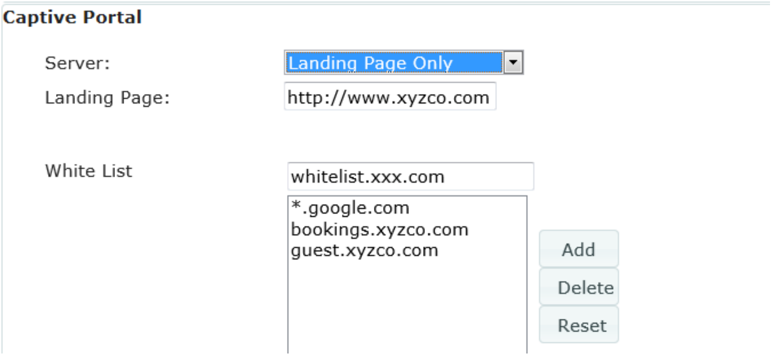
Figure 266. Captive Portal—External Splash Page

To set up external splash page usage, set **Server** to **External Splash**. Enter the URL of the external web server in **Redirect URL**, and enter that server's shared secret in **Redirect Secret**.

After the splash page, the user is redirected to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page**.

- Landing Page Only

  This option redirects the user to a specific landing page. If you select this option, enter the desired address in **Landing Page URL**.



Captive Portal

Server: Landing Page Only

Landing Page: http://www.xyzco.com

White List: whitelist.xxx.com

*.google.com
bookings.xyzco.com
guest.xyzco.com

Figure 267. Captive Portal—Landing Page Only

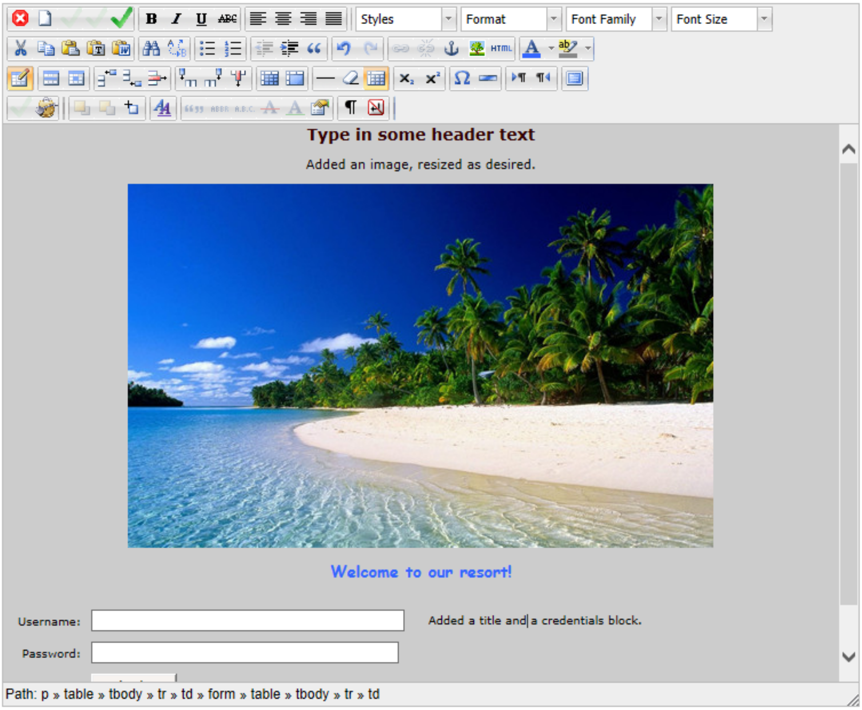
Editing an Internal Login or Internal Splash Page

If you set the Captive Portal **Server** to **Internal Login** or **Internal Splash**, the captive portal editor appears. Use it to create the captive portal page displayed when a user associates to this SSID.

The captive portal editor initially displays the current splash or login page that is defined on the AP, if any. If you switch SSIDs, your splash or login page will be automatically saved in a temporary workspace—however, we recommend that you work on the page until you are satisfied with it, and then apply it to the AP as described below to save the page. Otherwise, if you leave The Configuration Tab, your changes will be lost.

A note above the captive portal editor will inform you that APs running Avaya OS versions older than Release 6.6.0 must be rebooted for changes in the splash or login page to take effect. When you are done editing the captive portal page, save the changes to the AP by clicking **Apply Config** with **Save to flash** enabled. If a reboot is required, it does not occur automatically—you must initiate it yourself. See **“The Configure APs Toolbar” on page 110**.

The captive portal editor is an HTML editor. Since it is a WYSIWYG editor (What You See Is What You Get), it shows you exactly the way the page will appear.



Type in some header text

Added an image, resized as desired.

Welcome to our resort!

Username:

Password:

Added a title and a credentials block.

Path: p » table » tbody » tr » td » form » table » tbody » tr » td

Figure 268. Using the Captive Portal Editor

The rows of buttons at the top of the editor provide the editing features. Many of these buttons provide text editing functions that will be familiar, especially for users of Microsoft Word style editors. Other buttons add images, work with layers, or allow you to edit HTML source. Some of the more powerful buttons are highlighted in Figure 269, below. Two buttons are tailored especially for the captive portal page—they insert special purpose buttons on the captive portal page or create default login or splash pages.

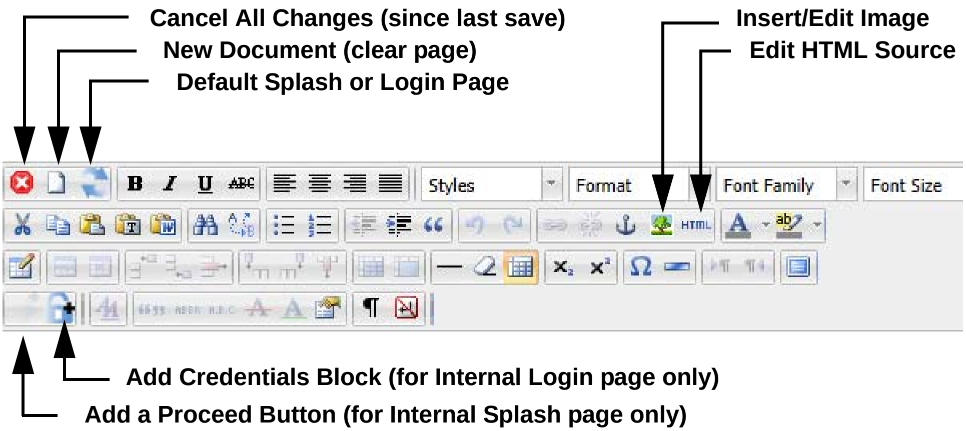
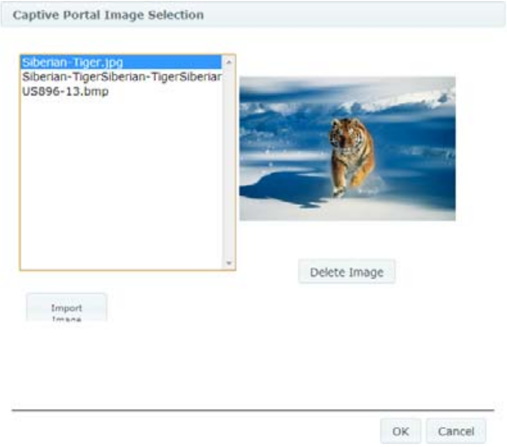

Cancel All Changes (since last save)
New Document (clear page)
Default Splash or Login Page
Insert/Edit Image
Edit HTML Source
Styles
Format
Font Family
Font Size
HTML
Add Credentials Block (for Internal Login page only)
Add a Proceed Button (for Internal Splash page only)

Figure 269. Captive Portal Editor Buttons

To use the Captive Portal Editor

- Hover the mouse over any button to display a tool tip describing the button's purpose.
- Use the **Default Splash or Login Page** button if you wish to use a default page. If your portal server type is **Internal Splash**, then the default page will have a **Proceed** button. If your portal page type is **Internal Login**, then the default page will have fields for entering **Username** and **Password**. You may delete the Avaya logo. Use the **Insert/Edit Image** button as described below to add your own logo at the cursor location. If you wish to add content before or after the default page, you may use the **Edit HTML Source** button described below.
- To create your own page instead, start typing in the blank display portion of the window, then use any of the provided text editing buttons to format and edit the text.
- Paste an image in place at the current cursor location, or click the **Insert/ Edit Image** button to open the Insert/Edit Image dialog. Use the Browse button to open the Captive Portal Image Selection dialog. Select one of the previously uploaded images and click **OK**, or click

Import Image to browse to the desired image and upload it to the WOS server. The image is inserted as a reference rather than directly inline. The HTML files uploaded to an AP for the captive portal will include the files for embedded images. Images may be in jpg, gif, or png format, and the size may be up to 2 MB. Click **Delete Image** if you wish to remove the selected image from the WOS server.



Captive Portal Image Selection

Siberian-Tiger.jpg
Siberian-TigerSiberian-TigerSiberiar
US896-13.bmp

Figure 270. Captive Portal Image Selection

When you return to the **Insert/Edit Image** dialog, you may enter an **Image Description** to present if the image cannot be displayed when viewed by the user. If you enter a **Title**, it will pop up like a tool tip when the user hovers the mouse over the image.

The **Appearance** and **Advanced** tabs allow you to change other attributes of the image as displayed to the user. For example, the Appearance tab allows you to specify a style from your Style Sheet (.css), if you are using one, for the image display. Click **Insert** or **Update** at the lower left when done.

Click the image and drag the handles to resize.

- Make changes directly in the HTML by using the **Edit HTML Source** button. In the HTML Source Editor window, make the desired changes. If you have HTML from another source that you want to use, you may paste it into this window. Click **Update** at the lower left when done. There is also an **Edit CSS Style** button to tweak many aspects of text display.

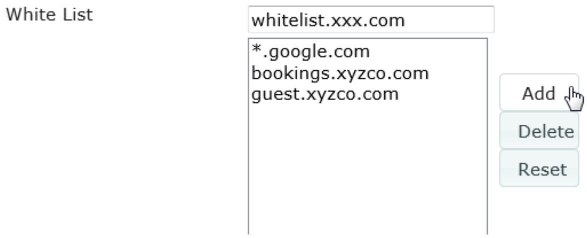
The **Insert/Edit Attributes** button allows you to add HTML attributes and/or JavaScript events to the content on your page.

- Add necessary controls to the portal page using the **Add a Proceed Button/ Add Credentials Block** button. If your portal page type is **Internal Splash** and your **Timeout** setting is **Never**, then this will add a **Proceed** button to your portal at the current line (at the left of the window). If your portal page type is **Internal Splash** and the **Timeout** setting is a non-zero number of seconds, then the **Add a Proceed Button** icon will not appear—the splash page will automatically close after the specified timeout and a proceed button is not needed.

  If your portal page type is **Internal Login**, then the **Credentials Block** button will add fields for entering **Username** and **Password**.
- There are **Undo** and **Redo** buttons. The **Cancel All Changes** button reverts the page to the last version that you saved. The **New Document** button restores you to a blank page.
- Remember that when you are done making changes to the internal splash or login page, you must click **Apply Config** with **Save to flash** enabled. Then the AP must be explicitly rebooted for the changes to take effect.
- You may find more information on using the features of the captive portal editor here.

White List Configuration for Captive Portal

On a per-SSID basis, the white list allows you to specify Internet destinations that stations can access without first having to pass the captive portal login/splash page. Note that a white list may be specified for a user group as well. See **"Group Management" on page 482**.



White List

whitelist.xxx.com

*.google.com
bookings.xyzco.com
guest.xyzco.com

Figure 271. White List Configuration for Captive Portal

To add a web site to the white list for this SSID, enter it in the provided field, then click **Create**. You may enter an IP address or a domain name. Up to 32 entries may be created.

Example white list entries:

- Hostname: www.yahoo.com (but not www.yahoo.com/abc/def.html)
- Wildcards are supported: *.yahoo.com
- IP address: 121.122.123.124

Some typical applications for this feature are:

- to add allowed links to the captive portal page
- to add a link to terms of use that may be hosted on another site
- to allow embedded video on captive portal page

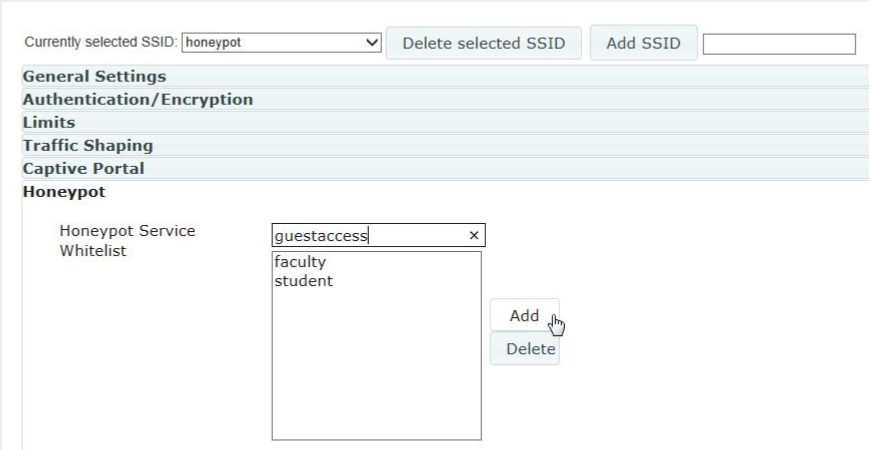
Note the following details of the operation of this feature:

- The list is configured on a per-SSID basis. You must have **captive portal** enabled for the SSID to see this section of the SSID Management page.
- When a station that has not yet passed the captive portal login/splash page attempts to access one of the white-listed addresses, it will be allowed access to that site as many times as requested.

- The station will still be required to pass through the configured captive portal flow for all other Internet addresses.
- The white list will work against all traffic -- not just http or https
- Indirect access to other web sites is not permitted. For example, if you add www.yahoo.com to the white list, you can see that page, but not all the ads that it attempts to display.
- The white list feature does not cause traffic to be redirected to the white list addresses.

SSID Management—Honeypot Service Whitelist

This section only appears if you have created an SSID named **honeypot**. You may define a whitelist of allowed SSIDs which are not to be honeypotted, as described in **“High Density 2.4G Enhancement—Honeypot SSID” on page 448**. Type in each SSID name, and click **Add** to add it to the whitelist. Up to 50 SSIDs may be listed. The SSID names entered in this list are not case-sensitive.


Currently selected SSID: honeypot

Honeypot Service Whitelist: guestaccess

faculty
student

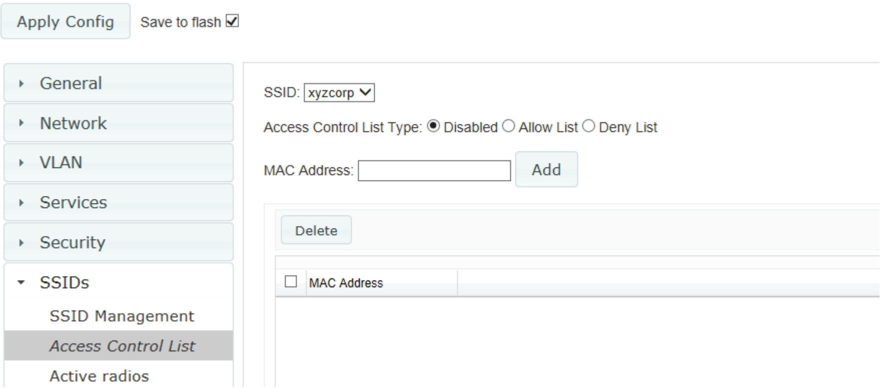
Figure 272. SSID Management: Honeypot Whitelist

You may use the “*” character as a wildcard to match any string at this position. For example, abc* matches any string that starts with **ABC** or **abc**. You may use a **?** as a wildcard to match a single character by surrounding the SSID name in quotes. For example, “**xyzco?**” will match any six-character long string that starts with **xyzco** (again, the match is not case-sensitive). If you do not use a wildcard, then the SSID name entered must be matched exactly in order to be whitelisted (except that case is not considered).

Use the honeypot feature carefully as it could interfere with legitimate SSIDs.

Per-SSID Access Control List

This window allows you to enable or disable the use of the per-SSID Access Control List (ACL), which controls whether a station with a particular MAC address may associate to this SSID. You may create access control list entries and delete existing entries, and control the type of list.



Save to flash ☑

SSID: xyzcorp

Access Control List Type: ● Disabled ○ Allow List ○ Deny List

MAC Address:

☐ MAC Address

Figure 273. Per-SSID Access Control List

There is one ACL per SSID, and you may select whether its type is an Allow List or a Deny List, or whether use of this list is disabled. You may create up to 1000 entries per SSID.

There is also a global ACL (see **“Access Control List” on page 431**). If the same MAC address is listed in both the global ACL and in an SSID’s ACL, and if either ACL would deny that station access to that SSID, then access will be denied.

Procedure for Configuring Access Control Lists

1. **SSID**: Select the SSID whose ACL you wish to manage.
2. **Access Control List Type**: Select **Disabled** to disable use of the Access Control List for this SSID, or select the ACL type—either Allow List or Deny List.
    - **Allow List**: Only allows the listed MAC addresses to associate to the AP. All others are denied.
    - **Deny List**: Denies the listed MAC addresses permission to associate to the AP. All others are allowed.

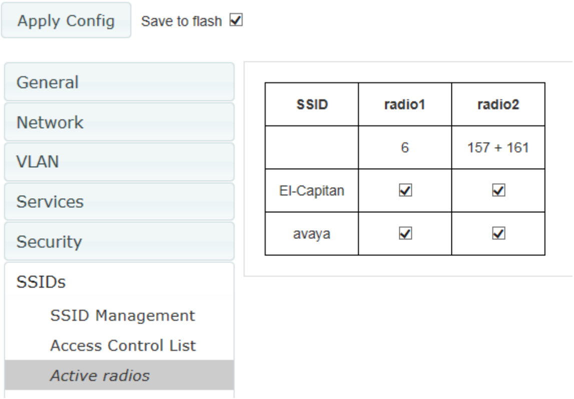
    In addition to these lists, other authentication methods (for example, RADIUS) are still enforced for users.

3. **MAC Address**: If you want to add a MAC address to the ACL, enter the new MAC address here, then click the **Add** button. The MAC address is added to the ACL. You may use a wildcard (*) for one or more digits to match a range of addresses.
4. **Delete**: You may delete selected MAC addresses from this list by clicking their **Delete** buttons.
5. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Active Radios

By default, when a new SSID is created, that SSID is active on all radios. This window allows you to specify which radios will offer that SSID. Put differently, you can specify which SSIDs are active on each radio.

This feature is useful in conjunction with WDS. You may use this window to configure the WDS link radios so that only the WDS link SSIDs are active on them.



SSID	radio1	radio2
	6	157 + 161
El-Capitan	☑	☑
avaya	☑	☑

Figure 274. Setting Active Radios per SSID

Procedure for Specifying Active Radios

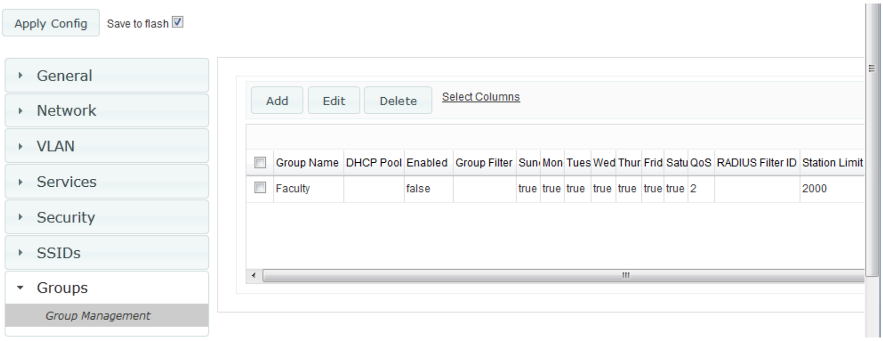
1. **SSID:** For a given SSID row, check off the radios on which that SSID is to be active. Uncheck any radios which should not offer that SSID.

2. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Groups

This is a status-only window that allows you to review user (i.e., wireless client) Group assignments. It includes the group name, Radius ID, Device ID, VLAN IDs and QoS parameters and roaming layer defined for each group, and DHCP pools and captive portal information defined for the group. You may click on a group's name to jump to the edit page for the group. There are no configuration options available on this page, but if you are experiencing problems or reviewing group management parameters, you may want to print this page for your records.

The **Limits** section of this window shows any limitations configured for your defined groups. For example, this window shows the current state of a group (enabled or disabled), how much group and per-station traffic is allowed, time on and time off, and days on and off.



□	Group Name	DHCP Pool	Enabled	Group Filter	Sun	Mon	Tues	Wed	Thur	Frid	Satu	QoS	RADIUS Filter ID	Station Limit
□	Faculty		false		true	true	true	true	true	true	true	2		2000

Figure 275. Groups

Understanding Groups

User groups allow administrators to assign specific network parameters to users (wireless clients) through RADIUS privileges rather than having to map users to an SSID tailored for that set of privileges. Groups provide flexible control over user privileges without the need to create large numbers of SSIDs.

A group allows you to define a set of parameter values to be applied to selected users. For example, you might define the user group **Students**, and set its VLAN, security parameters, captive portal, and traffic limits. When a new user is created, you can apply all of these settings just by making the user a member of the group.

The group allows you to apply a uniform configuration to a set of users in one step.

In addition, you can restrict the group so that it only applies its settings to group members who are connecting using a specific device type, such as iPad or phone. Thus, you could define a group named **Student-Phone** with **Device ID** set to **Phone**, and set the group's **VLAN Number** to 100. This group's settings will only be applied to group members who connect using a phone, and they will all use VLAN 100. Note that settings for the group in the RADIUS server will override any settings on this WMI page.

Almost all of the parameters that can be set for a group are the same as SSID parameters. This allows you to configure features at the user group level, rather than for an entire SSID. If you set parameter values for an SSID, and then enter different values for the same parameters for a user group, the **user group values have priority** (i.e., group settings will override SSID settings).

Group names are case-sensitive and can contain up to 32 alphanumeric characters (do not include spaces when defining Groups).

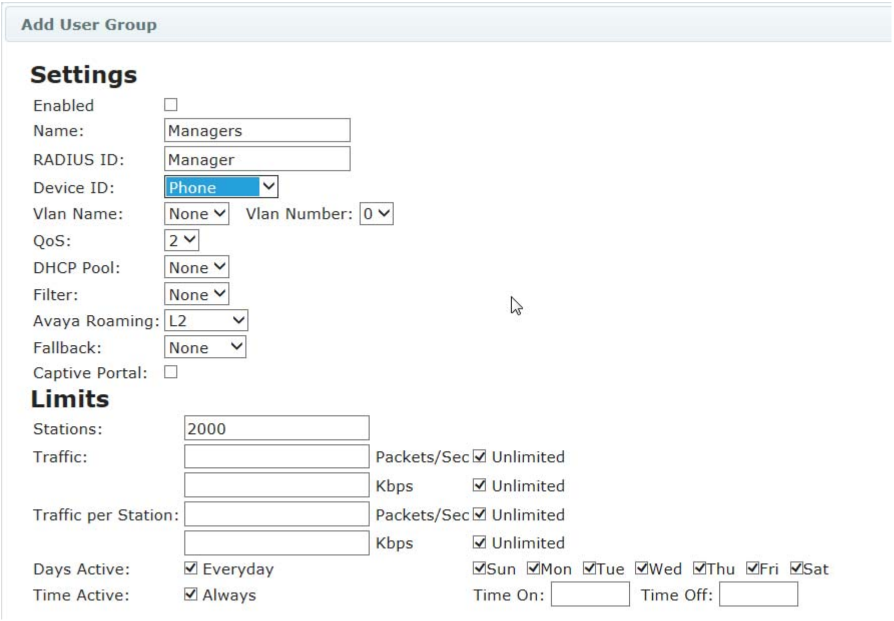
Using Groups

User accounts are used to authenticate wireless clients that want to associate to the AP. These accounts are established in one of two ways, using the **Security> Internal Radius** window or the **Security> External Radius** window. In either case, you may select a user group for the user, and that user group's settings will apply to the user:

- Internal Radius—when you add or modify a user entry, select a user group to which the user will belong.
- External Radius—when you add or modify a user account, specify the **Radius ID** for the user group to which the user will belong. This must be the same Radius ID that was entered in the Group Management window. When the user is authenticated, the external Radius server will send the Radius ID to the AP. This will allow the AP to identify the group to which the user belongs.

Group Management

This window allows you to manage groups (create, edit and delete), assign usage limits and other parameters on a per group basis, and configure the Captive Portal functionality.



Add User Group

Settings

Enabled □
Name: Managers
RADIUS ID: Manager
Device ID: Phone
Vlan Name: None Vlan Number: 0
QoS: 2
DHCP Pool: None
Filter: None
Avaya Roaming: L2
Fallback: None
Captive Portal: □

Limits

Stations: 2000
Traffic: Packets/Sec ☑ Unlimited
Kbps ☑ Unlimited
Traffic per Station: Packets/Sec ☑ Unlimited
Kbps ☑ Unlimited
Days Active: ☑ Everyday ☑Sun ☑Mon ☑Tue ☑Wed ☑Thu ☑Fri ☑Sat
Time Active: ☑ Always Time On: Time Off:

Figure 276. Adding a Group

Procedure for Managing Groups

1. To create a new group, click the **Add** button. The **Add User Group** dialog appears. You may create up to 16 groups.

   To configure and enable this group, proceed with the following steps.

2. **Enabled**: Check this box to enable this group or leave it blank to disable it. When a group is disabled, users that are members of the group will behave as if the group did not exist. In other words, the options

configured for the SSID will apply to the users, rather than the options configured for the group.

3. **Name**: Enter a new group name. Y

4. **RADIUS ID**: Enter a unique Radius ID for the group, to be used on an external Radius server. When adding a user account to the external server, this Radius ID value should be entered for the user. When the user is authenticated, Radius sends this value to the AP. This tells the AP that the user is a member of the group having this Radius ID.

5. **Device ID**: You may select a device type from this drop-down list, for example, **Notebook**, **phone**, **iPhone**, or **Android**. This allows you to apply the group settings only if a station authenticates as a user that is a member of the group and the station's device type matches **Device ID.** Select **none** if you do not want to consider the device type. If you have a Radius ID you should not enter a Device ID.

6. **VLAN Name**: (Optional) From the drop-down list, select a previously defined VLAN for this user's traffic to use (see **"VLAN" on page 391**).This user group's VLAN settings supersede Dynamic VLAN settings (which are passed to the AP by the Radius server). To avoid confusion, we recommend that you avoid specifying the VLAN for a user in two places.

7. **QoS**: (Optional) Select a value in this field for QoS (Quality of Service) priority filtering. The QoS value must be one of the following:

   - 0—The lowest QoS priority setting, where QoS makes its best effort at filtering and prioritizing data, video and voice traffic without compromising the performance of the network. Use this setting in environments where traffic prioritization is not a concern.
   - 1—Medium; QoS prioritization is aggregated across all traffic types.
   - 2—High, normally used to give priority to video traffic.
   - 3—The highest QoS priority setting, normally used to give priority to voice traffic.

The QoS setting you define here will prioritize wireless traffic for this group versus other traffic, as described in **"Understanding QoS Priority on the Wireless AP" on page 450**. The default value for this field is 2.

8. **DHCP Pool**: (Optional) To associate an internal DHCP pool to this group, select it from the pull--down list. Only one pool may be assigned. An internal DHCP pool must be created before it can be assigned. To create a DHCP pool, go to **"DHCP Server" on page 408**.

9. **Filter**: (Optional) If you wish to apply a set of filters to this user group's traffic, select the desired Filter List. See **"Filters" on page 538**.

10. **Avaya Roaming**: (Optional) For this group, select roaming behavior. Select **L2&L3** to enable fast roaming between radios or APs at Layer 2 and Layer 3. If you select **L2**, then roaming uses Layer 2 only. You may only select fast roaming at Layers 2 and 3 if this has been selected in Global Settings (Radio). You may select **Off** to disable fast roaming. See **"Understanding Fast Roaming" on page 487**.

11. **Fallback**: Network Assurance checks network connectivity for the AP. When Network Assurance detects a failure, perhaps due to a bad link or WDS failure, if Fallback is set to **Disable** the AP will automatically disable this group of users. This will disassociate current clients, and prevent new clients from associating. Since the AP's network connectivity has failed, this gives clients a chance to connect to other, operational parts of the wireless network. No changes are made to WDS configuration. See Step a on page 427 for more information on Network Assurance.

12. **Captive Portal**: (Optional) Check this box if you wish to enable the Captive Portal functionality. This will open a **Captive Portal** details section in the window, where your captive portal parameters may be entered. This feature may be used to display a splash screen when a user first associates to the wireless network. After that, it can (optionally) redirect the user to an alternate URL. See **"SSID Management—Captive Portal" on page 462** for details of captive portal usage and configuration. Note that the Group Management window only allows you to set up an **Internal Splash** page and a **Landing Page URL**. The authentication

options that are offered on the SSID Management page are not offered here. Since the group membership of a user is provided to the AP by a Radius server, this means the user has already been authenticated.

Group Limits

The Limits section allows you to limit the traffic or connection times allowed for this user group. Note that the Radios—Global Settings window and the SSID management windows also have options to limit the number of stations, limit traffic, and/or limit connection times. If limits are set in more than one place, all limits will be enforced:

- As soon as any station limit is reached, no new stations can associate until some other station has terminated its association. See Step 15 on page 497 in Global Settings (Radio) for a list of places where station limits are set.
- As soon as any traffic limit is reached, it is enforced.
- If any connection date/time restriction applies, it is enforced.

You can picture this as a logical AND of all restrictions. For example, suppose that a station's SSID is available MTWTF between 8:00am and 5:00pm, and the User Group is available MWF between 6:00am and 8:00pm, then the station will be allowed on MWF between 8:00am and 5:00pm.

To eliminate confusion, we recommend that you configure one set of limits, but not multiple limits.

13. **Stations**: Enter the maximum number of stations allowed on this group. The default is 2000.

14. **Overall Traffic**: Check the **Unlimited** checkbox if you do not want to place a restriction on the traffic for this group, or enter a value in the **Packets/Sec** or **Kbps** field and make sure that the **Unlimited** box is unchecked to force a traffic restriction.

15. **Traffic per Station**: Check the **Unlimited** checkbox if you do not want to place a restriction on the traffic per station for this group, or enter a value in the **Packets/Sec** or **Kbps** field and make sure that the Unlimited box is unchecked to force a traffic restriction.

16. **Days Active**: Choose **Everyday** if you want this group to be active every day of the week, or select only the specific days that you want this group to be active. Days that are not checked are considered to be the inactive days.

17. **Time Active**: Choose **Always** if you want this group active without interruption, or enter values in the **Time On** and **Time Off** fields to limit the time that group members may associate.

18. Click **OK** when done.

19. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Radios

The radio windows allow you to configure individual radios, establish settings for classes of radios, configure advanced RF features, and more.

APs have a fast roaming feature, allowing them to maintain sessions for applications such as voice, even while users cross boundaries between APs. Fast roaming is set up in the Global Settings (Radio) window and is discussed in:

- **"Understanding Fast Roaming" on page 487**

Radios are configured using the following windows:

- **"Radio Settings" on page 488**
- **"Global Settings (Radio)" on page 493**
- **"Global Settings .11a" on page 507**
- **"Global Settings .11bg" on page 510**
- **"Global Settings .11n" on page 514**
- **"Global Settings .11ac" on page 516**
- **"Advanced RF Settings" on page 519**
- **"Intrusion Detection" on page 525**
- **"LED Settings" on page 533**
- **"DSCP Mappings" on page 534**
- **"Roaming Assist" on page 535**

Understanding Fast Roaming

See also, **"Fast Transition Configuration" on page 496.**

To maintain sessions for real-time data traffic, such as voice and video, users must be able to maintain the same IP address through the entire session. With traditional networks, if a user crosses VLAN or subnet boundaries (i.e., roaming between domains), a new IP address must be obtained.

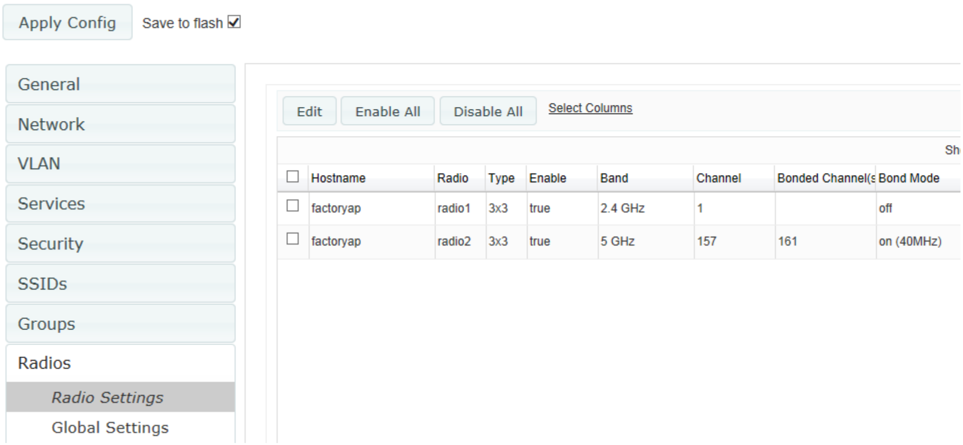
Fast Roaming is configured on two pages. To enable the fast roaming options that you want to make available on your AP, see Step 27 to Step 29 in **"Global**

Settings (Radio)" on page 493. To choose which of the enabled options are used by an SSID or Group, see **"Procedure for Managing General Settings" on page 455** or **"Procedure for Managing Groups" on page 482**.

Radio Settings

This window allows you to enable/disable radios, define the wireless mode for each radio, specify the channel to be used and the cell size for each radio, lock the channel selection, establish transmit/receive parameters, and reset channels.

For devices running AOSLite, such as the WAP9112, radio bands are fixed and may not be changed. An additional setting allows you to ***Disable 802.11b*** *to disallow connections from 802.11b clients.*



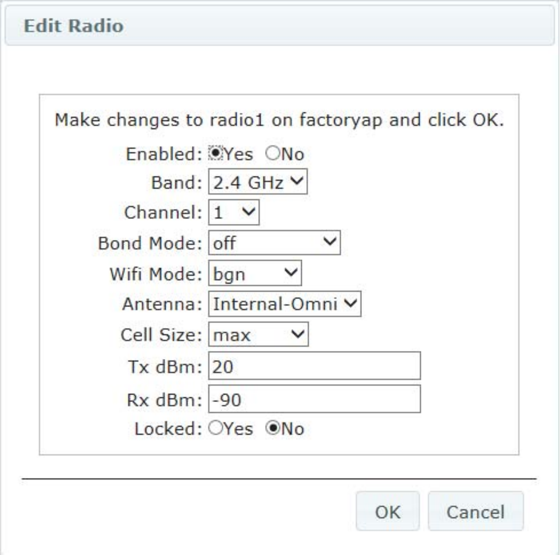
□	Hostname	Radio	Type	Enable	Band	Channel	Bonded Channel(s	Bond Mode
□	factoryap	radio1	3x3	true	2.4 GHz	1		off
□	factoryap	radio2	3x3	true	5 GHz	157	161	on (40MHz)

Figure 277. Radio Settings

Procedure for Manually Configuring a Particular Radio

1. Select the desired radio's checkbox on the left, and then click the **Edit** button. The **Edit Radio** dialog appears.

2. **Enabled**: set this to **Yes** to enable the radio, or set it to **No** to disable it.



Edit Radio

Make changes to radio1 on factoryap and click OK.

Enabled: ● Yes ○ No

Band: 2.4 GHz

Channel: 1

Bond Mode: off

Wifi Mode: bgn

Antenna: Internal-Omni

Cell Size: max

Tx dBm: 20

Rx dBm: -90

Locked: ○ Yes ● No

Figure 278. Changing Radio Settings

3. **Band**: select the wireless band for this radio from the choices available in the drop-down menu, either **2.4GHz** or **5 GHz**. Note that the band will change automatically, if necessary, based on the channel that you select. Choosing the **5GHz** band will automatically select adjacent channels if bonding is in use.

   One of the radios must be set to **monitor** mode to support Spectrum Analyzer, Radio Assurance (loopback testing), and Intrusion Detection features.

4. In the **Channel** column, select the channel you want this radio to use from the channels available in the drop-down list.

   As mandated by FCC/IC law, APs continually scan for signatures of military radar. If such a signature is detected, the AP will switch operation from conflicting channels to new ones. The AP will switch back to the original channel after 30 minutes if the channel is clear. If a particular radio was turned off because there were no available channels not affected by radar, the AP will now bring that radio back up after 30 minutes if that channel is clear. The 30 minute time frame complies with FCC/IC regulations.

5. **Bond:**

   - **Off**—Do not bond this channel to another channel.
   - **On (40MHz)**—Bond this channel to an adjacent channel. The bonded channel is selected automatically by the AP based on the **Channel** selected in Step 4. You will receive an error message if an overlapping channel is used by another radio. The choice of bonded channel is static—fixed once the selection is made.
   - **On (80MHz)**—Bond four adjacent channels, selected automatically based on the **Channel** selected in Step 4. You will receive an error message if an overlapping channel is used by another radio. The choice of banded channels is static—fixed once the selection is made. This option is only displayed for APs with 802.11ac radios.

   For 802.11n APs, this works together with the channel bonding options selected on the Global Settings .11n page.

6. **WiFi Mode**: select the IEEE 802.11 wireless mode (or combination) that you want to allow on this radio. When you select a WiFi Mode for a particular radio, your selection in the **Channel** column will be checked to ensure that it is a valid choice for that WiFi Mode. You will not be able to set the radio to 802.11n or 802.11ac if that mode is not supported and licensed on the AP, or if it is disabled on the Global Settings .11n or Global Settings .11ac page.

By selecting appropriate WiFi Modes for the radios on your APs, you can greatly improve wireless network performance. For example, if you have 802.11b and 802.11ac stations using the same radio, throughput on that radio is reduced greatly for the 802.11ac stations. By supporting 802.11b stations only on selected radios in your network, the rest of your 802.11a or 11ac radios will have greatly improved performance. Take care to ensure that your network provides adequate coverage for the types of stations that you need to support.

Load balancing automatically groups client devices by performance. See Step 24 in **"Global Settings (Radio)" on page 493**.

7. **Antenna**: This shows the type of antenna in use, based on the wireless band you selected for the radio.

8. **Cell Size**: Select **auto** to allow the optimal cell size to be automatically computed. To set the cell size yourself, choose either **small**, **medium**, **large**, or **max** to use the desired pre-configured cell size, or choose **manual** to define the wireless cell size manually. If you choose Manual, you must specify the transmit and receive power—in dB—in the **Tx dBm** (transmit) and **Rx dBm** (receive) fields. The default is **max**. If you select a value other than **auto**, the cell size will not be affected by cell size auto configuration. Note that ultra low power **Tx dBm** settings are possible. Values from -15dB to 5dB are provided specifically to help in high density 2.4 GHz environments. Note that some older AP models will only accept 0dBm as a minimum value.

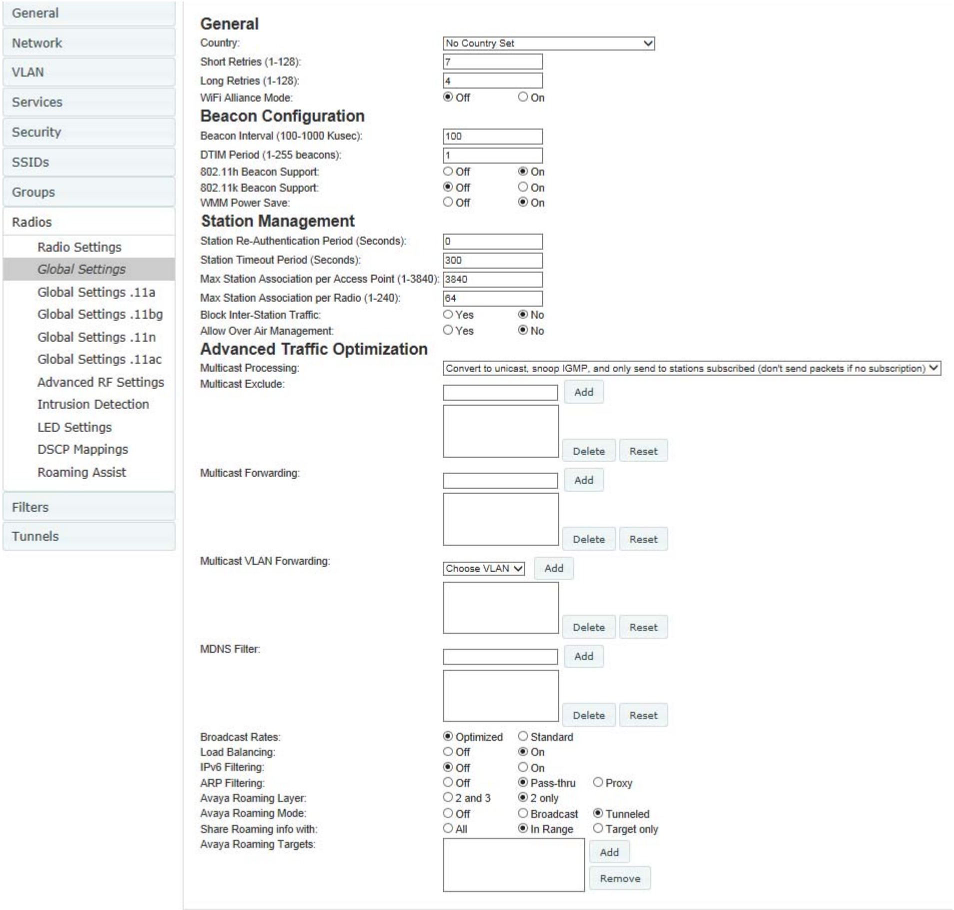
   When other APs are within listening range of this one, setting cell sizes to **Auto** allows the AP to change cell sizes so that coverage between cells is maintained. Each cell size is optimized to limit interference between sectors of other APs on the same channel. This eliminates the need for a network administrator to manually tune the size of each cell when installing multiple APs. In the event that an AP or an individual radio goes offline, an adjacent AP can increase its cell size to help compensate.

   The number of users and their applications are major drivers of bandwidth requirements. The network architect must account for the number of users within the AP's cell diameter. In a large office, or if multiple APs are in use, you may choose **Small** cells to achieve a higher data rate, since walls and other objects will not define the cells naturally.

9. **Locked:** select **Yes** if you want to lock in your channel selection so that the autochannel operation (see Advanced RF Settings) cannot change it.
10. Click **OK** when done.
11. Buttons at the bottom of the list allow you to **Enable All** or **Disable All** Radios.
12. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Global Settings (Radio)

This window allows you to establish global radio settings. Global radio settings include enabling or disabling all radios (regardless of their operating mode), and changing settings for beacons, station management, and advanced traffic optimization—including multicast processing, load balancing, and roaming. Changes you make on this page are applied to all radios, without exception.



General

Country: No Country Set

Short Retries (1-128): 7

Long Retries (1-128): 4

WiFi Alliance Mode: ● Off ○ On

Beacon Configuration

Beacon Interval (100-1000 Kusec): 100

DTIM Period (1-255 beacons): 1

802.11h Beacon Support: ○ Off ● On

802.11k Beacon Support: ● Off ○ On

WMM Power Save: ○ Off ● On

Station Management

Station Re-Authentication Period (Seconds): 0

Station Timeout Period (Seconds): 300

Max Station Association per Access Point (1-3840): 3840

Max Station Association per Radio (1-240): 64

Block Inter-Station Traffic: ○ Yes ● No

Allow Over Air Management: ○ Yes ● No

Advanced Traffic Optimization

Multicast Processing: Convert to unicast, snoop IGMP, and only send to stations subscribed (don't send packets if no subscription)

Multicast Exclude:

Multicast Forwarding:

Multicast VLAN Forwarding: Choose VLAN

MDNS Filter:

Broadcast Rates: ● Optimized ○ Standard

Load Balancing: ○ Off ● On

IPv6 Filtering: ● Off ○ On

ARP Filtering: ○ Off ● Pass-thru ○ Proxy

Avaya Roaming Layer: ○ 2 and 3 ● 2 only

Avaya Roaming Mode: ○ Off ○ Broadcast ● Tunneled

Share Roaming info with: ○ All ● In Range ○ Target only

Avaya Roaming Targets:

Figure 279. Global Settings—Radios (Avaya OS settings shown)

Procedure for Configuring Global Radio Settings

APs that run AOS Lite (WAP9112/WAP9114) support a small subset of the settings below. You will only see the following settings: Country, 802.11k Beacon Support, Fast Transition Configuration, and Block Inter-Station Traffic.

1. **Country**: This is a display-only value. Once a country has been set, it may not be changed.

   The channels that are available for assignment to a particular radio will differ, depending on the country of operation. If **Country** is set to **United States**, then 21 channels are available for 802.11a/n.

   If no country is displayed, the channel set defaults to channels and power levels that are legal worldwide—this set only includes the lower eight 5 GHz channels.

2. **Short Retries**: This sets the maximum number of transmission attempts for a frame, the length of which is less than or equal to the RTS Threshold, before a failure condition is indicated. The default value is 7. Enter a new value (1 to 128) in the **Short Retry Limit** field if you want to increase or decrease this attribute.

3. **Long Retries**: This sets the maximum number of transmission attempts for a frame, the length of which is greater than the RTS Threshold, before a failure condition is indicated. The default value is 4. Enter a new value (1 to 128) in the **Long Retry Limit** field if you want to increase or decrease this attribute.

4. **Wi-Fi Alliance Mode**: Set this **On** if you need AP behavior to conform completely to Wi-Fi Alliance standards. This mode is normally set to **Off**.

Beacon Configuration

5. **Beacon Interval**: When the AP sends a beacon, it includes with it a beacon interval, which specifies the period of time before it will send the beacon again. Enter the desired value in the **Beacon Interval** field, between 20 and 1000 Kusecs. A Kusec is 1000 microseconds = 1 millisecond. The value you enter here is applied to all radios.

6. **DTIM Period**: A DTIM (Delivery Traffic Indication Message) is a signal sent as part of a beacon by the AP to a client device in sleep mode, alerting the device to broadcast traffic awaiting delivery. The **DTIM Period** is a multiple of the **Beacon Interval**, and it determines how often DTIMs are sent out. By default, the DTIM period is 1, which means that it is the same as the beacon interval. Enter the desired multiple, between 1 and 255. The value you enter here is applied to all radios.

7. **802.11h Beacon Support**: This option enables beacons on all of the AP's radios to conform to 802.11h requirements, supporting dynamic frequency selection (DFS) and transmit power control (TPC) to satisfy regulatory requirements for operation in Europe.

8. **802.11k Beacon Support**: 802.11k offers faster and more efficient roaming. When enabled, each beacon lists the channels that nearby APs offer. This supports improved channel scanning, resulting in faster roam times and increased station battery life due to shorter scan times since the station knows where to look for nearby APs. The AP will also respond to requests from stations for an 802.11K Neighbor Report with additional information about nearby APs. This setting is only available for APs running Avaya OS Release 6.6 and above. It is enabled by default.

9. **WMM Power Save**: Click **On** to enable Wireless Multimedia Power Save support, as defined in IEEE802.11e. This option saves power and increases battery life by allowing the client device to doze between packets to save power, while the AP buffers downlink frames.

Fast Transition Configuration

This feature is currently available only on APs that run AOS Lite Release 8.0 or above (WAP9112/WAP9114).

Fast Transition (FT) Roaming (IEEE802.11r) reduces the time it takes a station to roam from one AP to another by pre-authenticating the station to neighboring APs. This is especially useful for sensitive voice-enabled clients, allowing them to roam more smoothly and reliably.

FT requires 802.11k to be enabled (see Step 8 above), and WPA2 authentication (see **"Global Settings" on page 428** and **"SSID Management—Authentication/ Encryption" on page 458**).

FT is enabled or disabled per SSID. After configuring the settings below, turn on **802.11r Support** for each SSID that is to run FT. See **"SSID Management—General Settings" on page 455**.

10. **Mobility Domain**: Information about stations that is used for Fast Transition is shared only between APs that are members of the same Mobility Domain. You should assign the same value to all APs that stations will roam between with FT. Enter a lower-case 4-character hexadecimal value (0000—ffff). The default is 0000.

11. **FT-over-DS** (Fast Transition over Distributed System): When FT-over-DS is on, fast transition takes place through the distributed system, i.e., the station contacts the AP it is currently connected to, and this AP requests authentication from the AP to which the station is roaming. When FT-over-DS is off, fast transition takes place "over the air", i.e., the station requests authentication directly from the AP to which it is roaming. In either case, the approval is received quickly since it has been pre-authenticated. FT-over-DS is off by default.

Station Management

12. **Station Re-Authentication Period**: This specifies an interval (in seconds) for station reauthentications. This is the minimum time period between station authentication attempts, enforced by the AP. This feature is part of the Avaya Advanced RF Security Manager (RSM).

13. **Station Timeout Period**: Specify a time (in seconds) in this field to define the timeout period for station associations.

14. **Max Station Association per AP**: This option allows you to define how many station associations are allowed per AP. Note that the **Max Station Association per radio** limit (below) may not be exceeded. If you have an unlicensed AP, this value is set to 1, which simply allows you to test the ability to connect to the AP.

15. **Max Station Association per Radio**: This defines how many station associations are allowed per radio. Note that in addition to **Max Station Association per AP** above, the SSID Management—Limits and Group Management windows also have a station limit option, and the windows for Global Settings .11a and Global Settings .11bg also have **Max Stations** settings. If multiple station limits are set, all will be enforced. As soon as any limit is reached, no new stations can associate until some other station has terminated its association.

16. **Block Inter-Station Traffic:** This option allows you to block or allow traffic between wireless clients that are associated to the AP. Choose either **Yes** (to block traffic) or **No** (to allow traffic). The default is **No**.

17. **Allow Over Air Management**: Choose **Yes** to enable management of the AP via the radios, or choose **No** (recommended) to disable this feature.

Advanced Traffic Optimization

18. **Multicast Processing:** This sets how multicast traffic is handled. Multicast traffic can be received by a number of subscribing stations at the same time, thus saving a great deal of bandwidth. In some of the options below, the AP uses IGMP snooping to determine the stations that are subscribed to the multicast traffic. IGMP (Internet Group Management Protocol) is used to establish and manage the membership of multicast groups.

    Multicast packet handling options are only applicable to downstream traffic transmitted from the AP to wireless stations. Select one of the following options:

- **Send multicasts unmodified**. This option is useful when multicast is not needed because no video or audio streaming is required or when it is used only for discovering services in the network. An example of this type of multicast usage is the Bonjour protocol used by AppleOS devices. This is the default setting.

The next three options convert multicast to unicast. Packets are sent directly to the stations at the best possible data rates. Because they are unicast packets, they will also benefit from 802.11 acknowledges. This approach significantly improves the quality of the voice and video multicast streams.

- **Convert to unicast and send unicast packets to all stations**. This option is useful when you need to stream voice or video traffic and none of the associated stations have the capability to subscribe to the multicast group through the use of IGMP join messages, but all of them need to receive the stream with good quality.
- **Convert to unicast, snoop IGMP, and only send to stations subscribed (send as multicast if no subscription)**. This option is useful when you need to stream voice or video multicast traffic to all stations, but some stations are capable of subscribing to multicast groups while other stations are not. The stations that do not subscribe will not benefit from conversion to unicast; their video or voice quality may be compromised.
- **Convert to unicast, snoop IGMP, and only send to stations subscribed (don't send packet if no subscription)**. This option is useful in well controlled environments when you need to stream voice or video multicast traffic only to stations that are capable of subscribing to multicast groups and there is no need for the rest of the stations to receive the data stream.

19. **Multicast Exclude:** This is a list of multicast IP addresses that will not be subject to multicast-to-unicast conversion. This list is useful on networks where applications such as those using multicast Domain Name System (mDNS) are in use. For example, Apple Bonjour finds local network

devices such as printers or other computers using mDNS. By default, the list contains the IPv4 multicast address for Apple Bonjour/ mDNS: 224.0.0.251.

To add a new IP address to the list, type it in the field and click the **Add** button to its right. You may only enter IP addresses - host names are not allowed. This is because mDNS is a link local multicast address, and does not require IGMP to the gateway.

To remove an entry, select it in the list and click **Delete**. To remove all entries from the list, click **Reset** (i.e., any unsaved changes are erased from the list).

20. **Multicast Forwarding**

Multicast Forwarding is an Avaya feature that forwards selected multicast traffic between wired VLANs and wireless SSIDs. For example, Apple devices use mDNS to advertise and find services, using local network multicasts that are not routed. This creates an issue when you are using Apple devices on the Wireless LAN, and have other devices that provide services connected on the wired infrastructure in a different VLAN, for example, printers and AppleTV devices. One way to address this issue is to set up multicast forwarding between the wireless SSID and the wired VLAN. This requires the wired VLAN to be trunked to the AP. Once configured correctly, mDNS traffic will be forwarded from the specified wireless network(s) to the specified wired VLANs and vice-versa, subject to any mDNS service filtering defined (Step 22).

Use multicast forwarding together with multicast VLAN forwarding (Step 21) and mDNS filtering (Step 22) to make services available across VLANs as follows:

- In **Multicast Forwarding**, enter a list of multicast addresses that you want forwarded, for example, 224.0.0.251 (the multicast address for Bonjour).
- In **Multicast VLAN Forwarding**, enter a list of VLANs that participate in the multicast forwarding.

- In **MDNS Filter**, specify the mDNS service types that are allowed to be forwarded.
  - If you leave this field blank, then there is ***no*** filter, and *mDNS packets for all service types are passed*.
  - If you enter service types, then this acts as an allow filter, and *mDNS packets are passed **only** for the listed service types*.

  Note that mDNS filtering may be used to filter the mDNS packet types that are forwarded within the same VLAN. Also, in conjunction with multicast forwarding, it may be used to filter the mDNS packet types that are forwarded across configured VLANs.

After you have entered these settings, when multicast packets arrive from the wired network from one of the **Multicast Forwarding Addresses** on any VLAN specified in **Multicast VLAN Forwarding,** they are forwarded to the corresponding wireless SSID for that VLAN.

Multicast packets coming in from the wireless network on an SSID tied to one of the specified VLANs and matching one of the **Multicast Forwarding Addresses** are forwarded to the specified VLANs on the wired network.

No modifications are made to the forwarded packets – they are just forwarded between specified VLANs and associated SSIDs.

Avaya strongly recommends the use of MDNS Filters (Step) *when using multicast forwarding. Only allow required services to be forwarded.*

Carefully monitor results, as forwarding may flood your network with multicast traffic. Experience has shown Bonjour devices to be very chatty. Also note that since this is link local multicast traffic, it will be sent to every wired port in the VLAN, as IGMP snooping does not work with link local multicast addresses.

To specify **Multicast Forwarding Addresses:** enter each IP address in the top field and click the **Add** button to its right. You may only enter IPv4 multicast addresses - host names are not allowed. To remove an entry, select it in the list and click **Delete**. To reset the list to the values in the

WOS database, click **Reset** (i.e., any unsaved changes are erased from the list).

21. **Multicast VLAN Forwarding:** This is a list of VLANs that participate in the multicast forwarding. Please see the description of multicast forwarding in Step 20 above.

The VLANs you enter must be explicitly defined (see ***"VLAN" on page 391****) in order to participate in multicast forwarding. In fact, the AP discards packets from undefined VLANs.*

To add a new VLAN to the list, enter its number or name in the top field and click the **Add** button to its right. You may enter multiple VLANs at once, separated by a space. To remove an entry, select it in the list and click **Delete**. To reset the list to what is in the WOS database, click **Reset** (i.e., any unsaved changes are erased from the list).

These VLANs must be trunked to the AP from the LAN switch, and be defined on the AP. See **"VLAN Management" on page 392** and **"SSID Management" on page 454**.

Note that Multicast Forwarding and mDNS Filtering capabilities also work if both devices are wireless. For example, let's say that AppleTV is using wireless to connect to an SSID that is associated with VLAN 56, and the wireless client is on an SSID that is associated with VLAN 58. Normally the wireless client would not be able to use Bonjour to discover the AppleTV because they are on separate VLANs. But if you add 224.0.0.251 to the ***Multicast Forwarding*** *list, then add VLANs 56 and 58 to the* ***Multicast VLAN Forwarding*** *list, then the wireless client will be able to discover the AppleTV. In this same scenario you could add AppleTV to the* ***MDNS Filter*** *list so that only MDNS packets for the AppleTV service type would be forwarded between VLANs 56 and 58.*

Note that all the VLANs that you add to this list do not have to be associated with SSIDs. As an example, say that AppleTV is on the wired network on VLAN 56, while the wireless device is connected to an SSID that is associated to VLAN 58. In this case, VLAN 56 and 58 need to be defined on the AP but only VLAN 58 needs to be associated to a SSID.

22. **MDNS Filter:** There are many different types of services that may be specified in multicast query and response packets. The mDNS filters let you restrict forwarding, so that multicast packets are forwarded only for the services that you explicitly specify. This list may be used to restrict the amount of Apple Bonjour multicast traffic forwarding. For example, you may restrict forwarding to just AppleTV and printing services. Please see the description of multicast forwarding in Step 20 above.

    The **MDNS Filter** operates as follows:

    - If you leave this field blank, then there is ***no*** filter, and *mDNS packets for all service types are passed*.
    - If you enter service types, then this acts as an allow filter, and *mDNS packets are passed **only** for the listed service types*.

    To add an mDNS packet type to the list of packets that may be forwarded, type it in the top field, or select an option from the drop-down list and click the **Add** button to its right. The drop-down list offers packet types such as **AirTunes**, **Apple-TV**, **iChat**, **iPhoto**, **iTunes**, **iTunes-Home-Sharing**, **Internet-Printing**, **Mobile-Device-Sync**, and **Secure-Telnet**.

    For example, to allow mirroring of an iPad on an Apple-TV, select **Apple-TV**.

    You may define your own type if you do not see the service you want in the drop-down list. Simply enter the mDNS service name that you would like to allow through. Custom mDNS packet types must be prefixed with an underscore, e.g., **_airvideoserver**.

    To remove an entry, select it in the list and click **Delete**. To reset the list to the values in the WOS database, click **Reset** (i.e., any unsaved changes are erased from the list).

23. **Broadcast Rates**: This changes the rates of broadcast traffic sent by the AP (including beacons). When set to **Optimized**, each broadcast or multicast packet that is transmitted on each radio is sent at the lowest transmit rate used by any client associated to that radio at that time. This results in each radio broadcasting at the highest AP TX data rate that can be heard by all associated stations, improving system performance. The rate is determined dynamically to ensure the best broadcast/multicast performance possible. The benefit is dramatic. Consider a properly designed network (having -70db or better everywhere), where virtually every client should have a 54Mbps connection. In this case, broadcasts and multicasts will all go out at 54Mbps vs. the standard rate. Thus, with broadcast rate optimization on, broadcasts and multicasts use between 2% and 10% of the bandwidth that they would in Standard mode.

    When set to **Standard** (the default), broadcasts are sent out at the lowest basic rate only—6 Mbps for 5GHz clients, or 1 Mbps for 2.4GHz clients. The option you select here is applied to all radios.

24. **Load Balancing:** Wi-Fi is a shared medium and only one device can transmit data at any time. Faster devices supporting 802.11ac standards have to wait until the slower devices finish transmitting data. This brings down the overall throughput of the network. For example, an 802.11n client operates more than four times slower than an 802.11ac client, and thus will take four times more air time to communicate a given amount of data. This starves the available bandwidth from faster clients, reducing performance significantly. Avaya solves this issue with an innovative technique which automatically separates devices onto different radios by their speeds and capability.

    The technique identifies station capabilities based on fingerprinting and automatically groups devices by performance. It works on all modes (802.11a/b/g/n/ac) and bands (2.4GHz and 5GHz). This results in improved performance for every WLAN client and optimized use of wireless radio resources. Factors including wireless band, number of spatial streams, 802.11ac and 802.11n capability, and signal to noise ratio are considered.

This feature also provides automatic load balancing designed to distribute wireless stations across multiple radios rather than having stations associate to the closest radios with the strongest signal strength, as they normally would. In wireless networks, the station selects the radio to which it will associate. The AP cannot actually force load balancing, however it can "encourage" stations to associate in a more optimal fashion to underused radios of the most advantageous type. This option enables or disables active load balancing between the AP radios.

If you select **On** and a radio is not the best choice for network performance, that radio will send an "AP Full" message in response to Probe, Association, or Authentication requests. This deters persistent clients from forcing their way onto overloaded radios.

Note that this type of load balancing is **not** used if:

- A station is re-associating—if it was already associated to this radio, it is allowed back on this radio immediately. This prevents the station from being bounced between different radios.
- The radio's **Band**, **WiFi Mode,** and **Channel** settings are not at their default values. For example, if the radio's WiFi mode is set to 11n-only, load balancing will not be used.
- If station counts (specified at the radio, SSID, or band level) are already exceeded.
- If a station has already been turned down a number of times when attempting to associate, i.e., the station will eventually be allowed onto the radio after a number of attempts have failed.

Choose **Off** to disable load balancing. Load balancing is **Off** by default.

25. **IPv6 Filtering**: this setting allows blocking of IPv6 traffic which may be a concern for IT managers. The Avaya AP currently bridges IPv6 traffic. Set IPv6 filtering **On** if you wish to prevent the forwarding of IPv6 packets through the AP in both directions—wired network to wireless and wireless network to wired. The default is **On**.

26. **ARP Filtering:** Address Resolution Protocol finds the MAC address of a device with a given IP address by sending out a broadcast message requesting this information. ARP filtering allows you to reduce the proliferation of ARP messages by restricting how they are forwarded across the network.

    You may select from the following options for handling ARP requests:

    - **Off**: ARP filtering is disabled. ARP requests are broadcast to radios that have stations associated to them.
    - **Pass-thru**: The AP forwards the ARP request. It passes along only ARP messages that target the stations that are associated to it. This is the default value.
    - **Proxy**: The AP replies on behalf of the stations that are associated to it. The ARP request is not broadcast to the stations.

    Note that the AP has a broadcast optimization feature that is always on (it is not configurable). Broadcast optimization restricts all broadcast packets (not just ARP broadcasts) to only those radios that need to forward them. For instance, if a broadcast comes in from VLAN 10, and there are no VLAN 10 users on a particular radio, then that radio will not send out that broadcast. This increases available air time for other traffic.

27. **Avaya Roaming Layer:**

28. **Avaya Roaming Mode:** This feature utilizes the Avaya Roaming Protocol ensuring fast and seamless roaming capabilities between radios or APs at Layer 2 and Layer 3 (as specified in Step 29), while maintaining security. Fast roaming eliminates long delays for re-authentication, thus supporting time-sensitive applications such as Voice over Wi-Fi (see **“Understanding Fast Roaming” on page 487** for a discussion of this feature). The roaming protocol uses a discovery process to identify other Avaya APs as fast roaming targets. This process has two modes:

    - **Broadcast**—the AP uses a broadcast technique to discover other APs that may be targets for fast roaming. This is the default.
    - **Tunneled**—in this Layer 3 technique, fast roaming target APs must be explicitly specified.

To enable fast roaming, choose **Broadcast** or **Tunneled**, and set additional fast roaming attributes (Step 29). To disable fast roaming, choose **Off**. If you enable Fast Roaming, the following ports **cannot** be blocked:

- **Port 22610**—reserved for Layer 2 roaming using UDP to share PMK information between APs.
- **Ports 15000 to 17999**—reserved for Layer 3 roaming (tunneling between subnets).

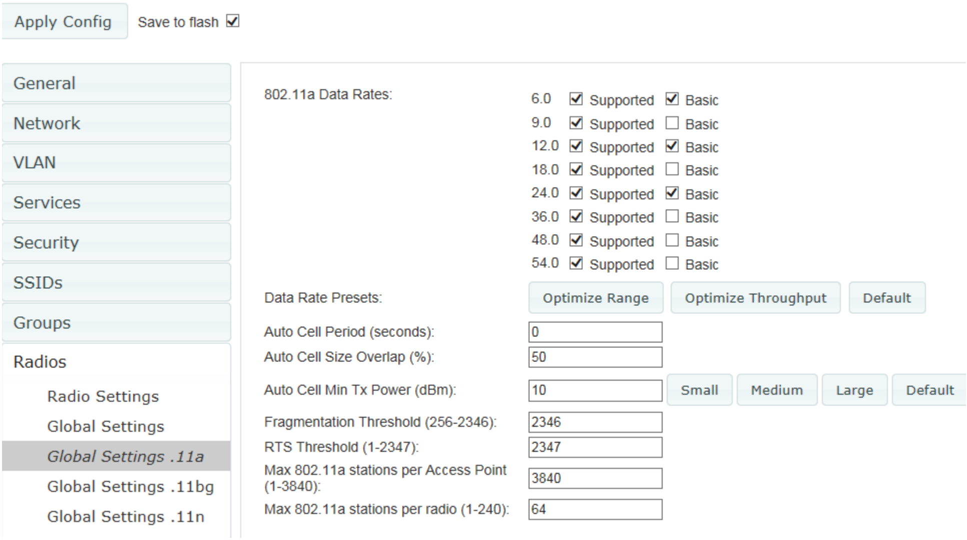
29. **Share Roaming Info With:** Three options allow your AP to share roaming information with all APs; just with those that are within range; or with specifically targeted APs. Choose either **All**, **In Range** or **Target Only**, respectively.

    a. **Avaya Roaming Targets:** If you chose **Target Only**, use this option to add target MAC addresses. Enter the MAC address of each target AP, then click on **Add** (add as many targets as you like). To find a target's MAC address, open the AP **Info** window on the target AP and look for radio **MAC Range**, then use the starting address of this range.

    To delete a target, select it from the list, then click **Delete**.

Global Settings .11a

This window allows you to establish global 802.11a radio settings. These settings include defining which 802.11a data rates are supported, enabling or disabling all 802.11a radios, and specifying the fragmentation and RTS thresholds for all 802.11a radios.



Save to flash ☑

802.11a Data Rates:

6.0	☑ Supported	☑ Basic
9.0	☑ Supported	□ Basic
12.0	☑ Supported	☑ Basic
18.0	☑ Supported	□ Basic
24.0	☑ Supported	☑ Basic
36.0	☑ Supported	□ Basic
48.0	☑ Supported	□ Basic
54.0	☑ Supported	□ Basic

Data Rate Presets:

Auto Cell Period (seconds): 0

Auto Cell Size Overlap (%): 50

Auto Cell Min Tx Power (dBm): 10

Fragmentation Threshold (256-2346): 2346

RTS Threshold (1-2347): 2347

Max 802.11a stations per Access Point (1-3840): 3840

Max 802.11a stations per radio (1-240): 64

Figure 280. Global Settings .11a

Procedure for Configuring Global 802.11a Radio Settings

1. **802.11a Data Rates:** The AP allows you to define which data rates are supported for all 802.11a radios. Select (or deselect) data rates by clicking in the corresponding **Supported** and **Basic** data rate check boxes.
   - **Basic Rate**—a wireless station (client) must support this rate in order to associate.
   - **Supported Rate**—data rates that can be used to transmit to clients.
2. **Data Rate Presets**: The wireless AP can optimize your 802.11a data rates automatically, based on range or throughput. Click **Optimize Range** to optimize data rates based on range, or click **Optimize Throughput** to

optimize data rates based on throughput. The **Default** button will take you back to the factory default rate settings.

To use the Autocell Size feature, any radios that will use autocell must have ***Cell Size*** *set to* ***auto****. It is not necessary for RF Monitor Mode to be turned on, or for there to be a radio set to monitor mode. See* **"RF Monitor" on page 520**

3. **Auto Cell Period (seconds)**: You may set up auto-configuration to run periodically, readjusting optimal cell sizes for the current conditions. Enter a number of seconds to specify how often auto-configuration will run. If you select **None**, then auto-configuration of cell sizing will not be run periodically. You do not need to run autocell often unless there are a lot of changes in the environment. If the RF environment is changing often, running autocell every twenty-four hours (86400 seconds) should be sufficient). The default value is **None**. If you wish to perform an immediate autocell procedure, please see **"The Configure APs Toolbar" on page 110**.

4. **Auto Cell Size Overlap (%)**: Enter the percentage of cell overlap that will be allowed when the AP is determining automatic cell sizes. For 100% overlap, the power is adjusted such that neighboring APs that hear each other best will hear each other at -70dB. For 0% overlap, that number is -90dB. The default value is **50%**.

5. **Auto Cell Min Tx Power (dBm)**: Enter the minimum transmit power that the AP can assign to a particular radio when adjusting automatic cell sizes. The default value is **10**. You may also set this in terms of minimum cell size: **Default**, **Large, Medium,** or **Small**.

6. **Fragmentation Threshold**: This is the maximum size for directed data packets transmitted over the 802.11a radio. Larger frames fragment into several packets, their maximum size defined by the value you enter here. Smaller fragmentation numbers can help to "squeeze" packets through in noisy environments. Enter the desired **Fragmentation Threshold** value in this field, between 256 and 2346.

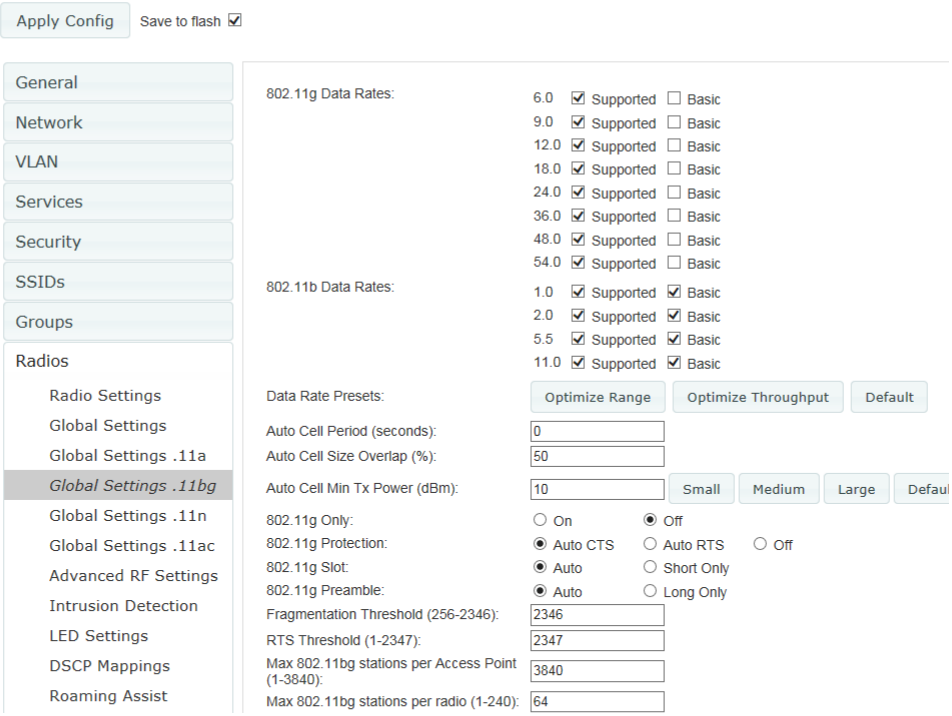
7. **RTS Threshold**: The Request To Send (RTS) Threshold specifies the packet size. Packets larger than the RTS threshold will use CTS/RTS prior to transmitting the packet—useful for larger packets to help ensure the success of their transmission. Enter a value between 1 and 2347.

8. **Max Stations per AP**: This defines how many total concurrent station associations are allowed for all 802.11a radios. If multiple station limits are set, all will be enforced. As soon as any limit is reached, no new stations can associate until some other station has terminated its association. See Step 15 on page 497 in Global Settings (Radio) for a list of places where station limits are set.

9. **Max Stations per Radio**: This defines how many station associations are allowed per 802.11a radio. If multiple station limits are set, all will be enforced. As soon as any limit is reached, no new stations can associate until some other station has terminated its association. See Step 15 on page 497 in Global Settings (Radio) for a list of places where station limits are set.

Global Settings .11bg

This window allows you to establish global 802.11b/g radio settings. These settings include defining which 802.11b and 802.11g data rates are supported, enabling or disabling all 802.11b/g radios, and specifying the fragmentation and RTS thresholds for all 802.11b/g radios.



802.11g Data Rates:	6.0	☑ Supported	□ Basic
	9.0	☑ Supported	□ Basic
	12.0	☑ Supported	□ Basic
	18.0	☑ Supported	□ Basic
	24.0	☑ Supported	□ Basic
	36.0	☑ Supported	□ Basic
	48.0	☑ Supported	□ Basic
	54.0	☑ Supported	□ Basic
802.11b Data Rates:	1.0	☑ Supported	☑ Basic
	2.0	☑ Supported	☑ Basic
	5.5	☑ Supported	☑ Basic
	11.0	☑ Supported	☑ Basic

Data Rate Presets: Optimize Range | Optimize Throughput | Default

Auto Cell Period (seconds): 0

Auto Cell Size Overlap (%): 50

Auto Cell Min Tx Power (dBm): 10 Small | Medium | Large | Defaul

802.11g Only: ○ On ● Off

802.11g Protection: ● Auto CTS ○ Auto RTS ○ Off

802.11g Slot: ● Auto ○ Short Only

802.11g Preamble: ● Auto ○ Long Only

Fragmentation Threshold (256-2346): 2346

RTS Threshold (1-2347): 2347

Max 802.11bg stations per Access Point (1-3840): 3840

Max 802.11bg stations per radio (1-240): 64

Figure 281. Global Settings .11bg

Note that 802.11b is disabled by default for Avaya OS, since 802.11b devices are becoming less and less common. These devices have a very slow data rate that drags down the performance of faster devices on the network. See Step 7 below.

Procedure for Configuring Global 802.11b/g Radio Settings

1. **802.11g Data Rates:** The AP allows you to define which data rates are supported for all 802.11g radios. Select (or deselect) 11g data rates by clicking in the corresponding **Supported** and **Basic** data rate check boxes.

   - **Basic Rate**—a wireless station (client) must support this rate in order to associate.
   - **Supported Rate**—data rates that can be used to transmit to clients.

2. **802.11b Data Rates**: This task is similar to Step 1, but these data rates apply only to 802.11b radios.

3. **Data Rate Presets**: The wireless AP can optimize your 802.11b/g data rates automatically, based on range or throughput. Click **Optimize Range** button to optimize data rates based on range, or click on the **Optimize Throughput** to optimize data rates based on throughput. **Default** will take you back to the factory default rate settings.

*To use the Autocell Size feature, any radios that will use autocell must have **Cell Size** set to **auto**. It is not necessary for RF Monitor Mode to be turned on, or for there to be a radio set to monitor mode. See* **"RF Monitor" on page 520**

4. **Auto Cell Period (seconds)**: You may set up auto-configuration to run periodically, readjusting optimal cell sizes for the current conditions. Enter a number of seconds to specify how often auto-configuration will run. If you enter **0**, then auto-configuration of cell sizing will not be run periodically. You do not need to run autocell often unless there are a lot of changes in the environment. If the RF environment is changing often, running autocell every twenty-four hours (86400 seconds) should be sufficient). The default value is **0**. If you wish to perform an immediate autocell procedure, please see **"The Configure APs Toolbar" on page 110**.

5. **Auto Cell Size Overlap (%)**: Enter the percentage of cell overlap that will be allowed when the AP is determining automatic cell sizes. For 100% overlap, the power is adjusted such that neighboring APs that hear each other best will hear each other at -70dB. For 0% overlap, that number is -90dB. The default value is **50%**.

6. **Auto Cell Min Tx Power (dBm)**: Enter the minimum transmit power that the AP can assign to a particular radio when adjusting automatic cell sizes. The default value is **10**. You may also set this in terms of minimum cell size: **Default**, **Large, Medium,** or **Small**.

7. **802.11g Only**: Choose **On** to restrict use to 802.11g mode only. In this mode, no 802.11b connections are allowed. Stations that only support 802.11b will not be able to associate. This is set to **On** by default for Avaya OS, to prevent performance from being unnecessarily slowed by older 802.11b devices that are becoming scarcer. This is set to **Off** by default for AOSLite.

8. **802.11g Protection**: You should select **Auto CTS** or **Auto RTS** to provide automatic protection for all 802.11g radios in mixed networks (802.11 b and g). You may select **Off** to disable this feature, but this is not recommended. Protection allows 802.11g stations to share a particular radio with older, slower 802.11b stations. Protection avoids collisions by preventing 802.11b and 802.11g stations from transmitting simultaneously. When **Auto CTS** or **Auto RTS** is enabled and any 802.11b station is associated to the radio, additional frames are sent to gain access to the wireless network.

    - Auto CTS requires 802.11g stations to send a slow Clear To Send frame that locks out other stations. Automatic protection reduces 802.11g throughput when 802.11b stations are present—Auto CTS adds less overhead than Auto RTS. The default value is Auto CTS.
    - With Auto RTS, 802.11g stations reserve the wireless media using a Request To Send/Clear To Send cycle. This mode is useful when you have dispersed nodes. It was originally used in 802.11b only networks to avoid collisions from "hidden nodes"—nodes that are so widely dispersed that they can hear the AP, but not each other.

When there are no 11b stations associated and an auto-protection mode is enabled, the AP will not send the extra frames, thus avoiding unnecessary overhead.

9. **802.11g Slot**: Choose **Auto** to instruct the AP to manage the 802.11g slot times automatically, or choose **Short Only**. Avaya recommends using **Auto** for this setting, especially if 802.11b devices are present.

10. **802.11b Preamble**: The preamble contains information that the AP and client devices need when sending and receiving packets. All compliant 802.11b systems have to support the long preamble. A short preamble improves the efficiency of a network's throughput when transmitting special data, such as voice, VoIP (Voice-over IP) and streaming video. Select **Auto** to instruct the AP to manage the preamble (long and short) automatically, or choose **Long Only**.

11. **Fragmentation Threshold**: This is the maximum size for directed data packets transmitted over the 802.11b/g radio. Larger frames fragment into several packets, their maximum size defined by the value you enter here. Enter the desired **Fragmentation Threshold** value, between 256 and 2346.

12. **RTS Threshold**: The RTS (Request To Send) Threshold specifies the packet size. Packets larger than the RTS threshold will use CTS/RTS prior to transmitting the packet—useful for larger packets to help ensure the success of their transmission. Enter a value between 1 and 2347.

13. **Max Stations per AP**: This defines how many total concurrent station associations are allowed for all 802.11bgn radios. If multiple station limits are set, all will be enforced. As soon as any limit is reached, no new stations can associate until some other station has terminated its association. See Step 15 on page 497 in Global Settings (Radio) for a list of places where station limits are set.

14. **Max Stations per Radio**: This defines how many station associations are allowed per 802.11bgn radio. If multiple station limits are set, all will be enforced. As soon as any limit is reached, no new stations can associate until some other station has terminated its association. See Step 15 on

page 497 in Global Settings (Radio) for a list of places where station limits are set.

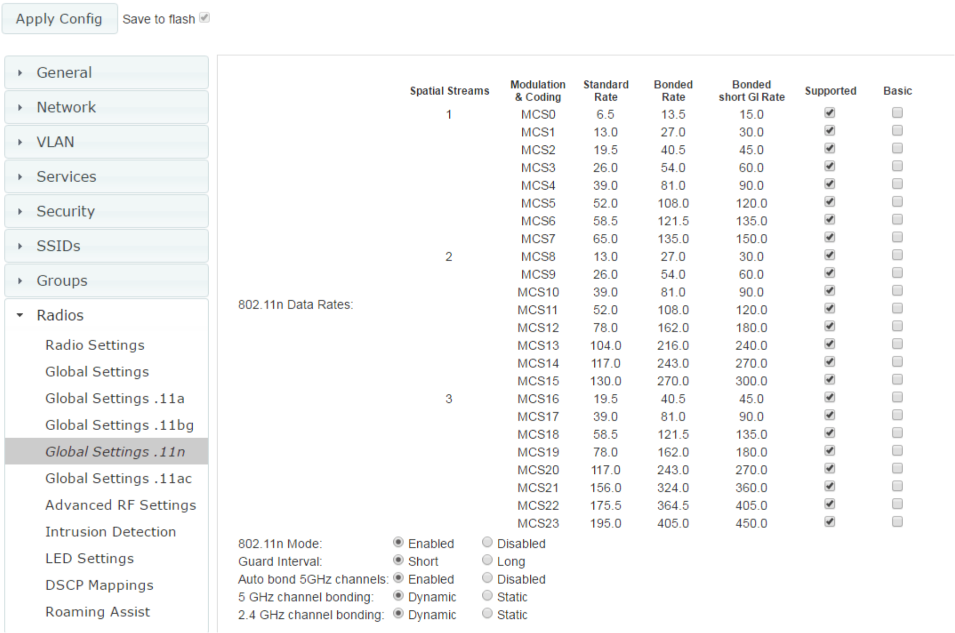
Global Settings .11n

This window allows you to establish global 802.11n radio settings. These settings include enabling or disabling 802.11n mode for the entire AP, and specifying whether auto-configured channel bonding will be static or dynamic.

Procedure for Configuring Global 802.11n Radio Settings

802.11n operation is allowed only if the AP's license includes this feature.

1. **802.11n Data Rates**: The AP allows you to define which data rates are supported for all 802.11n radios. Select (or deselect) 11n data rates by clicking in the corresponding **Supported** and **Basic** data rate check boxes.
   - **Basic Rate**—a wireless station (client) must support this rate in order to associate.
   - **Supported Rate**—data rates that can be used to transmit to clients.



802.11n Data Rates:

Spatial Streams	Modulation & Coding	Standard Rate	Bonded Rate	Bonded short GI Rate	Supported	Basic
1	MCS0	6.5	13.5	15.0	☑	□
	MCS1	13.0	27.0	30.0	☑	□
	MCS2	19.5	40.5	45.0	☑	□
	MCS3	26.0	54.0	60.0	☑	□
	MCS4	39.0	81.0	90.0	☑	□
	MCS5	52.0	108.0	120.0	☑	□
	MCS6	58.5	121.5	135.0	☑	□
	MCS7	65.0	135.0	150.0	☑	□
2	MCS8	13.0	27.0	30.0	☑	□
	MCS9	26.0	54.0	60.0	☑	□
	MCS10	39.0	81.0	90.0	☑	□
	MCS11	52.0	108.0	120.0	☑	□
	MCS12	78.0	162.0	180.0	☑	□
	MCS13	104.0	216.0	240.0	☑	□
	MCS14	117.0	243.0	270.0	☑	□
	MCS15	130.0	270.0	300.0	☑	□
3	MCS16	19.5	40.5	45.0	☑	□
	MCS17	39.0	81.0	90.0	☑	□
	MCS18	58.5	121.5	135.0	☑	□
	MCS19	78.0	162.0	180.0	☑	□
	MCS20	117.0	243.0	270.0	☑	□
	MCS21	156.0	324.0	360.0	☑	□
	MCS22	175.5	364.5	405.0	☑	□
	MCS23	195.0	405.0	450.0	☑	□

802.11n Mode: ● Enabled ○ Disabled
Guard Interval: ● Short ○ Long
Auto bond 5GHz channels: ● Enabled ○ Disabled
5 GHz channel bonding: ● Dynamic ○ Static
2.4 GHz channel bonding: ● Dynamic ○ Static

Figure 282. Global Settings .11n

2. **802.11n Mode**: Select **Enabled** to operate in 802.11n mode (this is the default). Use of this mode is controlled by the AP's license key. The key must include 802.11n capability, or you will not be able to enable this mode. See **"AP Details—System" on page 71** to view the features supported by your license key. Contact Avaya Customer support for questions about your license.

   If you select **Disabled**, then 802.11n operation is disabled on the AP.

3. **Guard interval**: Select **Short** to increase the data transmission rate by decreasing wait intervals in signal transmission. Select **Long** to use the standard interval. The default is Short.

4. **Auto bond 5 GHz channels**: Select **Enabled** to use Channel Bonding on 5 GHz channels and automatically select the best channels for bonding. The default is **Enabled**.

5. **5 GHz channel bonding**: Select **Dynamic** to have auto-configuration for bonded 5 GHz channels be automatically updated as conditions change. For example, if there are too many clients to be supported by a bonded channel, dynamic mode will automatically break the bonded channel into two channels. Select **Static** to have the bonded channels remain the same once they are selected. The Dynamic option is only available when **Auto bond 5 GHz channels** is enabled. The default is **Dynamic**.

6. **2.4 GHz channel bonding**: Select **Dynamic** to have auto-configuration for bonded 2.4 GHz channels be automatically updated as conditions change. Select **Static** to have the bonded channels remain the same once they are selected. The default is **Dynamic**.

Global Settings .11ac

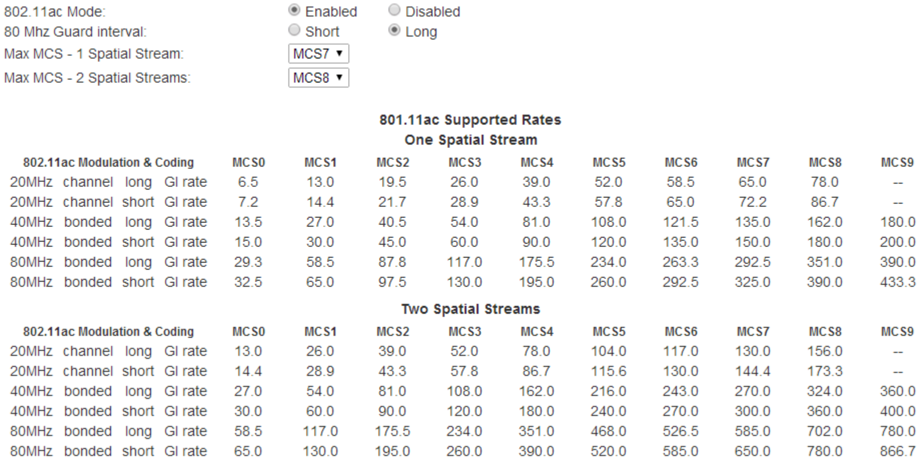
This window is displayed only for AP models with licensed 802.11ac radios. It allows you to establish global 802.11ac radio settings. These settings include enabling or disabling 802.11ac mode for the entire AP, setting a short or standard guard interval, and specifying the Modulation and Coding Scheme used with different numbers of streams.

Before changing your settings for 802.11ac, please read the discussion in “About IEEE 802.11ac” in the *Avaya WLAN AP 9100 Series (NN47252-102)*.

Procedure for Configuring Global 802.11ac Radio Settings

802.11ac operation is allowed only if the AP's license includes this feature.

1. **802.11ac Mode**: Select **Enabled** to allow the AP to operate in 802.11ac mode. If you select **Disabled**, then 802.11ac operation is disabled on the AP.



802.11ac Mode:	● Enabled	○ Disabled
80 Mhz Guard interval:	○ Short	● Long
Max MCS - 1 Spatial Stream:	MCS7 ▾	
Max MCS - 2 Spatial Streams:	MCS8 ▾	

801.11ac Supported Rates

One Spatial Stream

802.11ac Modulation & Coding	MCS0	MCS1	MCS2	MCS3	MCS4	MCS5	MCS6	MCS7	MCS8	MCS9
20MHz channel long GI rate	6.5	13.0	19.5	26.0	39.0	52.0	58.5	65.0	78.0	--
20MHz channel short GI rate	7.2	14.4	21.7	28.9	43.3	57.8	65.0	72.2	86.7	--
40MHz bonded long GI rate	13.5	27.0	40.5	54.0	81.0	108.0	121.5	135.0	162.0	180.0
40MHz bonded short GI rate	15.0	30.0	45.0	60.0	90.0	120.0	135.0	150.0	180.0	200.0
80MHz bonded long GI rate	29.3	58.5	87.8	117.0	175.5	234.0	263.3	292.5	351.0	390.0
80MHz bonded short GI rate	32.5	65.0	97.5	130.0	195.0	260.0	292.5	325.0	390.0	433.3

Two Spatial Streams

802.11ac Modulation & Coding	MCS0	MCS1	MCS2	MCS3	MCS4	MCS5	MCS6	MCS7	MCS8	MCS9
20MHz channel long GI rate	13.0	26.0	39.0	52.0	78.0	104.0	117.0	130.0	156.0	--
20MHz channel short GI rate	14.4	28.9	43.3	57.8	86.7	115.6	130.0	144.4	173.3	--
40MHz bonded long GI rate	27.0	54.0	81.0	108.0	162.0	216.0	243.0	270.0	324.0	360.0
40MHz bonded short GI rate	30.0	60.0	90.0	120.0	180.0	240.0	270.0	300.0	360.0	400.0
80MHz bonded long GI rate	58.5	117.0	175.5	234.0	351.0	468.0	526.5	585.0	702.0	780.0
80MHz bonded short GI rate	65.0	130.0	195.0	260.0	390.0	520.0	585.0	650.0	780.0	866.7

Figure 283. Global Settings .11ac (shown for 2x2 radios)

2. **80 MHz Guard interval**: This is the length of the interval between transmission of symbols (the smallest unit of data transfer) when you are using 80MHz bonded channels. (See the “80 MHz and 160 MHz Channel Widths (Bonding)” discussion in “About IEEE 802.11ac” in *Using the Avaya OS for Avaya WLAN AP 9100 Series (NN47252-102)*. Select **Short** to increase the data transmission rate by decreasing wait intervals in signal transmission. Select **Long** to use the standard interval. The default is Short.

3. **Beamforming**: Beamforming is used for directional signal transmission or reception. This method results in an increased range for devices supporting beamforming. Avaya Wave 2 products support beamforming only for 802.11ac beamforming-capable clients.

4. **MU-MIMO**: This stands for the Multiple-User form of Multiple-Input Multiple-Output wireless communication, which is available on Wave 2 802.11ac APs. This can help the AP be more efficient with MU-MIMO enabled clients. For example, the WAP9144's Wave 2 radios have 4 antennas each. The mix of client devices connecting to the AP is likely to average fewer antennas. If MU-MIMO is enabled, then the AP radio could, for example, communicate concurrently with two clients that each have 2-antenna radios with MU-MIMO capability.

5. **Max MCS**: Select the highest Modulation and Coding Scheme level that may be used with **1** or **2 Spatial Streams**. For models with 3x3 radios, there is also a setting for **3 Spatial Streams**. This setting may be used to limit the highest level of modulation to 64-QAM, or allow 256-QAM with its higher data rate. It also determines the coding scheme used for error correction. Higher MCS levels allocate fewer bits to error correction, and thus a higher proportion is used for data transfer. The default **Max MCS** value is **MCS9**.

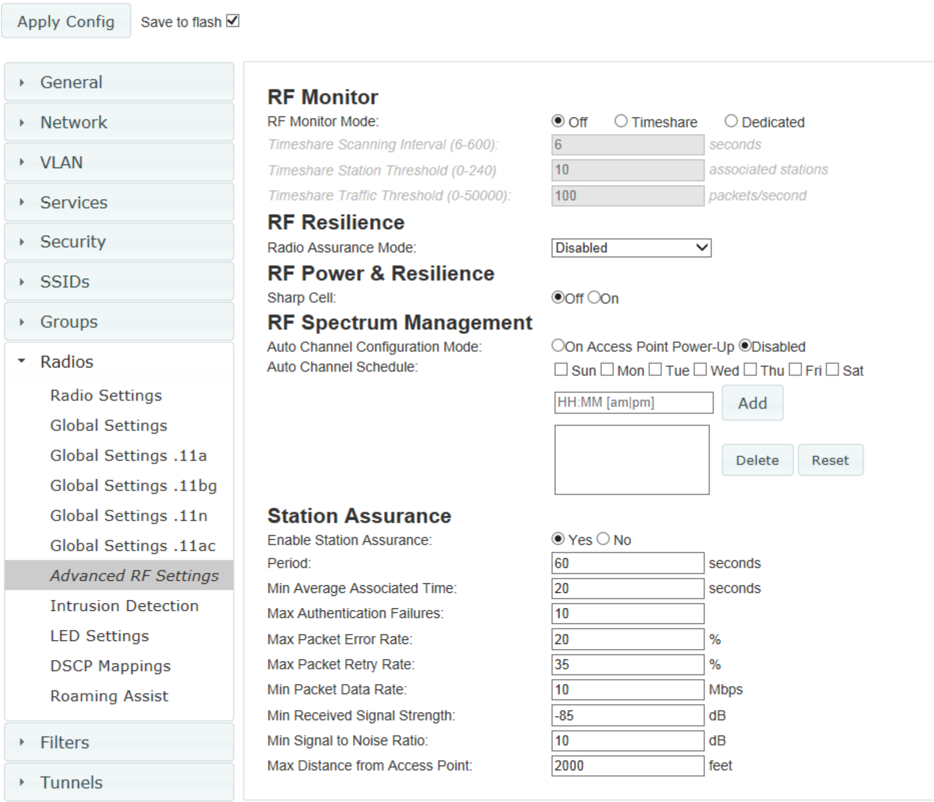
   The higher the MCS values, the higher the data rate, as shown in **802.11ac Supported Rates**, below. Higher MCS levels require higher signal-to-noise ratios (i.e., a less noisy environment) and shorter transmission distances. See the "Higher Precision in the Physical Layer" discussion in "About IEEE 802.11ac" in *Using the Avaya OS for Avaya WLAN AP 9100 Series (NN47252-102)*.

   The maximum number of separate data streams that may be transmitted by the antennas of each radio is determined by whether the AP has 2x2 or 3x3 radios. For a device that has 2x2 radios, such as the WAP9122/9132, the settings for three spatial streams are not shown. See the "Up to Eight Simultaneous Data Streams—Spatial Multiplexing" discussion in "About IEEE 802.11ac" in *Using the Avaya OS for Avaya WLAN AP 9100 Series (NN47252-102)*.

6. **802.11ac Supported Rates**: This list shows the optimum data rates that can be expected, based on the number of spatial streams that a station can handle, and on your settings for Max MCS, Guard Interval, and the use of bonded channels, up to 80MHz wide.

Advanced RF Settings

This window allows you to establish RF settings, including automatically configuring channel allocation and cell size, and configuring radio assurance. Changes you make on this page are applied to all radios, without exception.



RF Monitor

RF Monitor Mode: ● Off ○ Timeshare ○ Dedicated

Timeshare Scanning Interval (6-600): 6 *seconds*

Timeshare Station Threshold (0-240) 10 *associated stations*

Timeshare Traffic Threshold (0-50000): 100 *packets/second*

RF Resilience

Radio Assurance Mode: Disabled

RF Power & Resilience

Sharp Cell: ●Off ○On

RF Spectrum Management

Auto Channel Configuration Mode: ○On Access Point Power-Up ●Disabled

Auto Channel Schedule: □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

HH:MM [am|pm]

Station Assurance

Enable Station Assurance: ● Yes ○ No

Period: 60 seconds

Min Average Associated Time: 20 seconds

Max Authentication Failures: 10

Max Packet Error Rate: 20 %

Max Packet Retry Rate: 35 %

Min Packet Data Rate: 10 Mbps

Min Received Signal Strength: -85 dB

Min Signal to Noise Ratio: 10 dB

Max Distance from Access Point: 2000 feet

Figure 284. Advanced RF Settings

Procedure for Configuring Advanced RF Settings

Some features below, such as RF Intrusion Detection, are only available if the AP's license includes the Avaya Advanced RF Security Manager (RSM).

RF Monitor

1. **RF Monitor Mode:** RF monitoring permits the operation of features like intrusion detection. The monitor may operate in **Dedicated** mode, or in **Timeshare** mode which allows the radio to divide its time between monitoring and acting as a standard radio that allows stations to associate to it.

   In Timeshare mode, monitor functions are performed less frequently and thoroughly, which is likely to impact some features that rely on the monitor. In particular, rogue location information from this AP may not be frequent enough to identify and locate rogues. See **"Rogue Location" on page 252***.*

   Note that if you are performing configuration for Profiles and you select **Dedicated** mode, you will also see a setting for **Enable Timeshare for 2-Radio APs**. For details, see **"Settings that are only present in profile configuration" on page 210**.

   If **Timeshare** mode is selected, you may adjust the following settings:

   - **Timeshare Scanning Interval (6-600)**: number of seconds between monitor (off-channel) scans.
   - **Timeshare Station Threshold (0-240)**: when the number of stations associated to the monitor radio exceeds this threshold, scanning is halted.
   - **Timeshare Traffic Threshold (0-50000)**: when the number of packets per second handled by the monitor radio exceeds this threshold, scanning is halted.

RF Resilience

2. **Radio Assurance Mode**: When this mode is enabled, the monitor radio performs loopback tests on the AP. This mode requires RF Monitor Mode to be enabled (Step 1) to enable self-monitoring functions. It also requires an individual radio to be set to monitoring mode.

   The Radio Assurance mode scans and sends out probe requests on each channel, in turn. It listens for all probe responses and beacons. These tests are performed continuously (24/7). If no beacons or probe responses are observed from a particular radio for a predetermined period, Radio Assurance mode will take action according to the preference that you have specified:

   - **Alert only**—The AP will issue alerts in the Syslog, but will not initiate repairs or reboots.
   - **Repairs without reboot**—The AP will issue alerts and perform resets of one or all of the radios if needed.
   - **Reboots allowed**—The AP will issue alerts, perform resets, and schedule reboots if needed.
   - **Disabled**—Disable radio radio assurance tests (no self-monitoring occurs). Loopback tests are disabled by default.

RF Power and Resilience

3. **Sharp Cell:** This feature reduces interference between neighboring APs or other Access Points by limiting to a defined boundary (cell size) the trailing edge bleed of RF energy. Choose **On** to enable the Sharp Cell functionality, or choose **Off** to disable this feature. See also, “Planning Your Installation—Coverage and Capacity Planning” in *Using the Avaya OS for Avaya WLAN AP 9100 Series (NN47252-102)*.

   The Sharp Cell feature only works when the cell size is Small, Medium, or Large (or Auto)—but not Max. If an individual radio cell size is set to Max, the Sharp Cell feature will be disabled for that radio. This feature is available on 802.11n radios on Access Points, but not on 802.11ac radios.

RF Spectrum Management (Auto Channel Configuration)

*Note that Auto Channel normally assigns individual channels. However, if you select **Auto bond 5GHz channels** on the **Global Settings .11n** page, and have 40MHz channels set up prior to running Auto Channel, those bonds will be preserved. 80MHz bonds will not be preserved.*

Auto Channel assignment selects channel assignments for an AP's radios. When you start an AP's auto channel feature, the AP scans the surrounding area for RF activity on all channels and then automatically selects and sets its channels to the best available. This function is typically executed when initially installing APs in a new location. You may wish to repeat it periodically to account for changes in the RF environment over time. Note that the best way to run auto channel is from a map. See the **Auto Configure Channels** option (and also see the Auto Band option) in the **Configure** drop-down menu in **"Managing APs Within Maps" on page 241** and **"Channel Configuration" on page 253**.

When running auto channel on multiple APs, WOS will shut down radios on all of the APs being configured. It will then run auto channel on one AP at a time, and bring its radios back up when channels have been selected.

4. **Auto Channel Configuration Mode**: This option allows you to instruct the AP to auto-configure channel selection for each enabled radio when the AP is powered up. Choose **On AP PowerUp** to enable this feature, or choose **Disabled** to disable this feature.

5. **Auto Channel Schedule**: This option allows you to instruct the AP to auto-configure channel selection for each enabled radio at the times you specify here. Leave this field blank unless you want to specify one or more times at which the auto-configuration process is initiated. Auto Channel will run on the selected day[s} at the specified times. Time is specified in hours and minutes, using the format: **hh:mm [am|pm]**. If you omit the optional day specification, channel configuration will run daily at the specified time. If you do not specify am or pm, time is interpreted in 24-hour military time. For example, Sat 11:00 pm and Saturday 23:00 are both acceptable and specify the same time.

Station Assurance

Station assurance monitors the quality of the connections that users are experiencing on the wireless network. You can quickly detect stations that are having problems and take steps to correct them. Use these settings to establish threshold values for errors and other problems. Station assurance is enabled by default, with a set of useful default thresholds that you may adjust as desired.

When a connection is experiencing problems and reaches one of these thresholds in the specified period of time, the AP responds with several actions: an event is triggered, a trap is generated, and a Syslog message is logged. For example, if a client falls below the threshold for **Min Average Associated Time**, this "bouncing" behavior might indicate roaming problems with the network's RF design, causing the client to bounce between multiple APs and not stay connected longer than the time to re-associate and then jump again. This can be corrected with RF adjustments. Station assurance alerts you to the fact that this station is encountering problems.

6. **Enable Station Assurance**: This is disabled by default. Click **No** if you wish to disable it, and click **Yes** to enable it. When station assurance is enabled, the AP will monitor connection quality indicators listed below and will display associated information on the Station Assurance window. When a threshold is reached, an event is triggered, a trap is generated, and a Syslog message is logged.

7. **Period**: In seconds, the period of time for a threshold to be reached. For example, the AP will check whether Max Authentication Failures has been reached in this number of seconds.

8. **Min Average Associated Time**: (seconds) Station assurance detects whether the average length of station associations falls below this threshold during a period.

9. **Max Authentication Failures**: Station assurance detects whether the number of failed login attempts reaches this threshold during a period.

10. **Max Packet Error Rate**: (%) Station assurance detects whether the packet error rate percentage reaches this threshold during a period.

11. **Max Packet Retry Rate**: (%) Station assurance detects whether the packet retry rate percentage reaches this threshold during a period.

12. **Min Packet Data Rate**: (Mbps) Station assurance detects whether the packet data rate falls below this threshold during a period.

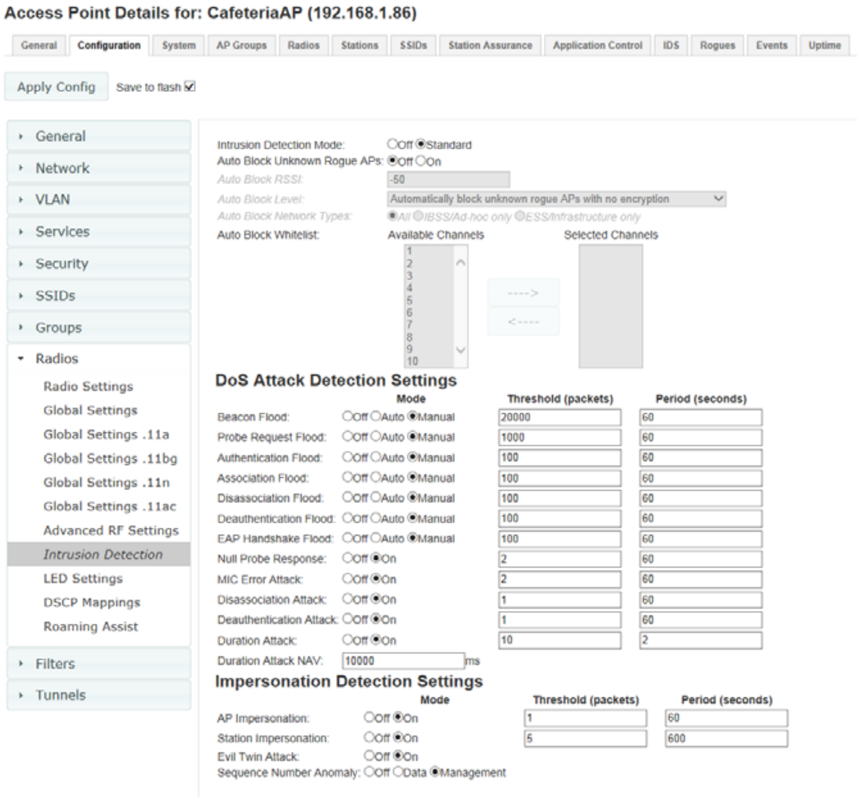
13. **Min Received Signal Strength**: (dB) Station assurance detects whether the strength of the signal received from the station falls below this threshold during a period.

14. **Min Signal to Noise Ratio**: (dB) Station assurance detects whether the ratio of signal to noise received from the station falls below this threshold during a period.

15. **Max Distance from AP**: **Min Received Signal Strength**: (feet) Station assurance detects whether the distance of the station from the AP reaches this threshold during a period.

Intrusion Detection

APs employ a number of Intrusion Detection System/Intrusion Prevention System (IDS/IPS) strategies to detect and prevent malicious attacks on the wireless network. This window allows you to adjust intrusion detection settings.



Access Point Details for: CafeteriaAP (192.168.1.86)

Save to flash ☑

Intrusion Detection Mode: ○Off ●Standard

Auto Block Unknown Rogue APs: ●Off ○On

Auto Block RSSI: -50

Auto Block Level: Automatically block unknown rogue APs with no encryption

Auto Block Network Types: ●All ○IBSS/Ad-hoc only ○ESS/Infrastructure only

Auto Block Whitelist: Available Channels: 1 2 3 4 5 6 7 8 9 10 — Selected Channels:

DoS Attack Detection Settings

	Mode	Threshold (packets)	Period (seconds)
Beacon Flood:	○Off ○Auto ●Manual	20000	60
Probe Request Flood:	○Off ○Auto ●Manual	1000	60
Authentication Flood:	○Off ○Auto ●Manual	100	60
Association Flood:	○Off ○Auto ●Manual	100	60
Disassociation Flood:	○Off ○Auto ●Manual	100	60
Deauthentication Flood:	○Off ○Auto ●Manual	100	60
EAP Handshake Flood:	○Off ○Auto ●Manual	100	60
Null Probe Response:	○Off ●On	2	60
MIC Error Attack:	○Off ●On	2	60
Disassociation Attack:	○Off ●On	1	60
Deauthentication Attack:	○Off ●On	1	60
Duration Attack:	○Off ●On	10	2
Duration Attack NAV:	10000 ms		

Impersonation Detection Settings

	Mode	Threshold (packets)	Period (seconds)
AP Impersonation:	○Off ●On	1	60
Station Impersonation:	○Off ●On	5	600
Evil Twin Attack:	○Off ●On		
Sequence Number Anomaly:	○Off ○Data ●Management		

Figure 285. Intrusion Detection Settings

The AP provides a suite of intrusion detection and prevention options to improve network security. You can separately enable detection of the following types of problems:

- **Rogue Access Point Detection and Blocking**

  Unknown access points are detected, and may be automatically blocked based on a number of criteria. See **“About Blocking Rogue APs” on page 528**.

- **Denial of Service (DoS) or Availability Attack Detection**

  A DoS attack attempts to flood an AP with communications requests so that it cannot respond to legitimate traffic, or responds so slowly that it becomes effectively unavailable. The AP can detect a number of types of DoS attacks, as described in the table below. When an attack is detected, the AP logs a Syslog message at the Alert level.

- **Impersonation Detection**

  These malicious attacks use various techniques to impersonate a legitimate AP or station, often in order to eavesdrop on wireless communications. The AP detects a number of types of impersonation attacks, as described in the table below. When an attack is detected, the AP logs a Syslog message at the Alert level.

Type of Attack	Description
DoS Attacks	
Beacon Flood	Generating thousands of counterfeit 802.11 beacons to make it hard for stations to find a legitimate AP.
Probe Request Flood	Generating thousands of counterfeit 802.11 probe requests to overburden the AP.
Authentication Flood	Sending forged Authenticates from random MAC addresses to fill the AP's association table.
Association Flood	Sending forged Associates from random MAC addresses to fill the AP's association table.

Type of Attack	Description
Disassociation Flood	Flooding the AP with forged Disassociation packets.
Deauthentication Flood	Flooding the AP with forged Deauthenticates.
EAP Handshake Flood	Flooding an AP with EAP-Start messages to consume resources or crash the target.
Null Probe Response	Answering a station probe-request frame with a null SSID. Many types of popular NIC cards cannot handle this situation, and will freeze up.
MIC Error Attack	Generating invalid TKIP data to exceed the AP's MIC error threshold, suspending WLAN service.
Disassociation Attack (Omerta)	Sending forged disassociation frames to all stations on a channel in response to data frames.
Deauthentication Attack	Sending forged deauthentication frames to all stations on a channel in response to data frames.
Duration Attack (Duration Field Spoofing)	Injecting packets into the WLAN with huge duration values. This forces the other nodes in the WLAN to keep quiet, since they cannot send any packet until this value counts down to zero. If the attacker sends such frames continuously it silences other nodes in the WLAN for long periods, thereby disrupting the entire wireless service.
Impersonation Attacks	
AP impersonation	Reconfiguring an attacker's MAC address to pose as an authorized AP. Administrators should take immediate steps to prevent the attacker from entering the WLAN.
Station impersonation	Reconfiguring an attacker's MAC address to pose as an authorized station. Administrators should take immediate steps to prevent the attacker from entering the WLAN.
Evil twin attack (SSID Spoofing)	Masquerading as an authorized AP by beaconing the WLAN's service set identifier (SSID) to lure users. Rogue APs engaging in this type of attack may be auto blocked. See **“SSID Spoofing Auto Block” on page 180**.

Type of Attack	Description
Sequence number anomaly	A sender may use an Add Block Address request (ADDBA - part of the Block ACK mechanism) to specify a sequence number range for packets that the receiver can accept. An attacker spoofs an ADDBA request, asking the receiver to reset its sequence number window to a new range. This causes the receiver to drop legitimate frames, since their sequence numbers will not fall in that range.

About Blocking Rogue APs

If you classify a rogue AP as **blocked** (see **"Rogues" on page 90**), then the AP will take measures to prevent stations from staying associated to the rogue. When the monitor radio is scanning, any time it hears a beacon from a blocked rogue it sends out a broadcast "deauth" signal using the rogue's BSSID and source address. This has the effect of disconnecting all of a rogue AP's clients approximately every 5 to 10 seconds, which is enough to make the rogue frustratingly unusable.

The Intrusion Detection window allows you to set up **Auto Block** parameters so that unknown APs get the same treatment as explicitly blocked APs. This may result in many APs being blocked so use caution with auto block, and be sure to abide by applicable regulations. ***See the Caution on page 530.*** By default, auto blocking is turned off. Auto blocking provides two parameters for qualifying blocking so that APs must meet certain criteria before being blocked. This keeps the AP from blocking every AP that it detects. You may:

- Set a minimum RSSI value for the AP—for example, if an AP has an RSSI value of -90, it is probably a harmless AP belonging to a neighbor and not in your building.
- Block based on encryption level.
- Block based on whether the AP is part of an ad hoc network or infrastructure network.
- Specify channels to be whitelisted. Rogues discovered on these channels are excluded from auto blocking. This allows specified channels to be freely used by customer or guests for their APs.

WOS can also auto block rogue APs that are engaging in spoofing (evil twin) attacks on your SSIDs. This is done on a system-wide basis, for all managed APs rather than for a particular AP or Profile network. See **"SSID Spoofing Auto Block" on page 180**.

RF Intrusion Detection and Auto Block Mode

Procedure for Configuring Intrusion Detection

1. **Intrusion Detection Mode:** This option allows you to choose the **Standard** intrusion detection method, or you can choose **Off** to disable this feature. See "AP Monitor and Radio Assurance Capabilities" in the Technical Support Appendix of *Using the Avaya OS for Avaya WLAN AP 9100 Series (NN47252-102)* for more information.

   - **Standard**—enables the monitor radio to collect Rogue AP information.
   - **Off**—intrusion detection is disabled. This is the default value.

2. **Auto Block Unknown Rogue APs:** Enable or disable auto blocking (see **"About Blocking Rogue APs" on page 528**). You will be shown a Caution statement (below) and the WMI will ask whether you wish to proceed. Note that in order to set **Auto Block RSSI** and **Auto Block Level**, you must set Auto Block Unknown Rogue APs to **On**. Then the remaining Auto Block fields will be active.

! *CAUTION: Selecting and engaging Auto Block may result in many APs being blocked. User caution in configuring and operating any form of Auto Block is highly recommended, as auto-blocking may be subject to significant statutory and U.S. Federal Communications Commission (FCC) regulatory controls, restrictions, enforcement actions and penalties.*

User is solely responsible for making sure that all uses of any auto-blocking feature(s) of this product are fully compliant with all applicable statutes, regulations, FCC enforcement actions and rules, etc. regarding Wi-Fi blocking. See for example FCC Enforcement Advisory No. 2015-01 dated January 27, 2015.

All uses of any auto-blocking feature(s) in this product are solely at User's discretion and individual choice. User assumes all liability and responsibility for all such uses. Avaya assumes no liability or responsibility for any discretionary decision by User to configure, engage and to use any auto-blocking feature(s) of this product.

3. **Auto Block RSSI:** Set the minimum RSSI for rogue APs to be blocked. APs with lower RSSI values will not be blocked. They are assumed to be farther away, and probably belonging to neighbors and posing a minimal threat.

4. **Auto Block Level:** Select rogue APs to block based on the level of encryption that they are using. The choices are:

   - Automatically block unknown rogue APs regardless of encryption.
   - Automatically block unknown rogue APs with no encryption.
   - Automatically block unknown rogue APs with WEP or no encryption.

5. **Auto Block Network Types:** Select rogues to automatically block by applying the criteria above only to networks of the type specified below. The choices are:

- **All**—the unknown rogues may be part of any wireless network.
- **IBSS/AD Hoc only**—only consider auto blocking rogues if they belong to an ad hoc wireless network (a network of client devices without a controlling Access Point, also called an Independent Basic Service Set—IBSS).
- **ESS/Infrastructure only**—only consider auto blocking rogue APs if they are in infrastructure mode rather than ad hoc mode.

6. **Auto Block White list:** Use this list to specify channels to be excluded from automatic blocking. If you have enabled **Auto Block**, it will not be applied to rogues detected on the whitelisted channels. Use the **Add Channel** drop-down to add entries to the **Channels** list, one at a time. You can delete entries from the list by selecting them from the **Remove Channel** drop-down list.

DoS Attack Detection Settings

7. **Attack/Event**: The types of DoS attack that you may detect are described in the Type of Attack Table on page 526. Detection of each attack type may be separately enabled or disabled. For each attack, a default **Threshold** and **Period (seconds)** are specified. If the number of occurrences of the type of packet being detected exceeds the threshold in the specified number of seconds, then the AP declares that an attack has been detected. You may modify the **Threshold** and **Period**.

   For the Flood attack settings, you also have a choice of **Auto** or **Manual**.

   - **Manual** mode—threshold and period settings are used to detect a flood. Packets received are simply counted for the specified time period and compared against the flood threshold. The default for all of the floods is **Manual** mode.
   - **Auto** mode—the AP analyzes current traffic for packets of a given type versus traffic over the past hour to determine whether a packet flood should be detected. In this mode, threshold and period settings are ignored. This mode is useful for floods like beacon or probe floods, where the numbers of such packets detected in the air can vary greatly from installation to installation.

8. **Duration Attack NAV (ms)**: For the duration attack, you may also modify the default duration value that is used to determine whether a packet may be part of an attack. If the number of packets having at least this duration value exceeds the **Threshold** number in the specified **Period**, an attack is detected.

Impersonation Detection Settings

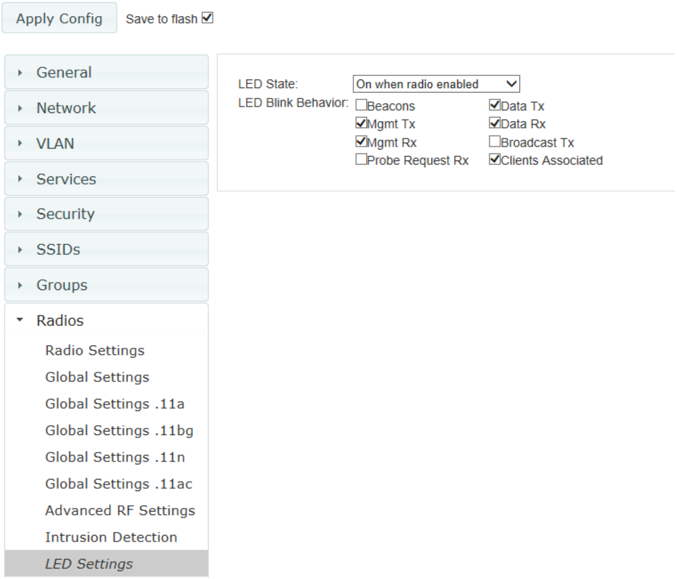
9. **Attack/Event**: The types of impersonation attack that you may detect are described in Impersonation Attacks on page 527. Detection of each attack type may be turned **On** or **Off** separately. For **AP** or **Station Impersonation** attacks, a default **Threshold** and **Period (seconds)** are specified. If the number of occurrences of the type of packet being detected exceeds the threshold in the specified number of seconds, then the AP declares that an attack has been detected. You may modify the **Threshold** and **Period**.

10. **Sequence number anomaly**: You may specify whether to detect this type of attack in **Data** traffic or in **Management** traffic, or turn **Off** this type of detection.

11. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

LED Settings

This window assigns behavior preferences for the AP's radio LEDs.



LED State: On when radio enabled

LED Blink Behavior: □Beacons ☑Mgmt Tx ☑Mgmt Rx □Probe Request Rx ☑Data Tx ☑Data Rx □Broadcast Tx ☑Clients Associated

Figure 286. LED Settings

Procedure for Configuring the Radio LEDs

1. **LED State:** This option determines which event triggers the LEDs, either when a particular radio is enabled or when a particular radio first associates with the network. Choose **On when radio enabled** or **On when station associated**, as desired. You may also choose **Disabled** to keep the LEDs from being lit. The LEDs will still light during the boot sequence, then turn off.

2. **LED Blink Behavior**: This option allows you to select when the radio LEDs blink, based on the activities you check here. From the choices available, select one or more activities to trigger when the LEDs blink.

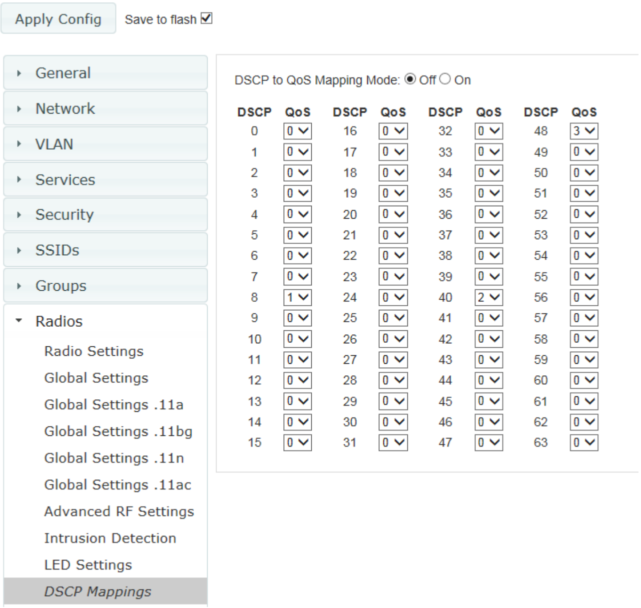
3. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

DSCP Mappings

DSCP is the 6-bit Differentiated Services Code Point (DiffServ) field in the IPv4 or IPv6 packet header, defined in RFC2474 and RFC2475. The DSCP value classifies the packet to determine the Quality of Service (QoS) required. DSCP replaces the outdated Type of Service (TOS) field.

The DSCP Mappings page shows the default mapping of each of the 64 DSCP values to one of the AP's four QoS levels, and allows you to change these mappings.

For a detailed discussion of the operation of QoS and DSCP mappings, please see **"Understanding QoS Priority on the Wireless AP" on page 450**.



DSCP to QoS Mapping Mode: ● Off ○ On

DSCP	QoS	DSCP	QoS	DSCP	QoS	DSCP	QoS
0	0	16	0	32	0	48	3
1	0	17	0	33	0	49	0
2	0	18	0	34	0	50	0
3	0	19	0	35	0	51	0
4	0	20	0	36	0	52	0
5	0	21	0	37	0	53	0
6	0	22	0	38	0	54	0
7	0	23	0	39	0	55	0
8	1	24	0	40	2	56	0
9	0	25	0	41	0	57	0
10	0	26	0	42	0	58	0
11	0	27	0	43	0	59	0
12	0	28	0	44	0	60	0
13	0	29	0	45	0	61	0
14	0	30	0	46	0	62	0
15	0	31	0	47	0	63	0

Figure 287. DSCP Mappings

Procedure for Configuring DSCP Mappings

1. **DSCP to QoS Mapping Mode:** Use the **On** and **Off** buttons to enable or disable the use of the DSCP mapping table to determine the QoS level applied to each packet.
2. **DSCP to QoS Mapping:** The radio buttons in this table show all DSCP values (0 to 63), and the QoS level to which each is mapped. To change the QoS level applied to a DSCP value, click the desired QoS level (0 to 3) underneath it.

Roaming Assist

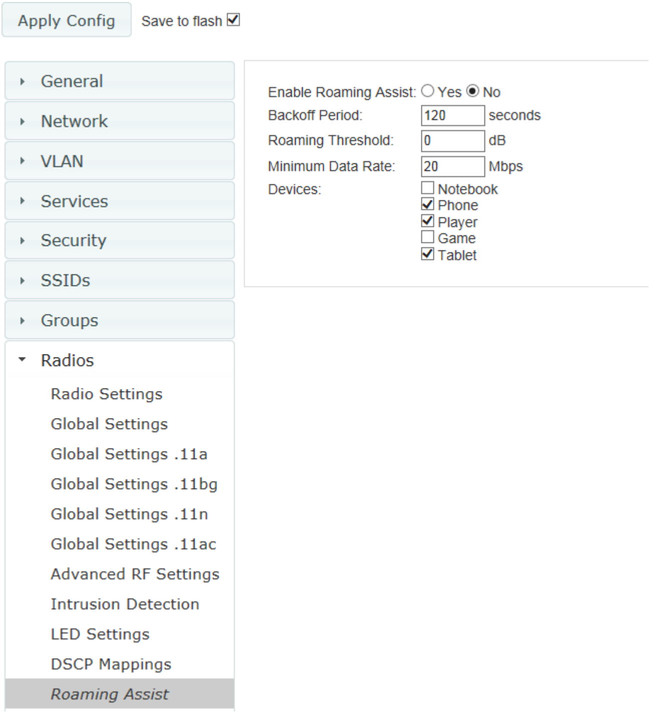
Roaming assist is an Avaya feature that helps clients roam to APs that will give them high quality connections. Some smart phones and tablets will stay connected to a particular radio with poor signal quality, even when there's a different radio with better signal strength within range. When roaming assist is enabled, the AP "assists" the device by deauthenticating it when certain parameters are met. This encourages a client with a high roaming threshold (i.e., a device that may not roam until signal quality has seriously dropped) to move to an AP that gives it a better signal. The deauthentication is meant to cause the client to choose a different radio. You can specify the device types that will be assisted in roaming.

The roaming threshold is the difference in signal strength between radios that will trigger a deauthentication. If the client's signal is lower than the sum of the threshold and the stronger neighbor radio's RSSI, then we "assist" the client. For example:

Threshold = -5
RSSI of neighbor = -65
RSSI of client = -75
-75 < (-5 + -65) : Client will roam

Another example:

Threshold = -15
RSSI of neighbor = -60
RSSI of station = -70
-70 > (-15 + -60) : Client will not roam



Enable Roaming Assist: ○ Yes ● No
Backoff Period: 120 seconds
Roaming Threshold: 0 dB
Minimum Data Rate: 20 Mbps
Devices: □ Notebook
☑ Phone
☑ Player
□ Game
☑ Tablet

Figure 288. Roaming Assist

Procedure for Configuring Roaming Assist

1. **Enable Roaming Assist:** Use the **Yes** and **No** buttons to enable or disable this feature.

2. **Backoff Period**: After deauthenticating a station, it may re-associate to the same radio. To prevent the AP from repeatedly deauthenticating the station when it comes back, there is a backoff period. This is the number of seconds the station is allowed to stay connected before another deauthentication.

3. **Roaming Threshold**: This is the difference in signal strength between radios that will trigger a deauthentication, as described in the discussion above. In most cases, this will be a negative number. Triggering occurs regardless of whether the data rate falls below the Minimum Data Rate.

4. **Minimum Data Rate**: Roaming assist will be triggered if the station's packet data rate is below this value (1-99 Mbps), regardless of whether the Roaming Threshold has been reached.

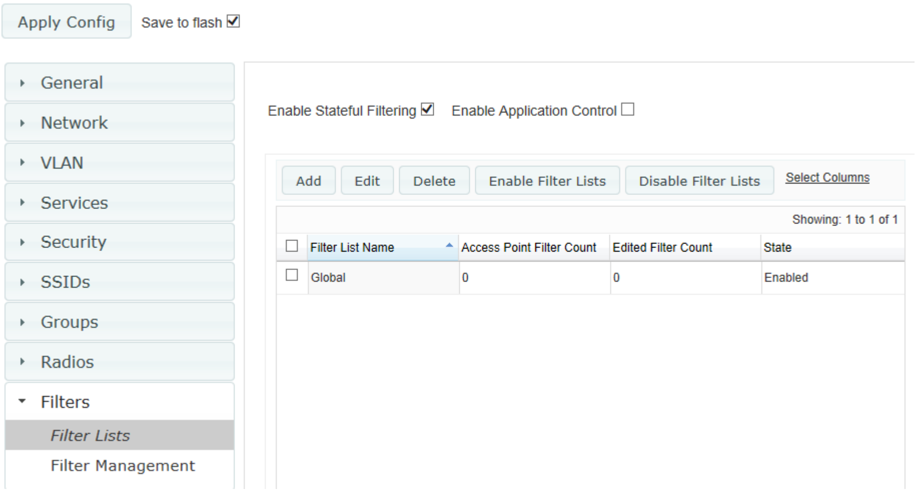
5. **Device Classes**: You can configure the device classes that will be assisted in roaming. Many small, embedded devices (such as the default device types: phones, tablets, music players) are sticky—they have high roaming thresholds that tend to keep them attached to the same radio despite the presence of radios with better signal strength. You may check off one or more entries, but use care since roaming assist may cause poor results in some cases.

   If no Device Classes are selected, then all devices are included in roaming assist. If you select entries, then stations matching any of your selected classes will be assisted when the Roaming Threshold or Minimum Data Rate trigger is satisfied.

Filters

The wireless AP's integrated firewall uses stateful inspection to speed the decision of whether to allow or deny traffic. Filters are used to define the rules used for blocking or passing traffic. Filters can also set the VLAN and QoS level for selected traffic.

The air cleaner feature (Preset Filters) offers a number of predetermined filter rules that eliminate a great deal of unnecessary wireless traffic.



Save to flash ☑

Enable Stateful Filtering ☑ Enable Application Control □

Showing: 1 to 1 of 1

□	Filter List Name	Access Point Filter Count	Edited Filter Count	State
□	Global	0	0	Enabled

Figure 289. Filter Lists

User connections managed by the firewall are maintained statefully—once a user flow is established through the AP, it is recognized and passed through without application of all defined filtering rules. Stateful inspection runs automatically on the AP. The rest of this section describes how to view and manage filters.

Filters are organized in groups, called Filter Lists. A filter list allows you to apply a uniform set of filters to SSIDs or Groups very easily.

Filter Lists

This window shows existing filter lists and allows you to create new ones. The AP comes with one predefined list, named **Global**, which cannot be deleted. Filter lists (including Global) may be applied to SSIDs or to Groups. Only one filter list at a time may be applied to a group or SSID (although the filter list may contain a number of filters). All filters are created within filter lists.

Note that smaller APs that use the AOSLite system software, such as the WAP9112 and the WAP9114, have many fewer settings than more powerful APs. Application Control policies are not supported. Settings that are not available on a particular AP are not displayed, or will be grayed out.

Procedure for Managing Filter Lists

1. **Enable Stateful Filtering:** Stateful operation of the integrated firewall can be enabled or disabled. If you have a large number of filters and you don't want to apply them in a stateful manner, you may use this option to turn the firewall off.
2. **Enable Application Control:** Operation of the Application Control feature can be enabled or disabled. See **"Application Control—Overview" on page 104**.

   Note that when you turn off Application Control, its per-AP statistics are zeroed out, but per-station statistics are not zeroed.
3. The list of Filter Lists shows the following information:
   1. **Filter List Name**
   2. **AP Filter Count**: The number of filters in this list.
   3. **Edited Filter Count**
   4. **State**: If the list is disabled, you may still add filters to it or modify it, but none of the filters will be applied to data traffic.

4. **Add**: Click this button to create a filter list. Enter its name in the dialog box, and optionally, enable it.

5. **Edit**: Click this button to edit one selected filter list.

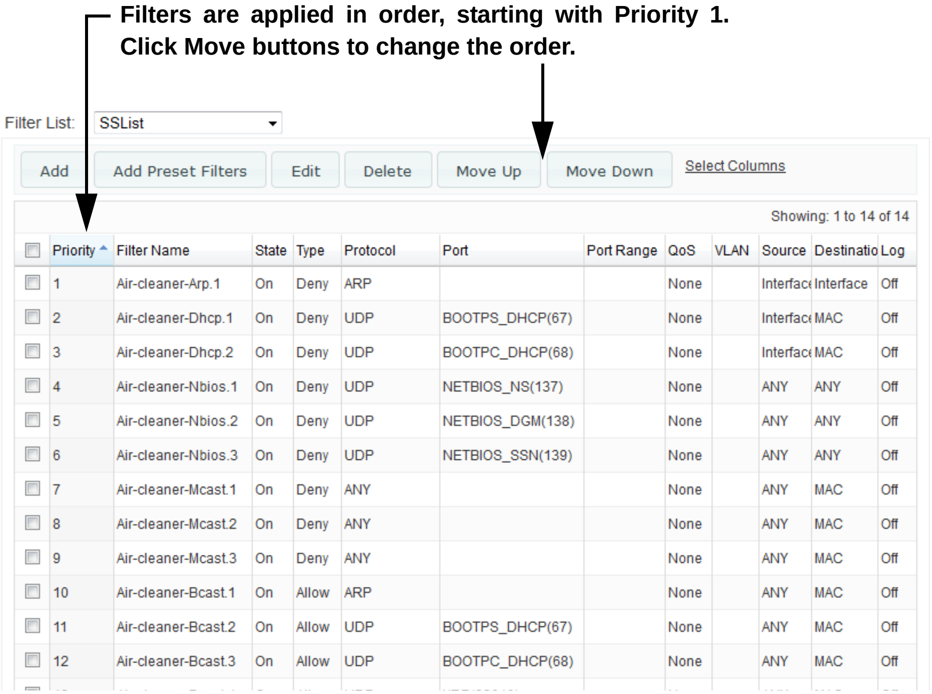
6. **Delete**: Click this button to delete the selected filter lists. The **Global** filter list may not be deleted.

7. **Enable/Disable Filter Lists**: Use these buttons to enable or disable all of the selected filter lists.

8. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Filter Management

This window allows you to create and manage filters that belong to a selected filter list, based on the filter criteria you specify.



Filters are applied in order, starting with Priority 1. Click Move buttons to change the order.

Filter List: SSList

Showing: 1 to 14 of 14

☐	Priority	Filter Name	State	Type	Protocol	Port	Port Range	QoS	VLAN	Source	Destinatio	Log
☐	1	Air-cleaner-Arp.1	On	Deny	ARP			None		Interface	Interface	Off
☐	2	Air-cleaner-Dhcp.1	On	Deny	UDP	BOOTPS_DHCP(67)		None		Interface	MAC	Off
☐	3	Air-cleaner-Dhcp.2	On	Deny	UDP	BOOTPC_DHCP(68)		None		Interface	MAC	Off
☐	4	Air-cleaner-Nbios.1	On	Deny	UDP	NETBIOS_NS(137)		None		ANY	ANY	Off
☐	5	Air-cleaner-Nbios.2	On	Deny	UDP	NETBIOS_DGM(138)		None		ANY	ANY	Off
☐	6	Air-cleaner-Nbios.3	On	Deny	UDP	NETBIOS_SSN(139)		None		ANY	ANY	Off
☐	7	Air-cleaner-Mcast.1	On	Deny	ANY			None		ANY	MAC	Off
☐	8	Air-cleaner-Mcast.2	On	Deny	ANY			None		ANY	MAC	Off
☐	9	Air-cleaner-Mcast.3	On	Deny	ANY			None		ANY	MAC	Off
☐	10	Air-cleaner-Bcast.1	On	Allow	ARP			None		ANY	MAC	Off
☐	11	Air-cleaner-Bcast.2	On	Allow	UDP	BOOTPS_DHCP(67)		None		ANY	MAC	Off
☐	12	Air-cleaner-Bcast.3	On	Allow	UDP	BOOTPC_DHCP(68)		None		ANY	MAC	Off

Figure 290. Filter Management

Note that filtering is secondary to the stateful inspection performed by the integrated firewall. Traffic for established connections is passed through without the application of these filtering rules.

Note that smaller APs that use the AOSLite system software, such as the WAP9112 and the WAP9114, have many fewer settings than more powerful APs. Application Control policies are not supported. Settings that are not available on a particular AP are not displayed, or will be grayed out.

Procedure for Managing Filters

1. **Filter List:** Select the filter list to display and manage on this window. All of the filters already defined for this list are shown, and you may create additional filters for this list.
2. **Add Preset Filters**: A number of predefined "Air Cleaner" filters are available using these buttons, as shown in You can use these very useful rules to eliminate a great deal of unnecessary wireless traffic, resulting in improved performance. For more information, please see the *Avaya WLAN AP 9100 Series (NN47252-102)*.

To create a new filter entry:

3. Click the **Add** button to display the New Filter dialog, showing the **Filter List Name** to which the new entry will belong. Enter the new **Filter Name**. The filter name must be unique within the list, but it may have the same name as a filter in a different filter list. Two filters with the same name in different filter lists will be completely unrelated to each other—they may be defined with different parameter values.
4. **Layer**: Select the network layer at which this filter will operate.
5. **Enable**: Use this field to enable or disable this filter.
6. **Type**: Choose whether this filter will be an **Allow** filter or a **Deny** filter. If you define the filter as an Allow filter, then any associations that meet the filter criteria will be allowed. If you define the filter as a Deny filter, any associations that meet the filter criteria will be denied.

   All of the remaining fields are optional.

7. **Traffic Limit Type/Traffic Limit**: Instead of prohibiting or allowing the specified traffic type, you may cap the amount of traffic allowed that matches this filter. First choose the units for the limit: kilobits per second (Kbps) for all stations in total or per station, or packets per second (pps) for all stations in total or per station. Then enter the numeric limit in the **Traffic Limit** field underneath.

8. **Protocol/Number**: Choose a specific filter protocol from the drop-down list, or choose **numeric** and enter a **Number**, or choose **ANY** to instruct the AP to use the best filter. This is a match criterion.

9. **Port/Number**: This is a match criterion. From the drop-down list, choose the target port for this filter. Choose **ANY** to instruct the AP to apply the filter to any port, or choose **NUMERIC** or **RANGE** and enter the port number or range in the provided fields.

10. **Source**: Define a source address to match as a filter criterion. Click the radio button for the desired type of address (or other attribute) to match. Then specify the value to match in the fields which appear. Choose **Any** to use any source address. Check **Not** to match any address except for the specified address.

11. **Destination**: Define a destination address to match as a filter criterion. Select the desired type of address (or other attribute) to match. Then specify the value to match in the fields which appear. Choose **any** to use any source address. Check **Not** to match any address except for the specified address.

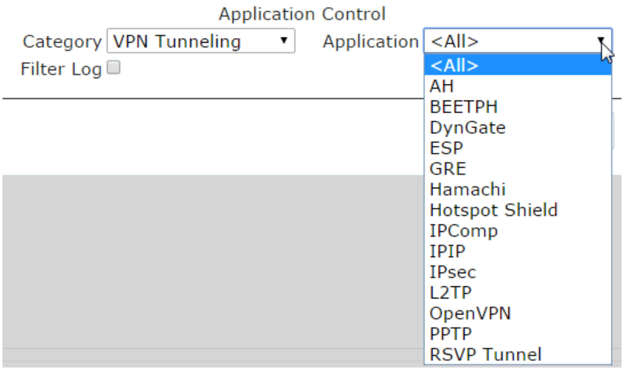
12. **DSCP:** (Differentiated Services Code Point or DiffServ—Optional) Set packets ingressing from the wireless network that match the filter criteria to this DSCP level (0 to 63) before sending them out on the wired network. Select the level from the drop-down list. Level 0 has the lowest priority; level 63 has the highest priority. By default, this field is blank and the filter does not modify DSCP level. See **“Understanding QoS Priority on the Wireless AP” on page 450**.

13. **QoS**: Set packets that match the filter criteria to this QoS level (0 to 3), selected from the drop-down list. Level 0 has the lowest priority; level 3 has the highest priority. By default, this field is blank and the filter does not modify QoS level. See **"Understanding QoS Priority on the Wireless AP" on page 450**.

14. **VLAN/Number**: Set packets that match the filter criteria to this VLAN. Select a VLAN from the list, or select **numeric** and enter the number of a previously defined VLAN (see **"VLAN" on page 391**). By default, this field is blank and the filter does not modify the VLAN.

To configure an Application Control filter, you may enter a **Category** and **Application** to be matched by the filter (see **"Application Control—Overview" on page 104**):

15. **Category**: If you wish this filter to apply to a particular category of application, such as **File-Transfer** or **VPN Tunneling**, select it from the listed options.



Application Control

Category: VPN Tunneling

Application: <All>

Filter Log □

Figure 291. Filter Category/Application

16. **Applications**: If you wish to further refine this filter to apply to a specific application within the selected **Category**, such as **OpenVPN**, select the desired application from the drop-down list.

17. **Filter Log**: If selected, log usage of this filter to Syslog.

18. Click **OK** when done.

Viewing, modifying, or deleting existing filter entries:

19. Select the desired filter entry. Click **Edit** to view or modify it.
20. **Move Up/Down**: The filters are applied in the order, starting with **Priority** level 1. To change an entry's position in the list, select it and click the **Move Up** or **Move Down** button.
21. **Delete**: Click this button to delete the selected filters.

Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Tunnels

Avaya APs offer GRE (Generic Routing Encapsulation) tunneling with VLAN support. This allows an AP to use tunnels to bridge Layer 2 traffic for one or more SSID-VLAN pairs onto a single destination network through the Layer 3 network. GRE tunneling is quite flexible, and can encapsulate many network layer protocols. As a result, it can support a variety of applications. For example, a Wi-Fi hotspot can allow guest logins and use the tunnel to give guests direct access to the Internet, without allowing access to the local network. In a small office, you may define a tunnel to connect users to the corporate office network. Tunnels may also used when providing cellular offload capability.

Tunnels may be implemented with:

- VTS —see **"Virtual Tunnel Server (VTS)" on page 391**.

To create a tunnel, you specify the **Local Endpoint**, which should be one of the AP's wired ports, and the **Primary Remote Endpoint**. A **Secondary Remote Endpoint** may also be specified in case of a failure at the first endpoint. Traffic for a VLAN-SSID pair is sent in GRE encapsulated packets across the Layer 3 network from the AP to the remote endpoint. When packets arrive, the encapsulation is stripped and the resultant packets are passed to your switch with 802.1q VLAN tags for final Layer 2 processing. The process occurs in reverse for packets traveling in the other direction. One tunnel is able to transport up to 16 VLANs.

The following pages are used to manage tunnels:

- Tunnel Management—creates and manages tunnels
- SSID Assignments—selects the SSIDs to be bridged by each tunnel

Tunnel Management

This window allows you to create and manage tunnels.

Procedure for Managing Tunnels

To create a new filter entry:

1. Click the **Add** button to display the Add Tunnel dialog. Enter the new tunnel's **Name**.
2. **Type**: Enter the type of tunnel, **none** or **gre**.
3. **Enabled**: The new tunnel is created in the disabled state. Click this checkbox to enable it.
4. **Local Endpoint**: Enter the IP address of the AP Gigabit port where the tunnel is to begin.
5. **Primary Remote Endpoint**: Enter the IP address of the remote endpoint of the tunnel.
6. **Secondary Remote Endpoint**: This provides a failover capability. If the primary tunnel fails, traffic is switched over to the secondary tunnel. Enter the IP address of the remote endpoint of the secondary tunnel.
7. **DHCP Option**: When this option is enabled, the AP snoops station DHCP requests and inserts relay agent information (option 82, in the circuit-ID sub-option) into these DHCP packets. Information inserted includes AP BSSID, SSID name, and SSID encryption type. Information is inserted as a colon-separated text string in the CIRCUIT ID value field in this format: [AP_MAC];[SSID];[ENC]

   [AP_MAC] length = 17 (aa:bb:cc:dd:ee:ff)

[SSID] length = length of SSID name
[ENC] length = 1 (encryption type: 'o' = open, 's' = non-open)

8. **MTU**: Set maximum transmission unit (MTU) size.

9. **Failover Ping Interval**: The tunnel mechanism will ping the current remote endpoint periodically to ensure that it is still reachable. Enter the ping interval (in seconds).

10. **Failover Ping Failures**: Enter the number of consecutive ping failures that will cause the AP to consider the tunnel to be down.

11. Click **OK** when done.

12. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

13. Proceed to SSID Assignments to define the SSIDs (and associated VLANs) for which each tunnel will bridge data. You may create up to 16 tunnels. Each will need an SSID/VLAN pair assigned to it so that it can function properly.

Viewing, modifying, or deleting existing filter entries:

14. Select the desired tunnel entry. Click **Edit** to view or modify it. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP.

15. **Delete**: Click this button to delete the selected filters.

SSID Assignments

This window allows you to select the SSIDs to be bridged by each tunnel. Station traffic for SSIDs assigned will be bridged through a tunnel regardless of whether these SSIDs have VLANs defined for them. If there is a VLAN defined for an SSID that is assigned to a tunnel, then station traffic bridged through that tunnel will be tagged accordingly.

Procedure for Assigning SSIDs

This window lists the tunnels and SSIDs that you have defined. SSIDs to be tunneled do not need to be associated with a VLAN (see **“SSID Management” on page 454**).

1. For each tunnel, select the SSIDs that are to be bridged to the remote endpoint. Clear the checkbox for any SSID that you no longer wish to include in the tunnel.

2. Click the **Apply Config** button at the top of the configuration window to apply these changes to the AP. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

WOS Administration

WOS may be administered from **The WOS Web Client**. The WOS web client has tools for WOS server administration.

An overview of managing the server is given in the following sections:

- **"About Managing the WOS Server" on page 549**
- **"About the WOS Database" on page 549**

Details of managing a server hosted on a Virtual Appliance are discussed in:

- **"Managing WOS on Virtual Appliances" on page 551**

About Managing the WOS Server

The tools for managing the WOS server are different, depending on the server's host platform.

- Managing the Virtual Appliance

  The Virtual Appliance running under VMware uses the browser-based WOS web client (**Figure 292 on page 551**) to manage the server. Database management functions are available in the web client.

  See the sections starting with **"Managing WOS on Virtual Appliances" on page 551**.

About the WOS Database

The WOS database maintains the properties, status, and statistics for all the managed wireless APs represented in the network, as well as configured maps, events and reports.

You can check memory use and free space available at any time when WOS is running. See **"Viewing WOS Server Status" on page 556**. That page also provides an option for reducing database size by deleting accumulated statistical data.

It is important to back up your database regularly, which means establishing a schedule that suits your network's activity.

***Note**: The WOS server does not have a default backup schedule, so it is **very important** for you to create a backup schedule after installation.*

You may set up a backup schedule to best suit your needs—the time required for a backup depends on the size of the database. And because WOS provides a client option for managing backups, they can be initiated from any client.

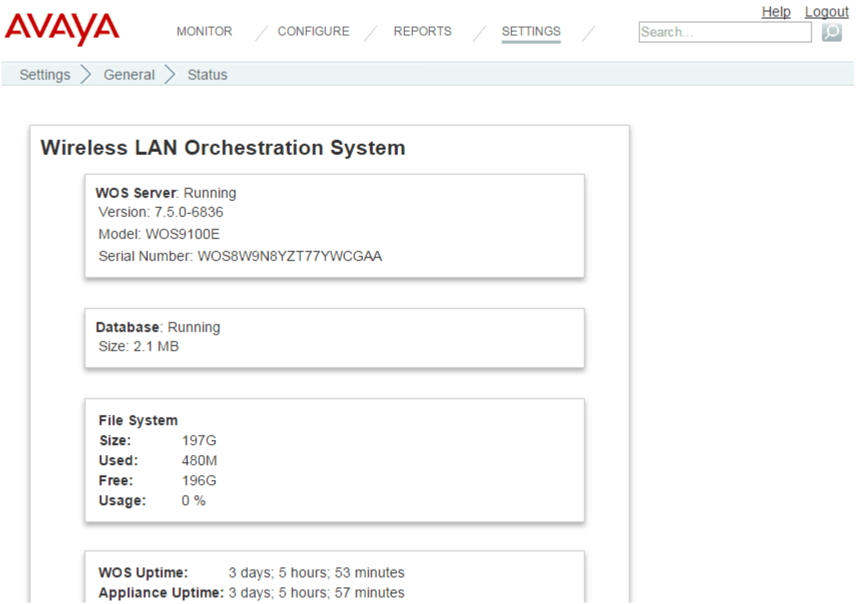
To manage the database, see:

- **"Database Backup Settings" on page 560**

WOS does not purge old backups automatically. We recommend that you periodically review the backup files on your file server and delete older ones as needed, depending on the space available on the server.

Managing WOS on Virtual Appliances

Use the browser-based WOS web client (**Figure 292**) to manage the WOS server. Use the web client to perform mandatory initial configuration, to restart or reboot the server, and for server maintenance. The WOS server is started automatically when your Appliance is restarted.



Wireless LAN Orchestration System

WOS Server: Running
Version: 7.5.0-6836
Model: WOS9100E
Serial Number: WOS8W9N8YZT77YWCGAA

Database: Running
Size: 2.1 MB

File System

Size:	197G
Used:	480M
Free:	196G
Usage:	0 %

WOS Uptime:	3 days; 5 hours; 53 minutes
Appliance Uptime:	3 days; 5 hours; 57 minutes

Figure 292. Server Management using the Web Client

The web client has multiple pages that manage settings for different WOS functions. Click **Settings** on the top of the page, then click one of the displayed links to go to the desired page. How to access the web client and descriptions of its pages are found in the following sections.

- **"Accessing the Web Client" on page 552**
- **"Initial Server Setup" on page 554**
- **"Viewing WOS Server Status" on page 556**
- **"Network Settings" on page 558**
- **"Date and Time Settings" on page 559**

- **"Database Backup Settings" on page 560**
- **"WOS Users" on page 570**
- **"Email Settings" on page 588**
- **"Polling Settings" on page 589**
- **"WOS Call-back Address" on page 591**
- **"Web Server" on page 592**
- **"SNMP Trap Receivers" on page 593**
- **"WOS Setup Wizard" on page 594**
- **"Admin RADIUS" on page 603**
- **"Audit Log" on page 607**
- **"Viewing Server Log Files" on page 608**
- **"Managing the WOS Server License" on page 610**
- **"Performing Server Upgrades" on page 611**
- **"Resetting the WOS Server" on page 612**

Accessing the Web Client

*Note: **Web client access to the WOS server requires access to port 9090 and 9443. Ensure** that this port is open in any firewalls that exist between your browser and the WOS server.*

To access the web client, set your browser's URL to the WOS server machine's IP address or host/domain name, followed by **:9090**. For example, **http://192.168.10.40:9090**.

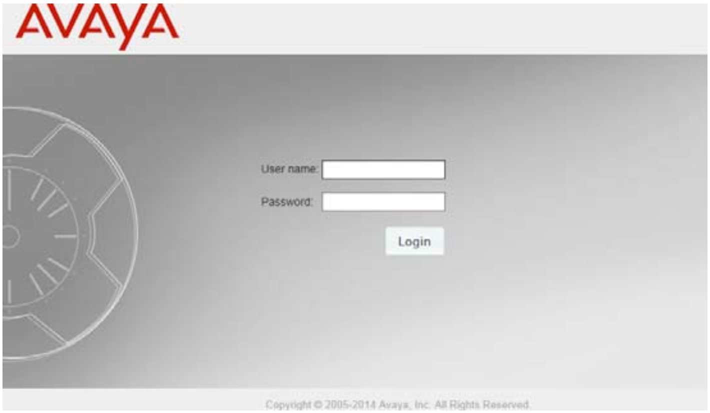


Figure 293. Starting the Web Client

Log in to the web client—the default for both fields is **admin**. In a few moments the web client Dashboard page appears. Click the **Settings** button at the top to display the Status page. (**Figure 292**) It shows a summary of the running state of the server. If you have not already performed the required initial setup for a newly installed server, proceed to **Initial Server Setup**, below. Otherwise, you may skip that section.

***Note**: You may use the Command Line Interface (CLI) to manage the WOS server. Access it at port 2022 and log in using **admin/admin**. Do **not** use port 22.*

Initial Server Setup

The following steps must be completed to configure the WOS server for proper performance. If you have already completed these steps, you may skip this section.

1. **“WOS Setup Wizard” on page 594**—use the WOS Setup Wizard to enter the license for the WOS server and start discovery of the wireless network.

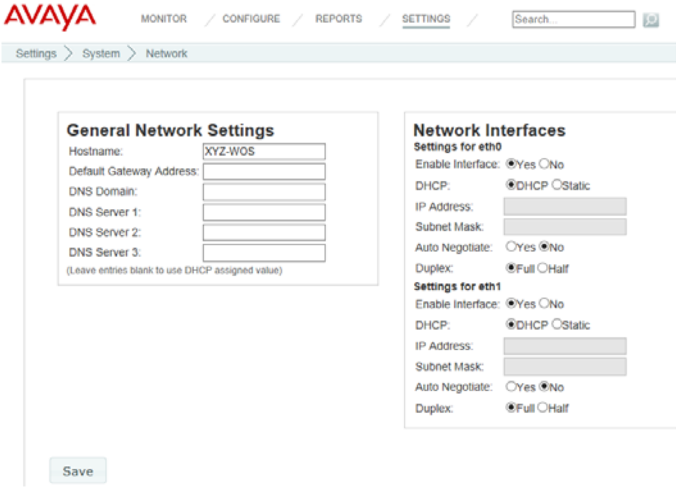
IMPORTANT! *The WOS server does not have a default backup schedule, so you must create one after installation.*

2. **“WOS Users” on page 570**—set up user accounts for WOS.

Initial Network Settings

Note: *The WOS Server requires a valid license for full operation. If one is not present, it will be requested when you open a client. See* **“Managing the WOS Server License” on page 610**.

1. Select **Settings** >**Network** to display the Network Settings window.



General Network Settings

Hostname: XYZ-WOS
Default Gateway Address:
DNS Domain:
DNS Server 1:
DNS Server 2:
DNS Server 3:
(Leave entries blank to use DHCP assigned value)

Network Interfaces

Settings for eth0
Enable Interface: ● Yes ○ No
DHCP: ● DHCP ○ Static
IP Address:
Subnet Mask:
Auto Negotiate: ○ Yes ● No
Duplex: ● Full ○ Half

Settings for eth1
Enable Interface: ● Yes ○ No
DHCP: ● DHCP ○ Static
IP Address:
Subnet Mask:
Auto Negotiate: ○ Yes ● No
Duplex: ● Full ○ Half

Figure 294. Changing Network Settings

2. We recommend that you assign a Static IP address to each Ethernet port that is connected. The Appliance uses DHCP by default. If you have configured reserved leases for the ports in your DHCP server, skip to **Step 3** below. If you leave the DNS fields on this page blank and you are using DHCP, then the gateway and DNS servers configured in your DHCP server will be used.

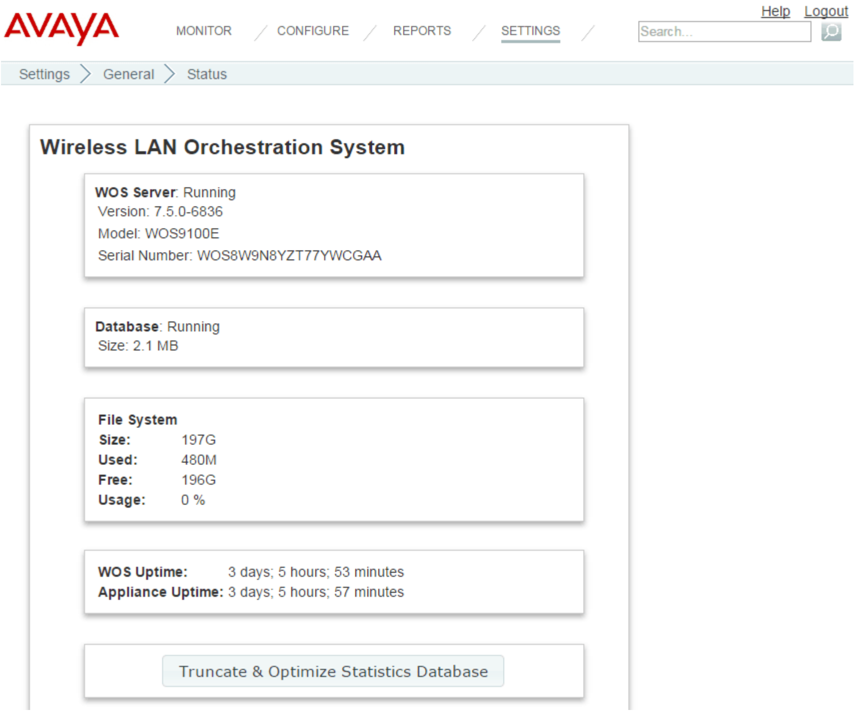
   If you have not assigned a reserved DHCP lease to the Appliance, select the **Static** option in **Configuration Server Protocol** under **Network Interfaces** for each Ethernet port that you are using. Make sure that **Enable Interface** is set to **Yes**, and enter the **IP Address** and **Subnet Mask**. Under **General Network Settings**, enter the **Default Gateway Address** and the **DNS Domain** and **DNS Servers**.

Note: *The default IP address for eth0 is 192.168.1.3; for eth1 it is 192.168.1.4.*

3. The **Hostname** of the Appliance is set to Avaya-**WOS** by default. If you wish to change the Appliance's DNS Hostname, please see **"General Network Settings" on page 558** for other changes that you should make to ensure proper operation of WOS in your network.

Viewing WOS Server Status

Click the **Status** link to review the status and version number of the WOS **Server**, and the status and size of the **Database** (in bytes). **File System** statistics show the size of your storage, how much is used, and how much space is available. WOS **Uptime** indicates how long the server has been running, while **Appliance Uptime** indicates how long the host computer has been running since its last reboot.



Wireless LAN Orchestration System

WOS Server: Running
Version: 7.5.0-6836
Model: WOS9100E
Serial Number: WOS8W9N8YZT77YWCGAA

Database: Running
Size: 2.1 MB

File System

Size:	197G
Used:	480M
Free:	196G
Usage:	0 %

WOS Uptime:	3 days; 5 hours; 53 minutes
Appliance Uptime:	3 days; 5 hours; 57 minutes

Figure 295. The Status Page

- **Truncate & Optimize Statistics Database**

  Use this button to delete **all** statistical data in the database, thus reducing its size and improving server performance. When you click this button, you must supply your user name and password. You will be advised to perform a backup first, since statistics will be permanently deleted. Access Point configuration data is not affected. The WOS server will be shut down, statistics are deleted, and the database is optimized and compacted. When this is complete, the WOS server is rebooted.

- **Restart Application**

  If WOS is not running properly, you may click the **Restart Application** button on the lower left to restart the WOS server software. If the server is currently running, an orderly shutdown will be performed first.

- **Reboot Appliance**

  The **Reboot Appliance** button will reboot the Management Appliance—this will shut down WOS related processes in an orderly manner before rebooting. Rebooting and restarting will take about two minutes on a new Management Appliance. As WOS is used and the database grows, startup integrity checks will take longer. For shutdown, see below.

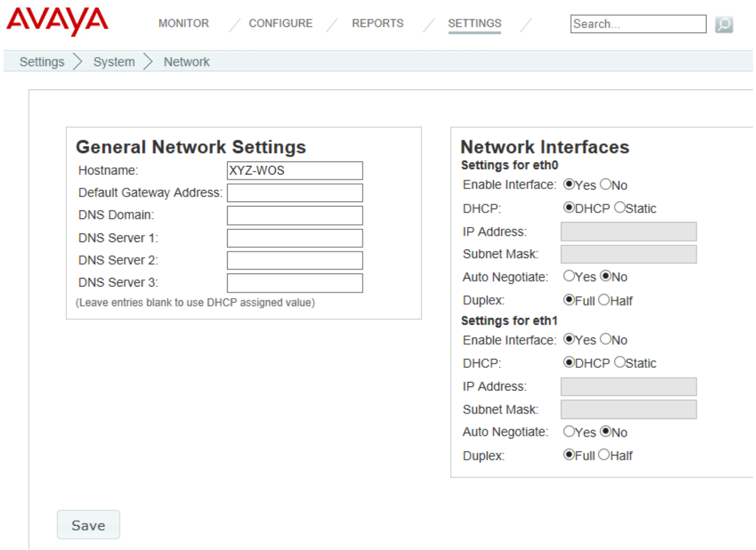
Shutting down the WOS Server

Shutting down the server incorrectly can cause problems the next time you start WOS. Use the following procedure:

1. Close all clients.
2. On the Status page, click the **Shutdown Appliance** button.
3. The Management Appliance will then gracefully shut down. A confirmation notice is displayed immediately when the shutdown process is initiated. It may take a few minutes for the Appliance to actually shut down and power itself off.

Network Settings

Select the **Network** link to display the Network Settings page. This page allows you to manage DNS settings for the server, and set the IP address and transmission parameters for the Ethernet ports.



General Network Settings

Hostname: XYZ-WOS
Default Gateway Address:
DNS Domain:
DNS Server 1:
DNS Server 2:
DNS Server 3:
(Leave entries blank to use DHCP assigned value)

Network Interfaces

Settings for eth0

Enable Interface: ● Yes ○ No
DHCP: ● DHCP ○ Static
IP Address:
Subnet Mask:
Auto Negotiate: ○ Yes ● No
Duplex: ● Full ○ Half

Settings for eth1

Enable Interface: ● Yes ○ No
DHCP: ● DHCP ○ Static
IP Address:
Subnet Mask:
Auto Negotiate: ○ Yes ● No
Duplex: ● Full ○ Half

Figure 296. Changing Network Settings

***Note**: You may use one or both of the WOS Management Appliance's Ethernet ports. If using both, then one of the ports is typically reserved for management.*

- **Network Interfaces—Settings for eth0 and eth1**

  Check that **Enable Interface** is set to **Yes** for each Ethernet port that you plan to use. **Auto Negotiate** should normally be left enabled, which is the default. This will correctly set the Ethernet port's speed and duplex mode automatically in most cases.

  For recommended IP addressing, please see **"Initial Network Settings" on page 554**.

- **General Network Settings**

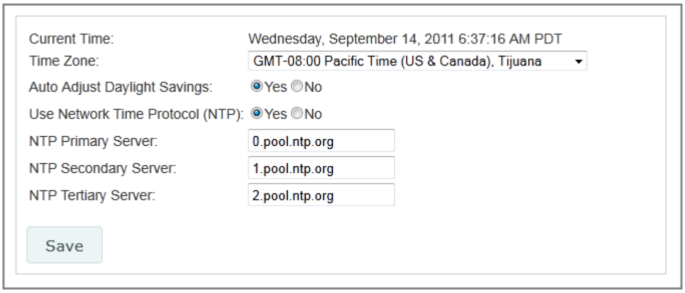
  The **Hostname** of the Appliance is set to **Avaya-WOS** by default. Note that hostnames are not case-sensitive. Avaya APs send traps to the hostname Avaya-**WOS** to announce their presence on the network and speed discovery. Thus, if you change the Appliance's DNS Hostname, you should create an alias in your network's DNS server to ensure that the Appliance is accessible using both the name **Avaya-WOS** and your new name.

If you have clicked the **Static** radio button under **Network Interfaces - Configuration Server Protocol**, you must enter the **Default Gateway Address** for this Appliance, and enter the **DNS Domain** and **DNS Servers**.

Click the **Save** button when you have finished making your changes.

Date and Time Settings

NOTE: *To use SNMPv3 successfully, system time must be set using an NTP server on both the WOS server host machine and all APs using SNMPv3. This is because SNMPv3 requires synchronization between the WOS server and the APs so that the system time difference between them never exceeds more than 150 seconds. If the time difference exceeds 150 seconds, SNMPv3 suspects a security breach and removes the SNMPv3 credentials for affected APs from the database. This means that the AP will appear to be down and statistics will not be polled until the AP is re-discovered. A manual refresh of the AP should remedy the situation. See* **"Add Devices" on page 163**.



Current Time:	Wednesday, September 14, 2011 6:37:16 AM PDT
Time Zone:	GMT-08:00 Pacific Time (US & Canada), Tijuana
Auto Adjust Daylight Savings:	● Yes ○ No
Use Network Time Protocol (NTP):	● Yes ○ No
NTP Primary Server:	0.pool.ntp.org
NTP Secondary Server:	1.pool.ntp.org
NTP Tertiary Server:	2.pool.ntp.org

Figure 297. Changing Date and Time Settings

Click the **Date & Time** link to display the Date and Time page. This page manages your time zone and sets the time manually or sets up Network Time Protocol usage to obtain accurate time settings automatically.

- **Time Zone** and **Daylight Savings Time**

  Select your local **Time Zone** from the drop-down list.

  Enable **Auto Adjust Daylight Savings** if you want the system to adjust for daylight savings automatically, otherwise click **No**.

- Using **Network Time Protocol**

  To have the time of day set automatically from an accurate time server, set **Use Network Time Protocol** to **Yes** (this is the default). You may modify the **NTP Servers** (primary, secondary, tertiary), or leave them at the default values which use NTP Pool time servers (http://www.pool.ntp.org/).

- Setting time manually

  Set **Use Network Time Protocol** to **No**. Use the **Adjust Time** and **Adjust Date** fields that appear to set the correct time and date.

Click the **Save** button when you have finished making your changes. After saving, WOS will reboot.

Database Backup Settings

The WOS server does not have a default backup schedule, so you should perform the following steps soon after you have installed the WOS server:

- **Manage Locations**—set up one or more locations for storing backup files.
- **Manage Schedules or Backup Now**—set up a schedule for performing backups.

The following pages are used to manage WOS backups:

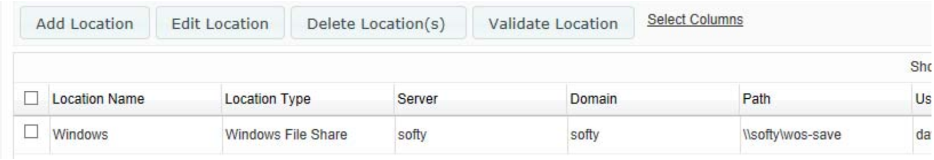
- **"Manage Locations" on page 561**
- **"Manage Schedules or Backup Now" on page 565**
- **"Restore" on page 567**
- **"Import Backup Archive" on page 568**
- **"Backup Status" on page 569**

Note: On the Virtual Appliance servers, the database and all configuration files are backed up, including any uploaded files for captive portals, software update, etc.

Manage Locations

This page sets backup locations for the WOS database. To display this page, click the **Manage Locations** link in the **Backup** section under **Settings** at the top of the web client page.

The Backup Locations list shows the entries that you have already created.



□	Location Name	Location Type	Server	Domain	Path	Us
□	Windows	Windows File Share	softy	softy	\\softy\wos-save	da

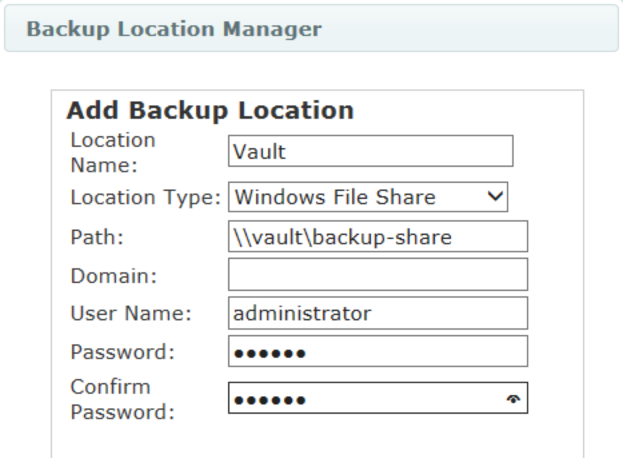
Figure 298. Backup Locations List

The WOS server has one predefined location, **local**, which is stored on the server machine's file system (although it does not appear in the Backup Locations list). For improved data protection, we recommend that you define and use at least one location for backups, other than on the server. For example, you might perform an on-site backup weekly and an off-site backup monthly.

To specify a backup location, click **Add Location**. Enter a **Name** for this location entry. The remainder of the entry depends on the **Location Type** that you select.

- **Location Type: Windows File Share** (Figure 299)
  - Specify the **Path** for the folder where files are to be stored. The path must use the Windows Uniform Naming Convention (UNC) format (\\*ComputerName**SharedFolder**Resource*) or the Server Message Block Protocol (SMB) format (smb://URL).
  - You may enter a **Domain** name if necessary. If the backup location is on a standalone server, you should normally leave the domain field blank.
  - Enter a **User Name** and **Password/Confirm Password** that will give you write privileges for that folder. While the username and

password are optional, we highly recommend that the backup file server be configured to require password protection.

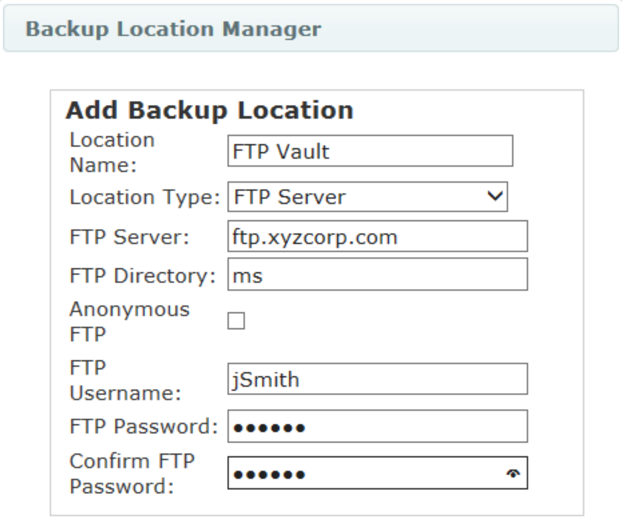


Add Backup Location

Location Name:	Vault
Location Type:	Windows File Share
Path:	\\vault\backup-share
Domain:	
User Name:	administrator
Password:	••••••
Confirm Password:	••••••

Figure 299. Backup Location—Windows File Share

- **Location Type: FTP** (Figure 300)
  - Specify the **FTP Server** where files are to be stored, for example, *ftp.xyzcorp.com*.
  - Specify the **FTP Directory** for the backup files.
  - If you do not select **Anonymous FTP,** enter an **FTP Username** and **FTP Password/Confirm FTP Password** that will give you write privileges for that folder.



Backup Location Manager

Add Backup Location

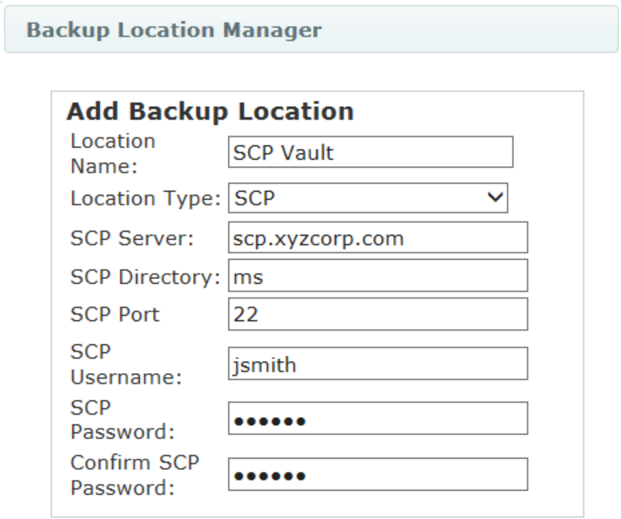
Location Name:	FTP Vault
Location Type:	FTP Server
FTP Server:	ftp.xyzcorp.com
FTP Directory:	ms
Anonymous FTP	□
FTP Username:	jSmith
FTP Password:	••••••
Confirm FTP Password:	••••••

Figure 300. Backup Location—FTP

- **Location Type: SCP** (Figure 301)

  SCP uses the Secure Copy Protocol, based on SSH, for data transfer.

  - Specify the **SCP Server** where files are to be stored—the hostname, DNS name, or IP address of the SCP server.
  - Specify the **SCP Directory** for the backup files.
  - If you need to change the **SCP Port** from the default value of **22**, enter it here.
  - Enter an **SCP Username** and **SCP Password/Confirm SCP Password** that will give you write privileges for that folder.



Backup Location Manager

Add Backup Location

Location Name:	SCP Vault
Location Type:	SCP
SCP Server:	scp.xyzcorp.com
SCP Directory:	ms
SCP Port	22
SCP Username:	jsmith
SCP Password:	••••••
Confirm SCP Password:	••••••

Figure 301. Backup Location—SCP

Click **OK** when done. WOS will verify that it is able to access the location and will inform you of its success or failure. This location will be added to the displayed list of backup locations. Click **Add Location** again if you wish to enter another backup location.

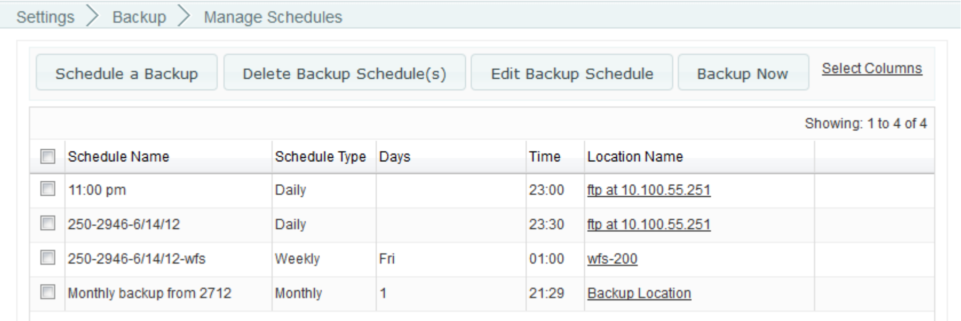
Note that you may change a location entry by selecting it and clicking **Edit Location**. You may delete one or more location entries by selecting them and clicking **Delete Location(s)**.

Once you have successfully specified the backup location, you may proceed to use the other Backup pages.

Manage Schedules or Backup Now

This page specifies when scheduled backups are to be performed automatically. To display it, click the **Manage Schedules** link or the **Backup Now** link in the **Backup** section under **Settings** at the top of the web client page.

The Schedule Name list shows the schedules that you have already created.

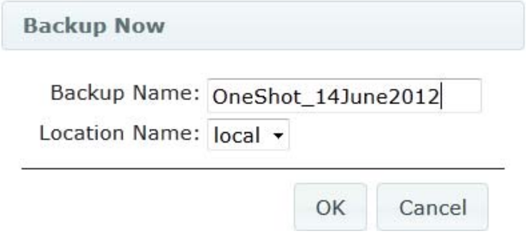

Settings > Backup > Manage Schedules
Schedule a Backup
Delete Backup Schedule(s)
Edit Backup Schedule
Backup Now
Select Columns

Showing: 1 to 4 of 4

□	Schedule Name	Schedule Type	Days	Time	Location Name
□	11:00 pm	Daily		23:00	ftp at 10.100.55.251
□	250-2946-6/14/12	Daily		23:30	ftp at 10.100.55.251
□	250-2946-6/14/12-wfs	Weekly	Fri	01:00	wfs-200
□	Monthly backup from 2712	Monthly	1	21:29	Backup Location

Figure 302. Backup Schedule List

If you wish to perform a one-time immediate backup, click the **Backup Now** link. Enter a **Backup Name** and select a **Location Name** specifying where to put the file. Click **OK**. You will automatically be taken to the **Backup Status** page to view the results.



Backup Name: OneShot_14June2012

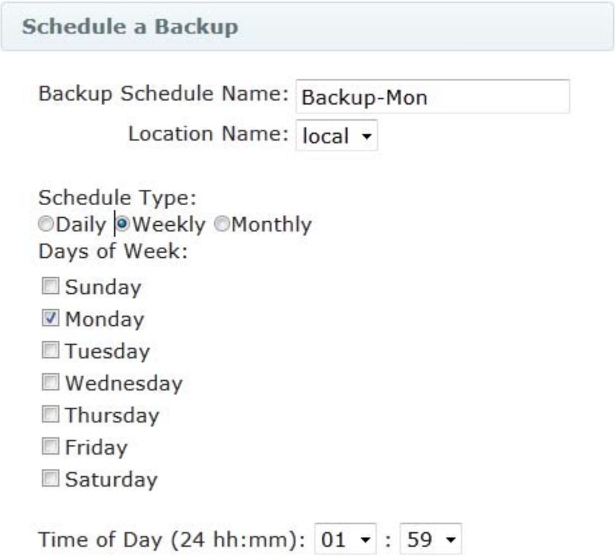
Location Name: local

Figure 303. Backup Now

To enter a schedule, click the **Schedule a Backup** button. (**Figure 304**) We recommend that you schedule backups for off-peak usage hours since they can generate significant activity on the server.

Enter a **Backup Schedule Name** for this schedule entry and select a **Location Name** to use for the backup. (**Figure 304**) If you wish the backup to go to multiple locations, you can schedule another backup for that location (or copy the backup file).

Select the **Schedule Type**: **Daily**, **Weekly**, or **Monthly**.



Schedule a Backup

Backup Schedule Name: Backup-Mon

Location Name: local

Schedule Type:
○ Daily ● Weekly ○ Monthly

Days of Week:
- □ Sunday
- ☑ Monday
- □ Tuesday
- □ Wednesday
- □ Thursday
- □ Friday
- □ Saturday

Time of Day (24 hh:mm): 01 : 59

Figure 304. Enter a Backup Schedule

Depending on the selected **Schedule Type**, different fields will be displayed. For a monthly backup, specify the day of the month (only one day may be selected, but you can always specify more schedule entries for additional monthly backup days). For a weekly backup, check all of the days of the week on which the backup is to be performed (one or more days are allowed).

Regardless of the selected **Schedule Type**, enter the **Time of Day** for the backup. Then click the **OK** button underneath. Your new schedule entry will be listed, showing its name and scheduled days and time. For example, **Figure 304** shows an entry named **Backup-Mon** which will be performed every Monday at 1:59AM.

To remove schedule entries, select them and then click **Delete Backup Schedule(s)**. This deletes schedule entries, not backups (like those that are listed on the **Restore** page).

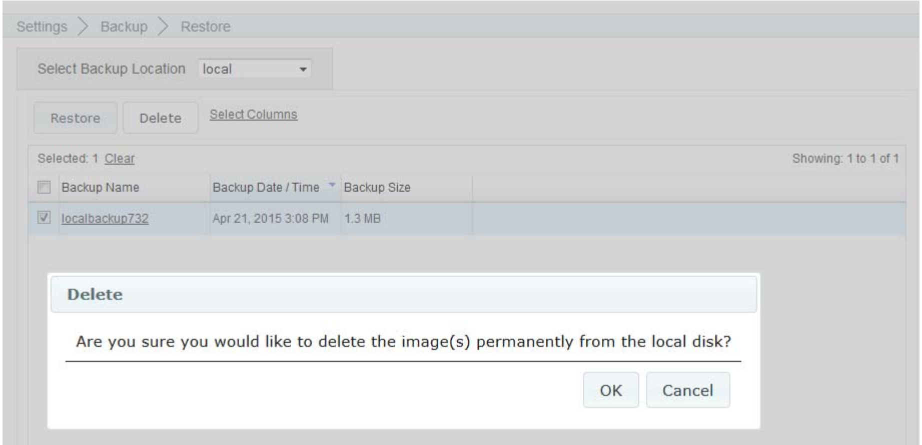
To edit a schedule entry, select it and then click **Edit Backup Schedule**.

To see the status of backups, including current and completed backups, use the **Backup Status** page.

Restore

This page lists completed backups and allows you to select and restore one of them, or to delete unneeded backups to free up space. To display this page, click the **Restore** link in the **Backup** section under **Settings** at the top of the web client page.

Choose a value from the drop-down list in **Select Backup Location** to display a list of all the backup files found in the specified location. Each backup is identified by its **Backup Name**, **Backup Date/Time**, and **Backup Size**. (**Figure 305**) The most recent backup is listed first.



Select Backup Location: local

	Backup Name	Backup Date / Time	Backup Size
☑	localbackup732	Apr 21, 2015 3:08 PM	1.3 MB

Are you sure you would like to delete the image(s) permanently from the local disk?

Figure 305. Restoring Backups

If you wish to restore your WOS database from a previously saved version, select that entry and click the **Restore** button. You will be asked enter your password to verify your permission to proceed.

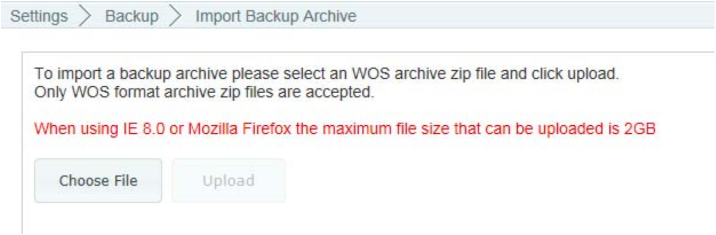
The restore operation can impact system performance and should be scheduled for off-peak hours. After the restore operation is complete, you **must** take these actions:

- Close all WOS client applications.
- Reboot the WOS Appliance.

To remove backups from the current backup location, click the checkboxes of the files that you want to remove, then click **Delete**. You will be asked to verify the deletion.

Import Backup Archive

This feature uploads a backup archive from a specified location to the WOS server so that it can be restored. This is instead of using a backup location. For example, you can back up a WOS server using the **local** backup location and then download the entire archive to another location via HTTP in the browser. You can then take that backup archive and import it to another WOS server.



To import a backup archive please select an WOS archive zip file and click upload.
Only WOS format archive zip files are accepted.

When using IE 8.0 or Mozilla Firefox the maximum file size that can be uploaded is 2GB

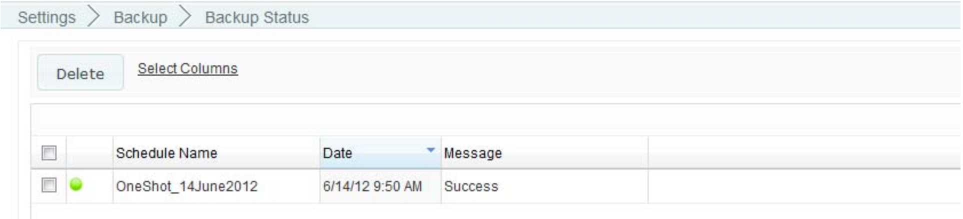
Figure 306. Import Backup Archive

Backups are archive zip files that have a specialized WOS format. Only files in this WOS-generated backup format are accepted for import.

To import a backup, click **Choose File** and browse to the desired file. Then click **Upload**.

Backup Status

This page lists current and recent backups and shows their status. To display it, click the **Backup Status** link in the **Backup** section under **Settings** at the top of the web client page.



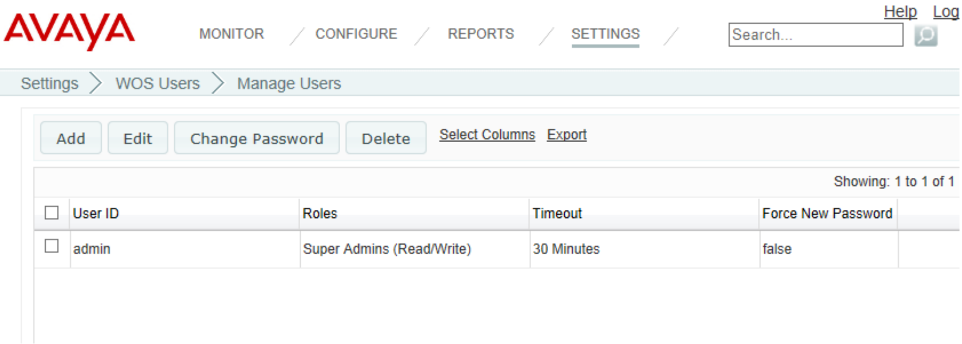
		Schedule Name	Date	Message
□	●	OneShot_14June2012	6/14/12 9:50 AM	Success

Figure 307. Backup Status

WOS Users

This page manages local WOS user accounts allowing access to WOS. You may add, edit, delete, or export accounts, or change passwords. Note that WOS access may also be authenticated using RADIUS—see **"Admin RADIUS" on page 603**. If you have configured Admin RADIUS servers, then authentication will be attempted using those first. If that fails, the local WOS user accounts will be tried.

Open the WOS Users page by clicking the **Settings** link near the top of the window, then select WOS **Users**. You may export values, or modify the display of this page (sorting, selecting columns, etc.) in the same way described in **"About Using the Access Points Page" on page 61**.

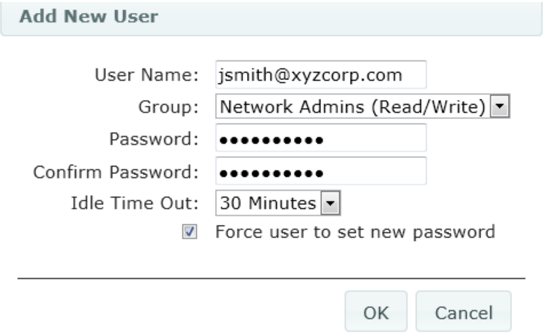


Showing: 1 to 1 of 1

□	User ID	Roles	Timeout	Force New Password
□	admin	Super Admins (Read/Write)	30 Minutes	false

Figure 308. Managing WOS User Accounts

This page contains a list of all user accounts currently available. (**Figure 308**) To create an account for a new WOS user, click the **Add** button on the upper left. The Add New User dialog is displayed. (**Figure 309**)



Add New User

User Name: jsmith@xyzcorp.com

Group: Network Admins (Read/Write)

Password: ●●●●●●●●●●

Confirm Password: ●●●●●●●●●●

Idle Time Out: 30 Minutes

☑ Force user to set new password

Figure 309. Add a WOS User Account

Enter the following fields, then click **OK** when done.

- **User Name**—Enter a unique name for the new user, just a user name is sufficient, e.g., **jsmith**.
- **Group**—Choose the privilege level from the drop-down list, either admins with read/write privileges (called **Super Admins**), or **Users** with read-only privileges. Read-only users can not make changes to WOS settings or to AP configuration.
- **Password**—Enter a password for this user.
- **Confirm Password**—Repeat the password for this user.
- **Idle Time Out**—If a user session is idle for this length of time, the user is logged out. Select an idle time from the drop-down list, or select **Never** to prevent the user from timing out.
- **Force user to set new password**—at the first login, the user will be prompted (and required) to enter a new password.

To modify the permissions or timeout for a user account, select the checkbox to the left of the entry and click the **Edit** button on the upper left. Make the desired changes and click **OK**. The changes will be applied the next time that the user logs in, but will not affect a currently logged in user.

To modify a user's password, select the checkbox to the left of the entry and click the **Change Password** button. You must correctly enter the user's **Old Password**, then enter the **New Password** and retype it in **Confirm Password**, then click **OK**.

To remove one or more user accounts, select the checkboxes to the left of the entries and click the **Delete** button. You will be asked to verify this action.

Customization

The Customization pages allow you to define your own custom fields and action buttons for the **Monitor—Access Points** and **Access Points (Configure)** pages. These fields allow you to add all kinds of information and functionality to WOS for APs. For example, you might use extra columns to add an Asset Tag to each AP, or to add notes on support cases.

Using a Custom Action, you might add a button to access your company's web portal for managing assets. Then you can open the portal to manage a selected AP with a click of the button.

These features are discussed in the following pages:

- **Create Custom Fields**

  Use this page to define a new column to add to the APs table, where you can place AP information that your company uses.

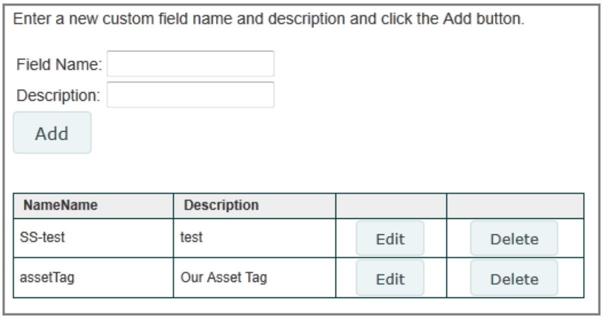
- **Create Custom Actions**

  Use this page to add a button for a new function. Define the action that the button will take by specifying a URL. The URL can start your desired web application with data based on the currently selected AP.

Create Custom Fields

This page is used to define a new column for the APs list. This column will be available on the **Monitor—Access Points** page and the **Access Points (Configure)** page. You may add up to five new columns and use them for any sort of information that you'd like to keep with each AP. For example, you might add an asset tag column, or a column for notes regarding support actions for this AP.

Open this page by selecting **Create Custom Fields** from the **Settings** menu near the top of the window.



Enter a new custom field name and description and click the Add button.

Field Name:

Description:

NameName	Description		
SS-test	test	Edit	Delete
assetTag	Our Asset Tag	Edit	Delete

Figure 310. Custom Fields Page

Enter the desired **Field Name** for the new column (this name will be used as the header for this column in the APs list), and add an optional **Description** for your reference if you wish. The description will only appear in the list of fields on the Custom Fields page—it is not used anywhere else. Click **Add** when done. You may repeat the procedure to create up to a total of five new fields. Each new column may be used to contain strings up to 255 characters long.

The new field will be displayed in the list below the **Add** button. You may remove an entry by clicking the **Delete** button to its right. You may modify the **Field Name** or **Description** by clicking the **Edit** button to its right. If you have populated this custom column with data, the data will be unaffected and will still exist under the edited **Field Name**.

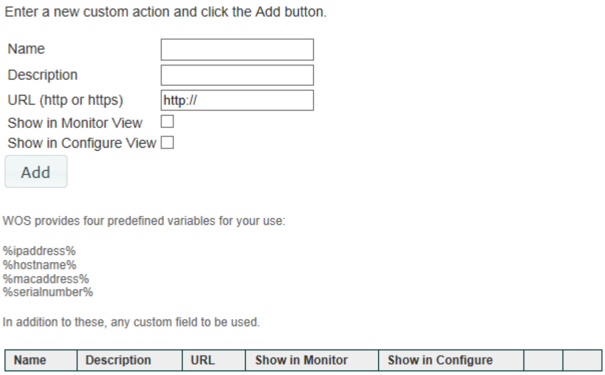
The new column is not automatically displayed on the APs list. To display it, go to the **Monitor—Access Points** page or the **Access Points (Configure)** page and use the **Select Columns** function. The new field is typically found by scrolling to the bottom of the **Hidden Columns** list. See **“Select Columns” on page 62** for more details.

To populate the new column with data for as many APs as you like, see **“Import Access Point Custom Fields” on page 128** or **“Custom Field Values” on page 126**.

Create Custom Actions

This page allows you to define a custom button that adds a new function to the APs list. Associate an action with the button by specifying a URL to open when the button is pushed. The URL can include variables. For example, suppose you added the new column titled **assetTag** to the APs list using the **Create Custom Fields**, and then you entered values for this field for each AP using the **Create Custom Actions** page. You could then define a new button labeled **Asset Tracking**, for example, that would go to your Asset Tracking Manager with a selected AP’s asset tag, using the URL:

http://track.xyzcorp.com/?assettagno=%assetTag%



Enter a new custom action and click the Add button.

Name	
Description	
URL (http or https)	http://
Show in Monitor View	□
Show in Configure View	□

WOS provides four predefined variables for your use:

%ipaddress%
%hostname%
%macaddress%
%serialnumber%

In addition to these, any custom field to be used.

Name	Description	URL	Show in Monitor	Show in Configure		

Figure 311. Custom Actions Page

You may choose to add the custom action button to the Monitor—**Access Points** page and/or to the **Access Points (Configure)** page. You may add a number of new custom actions.

Open this page by selecting **Create Custom Actions** from the **Settings** menu near the top of the window. (**Figure 311**)

Enter the desired **Name** for the new button (this name will be used as the button's label), and add an optional **Description** for your reference if you wish. The description will only appear in the list of entries on the Custom Actions page—it is not used anywhere else.

Enter the URL to go to when this custom button is pushed. The URL may include one or more variables:

> http://track.xyzcorp.com/?assettagno=%assetTag%

You may use **http** or **https**. To pass a custom field name to a variable in the URL, just surround the name with **%** signs, as shown above for the custom field that we defined named **assetTag**.

WOS provides four predefined variables for your use:

- %ipaddress%
- %hostname%
- %macaddress%
- %serialnumber%

Select the page(s) where you want the new custom action button to appear. Select **Show in Monitor View** to add the custom action to the Monitor—**Access Points** page. Select **Show in Configure View** to add the custom action to the **Access Points (Configure)** page. You may add the action to either, or to both.

Click **Add** when done.

The new custom action will be displayed in the list below the **Add** button. You may remove an entry by clicking the **Delete** button to its right. You may modify any of the actions settings by clicking the **Edit** button to its right.

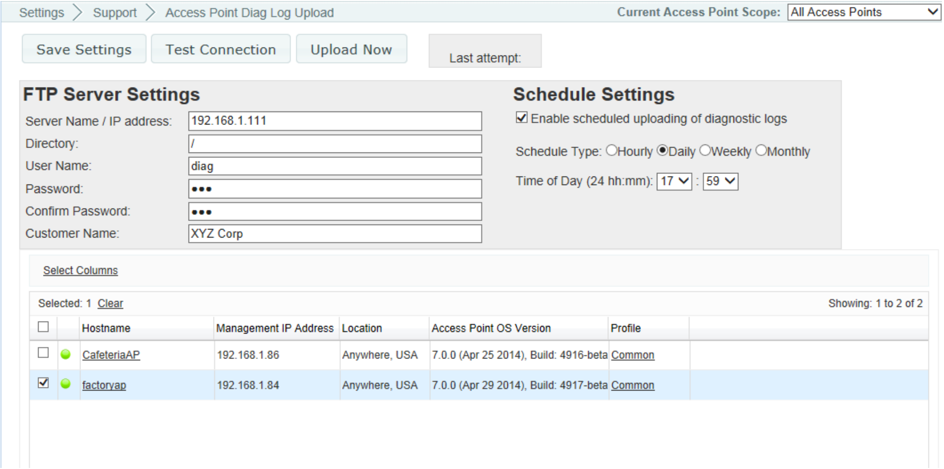
Support

The support pages provide automated processes for Avaya personnel to quickly gather the information they need to check on beta software performance and to provide information for future improvement. Currently, there is only one support page.

AP Diag Log Upload

This page is provided as a utility for gathering data from APs in your network that are running beta release software, although it may be used with APs running older Avaya OS versions as well. It provides a mechanism that can automatically upload AP diagnostic logs to Avaya so that the information required to monitor and improve beta product performance is available. You may also use this page to upload diagnostic files to your own FTP server.

The settings allow you to specify an FTP server for uploading log files, test the connection to the server, optionally set a schedule for uploading times, and select the APs from which to gather diagnostic logs. When an AP Diag Log Upload starts, all of the selected APs will generate diagnostic information, which is then uploaded by this utility.



Current Access Point Scope: All Access Points

FTP Server Settings

Server Name / IP address:	192.168.1.111
Directory:	/
User Name:	diag
Password:	•••
Confirm Password:	•••
Customer Name:	XYZ Corp

Schedule Settings

☑ Enable scheduled uploading of diagnostic logs

Schedule Type: ○Hourly ●Daily ○Weekly ○Monthly

Time of Day (24 hh:mm): 17 : 59

Selected: 1 Clear Showing: 1 to 2 of 2

□		Hostname	Management IP Address	Location	Access Point OS Version	Profile
□	●	CafeteriaAP	192.168.1.86	Anywhere, USA	7.0.0 (Apr 25 2014), Build: 4916-beta	Common
☑	●	factoryap	192.168.1.84	Anywhere, USA	7.0.0 (Apr 29 2014), Build: 4917-beta	Common

Figure 312. AP Diagnostic Log Upload

The settings for this page are described in the following sections:

- **Set Up FTP Server**
- **Enter a Schedule (optional)**
- **Select APs and Test Connection**

Set Up FTP Server

Specify **Server Name** or **IP Address**, the **Directory**, and login details. Typically, if Avaya personnel request your diagnostic logs, they will provide you all the details for connecting to the proper FTP server.

Enter a Schedule (optional)

If you want diagnostic logs to be sent automatically on a regular schedule, specify the **Schedule Type**: **Hourly**, **Daily**, **Weekly** or **Monthly**. Additional fields will be displayed as appropriate. For example, **Time of Day** is requested for a daily schedule.

Select APs and Test Connection

Select the check boxes to the left of the APs whose diagnostic files are to be collected. If you are sending data for a set of APs that are running a particular software release, you may find it handy to sort the APs by clicking on the **Software Version** column header.

When you are done, click the **Test Connection** button to check that the APs can connect to the specified FTP server and write files to it. When this test runs correctly, click the **Save Settings** button to save the FTP Server information, schedule (if any), and your other settings. Once you have selected the APs and verified the connection to the server, you may use the **Upload Now** button to do a one-shot collection and upload of diagnostic files.

WOS API

WOS provides an API interface conforming to the RESTful API model. Developers of custom applications may use this read-only API to fetch information from the WOS database. The interactive API Documentation page provides documentation for the API. Security for the WOS RESTful API is provided with tokens granted using an OAuth 2.0 mechanism.

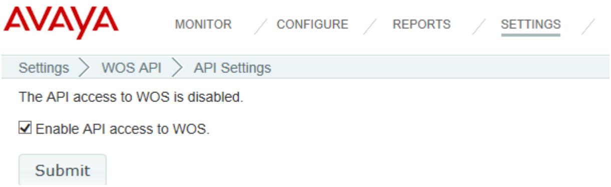
Your custom application may use the WOS API for purposes such as integrating with third party applications or creating your own applications for network analysis. Using the RESTful API eliminates the need to use SNMP which can be cumbersome for polling large amounts of data. Results are returned in JSON format (JavaScript Object Notation), a text-based open standard for human-readable data interchange. API documentation is tightly integrated with the server code. The **API Documentation** page allows you to interact with the API in a sandbox UI that gives clear insight into the API response to parameters and options.

The WOS API is described in the following topics:

- **"API Settings" on page 580**
- **"Obtaining an OAuth Token" on page 580**
- **"Using the API Interface" on page 581**
- **"API Documentation" on page 582**
- **"API Documentation Toolbar" on page 587**

API Settings

The WOS RESTful API is disabled by default. Use this page to enable granting of tokens and access to the WOS API. To open this page, click **Settings** at the top of the page and then use the **API Settings** link.



The API access to WOS is disabled.

☑ Enable API access to WOS.

Figure 313. API Settings

Make sure that the checkbox for **Enable API access to WOS** is checked, then click the **Submit** button.

Obtaining an OAuth Token

Security for the WOS RESTful API is provided with OAuth 2.0. Your custom application must request a token from an authorization server on the WOS server. That token is then presented to access the WOS API. The authorization server uses the OAuth 2.0 standard's client credential grant model. This allows you to obtain a token by presenting credentials from an admin or user account. Please note that the authorization server will issue only **one** token on behalf on of any account at any given time. If you have a need for multiple tokens, then you will need multiple accounts.

Presenting User Credentials for a Token

Enable API access to WOS as described in **API Settings** before requesting a token. A user-developed application must request a token by presenting the following information to this URL:

https://<*WOS-server hostname or IP addr*>:9443/oauth/token

- **client_id**: username of an administrator or user account on the AP (username and client_id must match).
- **client_secret**: password for the same account on the AP.
- **grant_type**: **client_credentials**

The authorization server provides a token that your application may use for read-only access the WOS API. This token remains valid for 7 days (604800 seconds). The token will not be affected by deletion of the original account associated with it, or by a password change on that account.

For example, you might use the cURL command below to request a token. In this example, the command is executed on the WOS server directly (localhost).

```
curl -X -v -d
'client_id=<username>&client_secret=<password>&grant_type=
client_credentials' -X POST “https://localhost:9443/oauth/token”
```

Example result:

```
{"access_token":"be0f81fb-b41f-44fa-b56a-c8979fdef949",
"token_type":"bearer","expires_in":604799,"scope":"read"}
```

Using the API Interface

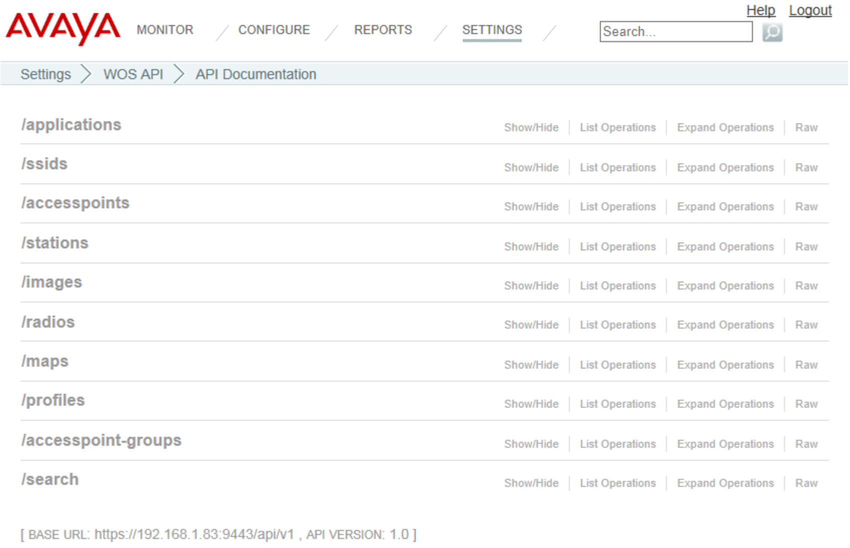
Once registration is completed and a token has been obtained, your application may access the RESTful API at the following URL. This is displayed on the bottom of the **API Documentation** page as **BASE URL**. Use the token that you obtained above, your client credentials, and the ***<api-name>*** and parameters described in the **API Documentation**.

```
https://<WOS-server hostname or IP addr>:9443/api/v1/<api-name>
```

The API response is described in detail in the **API Documentation**, and you may click the **Try it out** button to see the actual response to a particular call.

API Documentation

The API Documentation page lists all of the APIs that are available along with their calling parameters, if any, and allows you to perform sample calls and view sample output.



/applications Show/Hide | List Operations | Expand Operations | Raw

/ssids Show/Hide | List Operations | Expand Operations | Raw

/accesspoints Show/Hide | List Operations | Expand Operations | Raw

/stations Show/Hide | List Operations | Expand Operations | Raw

/images Show/Hide | List Operations | Expand Operations | Raw

/radios Show/Hide | List Operations | Expand Operations | Raw

/maps Show/Hide | List Operations | Expand Operations | Raw

/profiles Show/Hide | List Operations | Expand Operations | Raw

/accesspoint-groups Show/Hide | List Operations | Expand Operations | Raw

/search Show/Hide | List Operations | Expand Operations | Raw

[BASE URL: https://192.168.1.83:9443/api/v1 , API VERSION: 1.0]

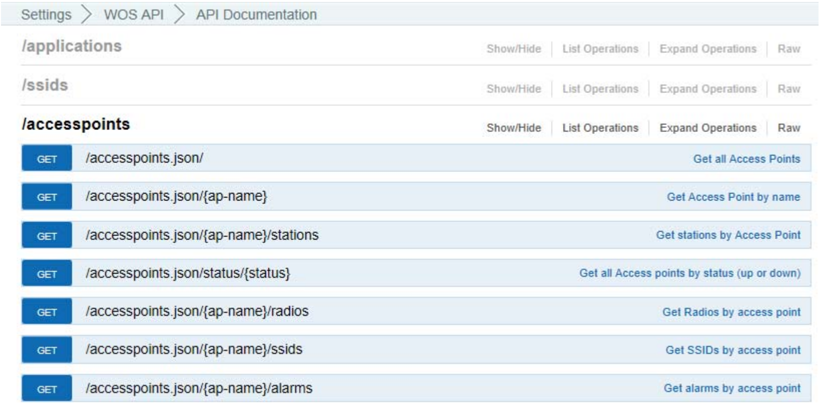
Figure 314. WOS API Documentation

The WOS API is read-only and consists almost entirely of GET methods. It may include POST methods, but the purpose of these is to fetch information in unusual cases.

API Types

The RESTful API on WOS is broken into a number of headings by type, such as: **applications, access points,** and **profiles**. Each heading is a node that may be clicked to expand or collapse the list of corresponding API requests available in WOS. Since this is a read-only API, the list consists almost exclusively of GET operations.

The figure below shows part of the list displayed by clicking **/accesspoints**. Click again to collapse (hide) the list. The **.json** string in the names shown, for example **GET /accesspoints.json/{ap-name}/ssids**, indicates that the return values use JSON formatting. A parameter in brackets, e.g., **{ap-name}**, indicates that information is returned for a particular item (in this case, the named Access Point), rather than for all Access Points.


Settings > WOS API > API Documentation

/applications — Show/Hide | List Operations | Expand Operations | Raw

/ssids — Show/Hide | List Operations | Expand Operations | Raw

/accesspoints — Show/Hide | List Operations | Expand Operations | Raw

GET	/accesspoints.json/	Get all Access Points
GET	/accesspoints.json/{ap-name}	Get Access Point by name
GET	/accesspoints.json/{ap-name}/stations	Get stations by Access Point
GET	/accesspoints.json/status/{status}	Get all Access points by status (up or down)
GET	/accesspoints.json/{ap-name}/radios	Get Radios by access point
GET	/accesspoints.json/{ap-name}/ssids	Get SSIDs by access point
GET	/accesspoints.json/{ap-name}/alarms	Get alarms by access point

Figure 315. API — Settings Requests List

GET requests are available for data shown in many of the monitor pages described in the section titled, **“About the Monitor Pages” on page 43**.

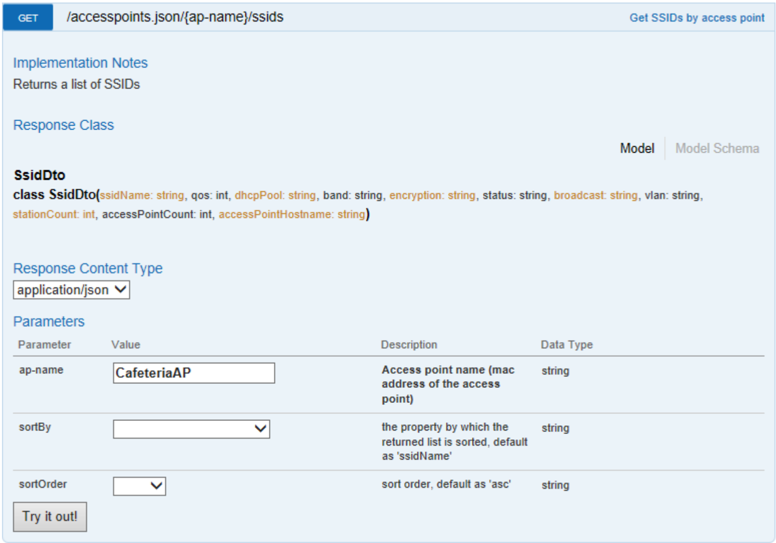
The **search** GET requests can be used to find a particular kind of object with an attribute that includes the search string. This search feature is quite similar to **“Searching” on page 65**. For example, if you use **GET /search.json/accesspoints/**

{search-query} to search for “100”, then the results would include Access Points whose IP Address or Hostname have “100” anywhere.

GET Requests

Each request name in the list is a link. To the right of the name is a brief summary of the command’s function. Click the link to see more information and to try the operation and see its output.

The figure below shows the request for **GET /accesspoints.json/{ap-name}/ssids**. Click again to collapse (hide) the API details.



/accesspoints.json/{ap-name}/ssids

Get SSIDs by access point

Implementation Notes

Returns a list of SSIDs

Response Class

SsidDto

class SsidDto(ssidName: string, qos: int, dhcpPool: string, band: string, encryption: string, status: string, broadcast: string, vlan: string, stationCount: int, accessPointCount: int, accessPointHostname: string**)**

Response Content Type

application/json

Parameters

Parameter	Value	Description	Data Type
ap-name	CafeteriaAP	Access point name (mac address of the access point)	string
sortBy		the property by which the returned list is sorted, default as 'ssidName'	string
sortOrder		sort order, default as 'asc'	string

Figure 316. API — GET Request Details

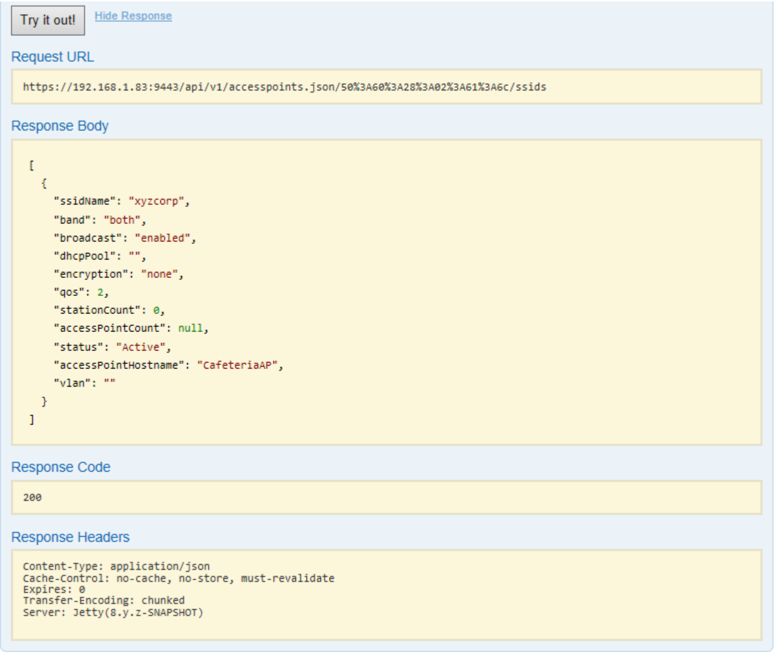
High-level details are shown, including:

- **Implementation Notes**: additional information about the function of this operation.
- **Response Class**: a list of the items returned and their types. Click Model Schema to show them as a JSON Schema (**http://json-schema.org/**).
- **Response Content Type** (limited to JSON at this time).

- **Parameters**: a list of the parameters for this operation. The **Description** field gives additional information about the expected value. Parameters that are not flagged as **(required)** are optional. Some parameters may constrain you to choosing values from a drop-down list. For example, **sortOrder** offers the options of **asc**ending or **desc**ending. In some cases, there may be two versions of a request, with and without parameters. For example, **GET /accesspoints.json/{ap-name}** returns data for a particular AP, while **GET /accesspoints.json/** returns data for all APs.

Trying a GET Request

The **Try it out!** button allows you to send the GET request to the WOS API and see its response. Developers can use this feature to design and implement applications that use this response.



Request URL

```
https://192.168.1.83:9443/api/v1/accesspoints.json/50%3A60%3A28%3A02%3A61%3A6c/ssids
```

Response Body

```
[
  {
    "ssidName": "xyzcorp",
    "band": "both",
    "broadcast": "enabled",
    "dhcpPool": "",
    "encryption": "none",
    "qos": 2,
    "stationCount": 0,
    "accessPointCount": null,
    "status": "Active",
    "accessPointHostname": "CafeteriaAP",
    "vlan": ""
  }
]
```

Response Code

```
200
```

Response Headers

```
Content-Type: application/json
Cache-Control: no-cache, no-store, must-revalidate
Expires: 0
Transfer-Encoding: chunked
Server: Jetty(8.y.z-SNAPSHOT)
```

Figure 317. API — GET Request Response

Enter the desired **Parameters** and click the **Try it out!** button. An example is shown in **Figure 317**.

The figure above shows the response for **GET /accesspoints.json/{ap-name}/ ssids**. The response is produced in the human-readable JSON format. The data shown are as described in **“The Access Points List” on page 66**. Click **Hide Response** if you wish to hide the output.

The **Request URL** field shows the exact form of the URL used to perform this operation. The **Response Code** and the **Response Header** are standard for HTTP(S).

The exact format of the returned data is displayed in the **Response Body** field. Use its scroll bar to view the entire response.

API Documentation Toolbar

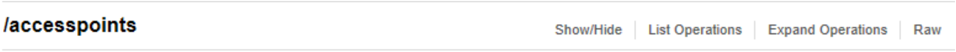


Figure 318. API Documentation Toolbar

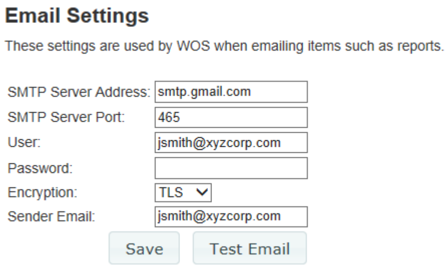
The Status and Settings sections each have a toolbar as shown above, offering the following options.

- **Show/Hide**—expands or collapses this list of GET requests. Hiding and then showing again displays the requests as they were before, i.e., expanded GET requests will still be expanded when displayed again.
- **List Operations**—expands this list of GET requests. Each individual entry is collapsed.
- **Expand Operations**—shows all of the GET requests in this list. Each individual entry is expanded.
- **Raw**—shows the source XML code for this list of GET requests. Click the link for the API Documentation page again to return to the normal display.

Applications

Email Settings

Some features, such as **Viewing a Report**, allow you to email information from WOS to yourself or others. When WOS needs to send email, it uses an SMTP server to do so. Before WOS can send any emails, you must specify which server to use and provide authentication information.



Email Settings

These settings are used by WOS when emailing items such as reports.

SMTP Server Address: smtp.gmail.com
SMTP Server Port: 465
User: jsmith@xyzcorp.com
Password:
Encryption: TLS
Sender Email: jsmith@xyzcorp.com

Figure 319. Changing the Email Server

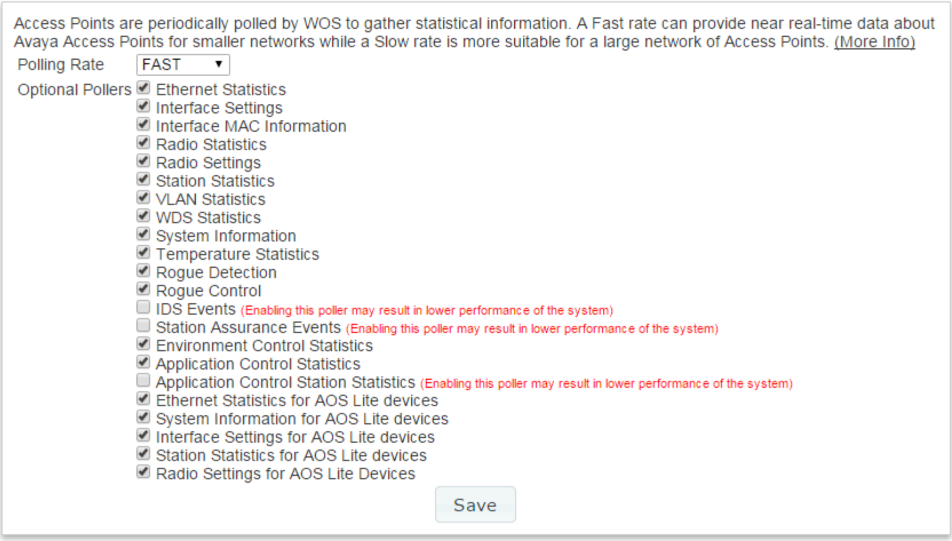
To specify the SMTP server for WOS to use, click **Settings** at the top of the page and then use the **Email** link. (**Figure 319**)

Enter your **SMTP Server Address** and **SMTP Server Port**. Specify the **User** and **Password** that WOS must use to access the server. Select an **Encryption** type.

When WOS sends an email, it will identify it as being sent from the email address that you specify in the **Sender Email** field. You may click the **Test Email** button to verify that you have specified the SMTP server correctly. Enter your email address in the dialog box that appears to check that WOS is able to use SMTP to successfully send an email.

Click **Save** when done.

Polling Settings



Access Points are periodically polled by WOS to gather statistical information. A Fast rate can provide near real-time data about Avaya Access Points for smaller networks while a Slow rate is more suitable for a large network of Access Points. (More Info)

Polling Rate: FAST ▾

Optional Pollers:

- ☑ Ethernet Statistics
- ☑ Interface Settings
- ☑ Interface MAC Information
- ☑ Radio Statistics
- ☑ Radio Settings
- ☑ Station Statistics
- ☑ VLAN Statistics
- ☑ WDS Statistics
- ☑ System Information
- ☑ Temperature Statistics
- ☑ Rogue Detection
- ☑ Rogue Control
- □ IDS Events (Enabling this poller may result in lower performance of the system)
- □ Station Assurance Events (Enabling this poller may result in lower performance of the system)
- ☑ Environment Control Statistics
- ☑ Application Control Statistics
- □ Application Control Station Statistics (Enabling this poller may result in lower performance of the system)
- ☑ Ethernet Statistics for AOS Lite devices
- ☑ System Information for AOS Lite devices
- ☑ Interface Settings for AOS Lite devices
- ☑ Station Statistics for AOS Lite devices
- ☑ Radio Settings for AOS Lite Devices

Figure 320. Changing Polling Rate

Click the **Polling** link to display the Polling page. This page changes the rate at which various types of network information are updated.

Most polling settings are enabled by default, but pollers such as **IDS Events**, **Station Assurance** Events, and Application Control Station Statistics are disabled by default since these place a load on the system and may result in lower performance. These must be explicitly enabled if you wish to use the corresponding data.

There are separate settings at the bottom of the list for data from APs that run AOSLite, such as the WAP9112. These are enabled by default. Note that these are the only poller settings available for AOSLite devices, and that the other poller settings do not affect AOSLite devices.

WOS offers a rich set of statistics in its **Dashboard**, **Reports**, and other windows. These statistics are obtained by polling the managed APs using SNMP. The default polling rate is **FAST**, providing near real-time data. If you have a large number of APs under management, we recommend that you decrease the polling speed to enhance WOS performance. Select **FAST**, **MEDIUM**, or **SLOW** from the drop-down list and click the **Save** button.

The following table summarizes the polling intervals used for the three polling rates.

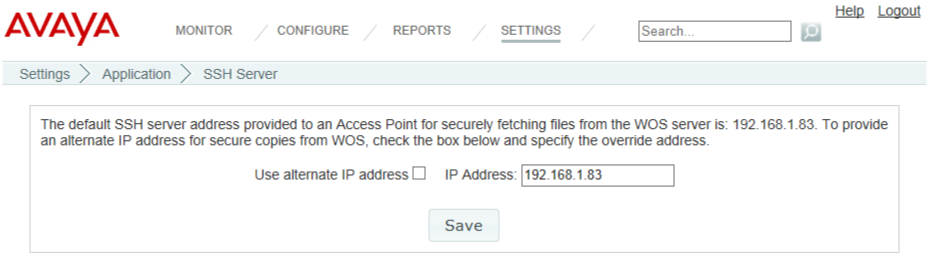
Item	Polling Interval FAST	Polling Interval MEDIUM	Polling Interval SLOW
AP Up/Down Status	1 minute	5 minutes	5 minutes
Statistics	40 seconds	80 seconds	120 seconds
Station Counts	40 seconds	80 seconds	120 seconds
Rogues	150 seconds	300 seconds	450 seconds

The following table summarizes the recommended polling intervals for various network sizes.

Polling Rate	Number of APs
Fast	up to 100
Medium	up to 250
Slow	over 250

After you change the polling rate, each AP will be reconfigured for the new polling interval. Depending on the number of APs under management, it might take some time to process the change on all APs (up to 10 seconds per AP). You may continue to use WOS while this change is proceeding.

WOS Call-back Address



The default SSH server address provided to an Access Point for securely fetching files from the WOS server is: 192.168.1.83. To provide an alternate IP address for secure copies from WOS, check the box below and specify the override address.

Use alternate IP address □ IP Address: 192.168.1.83

Figure 321. Changing the WOS Call-back Server

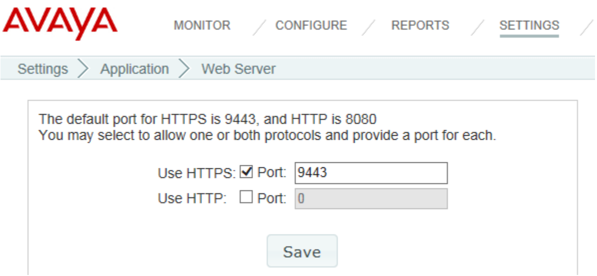
Some communication between APs and WOS, such as secured web-socket connections and **Perform or Schedule Upgrade** via SCP, use the WOS server's IP address by default. In some situations you may need to specify a different externally accessible IP address, for example if NAT is in use on the WOS server's network.

The current call back address is displayed. (**Figure 321**) To provide an alternate IP address for APs to access WOS, click the **Use alternate IP address** checkbox and enter the desired **IP Address**. Click **Save** when done.

Note that APs will use Port 22 for SSH to the WOS server.

Web Server

This page allows you to change default settings for HTTP and HTTPS access to the WOS server, including the ports used. This page is only available on some WAP models.



The default port for HTTPS is 9443, and HTTP is 8080
You may select to allow one or both protocols and provide a port for each.

Use HTTPS: ☑ Port: 9443
Use HTTP: □ Port: 0

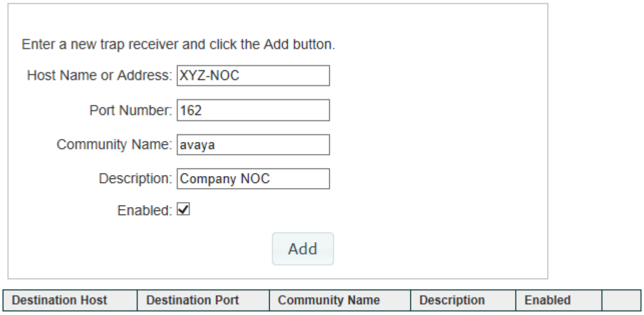
Figure 322. Web Server

By default, only HTTPS access is enabled, and it uses port 9443.

Note that the old URL for accessing WOS at *http://<wos-server>:9090* may still be used. It will automatically redirect you to HTTPS at the port configured above.

SNMP Trap Receivers

Just as APs send SNMP traps to the WOS server, the WOS server can send traps to top-level supervisory software. Any AP event that gets escalated to an alarm will be forwarded to the trap receivers that you set up. The receiver for these traps might be a Manager of Managers (MOM) or an application like HP OpenView running at the NOC. Use the **SNMP Trap Receivers** page to set up one or more destinations for these traps.



Enter a new trap receiver and click the Add button.

Host Name or Address: XYZ-NOC

Port Number: 162

Community Name: avaya

Description: Company NOC

Enabled: ☑

Destination Host	Destination Port	Community Name	Description	Enabled	

Figure 323. SNMP Trap Receivers

To open this page, click the **Settings** link at the top of the page. Then select **SNMP Trap Receivers** from the **Application** section (**Figure 323**). Enter the **Host Name or IP Address** of the destination that is to receive traps sent by the WOS server. If needed, change the **Port Number** from its default value of 162. Set the **Community Name** needed for access to this destination. Add a **Description** for this receiver if desired, and set **Enabled** to make this entry active. Click **Add** when done. The new entry will be displayed in the list of trap receivers.

If necessary, you may use the **Remove** button to the right of an entry to remove this trap receiver from the list.

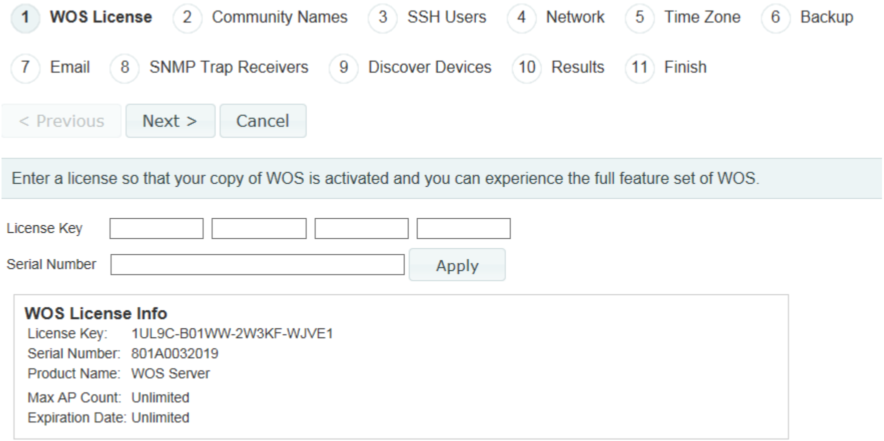
WOS Setup Wizard

The WOS Setup Wizard takes you through the basic starting steps for provisioning your server. All of these steps are available in their own web client pages, but the wizard guides you through the essential initial steps for licensing the server and then starting discovery of your wireless network.

If there are no APs in the WOS database (for example, the first time you start the web client), you will automatically be taken to the wizard. To open this page at other times, click the **Settings** link at the top of the page. Then select **WOS Setup Wizard** from the **Application** section.

Perform the wizard's steps as discussed in the following sections.

1. **WOS License** (Figure 324)



Enter a license so that your copy of WOS is activated and you can experience the full feature set of WOS.

WOS License Info

License Key: 1UL9C-B01WW-2W3KF-WJVE1
Serial Number: 801A0032019
Product Name: WOS Server
Max AP Count: Unlimited
Expiration Date: Unlimited

Figure 324. WOS Setup Wizard—WOS License

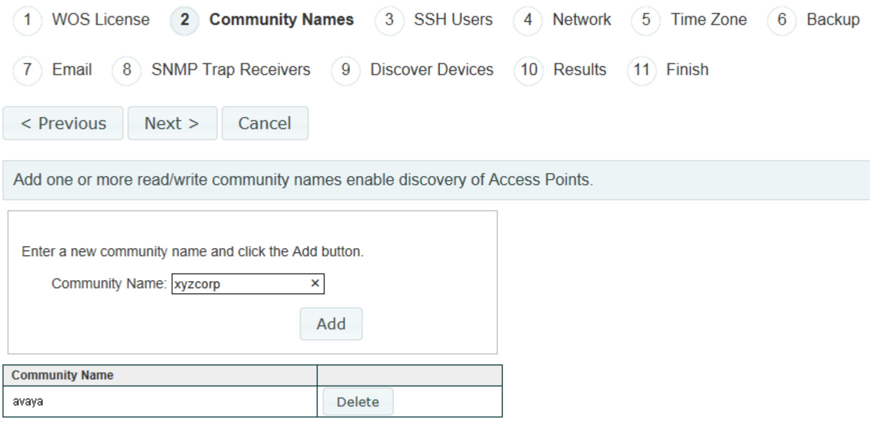
Avaya will supply you with a **License Key** and **Serial Number** for your server. Enter **both** of these fields exactly as they were provided to you (the fields are not case-sensitive), and click **Apply**.

After processing the license, the web client displays the following:

- **Product Name**—WOS server's product name.
- **Max Version**—the highest release number supported by this license. All incremental upgrades to the release shown are also supported. For example, if Max Version is 7.0, then this license will run Release 7.0.999, but Release 7.1 will require an updated license.
- **Max AP Count**—the server is licensed to manage a specific maximum number of APs. To manage additional APs, please contact Avaya to upgrade your license.
- **Expiration Date**—the date that this license expires.

Click **Next >** to proceed to the next step. For more information, please see **"Managing the WOS Server License" on page 610**.

2. **Community Names** (**Figure 325**)



Add one or more read/write community names enable discovery of Access Points.

Enter a new community name and click the Add button.

Community Name: xyzcorp

Community Name	
avaya	Delete

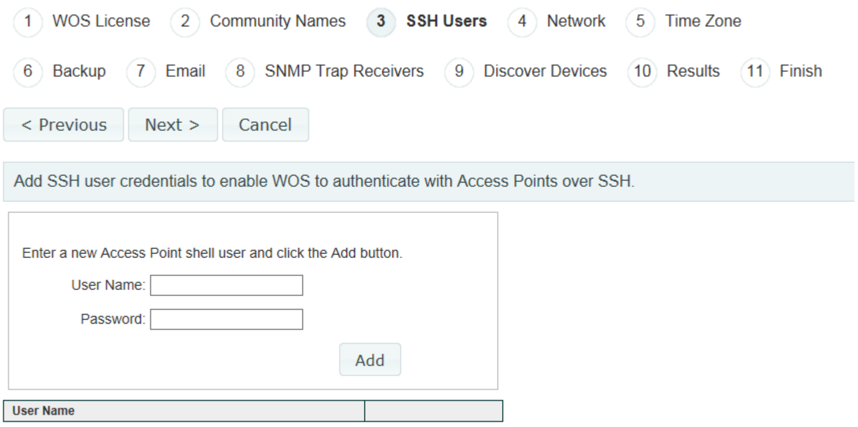
Figure 325. WOS Setup Wizard—Community Names

This page is used to add or delete SNMPv2 community names. The WOS discovery process searches networks using both SNMPv2 and SNMPv3. WOS discovery has default SNMPv2 entries which match the factory default SNMP v2 settings in APs. However, for proper security on your Avaya devices, we recommend that you change these defaults by setting your own SNMPv2 community strings on Avaya APs. Thus, you must add those community names or user names/passwords to WOS so that discovery can find those devices.

Enter the new **Community Name** and click **Add**.

Click **Next >** to proceed to the next step. For more information, please see **"SNMPv2 Settings" on page 168**.

3. **SSH Users** (**Figure 326**)



Add SSH user credentials to enable WOS to authenticate with Access Points over SSH.

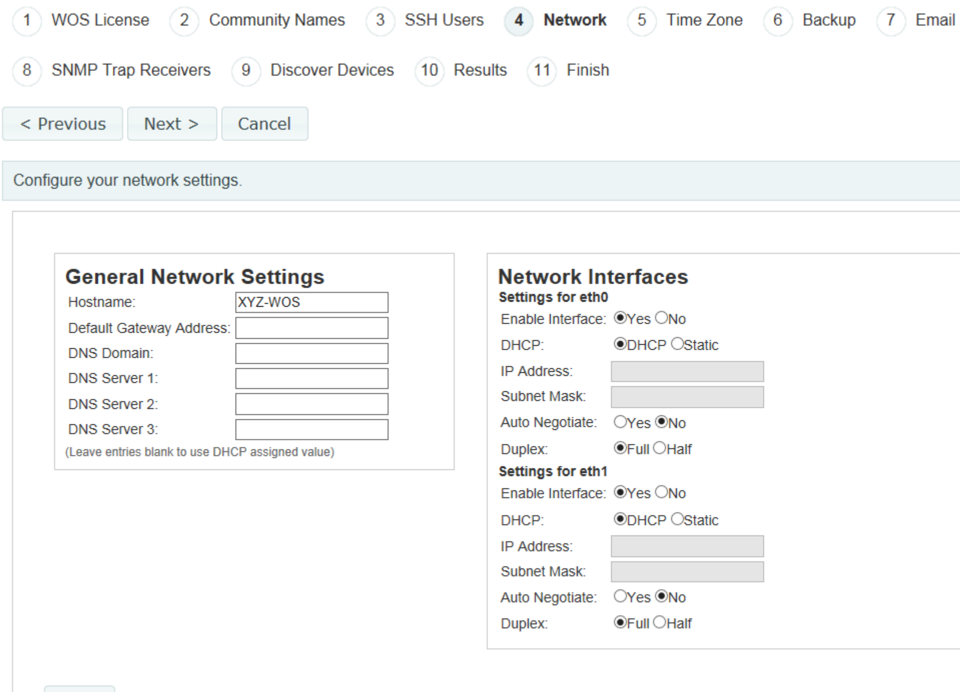
Enter a new Access Point shell user and click the Add button.

Figure 326. WOS Setup Wizard—SSH Users

Some actions, such as **Perform or Schedule Upgrade** and **Deploy Config Template**, require APs to download files. When it instructs an AP to fetch a file from the server, WOS needs to know a **User Name** and **Password** to gain access to the AP shell. Enter an AP's **User Name** and **Password**, and click **Add**. Repeat this for all of the accounts needed to gain access to all of your APs. When WOS needs access to an AP, it will try username/password pairs until it succeeds. It then records the values that worked, for the next time it needs to access that AP.

Click **Next >** to proceed to the next step. For more information, please see **"SSH Users" on page 172**.

4. **Network** (**Figure 327**)



Configure your network settings.

General Network Settings

Hostname: XYZ-WOS
Default Gateway Address:
DNS Domain:
DNS Server 1:
DNS Server 2:
DNS Server 3:
(Leave entries blank to use DHCP assigned value)

Network Interfaces

Settings for eth0

Enable Interface: ● Yes ○ No
DHCP: ● DHCP ○ Static
IP Address:
Subnet Mask:
Auto Negotiate: ○ Yes ● No
Duplex: ● Full ○ Half

Settings for eth1

Enable Interface: ● Yes ○ No
DHCP: ● DHCP ○ Static
IP Address:
Subnet Mask:
Auto Negotiate: ○ Yes ● No
Duplex: ● Full ○ Half

Figure 327. WOS Setup Wizard—Network

This step manages IP configuration for the server. For recommended IP addressing, please see **“Initial Network Settings” on page 554**.

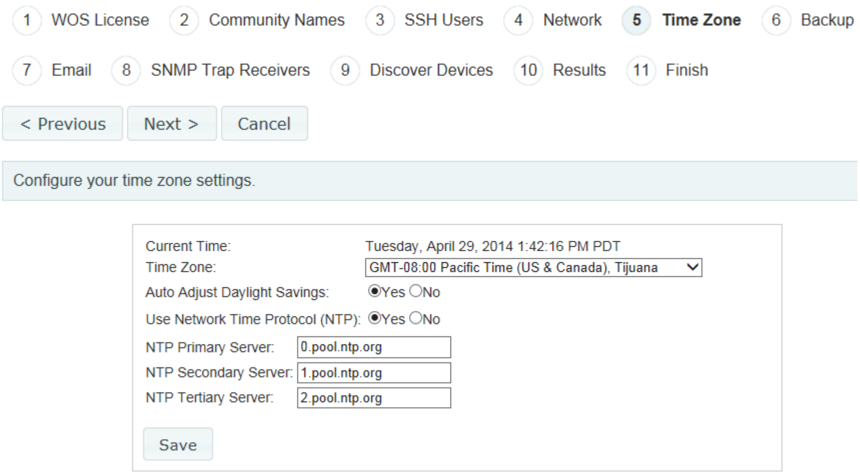
Hostname defaults to **Avaya-WOS**. Avaya APs send traps to **Avaya-WOS** to announce their presence and speed discovery. Thus, if you change the server’s Hostname, you should create an alias in your DNS server so that the server is accessible using both **Avaya-WOS** and the new host name.

Check that **Enable Interface** is set to **Yes** for each Ethernet port that you plan to use. **Auto Negotiate** should normally be left enabled.

The server uses DHCP by default. To set a static address, click **Static**. In this case, you must also enter the WOS server’s **Default Gateway Address**, and enter the **DNS Domain** and **DNS Servers**.

Click **Next >** to proceed to the next step.

5. **Time Zone** (**Figure 328**)



Configure your time zone settings.

Current Time:	Tuesday, April 29, 2014 1:42:16 PM PDT
Time Zone:	GMT-08:00 Pacific Time (US & Canada), Tijuana
Auto Adjust Daylight Savings:	● Yes ○ No
Use Network Time Protocol (NTP):	● Yes ○ No
NTP Primary Server:	0.pool.ntp.org
NTP Secondary Server:	1.pool.ntp.org
NTP Tertiary Server:	2.pool.ntp.org

Figure 328. WOS Setup Wizard—Time Zone

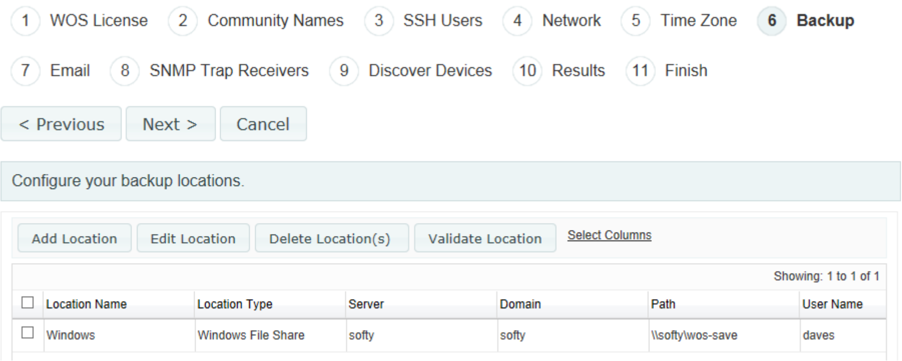
To use SNMPv3 successfully, system time must be set using the same NTP server on both the WOS server host machine and all APs using SNMPv3.

Select your local **Time Zone** from the drop-down list. Enable **Auto Adjust Daylight Savings** if you want the system to adjust for daylight savings automatically, otherwise click **No**.

Leave **Use Network Time Protocol** enabled. You may modify the **NTP Servers** or leave them at the default values which use NTP Pool time servers (http://www.pool.ntp.org/). All APs must use the same NTP server to be managed successfully.

Click **Next >** to proceed to the next step. For more information, please see **"Date and Time Settings" on page 559**.

6. **Backup** (**Figure 329**)



Configure your backup locations.

Showing: 1 to 1 of 1

□	Location Name	Location Type	Server	Domain	Path	User Name
□	Windows	Windows File Share	softy	softy	\\softy\wos-save	daves

Figure 329. WOS Setup Wizard—Backup

This page sets backup locations for the WOS database. For data protection, define and use at least one location for backups other than on the WOS server. When you are finished specifying the server type, path and account to use, WOS will verify that it is able to access the location and log in. See **"Manage Locations" on page 561** for more information.

Click **Add Location**. Enter the entry's **Name** and select a **Location Type**.

Windows File Share: specify the **Path** for the folder where files are to be stored. Use the Windows Uniform Naming Convention (UNC) format (\\*ComputerName**SharedFolder**Resource*) or the Server Message Block (SMB) format (*smb://URL*).

You may enter a **Domain** name if necessary. If the location is on a standalone server, you should normally leave the domain field blank. Enter a **User Name** and **Password/Confirm Password** that will give you write privileges.

FTP: specify the **FTP Server** used for backup, for example, *ftp.xyzcorp.com*. Specify the **FTP Directory** for the backup files. If you do not select **Anonymous FTP**, enter an **FTP Username** and **FTP Password/ Confirm FTP Password** that will give you write privileges.

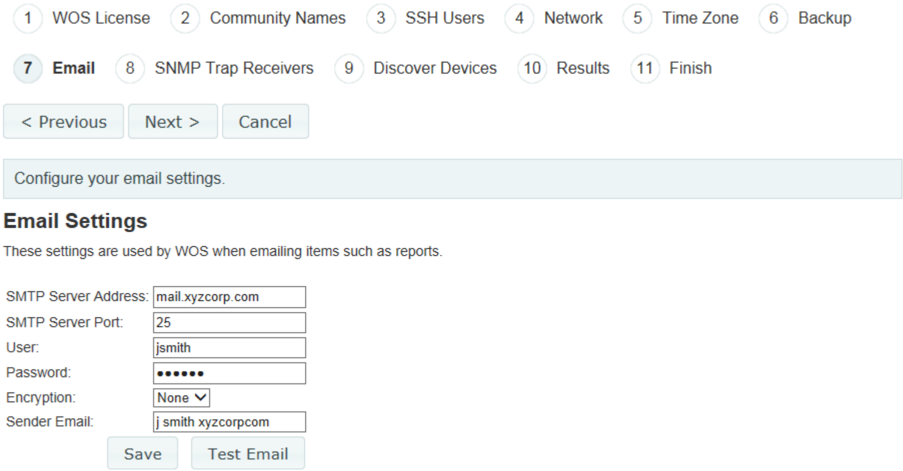
SCP (Secure Copy Protocol): specify the **SCP Server** used for backup, entering its hostname, DNS name, or IP address. Specify the **SCP**

Directory for the backup files. Enter an **SCP Username** and **SCP Password/Confirm SCP Password** that will give you write privileges.

Once you have specified backup locations and you are done with the wizard, see **"Manage Schedules or Backup Now" on page 565** to schedule automatic backups.

Click **Next >** to proceed to the next step.

7. **Email** (**Figure 330**)



Configure your email settings.

Email Settings

These settings are used by WOS when emailing items such as reports.

SMTP Server Address:	mail.xyzcorp.com
SMTP Server Port:	25
User:	jsmith
Password:	••••••
Encryption:	None
Sender Email:	j smith xyzcorpcom

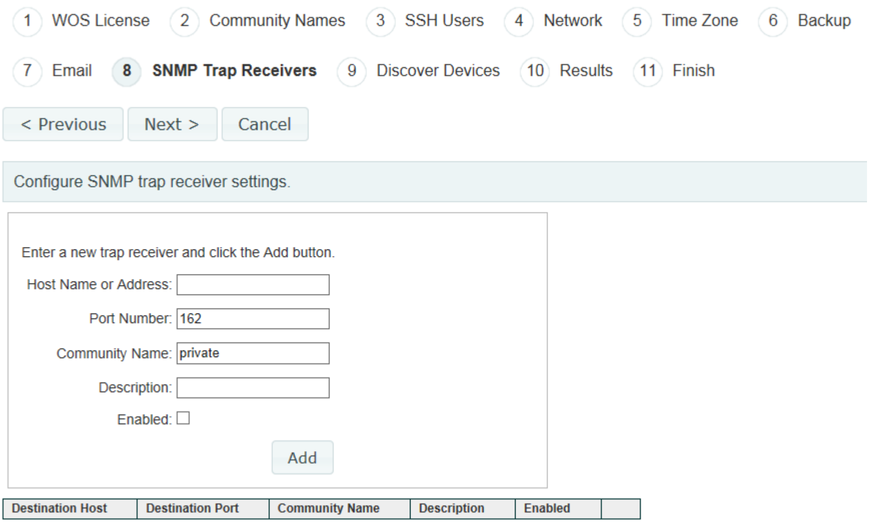
Figure 330. WOS Setup Wizard—Email

Some WOS features, such as reports and alarm notifications, send emails to specified recipients. WOS uses an SMTP server to send the emails. For more information, please see **"Email Settings" on page 588**.

Enter your **SMTP Server Address** and **Port**. Specify the **User** and **Password** for access to the server. Select an **Encryption** type. Emails will be identified as being sent from the address that you specify in **Sender Email**. Click **Test Email** to verify that you can successfully send an email.

Click **Next >** to proceed to the next step.

8. **SNMP Trap Receivers** (Figure 331)



Configure SNMP trap receiver settings.

Enter a new trap receiver and click the Add button.

Host Name or Address:

Port Number: 162

Community Name: private

Description:

Enabled: □

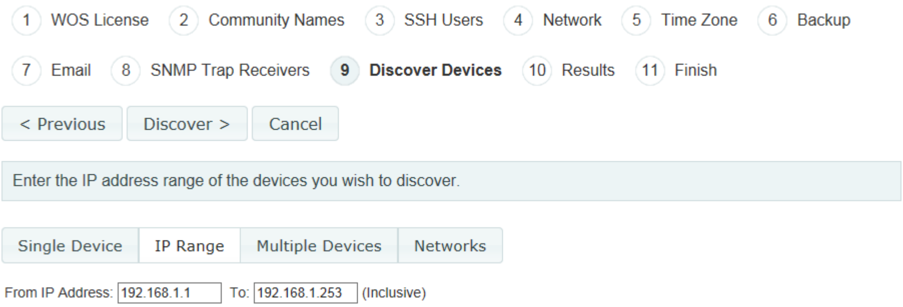
Destination Host	Destination Port	Community Name	Description	Enabled	

Figure 331. WOS Setup Wizard—SNMP Trap Receivers

The WOS server can send traps to top-level supervisory software. AP alarms will be forwarded to these trap receivers. Enter the **Host Name or IP Address** of the destination that is to receive traps sent by the WOS server. Set the **Community Name** needed for access to this destination. Add a **Description** for this receiver if desired, and set **Enabled**. Click **Add** when done with each entry.

Click **Next >** to proceed to the next step. For more information, please see **"SNMP Trap Receivers" on page 593**.

9. **Discover Devices** (Figure 332)



Enter the IP address range of the devices you wish to discover.

From IP Address: 192.168.1.1 To: 192.168.1.253 (Inclusive)

Figure 332. WOS Setup Wizard—Discover Devices

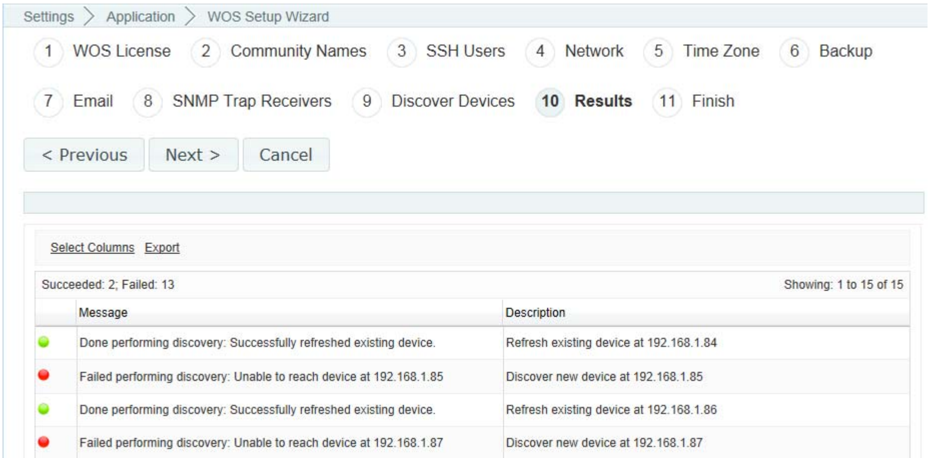
This step is used to add subnetworks or devices to WOS. You may individually add one or more APs, or specify a network and have WOS discover them. You may enter a single device IP address, a range of addresses, a list of addresses (the **Multiple Devices** option), or a subnetwork. The list option is useful if you have an Excel spreadsheet with a list of APs and their addresses.

Select whether to add a **Single Device**, an **IP Range**, **Multiple Devices,** or **Networks** by clicking the appropriate tab, then enter the requested IP information. If you enter a network, be careful to specify the smallest subnet that includes the APs, to avoid creating excess traffic by discovering a needlessly large network.

For more information, please see **"Discovery" on page 159** and **"Add Devices" on page 163**.

Click the **Discover** button to start discovery.

10. **Results** (**Figure 333**)



Succeeded: 2; Failed: 13 Showing: 1 to 15 of 15

	Message	Description
●	Done performing discovery: Successfully refreshed existing device.	Refresh existing device at 192.168.1.84
●	Failed performing discovery: Unable to reach device at 192.168.1.85	Discover new device at 192.168.1.85
●	Done performing discovery: Successfully refreshed existing device.	Refresh existing device at 192.168.1.86
●	Failed performing discovery: Unable to reach device at 192.168.1.87	Discover new device at 192.168.1.87

Figure 333. WOS Setup Wizard—Results

The Results step will display the discovery results for each requested address or network, listing whether discovery is **In Progress**, **Completed**, **Disabled**, or **Failed**.

You may use the **Cancel** button if you wish to abort discovery while still in progress. This will stop WOS from finding any additional devices, but will not remove any devices that have just been discovered.

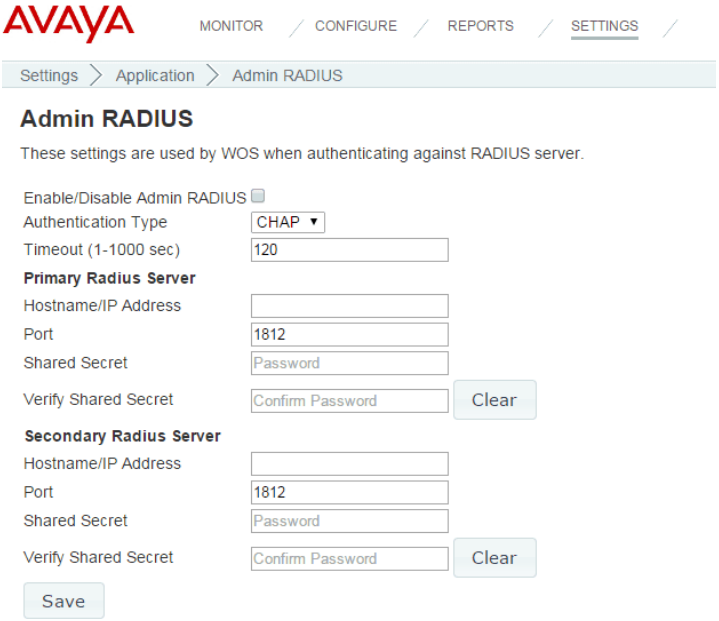
Admin RADIUS

This window allows you to specify a RADIUS server to be used for authentication of WOS users/administrators. This enables WOS access via the same RADIUS credentials that are used for authentication across your organization's other software resources. This is different from the **Admin RADIUS** setting in AP **Security**, which is an AP setting that controls accounts for logging in to APs directly.

Admin RADIUS servers defined in these settings take priority over local WOS administrator accounts configured on the **WOS Users** window. If you have Admin RADIUS enabled, and if the Primary RADIUS Server is configured, it is tried first. If it is down or if it denies authentication, the secondary RADIUS server is tried. If that also does not result in success, then the local accounts configured in **WOS Users** are tried.

About Creating Admin Accounts on the RADIUS Server

Permissions for WOS administrator accounts in RADIUS are controlled by the RADIUS Vendor Specific Attribute (VSA) named **Avaya-Admin-Role**. In the RADIUS server, set a user account's Avaya-Admin-Role to **read-only** for User (read-only) privileges. Set it to **read-write** for Super-Admin (read-write) privileges. For more information about the RADIUS VSAs used by Avaya, see "RADIUS Vendor Specific Attribute (VSA) for Avaya" in the Technical Support Appendix of *Using the Avaya OS for Avaya WLAN AP 9100 Series (NN47252-102)*.



Admin RADIUS

These settings are used by WOS when authenticating against RADIUS server.

Enable/Disable Admin RADIUS	□
Authentication Type	CHAP ▾
Timeout (1-1000 sec)	120
Primary Radius Server	
Hostname/IP Address	
Port	1812
Shared Secret	Password
Verify Shared Secret	Confirm Password
Secondary Radius Server	
Hostname/IP Address	
Port	1812
Shared Secret	Password
Verify Shared Secret	Confirm Password

Figure 334. Admin RADIUS

Procedure for Configuring Admin RADIUS

Use this window to enable/disable WOS login authentication via RADIUS, and to set up primary and secondary servers for authentication.

1. **Admin RADIUS Settings:**

    a. **Enable/Disable Admin RADIUS**: Click the checkbox to enable the use of RADIUS to authenticate users logging in to WOS. You will need to specify the RADIUS server(s) to be used.

    b. **Authentication Type**: Select the protocol used for authentication of administrators: **PAP** (the default) or **CHAP**.

    - **Password Authentication Protocol (PAP)**, is a simple protocol. PAP transmits ASCII passwords over the network "in the clear" (unencrypted) and is therefore considered insecure.
    - **Challenge-Handshake Authentication Protocol (CHAP)** is a more secure protocol. The login request is sent using a one-way hash function.

    c. **Timeout (seconds)**: Define the maximum time (in seconds) that WOS will wait for the RADIUS server to respond to the authentication request. If the request times out, WOS will try the next authentication method (the secondary server, and then the locally defined user accounts). The default is 120 seconds.

2. **Admin RADIUS Primary Server**: This is the RADIUS server that you intend to use as your primary server.

    a. **Host Name / IP Address**: Enter the IP address or domain name of this external RADIUS server.

    b. **Port Number**: Enter the port number of this RADIUS server. The default is 1812.

    c. **Shared Secret / Verify Secret**: Enter the shared secret that this RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.

The shared secret that you define must match the secret used by the RADIUS server.

3. **Admin RADIUS Secondary Server** (optional): If desired, enter an alternative external RADIUS server. If the primary RADIUS server becomes unreachable, the AP will "failover" to the secondary RADIUS server (defined here).

   a. **Host Name / IP Address**: Enter the IP address or domain name of this RADIUS server.

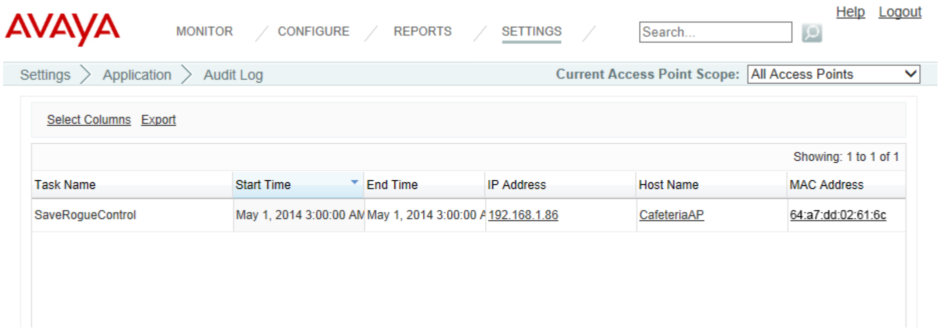
   b. **Port Number**: Enter the port number of this RADIUS server. The default is 1812.

   c. **Shared Secret / Verify Secret**: Enter the shared secret that this RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.

4. Click **Save** when done.

Audit Log

This page shows an audit trail (record) of all configuration changes that have been performed on your APs. Use the **Audit Log** link under **Settings** (in the **Application** section) to display the Audit Log page. This page displays the **Task Name** of each configuration change, its **Start** and **End Time**, the **IP** and **MAC Address** and **Host Name** of the AP, and the **Status** of the task. (Figure 335)



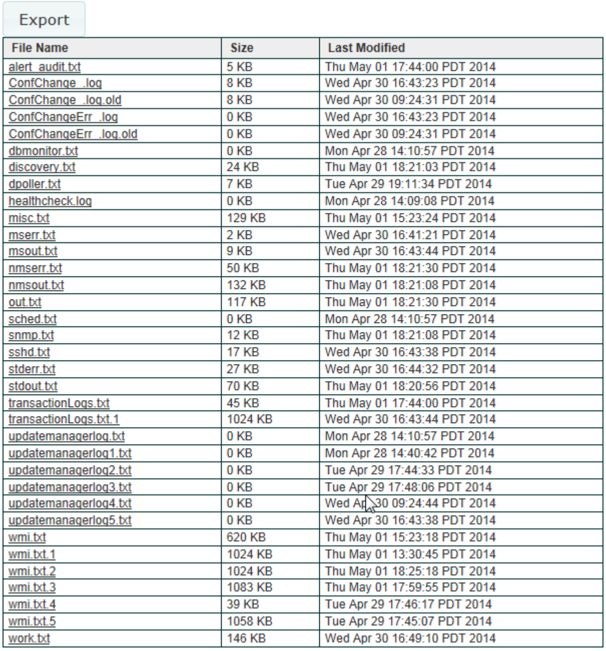
Current Access Point Scope: All Access Points

Showing: 1 to 1 of 1

Task Name	Start Time	End Time	IP Address	Host Name	MAC Address
SaveRogueControl	May 1, 2014 3:00:00 AM	May 1, 2014 3:00:00 A	192.168.1.86	CafeteriaAP	64:a7:dd:02:61:6c

Figure 335. Audit Log

Viewing Server Log Files

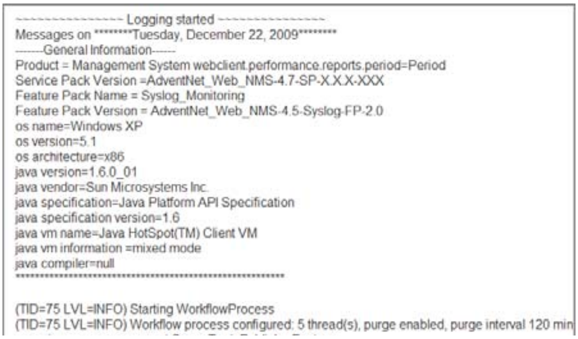


File Name	Size	Last Modified
alert_audit.txt	5 KB	Thu May 01 17:44:00 PDT 2014
ConfChange_.log	8 KB	Wed Apr 30 16:43:23 PDT 2014
ConfChange_.log.old	8 KB	Wed Apr 30 09:24:31 PDT 2014
ConfChangeErr_.log	0 KB	Wed Apr 30 16:43:23 PDT 2014
ConfChangeErr_.log.old	0 KB	Wed Apr 30 09:24:31 PDT 2014
dbmonitor.txt	0 KB	Mon Apr 28 14:10:57 PDT 2014
discovery.txt	24 KB	Thu May 01 18:21:03 PDT 2014
dpoller.txt	7 KB	Tue Apr 29 19:11:34 PDT 2014
healthcheck.log	0 KB	Mon Apr 28 14:09:08 PDT 2014
misc.txt	129 KB	Thu May 01 15:23:24 PDT 2014
mserr.txt	2 KB	Wed Apr 30 16:41:21 PDT 2014
msout.txt	9 KB	Wed Apr 30 16:43:44 PDT 2014
nmserr.txt	50 KB	Thu May 01 18:21:30 PDT 2014
nmsout.txt	132 KB	Thu May 01 18:21:08 PDT 2014
out.txt	117 KB	Thu May 01 18:21:30 PDT 2014
sched.txt	0 KB	Mon Apr 28 14:10:57 PDT 2014
snmp.txt	12 KB	Thu May 01 18:21:08 PDT 2014
sshd.txt	17 KB	Wed Apr 30 16:43:38 PDT 2014
stderr.txt	27 KB	Wed Apr 30 16:44:32 PDT 2014
stdout.txt	70 KB	Thu May 01 18:20:56 PDT 2014
transactionLogs.txt	45 KB	Thu May 01 17:44:00 PDT 2014
transactionLogs.txt.1	1024 KB	Wed Apr 30 16:43:44 PDT 2014
updatemanagerlog.txt	0 KB	Mon Apr 28 14:10:57 PDT 2014
updatemanagerlog1.txt	0 KB	Mon Apr 28 14:40:42 PDT 2014
updatemanagerlog2.txt	0 KB	Tue Apr 29 17:44:33 PDT 2014
updatemanagerlog3.txt	0 KB	Tue Apr 29 17:48:06 PDT 2014
updatemanagerlog4.txt	0 KB	Wed Apr 30 09:24:44 PDT 2014
updatemanagerlog5.txt	0 KB	Wed Apr 30 16:43:38 PDT 2014
wmi.txt	620 KB	Thu May 01 15:23:18 PDT 2014
wmi.txt.1	1024 KB	Thu May 01 13:30:45 PDT 2014
wmi.txt.2	1024 KB	Thu May 01 18:25:18 PDT 2014
wmi.txt.3	1083 KB	Thu May 01 17:59:55 PDT 2014
wmi.txt.4	39 KB	Tue Apr 29 17:46:17 PDT 2014
wmi.txt.5	1058 KB	Tue Apr 29 17:45:07 PDT 2014
work.txt	146 KB	Wed Apr 30 16:49:10 PDT 2014

Figure 336. Viewing Log Files

Use the **Server Logs** link under **Settings** (in the **General** section) to display the Logs page. This page displays a link for each of the working log (message) files generated by the WOS server while it is running. Click a link to view the contents of that file (**Figure 337**). These files journal the operation of the WOS server software, rather than reporting on the operation of the wireless network.

Log files are intended for use by Avaya Customer Support personnel. In certain situations, Support personnel may ask you to send them some of these files. Use the **Export** button to save log files to your file system. If you click this button on the Logs page (the page showing the list of log files), then WOS creates a zip file containing all of the logs. If you click **Export** on a page for a particular log file, then WOS creates a .csv file for that log. In either case, a dialog allows you to open or save the file and browse to the desired location for saving the export file. If you choose to open a .csv file rather than saving it and you have Excel installed on your workstation, an Excel window opens and displays the log file contents.

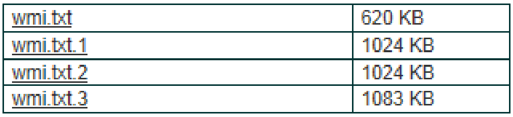


```
---------------- Logging started ----------------
Messages on ********Tuesday, December 22, 2009********
-------General Information------
Product = Management System webclient.performance.reports.period=Period
Service Pack Version =AdventNet_Web_NMS-4.7-SP-X.X.X-XXX
Feature Pack Name = Syslog_Monitoring
Feature Pack Version = AdventNet_Web_NMS-4.5-Syslog-FP-2.0
os name=Windows XP
os version=5.1
os architecture=x86
java version=1.6.0_01
java vendor=Sun Microsystems Inc.
java specification=Java Platform API Specification
java specification version=1.6
java vm name=Java HotSpot(TM) Client VM
java vm information =mixed mode
java compiler=null
*****************************************************

(TID=75 LVL=INFO) Starting WorkflowProcess
(TID=75 LVL=INFO) Workflow process configured: 5 thread(s), purge enabled, purge interval 120 min
```

Figure 337. Viewing a Selected Log File

If a listed log files grows too large, it is closed and renamed and a new file is started. The following example illustrates this. As shown in **Figure 338**, there are four **wmi.txt** files.

- **wmi.txt** contains the most recent entries.
- **wmi.txt.1**—the first time that wmi.txt grows too large, it is closed and renamed to wmi.txt.1. A new wmi.txt is created to capture ongoing new entries.
- **wmi.txt.2**—the second time that wmi.txt grows too large, it is closed and renamed to wmi.txt.2. Thus wmi.txt.1 contains the oldest entries, and wmi.txt.2 has the next oldest entries, etc. The number of log files is limited to 10 or 20 instances, depending on the log file type.



wmi.txt	620 KB
wmi.txt.1	1024 KB
wmi.txt.2	1024 KB
wmi.txt.3	1083 KB

Figure 338. Multiple Log Files

Managing the WOS Server License

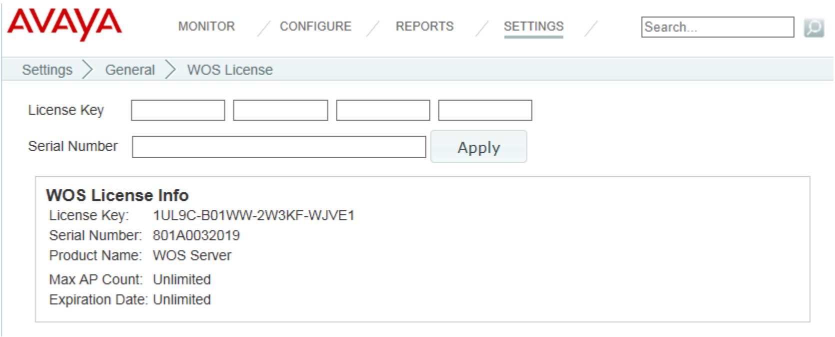
This section describes the license to use the WOS server. If you are looking for information regarding using WOS to manage AP licenses, please see **“Access Point Licenses” on page 182**.

For full operation, the WOS server must have a license installed. Until the license is installed, the server will operate in a default mode that allows it to manage only one AP. Thus, without an appropriate license, **Discovery** will stop at one AP and will not allow more APs to be added. If you do not have a valid license, you will be notified each time you start a WOS client.

Valid WOS licenses are typically for a particular number of radios. A two-radio AP (for example, the WAP9123/9133) consumes one license. A four-radio AP (for example, the WAP9172/9173) consumes two licenses. When WOS has discovered the maximum permitted number of radios, no additional APs will be discovered.

Use the following steps to enter your license.

1. Click the **Settings** button, then click **WOS License**. The WOS License Info page appears.



WOS License Info
License Key: 1UL9C-B01WW-2W3KF-WJVE1
Serial Number: 801A0032019
Product Name: WOS Server
Max AP Count: Unlimited
Expiration Date: Unlimited

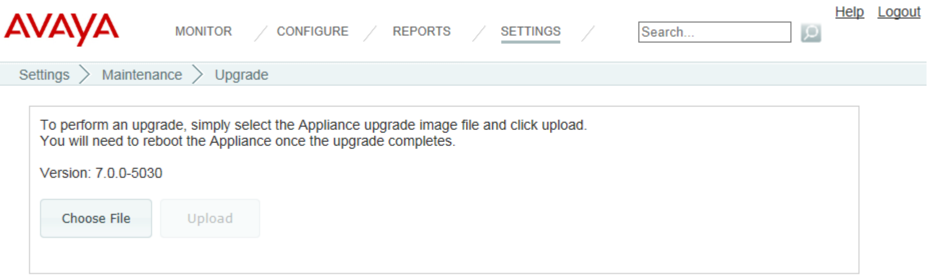
Figure 339. WOS Server License

2. Avaya will supply you with a **License Key** and **Serial Number** for your server. Enter **both** of these fields exactly as they were provided to you (the fields are not case-sensitive), and click **Apply**.

3. After processing the license information, the following additional fields will be shown:

   - **Product Name**—WOS server's product name.
   - **Max Version**—the highest release number supported by this license. All incremental upgrades to the release shown are also supported. For example, if Max Version is 7.0, then this license will run Release 7.0.999, but Release 7.1 will require an updated license.
   - **Max AP Count**—the server is licensed to manage a specific maximum number of APs. To manage additional APs, please contact Avaya to upgrade your license.
   - **Expiration Date**—the date that this license expires.

Performing Server Upgrades



To perform an upgrade, simply select the Appliance upgrade image file and click upload.
You will need to reboot the Appliance once the upgrade completes.

Version: 7.0.0-5030

Figure 340. Upgrading WOS Software

This page is used to update the Virtual Appliance. Select the **Upgrade** link to display the Upgrade page.

- .For the Virtual Appliance (VMware or Hyper-V)—a .vau file. For example:

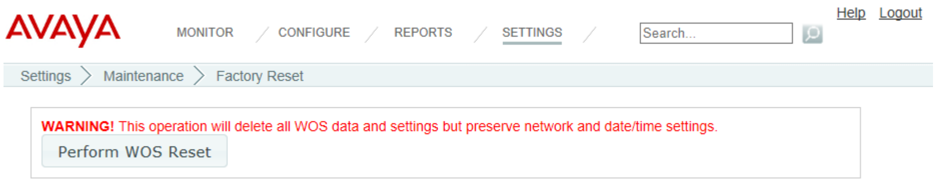
  WOS-7.0.0-4691.vau

The upgrade file contains an entire software upgrade, rather than having an incremental patch that depends on previous patches being installed. Please follow the instructions furnished with the release carefully.

1. When you receive a new release file from Avaya, place it where you will be able to browse to it from the web browser where you are running the web client.
2. Click **Settings** at the top of the page, then select the **Upgrade** link from the **Maintenance** section.
3. Next, click the **Choose File** button to browse to the .tar or .vau file. Click **Upload** to move the file to the server.
4. Click **Upgrade** to install the new software.

When the process is complete, a pop-up message will be displayed. It will inform you that you must reboot the Appliance. Click the **OK** button to close it. The new release becomes the current version of the WOS server.

Resetting the WOS Server



WARNING! This operation will delete all WOS data and settings but preserve network and date/time settings.

Figure 341. Resetting WOS

Use the **Factory Reset** link to display the Reset page. This page allows you to perform a reset on the server. This deletes all data in the WOS database (but it does not delete backup files). It also returns the WOS server back to all of its factory default settings, except that **Network Settings** and **Date and Time Settings** are retained.

Click the **Perform WOS Reset** button to perform the reset. You will be asked to verify that you wish to proceed.

When the reset is complete, your first action should be to specify **Database Backup Settings**.

Managing WOS Server Settings via the Web Client

The WOS web client allows you to change many WOS server settings on all platforms. Access it in the same way as described in **"Accessing the Web Client" on page 552**.

It has the following links:

- **WOS Users**—see **"WOS Users" on page 570**.
- **Email**—see **"Email Settings" on page 588**.
- **Polling**—see **"Polling Settings" on page 589**.
- **SSH Server**—see **"WOS Call-back Address" on page 591**.
- **SNMP Trap Receivers**—see **"SNMP Trap Receivers" on page 593**.
- **Backup**—see **"Database Backup Settings" on page 560**.
- **Server Logs**—see **"Viewing Server Log Files" on page 608**.
- **WOS License**—see **"Managing the WOS Server License" on page 610**.

Technical Support

This chapter provides valuable support information that can help you resolve technical difficulties. Before contacting Avaya, review all sections in this chapter and try to determine if your problem resides with WOS, the server platform, or your network infrastructure. Section headings for this chapter include:

- **"Frequently Asked Questions" on page 615**
- **"WOS Default Alarms and Events" on page 617**
- **"Location Service Data Formats" on page 619**
- **"Contact Information" on page 622**

Frequently Asked Questions

This section answers some of the most frequently asked questions regarding the functions and operation of WOS.

Q. **Why won't my browser connect to the WOS server to start the WOS client? I can ping the server.**

A. Remember to point the browser to Port 9090 on the server by appending **:9090** to the server address. For example:

http://192.168.10.40:9090

You will automatically be redirected to an HTTPS connection at port 9443, for example, **https://192.168.10.40:9443**.

Also note that if you selected a different port for accessing the WOS server during installation of the WOS server software, then you must append that port number to the URL instead of 9090. You may also use the web client to change the ports used for connections to WOS. See **"Web Server" on page 592**.

Q. **Why will WOS not discover an AP, even though the AP is connected to the network and functioning correctly?**

A. SNMPv2 or v3 (Simple Network Management Protocol) must be enabled on the AP. Log in to the AP and check the SNMP settings. If the problem persists, check that the AP is on the same subnet as the WOS server.

For discovery of a device (AP), the device must have SNMP enabled and its community string must match one of the strings listed in the Discovery window. See **"SNMPv2 Settings" on page 168**. The default SNMPv2 community string in WOS matches the AP default value.

When an AP boots up, it sends an SNMP trap to the WOS server's default hostname, **Avaya-WOS**. WOS can then add it to its discovered devices list. This Phone Home feature requires DNS to resolve the hostname **Avaya-WOS** correctly. Thus, if you change the host name of the WOS server, you must configure DNS to resolve **Avaya-WOS** to the actual name of the WOS server host.

Q. **WOS discovered my AP using SNMPv3, and the AP has connectivity and is running OK, but WOS reports that the AP is down.**

A. To use SNMPv3 successfully, system time must be set using an NTP server on both the WOS server host machine and on all APs using SNMPv3. This is because SNMPv3 requires synchronization between the WOS server and the APs so that the system time difference between them never exceeds more than 150 seconds. If the time difference exceeds 150 seconds, SNMPv3 suspects a security breach and removes the SNMPv3 credentials for affected APs from the database. This means that the AP will appear to be down and statistics will not be polled until the AP is re-discovered. A manual refresh of the AP will remedy the situation. See **"Add Devices" on page 163**.

Q. **When managing large AP deployments, will the performance of the network be compromised?**

A. No. WOS resides outside the data path, so performance bottlenecks and points of failure are eliminated.

Q. **Why didn't the maps I created appear the next time I logged in?**

A. You must always save your maps. Also, if you make changes and you want your changes to appear on all clients (not just your local machine) you must save the changes to the server.

WOS Default Alarms and Events

WOS alarms are generated in three ways:

- Custom alarms that you define. See **"Alarm Definitions" on page 154**.
- **Default Alarms and Events**—situations that WOS detects while monitoring the network. See the table below.
- Traps received from devices (APs). See the table in **Alarms from AP Traps or Other Device Traps**.

Default Alarms and Events

Type	Description	Severity
Alarm	Avaya AP up/down	**Critical**
Alarm	Third party AP up/down	**Critical**
Alarm	Switch up/down	**Critical**
Alarm	PoE up/down	**Critical**
Alarm	Duplicate AP IP address found (for APs)	**Major**
Alarm	Duplicate device IP address found (in case of switch or other devices)	**Major**
Alarm	Max radio count reached	**Major**
Alarm	Rogue control update failed for AP	**Minor (yellow)**
Event	New node discovered	**Info**
Event	Rogue classification update initiated on AP	**Info**
Event	Rogue update started	**Info**

Type	Description	Severity
Event	Rogue control update complete	**Info**

Alarms from AP Traps or Other Device Traps

For a full list of traps generated by the AP, please see the "FAQ and Special Topics" Appendix in *Using the Avaya OS for Avaya WLAN AP 9100 Series (NN47252-102)*.

Trap	Description
resetArray	AP was reset by admin
rebootArray	AP was rebooted by admin
softwareUploadFailure	Image upload failed
softwareUploadSuccess	Image upload succeeded
softwareUpgradeFailure	Image upgrade failed
softwareUpgradeSuccess	Image upgrade succeeded
dhcpRenewFailure	Unable to get IP address for AP from DHCP
cfgChange	An AP's configuration was changed
keepAlive	An AP stopped replying to WOS keep-alive messages
encDoorOpened	For an AP in an indoor enclosure with a properly connected tamper-evident switch, the enclosure has been opened
encDoorClosed	For an AP in an indoor enclosure with a properly connected tamper-evident switch, the enclosure has been closed
flashPartitionCorrupt	An AP's flash is corrupt
licenseUpdate	An AP's license was changed

Trap	Description
radioMixInvalid	In this software release, Wave 2 radio cards cannot be mixed with other radio types

Location Service Data Formats

Avaya APs are able to capture and upload visitor analytics data, acting as a sensor network in addition to providing wireless connectivity. This data is sent to the location server in different formats, based on the type of server. The **Location Server URL**, **Location Customer Key**, and **Location Period** for reporting data are configured under Location settings. See **"Location" on page 411** for details. If a **Location Customer Key** has been entered, data is sent encrypted using AES with that key.

Euclid Location Server

If the **Location Server URL** contains the string **euclid**, then it specifies a Euclid server. Data is sent at the specified intervals, in the proprietary format expected by the Euclid location server.

Non-Euclid Location Server

If the **Location Server URL** doesn't contain the string "euclid", then data is sent as a JSON object at the specified intervals, with the fields described in the table below.

Location service data formats are described in the table below. The **Use** field indicates whether a data item is included for a particular location server type:

- **E** indicates that this data is *only* sent for a Euclid location server.
- **N** indicates that this data is *only* sent for a non-Euclid location server.

See the footnotes at the end of the table for more information.

Field	Name	Use	Description
vs		E	Euclid header fixed value (3)
pf		E	Euclid header fixed value (11)
sn	MAC Address	E	Euclid header - AP MAC Address
sq	Message Count	E	Euclid header - Message Count
lh	Host Name	N	Header - AP host name
ln	Location Name	N	Header - AP location string
ld	Location Data	N	Defined below
vn	Version No.	N	Set to 1
ti	Time	N	Time of message
ma	MAC Address	N	Base Radio MAC Address
mc	Message Count	N	Running message count (resets to 0 when AP is rebooted)
lt	Location Table		Table of Stations and APs heard during this window
si	Station ID		Station MAC address (AES encrypted if cust-key is not blank)
bi	BSSID		BSSID that the station is on (AES encrypted if cust-key is not blank). Only stations that are associated to this AP will have a bi (BSSID) field, i.e., for unassociated stations the bi (BSSID) field will not be included.
sm	Station OUI		OUI of Station manufacturer (the top 3 bytes of the MAC address that can be used to look up the manufacturer), unencrypted
ap	AP Flag		1=AP, 0=Station
as	Assoc		1= Station is associated to AP
dm	Device Mfg	N	Station manufacturer

Field	Name	Use	Description
dt	Device Type	N	Type of device, such as iPhone or Android
dc	Device Class	N	Category of device, such as phone or notebook
px	Coordinate x	N	These location coordinates are sent to the AP byWOS. They appear only if the AP has been placed on an map in WOS. *
py	Coordinate y	N	
pz	Coordinate z	N	
pn	Number	N	Number of APs involved in the location calculation
po	Old	N	0 = New Multi-AP calculation used 1 = Old single AP multi-radio calculation
pt	Time	N	Time stamp for latest data used in location calculation
cn	Count		Count of frames heard from device during this window
ot	Origin Time		Timestamp of first frame in this window (Unix time in seconds)
ct	Current Time		Timestamp of last frame in this window (Unix time in seconds)
cf	Current Frequency		Frequency (MHz) last frame was heard on
is	Sum	E	Sum of values for receive interval
i2	Sum of Squares	E	Sum of squares of values for receive interval
i3	Sum of Cubes	E	Sum of cubes of values for receive interval
il	Interval Low		Minimum interval between frames (within 24 hr period)
ih	Interval High		Maximum interval between frames (within 24 hr period)
ss	Sum	E	Sum of values for signal strength
s2	Sum of Squares	E	Sum of squares of values for signal strength

Field	Name	Use	Description
s3	Sum of Cubes	E	Sum of cubes of values for signal strength
sl	Signal Low		Minimum signal strength (within 24 hr period)
sh	Signal High		Maximum signal strength (within 24 hr period)
so	Signal Origin		Signal strength of first frame heard
sc	Signal Current		Signal strength of last frame heard
pr	Probe Request		If per-radio data is enabled, for each radio hearing a probe request from a station: BSSID of receiving radio (MAC address) and the corresponding signal strength of last probe heard for the station on that radio ** Note that per-radio data cannot be enabled in WOS, but can be enabled for the Location Service directly on the AP.

* X, y, and z indicate the station location in terms of the number of pixels from the top left (x=0, y=0, z=0) on the WOS map, where x and y are the horizontal and vertical axes on the map, respectively, and z is typically the station's distance below the AP from the mounting site. The scale is the distance covered by a pixel in feet or meters based on the map's scale setting.

** Sample format with four radios receiving a station's probe request:

```
"pr":{"64:a7:dd:44:03:20":-69,"64:a7:dd:44:03:30":-68,"64:a7:dd:44:03:40":-70,
"64:a7:dd:44:03:60":-60}
```

Contact Information

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.

Glossary of Terms

802.11a

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 5 GHz and data rates of up to 54 Mbps.

802.11b

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 2.4 GHz and data rates of up to 11 Mbps.

802.11g

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 2.4 GHz and data rates of up to 54 Mbps.

802.11n

A supplement to the IEEE 802.11 WLAN specification that describes enhancements to 802.11a/b/g to greatly enhance reach, speed, and capacity.

Access Point

A high capacity wireless access point utilizing Gigabit LAN speeds and multiple wireless channels.

AES

(Advanced Encryption Standard) A data encryption scheme that uses three different key sizes (128-bit, 192-bit, and 256-bit). AES was adopted by the U.S. government in 2002 as the encryption standard for protecting sensitive but unclassified electronic data.

alarm

An alarm results from the correlation of events and represents a failure or fault in the network that may need immediate attention.

application client

An applet that resides on the local machine where the WOS server resides that provides access to the client interface.

authentication

The process that a station, device, or user employs to announce its identify to the network which validates it. IEEE 802.11 specifies two forms of authentication, open system and shared key.

bandwidth

Specifies the amount of the frequency spectrum that is usable for data transfer. In other words, it identifies the maximum data rate a signal can attain on the medium without encountering significant attenuation (loss of power).

browser client

A web-based application that provides remote access to the WOS client interface from a Web browser.

BSS

(Basic Service Set) When a WLAN is operating in infrastructure mode, each access point and its connected devices are called the Basic Service Set.

BSSID

The unique identifier for an access point in a BSS network. See also, **SSID**.

cell

The basic geographical unit of a cellular communications system. Service coverage of a given area is based on an interlocking network of cells, each with a radio base station (transmitter/receiver) at its center. The size of each cell is determined by the terrain and forecasted number of users.

channel

A specific portion of the radio spectrum—the channels allotted to one of the wireless networking protocols. For example, 802.11b and 802.11g use 14 channels in the 2.4 GHz band, only 3 of which don't overlap (1, 6, and 11). In the 5 GHz band, 802.11a uses 8 channels for indoor use and 4 for outdoor use, none of which overlap.

CoS

(Class of Service) A category based on the type of user, type of application, or some other criteria that QoS systems can use to provide differentiated classes of service.

default gateway

The gateway in a network that a computer will use to access another network if a gateway is not specified for use. In a network using subnets, a default gateway is the router that forwards traffic to a destination outside of the subnet of the transmitting device.

DHCP

(Dynamic Host Configuration Protocol) A method for dynamically assigning IP addresses to devices on a network. DHCP issues IP addresses automatically within a specified range to client devices when they are first powered up.

DHCP lease

The DHCP lease is the amount of time that the DHCP server grants to the DHCP client for permission to use a particular IP address. A typical DHCP server allows its administrator to set the lease time.

DNS

(Domain Name System) A system that maps meaningful domain names with complex numeric IP addresses. DNS is actually a separate network—if one DNS server cannot translate a domain name, it will ask a second or third until a server is found with the correct IP address.

domain

The main name/Internet address of a user's Internet site as registered with the InterNIC organization, which handles domain registration on the Internet. For example, the “domain” address for Avaya is: http://www.avaya.com, broken down as follows:

- **http://** represents the Hyper Text Teleprocessing Protocol used by all Web pages.
- **www** is a reference to the World Wide Web.
- **avaya** refers to the company.
- **com** specifies that the domain belongs to a commercial enterprise.

encryption

Any procedure used in cryptography to translate data into a form that can be decrypted and read only by its intended receiver.

frame

A **packet** encapsulated to travel on a physical medium, like Ethernet or Wi-Fi. If a packet is like a shipping container, a frame is the boat on which the shipping container is loaded.

gateway

The gateway in a network that a computer will use to access another network if a gateway is not specified for use. In a network using subnets, a default gateway is the router that forwards traffic to a destination outside of the subnet of the transmitting device.

Gigabit Ethernet

The newest version of Ethernet, with data transfer rates of 1 Gigabit (1,000 Mbps).

host name

Each computer running TCP/IP (regardless of the operating system) has a host name—also known as a machine name. Host names are used by networking applications, such as Telnet, FTP, Web browsers, etc. In order to connect to a computer running the TCP/IP protocol using its host name, the host name must be resolved to an IP address. Host name resolution is typically done by the Domain Name System (DNS). Changing a computer's host name does not change its NetBIOS name. See also, **DHCP lease** and **NetBIOS**.

icon

A graphical symbol used in the WOS client interface to represent objects, such as APs within a map, alarms and events. See also, **map symbol**.

Intrusion Detection System

An Avaya proprietary application that scans and monitors the WOS database for intruders.

MAC Address

(Media Access Control Address) A 6-byte hexadecimal address assigned by a manufacturer to a device.

managed network

The network under management by WOS. This includes all the APs discovered by WOS, and all of their radios and the devices that are associated to them.

map

A pictorial representation of your network or subnet. The background image for the default main map supplied with WOS is a global map of the world, but you can change the background image of any map at any time. For example, you may want to organize your maps to reflect a corporate organization based on functional areas, physical site layouts, or geographic areas.

map symbol

Also known simply as "symbols," these are graphical representations of APs in the WOS client interface maps. The symbol for an AP is a pictorial image of the Avaya Wireless AP. See also, **icon**.

Mbps

(Megabits per second) A standard measure for data transmission speeds (for example, the rate at which information travels over the Internet). 1 Mbps denotes one million bits per second.

MTBF

(Mean Time Between Failures) Used in reports, this shows the average time (in hours and minutes) between failures of an AP.

MTTR

(Mean Time To Repair) Used in reports, this shows the average time (in minutes) to restore functionality to the AP following a failure.

NetBIOS

(Network Basic Input Output System) All computers running the Windows® operating system have a NetBIOS name. The NetBIOS name is specified by the user when Windows® networking is installed and configured. In order to connect to a computer running TCP/IP via its NetBIOS name, the name must be resolved to an IP address. A computer's NetBIOS name is often the same as the computer's host name, because most users accept the default settings when installing their Windows® operating system.

NTP

(Network Time Protocol) An Internet standard protocol (built on top of TCP/IP) that ensures the accurate synchronization (to the millisecond) of computer clock times in a network of computers. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock.

packet

Data sent over a network is broken down into many small pieces—packets—by the Transmission Control Protocol layer of TCP/IP. Each packet contains the address of its destination as well the data. Packets may be sent on any number of routes to their destination, where they are reassembled into the original data. This system is optimal for connectionless networks, such as the Internet, where there are no fixed connections between two locations.

POE

This refers to Power over Ethernet modules that provide DC power to APs. Power is supplied over the same Cat 5e or Cat 6 cable that supplies the data connection to your Gigabit Ethernet switch, thus eliminating the need to run a power cable.

polling

The process of contacting a network, AP or group of APs and collecting statistical data about the device(s).

preamble

Preamble (sometimes called a header) is a section of data at the head of a **packet** that contains information that the access point and client devices need when sending and receiving packets. PLCP Has two structures, a long and a short preamble. All compliant 802.11b systems have to support the long preamble. The short preamble option is provided in the standard to improve the efficiency of a network's throughput when transmitting special data, such as voice, VoIP (Voice-over IP) and streaming video.

private key

In cryptography, one of a pair of keys (one public and one private) that are created with the same algorithm for encrypting and decrypting messages and digital signatures. The private key is provided only to the requestor and never shared. The requestor uses the private key to decrypt text that has been encrypted with the public key by someone else.

PSK

(Pre-Shared Key) A TKIP passphrase used to protect your network traffic in WPA.

public key

In cryptography, one of a pair of keys (one public and one private) that are created with the same algorithm for encrypting and decrypting messages and digital signatures. The public key is made publicly available for encryption and decryption.

QoS

(Quality of Service) QoS can be used to describe any number of ways in which a network provider guarantees a service's performance, such as an average or minimum throughput rate.

radio

A configurable wireless module (radio) dedicated to the Avaya Wireless AP family of products.

RADIUS

(Remote Authentication Dial-In User Service) A client-server security protocol, developed to authenticate, authorize, and account for dial-up users. The RADIUS server stores user profiles, which include passwords and authorization attributes.

rogue

Any wireless device that is visible on your network but not recognized. You have the option of defining all rogue devices as either Unknown, Known, or Approved. Based on your definition, you can deny or allow access to the network for any rogue device.

RSSI

(Received Signal Strength Indicator) A measure of the energy observed by an antenna when receiving a signal.

SNMP

(Simple Network Management Protocol) A standard protocol that regulates network management over the Internet.

SNTP

(Simple Network Time Protocol) A simplified version of NTP. SNTP can be used when the ultimate performance of the full NTP implementation described in RFC 1305 is not needed or justified.

SSID

(Service Set IDentifier) Every wireless network or network subset (such as a BSS) has a unique identifier called an SSID. Every device connected to that part of the network uses the same SSID to identify itself as part of the family—when it wants to gain access to the network or verify the origin of a data packet it is sending over the network. In short, it is the unique name shared among all devices in a WLAN.

subnet mask

A mask used to determine what subnet an IP address belongs to. An IP address has two components: (1) the network address and (2) the host address. For example, consider the IP address 150.215.017.009. Assuming this is part of a Class B network, the first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.

symbol

Refer to **map symbol** and **icon**.

Syslog

(SYStem LOGging) A protocol that allows a machine to send event notification messages across IP networks to event message collectors, known as Syslog servers. Syslog messages are based on the User Datagram Protocol (UDP). They are received on UDP port 514 and cannot exceed 1,024 bytes in length (they have no minimum length). See also, **UDP**.

threshold

A value that determines the minimum and maximum limit for collected data. If the collected data violates a defined threshold, the system reports the fault as needing attention.

TKIP

(Temporal Key Integrity Protocol) Provides improved data encryption by scrambling the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the encryption keys haven’t been tampered with.

transmit power

The amount of power used by a particular radio transceiver to send the signal out. Transmit power is generally measured in milliwatts, which you can convert to dBm.

UDP

(User Data Protocol) A connectionless protocol that works at the OSI transport layer. UDP provides datagram transport but does not acknowledge their receipt. UDP is the protocol used for processing Syslog messages. See also, **Syslog**.

VLAN

(Virtual LAN) A group of devices that communicate as a single network, even though they are physically located on different LAN segments. Because VLANs are based on logical rather than physical connections, they are extremely flexible. A device that is moved to another location can remain on the same VLAN without any hardware reconfiguration.

Wireless AP

A family of Avaya proprietary high capacity wireless access points utilizing multiple channels.

Avaya Release 8.0 4/11/17

Index