Cambium Networks™

Xirrus Management System

User's Guide

Release 8.2 - January 2018

This manual covers XMS-Enterprise. It does not cover XMS-Cloud.

Table of Contents

List of Figures

Introduction

This section introduces the Xirrus Management System (XMS), 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 Xirrus Family of Products" on page 1**
- **"XMS Product Overview" on page 2**
- **"Key Features and Benefits" on page 3**
- **"About this User's Guide" on page 6**

The Xirrus Family of Products

- **Xirrus Management System Enterprise (XMS-E)**

  XMS-E is a powerful management tool, designed to manage your wireless Access Points from anywhere in the network — ideal for large scale wireless deployments. XMS-E supports all Xirrus Access Point models.

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

  XMS-E is available for hosting on your own server:

  - **Xirrus Virtual Appliance — Virtualized XMS Enterprise (XMS-E) Server Software (XMS-9000-VM)**

    This package allows you to install and run XMS Enterprise (XMS-E) server software on your own virtual server.

- **XMS-Cloud (XMS-9500-CL)**

  XMS-Cloud is a cloud-based management platform that provides simplified monitoring and management of the Xirrus wireless Access Point network.

  This manual covers XMS-E. It DOES NOT cover XMS-Cloud.

- **Xirrus Wireless Access Points**

  Multiple versions of Xirrus Wireless Access Points with different numbers of radios support a variety of deployment applications. For more information on most APs, refer to the Xirrus *Wireless Access Point User's Guide*. Some smaller models, such as the XR-320, run the AOSLite operating system, and are managed only with the Xirrus Management System.

XMS Product Overview

The Xirrus Management System is a wireless network management application for managing a network of Xirrus Access Points. XMS provides centralized monitoring, configuration, reporting, and management functions for Access Points—either individually, by group, or for all Access Points.

Extended Management Capability

XMS 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 Access Points, radios, stations, and rogue devices. With its powerful discovery feature and map-based organization of your wireless Access Points, XMS streamlines the management of Access Point configurations.

XMS allows IT administrators to manage configurations, schedule firmware upgrades across multiple wireless Access Points, and create groups of wireless Access Points to simplify repetitive tasks. XMS 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 Xirrus 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

wireless Access Points, Xirrus developed XMS to facilitate faster and more cost-effective high capacity Wi-Fi rollouts across large campus environments.

XMS monitors wireless performance and gathers detailed reporting and statistical data for each Access Point residing in the network, or for the entire network as a whole. It also allows you to schedule firmware updates for individual wireless Access Points or groups of Access Points 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 a Xirrus 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 XMS to configure and manage your network of Access Points.

Centralized Configuration and Management

Allows you to view and manage your entire wireless network at Layer 3 using your existing Ethernet infrastructure. In addition, XMS discovers, authenticates and configures new wireless Access Points, making large scale deployments quick and easy. Configuration templates ensure consistent configuration of

Access Points across the network, and they are easily created by copying the configuration of a "known-good" Access Point.

Scalability

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

Security Management

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

Powerful Graphical Interface

XMS's client interfaces provide all the tools and features that are necessary to ensure your Access Point 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 XMS Dashboard (**Figure 1**) provides an at-a-glance overview of the security and performance of your Access Point network.
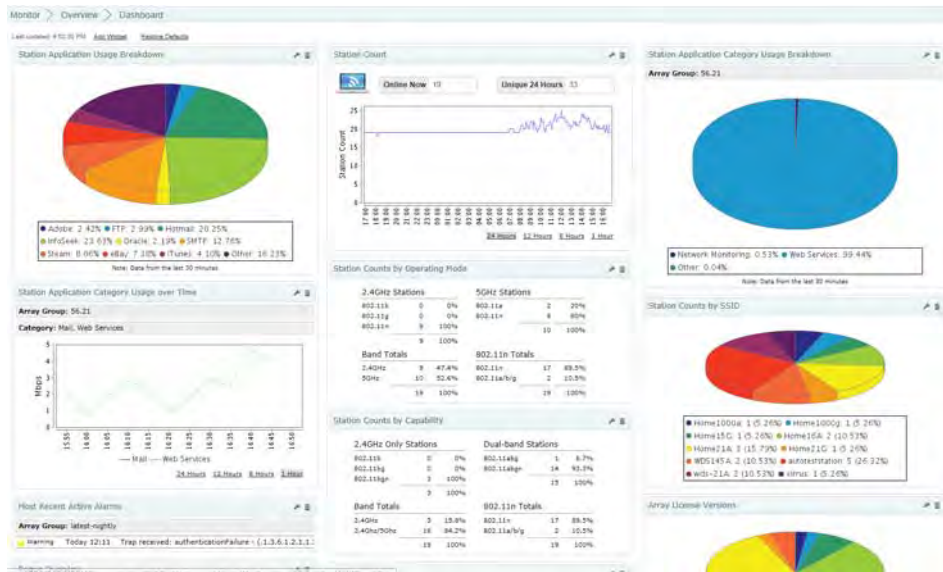
Figure 1. XMS Dashboard

Performance Monitoring

Continuously monitors and displays wireless performance.

Centralized Upgrade Management

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

Network Monitoring and Reporting

XMS displays all Access Point alerts and alarms to allow you to determine how to respond to faults in the Access Point network. It also monitors your Access Point network's performance and provides detailed reporting and statistical data for Access Points individually, by group of Access Points, by SSID, or by individual radios (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 XMS on their own virtual environment, to understand and navigate the XMS client interface, and to successfully manage their network of wireless Access Points with a browser-based interface. XMS is installed on your own VMware-based platform. This Guide does not cover the installation or management of Access Points in isolation from XMS. For procedures that deal with Access Points not centrally managed by XMS, refer to he Xirrus *Wireless Access Point User's Guide*.

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.

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

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

- **The XMS Web Client**
  Describes how to use the web client interface, including a summary of the wireless network monitoring, configuration, reporting, and XMS 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 Access Points as profile networks to ensure the deployment of consistent software and settings across each profile.

- **Managing Switches**

  Describes how to configure and manage Xirrus PoE+ Gigabit wired switches.

- **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**

  XMS generates detailed performance and status reports about the wireless network, all Access Points within the network, individual radios contained within each Access Point, and their client stations. This chapter provides instructions for reviewing and managing these reports in the web client.

- **Configuring a Wireless Access Point**

  XMS provides a configuration window that has options that allow you to easily configure settings on an Access Point.

- **XMS Administration**

  Provides instructions for managing the XMS 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 Xirrus contact information.

- **Glossary of Terms**

  Provides an explanation of terms directly related to XMS 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.

Xirrus Management System Products

The Enterprise version of the Xirrus Management System is offered as:

- **XMS (XMS-9000-VM or XMS-9000-HV)**—a virtualized XMS server software application package that allows you to install and run the XMS server software on your own virtual server under VMware or Hyper-V.

XMS (XMS-9000-VM or XMS-9000-HV)

The XMS Enterprise (XMS) server is designed to be run on a virtual platform. The application package allows you to install and run the XMS server on your own virtual machine under VMware or Hyper-V (XMS-9000-VM or -HV). For installation instructions, see **"Installing the XMS-9000-VM Virtual Appliance" on page 11** or **"Installing the XMS-9000-HV Virtual Appliance" on page 20**.

Take care not to over-subscribe RAM when using either version of the Virtual XMS 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.

XMS-9000-VM System Requirements

The recommended requirements for the system hosting the VMware-based XMS server are based on the scale of the Wi-Fi Access Point network to be managed—small, medium, or large. The XMS-9000-VM package must be installed on a server running VMware™. The versions that are supported are:

- VMware ESXi (recommended) Version 5.5, 6.0, or 6.5
- VMware vSphere (note that the XMS-E server custom setting form is supported through vCenter Client server)
- VMware Workstation

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

XMS-9000-HV System Requirements

The recommended requirements for the system hosting the Hyper-V version of the XMS server are based on the scale of the Wi-Fi Access Point network to be managed—small, medium, or large. The XMS-9000-HV package must be installed on a server running Microsoft Hyper-V™. The versions that are supported are:

- Windows Server 2012 R2 or 2016
- Hyper-V Server 2012 R2 or 2016
- Cores—at least 4
- Memory—8 GB minimum

You can check memory use and free space available at any time when XMS is running. See **"Viewing XMS Server Status" on page 600***. That page also provides an option for reducing database size by deleting accumulated statistical data.*

Please see the product datasheet 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 XMS server***. Follow the instructions in* **"Installing the XMS-9000-VM Virtual Appliance" on page 11**.

Installing the XMS-9000-VM Virtual Appliance

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

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

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** 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.
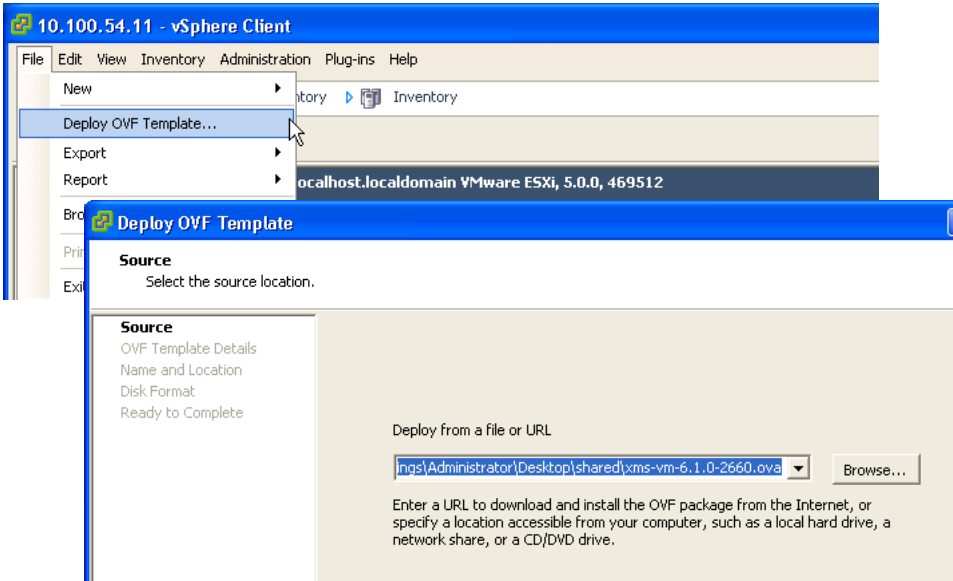
Figure 2. Opening the XMS Virtual Appliance in VMware ESXi

5. Follow the prompts to import the XMS Virtual Appliance. **IMPORTANT**: Select the XMS 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**.

When prompted by VMware ESXi to "Please enter the Hostname to assign to the VM," be sure to enter a valid domain name. Do not enter an IP address instead. An error may result in DNS settings not being configured.
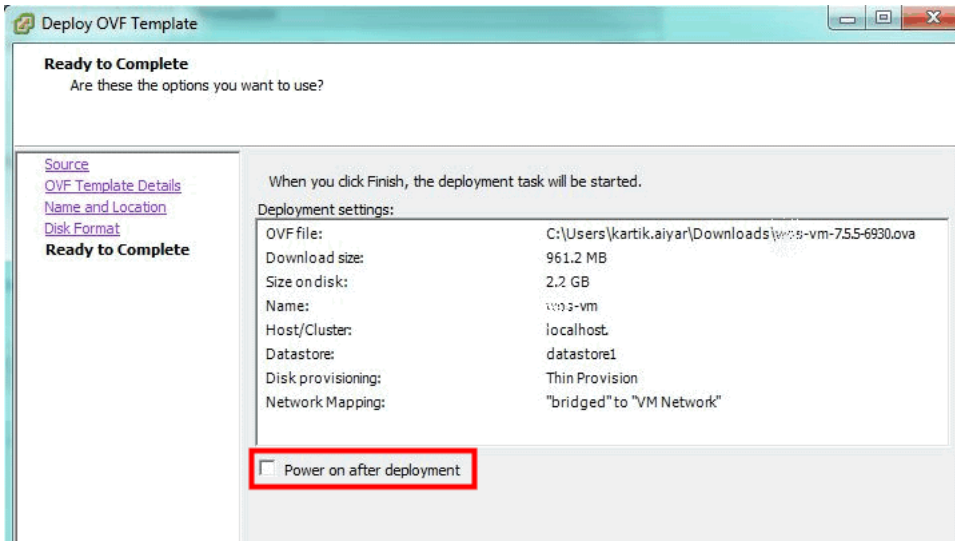
Figure 3. Don't start the XMS Server automatically (ESXi shown)

6. Once deployment is complete, right click the XMS 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 XMS Appliance as recommended in the datasheet.

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

You cannot increase the disk size once you have started using the XMS server—you have to follow the steps shown here to provide a larger disk. Also, you cannot just increase the size of an existing disk at this point. You must delete Disk 2, then recreate it with the required size.

Delete **Disk 2**, then display the **Add Hardware** dialog. Click **Hard Disk** then **Next**.
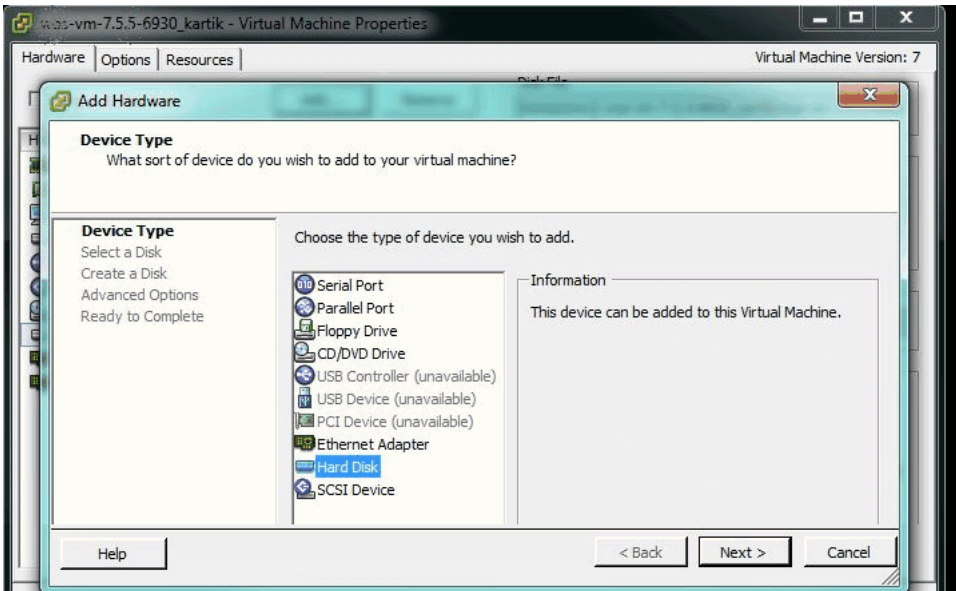
Figure 4. Creating a new, larger hard disk (ESXi shown)

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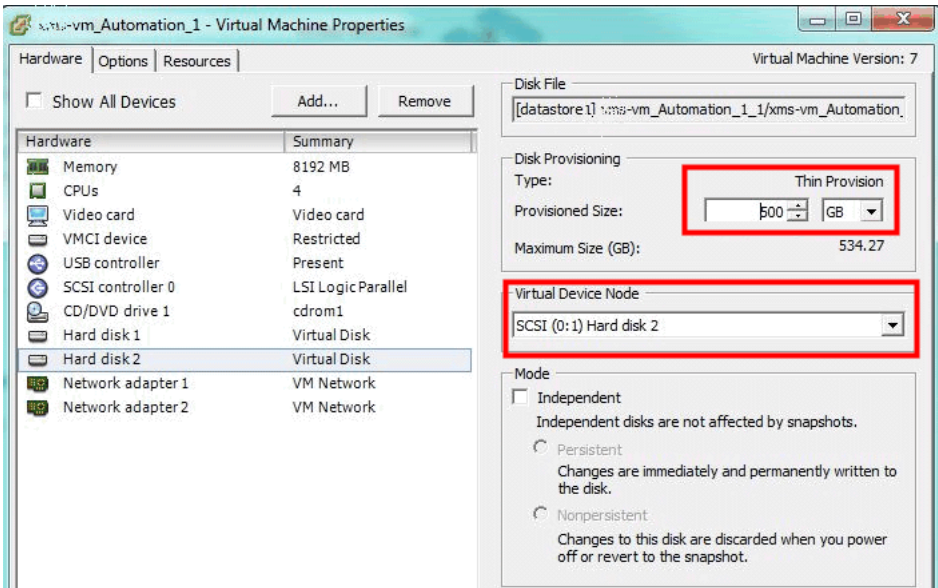
Figure 5. Creating a new, larger hard disk (continued, ESXi shown)

9. Start the XMS 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 XMS 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.
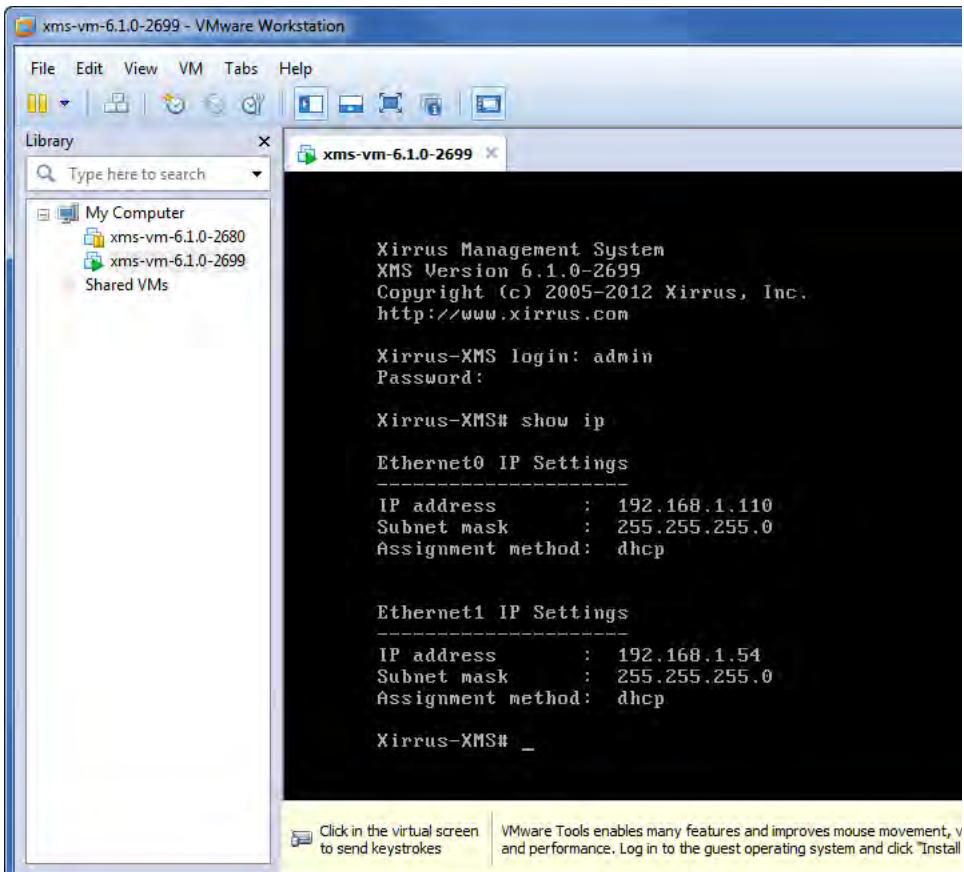
Figure 6. Starting the XMS Server on the Virtual Appliance

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 XMS 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 XMS server

13. Continue to **"Initial Server Setup for Virtual Appliances" on page 33** to configure and begin using the XMS server.

> *Licensing - The XMS 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 XMS 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 XMS 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**.
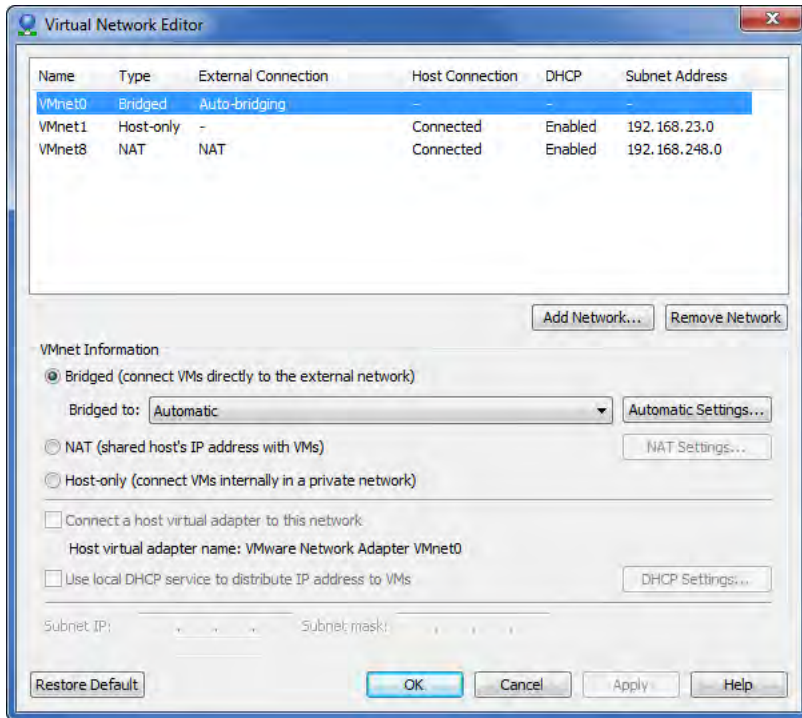
Figure 8. Using vmnetcfg.exe

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 XMS-9000-HV Virtual Appliance

The XMS Virtual Appliance for Hyper-V is supplied as an .exe file, for example, **XMS Hyper-V Installer-8.0.1-7301.exe**. It contains all the software that you need to install an XMS 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 XMS, 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.

    You will need a virtual switch to permit Internet access via a physical port on the host. This may be configured using the Virtual Switch Manager (see **Step 5**) before you begin installing the XMS server. If you do not create a virtual switch in advance, the installation process will prompt you to do so (**Step 3**).

2. Run the installer executable file, for example: **XMS Hyper-V Installer-8.0.1-7301.exe**. The XMS Hyper-V Installer Setup Wizard will walk you through the installation steps.

3. XMS-9000-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 XMS server, be sure to specify the IP address that APs should use for contacting the server. See **"XMS Call-back Address" on page 635**.
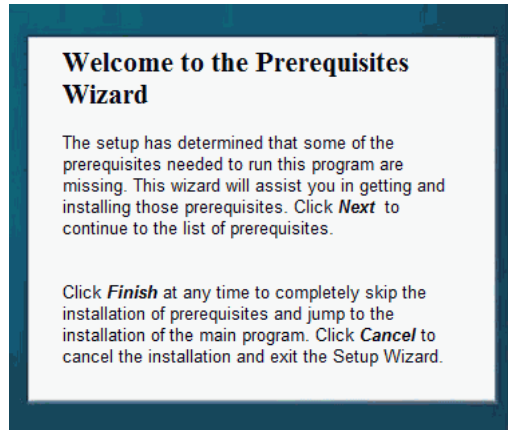
Figure 9. XMS Hyper-V Installer Setup Wizard

4. Select all listed prerequisites and click **Next**.
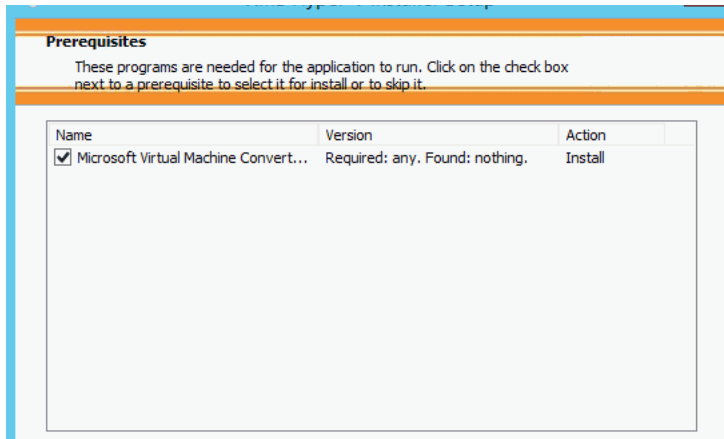
Figure 10. XMS Hyper-V Installer Prerequisites Wizard

5. The wizard will inform you that you need to set up a virtual switch and ask whether you wish to use the Virtual Switch Manager. Go ahead and start the manager.
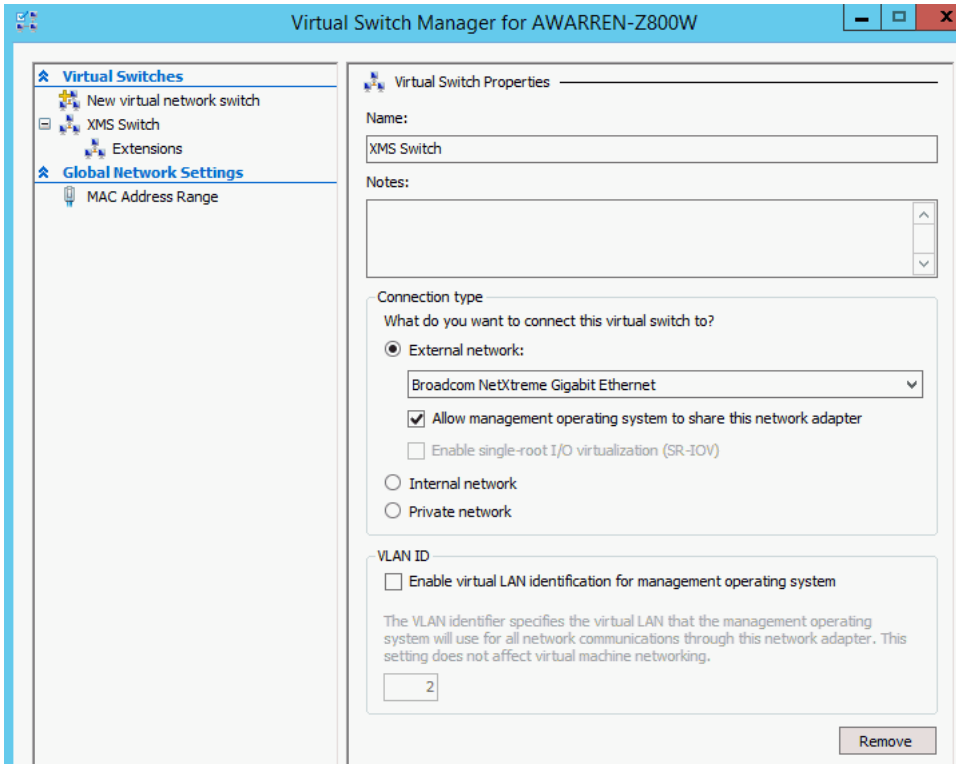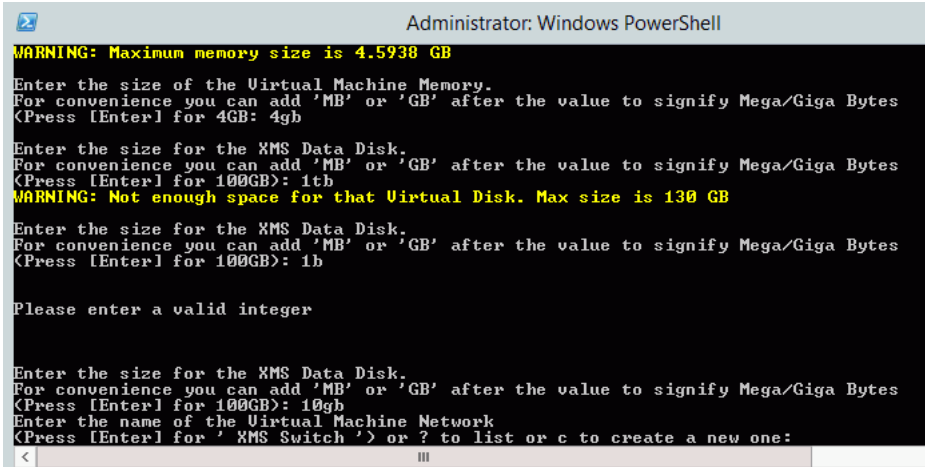
Figure 11. XMS Hyper-V Virtual Switch Manager

6. Enter a **Name** for this switch, such as XMS **Switch** (most characters are allowed in the name, including spaces). Select a **Connection Type**—this will usually be **External Network**. Select the desired physical port from the drop-down list. You may check the box to **Allow management operating system to share this network adapter** (optional). Click **OK** to create the virtual switch.

7. Click **Next>.** A Windows PowerShell window appears. In it, the XMS Hyper-V Installer continues to walk you through entering the remainder of the XMS server settings. (**Figure 12**)

    • If you have not yet created a Virtual Switch to connect a port on the virtual machine to a physical port that has Internet connectivity, do so

now. Enter a **Name** for the virtual switch, such as XMS **Switch**. The installer lists the available physical ports. Enter the **Index** of the desired port.

Figure 12. XMS Hyper-V Installer—PowerShell

- **Enter the VM Name** (name of the XMS server): Press the **Enter** key to use the default name for the server: **xirrus-xms**. If you use a different name, be aware that you **must** ensure that the name **xirrus-xms** resolves to your chosen server name. Please see **"How Discovery Works" on page 179**.

- **Start the XMS 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 XMS 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 XMS server's system disk).
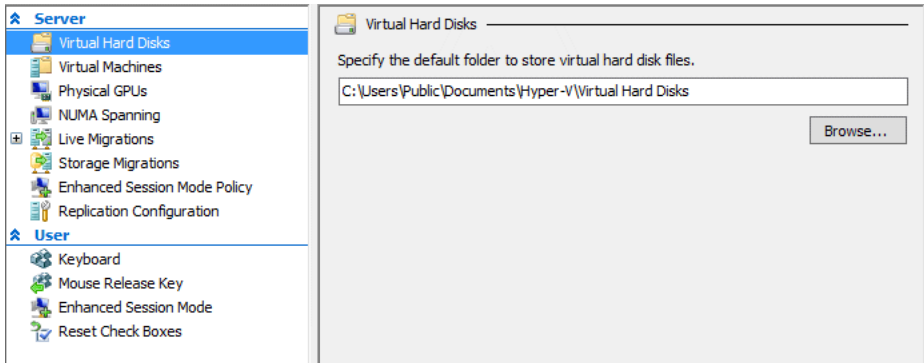
Figure 13. Hyper-V—Virtual Hard Disks

- **Enter the name of the Virtual Machine Network**: you may do one of the following.
  - Use the **Enter** key to accept the default switch whose name is shown. If there is only one switch defined, that is the default. If there are multiple virtual switches defined, then this is the first one.
  - Enter ? to list out the virtual switches that have been defined. Then enter the index number shown for the desired switch.
  - If you have not already created a virtual switch, enter **c**. This will take you to the Hyper-V Virtual Switch Manager to create a virtual switch as described in **Step 6** above.

8. After you have entered the settings above, the installation of the XMS server under Hyper-V proceeds. Messages will inform you of the progress of the installation, and of the location of the XMS server Virtual Hard Disk (vhd file).

9. The installer will ask whether you wish to start the XMS 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.

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

Getting Started with XMS

This chapter describes how to get started using XMS.

Section headings for this chapter include:

XMS Port Requirements

A number of ports are used by XMS and by various Access Point features. These ports must not be blocked by firewalls.

The **Port Requirements table on page 29** lists ports and the features that require them.
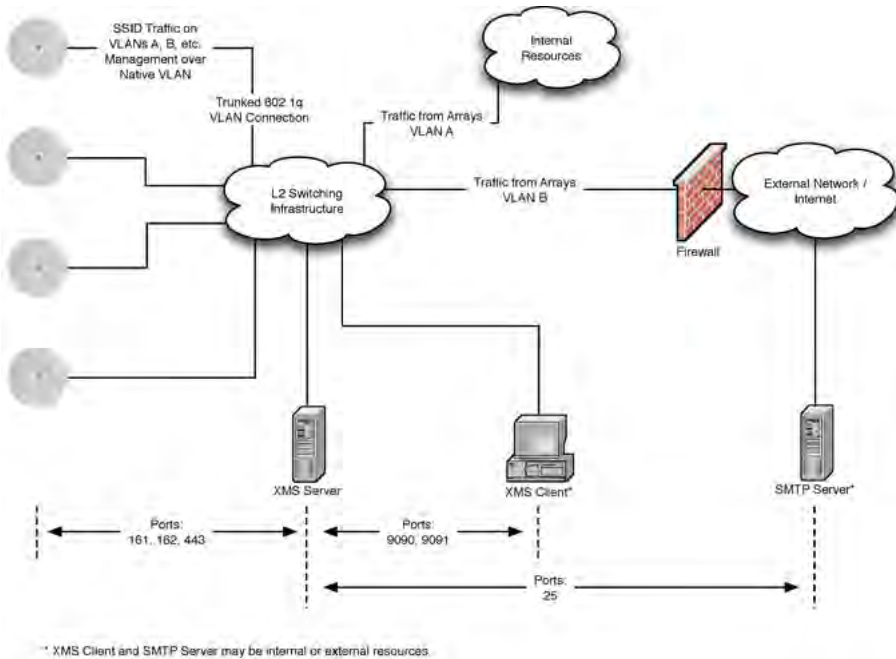
Figure 14. Sample Port Requirements for XMS

Note that Access Point port requirements are included in the table for your convenience—some of the Access Point ports shown are unrelated to communication with XMS. 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 XMS port requirements are illustrated in **Figure 14**. XMS requires ports 161, 162, and 443 to be passed between Access Points and the XMS server. Similarly, ports 9443, 9090, 9091, 9092, and 9443 are required for communication between the XMS server and XMS clients, and port 25 is typically used by the XMS server to access an SMTP server to send email notifications.

The following table lists port requirements for the Access Point and for XMS, how they are used, and whether they may be changed.

Port	Application	Peer	Configurable
XMS			
22 tcp	SSH	Access Points	Yes
25 tcp	SMTP	Mail Server	Yes
123 udp	NTP	NTP Server	No
161 udp	SNMP	Access Points	No
162 udp	SNMP Trap Receiver	Access Points	Yes
514 udp	Syslog server	Access Points	Via XMS config file
	Ping	Access Points	No
1099 tcp	RMI Registry	Internal*	No
2000 tcp	XMS Back-end Server	Internal*	No
2022 tcp	SSH	Access Point	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 Communications	Access Points	No
9090 tcp	XMS Client Server	XMS client	Via XMS config file
9091 tcp	XMS Client Server	XMS client	Via XMS config file
9092 tcp	XMS Client Server	XMS client	Via XMS config file
9443 tcp	XMS WMI SSL	XMS web client	Yes
9444 tcp	Secure Web Socket	Access Points	No
* Internal to XMS Server, no ports need to be unblocked on other network devices			
Access Point			
icmp	Ping	XMS 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	XMS Server	No

Port	Application	Peer	Configurable
162 udp	SNMP Traphost Note: Up to four Traphosts may be configured.	XMS Server	Yes - but required by XMS
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	(Xirrus Roaming)	Access Points	Yes
22612 udp	Xircon (Console Utility)	Admin Workstation	Yes

Starting and Managing the XMS Server

Manage the XMS server using its management tools:

- **Managing XMS on a Virtual Appliance**

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

Managing XMS on a Virtual Appliance

On the Virtual Appliance, the XMS server is started automatically when your computer is restarted. Use the browser-based XMS web client (**Figure 15**) to perform mandatory initial configuration, to restart or reboot the server, and for server maintenance.
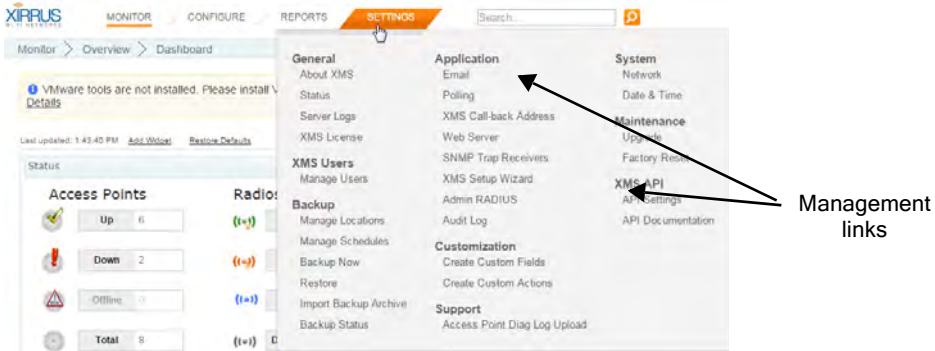
Figure 15. Server Management using the Web Client

To access the web client, set your browser's URL to the XMS 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: XMS web client access to the XMS server requires access to ports 9090 and 9443. Make sure that these ports are open in any firewalls between clients and the XMS 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 **XMS Setup Wizard**. This will lead you through entering your XMS server license and setting up discovery for your network of wireless Access Points. Proceed to **"Initial Server Setup for Virtual Appliances" on page 33** to perform required initial setup on the server.

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

If XMS is not running properly, you may click the **Restart Application** button on the lower left of the Status page to restart the XMS 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 XMS related processes in an orderly manner before rebooting. Rebooting and restarting will take about two minutes on a new Appliance. As XMS is used and

the database grows, startup integrity checks will take longer. For shutdown, see **"Shutting Down the XMS Server" on page 33**.

Initial Server Setup for Virtual Appliances

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

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

- **XMS Setup Wizard**

When those steps are complete, proceed to:

- Set the XMS polling interval based on your deployment size (see **"Polling Settings" on page 633**).

About the XMS User Interface

The XMS web client is a very fast and efficient way to view the status of your Access Point network and performing network management tasks. The Dashboard provides an at-a-glance overview of the health of your Access Point network; network discovery may be fine-tuned; RF heat maps display the RF coverage provided by your Access Points; alarms and events are displayed; pages for Access Points, radios, Stations, and SSIDs show detailed information and allow configuration; rogue devices are monitored; and Access Point 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 Access Points in one step. Reports on system performance may be created.

Shutting Down the XMS Server

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

1. Terminate all clients.

2. For Virtual Appliance servers—in the **Status** page of the XMS 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 XMS server has shutdown successfully you may shut down the computer.

The XMS Web Client

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

Starting the Web Client

Xirrus supports the latest version of the following browsers: Internet Explorer, Mozilla Firefox, Chrome, or Safari. A secure web browser is required.
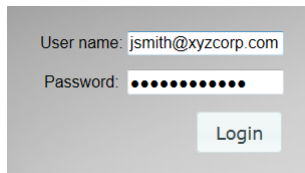
Figure 16. Login Window

To start the web client, point your workstation's browser to the IP address or hostname for the XMS 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 XMS 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 XMS functions. The menus are described in the following sections:

- **"About Monitor Pages" on page 36**
- **"About the Configure Pages" on page 38**
- **"About Reports Pages" on page 41**
- **"About Settings Pages" on page 42**
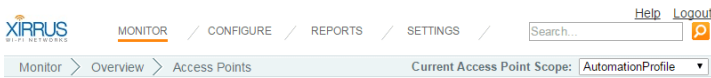
Figure 17. Mode Selection in XMS Web Client

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.
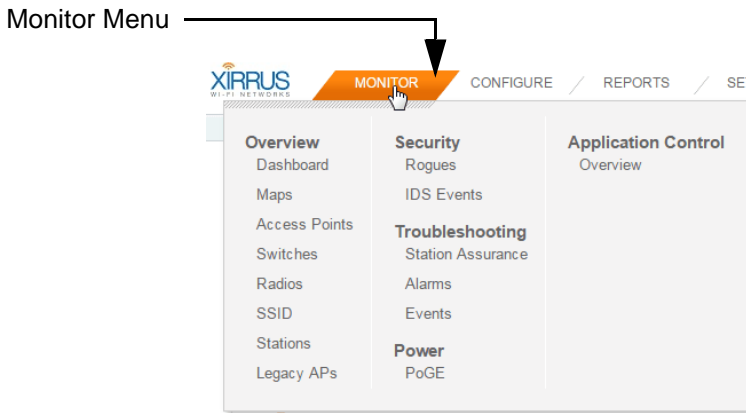
Figure 18. XMS Web Client Monitor Functions

The monitor options for XMS are shown in **Figure 18**. 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**
- **Switches**

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

Security

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

Troubleshooting

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

Power

- **PoGE**

Application Control

- **Application Control—Overview**

About the Configure Pages

> ✎ *Note that smaller APs that use the AOSLite system software, such as the XR-320, 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)
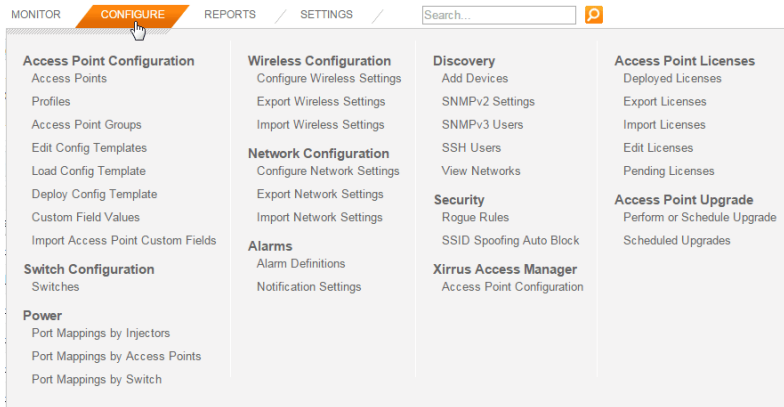
Figure 19. XMS Web Client Configure Functions

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 Access Points 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 Access Points page, which is the same as the Monitor > **Access Points** page. You must be logged in to XMS 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**

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

Switch Configuration
- **Switches**

Power
- **Port Mappings by Injectors**
- **Port Mappings by Access Points**
- **Port Mappings by Switch**

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. XMS 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 299**.
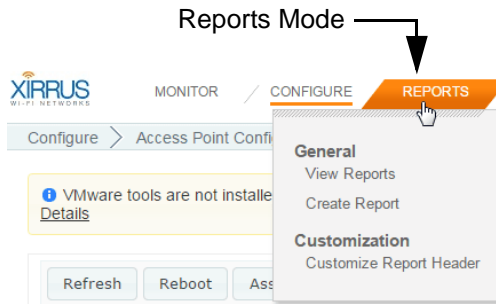
Figure 20. XMS Web Client Reports Functions

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

General

- **"View Reports" on page 301**

  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 307**

  This page lists all the types of reports available in XMS. 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 318**

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

About Settings Pages
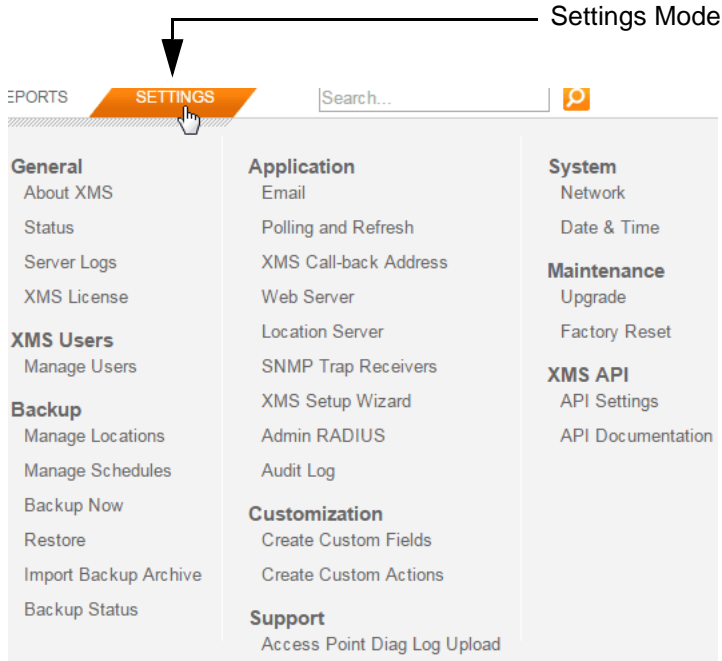
Figure 21. Settings Menus for XMS Server

These pages are used to change XMS 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 include the XMS Setup Wizard, which guides you through the initial steps for licensing the server and discovering the network. In addition, pages are offered to configure the virtual appliance. As shown in **Figure 21**, these include setting the network address and system date and time. All of these server administration functions are discussed in detail in **"Managing XMS on Virtual Appliances" on page 596**.

Settings for Virtual Platforms

General

- About XMS—Click this to display the current running XMS version as well as contact information.

- Status — Shows the running status of the XMS server. For details, see **"Viewing XMS Server Status" on page 600**.

- Server Logs—shows XMS server's operational logs. For details, see **"Viewing Server Log Files" on page 653**.

- XMS License—manages the license for the XMS software. For details, see **"Managing the XMS Server License" on page 655**.

XMS Users

- Manage Users—manages accounts for XMS users/administrators. See **"XMS Users" on page 615**.

Backup

- Backup—sets up XMS database backups. For details, see **"Database Backup Settings" on page 605**.

Application

- Email—specifies the SMTP server that XMS uses for sending emails. For details, see **"Email Settings" on page 632**.

- Polling—changes the frequency of polling Access Points. For details, see **"Polling Settings" on page 633**.

- XMS Call-back Address—changes the server address used by Access Points for some forms of communication. For details, see **"XMS Call-back Address" on page 635**.

- Web Server—changes the HTTP/HTTPS IP address used for accessing the XMS server. For details, see **"Web Server" on page 636**.

- Location Server—Sets the **Location** server information for all APs and profiles in one step. For details, see **"Location Server" on page 636**.

- SNMP Trap Receivers—the XMS server sends traps to supervisory software at these addresses when an alarm occurs. For details, see **"SNMP Trap Receivers" on page 638**.

- XMS Setup Wizard—initial setup steps for XMS server to enter license and discover Access Point network. For details, see **"XMS Setup Wizard" on page 639**.

- Admin RADIUS—specify RADIUS servers to be used for authenticating XMS logins. For details, see **"Admin RADIUS" on page 648**.

- Audit Log—shows all of the configuration changes that have occurred on managed Access Points. For details, see **"Audit Log" on page 652**.

Customization

- **Create Custom Fields**—defines custom columns to be displayed on Access Points pages. See **"Create Custom Fields" on page 619**.

- **Create Custom Actions**—defines custom actions to be offered on Access Points pages. See **"Create Custom Actions" on page 620**.

Support

- **Access Point Diag Log Upload**—uploads diagnostic information from selected Access Points to an FTP server.

XMS API

- **API Settings**—Controls API access to the XMS server. For details, see **"API Settings" on page 625**.

- **API Documentation**—describes the API and provides a sandbox for making sample calls. For details, see **"API Documentation" on page 627**.

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 XMS server, including the ports used. For details, see **"Web Server" on page 636**.

- Location Server—Sets the **Location** server information for all APs and profiles in one step. For details, see **"Location Server" on page 636**.

System

- Network—Configures IP and other port settings on the Appliance. For details, see **"Network Settings" on page 603**.

- Date & Time—Configures system time on the Appliance. For details, see **"Date and Time Settings" on page 604**.

Maintenance

- Upgrade—Upgrade the XMS server software. For details, see **"Performing Server Upgrades" on page 656**.

- Factory Reset—Reinitializes the XMS server and database. For details, see **"Resetting the XMS Server" on page 657**.

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 XMS-E are shown in **Figure 18**. 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**
- **Switches**
- **Radios**
- **SSID**
- **Stations**
- **Legacy APs**

Security

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

Troubleshooting

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

Power

- **PoGE**

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.
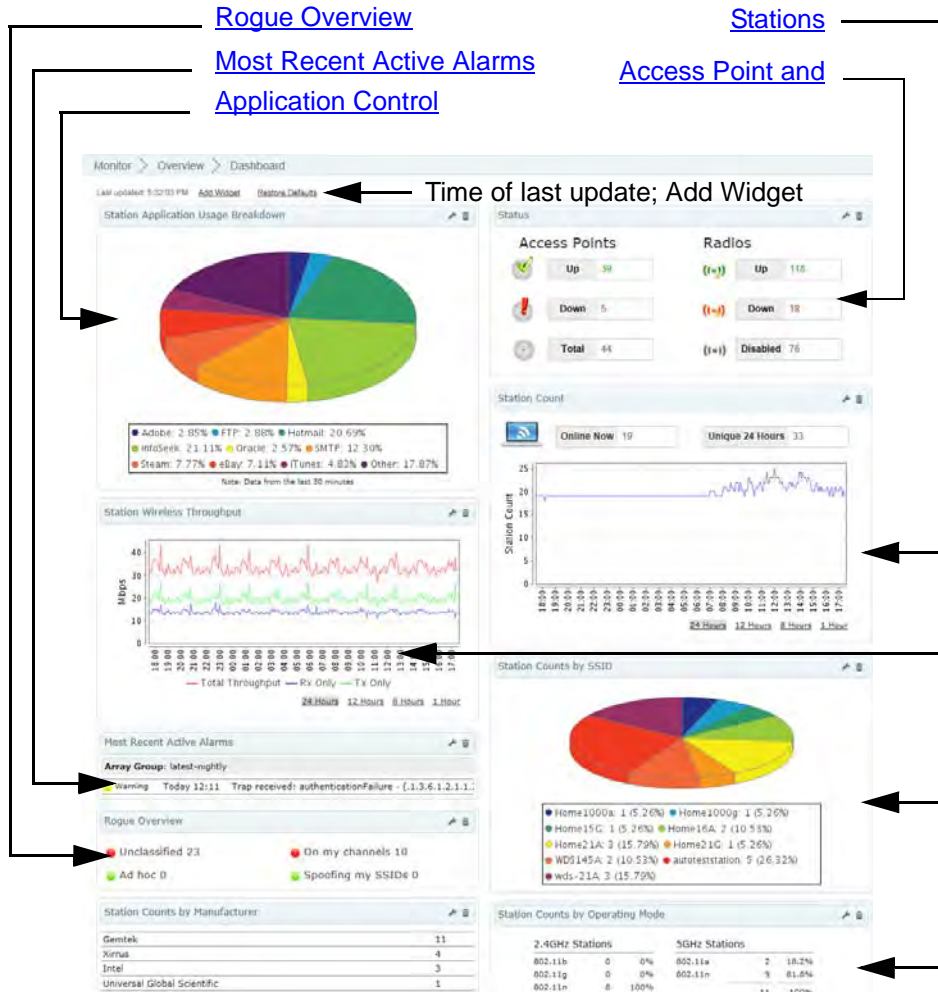
Figure 22. Dashboard

The following sections describe the use of the Dashboard:

- **"Dashboard Overview" on page 50**
- **"About Dashboard Data" on page 51**
- **"Application Control" on page 52**
- **"Access Point and Radio Status" on page 56**
- **"Most Recent Active Alarms" on page 58**
- **"Stations" on page 59**
- **"Rogue Overview" on page 63**
- **"Access Point Software and License Versions" on page 64**

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 18 on page 36**).
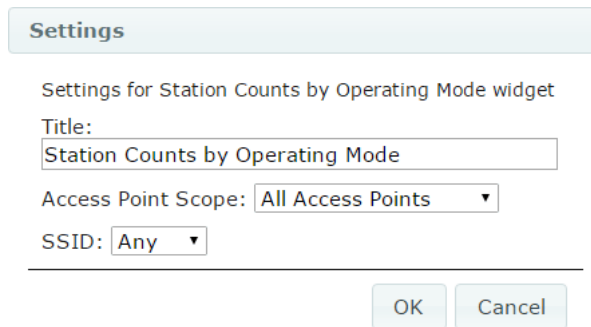
Figure 23. Three-column Arrangement of Widgets

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 23**, 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 Access Point **Scope** (profile network or group of Access Points). 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.

Figure 24. Change Widget Settings

In general, a count is faded if its value is zero. For example, if no Access Points 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 Access Points in the XMS **managed network** by default, although you may have a widget display data for just a selected Access Point **Scope** or a selected SSID by changing its settings. All widgets are updated to contain only data related to the selected Access Points (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 Access Points.

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 22**. Note that some values displayed in the Dashboard may lag with respect to actual current values—items in the XMS database are polled (updated) at differing intervals. When the Dashboard is refreshed, it simply picks up the current values in the database. The XMS server does not poll Access Points 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 633**.

The Dashboard refreshes data at the following rates by default:

- Performance data is updated on the Dashboard every 30 seconds. (This is true for Access Points 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 Access Points 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 Access Point **Scope** (see **"About Dashboard Data" on page 51**), categorized in a number of ways. Each XR Access Point uses Deep Packet Inspection (DPI—available only on XR Access Points) 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 112**.

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
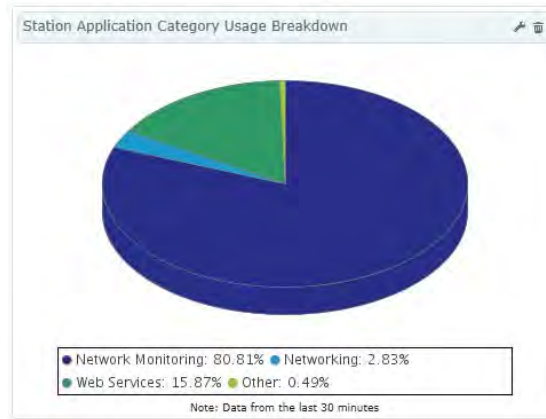
Figure 25. Dashboard - Station Application Category Usage Breakdown

This provides a breakdown of the categories of applications being used on the selected Access Points. 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
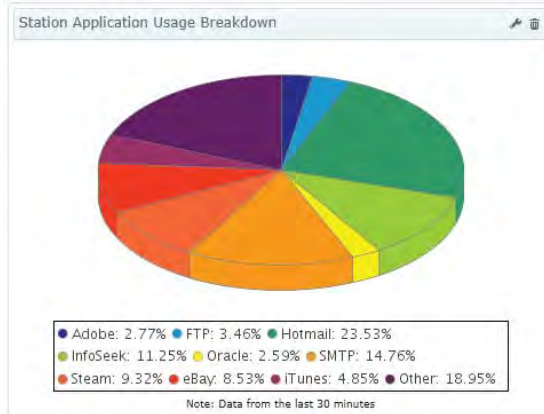
Figure 26. Dashboard - Station Application Usage Breakdown

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

Station Application Category Usage over Time
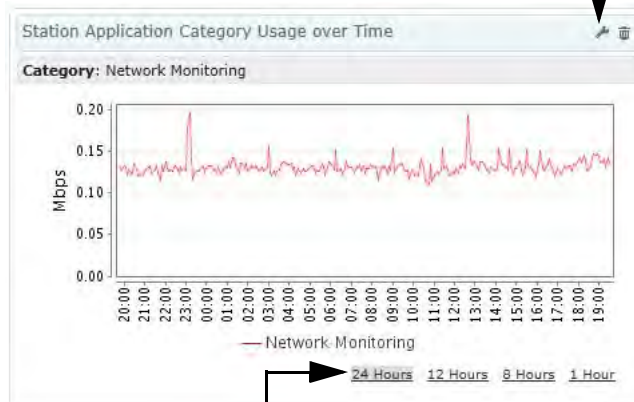
Figure 27. Dashboard - Station Application Category Usage over Time

This graph shows the amount of network traffic used by a selected category of application over time, on the selected Access Points. Select a Category of application and a time period as shown in **Figure 27**.

Station Application Usage over Time
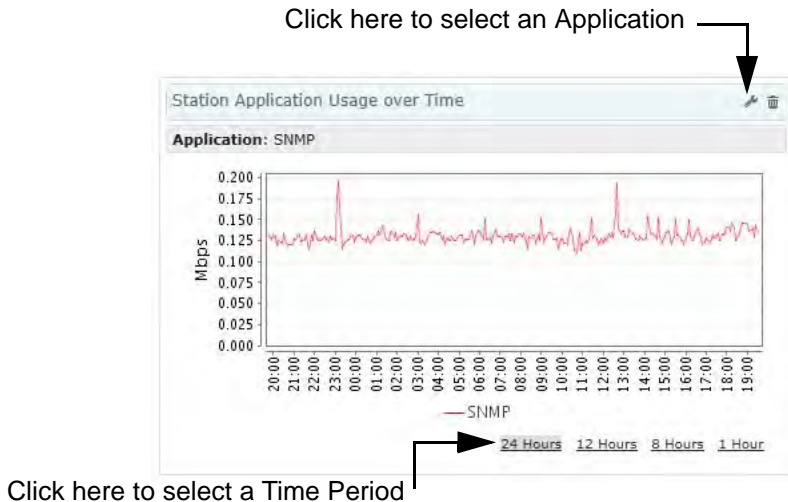
Figure 28. Dashboard - Station Application Usage over Time

This graph shows the amount of network traffic used by a selected application over time, on the selected Access Points. Select an application and a time period as shown in **Figure 28**. When selecting an application, select a category first - this helps narrow down the final selection of application, as Access Points recognize hundreds of applications.

Access Point and Radio Status

The Access Point 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 Access Point Group only (see **"Access Point Groups" on page 126**).
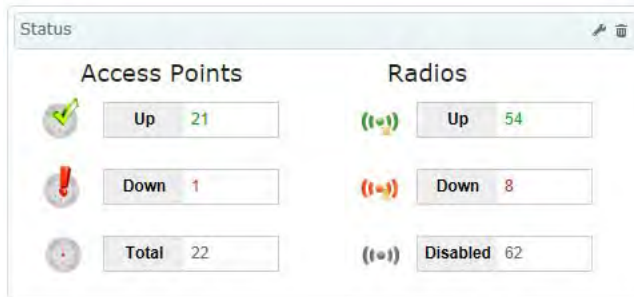
Figure 29. Dashboard - Access Point and Radio Status

Access Point Status Details

This is a summary of the status of the selected Access Points that are known to XMS. The entries show the count of Access Points 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 Access Points that are **up**, in the selected group. Click this button to show only Access Points whose status is up in the **Access Points** page.

- **Down (red)**—the number of Access Points that are **down**, in the selected group. An Access Point is considered to be down if XMS has been unable to communicate with it for over three minutes. Click this button to show only Access Points that are down in the **Access Points** page.

- **Off line (blue)**—the number of Access Points 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 123**.

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

Radio Status Details

This is a summary of the status of all radios on Access Points that are known to XMS in the selected Access Point 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 Access Points. 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 Access Points in the selected Access Point Group.

Figure 30. Dashboard - Recent Alarms

To see a complete list of wireless network alarms, use the web client **Alarms** page (see **"Alarms" on page 105**).

- **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 Access Points for the selected Access Point Group (see **"About Dashboard Data" on page 51**), categorized in a number of ways.
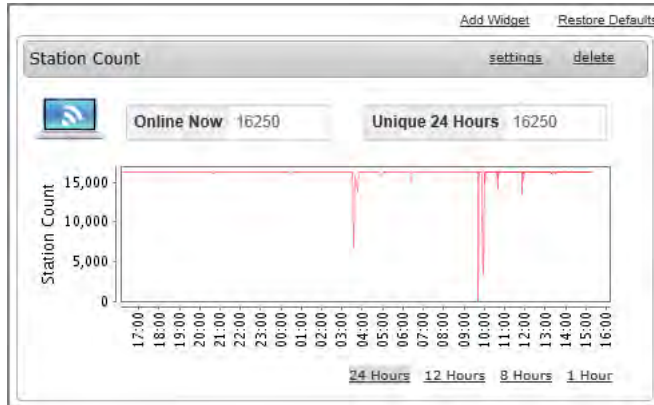
Figure 31. Dashboard - Station Count

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 Access Points known to XMS, and plots the number of stations over time. (**Figure 31**) Select the desired time period for the graph— 24 hours is the default.

Station Counts by Operating Mode

Figure 32. 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 Access Points.

Station Counts by Capability

Figure 33. 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
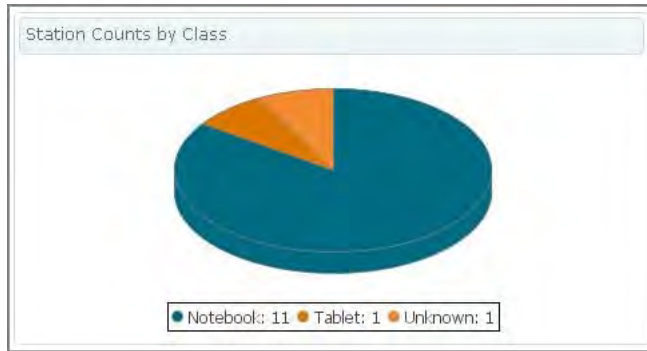
Figure 34. Dashboard - Station Count by Class

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

Figure 35. Dashboard - Station Count by Manufacturer

This provides a breakdown by station manufacturer of the number of stations that are currently associated to the selected Access Points. 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
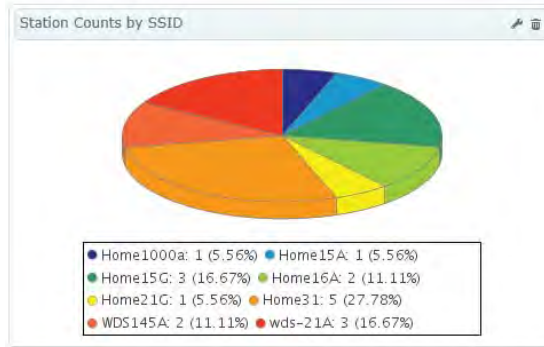
Figure 36. Dashboard - Station Counts by SSID

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
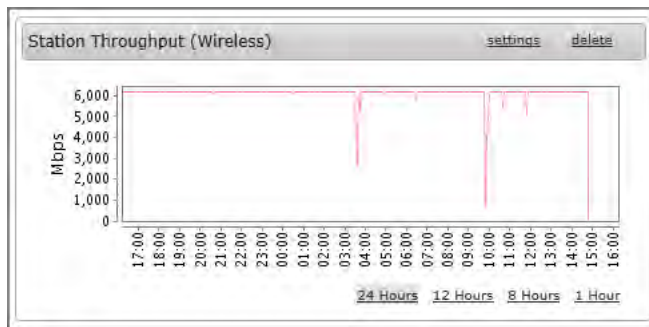
Figure 37. Dashboard - Station Throughput

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 Access Point Group in the wireless network (see **"About Dashboard Data" on page 51**), including counts of rogue APs. Each entry is a link—click it to display on the selected items on the **Rogues** page.
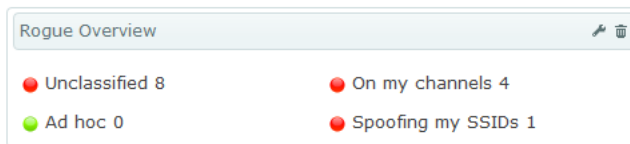
Figure 38. Dashboard - Rogue Overview

For more information about security and intrusion detection, please see **"Rogues" on page 97**.

This is a summary of the more dangerous APs that have been detected by the selected Access Points. 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 97**.

- **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 Access Point APs. 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 Access

Point 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.

Access Point Software and License Versions

These widgets summarize the software versions and license versions for Access Points in the selected Access Point Group (see **"About Dashboard Data" on page 51**).
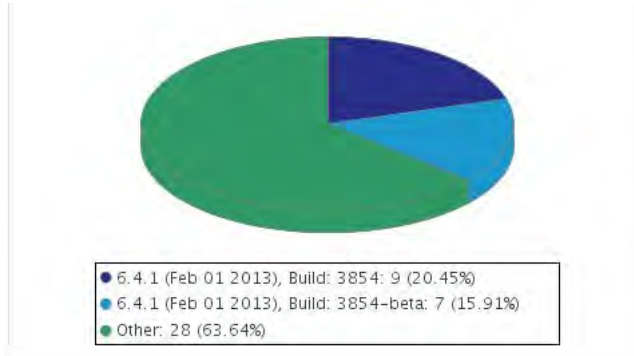
Figure 39. Dashboard - Access Point Software Versions

Two widgets describe versions:

- **Access Point Software Versions**
- **Access Point License Versions**

Access Point Software Versions

This shows the total number of Access Points running recent AOS software versions, in both tabular and graphical form. (**Figure 39**)

Access Point License Versions
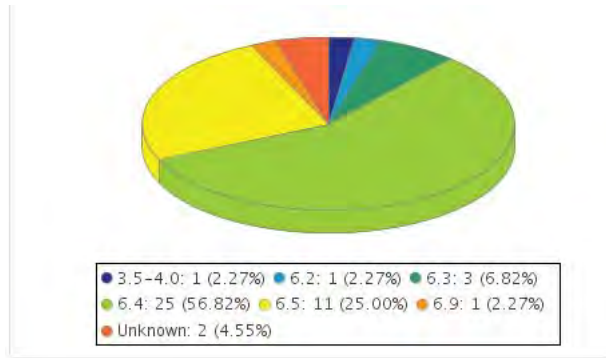
Figure 40. Dashboard - Access Point License Versions

This shows the total number of Access Points having various AOS license versions, in both tabular and graphical form.

Access Points

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

The following sections describe the Access Points page:

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

To perform bulk configuration on Access Points, please see **"Configure Network Settings" on page 159** and **"Discovery" on page 178**.

		Hostname	Management IP Address	Location	Model	Stations	Access Point OS Version	Profile	Gig1 MAC Address	
☐	🔴	Kartik-X2-120	10.100.85.110	California-S	X2-120	0	7.8.2-87-xap		48:c0:93:3c:36:a0	
☐	🟢	KARTIK-XD2-240	10.100.85.236	TestLocation	XD2-240	0	8.0.1 (Oct 14 2015), Build: 6426-beta	Frpm_AP_752	48:c0:93:5f:4c:8c	
☐	🟢	Kartik-XH2-120	10.100.85.208		XH2-120	0	7.5.2 (Sep 28 2015), Build: 6070-bet	Frpm_AP_752	50:60:28:08:0e:ac	

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

Refresh | Reboot | Assign to Profile | Pull Diagnostic Logs | Pull Config | Packet Capture | Configure▼ | Quick Config▼ | Power▼ | M

Select Columns Export   Showing: 1

Figure 41. Access Points Page

About Using the Access Points Page

A number of basic operations are available on the Access Points 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 Access Point Scope** allows you to filter the data displayed so that only information for members of the selected Access Point group or profile network is presented. Select the desired **Access Point 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 Access Points that are members of the selected profile are displayed.

This selection is persistent when you browse to other pages, until you change **Current Access Point 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 Access Points.

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 XMS 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.
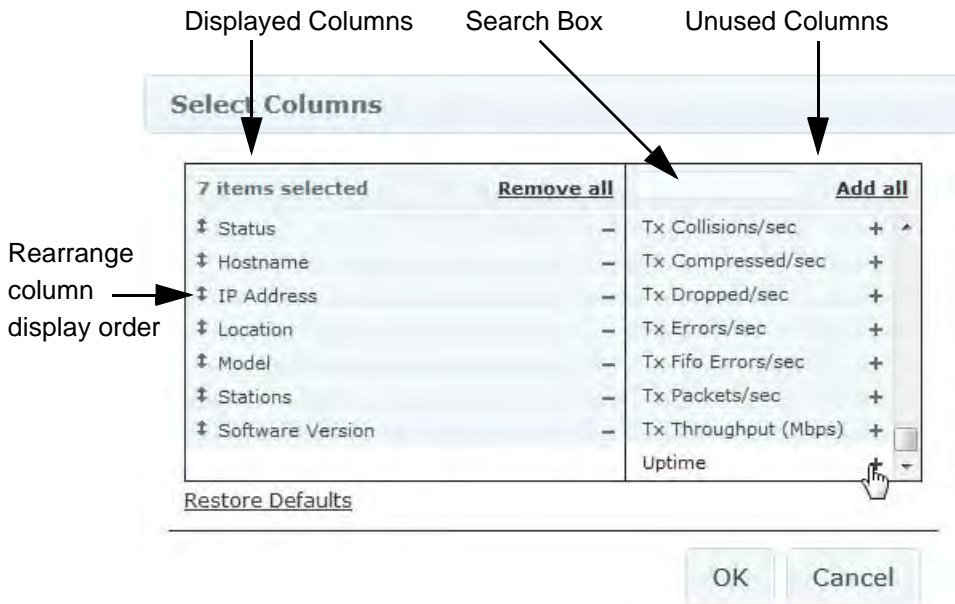
Figure 42. Table Column Chooser

You may type text into the Search Box shown above the right hand list in **Figure 42** 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 persistent on 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 Xirrus 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 Access Points 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.

Figure 43. Sorting on a Column

Searching

Enter a string in the **Search** box, and XMS 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 44**)

Figure 44. Search Results

Access Points, Stations, Rogues, Group Names, Profile Names, and even WMI menu options are shown. (**Figure 45**) If no results are displayed, then no matching entries could be found.

The following fields are searched:

- Access Points—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.

Figure 45. Search Results include Web Client Menu Options

The Access Points List

The Access Points List (**Figure 41 on page 66**) shows Access Points that have been discovered by XMS. Only Access Points that belong to the group selected in **Current Access Point Scope** are displayed. To search for a particular Access Point, see **"Searching" on page 70**. **The Access Points Toolbar** allows you to perform a number of operations selected Access Points.

Click on an Access Point's Hostname to access a variety of **Access Point Details** pages.

For each Access Point, the following information is shown by default:

- A green or red dot showing the current status of each Access Point

- The **Hostname**

- The **Management IP Address** of the Access Point

- The **Location** of the Access Point (if this information was configured on the Access Point)

- The **Model** of the Access Point. If you have expanded the capacity of an Access Point by adding modular 802.11ac APs to it (XI-867/1300), then the model is determined by the number and types of APs present. For example, if you add four 1300 Mbps (3X3 MIMO) IAPs to an XR-4420, the AP will display its model number as XR-4836 because it now has eight 3x3 IAPs including 802.11ac radios.

- The number of **Stations** associated to this Access Point

- The **AOS version** running on the Access Point

- The **Profile** network that the Access Point is a member of, if any (see **"Managing by Profiles" on page 211**)

- **Config Push** columns describe the last attempt to update ("push") configuration settings on an AP. The time of the last push is shown along with the result of the push. A message gives more information about the result of the push. Tip: if the status seems to be "stuck" at **In Progress**, click the **Refresh** button.

*A newly discovered Access Point will automatically be added to the default profile network, if one has been specified. See **"Managing by Profiles" on page 211** and the **Default** button in **"The Profiles Toolbar" on page 215**.*
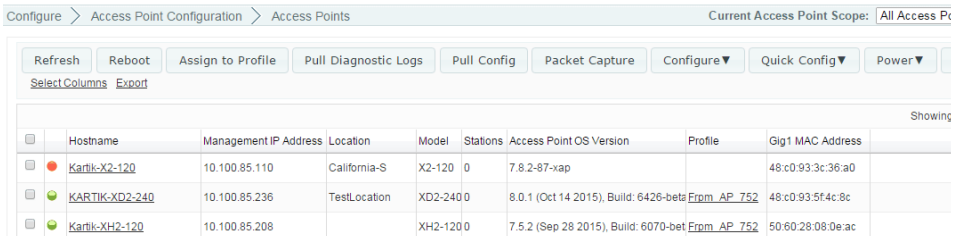
You may customize the columns shown in this list—many more columns are available. For example, selecting the **Licensed Features** column is the best way to see the features supported on all of your Access Points. See **"Select Columns" on page 67**.

An Access Point's Host Name will typically be used to identify the Access Point throughout the XMS 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 Access Points toolbar offers functions for Access Point management, including configuration, gathering diagnostic information, rebooting selected Access Points, and capturing packets. This toolbar is visible to XMS users with read-write privileges. XMS users with read-only privileges will see a restricted toolbar that only includes options for **Refresh**, **Pull Diagnostic Logs**, **Pull Config**, and **Packet Capture**.

Figure 46. The Monitor—Access Points Page Toolbar

Select one or more Access Points in the list by clicking their checkboxes in the first column. You may click the checkbox in the header row to select all Access Points, or click again to deselect all. The operations available are very similar to those offered on the Configure Access Points Toolbar. See **"The Configure Access Points Toolbar" on page 119** for details.

Access Point Details

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

- **"Access Point Details—General" on page 75**
- **"Access Point Details—Configuration" on page 76**
- **"Access Point Details—System" on page 77**
- **"Access Point Details—Access Point Groups" on page 78**
- **"Access Point Details—Radios" on page 79**
- **"Access Point Details—Stations" on page 79**
- **"Access Point Details—SSIDs" on page 80**

- **"Access Point Details—Station Assurance" on page 81**
- **"Access Point Details—Application Control" on page 81**
- **"Access Point Details—IDS" on page 83**
- **"Access Point Details—Rogues" on page 84**
- **"Access Point Details—Events" on page 84**
- **"Access Point Details—Uptime" on page 85**

Access Point Details—General

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

Figure 47. Access Point Details: General

It also offers a number of useful Access Point management functions. For more information on these functions, see **"The Configure Access Points Toolbar" on page 119**. Click the Access Point **WMI** button to open a browser window for the current Access Point's Windows Management Interface.

Access Point Details—Configuration

This page has an extensive menu of options for changing settings on the selected Access Point. It is described in its own chapter. See **" Configuring a Wireless Access Point" on page 411**.

Figure 48. Access Point Details: Configuration

Access Point Details—System

This page shows system information for the Access Point, 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 Access Point shows MAC addresses from 00:0f:7d:30:69:00-30:69:ff, addresses are assigned from this pool, starting at 00:0f:7d:30:69:00. Each radio's SSID will have its own address assigned.

Access Point Details for: Kartik-XR4436 (10.100.85.185)

| General | Configuration | **System** | Access Point Groups | Radios | Stations | SSIDs | Station Assurance | Application Control | IDS | Rogues | Events | U |

Model: XR4436

Software

Component	Version
SCD Firmware	4.03 (May 3 2012), Build: 4503
Boot Loader	7.1.0 (Aug 24 2015), Build: 7049
Radio Driver	3.1.0 (Jul 27 2015), Build: 3958
System Software	7.5.0 (Aug 03 2015), Build: 6033
License Key	17PTM-QXJ15-MY7KA-U0TR8
License Features	AOS 7.6 for 8 3x3 radios + RF Performance Manager + RF Analysis Manager + RF Security Manager + Application Control + Public Safety Band + 802 + 802.11n

Hardware

Component	Part Number	Serial Number	Date
Access Point	XR4436	XR404250F2F25	2014-Feb-07 19:32
Controller	100-0114-001.D2	0000995109	2014-Feb-07 19:29
Radio Module 1	100-0161-001.B1	0510005696	2014-Jul-07 20:06
Radio Module 2	-	-	-
Radio Module 3	100-0161-001.B1	1010004286	2014-Jul-08 3:23
Radio Module 4	-	-	-
Radio Module 5	100-0161-001.B1	1010004186	2014-Jul-07 20:46
Radio Module 6	-	-	-
Radio Module 7	100-0161-001.B1	1010004294	2014-Jul-08 3:57
Radio Module 8	-	-	-

FPGA

FPGA Status	Boot Version	SW Version
Switching Engine	3000-00.022	3000-00.022

Network Interfaces

Interface	MAC Address(es)
Gigabit 1	00:0f:7d:0f:2f:25
Gigabit 2	00:0f:7d:0f:2f:26

Figure 49. Access Point Details: System

If you have expanded the capacity of an Access Point by adding modular 802.11ac APs to it (XI-867/1300), the Hardware section will show both new and old APs currently installed. The model is determined by the number and types of APs

present. For example, if you add four 1300 Mbps (3X3 MIMO) IAPs to an XR-4420, the AP will display its model number as XR-4836 because it now has eight 3x3 IAPs including 802.11ac radios.

Access Point Details—Access Point Groups

This page lists the groups to which the Access Point belongs, if any. An Access Point may belong to multiple groups. To add this Access Point 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 **"Access Point Groups" on page 126**.

You may also remove this Access Point from membership in one or more groups. Select the groups from which the Access Point should be removed by clicking their checkboxes in the first column in the list. Then click **Remove from Group(s)**.
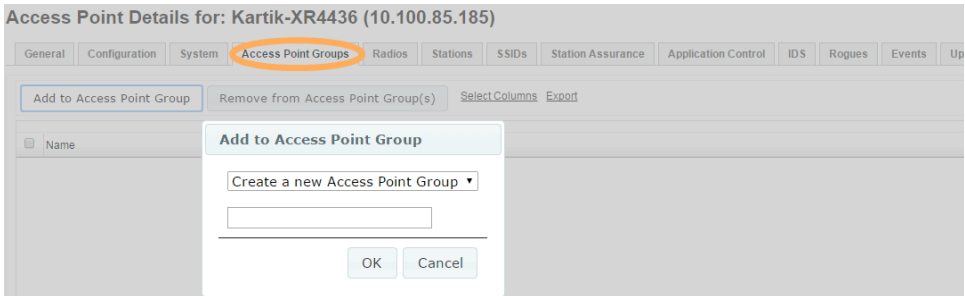
Figure 50. Access Point Details: Groups

Access Point Details—Radios

This page shows radio information for the Access Point, 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 88**). For more information, see **"Radios" on page 87** and **"Radio Settings" on page 533**.

Figure 51. Access Point Details: Radios

Access Point Details—Stations

This page lists stations associated to the Access Point, 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 92**. Many other columns may be chosen using **"Select Columns" on page 67**.

Figure 52. Access Point Details: Stations

Access Point Details—SSIDs

This page shows SSID information for the Access Point, 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 Access Point. **Internal Splash** or **Internal Login** portals are shown as the client will see them. For more information, see **"SSID" on page 89**. See **"SSID Management—Captive Portal" on page 502** to create a captive portal on an Access Point's SSID.
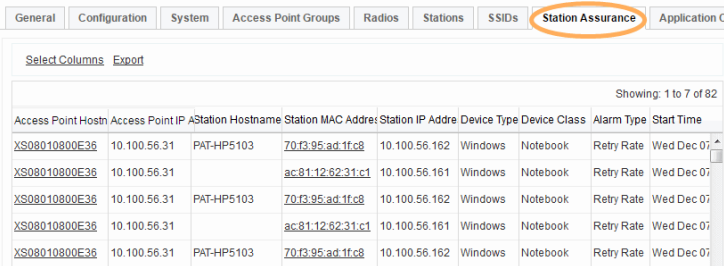
Figure 53. Access Point Details: SSIDs

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.

Access Point Details—Station Assurance

This page shows station assurance events for this Access Point, 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 Access Point, please see **"Station Assurance" on page 103**

Figure 54. Access Point Details: Station Assurance

Access Point Details—Application Control

✎   *This feature is only available if the Access Point license includes Application Control. See* **"About Licensing and Upgrades" on page 200**.

For an Access Point to produce Application Control data, you must enable the **Application Control** *option in the* **Configure** *menu on the Access Points Toolbar. See* **"The Access Points Toolbar" on page 73**.

Application control data (**Figure 55**) provides detailed information about how your wireless bandwidth is being used on an Access Point, 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**).
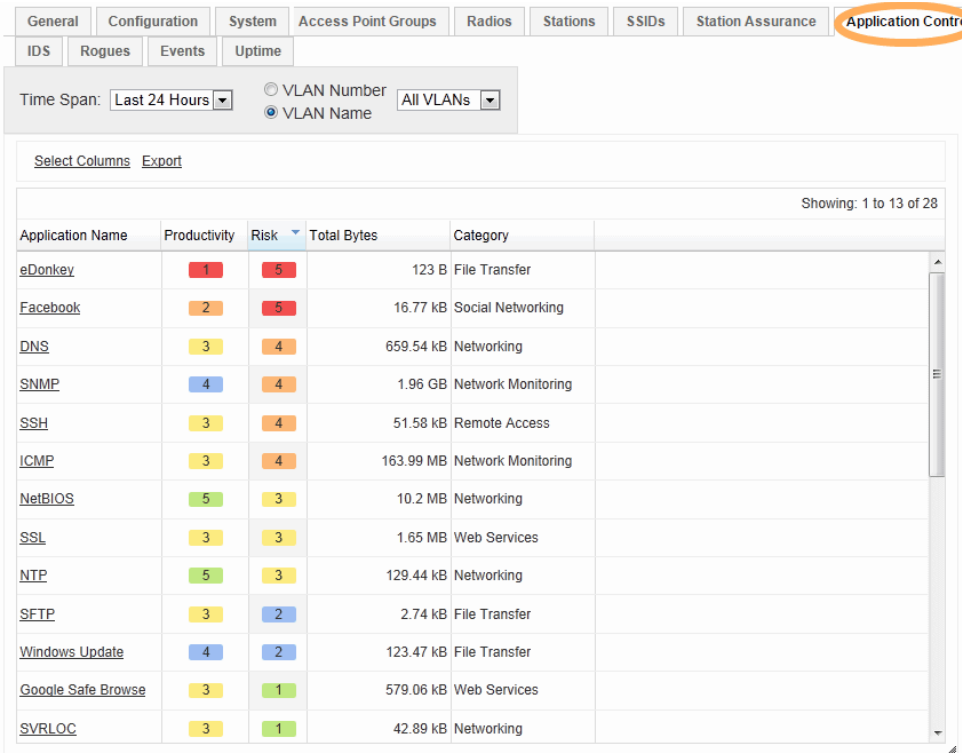
Figure 55. Access Point Details: Application Control

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., WebEx). Please see **"Application Control—Overview" on page 112** for more details.
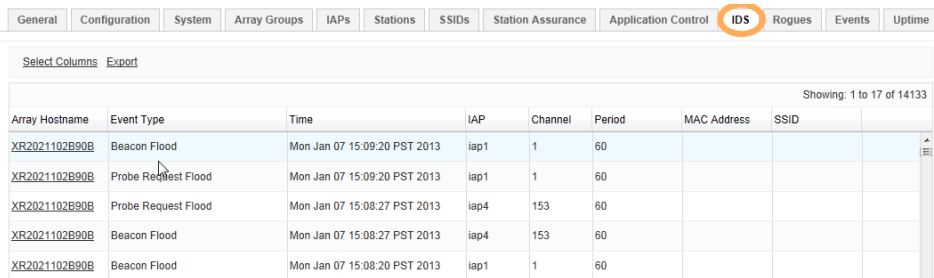
You may click the heading of any column to sort based on that column. Click again to sort in the reverse order.

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 Access Point**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 583**.

Access Point Details—IDS

This page shows Intrusion Detection System (IDS) events for this Access Point, listing any detected attacks.

Array Hostname	Event Type	Time	IAP	Channel	Period	MAC Address	SSID
XR2021102B90B	Beacon Flood	Mon Jan 07 15:09:20 PST 2013	iap1	1	60		
XR2021102B90B	Probe Request Flood	Mon Jan 07 15:09:20 PST 2013	iap1	1	60		
XR2021102B90B	Probe Request Flood	Mon Jan 07 15:08:27 PST 2013	iap4	153	60		
XR2021102B90B	Beacon Flood	Mon Jan 07 15:08:27 PST 2013	iap4	153	60		
XR2021102B90B	Beacon Flood	Mon Jan 07 15:08:20 PST 2013	iap1	1	60		

Figure 56. Access Point Details: IDS

Access Point Details—Rogues

This page shows rogue APs that have been detected by this Access Point, including band and channel assignments. For detailed information about a rogue, click its SSID. For more information about rogues, see **"Rogues" on page 97**. To use the Classify or Locate buttons, see **"The Rogues List" on page 98**.

Figure 57. Access Point Details: Rogues

Access Point Details—Events

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

Figure 58. Access Point Details: Events

Access Point Details—Uptime

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

Figure 59. Access Point Details: Uptime

Switches

This page is used to manage the Xirrus 24-port XT-5024 and 48-port XT-5048 PoE+ Gigabit wired access switches, as described in **"Managing Switches" on page 233**. You may click on any switch in the list to view **Switch Details**, including:

- **"Switch—General Information" on page 236**
- **"Switch—Configuration" on page 237**
- **"Switch—PoE Status" on page 249**

To specify which Access Point is being powered by each switch port, see **"Port Mappings by Switch" on page 146**.

Radios

The web client **Radio**s page lists the radios on all of the Access Points being managed by XMS. If you have expanded the capacity of an Access Point by adding modular 802.11ac APs to it (XI-867/1300), then this list shows the types of APs present. This is a display-only page, but values may be exported. To change settings on radios, please see **"Configure Wireless Settings" on page 155**.

The following sections describe the radios page:

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

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 60. Radios Page

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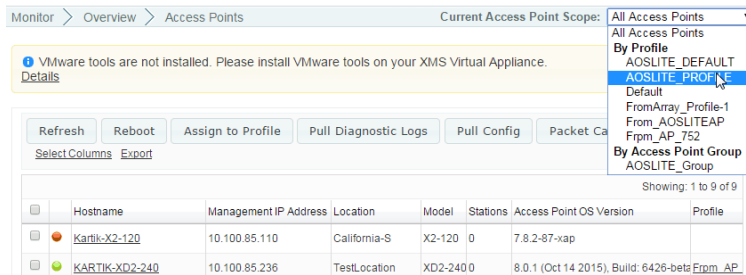
A number of basic operations are available on the radios page to allow you to customize it for your own use:

- **"Current Access Point Scope" on page 67**
- **"Select Columns" on page 67**
- **"Export" on page 68**
- **"Rearranging and Resizing Columns in a Table" on page 69**
- **"Sorting" on page 69**
- **"Searching" on page 70**

The Radios List

The Radios List (**Figure 60 on page 87**) shows all of the radios on Access Points that have been discovered by XMS. Only radios that belong to the **Current Access Point Scope** (selected on the upper right) are displayed.

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

- The Access Point **Hostname**. Click on this link to show the **Access Point 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.

Figure 61. 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 Access Point 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**

Figure 62. 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 67**
- **"Select Columns" on page 67**
- **"Export" on page 68**
- **"Rearranging and Resizing Columns in a Table" on page 69**
- **"Sorting" on page 69**
- **"Searching" on page 70**

The SSID List

The SSID List (**Figure 62 on page 89**) shows all of the SSIDs defined on Access Points in your managed network. Only SSIDs defined on Access Points that belong to the **Current Access Point 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 63 on page 91**)

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

  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 Access Point.

  Click the **SSID Details—Captive Portal** tab to list all of the Access Points 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 Access Points. See **"SSID Management—Captive Portal" on page 502** to create a captive portal on an Access Point's SSID.

- The Access Point **Count** shows the number of Access Points on which this SSID is defined.

- The **Station Count** shows the number of stations associated to this SSID.

SSID: xyzcorp

| Summary | Access Points | Stations | Captive Portal |

Last updated: 10:36:06 AM

Station Count

Station Wireless Throughput

Station Errors (%)
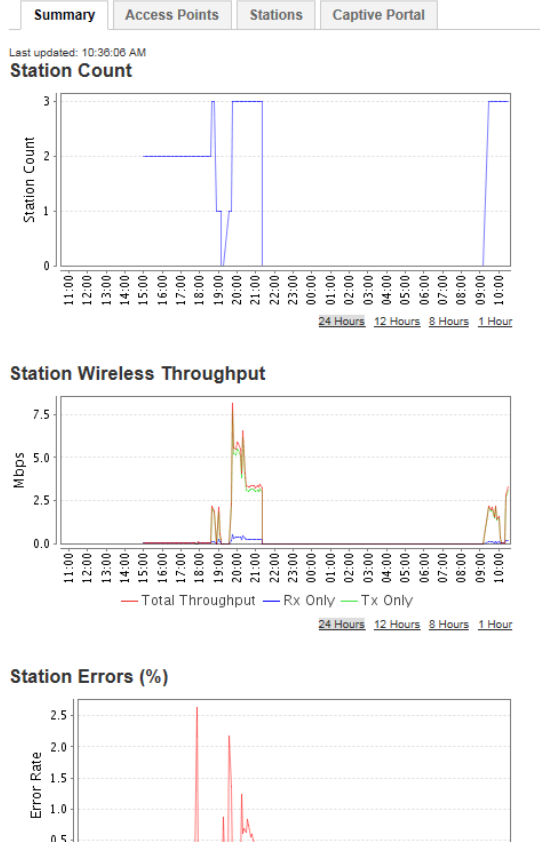
Figure 63. SSID Details—Summary

Stations

The web client Stations page lists the stations that are associated to all Access Points 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**

Figure 64. 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 67**
- **"Select Columns" on page 67**
- **"Export" on page 68**
- **"Rearranging and Resizing Columns in a Table" on page 69**
- **"Sorting" on page 69**
- **"Searching" on page 70**

The Stations List

The Stations List (**Figure 64 on page 92**) shows all of the stations associated to Access Points that have been discovered by XMS. Only Access Points that belong to the **Current Access Point 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 Access Points), 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 Access Points. This will terminate the current connections between each selected station and the Access Point to which it is associated.

- Select one station and click the **Locate** button to have XMS 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 Access Points that have been placed accurately on maps. See **"Adding Access Points to Maps" on page 270**.

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 65 on page 95**)

   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 Access Point 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 103**.

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 112**.

✐ *Application Control data is only available from XR Series Access Point models, and only if the Access Point license includes **Application Control**. See **"About Licensing and Upgrades" on page 200**. In order for an Access Point to produce Application Control data, you must have enabled the **Application Control** option in the **Configure** menu on the Access Points Toolbar. See **"The Access Points Toolbar" on page 73**.*

- 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 Access Point **Hostname** and Access Point **Location** of the Access Point to which the station is associated. Click the hostname to go to **Access Point Details**.
- The **Last Seen Date**—The last time the station was associated to the Access Point.
- 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 Access Point.
- The current **RSSI** (signal strength) of the connection as measured by the radio.

Figure 65. Station Details—General

Legacy APs

The Legacy APs page lists the non-Xirrus access points known to XMS 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 XMS. See **"Discovery" on page 178** for more information. (Note that XMS 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.

Figure 66. Legacy APs Page

You may customize the columns shown in this list—see **"Select Columns" on page 67**.

Rogues

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

*In order for Access Points to detect rogue APs, the Access Points must have one radio set to **monitor** as described in* **"Radio Settings" on page 533***. Intrusion Detection Mode must be set to Standard, as described in* **"Intrusion Detection" on page 569***. You may set a minimum signal strength threshold for considering an AP to be a rogue, in order to keep XMS from detecting too many irrelevant APs—see* **"Security—Rogue Rules" on page 195***.*

If you set blocking on for one of these rogue APs, the Access Point'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 Access Point managed by XMS as soon as possible. Also, XMS sends its latest device classifications to all managed Access Points daily at 3 AM.

Access Points have an Auto Block feature, described in **"About Blocking Rogue APs" on page 572.**

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

XMS adds rogues to this list as described in **"Populating the XMS Rogues and Rogue Rules Windows" on page 198**.

The following sections describe the Rogues page:

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

Figure 67. 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 67**
- **"Select Columns" on page 67**
- **"Export" on page 68**
- **"Rearranging and Resizing Columns in a Table" on page 69**
- **"Sorting" on page 69**
- **"Searching" on page 70**

The Rogues List

The Rogues List (**Figure 67 on page 98**) shows all of the rogues that have been detected by XMS. You may **Classify** entries by selecting them and using the provided button. To search for a particular rogue, see **"Searching" on page 70**. 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 Access Point, and a number of detecting Access Points must be members of the same map. See **"Locating Devices" on page 276** for details.

This list shows information about each rogue and the Access Point 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.
  - **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 Access Point 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.
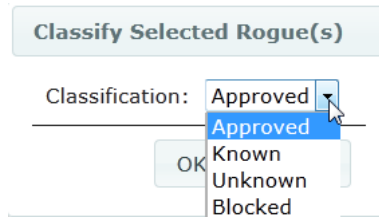
Figure 68. Classifying Rogues
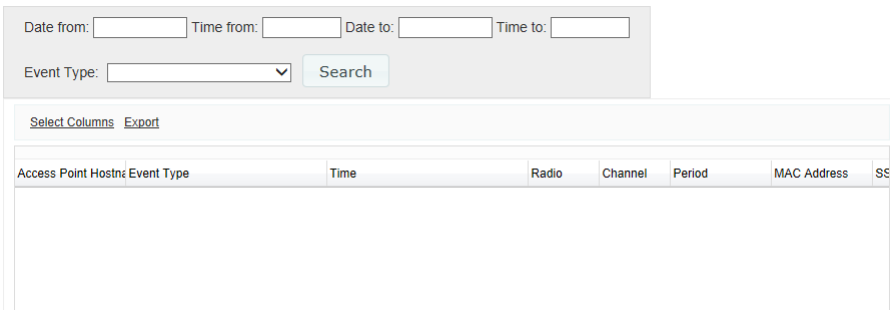
To set up rules to automatically classify groups of rogues (for example, by SSID, MAC address, or manufacturer), see **"Security—Rogue Rules" on page 195**.

- The rogue's **SSID**. Click the SSID to display the **Rogue Details—General** tab, showing additional details about this device. Click the **Detecting Access Points** tab for a list of Access Points 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 Access Point that detected it.

- The MAC Address of the Access Point that detected the rogue.

- The host name of the Access Point that detected the rogue. If the same rogue device is detected by a number of Access Points, 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 Access Point, please see the Access Point *User's Guide*.

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 633**.

Figure 69. 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)—XMS will search for entries of this type.

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

The following fields are displayed on the IDS Events page by default:
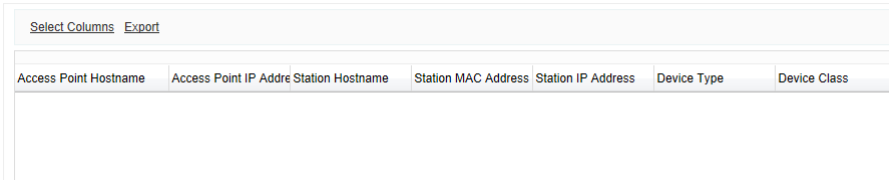
- **Access Point Hostname** of the Access Point on which the event occurred.
- **Event Type**—the type of attack, as described in **"Intrusion Detection" on page 569**.
- **Time**—the time that the event occurred.
- **Radio**—the affected radio.
- **Channel**—the affected channel.
- **Period**—the length 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 Access Point. When the Access Point 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 Access Point, click its **Hostname** and select the tab for the **Access Point 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 633**.

Figure 70. Station Assurance History

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

- The Access Point **Hostname** of the Access Point to which the station is associated.
- The Access Point **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 Access Point).
- 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 XMS for your **Current Access Point Scope**. All alarm levels are displayed—Critical, Major, Minor, Warning, and Clear. Values may be exported.

XMS allows you to define your own custom alarms. See **"Alarm Definitions" on page 172**. You may also send email notifications when alarms of a particular severity occur, as described in **"Notification Settings" on page 175**.

Figure 71. Alarms Page

The following sections describe the Alarms page:

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

For information on alarms due to file system space running low, see **"About Disk Usage Alarms" on page 601**.

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 67**
- **"Select Columns" on page 67**
- **"Export" on page 68**
- **"Rearranging and Resizing Columns in a Table" on page 69**
- **"Sorting" on page 69**

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)—XMS 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 71**) shows the alarms that have been received by XMS. Only alarms on Access Points that belong to the **Current Access Point 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 Access Point 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 Access Point that generated the alarm.

- The **Hostname** of the Access Point that generated the alarm.

- The **Source MAC** address of the Access Point that generated the alarm.

- A text **Description** of the alarm.

Events

The web client Events page lists the log and syslog messages received by XMS 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 Access Points to send syslog messages to XMS, refer to **"System Log" on page 443**.

XMS reconciles syslog activity on all wireless Access Points in the network. Syslog reporting is time-stamped, and to ensure that all syslog time-stamping is maintained by a universal clock for all Access Points, an NTP (Network Time Protocol) server should be used for the XMS server and for all managed Access Points. Without an NTP server assigned (no universal clock), each Access Point 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 438**.

Figure 72. Events Page

Only events on Access Points that belong to the **Current Access Point 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 Access Point, click its **Hostname** and select the tab for the **Access Point 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 109**.

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 67**
- **"Select Columns" on page 67**
- **"Export" on page 68**
- **"Rearranging and Resizing Columns in a Table" on page 69**
- **"Sorting" on page 69**

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)—XMS 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 XMS log files including syslog messages.

The Events List

The Events List (**Figure 71**) shows the events that have been received by XMS. Only events on Access Points that belong to the **Current Access Point Scope** are displayed. Events that trigger alarms are also shown in the **Alarms** window. This list shows information about each event and the Access Point 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 Access Point **IP Address** of the Access Point that generated the event.
- The **MAC Address** of the Access Point that generated the event.
- The Access Point **Hostname** of the Access Point that generated the event.
- The **Message**—a text description of the event.

PoGE

This page lists the Power over Gigabit Ethernet (PoGE) injectors in your Xirrus network. Only the PoGE models that have remote management capability are listed. Address and firmware information is shown. If you wish to view or manage associations between injector ports and Access Points, please see **"Discovery" on page 178**.

> **"Discovery" on page 178** *is used to associate Access Point ports with injector ports so that the XMS database reflects the physical connections powering Access Points in your network. You must specify these connections explicitly in XMS—they are not discovered automatically.*

Figure 73. Power over Gigabit Ethernet Page

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

- A green or red dot showing the current status of the injector.
- The **Injector Hostname**.
- The **IP Address** of the injector.
- The **MAC Address** of the injector.
- The **Firmware version** that is running on the injector.

Application Control—Overview

This page analyzes application usage over your entire Xirrus wireless network, or for your **Current Access Point Scope**. If you wish to see information for just one particular Access Point, please see **"Access Point Details—Application Control" on page 81**.

About Application Control

Access Points 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 Xirrus Access Points 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 see the Access Point *User's Guide*.

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 Access Points whose licenses include* ***Application Control***. *See* **"About Licensing and Upgrades" on page 200**.

In order for an Access Point to produce Application Control data, you must enable the ***Application Control*** *option in the* ***Configure*** *menu on the Access Points Toolbar. See* **"The Access Points Toolbar" on page 73**.

The Application Control—Overview Page
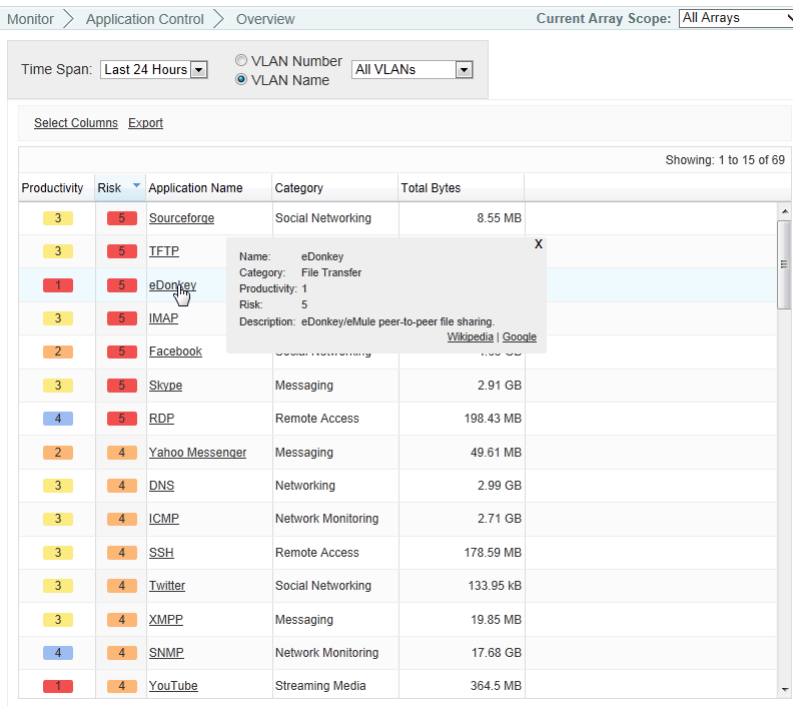
Figure 74. Application Control—Overview

This table provides detailed information about how your wireless bandwidth is being used on the selected Access Point 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., WebEx).

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 Access Point**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 93**.

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 583**.

Configuring the Network

About the Configure Pages

Note that smaller APs that use the AOSLite system software, such as the XR-320, 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 XMS 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**
- **Access Point Groups**
- **Edit Config Templates**
- **Load Config Template**
- **Deploy Config Template**
- **Custom Field Values**
- **Import Access Point Custom Fields**

Switch Configuration

- **Switches**

Power

- **Port Mappings by Injectors**
- **Port Mappings by Access Points**
- **Port Mappings by Switch**

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 Access Points Toolbar**
- **Profiles**
- **Access Point 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 Access Points in the XMS database and offers a number of operations on the selected Access Points. To display this page, click the Access Points link in the Access Point **Configuration** section under **Configure** at the top of the page. This page is identical to the Monitor—Access Points page (see **"Access Points" on page 66**).

The Access Points List shows Access Points that have been discovered by XMS. When you click on an Access Point's **Hostname**, you can access a variety of Access Point Details pages. These pages offer some very powerful features, including the **Configuration** page, which allows you configure most settings on that Access Point. See **"Access Point Details" on page 73** and **" Configuring a Wireless Access Point" on page 411** for more information.

The Configure Access Points Toolbar

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

Figure 75. The Configure Access Points Toolbar

> ✎ *Note that smaller APs that use the AOSLite system software, such as the XR-320, 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 Access Points in the list by clicking their checkboxes in the first column. You may click the checkbox in the header row to select all Access Points, or click again to deselect all. The following operations are available:

- **Refresh**—this option refreshes discovery on the selected Access Points.

- **Reboot**—this option reboots the selected Access Points. You will be asked to confirm the operation.

- **Assign to Profile**—this option assigns the selected Access Points to the profile that you specify. Since an Access Point may not be a member of more than one profile, the selected Access Points will be removed from any other profiles to which they belong. Access Points 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 Access Points 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 76**)

Pulling diagnostic logs from 8 array(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 76. Pull Diagnostic Logs

- **Pull Config**—this option pulls configuration files from the selected Access Points, containing each Access Point'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 Access Points. See **"About Packet Capture" on page 124**.

- **Configure**—select an option from this drop-down list to perform configuration on the selected Access Points. The following options are available:

  - **Network Settings** on the selected Access Points. See **"Import Wireless Settings" on page 158**.

  - **Radio Settings** on the selected Access Points. See **"Configure Wireless Settings" on page 155**.

  - **Optimize Channels**—this option starts auto channel, which computes the best channel assignments for the selected Access Points 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 Access Points Within Maps" on page 281**. See also, **"RF Spectrum Management (Auto Channel Configuration)" on page 566**.

✎ *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 Access Point 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 Power (Cell Size)**—this 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 Access Points, 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 Access Points 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 Access Points 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 77 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.
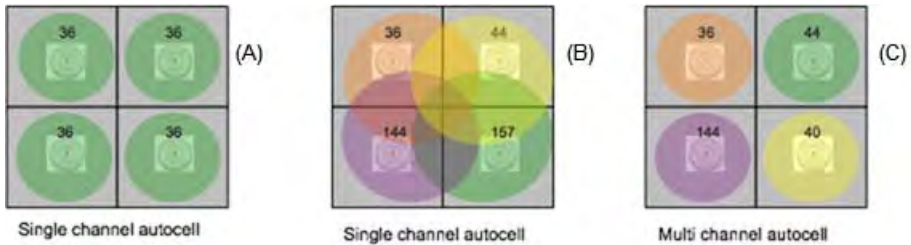
Figure 77. Autocell—Single Channel vs. Multi Channel

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 552** or **"Global Settings .11bg" on page 555**.

- **Enable Application Control**—this option enables deep packet inspection for traffic on the selected Access Points. See **"Application Control—Overview" on page 112**.

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

- **Quick Config**—select an option from this drop-down list to apply a predefined configuration that uses best practices on the selected Access Points. 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.

- **Power**—select an option from this drop-down list to control power on the selected APs. Actually, these commands are implemented by controlling the Power over Gigabit Ethernet (PoGE) injector that powers each target AP. These functions may only be applied to APs that are powered by managed PoGE injectors, and that already have mappings configured as described in "Port Mappings by Injectors" on page 139. You may choose to **Power On** or **Power Off** the selected APs. The **Power Cycle** option will turn power off and back on again, thus rebooting the AP.

- **More**
  - Choose the **Add to Access Point Group** option to add the selected Access Points to a group. (**Figure 78**) A dialog box allows you to select an existing group or **Create a new group**.
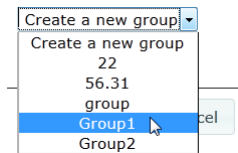
Figure 78. Adding Access Points to a Group

  - Choose the **Create Profile** option from the **More** drop-down list to create a new profile network containing the selected Access Points. See **"Managing by Profiles" on page 211**.

  - **Access Point WMI** connects to the Windows Management Interface for the selected Access Point (only one Access Point may be selected when using this command). After logging in to the Access Point, if you make any configuration changes, they apply only to that Access Point. They will not be propagated to other Access Points being managed by XMS. Note that you may also use XMS to configure an individual Access Point. See **" Configuring a Wireless Access Point" on page 411**.

  - Choose the **Delete** option from the **More** drop-down list to delete the selected Access Points from the XMS database.

- Choose the **Take AP(s) Out of Service** option from the **More** drop-down list to mark the selected Access Points 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 XMS 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 XMS 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 Access Points. See **"Create Custom Actions" on page 620** for more information.

About Packet Capture

Capture is performed on the selected Access Points according to your specified filter settings. (**Figure 79**) The capture includes 802.11 header information (for Access Points running AOS version 5.1 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 Access Point 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.

Figure 79. Packet Capture Dialog

Figure 80. Packet Capture in Progress

Profiles

Please see **"Managing by Profiles" on page 211**.

Access Point Groups

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

The Access Point Groups page lists all of the Access Point groups that have been defined in XMS. It allows you to **Add**, **Edit**, or **Delete** groups. To display this page, click the **Access Point Groups** link in the **Access Point 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 Access Points Toolbar**. Similarly, you may use the same link on the **Access Points (Configure)** to add an Access Point to a group.

Figure 81. Access Point Group Page

To modify an existing group, click **Edit**. The web client displays a list of all Access Points, with check marks in front of those that belong to the group. (**Figure 82**) You may check additional Access Points 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 Access Points. Check the Access Points that you wish to add to the group. Click **OK** when done.

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

Figure 82. Add or Edit Group

Config Templates

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

- **"About Config Template Files" on page 127**
- **"Edit Config Templates" on page 128**
- **"Load Config Template" on page 131**
- **"Deploy Config Template" on page 133**

About Config Template Files

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

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

The file may be copied from the existing configuration of an Access Point that you select as a model, or may be entirely typed in. For example, if Xirrus 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 Access Point, you may edit the file to contain only the settings that you wish to copy to other Access Points. The file makes incremental changes to the settings on an Access Point 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 Access Points before those features have been incorporated in XMS.

Edit Config Templates

> *This feature is intended for **advanced users** who are familiar with use of the Xirrus Wireless Access Point 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 Access Point. 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 Access Point **Configuration** section.

Figure 83. 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 84**)

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 XMS)
- 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
```

Save

Figure 84. Config Template Editor

Click **Save** when done. The editor closes, and your new file appears in the list of config templates. (**Figure 83**) 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 Access Point 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 128**!

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

Figure 85. Load from Access Point

1. **Step 1 - Select Access Points:** The web client displays a list of the Access Points in the XMS database (for your **Current Access Point Scope**). Select the checkbox to the left of the "model" Access Point in the list, then click **Next**. The web client displays a **Loading** message while the download proceeds.

2. **Step 2 - Config File Options:** (**Figure 86**) 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.

Figure 86. Load from Access Point - 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 128**. 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 Access Point from which it was downloaded.

When you download a config template from an Access Point, the file represents the entire configuration of the Access Point, except that XMS 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 Access Point, all of these settings will be applied to an Access Point 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 AOS primary and backup software images will be commented out as well in order to prevent these device-specific settings from being applied to multiple Access Points.

- The entire VLAN section, VTUN section, and the IP address are commented out. Since these settings can vary from one Access Point to another, it would be easy to create problems if they were copied to other Access Points.

Deploy Config Template

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

Figure 87. 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 Access Point **Configuration** section. The web client displays a list of the available config templates. (**Figure 87**)

Select the checkbox to the left of the desired config template, then click **Next**. The web client displays a list of the Access Points in the XMS database (for your **Current Access Point Scope**). (**Figure 88**)

Figure 88. Select Access Points for Deployment

Select the checkbox of one or more Access Points in the list to which the config template is to be deployed, then click **Next**. The web client displays deployment options. (**Figure 89**)

Figure 89. Select Deployment Options

Select the checkbox to **Permanently save this configuration on the Access Point**. If you do not check this box, the commands in the config template will be deployed on the selected Access Points, but they will not be saved. Thus, they will not be reapplied if you reboot the Access Point. Click **Deploy** to apply the config template to the selected Access Points. The web client displays deployment results. (**Figure 90**)

Figure 90. Deployment Results

The **Message** list indicates when the deployment is in progress for each of the selected Access Points, 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 619**) with data values. The page includes a **Bulk Edit** option that allows you to enter identical data for multiple Access Points 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 Access Points from a file, see **"Import Access Point Custom Fields" on page 138**.

Open this page by clicking the **Configure** link near the top of the window, then select **Custom Field Values** from the Access Point **Configuration** section. You may filter the Access Points displayed using **Current Access Point Scope**.
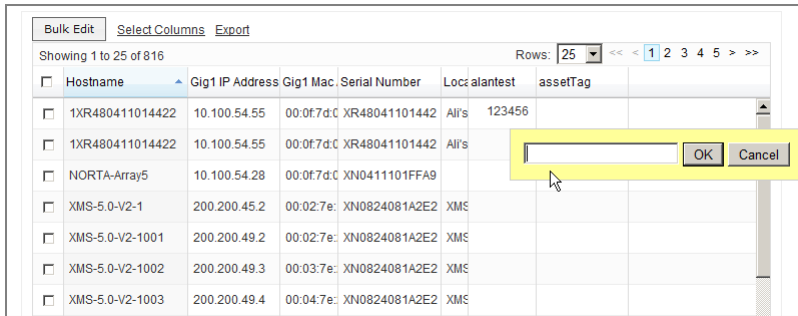
Figure 91. Custom Field Values—Adding a single value

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 Access Points 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 67** if you need more details. Note that you can also change the new column's position by simply dragging its column header in the Access Point list (see **"Rearranging and Resizing Columns in a Table" on page 69**).

To enter a value for an individual Access Point, simply click a cell in the custom column. (**Figure 91**) 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 Access Points 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 92**)
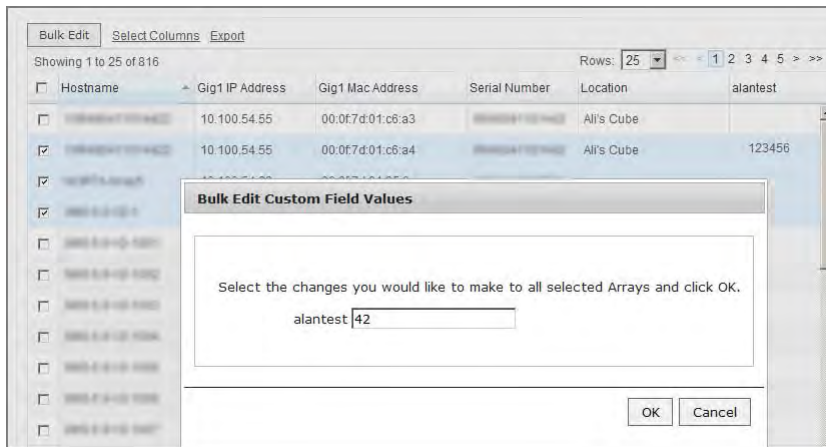
Figure 92. Bulk Configuration (Custom Field Values)

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

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 212**.

- **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 Access Points manually, see **"Custom Field Values" on page 135**.

Format of the CSV File

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

4. The second field in a row specifies the profile to which this Access Point 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 Access Point 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 Access Point 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 Access Points 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 Access Points manually, either by using the **Sync Access Points** 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 Access Point, then the later entries will override the previous ones.

Power

This section includes the following pages:

- **Port Mappings by Injectors**
- **Port Mappings by Access Points**
- **Port Mappings by Switch**

Port Mappings by Injectors

This page shows the Power over Gigabit Ethernet (PoGE) injectors in your network. (Only the PoGE models that have remote management capability are listed.) Tools are provided for associating each PoGE injector port with the Access Point port to which it is physically connected. You may then use XMS to monitor the status of injectors and to power down or power-cycle Access Points by controlling the injector ports that drive them. (See **"SNMPv2 Settings" on page 187**.)

This page shows all injector ports and indicates if ports are free or shows the Access Point ports to which they are connected.

The PoE page is used to associate Access Point ports with injector ports so that the XMS database reflects the physical connections powering Access Points in your network. You must specify these connections explicitly in XMS—they are not discovered automatically.

Figure 93. PoGE Port Mappings by Injector

Managing PoGE injectors with XMS

The following steps are required.

1. You **must** set up each injector that will be managed by XMS. The injector must meet these criteria:

    •   Must be manageable—must be one of the Xirrus managed PoGE injector models. The injectors use SNMPv2.

    •   Must have a static IP address—may be assigned a static address via DHCP or manually.

    •   Must be powered on to allow XMS to discover it.

    •   All injector configuration may be performed using the injector's Windows Management Interface (WMI), as described in the *Power over Gigabit Ethernet Installation and User Guide* (PN 812-0057-001, Rev J or higher).

    •   SNMP Community Names must match those expected by XMS for discovery (see **"SNMPv2 Settings" on page 187**). Change these strings from their factory default values to enhance security.

    •   (Recommended) The injector's user name and password should be changed from their factory default values to enhance security.

    Now you may perform the following steps to start managing the injector with XMS. Each step is described in its own section below.

2. **Add the Injector to XMS**—the XMS Discovery process adds the injector to XMS's managed devices database.

3. **Associate the Injector with an Access Point**—tell XMS which Access Point port is connected to each injector output port.

4. **Manage the Injector with XMS**—turn the injector on or off to save power at night or reboot the Access Point. See the **Power** menu options of **"The Configure Access Points Toolbar" on page 119**.

Add the Injector to XMS

XMS Discovery can find powered-up Xirrus injectors that are SNMP-capable and are reachable from the networks specified for discovery. The SNMP Community
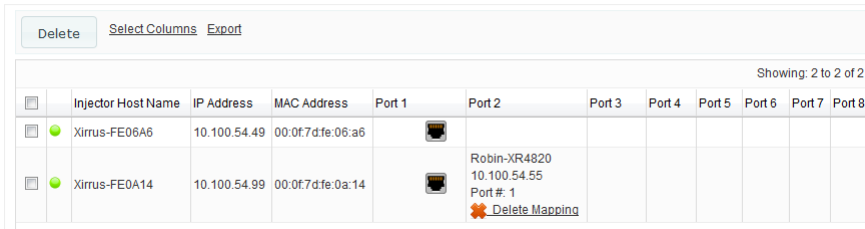
Name of an injector must match one of those listed for SNMPv2. See **"SNMPv2 Settings" on page 187**.

When the injector has been discovered, it will appear in the list of PoGE devices on the Port Mappings by Injector page (**Figure 93**), and you may proceed to the next section. If the injector has not yet been discovered, you may enter it manually as described in **"Add Devices" on page 183**.

Associate the Injector with an Access Point

Once XMS has discovered the injector, you must tell XMS which Access Point(s) are connected to it. Both the injector and the Access Point(s) must already be discovered before you may proceed.

1. From the web client click **Configure**, then click **Port Mappings by Injectors**. The Port Mappings by Injector page appears.

Figure 94. Injector and Access Point Associations

2. Find the row for the desired injector. The row shows the number of ports on the injector. Note that the icons ▣ indicate ports that are available for connection—injector ports that are not yet associated with an Access Point port. If a port already has an association, then the connected Access Point port is displayed. You may hover the mouse over the port to display the IP and MAC address of the Access Point being powered by the injector.

    Click ▣ the port to be associated with an Access Point. The mapping dialog appears, showing Access Point ports that are not mapped to an injector port.

Figure 95. Associating Injector and Access Point Ports

The mapping dialog lists Access Points, and shows an icon 🖳 for ports that have not yet been associated with an injector port. Some older Access Point models are not directly compatible with Xirrus managed PoGE injector models. Since power for these Access Points cannot be managed with XMS, no port icons are shown for them.

3. Find the row for the desired Access Point. Click the "unused port" icon 🖳 for the Access Point port that is physically powered by the selected injector port. The PoGE Injector and Access Point Port Mapping window (**Figure 94**) shows the new connection.

4. To delete a connection from XMS, click the **Delete Mapping** link for that port. To view the associations by Access Point in the web client, click the **Configure** > **Port Mappings by Access Points** link.

Manage the Injector with XMS

Once a Xirrus PoGE injector output port has been mapped to an Access Point port, you may turn the PoGE port on and off, and view its status. This is done via the **Power** menu options of **"The Configure Access Points Toolbar" on page 119**.

Port Mappings by Access Points

This page lists Access Points for your **Current Access Point Scope**, showing the power-capable Gigabit ports for each. Each port shows the injector port to which it is mapped, if any. (Only the PoGE models that have remote management capability are listed on this page.) Tools are provided for associating each Access Point port with the injector port which powers it. You may then use XMS to monitor the status of injectors and to power down or power-cycle Access Points by controlling the injector ports that drive them. (See **"The Access Points Toolbar" on page 73**.)

The PoE page is used to associate Access Point ports with injector ports so that the XMS database reflects the physical connections powering Access Points in your network. You must specify these connections explicitly in XMS—they are not discovered automatically.

Figure 96. PoGE Port Mappings by Access Point

The procedure for mapping the connection between an Access Point port and a PoGE injector port using this page is almost identical to the procedure described in **"Managing PoGE injectors with XMS" on page 142**. In the section titled, **"Associate the Injector with an Access Point" on page 143**, simply use the **Port Mappings by Access Point** page instead. (**Figure 96**)

Select the desired Access Point port on this page, and click on the port icon. A list of PoGE injectors is displayed. Select the injector port that is physically connected to this Access Point port.

Port Mappings by Switch

This read-only page lists all of the switch ports that are powering Xirrus Access Points, for all of the switches being managed by XMS. Each switch port that has a Xirrus device drawing power from it is listed, and shows the Access Point port to which it is connected. XMS gathers this information automatically—you do not need to (and cannot) manually map switch ports to Access Point ports. When a switch port begins supplying power to the PoE port of a Xirrus Access Point, the switch determines the MAC address and IP address of the connected device.

You may use other XMS pages to configure/monitor switches (see **"Managing Switches" on page 233**), and to view power consumption and to power-cycle ports in order to reboot Access Points (see **"Switch—PoE Status" on page 249**).

Configure > Power > Port Mappings by Switch							
Select Columns Export							
Switch Name	Switch IP Address	Switch MAC Address	Switch Port	Access Point Host Name	Access Point IP Address	Access Point MAC Addre	Access Point P
XT-5024-R1S1	10.110.37.191	50:60:28:00:c5:e3	8	sqa-XR2435-00CAD	10.110.37.35	00:0f:7d:20:0c:ad	Gig1/2
XT-5024-R1S1	10.110.37.190	50:60:28:00:c5:58	3	sqa-XR520-000E0	10.110.37.23	50:60:28:00:00:e0	Gig1
XT-5048-R1S2	10.110.37.192	50:60:28:00:cc:f1	11	sqa-XR630-0254D0	10.110.37.37	50:60:28:02:54:d0	Gig1/2
XT-5024-R1S1	10.110.37.191	50:60:28:00:c5:e3	2	XR073390254D0CAD	10.110.37.37	50:60:28:02:54:d0	Gig1/2
XT-5024-R1S1	10.110.37.191	50:60:28:00:c5:e3	1	sqa-XR24x5-0EEC83	10.110.37.33	00:0f:7d:0e:ec:83	Gig1/2

Figure 97. PoGE Port Mappings by Access Point

To change settings on switches, please see **"Managing Switches" on page 233**.

For each connected switch port, the following information is shown by default:

- The **Switch Name**
- The **Switch IP Address**
- The **Switch MAC Address**
- The **Switch Port**—the number of a port on the switch
- The Access Point **Host Name**
- The Access Point **IP Address**

- The Access Point **MAC Address**
- The Access Point **Port**—the name of the Access Point port that is connected to this switch port

If a Xirrus wireless device is unplugged from a switch port, its entry in this table is not removed. The entry will persist until that same Access Point port is connected to another switch port that is managed by XMS. In this case the table is properly updated, and will reflect only the new connection.

Access Point Upgrade

The Access Point Upgrade pages allow you to specify a software upgrade to apply to selected Access Points 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 148**
- **"Scheduled Upgrades" on page 154**

Perform or Schedule Upgrade

This page allows you to upgrade one or more Access Points to a new software release. To display this page, click the **Perform or Schedule Upgrade** link in the Access Point **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 Access Point to add new features that are not supported by your existing license, the Access Point must have the new license key that includes the upgraded features before upgrading. Similarly, if you are upgrading an Access Point for a new software release, the Access Point must have the new license key that enables the operation of that release before upgrading.

Access Points have a license Auto-provisioning and activation capability. An Access Point can contact the Mobilize server at Xirrus with its serial number and MAC address to obtain and install its latest license. License updates are performed **automatically** as part of the XMS upgrade process. For each selected Access Point, XMS will check if the requested upgrade requires a new license. If so, it will send a command to the Access Point to activate the license update process, and then wait to allow the license update to proceed. Note that this license activation process is supported on Access Points running AOS version 6.4 and above, and XMS will not attempt to activate a license auto-update for Access Points running earlier software. For Access Points running older software and needing a license update (or if the Access Points do not have access to the Xirrus Mobilize server), you will need to explicitly update their licenses with XMS as described in **"About Licensing and Upgrades" on page 200**. If an Access Point is

not able to contact the Xirrus Mobilize server, note that the upgrade will proceed anyway.

Major *and* minor releases will need a new license key, but patch releases will not. For example, to upgrade from AOS Release 8.0.5 to Release 8.1 requires a new license. To upgrade from AOS Release 8.0.1 to Release 8.0.2, use the existing license.

Figure 98. Access Point Upgrade

1. **Step 1 - Select Access Points:** Select all of the Access Points that are to be updated with the new software image. (**Figure 98**) Check that they all have licenses installed that will support the new release (see **"Deployed Licenses" on page 202**). Note that only Access Points in the selected **Current Access Point Scope** are listed. Click **Next**.

2. **Step 2 - Select Upgrade Source:** (**Figure 99**)

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

    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.

Figure 99. 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. Access Points must be running AOS version 7.0 or higher to support upgrade via HTTP.

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

3. **Step 3 - Select Software Versions:** (**Figure 100**)

   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 XMS, 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.

| 1 Select AP | 2 Select Upgrade Source | **3 Select Software Versions** | 4 Upgrade Summary | 5 Perform Up |

[< Previous] [Next >] [Cancel]

Select Software Versions

System Software	XS-6.4.1-3854.bin [▼] [...]
Reboot	☑
Use Custom Login	☐
User Name	[ ]
Password	[ ]
Confirm Password	[ ]
Enable Schedule	☑
Date Scheduled	05/12/2013
Time Scheduled	01:30

Hide Advanced

Allow non-standard ArrayOS file names	☐
Remove all unused images from Array	☑
SCD Firmware	[ ] [▼] [...]
Boot Loader	[ ] [▼] [...]

Figure 100. Select Software Versions

b.   Reboot: Check this if you want the Access Points to be rebooted when the upgrade is complete. This will cause the selected Access Points to run the new image. If this is left unchecked, then the new images will be uploaded to the selected Access Points but they will not be run until the Access Points 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 Access Point and it is running an AOS release greater than 3.5. Check this box and set up the login parameters required for uploading the image to Access Points. These values must match an admin account that is configured on the Access Point, else the upload to the Access Point will fail. By default, the upload uses Secure Channel Protocol (SCP) to authenticate access to each Access Point. The Access Point will accept logins that match any of its Admin accounts with write privileges. These accounts may be entered either directly on the

Access Point or using XMS. Also, this process will use any Access Point Shell Authentication information defined in the discovery dialog (see **"SSH Users" on page 190**). Note that Access Points 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 Xirrus Customer Support personnel, and enter the following fields as needed.

- **Allow non-standard AOS file names:** If Xirrus advises you that your files will have non-standard names, check this box.
- **Remove all unused images from Access Point:** If you wish to clean up old images from the Access Point, 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 Access Point 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 AOS 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 AOS 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 101**) Review these values carefully. Click the **Previous** button if you need to change anything.

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

| < Previous | Upgrade > | Cancel |

The following changes will be made:

Update Source:

    Source   (SCP Server)

Updating to:

    System Software   6.0.6-3132

Reboot if successful

Figure 101. Upgrade Summary
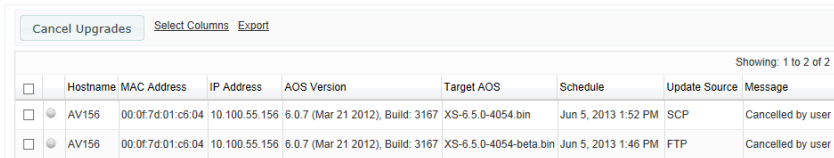
The web client will apply the upgrades you entered, and display the success or failure of the operation on the selected Access Points.

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 Access Point **Upgrade** section under **Configure** at the top of the page.

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

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

		Hostname	MAC Address	IP Address	AOS Version	Target AOS	Schedule	Update Source	Message
☐	○	AV156	00:0f:7d:01:c6:04	10.100.55.156	6.0.7 (Mar 21 2012), Build: 3167	XS-6.5.0-4054.bin	Jun 5, 2013 1:52 PM	SCP	Cancelled by user
☐	○	AV156	00:0f:7d:01:c6:04	10.100.55.156	6.0.7 (Mar 21 2012), Build: 3167	XS-6.5.0-4054-beta.bin	Jun 5, 2013 1:46 PM	FTP	Cancelled by user

Figure 102. Scheduled Upgrades

The following information is show for each Access Point, by default:

- **Hostname, MAC Address, IP Address**—these identify the Access Point to upgrade.

- **AOS Version**—the software version that was running on the Access Point before the upgrade.

- **Target AOS**—the new software version to which the Access Point 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 XR-320.*

The Configure Wireless Settings page provides very convenient options for configuring settings on a per-radio (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 159** page. See **"Individual vs. Bulk Edits" on page 160** 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**.

Figure 103. Configure Wireless Settings Page

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

To Modify Wireless Settings

1. **Select Access Points:** 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 Access Points in the selected **Current Access Point 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 533** 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 104**) 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 Access Points, use the **Bulk Edit** button. See **"To modify multiple rows at once with Bulk Edit" on page 161**.

    Click **Finish** when done. XMS applies the changes to the selected Access Points.

Figure 104. Editing the Radio Settings Page

3. **Apply Settings:** The web client will display the success or failure of the configuration operation for each selected Access Point (status is reported on a per-AP basis, rather than for each radio).

Export Wireless Settings

This option exports channel and other radio settings on selected Access Points 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 Xirrus 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 168** for instructions. To import a file that was exported from the Wireless Settings page, see **"Import Wireless Settings" on page 158**.

Note that Import and Export Wireless Settings are not available for smaller APs that use the AOSLite system software, such as the XR-320.

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 157** 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 170** 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 Access Point 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 Access Points in one step. **"Individual vs. Bulk Edits" on page 160** 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 Access Points in the selected **Current Access Point 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 160**
- **"Individual vs. Bulk Edits" on page 160**
- **"Modify Network Settings (Basic)" on page 163**
- **"Modify Network Settings (Advanced)" on page 164**

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 67**
- **"Select Columns" on page 67**
- **"Rearranging and Resizing Columns in a Table" on page 69**
- **"Sorting" on page 69**

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 Access Points. 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 Access Points. (**Figure 107**)

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 105**) 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.

Figure 105. Editing Individual Rows

To modify multiple rows at once with Bulk Edit

Select the Access Points 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 106** 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 Access Points 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 Access Point **Host Names** cannot be bulk configured. Bulk edit fields that are left blank will be unchanged on Access Points.

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: [   ]

OK   Cancel

Figure 106. 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 Access Points. 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 Access Points:** 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.

Figure 107. 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 108**) 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 Access Points, use the **Bulk Edit** button. See **"To modify multiple rows at once with Bulk Edit" on page 161**.

   Click **Finish** when done. XMS applies the changes to the selected Access Points.

Figure 108. 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 Access Points.

Modify Network Settings (Advanced)

1. **Select Access Points:** Select the **Advanced** option (to the right of the **Next>** button). Select the checkbox to the left of each Access Point 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.

Figure 109. Configure Network Settings Page (Advanced)

2. **Access Point 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 110**) 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 Access Points, use the **Bulk Edit** button. See **"To modify multiple rows at once with Bulk Edit" on page 161**.

Figure 110. Editing the Access Point 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**.

Figure 111. Editing the Access Point 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.

Figure 112. Editing the Access Point 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 421** for an explanation of the **Port Mode** options.

Figure 113. Editing the Access Point Network Settings Page (Bond)

Click **Finish** when done. XMS applies the changes to the selected Access Points.

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

Export Network Settings

This option exports IP and other network settings on selected Access Points 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 Xirrus 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 170**.

1. **Step 1 - Select Access Points:** 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 Access Points in the selected **Current Access Point Scope** are listed.

Figure 114. 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 114**) 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.

Figure 115. 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 Access Points by importing a file that was exported from the Export Network Settings page. See **"Export Network Settings" on page 168** 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 116**) Next, click the **Upload** button.

    Click **Next>** when the **Upload Complete** message appears.
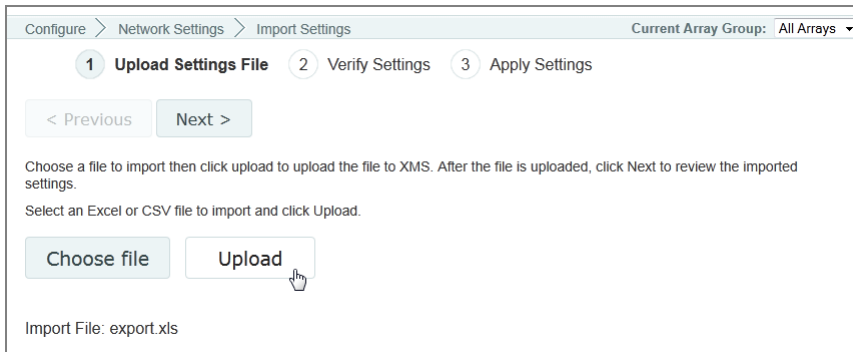
Figure 116. Import Network Settings

2. **Step 2 - Verify Settings:** This page lists network settings for all of the Access Points that were included in the imported file. (**Figure 117**) 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 161**. 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.

Figure 117. 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 Access Points.

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 XMS to monitor a specified operating condition on all Access Points and issue an alarm if your stated criteria are met on any Access Point. 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-Access Point.

Settings for alarm values and thresholds are based on your network and its usage. Values may be set to monitor conditions that are becoming a concern. For example, you may wish to set an alarm if Ethernet errors reach a certain level because you notice that they have been increasing. Or perhaps an AP has been handling a large number of clients and an alarm should be set if a station count reaches a certain number.

Open this configuration page by clicking the **Configure** link near the top of the window, then select **Alarm Definitions** from the **Alarms** section. (**Figure 118**) This page lists all of the alarms that you have created.

Figure 118. 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 119**)

Figure 119. 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 119**, 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 Access Point 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 Access Point recovers into the non-alarm range by the amount set in deadband.

For example, in **Figure 120**, 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 Access Point 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.

Figure 120. 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 633**.)

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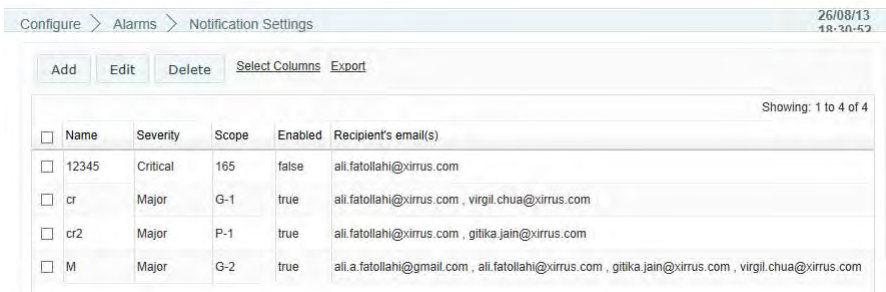
One interesting alarm type may be used to help find iPads and other devices that have gone missing. Under **Alarm Category** select **Station Status**. Then set **Alarm Type** to **Alarm when a particular station is associated to an Access Point**. Enter the **MAC address** of the missing device. XMS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

Notification Settings

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

Notifications may be restricted to apply only to a selected Access Point scope—a set of Access Points belonging to a selected profile or Access Point group. For example, say XMS is managing multiple Access Point networks at sites in different cities, and that you have defined a profile network for each city. When an alarm occurs for an Access Point, you may wish to notify only the IT personnel managing that Access Point'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 121**) This page lists all of the notifications that you have created.

Figure 121. Alarm Notification Settings

Click the **Add** button to display the **Add Notification** dialog and create a new entry. (**Figure 122**) 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 Access Point **Scope** for this notification. Only alarms on Access Points 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* XMS-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 Access Point **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 XMS will use for sending email notifications, along with the email account to use and the name of the sender. See **"Email Settings" on page 632**.

Figure 122. 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 XMS find the Xirrus Access Points, wired switches, and managed Power over Ethernet (PoE) injectors 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, the **Switches** list, or the **Port Mappings by Injectors** list. You can enter SNMP settings, add devices and networks, and enter Access Point SSH user information.

Note that you must configure the SSH Users page for XMS to be able to manage APs, so be sure to go to this page.

For an overview of how discovery adds devices and how SNMP must be configured on Access Points and on XMS 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 183**

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

- **"SNMPv2 Settings" on page 187**

    Adds or deletes SNMPv2 community names.

- **"SNMPv3 Users" on page 189**

    Adds or deletes SNMPv3 users.

- **"SSH Users" on page 190**

    Add user accounts that XMS can use when it must log in to Access Points for some management functions.

- **"View Networks" on page 191**

    Adds a subnetwork for XMS to scan for Xirrus devices.

● **"What If My Device Is Not Discovered?" on page 193**

What to do if XMS has not discovered a device that you expected to find on the **Access Points** list, the **Switches** list, or the **Port Mappings by Injectors** list.

Note that in this chapter, the term *device* refers to a Xirrus Access Point or wired switch, or a Xirrus-supplied managed PoGE injector.

How Discovery Works

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

*XMS requires AP login information to provide it with management access to Access Points. This information **MUST** be set up on the **SSH Users** page.*

*NOTE: To use SNMPv3 successfully, system time must be set using an NTP server on both the XMS server host machine and all Access Points using SNMPv3. This is because SNMPv3 requires synchronization between the XMS server and the Access Points 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 Access Points from the database. This means that the Access Point will appear to be down and statistics will not be polled until the Access Point is re-discovered. A manual refresh of the Access Point should remedy the situation. See **"Add Devices" on page 183**.*

*To allow XMS to find a Xirrus device (Access Point, switch, or PoGE injector), 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 187**. The default SNMPv2 community string in XMS matches the Access Point default value.*

XMS usually adds devices to its database using the **Phone Home** feature that relies on an Access Point sending an SNMP trap to the XMS server's hostname. A **Discovery** tool that uses SNMP is also available.

Phone Home

Any time an Access Point boots up or its IP address changes, it announces its presence on the network. It does this by sending an SNMP trap to the XMS server's default hostname, **xirrus-xms** (this name is not case-sensitive). XMS 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 **xirrus-xms** can be resolved to the IP address of the XMS server. Note that you can configure APs to send traps to different hostnames/IP addresses or to additional hosts, but a reboot is required after this configuration change in order to send a trap to the new target.

As soon as a new device is plugged in, it "adds itself" to XMS 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 load that accompanies the process. Any devices that phone home to XMS are added to the **Access Points** window or the PoE injectors list in **Port Mappings by Injectors** and become part of the XMS **managed network**.

Discovery

XMS's discovery feature uses SNMP to find networks and devices that can be reached from the server's network. Despite the advantages of the Phone Home feature, discovery is still needed when you first start using XMS, and later for finding added Xirrus-supplied managed power injectors and wired switches. Discovery will find your current network of Xirrus 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 **xirrus-xms**.

> *If you do not have a valid license for the XMS server, you are limited to managing one Access Point. Valid XMS licenses are typically for a particular number of Access Point radios. In either case, when XMS has discovered the maximum permitted number of radios, no additional Access Points will be discovered.*

Devices that do not have SNMP enabled will **not** be discovered by XMS and cannot be managed by XMS.

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, the **Switches** list, or the **Port Mappings by Injectors** list can be managed by XMS.

How to Perform Discovery

This section provides a quick summary of the steps required to add devices to XMS via discovery. Note that using the **Phone Home** feature is the preferred way to add APs because it is simpler and more efficient—it should be used in most cases.

Once started, Discovery uses SNMP to automatically find Xirrus Access Points, wired switches, and PoE injectors in the subnets that you specify. (**Figure 123**) No networks are discovered by default, so you must add the subnets containing your Access Points.

1. For proper management of APs after discovery, you must enter their login credentials as described in **"SSH Users" on page 190**.

2. To add **SNMPv2 Community Names** or **SNMPv3 Users** to match the strings being used by your devices, click **SNMPv2 Settings** or **SNMPv3 Users**. For XMS 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 (**xirrus**) allows XMS to discover new Access Points that still have default SNMP settings (SNMPv2 is enabled by default with its **Read Write Community String** set to **xirrus**).

Enter the appropriate SNMP settings. For more details, see **"SNMPv2 Settings" on page 187**.

3. To add networks to be discovered, click the **Add Devices** link under **Discovery**. (**Figure 123**) 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 **Next>** so that the discovery process will be initiated.

Discovery begins soon after adding a network.

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

Figure 123. Discovering Networks

Add Devices

This page is used to add subnetworks or devices to XMS. It allows a great deal of flexibility in adding devices. You may individually add one or more devices to XMS, rather than specifying a network and having XMS 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 Access Points 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**.

Discovery looks for all device types at each address in this order: AOSLite devices, then AOS devices, and then Xirrus wired switches or management-capable PoE power supplies. To speed discovery by reducing the types of devices that you scan for, click the **Advanced options** link. By default, discovery looks for all of the listed device types. Uncheck any device type that you don't need to discover.

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

● **Single Device (Figure 124)**

Enter the **IP Address** of the single device to be added to XMS. Click the **Next** button.

Figure 124. Discover a Single Device

XMS will display the results of discovery for the device. (**Figure 125**)

Figure 125. Discovery Results—Single Device

- **IP Range (Figure 126)**

  Enter the start of the range in the **From IP Address** field. Enter the end of the range in the **To** field. XMS will check every address in the range, up to and including the **To** address. Click the **Next** button. At each address, if it finds a Xirrus Access Point, wired switch, or management-capable PoE power supply, XMS will add the device to its list of discovered devices.

Figure 126. Discover a Range of IP Addresses

XMS will display the results of discovery for the IP range. You may click the **Cancel** button to stop discovery. (**Figure 125**) Canceling will not remove devices that have already been discovered for this range.

- **Multiple Devices (Figure 127)**

  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 **Next** button. XMS will check every address in the list. At each address, if it finds a Xirrus Access Point, wired switch, or management-capable PoE power supply, XMS will add the device to its list of discovered devices.

Figure 127. Discover a List of IP Addresses

XMS displays the results of discovery, listing whether it succeeded or failed at each address. If discovery fails at an address, XMS will still try all the rest of the addresses that you entered. Note that if you enter a device that is already in the XMS database, XMS 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 XMS from finding any additional devices, but will not remove any devices that have just been discovered.

●   **Networks (Figure 128)**

Enter the subnet's **Network Address** and **Subnet Mask**, then click **Add**. Continue adding subnetworks as required. Click **Next** 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.

Figure 128. Discover Networks

After you click the **Next** button, XMS will attempt to discover a Xirrus Access Point 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**.

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

If XMS has not discovered a device that you expected to find on the **Access Points** list, the **Switches** list, or the **Port Mappings by Injectors** page, see **"What If My Device Is Not Discovered?" on page 193**.

To see more discovery results, see **"View Networks" on page 191**.

SNMPv2 Settings

For a device to successfully **Phone Home** *(announce its presence to XMS) 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 XMS discovery process searches networks using both SNMPv2 and SNMPv3. Discovery will search for devices using SNMPv3 first. See **"SNMPv3 Users" on page 189** for more information. When an Access Point is discovered using SNMPv3, then XMS uses that version for communication with the Access Point from then on. When an Access Point or PoE injector is discovered via SNMPv2, then XMS uses SNMPv2 to communicate with the device. Injectors support SNMPv2 only.

XMS discovery has default SNMPv2 entries which match the factory default SNMP v2 settings in Access Points and PoE injectors. However, for proper security on your Xirrus devices, we recommend that you improve security on Xirrus 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 XMS 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 129**)

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

Figure 129. SNMPv2 Settings

The next time that the discovery process runs after adding a new SNMP v2 entry, XMS 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 191**.

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. XMS 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 XMS 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.

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

XMS discovery has default SNMPv2 entries which match the factory default SNMPv2 settings in Access Points and PoE injectors. However, for proper security on your Xirrus devices, we recommend that you improve security on Xirrus 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 XMS for discovery to find those devices.

Figure 130. SNMPv3 Users

*NOTE: Both XMS and Xirrus APs have matching default SNMPv3 usernames and passwords. The default read-write username and password are **xirrus-rw**; the default read-only username and password are **xirrus-ro**.*

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 130**)

Enter the new **User Name,** and **Authentication** and **Privacy Passwords**. Set the **Authentication Type** to match your Access Points. 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, XMS 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 191**.

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. XMS will continue to manage the device using the original user name as long as the device is still configured to use it.
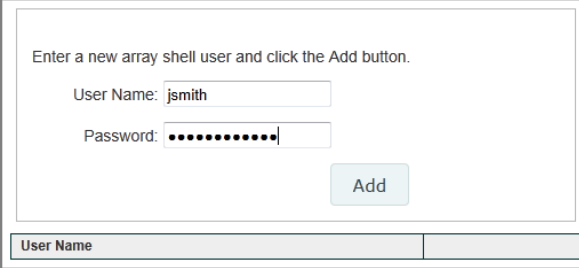
SSH Users

XMS requires AP login information to provide it with management access to Access Points. Depending on the configuration of an AP, authentication may use the AP's local accounts or may use a RADIUS server. In either case, XMS needs to know a **Username** and **Password** to gain access to the Access Point shell.

To define this Access Point 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 131**)

Enter an Access Point's **User Name** and **Password**, and click **Add**. The new entry will appear in the Access Point Shell Authentication list, located under the dialog box. You may use the **Delete** button to remove a selected entry, if necessary.
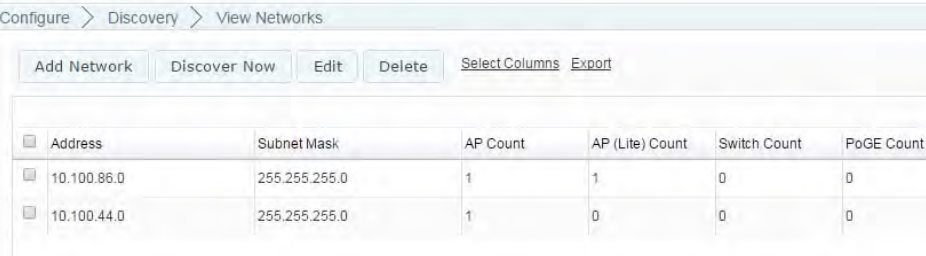
Figure 131. Adding SSH Users

These authentication entries are not used by the discovery process itself, but are managed on this page for convenience. When XMS needs to log in to an Access Point's shell, it tries entries from the list until it finds one that works. Then it will remember to use this login for this Access Point. On future login attempts to the same Access Point, 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 132**)

Figure 132. 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.

- **AP Count**—the number of APs running AOS discovered on this network so far.

- **AP (Lite) Count**—the number of APs running AOSLite discovered on this network so far.

- **Switch Count**—the number of Xirrus switches discovered on this network so far.

- **PoGE Count**—the number of Xirrus-supplied manageable PoE power injectors discovered on this network so far.

- **Legacy AP Count**—the number of non-Xirrus 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.

Note that discovery will not remove devices from the XMS 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 XMS server, you are limited to managing one Access Point. Valid XMS licenses are typically for a particular number of Access Point radios. In either case, when XMS has discovered the maximum permitted number of radios, no additional Access Points will be discovered. See **"Managing the XMS Server License" on page 655**.

XMS Discovery will find devices that are reachable from the XMS server's network if their SNMP settings match those configured on the XMS server. If your Access Point or PoE injector has not been discovered, check the following.

1. Have you discovered the maximum number of Access Points allowed by your XMS license?

2. Have you configured logins for all APs in **SSH Users**?

3. Is the device powered up and fully booted?

4. For an Access Point/wired switch—is SNMP enabled? (SNMPv2 is always enabled on Xirrus managed PoE injector models.)

5. Does the XMS server have connectivity to the device (i.e., is the device connected and can you ping it?).

6. 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 XMS match.

7. 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.

8. To launch discovery immediately on a network, see **"Add Devices" on page 183**.

9. You may add a device explicitly, using its IP address. See **"Discover a Single Device" on page 183**. If the device is detected by XMS 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 97**), based on SSID, BSSID, or manufacturer. You may classify rogues as **Blocked**, so that the Access Point 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 97**. *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 199**, *and* **"Intrusion Detection" on page 569**.

Configure > Security > Rogue Rules

Ignoring Rogue APs with an RSSI less or equal to -80

☑ Ignore Rogue APs with RSSI less than: -80

Submit

| Add | Edit | Delete | Select Columns | Export |

	Name	Type	Data	Classification	Status
☐	Xirrus Arrays	BSSID	00:0f:7d:*	Known	Active
☐	More Xirrus Arrays	BSSID	50:60:28:*	Known	Active

Figure 133. 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 XMS 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 Access Points) 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 Access Points (see **"Populating the XMS Rogues and Rogue Rules Windows" on page 198**). You may edit existing rules, if you wish.

To create a rogue rule, click the **Add** button on the upper left. (**Figure 133**) In the Add Rogue Classification Rule dialog box (**Figure 134**), enter a unique **Rule Name** for your new rule.

Figure 134. 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, **00:0f:7d**, **50:60:28**, and **48:c0:93** are the OUIs of Xirrus, so the strings **00:0f:7d:***, **50:60:28:***, and **48:c0:93**:* will uniquely match all Xirrus Access Points.

  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 Access Points. Note that rules created on newer Access Points have a **Match Only** setting that will specify either a BSSID or an SSID, although these Access Points will still process the old-style rules. On older Access Points, rules with type set to SSID, BSSID/SSID, or BSSID will all be processed on the Access Point as though they were BSSID/SSID rules. Rules with type set to Manufacturer will be dropped on older Access Points. (Manufacturer is supported on AOS 4.0.6 or higher, and on AOS 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 Xirrus Access Points to **Known**. See **"The Rogues List" on page 98** for an explanation of rogue classifications.

Leave the **Enforced** checkbox checked if you wish to have the rule pushed to all managed Access Points, otherwise clear the checkbox.

- **Enforced** rules are pushed (sent) to all managed Access Points to become part of the Access Points' Rogue Control Lists. If the Access Point has a conflicting rule (for the same wildcard pattern, but with a different classification), the XMS rule will replace the Access Point rule.

- **Unenforced** rules are not pushed to managed Access Points. This way, if an Access Point 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 XMS Rogues and Rogue Rules Windows

When the XMS server is first started, the Rogues list is empty (see **"Rogues" on page 97**), and there are only two default rules: all Xirrus Access Points (BSSID 00:0f:7d:*, 48:c0:93:* or 50:60:28:*) are Known. This rule is Enforced—it is sent out to all Access Points.

In order to populate the **Rogues** list, XMS fetches the rogue devices and Rogue Control List entries from each discovered Access Point. Thereafter during operation of XMS, Access Points are polled for new entries. Also during operation, when a new Access Point is discovered, XMS 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 Access Point and added to the XMS database it is marked as **Enforced**, and thus it will be "pushed" to all managed Access Points. On the other hand, when a *rule* is read from an Access Point and added to the XMS database, it is marked as **Unenforced**. This prevents the rule from being sent out to all managed Access Points, possibly overriding existing rules that were explicitly configured in Access Points. Once a rule has been added to the XMS database, if additional rules for the same BSSID/SSID are later read from other Access Points, they are ignored.

If you set a rule to Enforced, it will be sent out to each managed Access Point and become part of its Rogue Control List.

SSID Spoofing Auto Block

XMS 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 Access Points 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 574**. Clearing the checkbox will disable this feature.

Spoofing is detected by Access Points managed by XMS. In order to be able to detect this type of attack, Access Points must have **Intrusion Detection Mode** set to **Standard**, and have detection of **Evil Twin Attacks** enabled. These settings may be made by XMS for individual Access Points or for Profile networks. See **"Intrusion Detection" on page 569** and **"Profile Details—Configuration" on page 223**.

Configure 〉 Security 〉 SSID Spoofing Auto Block

Auto Blocking of rogue APs involved in SSID Spoofing (Evil Twin) Attacks is enabled.

☑ Enable Auto Blocking of SSID Spoofing (Evil Twin) Attack

Submit
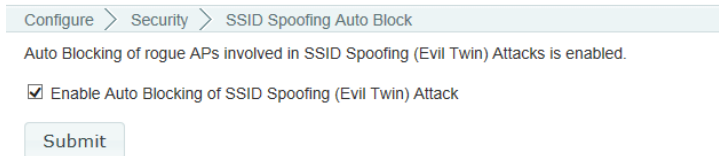
Figure 135. Auto Blocking SSID Spoofing Attacks

Suppose you add a new SSID to your Access Point 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 97**
- **"Security—Rogue Rules" on page 195**
- **"About Blocking Rogue APs" on page 572**

Access Point Licenses

These pages display and manage the licenses for Access Points in your Xirrus network. You may view the license of each Access Point 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 XMS to manage Access Point licenses. If you are looking for information regarding the XMS server's license, please see **Managing the XMS Server License**.

About Licensing and Upgrades

For AOS Release 7.0 and above, when a newly deployed Access Point boots up, it automatically contacts Xirrus with its serial number and MAC address and obtains its license key. Any unlicensed Access Point will auto-license in this way after it boots up, if it has Internet connectivity.

XMS manages the licenses for large numbers of Access Points. You can easily view licensing information for your Access Points and manage individual licenses. The license utility can apply bulk licenses in one step, by simply importing the .csv license file issued by Xirrus. Similarly, when it's time to upgrade all of your Access Points with new features or a major software release, the required licenses may all be installed in one step.

An Access Point's license determines many of the features that are available on the Access Point. 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 **"Advanced Feature Sets"** in the **Introduction** chapter of the *Xirrus Wireless Access Points User's Guide.*

If you are upgrading an Access Point to add new features that are not supported by your existing license, **the Access Point must have the new license key that includes the upgraded features before upgrading**.

Similarly, if you are upgrading an Access Point for a new software release, **the Access Point must have the new license key that enables the operation of that release before upgrading**. Major releases will need a new license key, but minor releases will not. For example, to upgrade from AOS Release 7.0.5 to Release 7.1, you need a new license. To upgrade from AOS Release 7.0.5 to Release 7.0.8, use the existing license.

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 Access Points in the selected **Current Access Point Scope** are listed.

Figure 136. Access Point License Management - Deployed Licenses

Initially, this page displays a list of all *deployed* Access Point licenses being managed by XMS. This is a list of all discovered Access Points and their licenses. By default the following is shown for each Access Point: the **License Key**, the **Hostname** along with the **Access Point 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 Access Points, described above.
- **Export Licenses**

- **Import Licenses**
- **Edit Licenses**
- **Pending Licenses**

*If you change a license directly using the CLI or WMI on an Access Point whose license status is **Deployed**, XMS will detect the change and display the changed license in the list of deployed licenses.*

However, if XMS has a license pending for that Access Point, that license will be deployed as soon as XMS is able to do so, replacing the license in the Access Point.

Export Licenses

At times, you may wish to export Access Point licenses to a file. For example, you may want a consolidated record of some or all of your licenses, or Xirrus Customer Service may request this information to 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 209**.

To export deployed licenses from the web client, select the **Export Licenses** page from the **Licenses** section of the **Configure** menu. Note that only Access Points in the selected **Current Access Point 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 137**)

Figure 137. Exporting Access Point 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.

Figure 138. Sample Export File

This exports the selected deployed licenses into a file of the selected format. A sample export file is shown in **Figure 138**.

Import Licenses

Use this feature to import a .csv or .xls file with licensing information for any number of Access Points. For example, to upgrade your entire Xirrus wireless network for Application Control, you must first deploy licenses for that feature. Xirrus 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 Access Points.

After your license file has been imported, any licenses that are for XMS managed Access Points (i.e., those that have been discovered) will be deployed to those Access Points. The Access Point is not rebooted but the radios will go down and up, so that station associations will be disrupted briefly. The Access Point will start using the new license, and will support the capabilities shown in the **Features** column.

A license for an Access Point that is not yet under XMS management will be deployed as soon as the target Access Point is discovered. Similarly, a license for a managed Access Point 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 203**). 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. (**Figure 139**) Check that the licenses imported correctly. If necessary, you may edit any **License Key** by clicking on it.

Figure 139. Importing Access Point Licenses

Click **Finish** to complete the import process. Any license that cannot be deployed now either because the Access Point has not yet been discovered by XMS or because the Access Point is off line will be placed in the pending list and will be deployed when the Access Point is available. The **Status** field will show the results for each Access Point.

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 140**) Note that only Access Points in the selected **Current Access Point Scope** are listed.
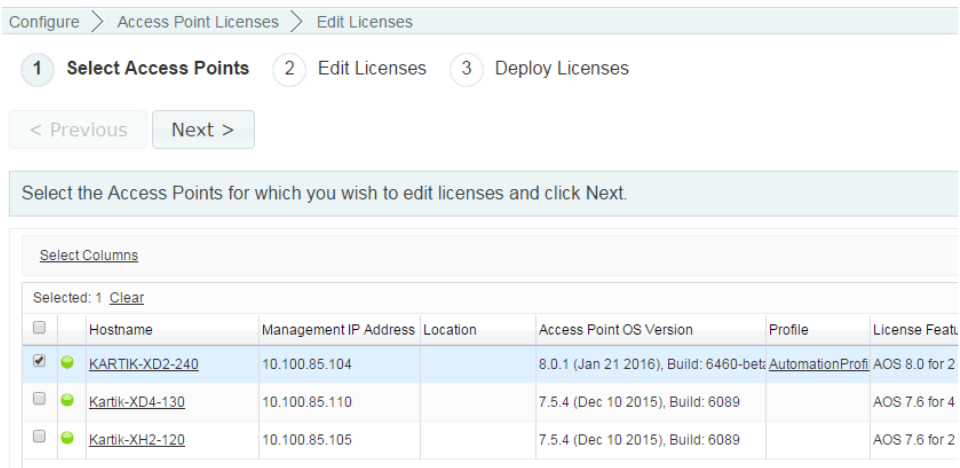
Figure 140. Select Access Point Licenses to Edit

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 141**)

To modify a license, click the Access Point'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 Access Points, and the status of the operation will be displayed for each Access Point.

Figure 141. Editing Access Point Licenses

You may not delete deployed licenses, but you may delete those that have not yet been deployed. See **"Pending Licenses" on page 209**.

Also note that you may not enter new licenses "by hand". To add a new license, please see **"Import Licenses" on page 205** and **"Pending Licenses" on page 209**.

Pending Licenses

Pending licenses are those that XMS 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 142**)

Note that if an Access Point 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.

Figure 142. Access Point Licenses Pending Deployment

License Status may have the following values:

- **Access Point Not Discovered**—a new license that has not been installed because the designated Access Point has not been discovered yet (i.e., the Access Point is not listed in the **Access Points** page). This does not mean that XMS cannot find the Access Point in your network, but rather that the discovery process has not yet added it. To add the Access Point to XMS using the web client, see **"Add Devices" on page 183** or **"View Networks" on page 191**. When the Access Point is discovered, XMS 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 207**. Use the **Deploy Now** button to "push" the corrected license to the Access Point.

- **Pending Deployment**—a previously discovered Access Point is currently unreachable or down, and XMS 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 XMS immediately attempt to deploy the selected licenses on their target Access Points. 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 Access Point is not rebooted but the radios will go down and up, so that station associations will be disrupted briefly. The Access Point 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

XMS provides profiles for ease of management. A profile allows you to specify a set of Access Points and manage them as a group. After creating a profile, you then define a uniform configuration and AOS software release to be applied to all of the member Access Points. This "manage by network" feature eliminates the time-consuming and error-prone task of configuring and managing Access Points individually, and ensures the deployment of consistent software and settings across each profile. You can add Access Points 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 XR-320. AOSLite profiles have a small number of settings, consistent with the simple configuration of these APs.

- **AOS Profiles** are for the rest of the Xirrus AP models, which run AOS software. AOS profiles have a rich set of configuration options, just as AOS 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 XMS discovers an Xirrus 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 Access Points should not be configured individually directly via their CLI or WMI. This usually results in temporary inconsistencies between the Access Point configuration and the XMS database. Note that member Access Points can be configured individually via XMS, 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 **Access Point Details—Configuration** *tab in XMS, you must then use the* **Refresh** *button for this AP (on the* **Access Point Details** *page or on the* **The Access Points List** *page). When you refresh the AP, XMS will update its database with the current configuration of the AP. When a profile change is applied to the AP, XMS pushes out configuration changes to the AP based on the AP's current configuration as shown in the XMS database. After making a "manual" change, you must use the Refresh button, or risk having subsequent profile changes fail because XMS is unaware of the AP's current settings.*

Settings that must be unique per Access Point are automatically excluded from management by the profile. For example, the Access Point IP address and hostname must be different for each Access Point, 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 Access Point.

Member Access Points need not be running AOS Release 6.5 or above to be managed as part of a profile.

Profiles

The web client Profiles page lists all of the profiles being managed by XMS, and allows you define new profiles and perform selected functions on them. To display this page, click the **Profiles** link in the Access Point **Configuration** section under **Configure** at the top of the page.
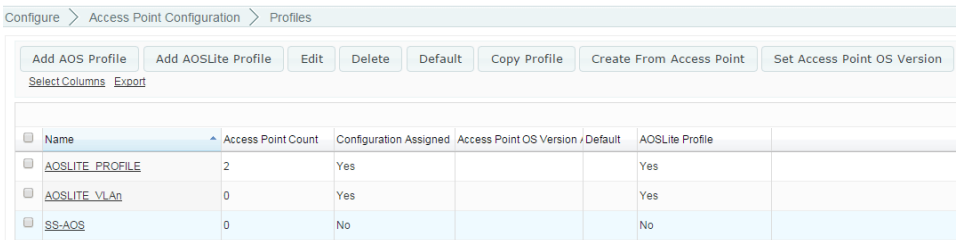
To start using profiles, follow these basic steps:

1. **Create a profile** and assign Access Points to it. See **Add AOS Profile** and **Add AOSLite Profile** in the **"The Profiles Toolbar" on page 215**. Alternatively, for AOS profiles only, you may import a .csv file that contains assignments to profiles for many Access Points and will create those profiles if needed, as described in **"Import Access Point Custom Fields" on page 138**.

2. **Specify the software release** to be run on the profile network. See **Set AP OS Version** in the **"The Profiles Toolbar" on page 215**.

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 223**.

The following sections describe the Profiles page:

- **About Using the Profiles Page**
- **The Profiles List**
- **The Profiles Toolbar**
- **Profile Details**
  - **Profile Details—Access Points**
  - **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	

Configure > Access Point Configuration > Profiles

Add AOS Profile | Add AOSLite Profile | Edit | Delete | Default | Copy Profile | Create From Access Point | Set Access Point OS Version
Select Columns Export

Figure 143. Profiles Page

About Using the Profiles Page

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

- **"Select Columns" on page 67**
- **"Export" on page 68**
- **"Select Rows" on page 69**
- **"Rearranging and Resizing Columns in a Table" on page 69**
- **"Sorting" on page 69**
- **"Searching" on page 70**

The Profiles List

The Profiles List (**Figure 143 on page 213**) 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 Access Points, 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 Access Points and show the status of the operations performed on them.

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

- The **Name**
- The Access Point **Count** of member Access Points
- 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 Access Points 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.

| Add AOS Profile | Add AOSLite Profile | Edit | Delete | Default | Copy Profile | Create From Access Point | Set Access Point OS Version | Sy |
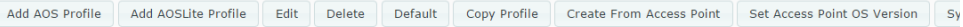
Figure 144. The Monitor—Access Points Page Toolbar

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 Access Points. 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 Access Points Toolbar**. Alternatively, for AOS profiles only, you may import a .csv file that contains assignments to profiles for many Access Points and will create those profiles if needed, as described in **Import Access Point Custom Fields**.

Add New AOS Profile

Profile Name: EastCampus-Munroe4

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

Showing: 1 to 2 of 2

	Hostname	Management IP Addres	Location	Access Point OS Version	Profile	
	Kartik-XD4-130	10.100.85.110		7.5.4 (Dec 10 2015), Build: 6089		
	Kartik-XH2-120	10.100.85.105		7.5.4 (Dec 10 2015), Build: 6089		

Figure 145. Add a Profile

Enter the new **Profile Name**, then select the Access Points that are to be members of this profile. Only Access Points 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 Access Point is shown. Click **OK** when done.

Note that you may also add Access Points to a profile from **The Access Points List**, using the **Assign to Profile** button in **The Configure Access Points Toolbar**.

An Access Point may not be a member of more than one profile. If you wish to move an Access Point 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 Access Points Toolbar**. The **Assign to Profile** button will remove each selected Access Point from its old profile assignment (if any) and add it to the specified profile in one step. See **"The Configure Access Points Toolbar" on page 119**.

● **Edit**—this option allows you to change which Access Points are members of the profile. The Access Points listed include both the profile's current members, and Access Points that are not already assigned to another profile.

Edit a Profile

Profile Name: SS-AOS

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

Showing: 1 to 2 of 2

		Hostname	Management IP Addres	Location	Access Point OS Version	Profile	
☐	●	Kartik-XD4-130	10.100.85.110		7.5.4 (Dec 10 2015), Build: 6089		
☐	●	Kartik-XH2-120	10.100.85.105		7.5.4 (Dec 10 2015), Build: 6089		

Figure 146. Edit a Profile

You may check Access Points 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 Access Points from the XMS 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 Access Points as described in **"Import Access Point Custom Fields" on page 138**. These assignments will replace any current assignments of Access Points to profiles, and they may then be edited as well.
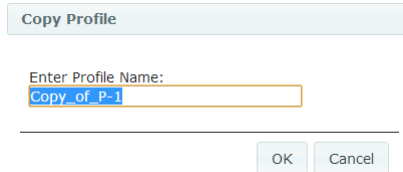
When you add an Access Point to an existing profile that has a software version and or configuration defined, the new member is checked for compliance with this profile. If needed, jobs are triggered to upgrade the software version and/or update the configuration. Note that if both are needed, the software 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 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.

- **Delete—**this option deletes the selected profiles. It does not delete the member Access Points from the XMS database - they just cease to be assigned to a profile. The configuration and software version of these Access Points are untouched by this deletion. You will be asked to confirm the operation.

- **Default**—this option sets one selected profile as the default. When Access Points are discovered, they are automatically added as members of the default profile. These Access Points 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 147. Copy a Profile

The new profile is created with no member Access Points. Use the **Edit** button to add the desired Access Points to it. The new profile's Configuration and AOS Version are identical to those of the original profile until you change them.

- **Create From Access Point**—this option creates a new profile with an initial configuration that is copied from the selected Access Point. This is useful if you already have a Xirrus network deployed and wish to create profiles to mirror the existing settings, or if you prefer to perform configuration directly on an Access Point 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: XD4-Profile

Select Columns

Selected: 1 Clear   Showing: 1 to 3 of 3

		Hostname	Management IP Addres Location	Access Point OS Version	Profile
☐	🟢	KARTIK-XD2-240	10.100.85.104	8.0.1 (Jan 21 2016), Build: 6460	AutomationPro
☑	🟢	Kartik-XD4-130	10.100.85.110	7.5.4 (Dec 10 2015), Build: 6089	
☐	🟢	Kartik-XH2-120	10.100.85.105	7.5.4 (Dec 10 2015), Build: 6089	

OK   Cancel

Figure 148. Create a Profile from an Access Point

You may also create a profile from a selected Access Point in **The Access Points List** or from an **Access Point Details** page, by selecting **More > Create Profile** from **The Configure Access Points Toolbar**.

The new profile is created with no member Access Points and no AOS Version. Use the **Edit** button to add the desired Access Points to it. The new profile's Configuration settings are identical to those of the prototype Access Point until you change them, except as noted below.

• The rules listed in **"Settings that are omitted from profile configuration" on page 225** 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 Access Points do. For example, if the prototype Access Point has more than 8 SSIDs configured, you will see an error message.

- **Admin Management** accounts and **Admin Privileges** are not copied from the prototype Access Point. 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 225** are not included in the profile.

- The profile is created using the configuration data for the Access Point that is already in the XMS database, rather than reading the configuration directly from Access Point. If you wish, you may refresh the Access Point prior to creating the profile, using the **Refresh** button on **The Access Points List** page—this will update XMS with the latest configuration.

- **Set Access Point OS Version**

  Click this button to set up the desired AOS or AOSLite software version for this profile network. You can specify the software version regardless of whether or not the profile contains any member Access Points. It is also possible to use this to roll back the profile network to an earlier software version, although the downgrade will fail for Access Points that don't support the older software.

  Follow the same steps described in **"Perform or Schedule Upgrade" on page 148**, except that you will not be asked to specify the Access Points 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 Access Point licenses will be updated if necessary prior to the upgrade, also as described in **"Perform or Schedule Upgrade" on page 148**.

Figure 149. Set Profile's Software Image

Member Access Points will be checked for the correct software version when:

- You enter a different software version in **Set AP OS Version**.

- An Access Point is added to the profile network either via discovery, or by using the **Edit** button.

- You click the **Sync Access Points** 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 Access Points to run a specific software version.

- **Sync Access Points—**Click this button to check that **all** member Access Points 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 XMS to make configuration changes to individual member Access Points 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—Access Points" on page 222**—a list of member Access Points.

- **"Profile Details—Configuration" on page 223**—this tab allows you to define the configuration settings for all member Access Points.

- **"Profile Details—Job Status" on page 231**—this tab shows all the configuration/software upgrade jobs for member Access Points, along with their status.

Profile Details—Access Points

This page lists the member Access Points 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 Access Points are members of this profile, as described for the **Edit** button in **"The Profiles Toolbar" on page 215**.

Figure 150. Profile Details: General

Click the **Configuration** tab to define the Access Point settings for this network.

Profile Details—Configuration

This page has an extensive menu of options for defining the configuration profile on the member Access Points. Almost all of the settings that are available in the Access Point Windows Management Interface (WMI, for non-AOSLite devices only) are also available here.

Figure 151. 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 Access Point, 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 225**.

> ✎ *Note that smaller APs that use the AOSLite system software, such as the XR-320, 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 Access Point" on page 411**. When you create a new profile, it will have the default configuration setting values shown in **Default Profile Configuration**, below.

One special feature allows you to configure settings that are not available in **Configuring a Wireless Access Point**. The **Templates** page applies a **Config Template** to each AP after the rest of the profile configuration has been pushed to the AP. You may select different templates to apply to different **Access Point Groups**. See **"Templates" on page 227**.

> ✎ *If you plan to define a required AOS version for this profile network, we strongly recommend that you do that first using the **Set AOS Version** button, as described in **The Profiles Toolbar**. The profile performs the required software upgrades before updating configuration on member Access Points. 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 Access Point 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

Tab	Setting	Value
Services> SNMP	Context Engine ID	Not displayed
Services> Location	Location Support	Disabled
SSIDs> SSID Management	Name	xirrus (same for AOSLite devices)
Radios> Global Settings	Country	AOSLite—United States; AOS—Not set. See **"Settings with special handling in profile configuration" on page 227**.
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 Access Point IP address must be unique, and the assigned address must not be changed when the profile configuration is "pushed" to the Access Point. 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 Access Point.

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 XMS 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 Access Point" on page 411**. These are special settings that deal with the differences in the range of Access Point models. Currently, there is only one such setting, and it is only for AOS Profiles.

- **Radios > Advanced RF Settings**: **Enable Timeshare for 2-Radio Access Points**— By default, the **RF Monitor Mode** on profile-member Access Points 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 Access Points, but it is inefficient usage of radio resources for Access Points 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 Access Points** to **Yes**. Then Access Points 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 564** 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 needs additional explanation. These settings typically deal with the differences in the capabilities of Access Point 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 Access Points where it isn't already set.

- **VLANs > VLAN Management**—You may define up to 64 VLANs in a profile. Some Access Points support 64 VLANs, but smaller APs may only support 16, depending on the software release. 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.

- **SSIDS > SSID Management > Captive Portal > Server**—If you configure this to use a **Cloud Guest Access Portal**, the guest portal works with all of the profile's member APs that are running Release 7.1 or above. If the profile includes APs that are running a lower release, we suggest that you upgrade them prior to configuring the guest portal. Profile member APs running earlier releases will have SSIDs automatically disabled, if those SSIDs are assigned to the guest portal. See **"SSID Management—Captive Portal" on page 502**.

Templates

Some AP settings are not available using the **Profile Details—Configuration** tab. **Config Templates** solve this problem by using a CLI config file to configure advanced features. You can set up profiles to automatically deploy config templates to APs. When a new AP is added to XMS, the config template will be applied to the AP after the rest of profile configuration is applied to it. If the config template has different values for some settings than the profile does, the template settings will override previously applied values. The results of applying the config template will be reported as part of profile configuration status in **Profile Details—Job Status**.

About using config templates in a profile

Config Templates are configuration files—they may be created by using XMS to download the configuration of an AP that has desired settings and editing the file

in XMS so that it includes exactly the settings needed. XMS also allows you **To create a config template from beginning to end ("from scratch")** and edit that file, with the option of copying and pasting CLI commands from an existing config file.

Multiple config templates can be assigned to the profile. If the profile has APs belonging to different **Access Point Groups**, then you can select which template is to be used for members of each AP group. Only one template may be assigned to an AP group in a profile, but the same template may be assigned to other AP groups in the same profile. Template assignments in different profiles are independent of each other, so the same config template could be used in other profiles as well, with the same or different AP group assignments. A **Default** template is assigned to any APs that are not members of AP groups that have a specific template explicitly assigned to them.

If you remove an AP from one profile and add it to a different profile, the template assigned to the new profile is applied to the AP after the rest of the new profile's configuration has been applied.

To assign config templates to a profile
Note that the **Templates** link is not available for AOSLite profiles, and you must have already created at least one config template for this link to appear.

1. Create the config templates that you will be using. If you plan to assign different templates to APs based on their AP group membership, create the AP groups and assign APs to them. See **"Access Point Groups" on page 126** and **"Config Templates" on page 127**.

2. In the **Profile Details—Configuration** tab, select **Templates** at the lower left, and then click **Template Settings**. The Template Settings page lists the config templates that have so far been assigned to this profile, and the AP groups that they are associated with.
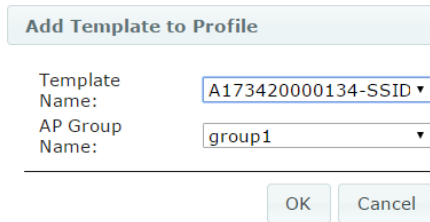
Figure 152. Template Settings Page

The order of the templates in the list is important - XMS searches the list starting with the highest **Priority** entry (Priority 1). When an AP is added to XMS, if the AP belongs to a group, then the first template it finds associated to a group that includes the AP (if there is at least one) is used. It no such templates are found, or if the AP does not belong to a group, then the **Default Template** is used if it has been set. Only one template is applied to an AP.

3. Select a **Default Template** from the drop-down list that shows all of the **Config Templates** in XMS. This step is optional, but if there is no default template, then config templates will only be applied to APs belonging to groups that have a config template specified.

4. To add a config template to the list, click **Add**. Select the **Template Name** from the drop-down that lists all currently defined **Config Templates**. Then you must select an **AP Group Name** from the drop-down that lists **Access Point Groups**. See **"About using config templates in a profile" on page 227** for details on adding multiple templates to a profile.

Figure 153. Add or Edit a Config Template

5. As discussed in **Step 2** above, when this profile is applied to an AP, the list of templates is searched in priority order starting from Priority 1. You may change the order of entries by using the **Move Up** and **Move Down** buttons.

6. You can **Edit** or **Delete** entries using the buttons in the tool bar.

7. Click the **Apply Config** button at the top of the page to apply these changes to the profile and make these changes permanent.

Profile Details—Job Status

This page shows jobs launched for member Access Points by the profile. You may select whether to show **AOS Upgrades**, Access Point **Config** updates, **Discovery**, or **All Jobs**. Note that if **AOS Upgrades** and Access Point **Config** updates need to be performed for the same Access Point, 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

Access Points	Configuration	Job Status

Job Type: All Jobs

Select Columns Export

Showing:

	Status Updated	Hostname	Access Point OS Version	Target Access Point OS	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	50:60:28:02:6

Figure 154. 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 Access Point that is being updated by this job.

- **Management IP Address**—the IP address of the member Access Point that is being updated by this job.

- **Job Type**—the type of update that this job is performing—**AOS Upgrade** or Access Point **Config**.

- **AOS Version**—the current AOS version running on the member Access Point that is being updated by this job.

- **Target AOS**—the AOS version defined for this profile network, if any.

- **Message**—information about the job performed on the Access Point, if successful; or the type of failure, otherwise.

Managing Switches

XMS manages Xirrus 24-port XT-5024 and 48-port XT-5048 PoE+ Gigabit wired access switches. Pages are provided for monitoring these switches, and for common configuration tasks. Switch management pages are very similar to Access Point management pages, for ease of use.

Xirrus 24- and 48-port switches offer intelligent power distribution across all ports. IEEE802.3at (PoE+) and 802.3af (PoE) is available on every port. These switches may be used to power Xirrus Access Points and APs that are compatible with 802.3af or 802.3at, such as the XR-520 AP.

Many Xirrus Access Point models require Xirrus-supplied injectors. Their power requirements are not compatible with the XT-5024/XT-5048. See the Quick Installation Guide for the Access Point model for more information about powering it.

Switch management is discussed in the following topics:

- **"Switch Discovery" on page 234**
- **"Monitoring Switches" on page 234**
- **"Configuring Switches" on page 235**
- **"Switch Details" on page 236**
- **"Switch—General Information" on page 236**
- **"Switch—Configuration" on page 237**
- **"Switch Configuration—System" on page 237**
- **"Switch Configuration—IP" on page 238**
- **"Switch Configuration—PoE Configuration" on page 240**
- **"Switch Configuration—VLAN" on page 244**
- **"Switch—PoE Status" on page 249**

To see which Access Point port is being powered by each switch port, see **"Port Mappings by Switch" on page 146**.

Switch Discovery
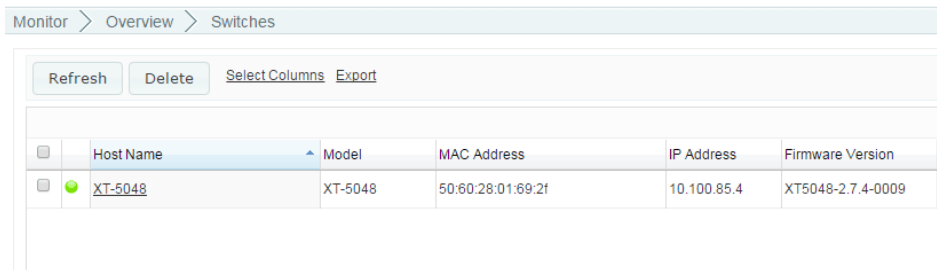
Xirrus wired switches are discovered in exactly the same way as Access Points. When you tell XMS what subnets to run discovery on to find Access Points, it will find XT-5024 and XT-5048 switches and Xirrus-supplied managed power injectors at the same time. Please see the discussion starting with **"Discovery" on page 178** for complete details.

When a wired switch has been discovered, it will appear on the **Switches List (Monitor)** as shown below.

Monitoring Switches

This page lists the switches in the XMS database. To display it, click the **Switches** link under **Monitor** at the top of the page. This page is identical to the Configure—Switches page (see **"Configuring Switches" on page 235**).

The Switches List shows Xirrus wired PoE+ switches that have been discovered by XMS (see **Switch Discovery**). Each switch entry is identified by its MAC address, and also displays the unit's **HostName**, **Model** (**XT-5024** and **XT-5048**), **IP Address**, and running **Firmware Version**. A green or red dot shows the current status of each switch. For detailed information on the status of the switch and its individual ports, see **"Switch—PoE Status" on page 249**.

Monitor > Overview > Switches

		Host Name	Model	MAC Address	IP Address	Firmware Version
☐	🟢	XT-5048	XT-5048	50:60:28:01:69:2f	10.100.85.4	XT5048-2.7.4-0009

Refresh | Delete | Select Columns | Export

Figure 155. Switches List (Monitor)

Please see **"Configuring Switches" on page 235** for the operations available on this page. To see which Access Point port is being powered by each switch port, see **"Port Mappings by Switch" on page 146**.

Configuring Switches

This page lists the switches in the XMS database. To display it, click the **Switches** link in the **Switch Configuration** section under **Configure** at the top of the page. This page is identical to the Monitor—Switches page (see **"Monitoring Switches" on page 234**).

Figure 156. Switches List (Configure)

The switches list offers the following functions:

- Click on a switch's **Name** (MAC Address) to access the Switch Details pages. These offer some powerful features, especially the **Configuration** page, which allows you configure the most commonly used settings on that switch. See **"Switch Details" on page 236** for more information.

- Click the **Refresh** button to refresh discovery and status on the selected switches. Status is automatically polled every 30 seconds.

- Click the **Delete** button if you wish to remove the selected switches from the database.

In addition, a number of common operations are available on the Switches page to allow you to customize it for your own use. These functions are similar to the functions available on the **The Access Points List**:

- **"Select Columns" on page 67**
- **"Export" on page 68**
- **"Select Rows" on page 69**
- **"Rearranging and Resizing Columns in a Table" on page 69**
- **"Sorting" on page 69**
- **"Searching" on page 70**

Switch Details

By clicking the MAC Address of a switch in the Switches List (from either the monitor page or the configure page), you may view or configure a variety of details about the selected unit. The details page for a switch has three tabs:

- The **General** tab shows status and version information. See **"Switch—General Information" on page 236**.

- **Configuration** tab—configures the most commonly used switch settings for system information, IP network and VLAN settings, and PoE settings. See **"Switch—Configuration" on page 237**.

- **PoE Status** tab—this tab shows details of power usage for each individual port and for the switch as a whole, as well as the status of each port. See **"Switch—PoE Status" on page 249**.

To specify which Access Point is being powered by each switch port, see **"Port Mappings by Switch" on page 146**.

Switch—General Information

Select the **General** tab to display status and version details.
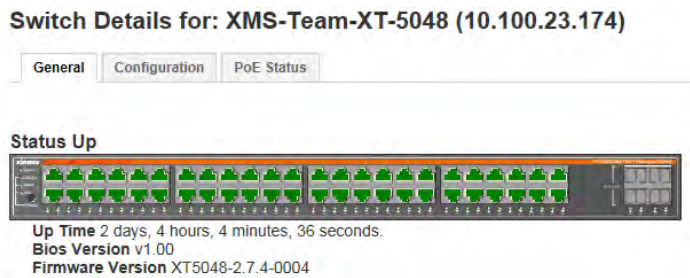
Figure 157. Switch Details—General Information

- The running status of the switch is indicated as **Status Up** or **Status Down**.

- The time since the last boot is shown in **Up Time**.

- Running software is indicated in **Bios Version** and **Firmware Version**.

Switch—Configuration

The Configuration tab allows you to manage the following settings:

- **"Switch Configuration—System" on page 237** sets the hostname and contact information.

- **"Switch Configuration—IP" on page 238** configures IP network settings.

- **"Switch Configuration—PoE Configuration" on page 240** sets port priority and enables/disables each port.

- **"Switch Configuration—VLAN" on page 244** configures VLAN settings.

Switch Configuration—System

This window allows you to set general information about this switch, including changing its host name and setting administrator contact information.

Figure 158. Switch Details—System Information

Procedure for Configuring System Information

1. **Hostname:** Specify a unique host name for this switch. The host name is used to identify the switch on the Layer 3 network. Use a name that will be meaningful within your network environment.

2. **Location Information**: Enter a brief but meaningful description that accurately defines the physical location of the switch. 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 name and contact information for the person responsible for administering the switch at the designated location.

4. Click the **Apply Config** button at the top of the configuration window to apply these changes to the switch. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Switch Configuration—IP

This window manages network interface settings. For each setting, the **Current** value on the switch is shown on the right. In the **Configured** column on the left, there are fields where you may change IP settings—these fields simply display the last values that you typed in, and they initially show factory default values. If you change any values, they will not be applied on the switch and reflected in the **Current** values until after you click the **Apply Config** button.

Figure 159. Switch Details—IPv4

Procedure for Configuring the Network Interfaces

1. **Use DHCP Client**: use this option to instruct the switch to use **DHCP** to obtain its IP address, or turn off this option if you intend to perform IP configuration manually. If you turn off **Use DHCP client**, you must specify a static IP address, subnet mask, and default gateway below. If **Use DHCP Client** is enabled, then all of the fields below it are disabled except for **VLAN ID**.

   *If **Use DHCP Client** is enabled but the switch is unable to obtain an IP address via DHCP, the switch will use the settings that are shown in the **Configured** column.*

2. **IP Address**: If you turned off the **DHCP Client** option, enter a valid static IP address for the switch. To use remote management (Web or **SNMP**), a valid IP address must be established.

3. **IP Mask**: If you turned off the **DHCP Client** 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 switch is located.

4. **IP Gateway**: If you turned off the **DHCP Client** option, enter a valid IP address for the **default gateway**. This is the IP address of the router that the switch uses to transmit data to other networks.

5. **VLAN ID**: Specify the VLAN number to be used as the switch management VLAN. By default, all ports are in VLAN 1. This VLAN is untagged. Be **very** careful when changing this value. Changing the VLAN ID can cause you to be unable to connect to the switch if the network interface is not correct. We recommend that you leave this unchanged unless you have determined that a change is required.

6. **DNS Server**: Enter the IP address of a DNS server to be used to resolve domain names and host names to IP addresses.

7. Click the **Apply Config** button at the top of the configuration window to apply these changes to the switch. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Switch Configuration—PoE Configuration

This window displays power settings for switch ports. You may manage power injection for each port, and set the priority for allocating power to the port.

Above the list of ports, **Primary Power Supply (W)** shows the maximum total power that is available for ports on this switch model. (See **"Switch—PoE Status" on page 249** for details of how much power each port is using at this time.)

Figure 160. Switch Details—PoE Configuration

Retry Time—when a port draws more power than permitted by its **Maximum Power** setting (see below), the switch turns off power to that port. The switch waits Retry Time seconds before trying to turn power back on to an overloaded port. If Retry Time is set to 0, the switch will not attempt to turn power back on to ports, and overloaded ports will remain off until you turn them back on manually.

For each switch port, the following settings are shown. They may be modified with the **Bulk Edit** button.

- **PoE Mode**: On the XT-5024, this should normally be set to **High Inrush**. This value is required for compatibility with some devices, for example, some Xirrus Access Points and APs. Some devices draw a large amount of

power initially when they power up, causing the switch port to incorrectly detect a malfunction on the device being powered. The High Inrush setting allows these devices to be correctly detected. High Inrush should be used with all devices—it will not impair the detection of devices that do not require this special handling.

Enable allows the injection of power on this port, and this value should be used for the XT-5048, which does not have a High Inrush setting. **Disable** turns off the injection of power on this port—only data traffic is transmitted on the port.

- **Priority**: This is the priority of this port for power allocation, if the power drawn by all ports exceeds the power available on the switch (as shown in **Primary Power Supply**). If there is insufficient power, the switch will first turn off ports assigned **Low** priority, then ports assigned **High** priority. Power will be dropped last from ports that have **Critical** priority. One of the ports with the lowest priority will be turned off, starting from the highest port number. Additional ports are turned off one at a time as necessary, following the same rule. When the over power-budget situation ends, the switch will automatically reallocate power to ports that were turned off due to insufficient total power. The ports that were turned off last are normally restored first, since they are the higher priority ports. Note that this process for restoring ports is not related to **Retry Time**.

- **Maximum Power (W)**: This is the maximum amount of power that this port is allowed to supply. If the connected device begins to exceed this maximum, power is cut off to this port. You may specify a different maximum for each of the switch's copper ports, if you wish. The default value is 30W.

You must set Maximum Power to the highest level that the Access Point or AP may need to draw. If the Access Point becomes heavily loaded and requires more power than you have set in Maximum Power, the powered device will reboot as the overload causes the port to be turned off and then on again after a delay of Retry Time seconds.

The maximum power that the switch can supply to a port is normally 30W—however, on the XT-5024 and XT-5048, the first twelve copper ports (Ports 1-12) can each be set to supply up to 38W. Standard power is 15.4W for IEEE802.3af compliant devices, and 30W for IEEE802.3at compliant devices.

Switch power is dynamically pooled from the power supply across all of the switch's ports. *Over-subscription* of power is permitted, i.e., the sum of the maximum power specified for all of the ports may exceed the value shown for **Primary Power Supply**. For example, the maximum power that an XT-5024 can supply is 370 W. As an example, you may enable PoE on 15 ports and set maximum power on each of them to 30W, a total of 450W. Let's say that each of your powered devices typically draws 20W, and may occasionally require peak power of up to 30W when very busy. Since the typical total power usage is 15 x 20 = 300W and power is pooled across the ports, the switch has 70W to spare that may be drawn by devices needing more power.
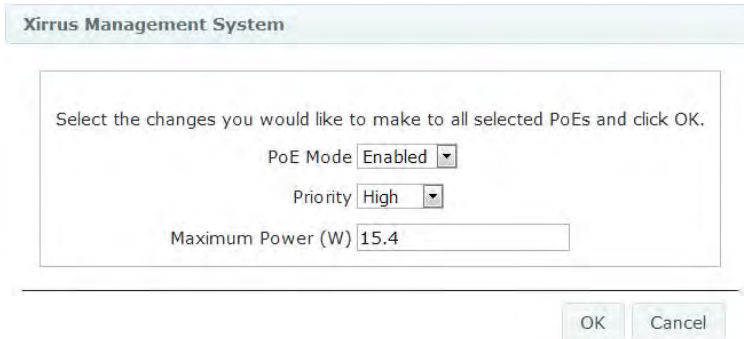
We recommend that you do not over-subscribe the switch's available power by more than 20%. If connected devices attempt to draw more power than the switch can deliver, power will be turned off on ports as described above, based on the **Priority** setting of each port.

The switch waits **Retry Time** seconds before trying to restore power to overloaded ports.

Procedure for PoE Configuration

1. **Retry Time**: The switch waits this number of seconds before trying to turn power back on to overloaded ports. Adjust this time if needed. The default is 60 seconds.

2. **Bulk Edit**: Click this button to change the settings of one or more ports at the same time. Select the checkboxes of the ports that you wish to edit to have identical settings. All of these ports will be configured to have the settings that you specify in the Bulk Edit dialog box. (**Figure 161**)

Figure 161. Switch Details—PoE Bulk Edit

3. Configure PoE settings as follows. For detailed explanations of these settings, see the discussion above.

- **PoE Mode**: Select **High Inrush** for XT-5024 switches to ensure that PoE power operates correctly with all powered devices. Select **Enabled** for XT-5048 switches to enable power injection on this port.

- **Priority**: Select the priority of this port for power allocation, **Low**, **High**, or **Critical**.

- **Maximum Power (W)**: Select the maximum power that this port is allowed to supply. The default value is 30W. Decimal numbers are allowed, e.g., 15.4. Exceeding this peak value causes the switch to detect an overload and shut off power to the port. Standard power is 15.4W for IEEE802.3af compliant devices, and 30W for IEEE802.3at compliant devices. The maximum power is 30W—however, on the XT-5024 and XT-5048, Ports 1-12 can each be set to supply up to 38W. See the discussion following **Figure 160 on page 240** for more information.

4. Click the **Apply Config** button at the top of the configuration window to apply these changes to the switch. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Switch Configuration—VLAN

This window allows you to create and manage VLANs, including defining the ports that are members of each VLAN. The following pages are used to manage VLANs:

- **"Switch Configuration—VLAN Membership" on page 244**—used to create VLANs and specify the ports that are members.
- **"Switch Configuration—VLAN Ports" on page 246**—used to configure a number of attributes of VLAN behavior, on a per port basis.

Switch Configuration—VLAN Membership

This page creates and modifies VLANs, and specifies the ports that are included in the VLAN.

The list of VLANs shows the VLANs that you have already created, identifying them by **VLAN Name** and **VLAN ID**. Each VLAN's entry indicates the ports that it includes, represented by green dots ●. You may **Add** new VLANs, and **Edit** or **Delete** existing VLANs.

Figure 162. Switch Details—VLAN Membership

Procedure for VLAN Creation and Membership Configuration

1. To create a VLAN, click the **Add** button.

2. Enter the **Name** of the VLAN, and a unique **VLAN ID** number. The Name may be up to 32 alphanumeric characters long.

Figure 163. Switch Details—VLAN: Create/Membership

3. Select the membership setting for each port:

   • **blank**—leave the setting blank to exclude this port from the VLAN. This is the default for all ports.

   • **member**—select this to make the port a member of the VLAN.

   • **forbidden**—this port is forbidden to join the VLAN. GVRP cannot automatically add this port to the VLAN.

4. You may select the checkbox to the left of a VLAN and click the **Edit** or **Delete** button to modify or remove a VLAN.

5. Click the **Apply Config** button at the top of the configuration window to apply these changes to the switch. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Switch Configuration—VLAN Ports

This page configures the VLAN settings for switch ports. For each port, the following settings are shown. They may be modified with the **Bulk Edit** button.

Switch Details for: XMS-Team-XT-5048 (10.100.23.30)

| General | Configuration | PoE Status |

Apply Config   Save to flash ☑

| ▸ System |
| ▸ IP |
| ▸ PoE |
| ▾ VLAN |
| VLAN Membership |
| *Ports* |

Bulk Edit   Select Columns   Export

Showing:

☐	Port ▲	Egress Rule	Native VLAN
☐	1	Hybrid	1
☐	2	Hybrid	1
☐	3	Hybrid	1
☐	4	Hybrid	1
☐	5	Hybrid	1
☐	6	Hybrid	1

Figure 164. Switch Details—VLAN Ports

- **Native VLAN**: The VLAN that carries untagged traffic on this port. When multiple VLANs are trunked on the same port, traffic for each VLAN is tagged with its VLAN number as specified in IEEE802.1q. Untagged traffic is automatically assigned to the native VLAN, and native VLAN traffic is not tagged when the port transmits it. The allowed values are 1 through 4094. The default value is 1. Note: The port must be included as a member of the Native VLAN (see **"Switch Configuration—VLAN Membership" on page 244**).

- **Port Type**: Port type should normally be set to **C-port**.

  - **C-port** is a Customer Port. This is the default setting, and you should normally leave the port type as **C-port**.

  The following settings are for special situations, such as QinQ, and are not typically used. These settings support IEEE 802.1ad Provider Bridging, also known as Stacked VLANs or QinQ. It essentially implements multiple levels of VLANs by supporting multiple tags in a

frame, allowing customers to run their own VLANs inside a VLAN established for them by a service provider. Thus, the service provider can just configure one VLAN for the customer and the customer can then treat that VLAN as if it was a trunk.

- **Unaware** classifies all frames to the Port VLAN ID and tags are not removed.
- **S-port** is a Service port.
- **Custom S-port** is an S-port with a Custom TPID (tag protocol identifier).

● **Ingress Filtering**: This setting determines the port's VLAN ingress processing. If ingress filtering is **Enabled** and this port is not a member of the VLAN specified in a frame, the frame is discarded.

● **Frame Type**: This setting determines the types of frames that are accepted by VLAN ingress processing—**All** frames, only **Tagged** frames, or only **Untagged** frames. If the port only accepts tagged frames, untagged frames received on that port are discarded.

● **Egress Rule**: This setting determines VLAN egress processing—it controls whether and how VLAN tagging occurs on outgoing frames.

- If **Trunk** is selected, outgoing VLAN traffic is tagged with the VLAN's ID. This mode is normally used for ports connected to VLAN-aware switches.
- If **Hybrid** (the default value) is selected, this VLAN's tag is inserted in the frame unless the frame is belongs to the Native VLAN.
- If **Access** is selected, all frames transmitted on the port are sent untagged.

Procedure for VLAN Port Configuration

1. To configure identical VLAN Port settings for one or more ports, click their checkboxes and then click the **Bulk Edit** button.

2. The Bulk Edit dialog box allows you to configure settings for **Native VLAN**, **Port Type**, **Ingress Filtering**, **Frame Type**, and **Egress Rule**. See the discussion above for descriptions of these settings.

Bulk Edit VLAN Ports

Select the changes you would like to make to all selected VLAN Ports and click OK.

Native VLAN 1

Port Type C-Port

Ingress Filtering Disabled

Frame Type All

Egress Rule Hybrid

OK   Cancel

Figure 165. Switch Details—VLAN Ports Bulk Edit

3. Click **OK** when done.

4. Click the **Apply Config** button at the top of the configuration window to apply these changes to the switch. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Switch—PoE Status

Select the **PoE Status** tab to view details of power usage for each individual port and for the switch as a whole, as well as the status of each port. This page also has a **Power Cycle** button that allows you to turn the selected ports off and on in one step, to perform a reset of the devices being powered by those ports.

Switch Details for: XT-5048 (10.100.23.30)

| General | Configuration | PoE Status |

Total Power Requested (W): 30.800000 **Total Power Allocated (W):** 30.800000
Total Power Used (W): 14.200000 **Total Current Used (mA):** 267.000000

Power Cycle Select Columns Export

Showing: 41 to 48 of 48

	Local Port ▲	PD Class	Power Requested (W)	Power Allocated (W)	Power Used (W)	Current Used (mA)	Priority	Port Status
☐	40	3	15.4	15.4	7	132	Low	PoE turned ON
☐	41	0	0	0	0	0	Low	No PD detected
☐	42	3	15.4	15.4	7.2	135	Low	PoE turned ON
☐	43	0	0	0	0	0	Low	No PD detected
☐	44	0	0	0	0	0	Low	No PD detected
☐	45	0	0	0	0	0	Low	No PD detected
☐	46	0	0	0	0	0	Low	No PD detected
☐	47	0	0	0	0	0	Low	No PD detected

Figure 166. PoE Status tab (Configure)

This page displays the following information.

Switch Power Statistics

- **PD Class**: The class of the powered device (PD) that the switch has detected on this port. The class indicates the maximum level of power expected to be supplied by the switch port for the PD.

  - Class 0—15.4 W

  - Class 1—4 W

  - Class 2—7 W

  - Class 3—15.4 W

  - Class 4—30 W

- **Power Requested (W)**: the amount of power that the PD has requested to have reserved. This is based on the PD, rather than the **Maximum Power** setting that you configured on this port.

- **Power Allocated (W)**: the amount of power that the switch has allocated for the PD.

- **Power Used (W)**: how much power the PD is currently using.

- **Current Used (mA)**: how much current the PD is currently drawing.

- **Priority**: the priority setting that you configured on this port.

- **Port Status**: the operating status of this port. May be one of:

  - PoE disabled—the **PoE Mode** setting for this port is **Disabled**.

  - No PD detected—the **PoE Mode** setting for this port is **Enabled**, but no compliant PD has been detected.

  - PoE turned ON—a PD has been detected, and power is being supplied.

  - PD Overload—the PD has attempted to draw more power than the **Maximum Power** setting allows, and the port has been turned off. The switch will attempt to turn the port back on at an interval defined by the **Retry Time** setting.

To see which Access Point port is being powered by each switch port, see **"Port Mappings by Switch" on page 146**.

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 XR-320, 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 Access Point, its radios and associated stations. Access Point 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 Access Points. 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-Access Point correction. By leveraging the RF analysis capabilities available on the Access Point, XMS 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 XMS 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 254**—provides an overview of the map window.

- **"Migrating Maps from Earlier Releases" on page 262**—XMS is furnished without any default maps. However, if you have already created maps in pre-6.2 releases of XMS, 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 263**—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 265**—follow these instructions to create a new map.

- **"Setting the Map Scale and North Direction" on page 267**—set the distance scale for the map, so that RF contours will display accurately.

● Select the Access Points that belong on the map. Rotate each Access Point on the map so that the monitor radio has the correct orientation (Note that many XR Access Points can automatically detect North, and XMS places these on the map in the correct orientation). See **"Adding Access Points to Maps" on page 270**.

● After completing the steps above, you may use the **RF Heat Contour Map** to present a live display of RF coverage by Access Point. To manage Access Points, see **"Managing Access Points Within Maps" on page 281**.

● 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 287** and **"Map Layers Panel" on page 295**.

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.
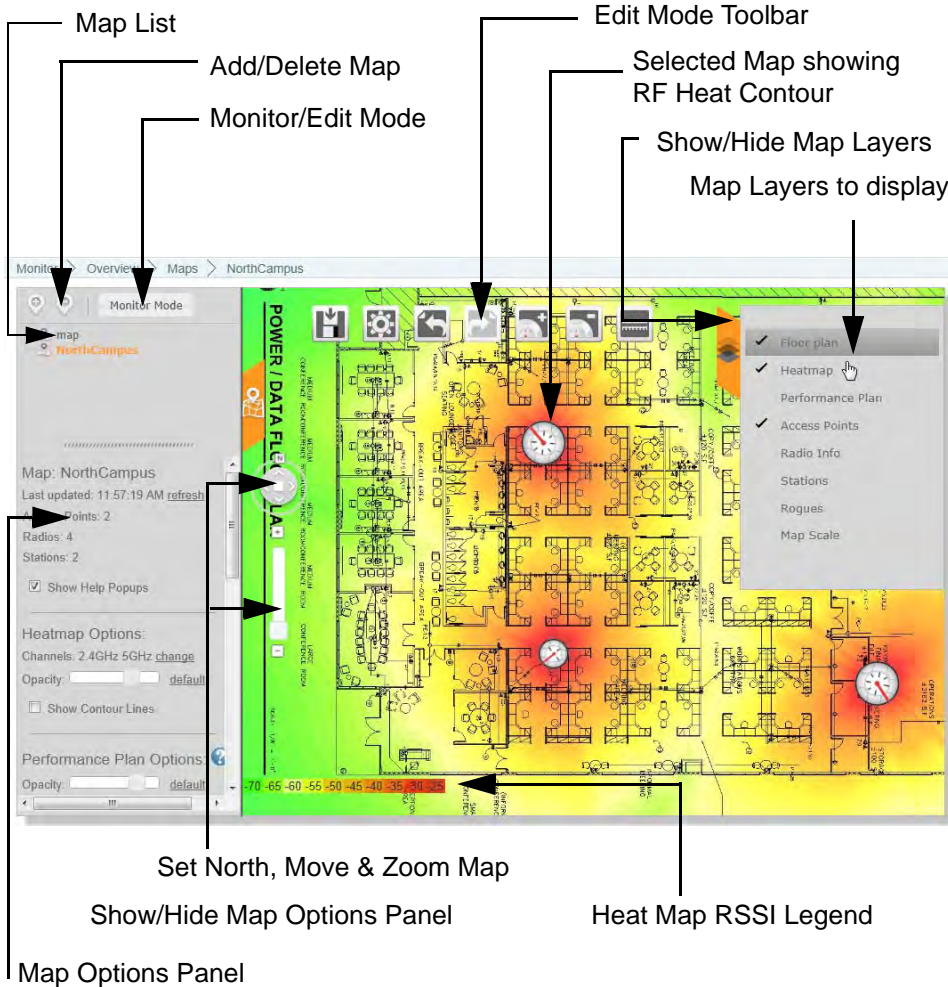
Figure 167. Main Map with RF Heat Contours Enabled

No default maps are provided. If you have created maps in a previous release of XMS, they will be present after you upgrade. When you upgrade to a new release

of XMS, maps created in earlier releases will be automatically migrated. See **"Migrating Maps from Earlier Releases" on page 262**. You may create new maps as described in **"Adding a New Map" on page 265**.

The map window has the following parts:

- **The Map List**
- **RF Heat Contour Map**
- **Performance Plan**
- **Map Options Panel**
- **Map Layers Panel**
- **Access Point Management Panel**

The Map List

This list shows all of the maps in the XMS database. If the Map List is not visible at the left of the map, click the Map Options tab as shown in **Figure 168**.
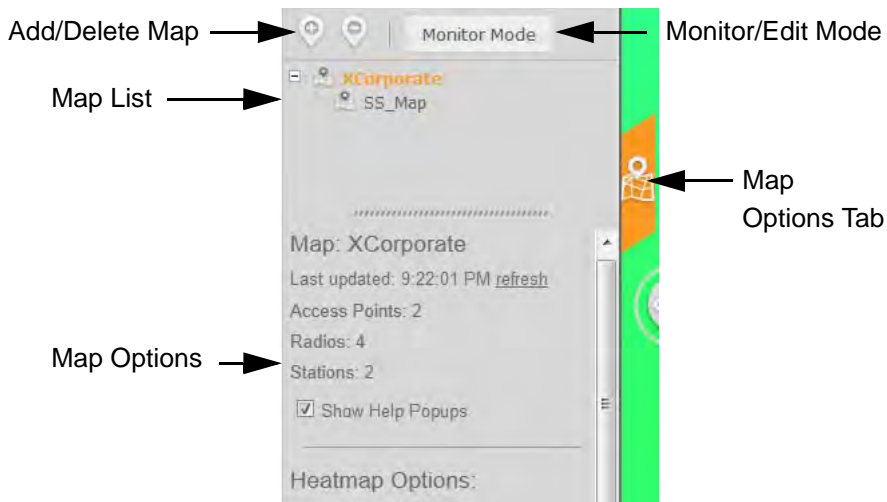
Figure 168. The Map List and Map Options Panel

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 Access Points 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 Access Point to display a popup identifying the Access Point, or double-click an Access Point to show more information about it. See **"Viewing Access Point, Station, or Rogue Details" on page 273**.
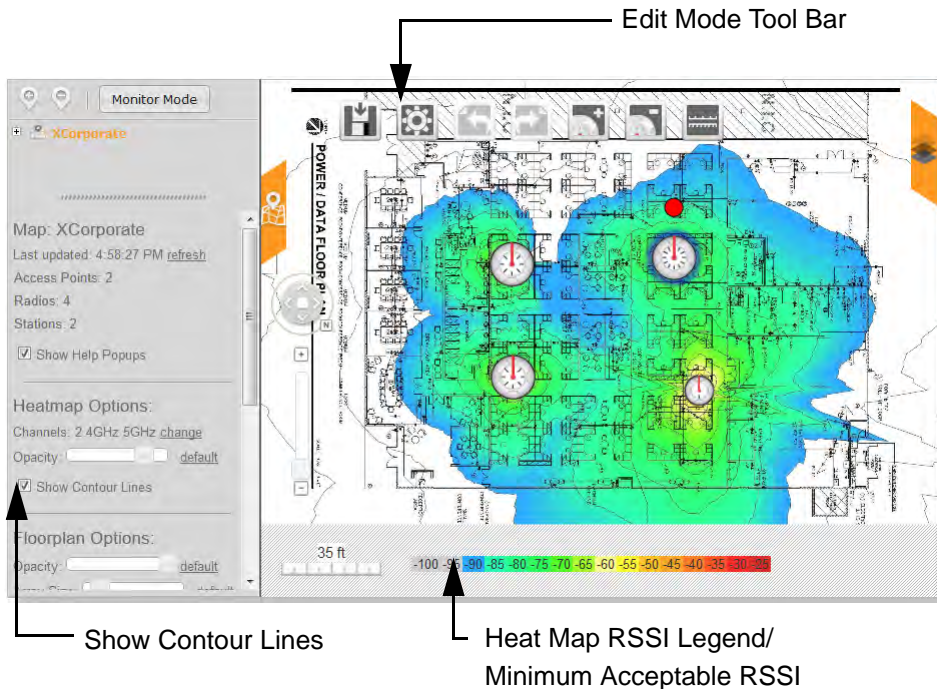
Figure 169. Main Map Showing RF Heat Contours

When enabled, RF contour lines are displayed on this map to show the strength of RF signals broadcast by each Access Point. To display contours, enable **Show Contour Lines** in **Heatmap Options** in the Map Options panel (see **"Map**

Options Panel" on page 287). If an Access Point's radios are disabled, no contours are displayed for that Access Point. 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 169**.

> *You may add any model of Xirrus Access Points to a map (see **"Adding Access Points to Maps" on page 270**). However, units that use external antennas (such as XR520H, XR-1230H, etc.) 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**.

Performance Plan Throughput Legend ⌐

Figure 170. 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 290** to set the characteristics of your network.

In addition, settings on the Access Point 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 Access Points 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

XMS maps have two modes of operation:

- **Edit Mode**—this mode displays the **Edit Mode Toolbar** (**Figure 169**) and allows you to make basic changes to a map, such as adding, moving, orienting, and deleting Access Points, 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 Access Points. In monitor mode, you may use the **Map Options Panel** and **Map Layers Panel** to customize the map display. You may also use the **Access Point Management Panel** to manage the map's Access Points with functions such as rebooting or configuring settings on Access Points. See **"Managing Access Points Within Maps" on page 281**. The Access Point Management panel is not available in edit mode.

XMS 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 Access Point Management Panel.

Use the button shown below to change modes. (**Figure 171**) 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 171. Add/Delete a Map and Edit/Monitor Mode Buttons

Overview of Map Features

The operations available in the map window depend on your XMS account privileges and the selected map mode, as discussed above in **Map Modes of Operation and User Privileges**.

XMS offers the following map functions:

- **Add** or **Delete Map** (edit mode and monitor mode)—the plus and minus buttons provide these functions. (**Figure 171**) See **"Adding a New Map" on page 265**.

- **Edit** or **Monitor Mode**—map modes determine the operations that are available. (**Figure 171**) See **"Map Modes of Operation and User Privileges" on page 259**.

- **Map List** (edit mode and monitor mode)—select the desired map from this tree structured list. (**Figure 168**) See **"The Map List" on page 255**.

- **Access Point, Station**, or **Rogue Info**—double-click an Access Point on the map (single click a station or rogue) to show detailed information about the item. See **"Viewing Access Point, Station, or Rogue Details" on page 273**.

- **Map Options Panel** (edit mode and monitor mode)—these options affect a number of aspects of the map display. (**Figure 168**) 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 Access Point icons, and how much information to display for individual Access Point radios.

- • **Rogue Location** shows rogues that have been detected.

- • **Station Location** shows stations that are associated to Access Points.

- • **Channel Configuration** performs an automatic channel configuration on Access Points.

See **"Map Options Panel" on page 287** 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 167**)

- • **Floorplan**
- • **Heatmap**
- • **Performance Plan**
- • **Access Points**
- • **Radio Info**
- • **Stations**
- • **Rogues**
- • **Map Scale**

See **"Map Layers Panel" on page 295** for a detailed discussion of the Map Layers panel.

● **Access Point Management Panel** (monitor mode only)—allows you to perform the following operations on the selected Access Points:

- • **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.

- **Power** allows you to perform Power On, Power Off, and Power Cycle (power off, then on again).

- **More** offers Add to Group and Delete operations, and allows access to the Access Point's WMI.

  See **"Managing Access Points Within Maps" on page 281** 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 285**.

Migrating Maps from Earlier Releases

When you upgrade your XMS server, any maps that you have already created are automatically migrated to new maps that are compatible with the current XMS 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 XMS 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 267**
- **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.

XMS 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 XMS 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

XMS allows you to add maps. Existing maps are displayed in the Maps list. Note that the currently selected map is highlighted in orange.
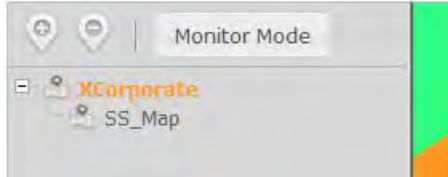
Figure 172. Maps List

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 263**.

2. Click the **Add Map** button above the Maps List. (You do not need to be in edit mode to add a map. XMS 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.
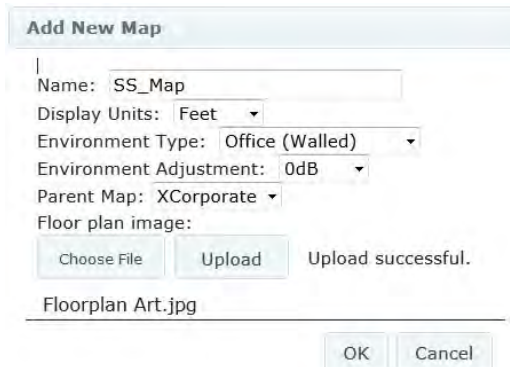
Figure 173. Add New Map Window

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. XMS 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 the Xirrus *Wi-Fi Access Point User's Guide.*

    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 XMS client). Click **Upload**.

9. Click **OK** to create the new map. If you were not already in edit mode, XMS 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.
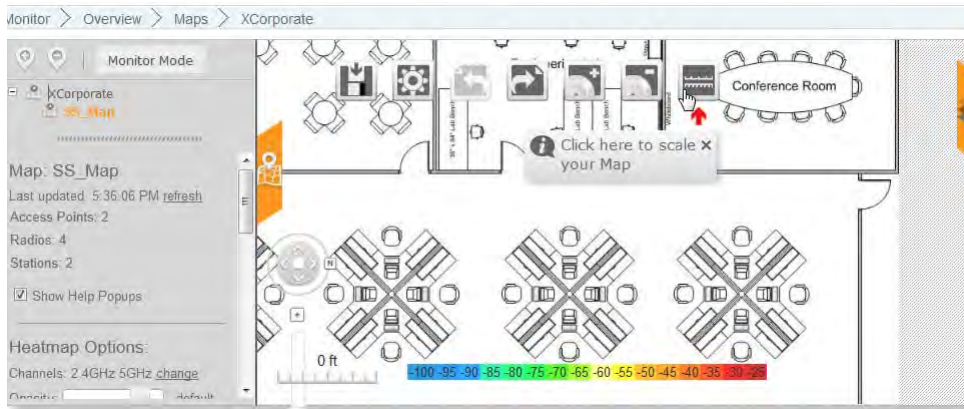
Figure 174. New Map (showing prompt for scaling the map)

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 XMS direct you.

- **"Setting the Map Scale and North Direction" on page 267**
- **"Adding Access Points to Maps" on page 270**

To work with the Access Points that you have placed on the map, see **"Managing Access Points Within Maps" on page 281**.

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. Some Access Points (XR models) 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.
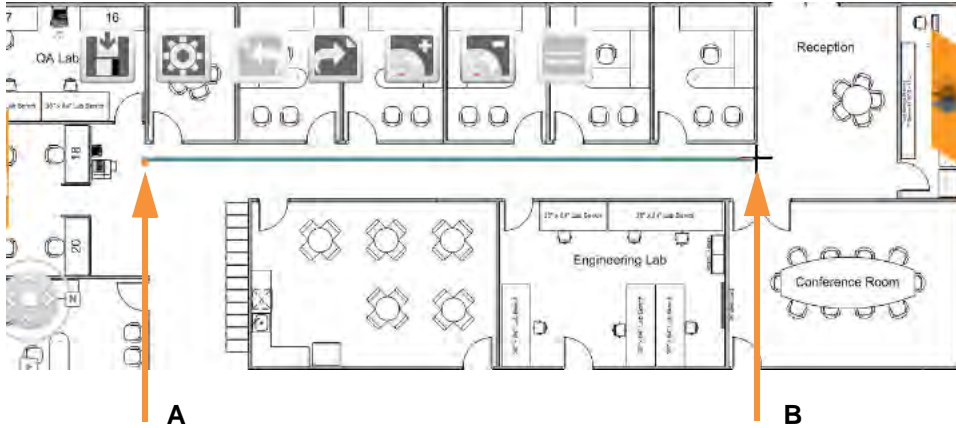
Figure 175. Calibrating the Map Scale

1. Measure a wall or other feature that is represented accurately on the map. **Figure 175** 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.
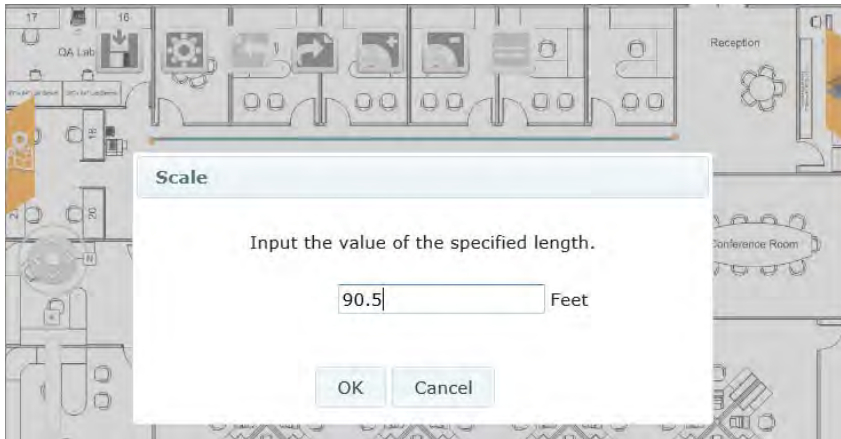
Figure 176. Edit Map Scale

4. Enter the measured length of the wall. Click **OK**.

5. Now XMS prompts you to set North on the map.

Click and drag "N" until it points to the direction of North at your site.

Figure 177. XMS 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.

XMS will now prompt you to add Access Points to the map.

Adding Access Points to Maps

After you create a map and set its scale and set its north, the next step is to add Access Points to the map, locating them to match their physical locations as closely as possible. Each Access Point may only belong to one map at a time.

The procedure below describes how to add an Access Point to the map, move it, or delete it.

To add an Access Point to the map, use the following procedure.

1. Click the **Add Access Points** button. ![icon] XMS displays the **Select Access Points** list.

2. Check the desired Access Points in the **Select Access Points** list as shown in **Figure 178**. If an Access Point already belongs to another map, it will not be shown on this list. If you need to add such an Access Point to this map, you will need to explicitly delete it from its current map first.

3. Click to select Access Points from the list.

Figure 178. Adding Access Points to a Map

4. Click the **OK** button when done.

    The Access Points will appear on the map, and XMS prompts you to orient the Access Points. You must rotate each Access Point 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.

The red line on each Access Point indicates its orientation. For XR Access Point models, this line shows the orientation of radio **iap1**. Note that XMS may automatically determine the orientation of XR models with respect to the map. In this case you do not need to explicitly orient them. If the orientation is inaccurate or the Access Point does not support this feature, you should manually adjust the Access Point to correctly indicate the direction of the monitor radio.
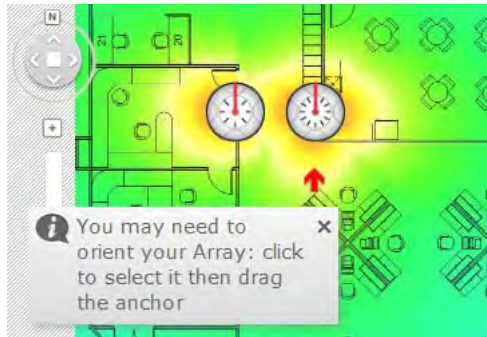
Figure 179. Access Points Added to Map

5. Click an Access Point to select it. A large red dot appears outside the Access Point, indicating its orientation. Drag the red dot to the desired angle.
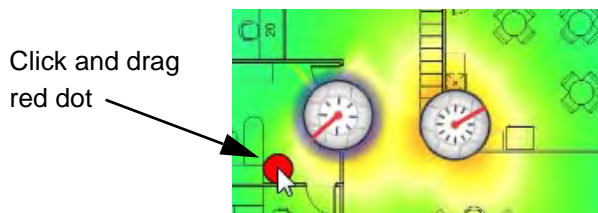
Figure 180. Orienting an Access Point

6. Move the Access Points to the proper location on the map. Click each Access Point and drag it to the desired position.

7. To remove one or more Access Points from the current map, select them and click the **Remove Access Points** button. You will be ask to verify the deletions. This will remove Access Points from the map without deleting them from the XMS database.

8. 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 XMS server.

XMS will prompt you to save the map before it will allow you to switch to another web client page.

Viewing Access Point, Station, or Rogue Details

If you hover the mouse over an item on the map (Access Point, station, or rogue), XMS will show the hostname of the device and its IP address (or MAC address for rogue devices). To see additional information about an Access Point, double-click it (single click a station or rogue). The details shown differ according to the type of device.

Access Point Details

Double-clicking on an Access Point allows you to select from three tabs showing general Access Point **Info**, **Station Count**, or **Station Throughput**. (**Figure 181**) This is an abbreviated presentation of the same information that is shown on the **Access Point 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 Access Point Details** link on the **Info** tab. For a description of any of the information presented on these tabs, please see **"Access Point Details" on page 73**.
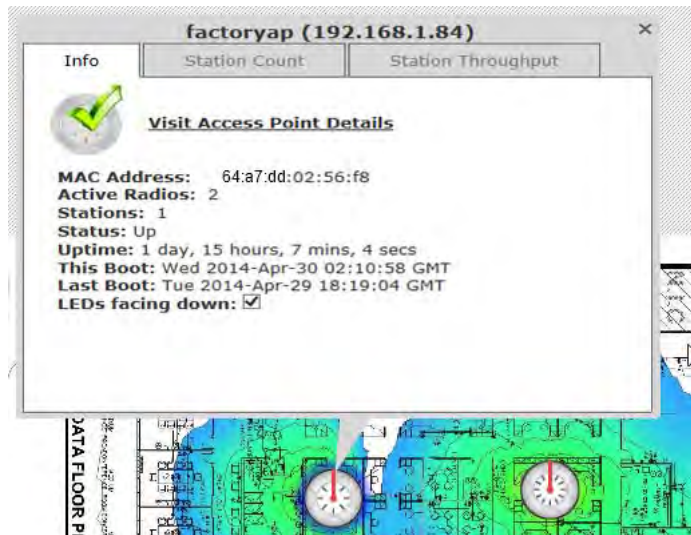
Figure 181. Map Access Point Details

Station Details

Clicking on a station allows you to select from two tabs showing general **Info** or **Throughput**. (**Figure 182**) 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 92**.
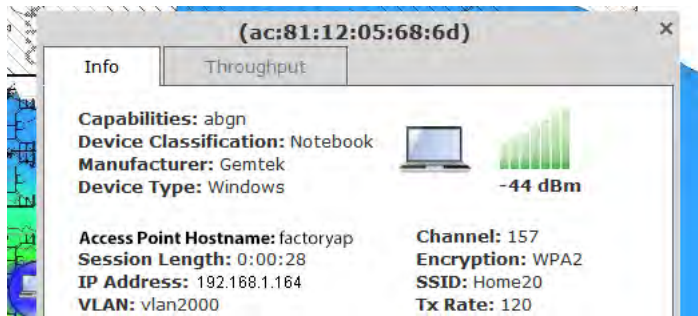
Figure 182. Map Station Details

Rogue Details

Clicking on a rogue shows general **Info** about the rogue. (**Figure 183**) 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 98**.
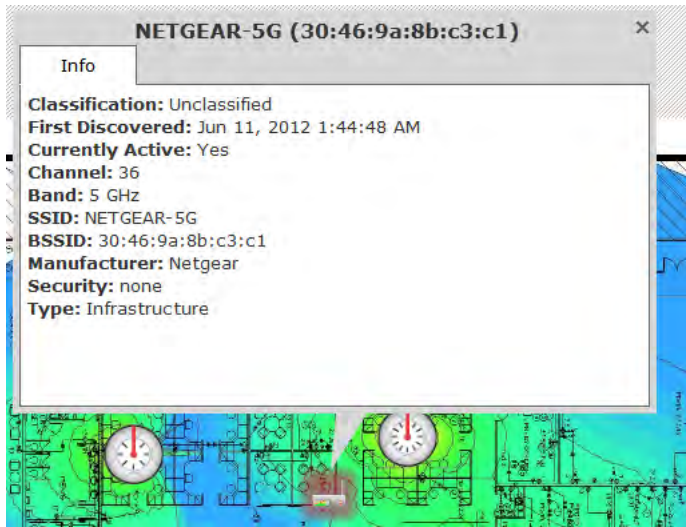
Figure 183. Map Rogue Details

Locating Devices

The XMS Location feature leverages the RF capability of the wireless Access Point 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. XMS Location is available for stations that are associated to an Access Point that is a member of a map. For accuracy, this feature requires at least three Access Points, and the station or rogue should be located inside the region formed by the Access Points.

Located Station
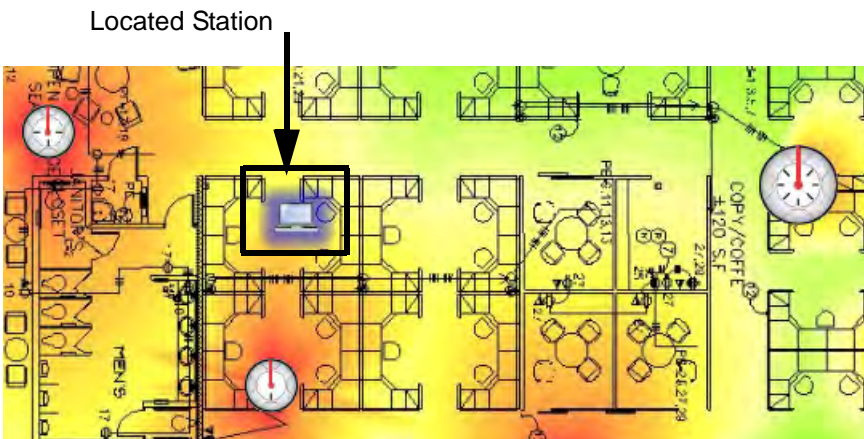
Figure 184. Using the Location Feature

The location feature is described in the following sections:

- **Understanding Locationing**
- **Preparing to Use XMS Location**
- **Using XMS Location**

Understanding Locationing
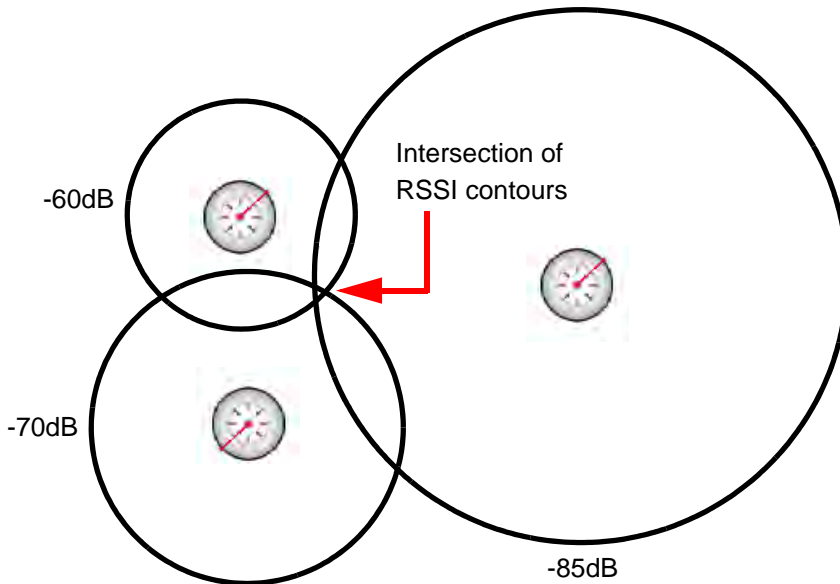
Figure 185. Determining Position

XMS 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 Access Point 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 Access Point. A simplified representation of this is illustrated in **Figure 185**, showing the RF contour of the observed signal strength as a circle around the Access Point. Each circle shows possible locations of a station, based on that Access Point's signal strength observation. In the diagram, if there were only two Access Points reporting, the circles would intersect at two points, giving two possible locations for that station. When you add additional Access Point observations, the intersection of the circles defines the station's most likely location. Actually, XMS has much more information than a simple radius (circle) to work with, due to the advanced design of the WiFi Access Point. The Access Point'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-Access Point correction and take RF attenuation due to building construction into account.

Preparing to Use XMS Location

You must complete the following steps before locating a device to get the best results.

- **Planning**—XMS is able to locate a device most accurately when Access Points are located around the perimeter of the area to be monitored, as shown in **Figure 184 on page 276**. This is in contrast to placement of Access Points for greatest Wi-Fi coverage, where we recommend that you place Access Points away from exterior walls.

- **Adding a New Map**—Create an XMS 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 Access Points to Maps**—As you place your Access Points on the map, be certain to get their locations as precise as possible. XMS will only locate stations that are associated to an Access Point that is a member of a map. The orientation of the Access Points must also be as accurate as possible.

Using XMS 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 XMS location algorithm will locate a selected station that is associated to an Access Point on a map or a selected rogue that has been detected by an Access Point 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. XMS determines which map contains the Access Point to which the station is associated (for a rogue, it finds a map that has an Access Point that detected the rogue). That map window will be displayed, and the location of the station or rogue is displayed. See **Figure 184 on page 276**. You may click the station or rogue to see detailed information about it, as described in **"Viewing Access Point, Station, or Rogue Details" on page 273**.

4. If the associated Access Point is not a member of any map, an error message will inform you of this problem. You must add the Access Point 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 XMS 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 287**.

2. To display stations, see **"Station Location" on page 293**.

3. To display rogues, see **"Rogue Location" on page 292**.

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.
   XMS 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 Access Points Within Maps

The map offers management functions for the Access Points 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 Access Points from the map.

1. The map must be in Monitor Mode to perform Access Point management. Click the **Monitor Mode** button if necessary to switch to this mode. See **"Map Modes of Operation and User Privileges" on page 259**.

2. Select the Access Points that you wish to manage. You may use Ctrl + click to select multiple Access Points.

3. Click the tab as shown in **Figure 186** to display the Access Point Management Panel, which lists all of the available Access Point operations.
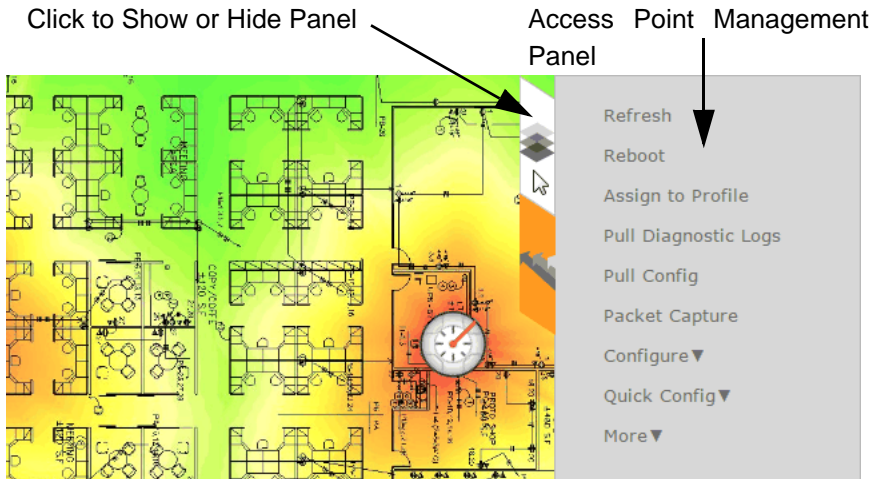
Figure 186. Access Point Management Panel

4. Select the desired operation from the Access Point 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 Access Points that you selected on the map.

The Access Point operations are summarized below. Please see **"The Configure Access Points Toolbar" on page 119** for detailed usage information.

- **Refresh**—this option refreshes discovery on the selected Access Points.

- **Reboot**—this option reboots the selected Access Points. You will be asked to confirm the operation.

- **Assign to Profile**—this option adds the selected Access Points to a profile.

- **Pull Diagnostic Logs**—this option initiates a task that instructs the selected Access Points 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 Access Points, containing each Access Point'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 Access Points. See **"About Packet Capture" on page 124**.

- **Configure** — select an option from this drop-down list to configure the selected Access Points.

  - You may modify **Network Settings** as described in **"Configure Network Settings" on page 159**.

  - You may modify **Radio Settings** as described in **"Configure Wireless Settings" on page 155**.

  - The **Optimize Channels** option computes the best channel assignments for the selected Access Points in the local RF environment. See **"RF Spectrum Management (Auto Channel Configuration)" on page 566**. The map is actually the best place to perform an auto channel. Since the map has information locating where the Access Points are in relationship to each other, auto

channel is performed on the Access Points in the correct order to yield the best results. The options for auto channel are described in **"Channel Configuration" on page 293**.

✎ *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 Access Point 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 Access Points within earshot. It does this by determining how many Access Points 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 Access Points Toolbar" on page 119**.

- **Enable/Disable Application Control**—this feature analyzes the application usage on your Access Point. Use these links to turn this feature on or off. See **"Application Control—Overview" on page 112** for more information. Application Control is only available on an Access Point 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 Access Point for high density settings such as lecture halls, convention centers, stadiums, etc.

- **Power**—select an option from this drop-down list to control power on the selected Access Points. Actually, these commands are implemented by controlling the Power over Gigabit Ethernet (PoGE) injector that powers each target Access Point. These functions may only be applied to Access Points that are powered by managed PoGE injectors, and that already have mappings configured as described in**"Managing PoGE injectors with XMS" on page 142**. You may choose to **Power On** or **Power Off** the selected Access Points. The **Power Cycle** option will turn power off and back on again, thus rebooting the Access Point.

- **More**

  - Choose the **Add to Access Point Group** option to add the selected Access Points 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 211**.

  - Choose **Access Point WMI** to open a WMI session with the Access Point in a new browser window.

  - Choose the **Delete** option from the **More** drop-down list to delete the selected Access Points from the XMS database.

  - Choose the **Take AP(s) Out of Service** option from the **More** drop-down list to mark the selected Access Points 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 XMS 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 XMS 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 Access Points. See **"Create Custom Actions" on page 620** for more information.

Zooming or Moving the Map

The zoom and move controls (**Figure 187**) are located at the lower left of the map window.
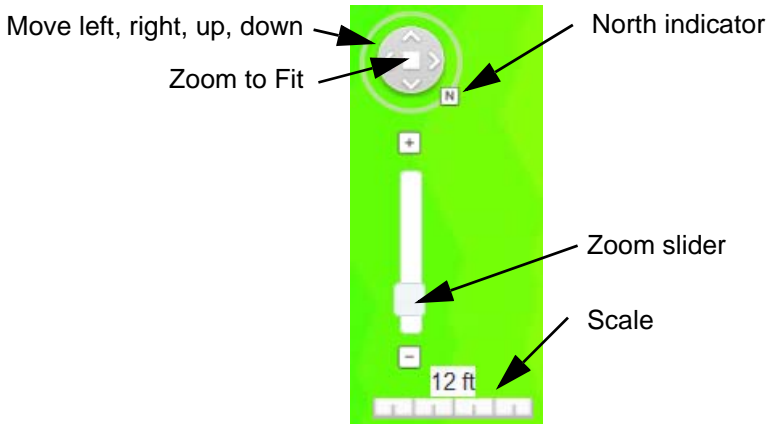
Figure 187. Map Zoom and Move Controls

Moving the Map

There are two ways to move the map:

- Click the arrow controls shown in **Figure 187** 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 187** to zoom in or out.
- Use the mouse wheel to expand or shrink map size.
- Click the Zoom to Fit square shown in **Figure 187** 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 259**.

Save Map

Map Settings

Scale Map

Remove Access Points

Add Access Points

Redo

Undo
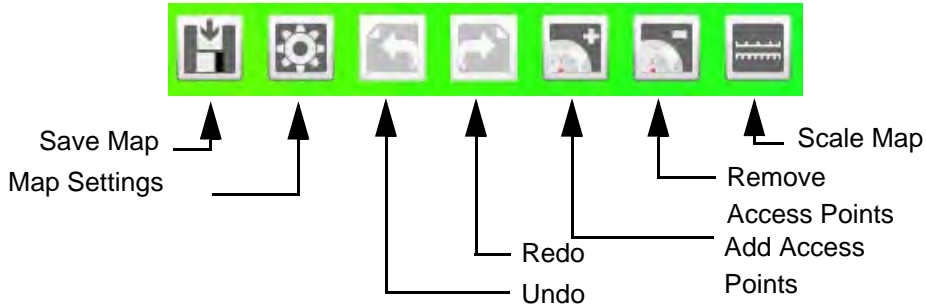
Figure 188. Map Edit Mode Toolbar

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 272**.

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 265**.

Undo
Click to undo the last change to a map, for example to undo the removal of an Access Point. 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 Access Point

Click to add Access Points to a map, as described in **"Adding Access Points to Maps" on page 270**.

Remove Access Points

Click to remove the selected Access Points (one or more) from a map. Note that the Access Points 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 267**.

Map Options Panel

Figure 189. 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 259**). Click the Map Options tab to show or hide the panel. (**Figure 189**)

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 Access Points 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 Access Point icons, and how much information to display for individual Access Point radios.

- **Rogue Location** shows rogues that have been detected.

- **Station Location** shows stations that are associated to Access Points.

- **Channel Configuration** performs an automated channel allocation procedure.

Map Options

See **Figure 189**.

- 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 Access Points, 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 286** *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 Access Points, etc.).

Heatmap Options
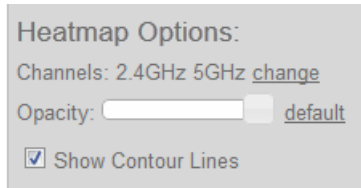
Figure 190. Heatmap Options

- **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.

Figure 191. 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 191**)

- 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 Access Point radios are also used as inputs to the predictive analysis.
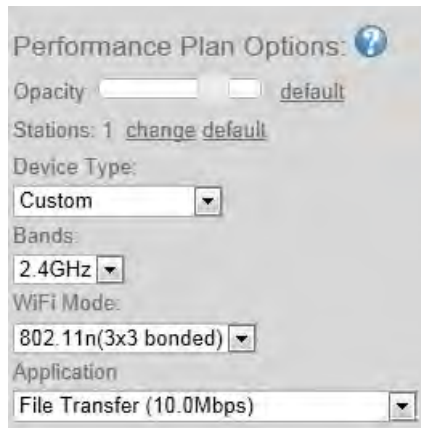
Figure 192. Performance Plan Options

● **Stations**—number of stations on the map. This starts out as the actual number of stations currently associated to Access Points 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
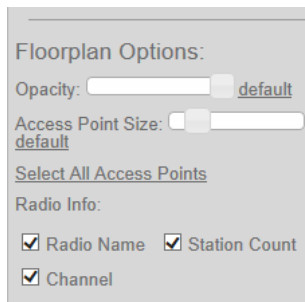
Figure 193. Map Floorplan Options

- 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 Access Point **Size** slider adjusts the display size of the Access Point icons. To restore Access Points 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 296**). You may show or hide display of **Radio Name**, **Station Count**, and **Channel** on the radios.

Rogue Location

Figure 194. Map Rogue Location Options

- Click **Locate Rogues** to show rogues that have been detected by Access Points on this map. Rogues will not be shown until you click this button. XMS 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 97** 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 Access Points on this map are set to Timeshare mode, rogue location information from these Access Points may not be sufficient to identify and locate rogues. See* **"RF Monitor" on page 564**.

Station Location
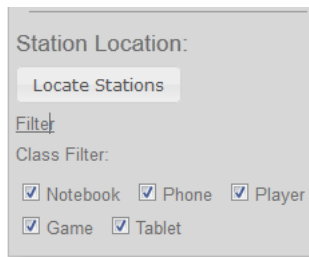
Figure 195. Map Station Location Options

- Click **Locate Stations** to show stations that are associated to Access Points on this map. Stations will not be shown until you click this button. XMS 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
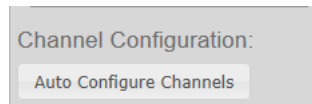
Figure 196. Auto Channel Configuration

- 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 Access Points are in relationship to each other, auto channel is performed on all of the Access Points on the map (regardless of which are selected) in the correct order to yield the best results. Each Access Point 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 197**)

- **Negotiate**: negotiate air-time with other Access Points before performing a full scan. Negotiating is slower, but if multiple Access Points are configuring channels at the same time the Negotiate option ensures that multiple Access Points 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 Access Points 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 552**.

- **Include WDS**: automatically assign 5GHz to WDS client links.

Figure 197. Map Auto Channel Options

Map Layers Panel
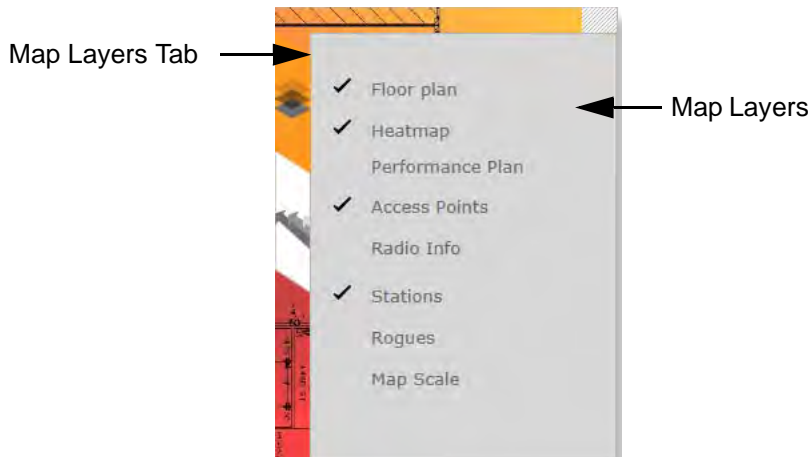
Figure 198. Map Layers Panel

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 259**). Click the Map Layers tab to show or hide the panel. (**Figure 198**) 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**
- **Access Points**
- **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 291**.

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 289**.

Performance Plan

When enabled, this layer shows predicted throughput over the map based on the type of usage you select.

Access Points

When enabled, this layer shows the location of Access Points on the map.

Radio Info
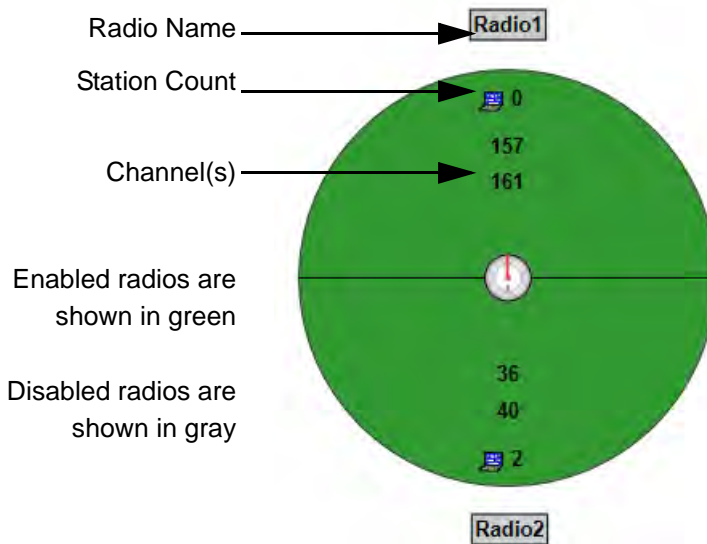
Figure 199. Radio Info Layer (XR-1000 shown)

When enabled, this layer shows each Access Point's radios on the map. Active radios are green, disabled radios are gray, and radio failure is shown in red. (**Figure 199**) 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 291**.

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 XMS 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 279**.

- 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 279**.

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 XMS 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 279**.

- 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 279**.

Map Scale

If you wish to show the map scale, you must enable this.

Managing Reports

XMS generates performance reports about the network, all wireless Access Points within the network, the individual radios contained within each Access Point, 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 299**
- **"Application Control Reports" on page 319**
- **"Traffic Reports" on page 332**
- **"Station Reports" on page 362**
- **"Access Point Reports" on page 391**
- **"RF Reports" on page 399**
- **"Security Reports" on page 402**

> ✎ *Note that smaller APs that use the AOSLite system software, such as the XR-320 and X2-120, 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 Access Points. 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 Access Points 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 105** and **"Events" on page 108**.

Sample reports shown in this chapter may show multiple Access Points managed by XMS. In some cases you may see examples where only one Access Point is under management. The results are the same regardless of how many Access Points are being addressed.

Topics for this section include:

- **"View Reports" on page 301**
- **"Viewing a Report" on page 303**
- **"Create Report" on page 307**
- **"Selection Criteria" on page 314**
- **"Customize Report Header" on page 318**

The data in most reports is delayed by 30 minutes. Exceptions are Access Point Inventory, Access Point 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.
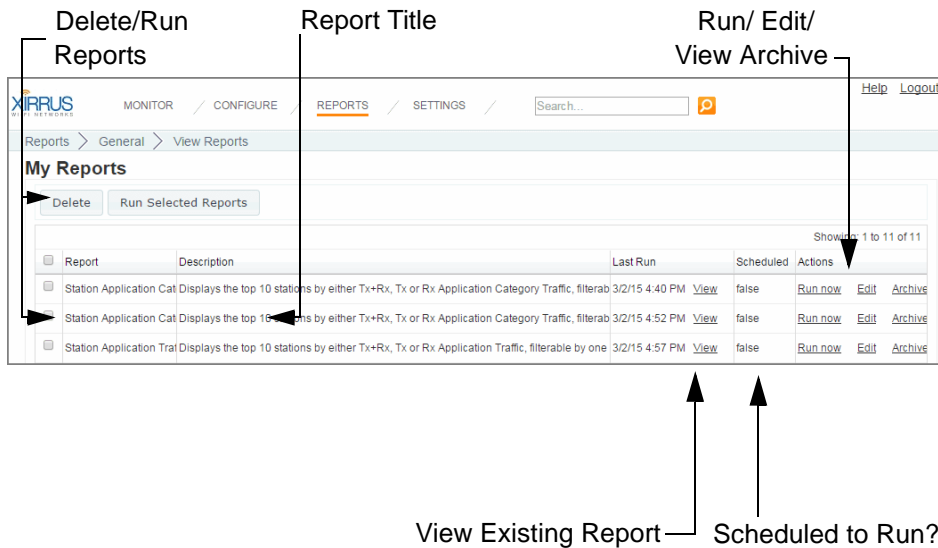
Figure 200. View Reports Window

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 303**).

- **Scheduled**—**true** indicates that the report has been scheduled to run at some time in the future.

Figure 201. Actions for Reports

- **Actions (Figure 201)**—this column allows you run or edit this report, or see all of its saved runs.
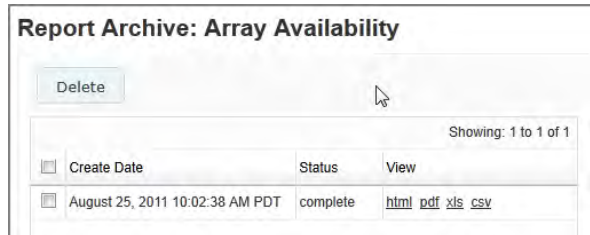
  Click **Run Now** to start a report immediately. The **Report Queue** page will be displayed, showing the status of the report. You may go to other web client pages to perform tasks while the report is generated. Generating reports may take some time on large Access Point networks.

  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 314**. 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 202**) 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 303** for more details. You may click the **Delete** link in front of a report if you wish to remove it.

Figure 202. Archived Reports List

Viewing a Report
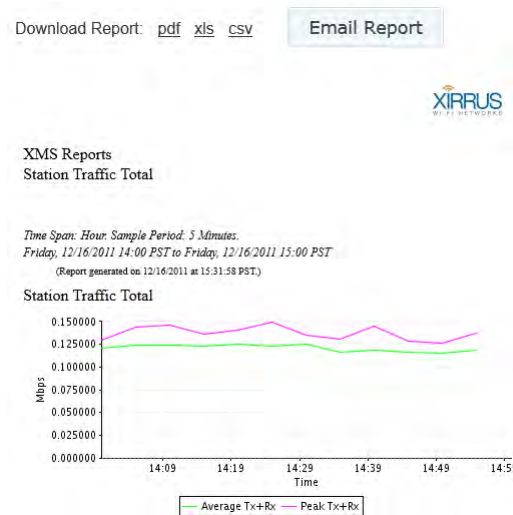
Figure 203. Viewing a Report

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 203**)

- 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 202**.

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 203**), while others may include charts (**Figure 204**). Information included in the report is determined by the **Selection Criteria** that you set up when creating the report.

Figure 204. 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 sample period will be longer. Short reporting periods, such as six hours, will be more granular and will have a shorter sample period.

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 205**) (Note that this button may not be displayed if you have not specified a mail server that XMS can use to send emails, as described in **"Email Settings" on page 632**.)

Figure 205. 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, Array Scope, Array Network, Map, Array

Application Traffic
Displays Tx and Rx averages or peak total Wireless Application Traffic, filterable by one or more Applications, Array Scope, Array Network, Map, Array and V

Station Application Category Traffic
Displays the top 10 stations by either Tx+Rx, Tx or Rx Application Category Traffic, filterable by Application Category, Array Scope, Array Network, Map and

Station Application Traffic
Displays the top 10 stations by either Tx+Rx, Tx or Rx Application Traffic, filterable by one or more Applications, Array Scope, Array Network, Map and Array.

Traffic Reports

Top Arrays by Wired Traffic
Displays the top arrays by wired traffic, filterable by Array Scope, Array Network and Map.

Top Arrays by Wireless Traffic
Displays the top arrays by wireless traffic (no management traffic), filterable by Array Scope, Array Network, Map, Device Class, and Device Type.

Wireless Traffic
Displays Tx and Rx average or peak wireless megabits per second, filterable by Array Scope, Array Network, Map, Array, and IAP.

Wireless Errors
Displays total wireless drops and errors, filterable by Array Scope, Array Network, Map, Array, and IAP.

Station Traffic
Displays Tx and Rx average or peak station megabits per second, filterable by Array Scope, Array Network, Map, Array, SSID, IAP, Device Class, and Devic

Station Errors
Displays total station error and retry rates, filterable by Array Scope, Array Network, Map, Array, IAP, SSID, Device Class, and Device Type.

Ethernet Traffic
Displays Tx and Rx averages or peak total Ethernet megabits per second, filterable by Array Scope, Array Network, Map, Array, and VLAN.

Ethernet Errors
Displays total Ethernet drops and errors, filterable by Array Scope, Array Network, Map, Array, and VLAN.

Top Station Types by Throughput
Displays the top station by traffic (Tx+Rx Mbps), filterable by Array Scope, Array Network, Map, Array, Device Class, and Device Type.

Station Reports

Stations by Wi-Fi Band
Displays a count of stations by Wi-Fi Band, filterable by Array Scope, Array Network, Map, Array, Device Class, and Device Type.

Station Counts by SSID
Displays a pie chart and table of unique station counts by SSID, filterable by Array Scope, Array Network, Map, Array, Device Class, and Device Type.

Station Activity Over Time Period
Displays a list of stations, total session time, total tx megabits, and total rx megabits, filterable by Array Scope, Array Network, Map, Array, SSID, Device Clas

Station Sessions
Displays a list of sessions for stations, filterable by Array Scope, Array Network, Map, Array, Device Class, and Device Type.

Station Classification
Displays stations by unique device class, filterable by Array Scope, Array Network, Map, Array, Device Class, and Device Type.

Station Manufacturers
Displays stations by manufacturer, filterable by Array Scope, Array Network, Map, Array, Device Class, and Device Type.

Station Assurance
Displays a list of Station Assurance events, filterable by Array Scope, Array Network, Map, Array, Station Assurance Event Type, Device Class, and Device T

Associated Stations
Displays Array-to-Station association counts over time, filterable by Array Scope, Array Network, Map, Array, IAP, Device Class, and Device Type.

Stations by Array
Displays Array-to-Station association counts, filterable by Array Scope, Array Network, Map, IAP, Device Class, and Device Type.

Unique Station Count
Displays unique wireless station counts, filterable by Array Scope, Array Network, Map, Array, SSID, Vlan, Media, Association Type, Device Class, Wi-Fi Ba

Array Reports

Array Inventory
An inventory of Arrays, filterable by Array Scope, Array Network, and Map.

Array Availability

Figure 206. 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 207**)

Figure 207. 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 309**
- **"To create a report" on page 311**
- **"Report Queue" on page 313**

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 Access Points or Access Point groups to include in the report. For details, see **"Selection Criteria" on page 314**. 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 Access Points by Wired Traffic**—shows the ten Access Points with the highest level of wired traffic.

- **Top Access Points by Wireless Traffic**—shows the ten Access Points 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 Access Point gigabit Ethernet ports.

- **Ethernet Errors**—total drops and errors for the Access Point 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 Access Point-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 Access Point**—Access Point-to-Station association counts.
- **Unique Station Count**—wireless station counts.

Access Point Reports

These reports display information about managed Access Points and their reliability statistics.

- **Access Point Inventory**—an inventory of Access Points.
- **Access Point Availability**—table of Access Point availability statistics.
- **Grouped Access Point Availability**—table of uptime percentage by profile or Access Point 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.

XMS 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 Access Points 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 314**.

● **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 XMS will use to send the email. Please see **"Email Settings" on page 632**.

● 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 208. 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 307**. 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 **Access Point Group** and a particular radio, the report will show results for just the selected radio on all Access Points 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.

- **Access Point Scope**—the drop-down list shows all of the profile networks and Access Point groups that you have defined in XMS. Select

an entry to report on just the Access Points that are members of the group or profile, or select **All Access Points**. For more information, see **"Access Point Groups" on page 126** or **"Profiles" on page 126**.

- **Map**—the drop-down list shows all of the maps that you have defined in XMS. Each map may have multiple Access Points located on it, and an Access Point may only belong to one map. Select a map to report on just the Access Points that are assigned to the map, or select **All Maps**. For more information, see **"Working with Maps" on page 251**.

- **Access Point**—the drop-down list shows all of the Access Points being managed in XMS. Select an Access Point to report on just that one Access Point, or select **All Access Points**. You cannot make more than one choice from the drop-down list. If you have selected a Group, then this list will only contain Access Points 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 Access Point **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: Access Point **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 6 Hours**, then the report will include data from the six hours 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 Access Points wirelessly, then the client device class is Access Point.

  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.

- **Exclude Out of Service APs**—select **Yes** from the drop-down list to completely omit all APs that are out of service when computing results.

- **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 Access Points: **802.11b, 802.11n**, etc. Select a mode to report on just data for Access Point 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 87**.

- **SSID**—the drop-down list shows all of the SSIDs that you have defined in XMS. Select an SSID to report on just data for that one SSID, or select **All SSIDs**. For more information, see **"SSID" on page 89**.

- **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 XMS. 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 433**.

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 209**)n
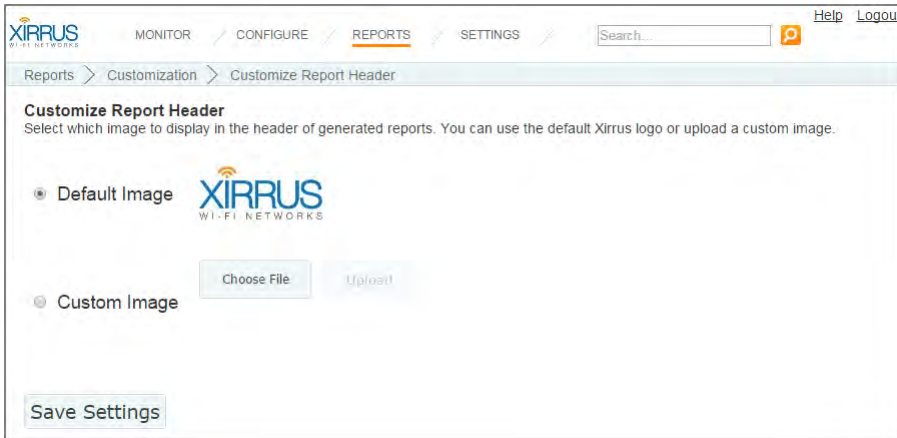
Figure 209. Customize Report Header Page

Select **Default Image** to use the default Xirrus 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 XMS does not impose a particular size limit on the image file, but the Xirrus 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 Access Points by the selected applications. Each XR Access Point uses Deep Packet Inspection (DPI—available only on XR Access Points) to determine what applications are being used, and how much bandwidth they are consuming. For more information, see **"Application Control—Overview" on page 112**.

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 Access Points whose licenses include **Application Control**. See* **"About Licensing and Upgrades" on page 200***.*

  *In order for an Access Point to produce Application Control data, you must enable the **Application Control** option in the **Configure** menu on the Access Points **Toolbar**. See* **"The Access Points Toolbar" on page 73***.*

Application Category Traffic

This report provides statistical data for wireless traffic flow generated by a selected category of applications. (**Figure 210**) The graph at the top of the window displays wireless traffic for that category, summed over the selected Access Points for the selected time range.

A table shows traffic generated by this application category on each Access Point. 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 Access Points capable of generating application control data.

Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
Category	Include only traffic for the selected category of applications, such as File Transfer or Social Networking.
Access Point Scope	Include only Access Points that are members of the selected Access Point group or profile.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

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.

Figure 210. Application Category Traffic Report

Table Details for the Application Category Traffic Report

The table portion of the report shows traffic statistics for each selected Access Point, organized by the following column headers:

- **Access Point Hostname**
  The host name assigned to the Access Point. Only Access Points that meet your selection criteria are included.

- **Access Point MAC Address**
  This is the Access Point's MAC address.

- **Management IP Address**
  This is the Access Point'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 Access Points for the selected time range (**Figure 211**).

A table shows traffic generated by each application on each Access Point. 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 Access Points capable of generating application control data.

Selection Criterion	Description (see **"Selection Criteria" on page 314** 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.
Access Point Scope	Include only Access Points that are members of the selected Access Point group or profile.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 314** for details)
Schedule	Run the report at this time. See **"Schedule" on page 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

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.

Figure 211. 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 Access Point, organized by the following column headers:

- **Access Point Hostname**
  The host name assigned to the Access Point. Only Access Points that meet your selection criteria are included.

- **Access Point MAC Address**
  This is the Access Point's MAC address.

- **Access Point IP Address**
  This is the Access Point'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 212**) 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 Access Points 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. Note that the report includes only Access Points capable of generating application control data (i.e., XR Series Access Points running AOS Release 6.4 or higher). If you select other Access Points, they will not generate any information for this report.

Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
Category	Include only traffic for the selected category of applications, such as File Transfer or Social Networking, or select **All**.
Access Point Scope	Include only Access Points that are members of the selected Access Point group or profile.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

Figure 212. 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 Access Points 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/Access Point** 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 213**) 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 Access Points 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. Note that the report includes only Access Points capable of generating application control data (i.e., XR Series Access Points running AOS Release 6.4 or higher). If you select other Access Points, they will not generate any information for this report.

Selection Criterion	Description (see **"Selection Criteria" on page 314** 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.
Access Point Scope	Include only Access Points that are members of the selected Access Point group or profile.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.

Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

Figure 213. 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 Access Points 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/Access Point** 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 Access Points are designed to handle Gigabit Ethernet speeds.

With their high-speed capability, your Access Points can easily handle time-sensitive traffic, such as voice and video. The high capacity XR-6000 Series Wireless Access Point has four Gigabit uplink ports, an optional 10 Gigabit fiber connection, and up to 16 radios, providing a maximum wireless capacity of up to 7.2 Gbps, which offers ample reserves for the high demands of current and future applications.

> ✎ *Note that smaller APs that use the AOSLite system software, such as the XR-320 and X2-120, 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 Access Points by Wired Traffic**
  Shows the ten Access Points with the highest level of wired traffic.

- **Top Access Points by Wireless Traffic**

  Shows the ten Access Points with the highest level of wireless traffic (not including management traffic).

- **Wireless Traffic**

  Shows wireless throughput statistics for Access Points.

- **Wireless Errors**

  Shows wireless error statistics for Access Points.

- **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 Access Points.

- **Ethernet Errors**

  Shows Ethernet error statistics for Access Points.

- **Top Station Types by Throughput**

  Shows station types generating the highest traffic demand (Tx+Rx Mbps).

Top Access Points by Wired Traffic

This report displays the ten Access Points with the highest level of wired traffic, based on the traffic flow through the Gigabit ports on each wireless Access Point for the selected time period. (**Figure 214**) The bar chart at the top of the window identifies the Access Points (among the set you selected) with the highest throughput on the wired ports for the selected time range. If you selected less than ten Access Points, then all of them will be shown.

A table shows throughput on the wired ports for each Access Point managed by XMS (not just the selected Access Points). 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 314** for details)
Access Point Scope	Include only Access Points that are members of the selected Access Point group or profile.
Map	Include only Access Points 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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

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.

Figure 214. Top Access Points by Wired Traffic Report

Table Details for the Top Access Points by Wired Traffic Report

The table portion of the report shows throughput for all managed Access Points (not just the selected Access Points), organized by the following column headers:

- **Access Point Hostname**

   The host name assigned to the Access Point. Only Access Points that meet your selection criteria are included.

- **Throughput (Mbps)**

   Shows the throughput (in megabits per second) achieved by the Access Point's wired ports for the time period you specified.

Top Access Points by Wireless Traffic

✎ *Note that smaller APs that use the AOSLite system software, such as the XR-320 and X2-120, do not contribute data to all reports. In particular, they do not generate any radio (wireless) statistics.*

This report shows the ten Access Points with the highest level of wireless traffic for the selected Access Points and devices (not including management traffic). The bar chart at the top of the window identifies the Access Points (among the set you selected) with the highest wireless throughput for the selected time range. If you selected less than ten Access Points, then all of them will be shown (**Figure 215**).

A table shows wireless throughput for each Access Point. 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 314** for details)
Access Point Scope	Include only Access Points that are members of the selected Access Point group or profile.
Map	Include only Access Points 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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

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.

Figure 215. Top Access Points by Wireless Traffic Report

Table Details for the Top Access Points by Wireless Traffic Report

The table portion of the report shows throughput for the selected Access Points, organized by the following column headers:

- **Access Point Hostname**
  The host name assigned to the Access Point. Only Access Points that meet your selection criteria are included.

- **Throughput (Mbps)**

  Shows the wireless throughput (in megabits per second) achieved by the Access Point for the devices and time period you specified.

Wireless Traffic

✎ *Note that smaller APs that use the AOSLite system software, such as the XR-320 and X2-120, 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 Access Point. (**Figure 216**) The graph at the top of the window displays wireless data summed over the selected Access Points for the selected time range.

A table shows throughput for each Access Point, 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.

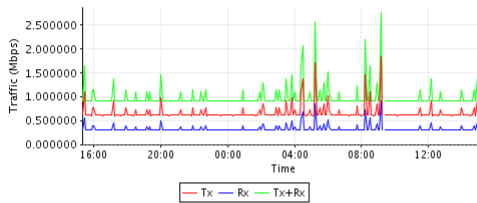| Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
Access Point Scope	Include only Access Points that are members of the selected Access Point group or profile.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

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.

XMS Reports
Wireless Traffic Tx+Rx

Time Span: Day
Wednesday, 04/13/2011 01:32 PDT to Thursday, 04/14/2011 01:32 PDT

Wireless Traffic Tx+Rx

Wireless Traffic Tx+Rx

Row Count: 13

Array Hostname	Array IP Address	IAP Name	IAP MAC Address	Min (Mbps)	Max (Mbps)	Avg (Mbps)
XN16520901140	10.100.54.26	abgn1	00:0f:7d:07:46:20-2e	0.000	0.000	0.000
XN16520901140	10.100.54.26	abgn2	00:0f:7d:07:46:60-6e	0.000	0.000	0.000
XN16520901140	10.100.54.26	abgn3	00:0f:7d:07:46:a0-ae	0.000	0.000	0.000
XN16520901140	10.100.54.26	abgn4	00:0f:7d:07:46:e0-ee	0.000	0.000	0.000
XN16520901140	10.100.54.26	an1	00:0f:7d:07:46:10-1e	0.000	0.000	0.000
XN16520901140	10.100.54.26	an10	00:0f:7d:07:46:d0-de	0.000	0.000	0.000
XN16520901140	10.100.54.26	an11	00:0f:7d:07:46:f0-fe	0.000	0.000	0.000
XN16520901140	10.100.54.26	an12	00:0f:7d:07:46:00-0e	0.000	0.000	0.000

Figure 216. 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 Access Points, organized by the following column headers:

- **Access Point Hostname**
  The host name assigned to the Access Point. Only Access Points that meet your selection criteria are included.

- **Access Point IP Address**
  This is the Access Point's IP address.

- **Radio Name**
  Each radio in each Access Point 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 XR-320 and X2-120, 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 Access Point radios in the XMS managed network, based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
Access Point Scope	Include only Access Points that are members of the selected Access Point group or profile.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

Access Point errors reported are packet error rate, packet retry rate, and encryption retry rate, shown as a percentage of the total number of packets. (**Figure 217**) The graph shows the weighted average wireless error percentages for all Access Points, 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:

- **Access Point Hostname**

  The host name assigned to the Access Point.

- **Access Point MAC Address**

  This is the Access Point's MAC address.

- **Access Point IP Address**

  The IP address assigned to the Access Point.

- **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.
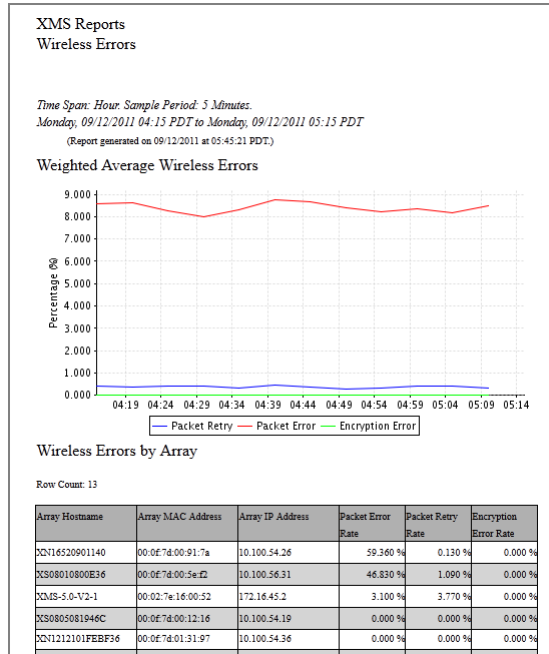
Figure 217. Wireless Errors Report

- **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 XR-320 and X2-120, 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 Access Points. Throughput summed over all stations is represented in a graph at the top of the window (**Figure 218**). 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 314** for details)
Access Point Scope	Include only Access Points that are members of the selected Access Point group or profile.
Map	Include only member Access Points of the selected map.
Access Point	Include only the selected Access Point.
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 314** 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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

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:

● **Access Point Hostname**
The host name of the Access Point 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, Access Point**/WDS Link** are shown here.
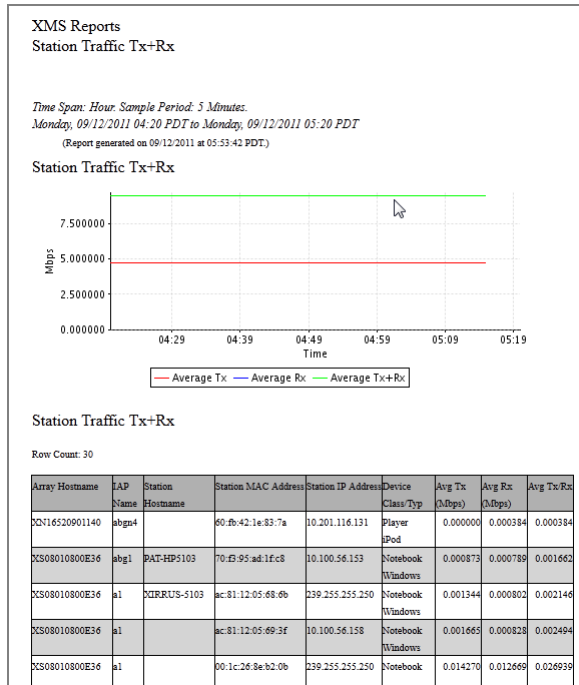
Figure 218. Station Traffic Report (Tx+Rx)

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 XR-320 and X2-120, 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 XMS, based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
Access Point Scope	Include only Access Points that are members of the selected Access Point group or profile.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

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 219** shows an

example of the error report for stations. The graph shows the packet error and packet dropped error percentages for all Access Points.

Table Details for the Station Errors Report

The results shown in this report are organized by the following column headers:

- **Access Point Hostname**
  The host name of the Access Point 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.
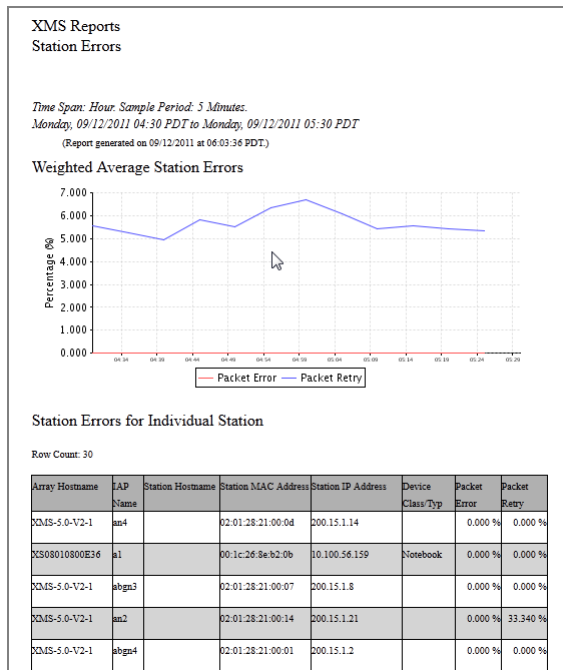
Figure 219. Station Errors Report

- **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, Access Point**/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 Access Points. (**Figure 220**) The graph at the top of the window displays aggregate data throughput across all Access Points for the selected time range.

A table shows average and peak Ethernet rates for each Access Point. 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 314** for details)
Access Point Scope	Include only Access Points that are members of the selected Access Point group or profile.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

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.
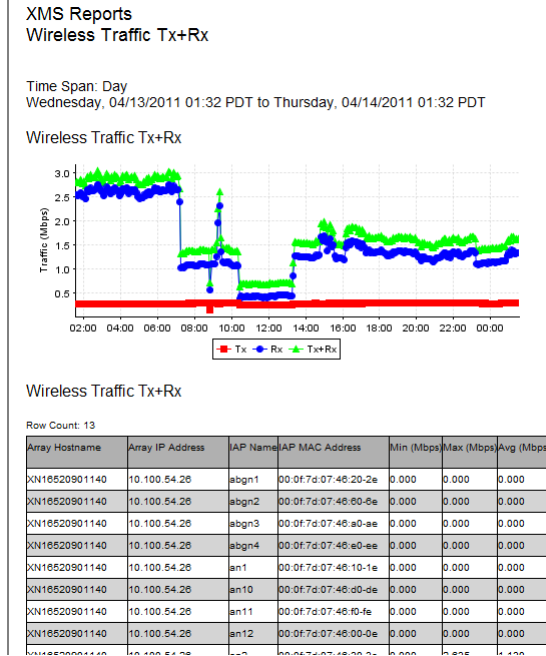
XMS Reports
Ethernet Traffic Tx+Rx

Time Span: Hour. Sample Period: 5 Minutes.
Monday, 09/12/2011 04:40 PDT to Monday, 09/12/2011 05:40 PDT
(Report generated on 09/12/2011 at 06:11:11 PDT.)

Ethernet Traffic Tx+Rx

Ethernet Traffic Tx+Rx

Row Count: 13

Array Hostname	Array MAC Address	Management IP Address	Average Tx (Mbps)	Average Rx (Mbps)	Average Tx/Rx (Mbps)
XMS-5.0-V2-1	00:02:7e:16:00:52	172.16.45.2	4.466340	4.462006	8.928346
XN0414091C4EB	00:0f:7d:00:92:2d	10.100.54.21	0.005430	0.023282	0.028712
XN08310800F3E	00:0f:7d:00:26:08	10.100.54.121	0.008573	0.026257	0.034830
XN1212101FEBF36	00:0f:7d:01:31:97	10.100.54.36	0.155149	0.153944	0.309093
XN123810220A3	00:0f:7d:01:95:b1	10.100.54.29	0.011262	0.031034	0.042296
XN16520901140	00:0f:7d:00:91:7a	10.100.54.26	0.032497	0.049330	0.081827
XR4012601C5B6	00:0f:7d:01:c5:b6	10.100.54.55	0.007456	0.031036	0.038492

Figure 220. 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 Access Points, organized by the following column headers:

- **Access Point Hostname**

  The host name assigned to the Access Point. Only Access Points that meet your selection criteria are included.

- **Access Point MAC Address**

  This is the Access Point's MAC address.

- **Management IP Address**

  This is the Access Point'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 Access Point for the time period you specified.

- **Average Rx (Mbps)**
  Shows the average receive throughput (in megabits per second) achieved by the Access Point for the time period you specified.

- **Average Tx+Rx (Mbps)**
  Shows the average total throughput (in megabits per second) achieved by the Access Point 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 Access Point for the time period you specified.

- **Peak Tx/Rx (Mbps)**
  Shows the maximum total throughput (in megabits per second) achieved by the Access Point for the time period you specified.

Ethernet Errors

This report shows Ethernet communication errors for the Gigabit ports for Access Points in the XMS managed network, based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
Access Point Scope	Include only Access Points that are members of the selected Access Point group or profile.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

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 221)**
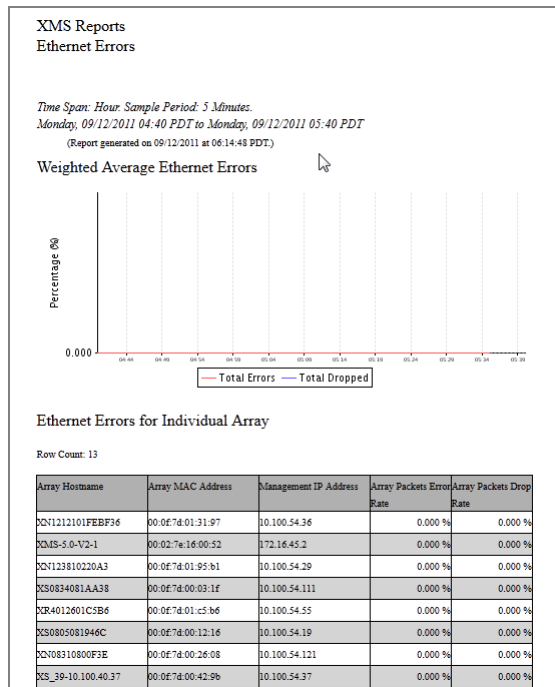
Figure 221. Ethernet Errors Report

Table Details for the Ethernet Errors Report

The results shown in this report are organized by the following column headers:

- **Access Point Hostname**
  The host name assigned to the Access Point.

- **Access Point MAC Address**
  This is the Access Point's MAC address.

- **Management IP Address**
  The IP address assigned to the Access Point.

- **Access Point 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.

- **Access Point 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 XR-320 and X2-120, 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 Access Points at any time during the specified time period.

Note that if you are using Wireless Distributed System (WDS) links to carry traffic between Access Points wirelessly, client link stations will be included. These stations can be recognized by their **Device Class** and **Type**—Access Point and **WDS Link**.

The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
Access Point Scope	Include only member Access Points of the selected Access Point group.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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.

Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
Schedule	Run the report at this time. See **"Schedule" on page 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

Use the bar chart for an at-a-glance overview of the station devices generating the most traffic in your wireless network.
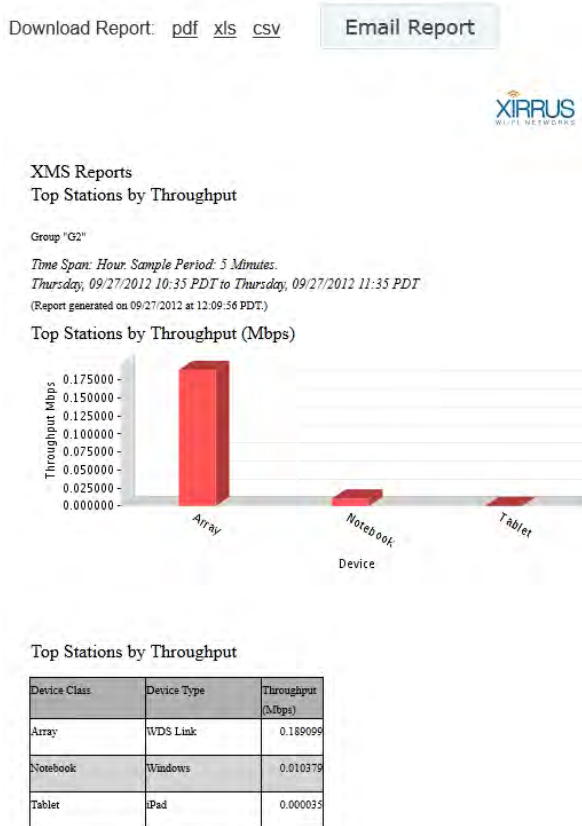
Figure 222. Top Station Types by Throughput Report

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, Access Point 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 Access Point includes a number of radios, with each radio capable of associating up to 96 client stations. And because XMS can support many Access Points, the number of clients that can be associated may be quite large. Note that typically, the monitor radio is enabled for monitoring only (default), and client stations cannot associate with this radio.

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 Access Points.

- **Stations By Access Point**

  Allows you to review station association data based on selected Access Points, 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 Access Points at any time during the specified time period. A pie chart shows the distribution of stations by band. (**Figure 223**)

The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
Access Point Scope	Include only member Access Points of the selected Access Point group.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

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.
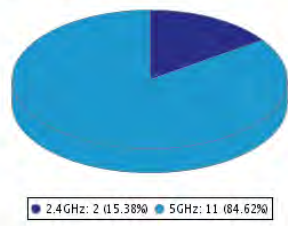
Figure 223. Stations by Wi-Fi Band Report

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 Access Points at any time during the specified time period. A pie chart shows the distribution of SSID usage. (**Figure 224**)

If you are using WDS links to carry traffic between Access Points wirelessly, client link stations will be included. The **Device Class** and **Type** of these stations are Access Point and **WDS Link**, respectively.

The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
Access Point Scope	Include only member Access Points of the selected Access Point group.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

Use the pie chart for an at-a-glance overview of the proportion of stations using each SSID.

Figure 224. 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 Access Points 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 Access Points wirelessly, client link sessions will be displayed. These sessions can be recognized by their **Device Class** and **Type—Access Point** and **WDS Link**.

The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
Access Point Scope	Include only member Access Points of the selected Access Point group.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

XMS Reports
Station Activity Over Time Period

Time Span: Hour. Sample Period: 5 Minutes.
Monday, 09/30/2013 14:55 PDT to Monday, 09/30/2013 15:55 PDT
(Report generated on 09/30/2013 at 16:29:51 PM PDT)
Station Activity Over Time Period

Row Count: 5

Station MAC Address	Station Hostname	Device Class/Type	SSID	Total Session Duration	Tx (Mb)	Rx (Mb)
00:1e:65:6c:08:5a	LSCHILDER-M750B	Notebook Windows	xirrus	3 days 6 hrs 41 min 17 sec	4.69	1.85
14:5a:05:2f:72:1f			xirrus	7 hrs 52 min 24 sec	1.68	0.38
34:c0:59:77:bb:5c	AdamDavsiPhone6	Phone iPhone	xirrus	2 hrs 10 min 36 sec	34.89	3.30
5c:96:9d:49:4d:44			xirrus		0.00	0.00
b4:f0:ab:b4:88:be	iPhone	Phone iPhone	xirrus	46 sec	0.00	0.00

Figure 225. 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, Access Point/**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 six hours. If a station was associated during that interval 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 Access Points wirelessly, client link sessions will be displayed. These sessions can be recognized by their **Device Class** and **Type**—Access Point and **WDS Link**.

The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
Access Point Scope	Include only member Access Points of the selected Access Point group.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

XMS Reports
Station Sessions

Time Span: Month. Sample Period: 2 Hours.
Wednesday, 12/07/2011 14:00 PST to Friday, 01/06/2012 14:00 PST
(Report generated on 01/06/2012 at 15:40:01 PST.)

Station Sessions Chart

Sessions shorter than 1 Min: 23 (23.47%)
Sessions between 1 Min – 5 Min: 32 (32.65%)
Sessions between 5 Min – 15 Min: 16 (16.33%)
Sessions between 15 Min – 30 Min: 7 (7.14%)
Sessions between 30 Min – 1 Hr: 4 (4.08%)
Sessions between 1 Hr – 1 Day: 8 (8.16%)
Sessions longer than 1 Day: 8 (8.16%)

Station Sessions Table

Row Count: 98

Station MAC Address	Station Hostname	Station IP Address	Array Hostname	Array IP Address	Device Class/Type	Time Associated and Session Duration
00:05:4e:4e:ef:8f	XIRRUS-3AABFBA9	10.100.56.163	XS08010800E36	10.100.56.31	Notebook Windows	Dec 20 2011 16:12:27 23 hrs 38 min 34 sec
00:05:4e:4e:ef:8f	xirrus-3aabfba9	10.100.56.169	XS08010800E36	10.100.56.31	Notebook Windows	Dec 3 2011 11:54:53 7 days 1 hrs 43 min 6 sec
00:06:5b:23:00:01		10.100.44.11	XR6000	10.100.44.185		Dec 20 2011 17:00:19 3 min 53 sec
00:06:5b:23:00:04		10.100.44.14	XR6000	10.100.44.185		Dec 20 2011 17:10:17 8 min 26 sec
00:06:5b:23:00:05		10.100.44.15	XR6000	10.100.44.185		Dec 20 2011 17:05:41 2 min 18 sec

Figure 226. 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.

- **Access Point Hostname**
  The host name of the Access Point to which the station is associated.

- **Access Point IP Address**
  The IP address of the Access Point 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, Access Point**/WDS Link** are shown here.

- **Time Associated and Session Duration**
  The time that the session started (i.e., when the client associated to the Access Point), 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 Access Points 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 Access Points wirelessly, client link stations will be included. These stations can be recognized by their **Device Class** and **Type**—Access Point and **WDS Link**.

The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
Access Point Scope	Include only member Access Points of the selected Access Point group.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

Use the pie chart for an at-a-glance overview of the proportion of station device classes in your wireless network.
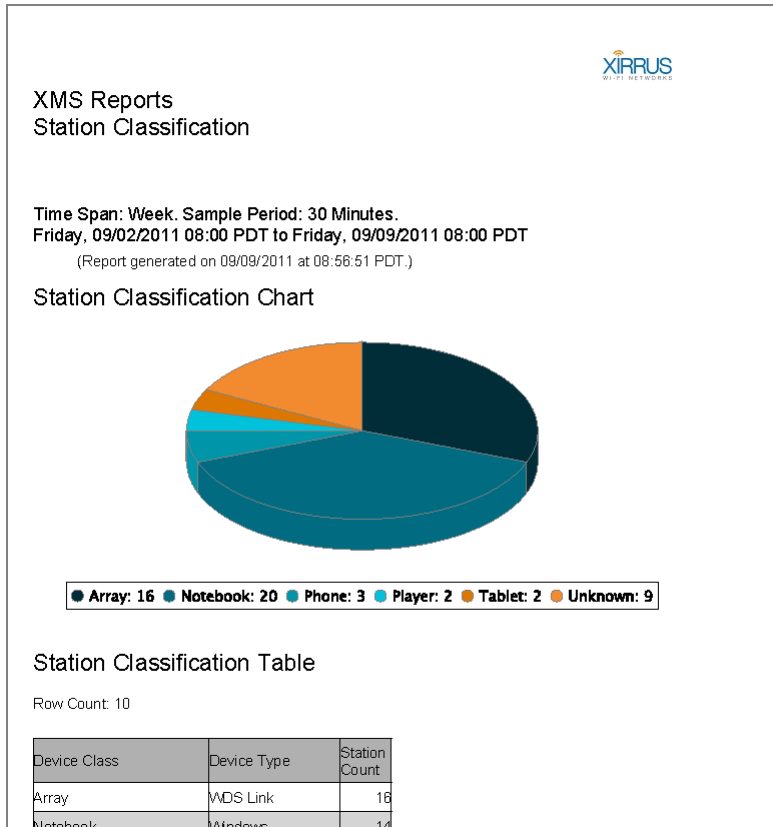
Figure 227. Station Classification Report

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, Access Point 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 Access Points 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 314** for details)
Access Point Scope	Include only member Access Points of the selected Access Point group.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

Use the pie chart for an at-a-glance overview of the proportion of manufacturers in your wireless network.

XMS Reports
Station Manufacturers

Time Span: Week. Sample Period: 30 Minutes.
Thursday, 12/29/2011 05:00 PST to Thursday, 01/05/2012 05:00 PST
(Report generated on 01/05/2012 at 05:53:12 PST.)

Station Manufacturer Chart

- Apple: 2 (22.22%)
- Gemtek: 2 (22.22%)
- HTC: 1 (11.11%)
- Intel: 1 (11.11%)
- Motorola: 1 (11.11%)
- Other: 0 (0.00%)
- Philips: 1 (11.11%)
- Universal Global Scientific: 1 (11.11%)
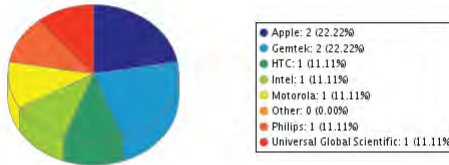
Station Manufacturer Table

Row Count: 7

Manufacturer	Device Class	Device Type	Station Count
Apple	Phone	iPhone	2
Gemtek	Notebook	Windows	2
HTC	Phone	Android	1
Intel	Notebook	Windows	1
Motorola	Unknown	Unknown	1
Philips	Notebook	Windows	1
Universal Global	Notebook	Windows	1

Figure 228. 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 Access Point. When an Access Point 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 103** in the *Wireless Access Point User's Guide* for more information.
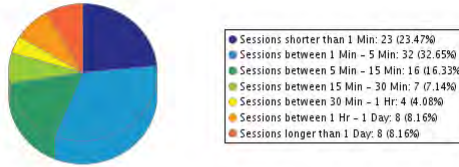
The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
Access Point Scope	Include only member Access Points of the selected Access Point group.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

Download Report: pdf xls csv

XMS Reports
Station Assurance

Time Span: Hour, Sample Period: 5 Minutes.
Sunday, 09/11/2011 22:35 PDT to Sunday, 09/11/2011 23:35 PDT
  (Report generated on 09/12/2011 at 00:05:09 PDT.)

Station Assurance Table

Row Count:
45

Array Hostname	Array IP Address	Station MAC and IP Address	Station Hostname	Type	Device Class/Typ	Start Time	End Time
XS08010800E36	10.100.56.31	00:24:d7:dd:2f:90		Data Rate	Notebook	09/09/2011 18:45:32	Currently Active
XS08010800E36	10.100.56.31	58:1f:aa:c1:e9:8c		Data Rate		09/09/2011 11:07:35	Currently Active
XN16520901140	10.100.54.26	60:fb:42:1e:83:7a		Data Rate	Player iPod	09/11/2011 23:34:26	09/11/2011 23:34:26
XN16520901140	10.100.54.26	60:fb:42:1e:83:7a		Data Rate	Player iPod	09/11/2011 19:29:26	Currently Active
XN16520901140	10.100.54.26	60:fb:42:1e:83:7a		Data Rate	Player iPod	09/11/2011 19:23:26	Currently Active
XN16520901140	10.100.54.26	60:fb:42:1e:83:7a		Data Rate	Player iPod	09/11/2011 19:18:26	Currently Active
XN16520901140	10.100.54.26	60:fb:42:1e:83:7a		Data Rate	Player iPod	09/11/2011 19:14:26	Currently Active

Figure 229. 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 Access Point to which it is associated, the type of connectivity problem, and the session start and end time.

● **Access Point Hostname**
  The host name of the Access Point to which the station is associated.

- **Access Point IP Address**

  The IP address of the Access Point 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, Access Point**/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 230**). 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 Access Points, selected radios, and/or selected device type/class.

Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
Access Point Scope	Include only Access Points that are members of the selected Access Point group or profile.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

Station Classification Chart

This pie chart provides a quick overview of Wi-Fi clients, showing the proportions of different device classes.
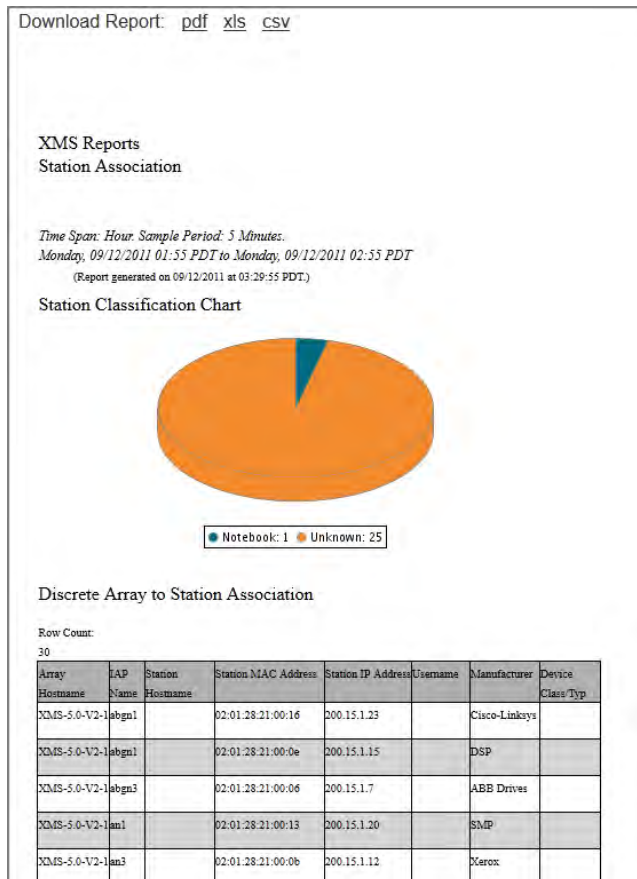
Figure 230. Station Association

Discrete Access Point to Station Association

This table presents a list of all stations associated to the selected Access Points/ radios/devices based on the time period you specify. The results shown in this window are organized by the following column headers:

● **Access Point Hostname**
The host name of the Access Point 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, Access Point**/WDS Link** are shown here.

Stations By Access Point

This report displays a bar chart showing the number of stations associated to those Access Points that have the highest station count (**Figure 231**). The table below gives minimum and maximum counts of clients per Access Point. The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
Access Point Scope	Include only Access Points that are members of the selected Access Point group or profile.
Map	Include only Access Points 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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

Total Access Point to Station Associations

This table shows the minimum and maximum number of stations that have been associated to each Access Point, with the following information:

- **Access Point Name**
  The host name assigned to the Access Point.

- **Access Point MAC Address**
  This is the Access Point's MAC address.

- **Access Point IP Address**

  The IP address assigned to the Access Point.

- **Min Stations in 5 Minutes**

  Shows the lowest number of stations concurrently associated to each Access Point 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 Access Point 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 Access Point 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 Access Point during the time period.

Xirrus 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
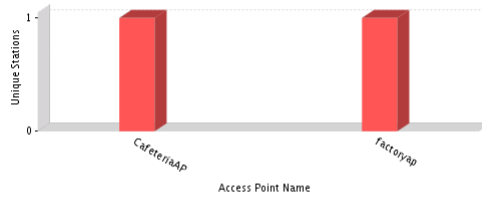
Total Access Point to Station Associations

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 231. Station Association (By Access Point) 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 314** for details)
Access Point Scope	Include only member Access Points of the selected Access Point group.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.
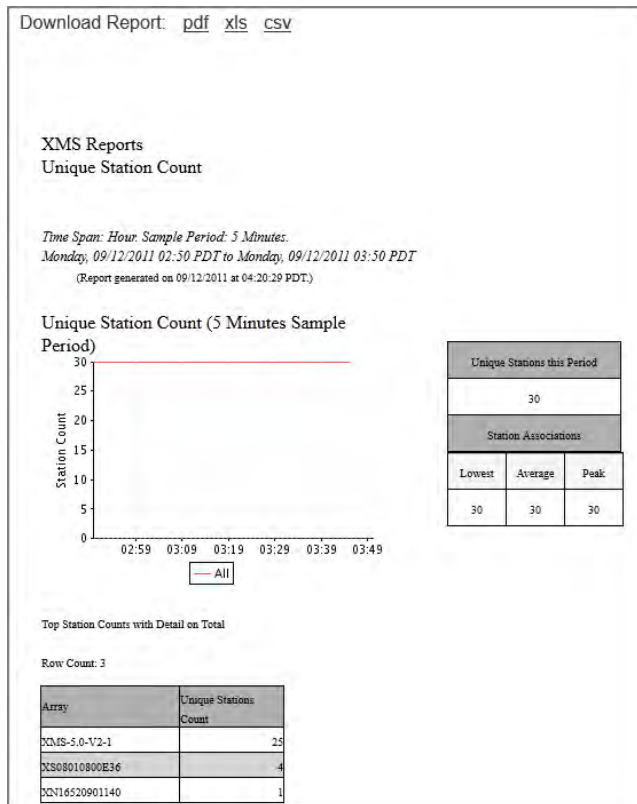
Figure 232. Unique Station Count Report

The graph is detailed on (i.e., broken out into categories by) your choice of category:

- Total—show totals only.
- Access Point Name—show station count by Access Point.
- 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 232**, 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

Access Point status reports provide utility functions, such as listing all Access Points for you and showing reliability statistics.

The following reports are available in this section:

- **Access Point Inventory**

  Provides a list of all Access Points 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 Access Points in each profile or Access Point group have been up.

Access Point Inventory

This report creates an inventory list for your use (**Figure 233**). The result is a list of all your managed wireless Access Points 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 314** for details)
Access Point Scope	Include only Access Points that are members of the selected Access Point group or profile.
Map	Include only Access Points 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 314** for details)
Schedule	Run the report at this time. See **"Schedule" on page 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

Table Details for the Access Point Inventory Report

The table portion of the report shows the name, addresses, and serial number of the selected Access Points, organized by the following column headers:

- **Access Point Hostname**

  The host name assigned to the Access Point. Only Access Points that meet your selection criteria are included.

- **Access Point MAC Address**

  This is the Access Point's MAC address.

- **IP Address**

  This is the Access Point's IP address.

- **Location**

  The physical location information that you entered for this Access Point, if any.

- **Serial Number**

  This is the Access Point's serial number.

Xirrus Reports
Access Point Inventory

(Report generated on 02/26/2016 at 11:55:10 AM PST)

Access Point Inventory

Row Count: 3

Access Point Hostname	Access Point MAC Address	Access Point IP Address	Location	Map	Serial Number
XR214120F2CC7	00:0f:7d:0f:2c:c7	10.100.86.109			XR214120F2CC7
XR21426056D54	50:60:28:05:6d:54	10.100.86.101	Thousand Oak Headoffice		XR21426056D54
XR523510084E6	50:60:28:00:84:e6	10.100.86.61			XR523510084E6

Figure 233. Access Point Inventory Report

Access Point Availability

This report shows system reliability statistics for the wireless network, based on **Selection Criteria**. **Figure 234** shows an example of the Access Point Availability report.

| Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
Access Point Scope	Include only Access Points that are members of the selected Access Point group or profile.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
Exclude Out of Service APs	Include only Access Points that are in service.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

Time Span: Date/Time. Sample Period: 5 Minutes.
Friday, 02/26/2016 10:25 PST to Friday, 02/26/2016 11:25 PST

(Report generated on 02/26/2016 at 11:59:25 AM PST)

Access Point Availability

Row Count: 3

Hostname	IP Address	Total Down Time	MTBF	MTTR	Uptime (%)
XR214120F2CC7	10.100.86.109	0 days, 0 hrs, 0 mins	0 days, 1 hrs, 0 mins	0 days, 0 hrs, 0 mins	100.0
XR21426056D54	10.100.86.101	0 days, 0 hrs, 0 mins	0 days, 1 hrs, 0 mins	0 days, 0 hrs, 0 mins	100.0
XR523510084E6	10.100.86.61	0 days, 0 hrs, 9 mins	0 days, 0 hrs, 16 mins	0 days, 0 hrs, 3 mins	84.9261

Figure 234. Access Point Availability Report

Table Details for the Access Point Availability Report

The Access Point Availability report is generated as a table. The results are organized by the following column headers:

- **Hostname**
  The host name assigned to the Access Point.

- **IP Address**
  The IP address assigned to the Access Point.

- **Total Down Time**
  Shows the total time (in minutes) that this Access Point 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 Access Point 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 Access Point 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 Access Point has been up and running successfully, based on a percentage of the total time for the time period specified for this report.

   If XMS is non-operational for a period of time, Access Point availability information for this report is extrapolated from the last known state of the Access Point prior to XMS going off-line.

Grouped Access Point Availability

This report shows system reliability statistics for your wireless network grouped by **Profiles** or by **Access Point Groups**, based on your **Selection Criteria**. **Figure 235** 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 314** for details)
Display Availability by	Show average AP availability for Access Point groups or for profiles.
Exclude Out of Service APs	Include only Access Points that are in service.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

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 235. Grouped Access Point Availability Report

Table Details for the Grouped Access Point Availability Report

The Access Point Availability report is generated as a table. The results are organized by the following column headers:

- **Profile** or **Access Point Group**

  The profile or Access Point group name for each row.

- **Access Point Count**

  The number of Access Points in this profile or Access Point group.

- **Average Uptime**

  Shows the average percentage of time that the Access Points in this profile or Access Point 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 531**. 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 314** for details)
Access Point Scope	Include only Access Points that are members of the selected Access Point group or profile.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
Table Row Limit	Total number of rows.
Schedule	Run the report at this time. See **"Schedule" on page 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

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:

- **Access Point Hostname**
  The host name assigned to the Access Point that the radio belongs to.

Figure 236. Channel Usage Report

● **Access Point IP Address**
   The IP address assigned to the host Access Point.

● **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 Access Points 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 Access Point's line rate encryption ensures high performance when encryption is in use. For more information about security, go to **"Rogues" on page 97** and **"IDS Events" on page 101**.

Security reports provide data based on the security parameters defined for your network of Access Points, 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 Access Points, please see the *Access Point User's Guide.*

The information displayed in this window is based on your **Selection Criteria**.

Selection Criterion	Description (see **"Selection Criteria" on page 314** for details)
Access Point Scope	Include only member Access Points of the selected Access Point group.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

Figure 237. IDS Events Report

Table Details for the IDS Events Report

For each IDS event included in the selection criteria, the table shows the detecting Access Point, the time and channel on which the attack occurred, and the SSID and MAC address of the attacker, if appropriate.

- **Access Point MAC Address**
  The MAC address of the detecting Access Point.

- **Access Point Hostname**
  The host name of the detecting Access Point.

- **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 Access Point (if monitoring is enabled). XMS collects this information from the Access Points in its managed network. As access points are switched off and on, the list of detected rogues changes. Please see **"Rogues" on page 97** 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 314** for details)
Access Point Scope	Include only Access Points that are members of the selected Access Point group or profile.
Map	Include only Access Points that are members of the selected map.
Access Point	Include only the selected Access Point.
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 312**.
Email Report To	After running, email the report. See **"Email Report To" on page 312**.

The chart (**Figure 238**) shows the percentages of rogue devices based on their classifications.

- **Unclassified**
  These rogues have not yet been classified.
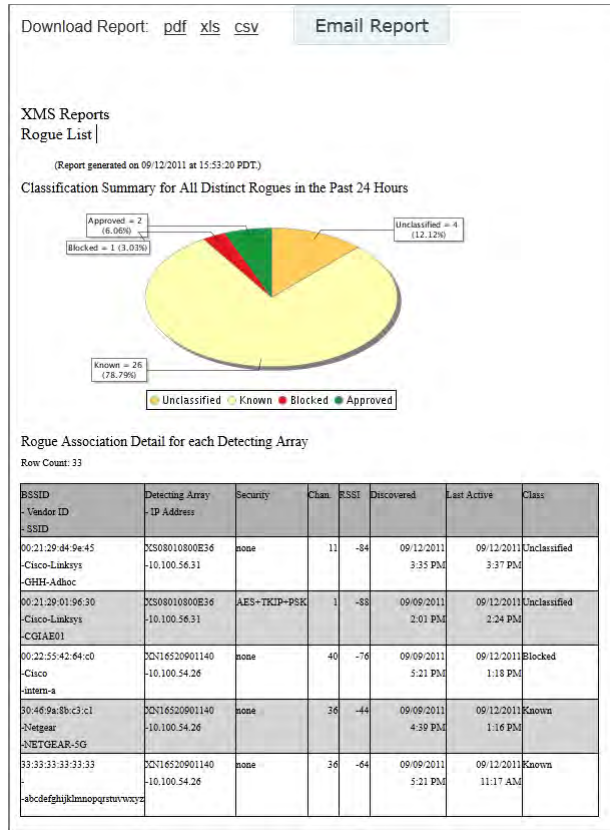
Figure 238. Rogue List Report

- **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 Access Point 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 Access Point—IP Address**
  Shows the host name and IP address of the Access Point 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 Access Point.

- **Discovered**
  This is the date and time that the rogue was discovered by the detecting Access Point.

- **Last Active**

  This is the date and time that the rogue was last seen by the detecting Access Point, or **Active** if the rogue is still active.

- **Class**

  The classification of the rogue, as defined above.

Configuring a Wireless Access Point

The following topics describe how to configure a selected Access Point using the **Configuration** tab on the Access Point Details window. This tab provides a menu with an extensive set of convenient options for changing Access Point settings.

The following WMI windows allow you to establish configuration parameters for your Access Point, and include:

✎　　*Note that smaller APs that use the AOSLite system software, such as the XR-320, 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 413**
- **"Network" on page 414**
- **"VLAN" on page 433**
- **"Services" on page 438**
- **"Security" on page 455**
- **"SSIDs" on page 486**
- **"Groups" on page 524**
- **"Radios" on page 531**
- **"Filters" on page 582**
- **"Tunnels" on page 589**

The Configuration Tab

To reach this window, select the Access Point**s** link in the Access Point **Configuration** section under **Configure** at the top of the window. You may also arrive at this window by selecting the Access Point**s** link in the **Overview** section under **Monitor** at the top of the window. Locate the desired Access Point in the list. Its **Hostname** field is a link—click it to go to the Access Point Details window, and then select the **Configuration** tab (Figure 239).

Figure 239. 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 Access Point, 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 Access Point'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 Access Point 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 Access Point, including changing its host name and license, and setting administrator contact information.

Figure 240. General Information

Procedure for Configuring General Information

1. **Hostname:** Specify a unique host name for this Access Point. The host name is used to identify the Access Point on the network. Use a name that will be meaningful within your network environment, up to 64 alphanumeric characters. The default is the Access Point's serial number.

2. **Location Information**: Enter a brief but meaningful description that accurately defines the physical location of the Access Point. 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 Access Point 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 Xirrus 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 415**
- **"AP Switch" on page 418**
- **"Bonds and Bridging" on page 421**
- **"DNS Settings" on page 429**
- **"CDP Settings" on page 430**
- **"LLDP Settings" on page 431**

Interfaces

✎ *Note that smaller APs that use the AOSLite system software, such as the XR-320 and the X2-120, 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 Access Point.

Figure 241. 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 Access Point via the selected network interface, or choose **No** to deny all management privileges for this interface. This option is only available for the Gigabit interfaces.

3. **Auto Negotiate**: This feature allows the Access Point 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. 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 Access Point to use DHCP when assigning IP addresses to the Access Point, 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 Access Point. 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 Access Point 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 Access Point 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 Access Point. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

AP Switch

This window is only available for the XR-320, 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 XR-320, enable them and configure them on this window.

Figure 242. Network Interface Settings

Procedure for Configuring AP Switch Ports (for XR-320 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 433**). 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 433**). Use the right arrow to move the VLANS to be included to the **Selected VLANS** list.

2. **Authentication**:

Figure 243. AP Switch Authentication (XR-320)

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 Access Point. 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. XR-6000 Series Access Points have four Gigabit ports, and you may specify which ports are bonded to work together as a pair. You may also select more than two ports to work together in one group.

A special option lets you configure bridging between the gigabit ports on an Access Point that has two of these ports.
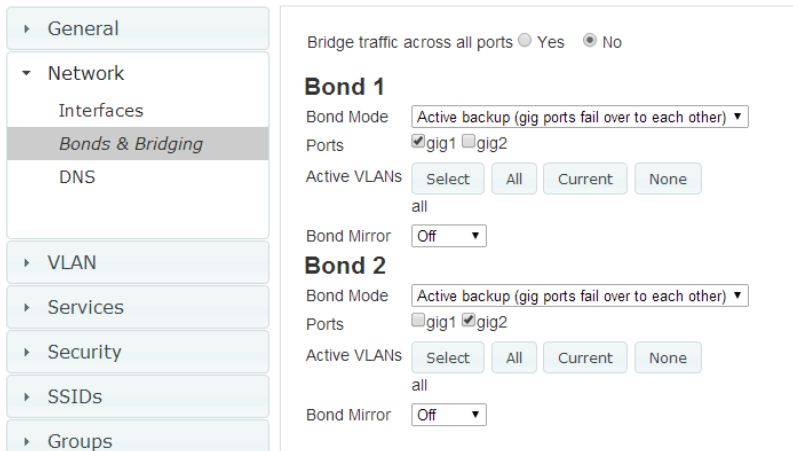
Figure 244. Network Bonds and Bridging

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 245).
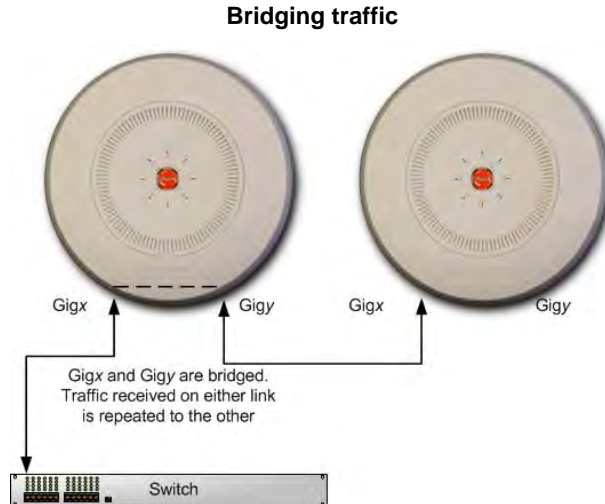
Bridging traffic

Figure 245. Bridging Traffic

This option is only available on Access Points 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 Access Point acts as a wired bridge—this allows Access Points to be chained and still maintain wired connectivity.

✎   *Each Access Point in a chain must have power supplied to its PoE port from a compatible power injector or powered switch port.* ***An Access Point does not supply power to another Access Point.***

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 Access Points, the endpoint Access Point 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 428.

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 428). In Access Points 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 Access Point 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 246 (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 Access Point would fail over traffic to the third Gigabit port.

(a) Active backup   **(b) Aggregate using 802.3ad**
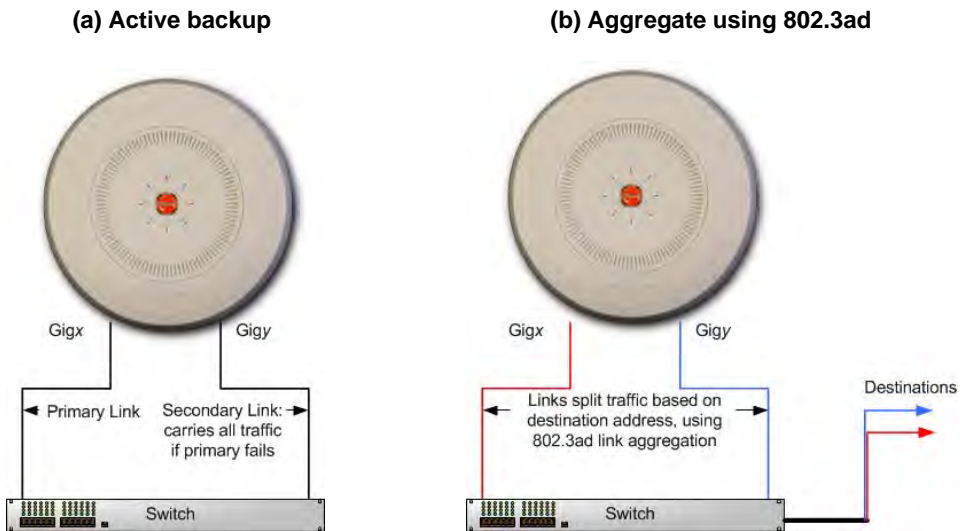
Figure 246. Port Modes (a, b)

b. **Aggregate Traffic from gig ports using 802.3ad**—The Access Point 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 246 (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 247 (c).

(c) Transmit on all ports
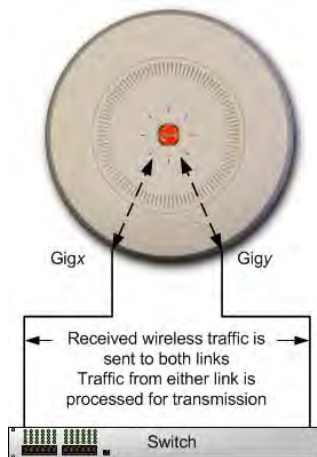
Figure 247. Port Modes (c)

(d) Load balance traffic
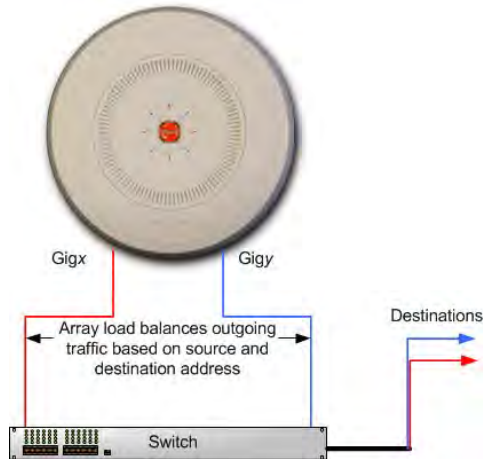
Figure 248. Port Modes (d)

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 248 (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 Access Points 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 all**. A link near the bottom allows you to **Display by VLAN name** rather than by number.
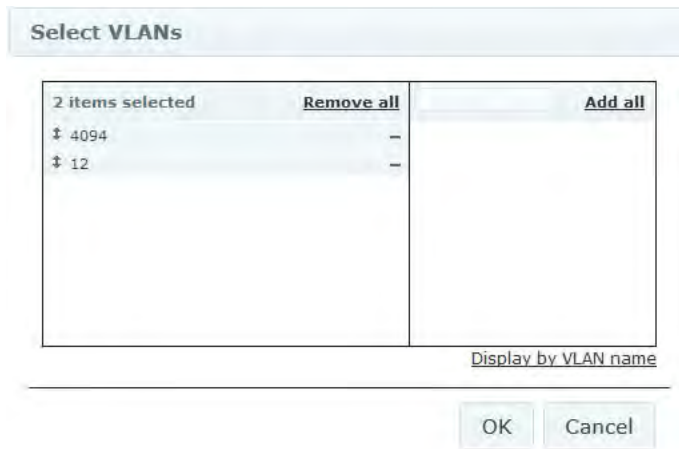
Figure 249. Select Active VLANs for this Bond

   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 433**) to be passed, click the **Current** button. Essentially, this "fixes" the Active VLANs list to contain the Access Point'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 250) All wireless traffic received on the Access Point 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.

Figure 250. Mirroring Traffic

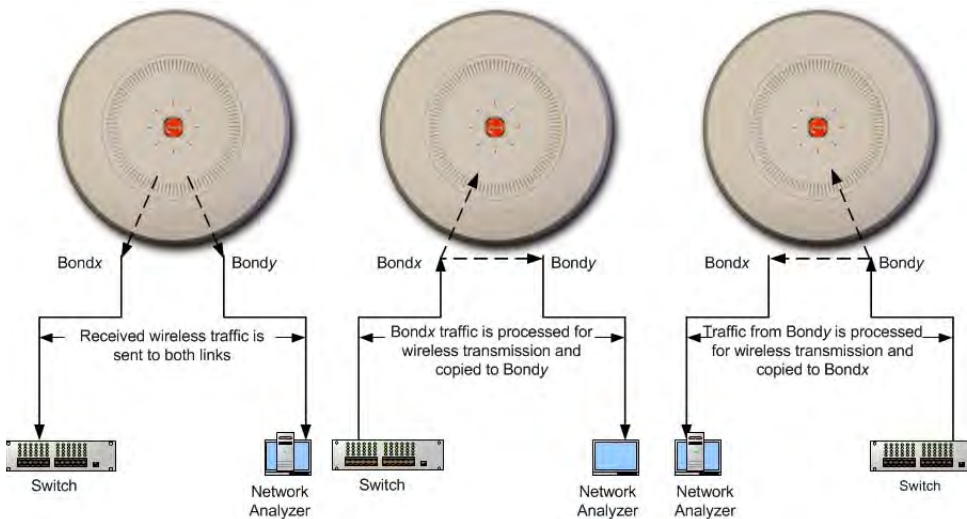7. When done configuring bonds as desired, click the **Apply Config** button at the top of the configuration window to apply these changes to the Access Point. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

DNS Settings

This window allows you to establish your DNS (Domain Name System) settings. The Access Point uses these DNS servers to resolve host names into IP addresses. The Access Point also registers its own Host Name with these DNS servers, so that others may address the Access Point using its name rather than its IP address. An option allows you to specify that the Access Point'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 Access Point are defined along with DHCP pools. See **"DHCP Server" on page 450**. At least one DNS server must be set up if you want to offer clients associating with the Access Point the ability to use meaningful host names instead of numerical IP addresses.

Figure 251. 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 Access Point's IP address, click **Yes**. The Access Point will then obtain its DNS domain and server settings from the network DHCP server that

assigns an IP address to the Access Point, rather than using the DNS Server fields above. You may also configure that DHCP server to assign a host name to the Access Point.

6. Click the **Apply Config** button at the top of the configuration window to apply these changes to the Access Point. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

CDP Settings

✐   *Note that smaller APs that use the AOSLite system software, such as the XR-320 and the X2-120, 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.*

The Cisco Discovery Protocol 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. Wireless Access Points can both advertise their presence by sending CDP announcements, and gather and display information sent by neighbors.

This window allows you to establish your CDP settings.

Figure 252. CDP Settings

Procedure for Configuring CDP Settings

1. **Enable CDP:** When CDP is enabled, the Access Point sends out CDP announcements of the Access Point's presence, and gathers CDP data sent by neighbors. When disabled, it does neither. CDP is disabled by default.

2. **CDP Interval**: The Access Point sends out CDP announcements advertising its presence at this interval. The default is 60 seconds.

3. **CDP Hold Time**: CDP information received from neighbors is retained for this period of time before aging out of the Access Point's neighbor list. The default is 180 seconds.

4. Click the **Apply Config** button at the top of the configuration window to apply these changes to the Access Point. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

✎ *CDP works on untagged interfaces. It will not always work with tagged interfaces on Cisco devices, since they might switch from using CDP to DTP on tagged trunk links.*
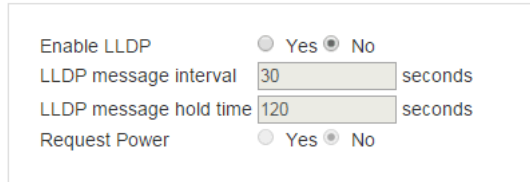
LLDP Settings

This page controls LLDP settings. Link Layer Discovery Protocol (LLDP) is a Layer 2 network protocol similar to CDP, used to share information (such as the device manufacturer and model, network capabilities, and IP address) with other directly connected network devices. Access Points can both advertise their presence by sending LLDP announcements, and gather and display information sent by neighbors. The Request Power feature allows you to ask for extra power— for example, this lets the XR-320 power its PoE AP Switch port (LAN4).

Procedure for Configuring LLDP Settings

1. **Enable LLDP:** When LLDP is enabled, the Access Point sends out LLDP announcements of its presence, and gathers LLDP data sent by neighbors. When disabled, it does neither. LLDP is disabled by default.

2. **LLDP message interval**: The Access Point sends out LLDP announcements advertising its presence at this interval. The default is 30 seconds.

Figure 253. LLDP settings

3. **LLDP message hold time**: LLDP information received from neighbors is retained for this period of time before aging out of the Access Point'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**: You must enable LLDP before enabling this feature. If Request Power is set to **Yes** and LLDP discovers a device port that supplies power to this Access Point (on a powered switch, for example), the Access Point checks that the port is able to supply the peak power that is required by this Access Point 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 Access Point 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 Access Point issues a Syslog message and keeps the radios down for ten minutes. The radios may be enabled manually after this (see **"Radio Settings" on page 533**).

Using this feature provides a more graceful way of handling an underpowered situation on a Wi-Fi device. When the radios are turned off, XMS can notify you, rather than having to hunt down an intermittent problem. This feature is disabled by default.

VLAN

A Virtual LAN (VLAN) is 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

Xirrus Access Points support Layer 2 tunneling with Virtual Tunnels. This allows an Access Point 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 Access Point has low overhead and latency for virtual tunnel connections, with high resilience. The Access Point 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 Access Point to use tunneling for a VLAN, simply enter the IP address, port and secret for the tunnel server as described in Step 12 on page 437.

VTun may be configured for a number of different tunnel types, protocols, and encryption types. For use with Access Points, 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 Access Point is a client of the Virtual Tunnel Server. When you specify a VTS for an active VLAN-SSID pair, the Access Point contacts the VTS. The server then

creates a tunnel session to the Access Point. VTun encapsulated packets will cross the Layer 3 network from the Access Point 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.

Figure 254. VLAN Management

> *The Wireless Access Point supports dynamic VLAN assignments specified by RADIUS policy settings. When RADIUS sends these assignments, the Access Point dynamically assigns wireless stations to VLANs as requested. VLAN tags on traffic are passed through the Access Point (i.e., VLAN tags are not stripped).*
>
> *It is critical to configure all VLANs to be used on the Access Point, even those that will be dynamically assigned.*

The maximum number of VLANs that you may create is determined by the limit for this Access Point. It depends on the type of Access Point, and the release version of AOS that it is running.

Procedure for Managing VLANs

1. **Default Route:** This option sets a default route from the Access Point. The Access Point supports a default route on native and tagged interfaces. Once the default route is configured the Access Point 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 Access Point management is tagged or untagged. If you select a Native VLAN, then that VLAN will use an untagged (Native) link. Otherwise, the Access Point will use 802.1Q tagging and a specific VLAN ID with management enabled for management of the Access Point.

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.

Figure 255. Creating a VLAN

5. **Name/VLAN ID**: Enter a name and number for the new VLAN (1-4094).

6. **Management**: Check this box to allow management over this VLAN.

7. **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.

8. **Xirrus Roaming**: Check this box to allow roaming over this VLAN.

9. **IP Address**: If the DHCP option is disabled, enter a valid IP address for this VLAN association.

10. **Subnet Mask**: If the DHCP option is disabled, enter the subnet mask IP address for this VLAN association.

11. **Gateway**: If the DHCP option is disabled, enter the IP gateway address for this VLAN association.

12. **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 433**.

13. **New Secret/Confirm Secret**: Enter the password expected by the tunnel server.

14. **Port**: If this VLAN is to be tunneled, enter the port number of the tunnel server.

15. Click the **Apply Config** button at the top of the configuration window to apply these changes to the Access Point. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Services

Services on the Access Point include DHCP, SNMP, Syslog, Netflow, WiFi Tag, and Network Time Protocol (NTP) services.

The following sections discuss configuring services on the Access Point:

- **"Time Settings (NTP)" on page 438**
- **"NetFlow" on page 440**
- **"Wi-Fi Tag" on page 441**
- **"System Log" on page 443**
- **"SNMP" on page 447**
- **"DHCP Server" on page 450**
- **"Location" on page 453**

Time Settings (NTP)

This window allows you to manage the Access Point's time settings, including synchronizing the Access Point's clock with a universal clock from an NTP server. We recommend that you use NTP for proper operation of SNMP in XMS, since a lack of synchronization will cause errors to be detected. Synchronizing the Access Point'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 Access Point allows you to enter optional authentication information.

Figure 256. 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 XMS works best when synced to a time server. Access Points managed by XMS 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 Access Point 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. NetFlow is a proprietary but open network protocol developed by Cisco Systems for collecting IP traffic information. When NetFlow is enabled, the Access Point will send IP flow information (traffic statistics) to the designated collector.

NetFlow sends per-flow network traffic information from the Access Point. 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.

Figure 257. 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 AOS 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 Access Point 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 Access Point 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.

Figure 258. 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 Access Point which the Wi-Fi tagging server will use to query the Access Point for tagging data. When queried, the Access Point will send back information on the tags it has observed. For each, the Access Point 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 Access Point 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 Access Point 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 Access Point events.

Figure 259. 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 Access Point'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 (see **"About Using the Splunk Application for Xirrus Access Points" on page 446**).

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**. See **"About Using the Splunk Application for Xirrus Access Points" on page 446**.

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 Access Point'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. XMS 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. XMS 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 Access Point. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

About Using the Splunk Application for Xirrus Access Points

Splunk may be used to provide visibility into client experience and analyze usage on XR Series Wireless Access Points. The Splunk application has been developed to present this operational intelligence at a glance. The app includes field extractions, event types, searches and dashboards to help shine a light on station status and activity.

To use Splunk, set up your Splunk server with the Splunk application—available from www.splunk.com. Configure the Access Point to send data to Splunk by setting a **Primary**, **Secondary**, or **Tertiary Server Address** to the IP address or hostname of your Splunk server. Then set **Station Formatting** to **Key/Value** to send data in Splunk's expected format.

You may specify Server Addresses for Syslog servers and a Splunk server on the same Access Point. Selecting the **Key/Value** option will not cause any problems with Syslog.

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 Access Point by the Xirrus Management System (XMS) and other SNMP management tools. SNMP v3 was designed to offer much stronger security. You may enable either SNMP version, or both.

Figure 260. SNMP

For a summary of traps sent by the AP, see the section about traps in Appendix B of the *Xirrus Wireless Access Point User's Guide*. Complete SNMP details for the Access Point are found in the Xirrus MIB, available at support.xirrus.com, in the **Downloads** section (login is required to download the MIB).

NOTE: If you are managing your Access Points with XMS, it is very important to make sure that your SNMP settings match those that you have configured for XMS. XMS 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 Xirrus Management System, SNMP v2 (**not** SNMP v3) must be enabled on each Access Point to be managed with XMS. The default for this feature is Yes (enabled).

2. **Read-Write Community String**: Enter the read-write community string. The default is **xirrus**.

3. **Read-Only Community String**: Enter the read-only community string. The default is **xirrus_read_only**.

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 Access Point. The default is **xirrus-rw**.

9. **Read-Write Authentication Password**: Enter the read-write password for authentication (i.e., logging in). The default is **xirrus-rw**.

10. **Read-Write Privacy Password**: Enter the read-write password for privacy (i.e., a key for encryption). The default is **xirrus-rw**.

11. **Read-Only Username**: Enter the read-only user name. This username and password do not allow configuration changes to be made on the Access Point. The default is **xirrus-ro**.

12. **Read-Only Authentication Password**: Enter the read-only password for authentication (i.e., logging in). The default is **xirrus-ro**.

13. **Read-Only Privacy Password**: Enter the read-only password for privacy (i.e., a key for encryption). The default is **xirrus-ro**.

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 **Xirrus-XMS**. Thus, the Access Point will automatically communicate its presence to XMS (as long as the network is configured correctly to allow this host name to be resolved—note that DNS is not normally case-sensitive).

For a definition of the traps sent by Xirrus Wireless Access Points, you may download the Xirrus MIB from support.xirrus.com (login required). Search for the string **TRAP** in the MIB file.

15. **Keepalive Trap Interval** (minutes): Traps are sent out at this interval to indicate the presence of the Access Point on the network. Keepalive traps are required for proper operation with XMS. 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 Access Point. 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 Access Point 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 Access Point, 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.

Figure 261. 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.

Figure 262. 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 429**.

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 429**.

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 Access Point. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Location

*You can use **Settings > Location Server** to set all APs and Profiles globally to use the same Location Server, in one step. See **"Location Server" on page 636**. If you use this global setting, the **Services > Location** page for profiles configuration and for AP configuration will no longer be displayed (i.e., they are hidden).*

Xirrus Access Points 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 Access Point to send collected data to a location analytics server, such as Euclid. Note that APs that run AOSLite do not provide location data.

Figure 263. Location

When Location Support is enabled, the Access Point 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 Access Point. Multiple data points may be sent for a station—for Access Points running AOS Release 7.1 or later, data is sent for each radio that sees a probe request from the station. The Access Point 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 664**.

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 Access Point 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 Access Point will send JSON-formatted messages in the form required by Euclid via HTTPS.

   For any other location analytics server, enter its URL. The Access Point will send JSON-formatted messages in the form described in **"Location Service Data Formats" on page 664**.

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 Access Point. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Security

Access Point 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 455**.

For information about secure use of the WMI on the Access Point, refer to:

- **"About Creating Admin Accounts on the RADIUS Server" on page 462**
- **"About Creating User Accounts on the RADIUS Server" on page 475**

The security setting windows that are available are different for APs that run AOSLite (XR-320 and X2-120) and those that run AOS.

Security Settings for AOS Devices and Profiles

Security settings are configured with the following windows on all XMS versions:

- **"Admin Management" on page 459**
- **"Admin Privileges" on page 460**
- **"Admin RADIUS" on page 462**
- **"Management Control" on page 465**
- **"Global Settings" on page 469**
- **"Access Control List" on page 472**
- **"External Radius" on page 474**
- **"Internal Radius" on page 479**
- **"Airwatch" on page 481**

Security Settings for AOSLite Devices and Profiles

- **"Admin Management" on page 459** (Only available in profiles)
- **"Global Settings" on page 469**
- **"Radius (for AOSLite Only)" on page 478**

Understanding Security

The Xirrus Wireless Access Point incorporates many configurable security features. After initially installing an Access Point, 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 XMS offers powerful management features for small or large Xirrus wireless deployments, and can audit your configuration settings automatically. In addition, using the XMS 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 Access Point 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.

Configuring a Wireless Access Point

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 Access Point 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 494**). 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 469**).

● **Choosing an authentication method**: User authentication ensures that users are who they say they are. For this purpose, the Access Point 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 Access Point.

   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 Access Point) 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 Access Point will accept up to 1,000 ACL entries.

Admin Management

Note that for AOSLite profiles, this window simply allows you to change the Password for the single account on these devices (admin). You cannot directly configure the password on a selected device—this change can only be made in an AOSLite profile.

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.
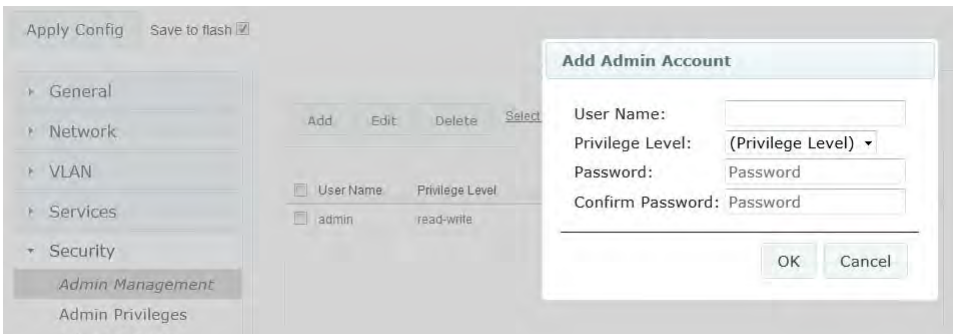
Figure 264. Admin Management

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 460**).

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 Access Point. 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 Access Point 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 Access Point. For example, say that you set the privilege level to 4 for Reboot Access Point, 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 Access Point, 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 Access Point configuration. Higher privilege levels may be used to define additional privileges for specific configuration sections.

Apply Config   Save to flash ☑

- ▸ General
- ▸ Network
- ▸ VLAN
- ▸ Services
- ▾ Security
  - Admin Management
  - *Admin Privileges*
  - Admin RADIUS
  - Management Control
  - Global Settings
  - Access Control
  - External RADIUS
  - Internal RADIUS
  - AirWatch
- ▸ SSIDs
- ▸ Groups
- ▸ IAPs
- ▸ Filters
- ▸ Tunnels

Privilege Levels

Edit

Showing: 1

	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 265. 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 Access Point. 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 Access Points has these benefits:

- Centralized control of administrator accounts.

- Less effort—you don't have to set up user names and passwords on each Access Point; just enter them once on the RADIUS server and then all of the Access Points 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 Access Point 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 Access Point if the RADIUS server is down.

About Creating Admin Accounts on the RADIUS Server

Permissions for RADIUS administrator accounts are controlled by the RADIUS **Xirrus-Admin-Role** attribute. This is a Vendor Specific Attribute (VSA). To define the privileges permitted to an administrator account, set the value of its Xirrus-Admin-Role attribute to the desired **Privilege Level Name** string, as defined in "Admin Privileges" on page 460. For more information about the RADIUS VSAs

used by Xirrus, see "RADIUS Vendor Specific Attribute (VSA) for Xirrus" in the Technical Support Appendix of the Xirrus *Wireless Access Point User's Guide*.

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 Access Point using the Admin Management window: the user name and password must be between 5 and 50 characters, inclusive.

Figure 266. 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 Access Point.

1. **Admin RADIUS Settings:**

    a. **Enable Admin RADIUS**: Click **Yes** to enable the use of RADIUS to authenticate administrators logging in to the Access Point. 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 Access Point 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 Access Point management interfaces and set their inactivity time-outs. The supported range is 300 (default) to 100,000 seconds. (Figure 267)

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 Access Point for the specified period of time (in seconds). The default is 0.

Figure 267. Management Control

2. **SSH**—enabling SSH on APs is critical to allow XMS to manage them properly.

    a. **On/Off**: Choose **On** to enable management of the Access Point over a Secure Shell (SSH-2) connection, or **Off** to disable this feature. Be aware that only SSH-2 connections are supported by the Access Point. SSH clients used for connecting to the Access Point 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 Access Point 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 HTTPS. The default port is 443.

5. **Xircon**

The Xircon utility connects to Xirrus XR Series Access Points 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. Please see the Xircon *User's Guide* for more information. You can enable or disable Xircon access to the Access Point as instructed below.

!   *Warning: If you disable Xircon 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 Access Point to Xirrus.*

    a. **On/Off**: Choose **On** to enable Xircon access to the Access Point at the AOS (CLI) and Xirrus Boot Loader (XBL) levels, or **Off** to disable access at both levels. On models that have no console port, Xircon access is **On** by default. On all other Access Point models, Xircon access is **Off** by default.

    b. **AOS only**: Choose this radio button to enable Xircon access at the AOS level only (i.e., Xircon can access CLI only). Access to the Access Point at the Xirrus Boot Loader (XBL) level is disabled.

    c. **Boot only**: Choose this radio button to enable Xircon access at the Xirrus Boot Loader (XBL) level only. AOS level (CLI) access to the Access Point is disabled.

    d. **Connection Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your Xircon 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 Xircon. The default port is 22612.

6. **Serial**

This setting is only available for Access Points that have a Console (serial) port.

a. **On/Off**: Choose **On** to enable management of the Access Point 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 Access Points 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 Access Point for auditing PCI-DSS restrictions. See the *Xirrus Wireless Access Point User's Guide* for more information.

c. **Spanning Tree Protocol**: Click **On** to enable Spanning Tree Protocol (STP) on this AP. STP is used in Layer 2 networks to turn off ports when necessary to prevent network loops. It is **Off** by default, and is turned on automatically if you are using WDS to interconnect APs using wireless links. Use the **On** button to enable spanning tree if your network topology requires it. See the *Xirrus Wireless Access Point User's Guide* for more information.

8. Click the **Apply Config** button at the top of the configuration window to apply these changes to the Access Point. 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 455**.

Figure 268. 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 474** and **"Internal Radius" on page 479**.

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 Access Points.*

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 Access Point'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 Access Points.

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 Access Point. 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 Access Point 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 Access Point. 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 521**). 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.
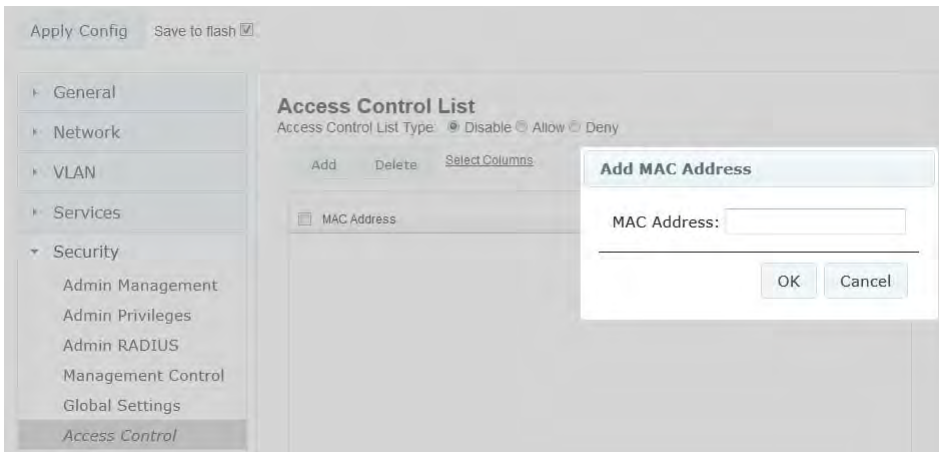
Figure 269. Access Control List

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 Access Point. All others are denied.

- **Deny**: Denies the listed MAC addresses permission to associate to the Access Point. 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 Access Point. 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 469**.

Figure 270. External RADIUS Server

If you want to include user group membership in the RADIUS account information for users, see **"Understanding Groups" on page 524**. User groups allow you to easily apply a uniform configuration to a user on the Access Point.

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 Xirrus. For example, you would use the VSA named **Xirrus-User-VLAN** if you wish to set the VLAN for a user account in RADIUS. For more information about the RADIUS VSAs used by Xirrus, see "RADIUS Vendor Specific Attribute (VSA) for Xirrus" in the Technical Support Appendix of the Xirrus *Wireless Access Point User's Guide*.

Procedure for Configuring an External RADIUS Server

1. **External RADIUS Settings:** Define the settings used for RADIUS Dynamic Authorization.

   a. **Timeout (seconds)**: Define the maximum idle time (in seconds) before the external RADIUS server's session times out. The default is 600 seconds.

   b. **DAS Port**: RADIUS Dynamic Authorization port. Some RADIUS servers have the ability to contact the Access Point (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 Access Point to change a user's privileges due to dynamically changing session authorizations. RADIUS will use the DAS port on the Access Point for this purpose. The default is port **3799**.

   c. **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 Access Point 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.

   d. **DAS Time Window**: This is the time window used with the **DAS Event-Timestamp**, above.

2. **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.

3. **External RADIUS Secondary Server** (optional): If desired, enter an alternative external RADIUS server. If the primary RADIUS server becomes unreachable, the Access Point 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.

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 Access Point—**BSSID:SSID** (default), **BSSID**, or **Ethernet-MAC**.

      b. **Station MAC Format**: Define the format of the **Station MAC** RADIUS attribute sent from the Access Point—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 Access Point 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 AOS Release 7.1 and up. This attribute is used, for example, by Aruba ClearPass 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 Access Point 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 Access Point 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 Access Point. 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 Access Point (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 Access Point to change a user's privileges due to dynamically changing session authorizations.

Figure 271. 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 Access Point 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 Access Point 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 Access Point's internal RADIUS server for user authentication. However, the internal RADIUS server will only authenticate wireless clients that want to associate to the Access Point. 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 469**.

Figure 272. Internal RADIUS Server

> ✐ *Clients using PEAP may have difficulty authenticating to the Access Point 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.

Figure 273. 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 524**.

5. **Password**: (Optional) Enter a password for the user.

Configuring a Wireless Access Point

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 Access Point. 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.

Figure 274. AirWatch Settings

APs (running AOS Release 6.5 or higher) 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 Access Point 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 Access Point, you must have an AirWatch account, already set up with your organization's compliance policies and other configuration as required by AirWatch.

The Access Point 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 483**.

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 Access Point will call to determine the enrollment and compliance status of a mobile device attempting to connect to the Access Point. The steps that the user will need to take are described in **"User Procedure for Wireless Access" on page 483**.

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 S**ystem / 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 Access Point, 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 Access Point. See **"User Procedure for Wireless Access" on page 483** 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 13 on page 497).

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 Access Point 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 Access Point 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 Access Point 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 Access Point 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.

Figure 275. 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.

Configuring a Wireless Access Point

- 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 Access Point, go to **"Understanding SSIDs" on page 487**. For a description of how QoS operates on the Access Point, see **"Understanding QoS Priority on the Wireless Access Point" on page 490**.

SSIDs are managed with the following windows:

- **"SSID Management" on page 494**
- **"Per-SSID Access Control List" on page 521**
- **"Active Radios" on page 523**

SSIDs are discussed in the following topics:

- **"Understanding SSIDs" on page 487**
- **"High Density 2.4G Enhancement—Honeypot SSID" on page 489**
- **"Understanding QoS Priority on the Wireless Access Point" on page 490**

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 Access Points 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 XR-320 and the X2-120, 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 Access Point offers a feature targeting this problem—a "honeypot" SSID. Simply create an SSID named **honeypot** (lower-case) on the Access Point, 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 Access Point. 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 520**.
- SSIDs that are encrypted and/or authenticated.
- SSIDs that are configured on this Access Point, whether or not they are enabled.

Traffic for a station connected to the honeypot SSID may be handled in various ways using other Access Point 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 502**);
- it may be filtered (see **"Filters" on page 582**);
- or it may be dead-ended by defining a specific dead-end VLAN on the honeypot SSID to "trap" stations (see **"VLAN" on page 433**).

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 520**.

Understanding QoS Priority on the Wireless Access Point
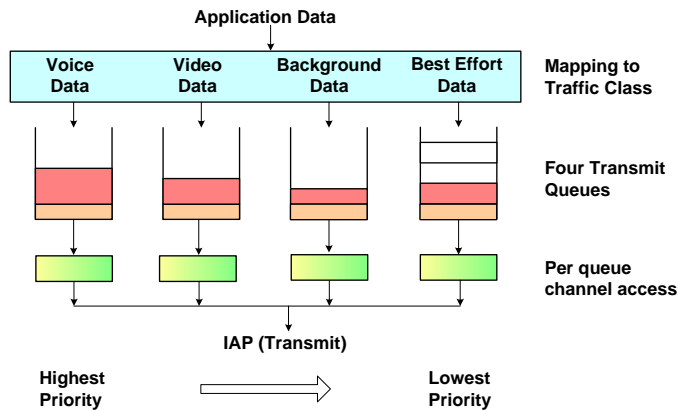
Figure 276. Four Traffic Classes

The wireless Access Point'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 Access Point has four separate queues for handling wireless traffic at different priorities, and thus it supports four traffic classes (QoS levels).
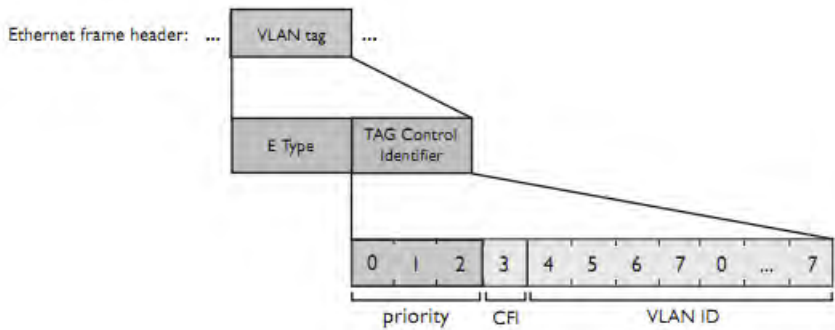
Figure 277. Priority Level—IEEE 802.1p (Layer 2)

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 Access Point implements four wireless QoS levels, user priorities are mapped to QoS as described below.
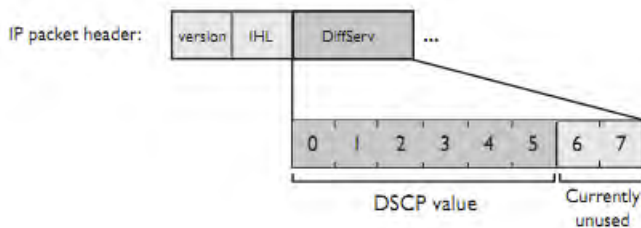
Figure 278. Priority Level—DSCP (DiffServ - Layer 3)

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 Access Point'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 Access Point 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
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 Access Point QoS (Wireless)	TO Priority Tag 802.1p (Wired)
1 (Lowest priority)	1
0	0
2 (Default)	5

FROM Access Point QoS (Wireless)	**TO** Priority Tag 802.1p (Wired)
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 494**. If multiple SSIDs are used, packets from the SSID with higher priority are transmitted first.

- The Access Point 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 524**, and **"Filters" on page 582**.

  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 585**. This allows the QoS priority level to be assigned based on protocol, source, or destination.

Voice Support

- The QoS priority implementation on the Access Point 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.

Figure 279. SSID Management

✎ *If you are planning to use the Xirrus Cloud EasyPass Portal feature, you should perform the cloud-based portion of your configuration before creating corresponding SSIDs in XMS. See* **"SSID Management—Captive Portal" on page 502**.

This page has the following sections. Click a section heading to expand that section.

- **"SSID Management—General Settings" on page 495**
- **"SSID Management—Authentication/Encryption" on page 498**
- **"SSID Management—Limits" on page 500**
- **"SSID Management—Traffic Shaping" on page 501**
- **"SSID Management—Captive Portal" on page 502**
- **"SSID Management—Honeypot Service Whitelist" on page 520**

When done, click the **Apply Config** button near the top of the window to apply these changes to the Access Point. 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 279)) 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.

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 Access Point 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 Access Point" on page 490**. 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 450**.

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 582**.

11. **Xirrus Roaming**: For this SSID, select whether to enable fast roaming between radios or Access Points at **L2&L3** (Layer 2 and Layer 3), at **L2** (Layer 2 only), or disable roaming (**Off**). You may only select fast roaming at Layers 2 and 3 if this has been selected in Global Settings (Radio). See **"Understanding Fast Roaming" on page 531**.

12. **Fallback**: Network Assurance checks network connectivity for the Access Point. When Network Assurance detects a failure, perhaps due to a bad link or WDS failure, if Fallback is set to **Disable** the Access Point will automatically disable this SSID. This will disassociate current clients, and prevent new clients from associating. Since the Access Point'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 468 for more information on Network Assurance.

13. **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 481**.

✎ *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.

Figure 280. 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 Access Point) 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 469). For an overview of the security options, see **"Understanding Security" on page 455**.

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 469**). 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 470**. 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 475**). 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 529** 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.

Figure 281. 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 542 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.
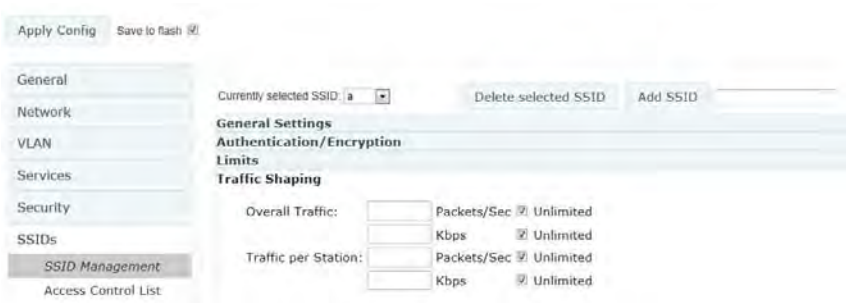
Figure 282. SSID Management: Traffic Shaping

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 Access Point 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 Access Point will enforce the limit it reaches first.

SSID Management—Captive Portal

> ✎ *Note that smaller APs that use the AOSLite system software, such as the XR-320 and the X2-120, have many fewer settings than more powerful APs. For these APs, the only type of Captive Portal supported is the EasyPass Portal. 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.

- **Access Point-based captive portal** options (i.e., web page redirect— WPR) are hosted on the AP. XMS includes a What You See Is What You Get (WYSIWYG) HTML editor for creating a splash page or login page for the portal.

- **Cloud-based EasyPass™ Portals**—Xirrus offers an optional, cloud-based access portal manager that enables you to easily provide secure and controlled access to your Wi-Fi network. To use this feature, you must have an EasyPass Portal license (contact Xirrus Sales for more information). Once you log in to the Cloud portal manager as instructed in your welcome email, you can build and manage one or more portals and specify which SSIDs will send guests to each portal. The majority of EasyPass portal configuration is performed in the Cloud portal manager.

  Xirrus offers seven kinds of captive portals, configured in To Configure an EasyPass Portal.

  - EasyPass Self-registration—provides access to guests in organizations like companies and schools by allowing guests to register themselves. Users (for example, parents visiting a school) sign themselves up for an account. If desired, you may set up the portal to require approval by company personnel.

  - EasyPass Guest Ambassador registration—provides access to guests by having an employee "sponsor" register them, using Cloud-based tools. Guest accounts may be administered easily by non-IT staff such as a receptionist.

  - EasyPass One Click Access—all guests have access without an account needing to be created.

- EasyPass Onboarding—allows employees or students to securely connect their personal devices to a corporate or school network without requiring IT assistance. You create accounts that allow Bring Your Own Device (BYOD) users to register their own devices, including printers.

- EasyPass Vouchers—these provide temporary access in public locations such as coffee shops and restaurants. **EasyPass** generates temporary accounts in bulk, which you can then hand out to visitors.

- EasyPass Google or Microsoft Azure Login—organizations and schools can authenticate users using Google or Azure credentials against their own domains or Google or Azure domains. You can use Google or Azure applications and authentication infrastructure without maintaining your own domain infrastructure. Users log in using their Google or Azure credentials, and two-factor authentication is supported (if this has been configured in the Google, it will ask users for a pin code which is sent after entering credentials).

*Note that Google and Azure logins require a white list entry to allow client access to google.com or microsoft.com. XMS provides a number of these entries automatically. However, if customers are logging in from other countries and are unable to gain access, you must add white list entries for their local websites. For example, **www.google.com.vn** adds access for Google login clients in Vietnam. You may use wild cards to add access for all countries (e.g., **www.google.com.***). For more information, see* **"White List Configuration for Captive Portal" on page 519***.*

- EasyPass Personal Wi-Fi—creates secure private wireless networks for guests, visitors, and employees over a public wireless network. A user (for example, a guest staying at a hotel) signs up to create a custom, secure SSID by simply entering a name and password for it. All of the user's devices can be connected to that SSID.

> ✎ *Note that statistics for personal SSIDs are not collected or displayed separately from the parent SSIDs statistics.*

EasyPass features include:

- EasyPass portals are supported by both AOS and AOSLite profiles and devices.

- Support for multiple simultaneous portals—for example, you might have a portal for Contractors that requires company approval but has guest accounts that do not expire, and a portal for Visitors whose accounts do not require approval, but expire daily.

- Email/SMS login notification—notification may be set up via email or via SMS texts to a mobile phone.

- Integrated WYSIWYG editor—a simple editor provides a rich set of options for creating a custom splash page.

Procedure for Managing Captive Portal Settings

- To Configure an EasyPass Portal
- To Configure an AP-based Captive Portal

To Configure an EasyPass Portal

1. First, you must configure an EasyPass Portal for this SSID in the Cloud. Log in to your Xirrus Cloud account as instructed in your welcome email. Click **HELP** and follow the instructions to create your portal.

> ✎ *You should configure an EasyPass Portal for this SSID in the Cloud before creating the SSID here in XMS-Enterprise (XMS-E). However, if you already have defined SSIDs in XMS-E, the portal will still work properly if you ensure that the **Captive Portal: Server** setting for each of the portal's SSIDs is set to **Disabled** until your Cloud configuration per Step 1 and Step 2 is complete. Then proceed with Step 3 below.*

2. Still in the Cloud, select the portal's **SSIDs** page, and click **+Assign SSIDs** to enter the SSIDs that will use this guest portal. Enter the SSID names *very carefully*—they are case-sensitive and must exactly match the names that you will enter in XMS-E.

3. Return to XMS-E to complete your set up. XMS-E only has one setting to configure an AP for use with your cloud-based EasyPass portal. For one of the SSIDs that have been assigned to a portal in the Cloud, click **Captive Portal** and set the **Server** to **EasyPass Portal**. The SSID will use whatever portal it has been assigned to in the Cloud—that s why it is important to do the portal setup in the Cloud before you set the Server to EasyPass Portal.

   You must have an EasyPass Portal account to use this feature, and the AP must be running at least AOS Release 8.1.2 or AOSLite Release 8.0. You will not see the EasyPass Portal option in the drop-down list for a device if the AP is running a software version that does not support it.

4. If this portal is an EasyPass Personal portal, click the **Personal** checkbox. Personal SSIDs created by users are listed and managed in the Cloud EasyPass Portal manager.

5. Click **Apply Config**. The EasyPass Portal that includes the current SSID will be used to provide access when users connect to this SSID on this AP. In addition, the AP's configuration in XMS-E will be updated by the Cloud as follows—all other SSIDs assigned to that same portal in the Cloud will also be set to use the EasyPass Portal, **if** the SSIDs are defined for this AP and the names are an exact match for the SSID names configured in the Cloud. You can verify this by checking the **Captive Portal—Server** setting for those SSIDs on this AP. They will also be changed to **EasyPass Portal** automatically.

> *For SSIDs associated with an EasyPass Onboarding portal, XMS configures the settings in **SSID Management—Authentication/Encryption** to values required for onboarding after you click **Apply Config**. These settings will be grayed out so that you cannot change them. This is because each Onboarding user account (for example, each student in a dorm) is assigned a unique user preshared key (U-PSK) by the Cloud, and the settings for U-PSK are essential to proper operation of onboarding. Graying out the authentication/encryption page keeps you from changing these critical values.*

6. Repeat Step 3 to Step 5 for each of the portals that you have created in the Cloud. For each portal, select one of the SSIDs assigned to it and perform these steps.

7. To change the portal used on an SSID (let's say we want to change MySSID from Portal-A to Portal-B), use the Cloud portal manager. On the **SSIDs** tab of the new portal (Portal-B in this example), simply assign MySSID to the portal. This automatically removes MySSID from Portal-A. In XMS-E, the **Captive Portal—Server** setting is already set to **EasyPass Portal** for MySSID. Stations connecting to MySSID will use Portal-B, as specified in the Cloud.

8. To delete a cloud portal used on one or more AP SSIDs you **must** first delete those SSIDs in XMS-E, then click **Apply Config** and verify that the deletion was successfully applied to the AP. You must do this for all profiles or APs that use those SSIDs. After that, you can log in to your Cloud account and delete the associated access portal.

9. If you configure a profile's SSID to use an EasyPass Portal, the information in Steps 1 to 5 applies to all of the profile's member APs that are running suitable software versions. If the profile includes APs that are running a lower release, we suggest that you upgrade them prior to configuring the guest portal. Profile member APs running earlier releases will have SSIDs automatically disabled, if those SSIDs are assigned to the guest portal.

To Configure an AP-based Captive Portal

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 519**.

> *When using a captive portal, it is particularly important to adhere to the SSID naming restrictions detailed in **Step 1 on page 495**.*

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.
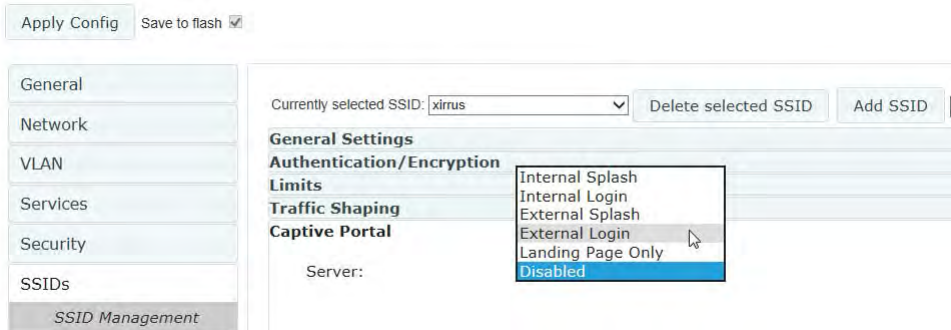
Figure 283. Captive Portal Server Types

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 526**. Note that if you change the management HTTPS port, captive portal uses that port, too. See **"HTTPS" on page 466**.

When users roam between Access Points, 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 Access Point 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 509**
- **"Internal Login page" on page 510**

- **"External Login page" on page 512**
- **"External Splash page" on page 513**
- **"Landing Page Only" on page 514**

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 519**.

- Internal Splash page
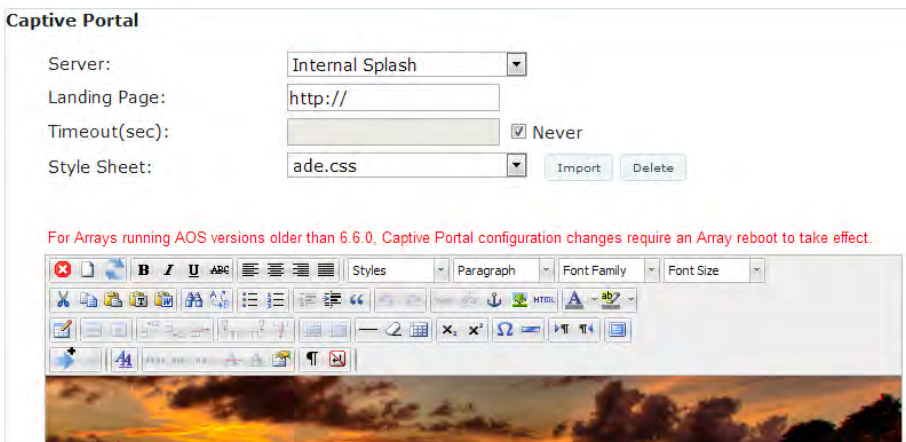
Figure 284. Captive Portal—Internal Splash Page

This option displays a splash page instead of the first user-requested URL. The splash page files reside on the Access Point. 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 514**.

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 290 on page 516). 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 XMS 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 Access Point for the captive portal will include the CSS file.

● Internal Login page

Figure 285. 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 Access Point) 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 514**.

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 XMS 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 Access Point 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 498**).

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 Access Point for authentication.

Figure 286. Captive Portal—External Login Page

Authentication occurs according to your configured authentication information (see **"SSID Management—Authentication/Encryption" on page 498**). 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.

Figure 287. 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**.

Figure 288. 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 Access Point, 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 Access Point 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 Access Points running AOS 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 Access Point 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 Access Points Toolbar" on page 119**.

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.
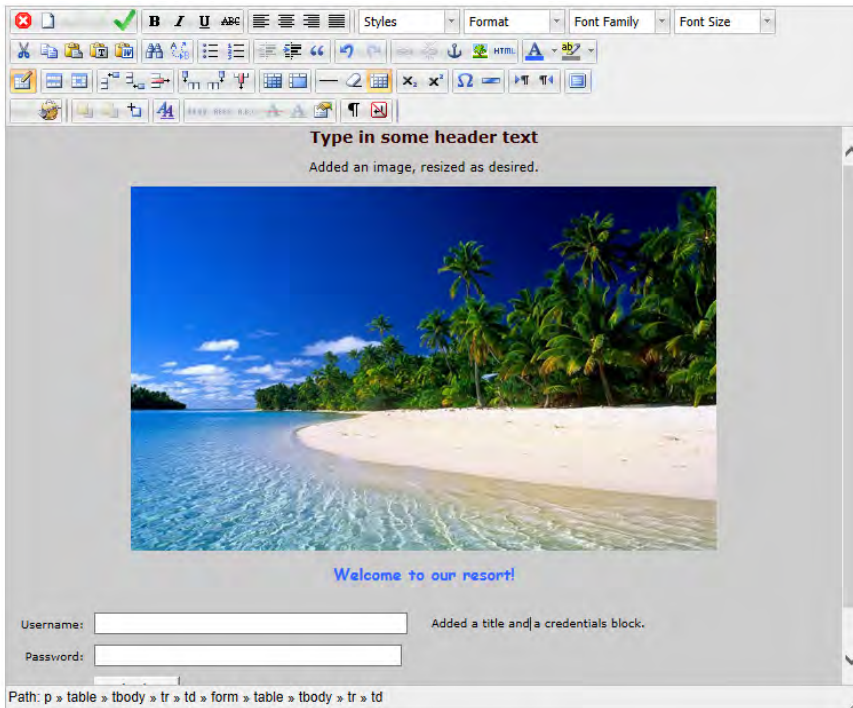
Figure 289. Using the Captive Portal Editor

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 290, 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

Add Credentials Block (for Internal Login page only)
Add a Proceed Button (for Internal Splash page only)
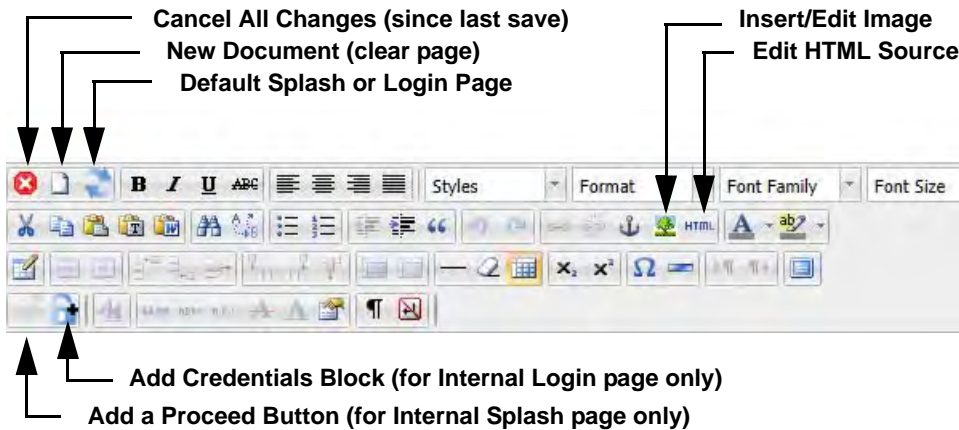
Figure 290. Captive Portal Editor Buttons

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 Xirrus 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 XMS server. The image is inserted as a reference rather than directly inline. The HTML files uploaded to an Access Point 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 XMS server.
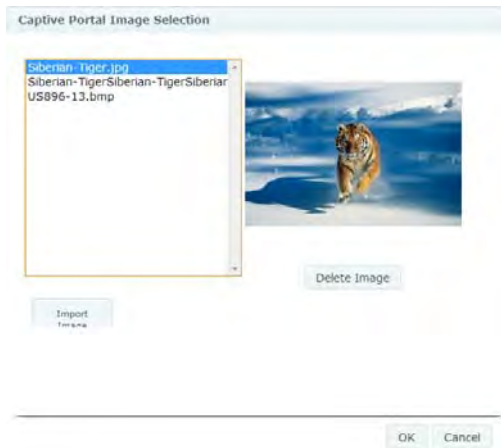
Figure 291. Captive Portal Image Selection

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 Access Point 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 526**.

White List   whitelist.xxx.com

                                 *.google.com
                                 bookings.xyzco.com
                                 guest.xyzco.com   Add

                                                Delete

                                                Reset
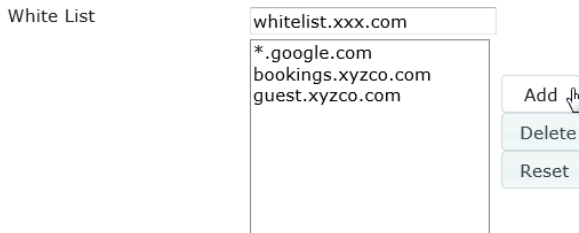
Figure 292. White List Configuration for Captive Portal

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 489**. Type in each SSID name, and click **Add** to add it to the whitelist. Up to 150 SSIDs may be listed. The SSID names entered in this list are not case-sensitive.

Figure 293. SSID Management: Honeypot Whitelist

✎   *Up to 150 whitelist entries are allowed for APs running AOS 8.4 and above. APs with older versions of AOS only handle 50 entries, so only the first 50 entries will be sent to those APs.*

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.

Figure 294. 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 472**). 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 Access Point. All others are denied.

   - **Deny List**: Denies the listed MAC addresses permission to associate to the Access Point. 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 Access Point. 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.

Figure 295. 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 Access Point. 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.

For information to help you understand groups, see Understanding Groups below.

Figure 296. 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 Access Point. 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 Access Point. This will allow the Access Point 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.

Figure 297. 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 Access Point. This tells the Access Point 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 433**).This user group's VLAN settings supersede Dynamic VLAN settings (which are passed to the Access Point 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 Access Point" on page 490**. 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 450**.

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 582**.

10. **Xirrus Roaming**: (Optional) For this group, select roaming behavior. Select **L2&L3** to enable fast roaming between radios or Access Points 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 531**.

11. **Fallback**: Network Assurance checks network connectivity for the Access Point. When Network Assurance detects a failure, perhaps due to a bad link or WDS failure, if Fallback is set to **Disable** the Access Point will automatically disable this group of users. This will disassociate current clients, and prevent new clients from associating. Since the Access Point'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 468 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 502** 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 Access Point 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 542 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 Access Point. 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. If you have expanded the capacity of an Access Point by adding modular 802.11ac APs to it (XI-867/1300), then you will see the number and types of APs present.

Access Points have a fast roaming feature, allowing them to maintain sessions for applications such as voice, even while users cross boundaries between Access Points. Fast roaming is set up in the Global Settings (Radio) window and is discussed in:

- **"Understanding Fast Roaming" on page 531**

Radios are configured using the following windows:

- **"Radio Settings" on page 533**
- **"Global Settings (Radio)" on page 538**
- **"Global Settings .11a" on page 552**
- **"Global Settings .11bg" on page 555**
- **"Global Settings .11n" on page 559**
- **"Global Settings .11ac" on page 560**
- **"Advanced RF Settings" on page 563**
- **"Intrusion Detection" on page 569**
- **"LED Settings" on page 577**
- **"DSCP Mappings" on page 578**
- **"Roaming Assist" on page 579**

Understanding Fast Roaming

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.

Mobile wireless users are likely to cross multiple roaming domains during a single session (especially wireless users of VoIP phones). **Layer 3 roaming** allows

a user to maintain the same IP address through an entire real-time data session. The user may be associated to any of the VLANs defined on the Access Point. The Layer 3 session is maintained by establishing a tunnel back to the originating Access Point. You should decide whether or not to use Layer 3 roaming based on your wired network design. Layer 3 roaming incurs extra overhead and may result in additional traffic delays. You may configure one SSID for Layer 3 fast roaming with up to 25 APs.

Fast Roaming is configured on two pages. To enable the fast roaming options that you want to make available on your Access Point, see Step 27 to Step 29 in **"Global Settings (Radio)" on page 538**. To choose which of the enabled options are used by an SSID or Group, see **"Procedure for Managing General Settings" on page 495** or **"Procedure for Managing Groups" on page 526**.

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 XR-320, 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.*

Apply Config   Save to flash ☑

| General |
| Network |
| VLAN |
| Services |
| Security |
| SSIDs |
| Groups |
| Radios |
| *Radio Settings* |
| Global Settings |

Edit   Enable All   Disable All   Select Columns

Sh

	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 298. 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.

Figure 299. 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, Access Points continually scan for signatures of military radar. If such a signature is detected, the Access Point will switch operation from conflicting channels to new ones. The Access Point 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 Access Point 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 Access Point 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 Access Points with 802.11ac radios.

    For 802.11n Access Points, 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 Access Point, 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 Access Points, 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.

> *ACExpress load balancing automatically groups client devices by performance. See* **Step 24** *in* **"Global Settings (Radio)" on page 538***.*

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 Access Point models will only accept 0dBm as a minimum value.

When other Access Points are within listening range of this one, setting cell sizes to **Auto** allows the Access Point to change cell sizes so that coverage between cells is maintained. Each cell size is optimized to limit interference between sectors of other Access Points on the same channel. This eliminates the need for a network administrator to manually tune the size of each cell when installing multiple Access Points. In the event that an Access Point or an individual radio goes offline, an adjacent Access Point 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 Access Point's cell diameter. In a large office, or if multiple Access Points 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 Access Point. 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.

Figure 300. Global Settings—Radios (AOS settings shown)

Procedure for Configuring Global Radio Settings

> APs that run AOS Lite (XR-320/X2-120) 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 Access Point behavior to conform completely to Wi-Fi Alliance standards. This mode is normally set to **Off**.

Beacon Configuration

5. **Beacon Interval**: When the Access Point 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 Access Point 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 Access Point'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 Access Point 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 Access Points running AOS 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 Access Point buffers downlink frames.

Fast Transition Configuration

✎ *This feature is currently available only on APs that run AOSLite (XR-320/ X2-120).*

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 469** and **"SSID Management—Authentication/ Encryption" on page 498**).

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 495**.

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 Access Point. This feature is part of the Xirrus 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 Access Point**: This option allows you to define how many station associations are allowed per Access Point. Note that the **Max Station Association per radio** limit (below) may not be exceeded. If you have an unlicensed Access Point, this value is set to 1, which simply allows you to test the ability to connect to the Access Point.

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 Access Point** 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 Access Point. 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 Access Point 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 Access Point 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 Access Point 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 a Xirrus 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 Access Point. 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.

*Xirrus 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 XMS 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 433**) in order to participate in multicast forwarding. In fact, the Access Point 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 XMS database, click **Reset** (i.e., any unsaved changes are erased from the list).

These VLANs must be trunked to the Access Point from the LAN switch, and be defined on the Access Point. See **"VLAN Management" on page 434** and **"SSID Management" on page 494**.

✎ *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 Access Point 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 XMS 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 Access Point (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 Access Point 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. Xirrus solves this issue with ACExpress™ which automatically separates devices onto different radios by their speeds and capability.

ACExpress 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 Access Point 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 Access Point radios.

If you select **On** and an IAP 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 ACExpress 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 Xirrus Access Point currently bridges IPv6 traffic. Set IPv6 filtering **On** if you wish to prevent the forwarding of IPv6 packets through the Access Point 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 Access Point 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 Access Point replies on behalf of the stations that are associated to it. The ARP request is not broadcast to the stations.

Note that the Access Point 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. **Xirrus Roaming Layer:** Select whether to enable roaming capabilities between radios or Access Points at Layer **2 and 3**, or at Layer **2 only**. Depending on your wired network, you may wish to allow fast roaming at Layer 3. This may result in delayed traffic.

28. **Xirrus Roaming Mode:** This feature utilizes the Xirrus Roaming Protocol ensuring fast and seamless roaming capabilities between radios or Access Points 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 531** for a discussion of this feature). The roaming protocol uses a discovery process to identify other Xirrus Access Points as fast roaming targets. This process has two modes:

    • **Broadcast**—the Access Point uses a broadcast technique to discover other Access Points that may be targets for fast roaming. This is the default.

    • **Tunneled**—in this Layer 3 technique, fast roaming target Access Points 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 Access Points.

    • **Ports 15000 to 17999**—reserved for Layer 3 roaming (tunneling between subnets).

29. **Share Roaming Info With:** Three options allow your Access Point to share roaming information with all Access Points; just with those that are within range; or with specifically targeted Access Points. Choose either **All**, **In Range** or **Target Only**, respectively.

    a. **Xirrus Roaming Targets:** If you chose **Target Only**, use this option to add target MAC addresses. Enter the MAC address of each target

Access Point, then click on **Add** (add as many targets as you like). To find a target's MAC address, open the Access Point **Info** window on the target Access Point 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.

Figure 301. Global Settings .11a

Procedure for Configuring Global 802.11a Radio 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 564***

1. **Set Cell Size:** This setting applies to all 802.11a radios. Select **auto** to allow the optimal cell size (i.e., power setting of each radio) to be automatically computed. To set the cell size yourself, choose either **small**, **medium**, or **large**. If you select a value other than auto, the cell size will not be affected by cell size auto configuration. See Step 8 on page 536 for more information or if you wish to set this value for individual radios (Radio Settings override the settings made on this page).

2. **Optimize Power Period (seconds)**: You may set up auto-configuration to run periodically, readjusting optimal cell sizes (i.e., radio power) 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 Access Points Toolbar" on page 119**.

3. **Optimize Power Cell Size Overlap (%)**: Enter the percentage of cell overlap that will be allowed when the Access Point is determining automatic cell sizes. For 100% overlap, the power is adjusted such that neighboring Access Points that hear each other best will hear each other at -70dB. For 0% overlap, that number is -90dB. The default value is **50%**.

4. **Optimize Power Min Tx Power (dBm)**: Enter the minimum transmit power that the Access Point 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**.

5. **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.

6. **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.

7. **Max Stations per Access Point**: 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 542 in Global Settings (Radio) for a list of places where station limits are set.

8. **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 542 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.

Figure 302. Global Settings .11bg

Note that 802.11b is disabled by default for AOS, 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 5 below.

Procedure for Configuring Global 802.11b/g Radio Settings

> *To use the Optimize Power (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 564***

1. **Set Cell Size:** This setting applies to all 802.11bg radios. Select **auto** to allow the optimal cell size (i.e., power setting of each radio) to be automatically computed. To set the cell size yourself, choose either **small**, **medium**, or **large**. If you select a value other than auto, the cell size will not be affected by cell size auto configuration. See Step 8 on page 536 for more information or if you wish to set this value for individual radios (Radio Settings override the settings made on this page).

2. **Optimize Power Period (seconds)**: You may set up auto-configuration to run periodically, readjusting optimal cell sizes (i.e., radio power) 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 Access Points Toolbar" on page 119**.

3. **Optimize Power Cell Size Overlap (%)**: Enter the percentage of cell overlap that will be allowed when the Access Point is determining automatic cell sizes. For 100% overlap, the power is adjusted such that neighboring Access Points that hear each other best will hear each other at -70dB. For 0% overlap, that number is -90dB. The default value is **50%**.

4. **Optimize Power Min Tx Power (dBm)**: Enter the minimum transmit power that the Access Point 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**.

5. **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 AOS, 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.

6. **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 Access Point, but not each other.

    When there are no 11b stations associated and an auto-protection mode is enabled, the Access Point will not send the extra frames, thus avoiding unnecessary overhead.

7. **802.11g Slot**: Choose **Auto** to instruct the Access Point to manage the 802.11g slot times automatically, or choose **Short Only**. Xirrus recommends using **Auto** for this setting, especially if 802.11b devices are present.

8. **802.11b Preamble**: The preamble contains information that the Access Point 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 Access Point to manage the preamble (long and short) automatically, or choose **Long Only**.

9. **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.

10. **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.

11. **Max 802.11bg Stations per Access Point**: 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 542 in Global Settings (Radio) for a list of places where station limits are set.

12. **Max 802.11bg 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 542 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 Access Point, and specifying whether auto-configured channel bonding will be static or dynamic.

Procedure for Configuring Global 802.11n Radio Settings
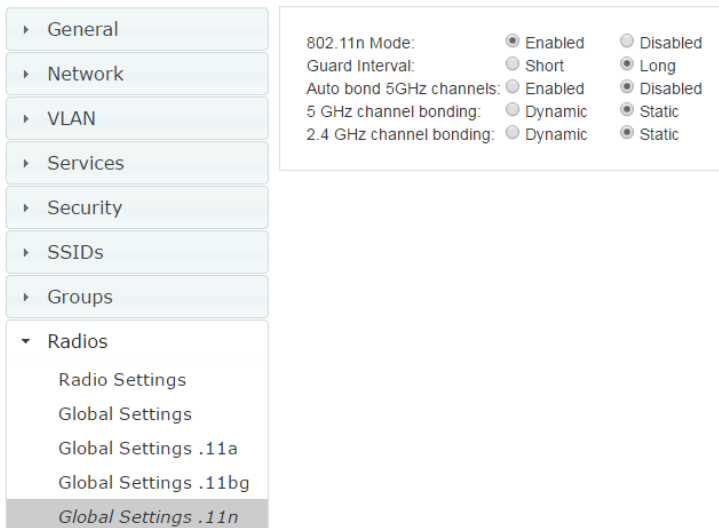
Figure 303. Global Settings .11n

1. **802.11n Mode:** Select **Enabled** to operate in 802.11n mode (this is the default). Use of this mode is controlled by the Access Point's license key. The key must include 802.11n capability, or you will not be able to enable this mode. See **"Access Point Details—System" on page 77** to view the features supported by your license key. Contact Xirrus Customer support for questions about your license.

   If you select **Disabled**, then 802.11n operation is disabled on the Access Point.

2. **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.

3. **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**.

4. **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**.

5. **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 Access Point 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 Access Point, 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 Xirrus *Wireless Access Point User's Guide*.

Procedure for Configuring Global 802.11ac Radio Settings

✎ *802.11ac operation is allowed only if the Access Point's license includes this feature.*

1. **802.11ac Mode**: Select **Enabled** to allow the Access Point to operate in 802.11ac mode. If you select **Disabled**, then 802.11ac operation is disabled on the Access Point.
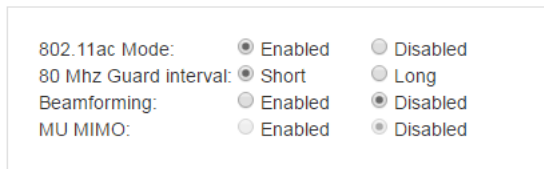
Figure 304. Global Settings .11ac (shown for 2x2 radios)

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 Xirrus *Wireless Access Point User's Guide*. 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. Xirrus 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 XD2-240'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 the Xirrus *Wireless Access Point User's Guide*.

The maximum number of separate data streams that may be transmitted by the antennas of each radio is determined by whether the Access Point has 2x2 or 3x3 radios. For a device that has 2x2 radios, such as the XR-620, 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 the Xirrus *Wireless Access Point User's Guide*.

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.

Figure 305. Advanced RF Settings

Procedure for Configuring Advanced RF Settings

> *Some options below, such as RF Intrusion Detection, are only available if the Access Point's license includes the Xirrus 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 Access Point may not be frequent enough to identify and locate rogues. See* **"Rogue Location" on page 292**.

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 Access Points**. For details, see **"Settings that are only present in profile configuration" on page 226**.

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 Access Point. 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 Access Point will issue alerts in the Syslog, but will not initiate repairs or reboots.

   • **Repairs without reboot**—The Access Point will issue alerts and perform resets of one or all of the radios if needed.

   • **Reboots allowed**—The Access Point 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 Access Points 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 the Xirrus *Wireless Access Point User's Guide*.

   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 Access Point's radios. When you start an Access Point's auto channel feature, the Access Point 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 Access Points 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 Access Points Within Maps" on page 281** and **"Channel Configuration" on page 293**.

When running auto channel on multiple Access Points, XMS will shut down radios on all of the Access Points being configured. It will then run auto channel on one Access Point 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 Access Point to auto-configure channel selection for each enabled radio when the Access Point is powered up. Choose **On Access Point PowerUp** to enable this feature, or choose **Disabled** to disable this feature.

5. **Auto Channel Schedule**: This option allows you to instruct the Access Point 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 Access Point 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 Access Points 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 Access Point 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 Access Point 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 Access Point**: **Min Received Signal Strength**: (feet) Station assurance detects whether the distance of the station from the Access Point reaches this threshold during a period.

Intrusion Detection

Access Points 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.

Figure 306. Intrusion Detection Settings

The Access Point 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 572**.

- **Denial of Service (DoS) or Availability Attack Detection**

  A DoS attack attempts to flood an Access Point with communications requests so that it cannot respond to legitimate traffic, or responds so slowly that it becomes effectively unavailable. The Access Point can detect a number of types of DoS attacks, as described in the table below. When an attack is detected, the Access Point 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 Access Point detects a number of types of impersonation attacks, as described in the table below. When an attack is detected, the Access Point 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 Access Point.
Authentication Flood	Sending forged Authenticates from random MAC addresses to fill the Access Point's association table.

Type of Attack	Description
Association Flood	Sending forged Associates from random MAC addresses to fill the Access Point's association table.
Disassociation Flood	Flooding the Access Point with forged Disassociation packets.
Deauthentication Flood	Flooding the Access Point 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 Access Point'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.

Type of Attack	Description
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 199**.
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 97**), then the Access Point 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 574.* 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 Access Point 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.

XMS 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 Access Points rather than for a particular AP or Profile network. See **"SSID Spoofing Auto Block" on page 199**.

RF Intrusion Detection and Auto Block Mode

Procedure for Configuring Intrusion Detection

1. **Intrusion Detection Mode:** Choose an intrusion detection method, or choose **Off** to disable this feature. See "Access Point Monitor and Radio Assurance Capabilities" in the Technical Support Appendix of the Xirrus *Wireless Access Point User's Guide* for more information.

   - **Standard**—enables the monitor radio to collect Rogue AP information.

   - **Off**—intrusion detection is disabled. This is the default value.

   - **Auto Block:** Enable or disable auto blocking of unknown rogue APs (see **"About Blocking Rogue APs" on page 572**). 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 select the **Auto Block** option. 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. Xirrus 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.*

2. **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.

3. **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.

4. **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.

5. **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

6. **Attack/Event**: The types of DoS attack that you may detect are described in the Type of Attack Table on page 570. 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 Access Point 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 Access Point 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.

7. **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

8. **Attack/Event**: The types of impersonation attack that you may detect are described in Impersonation Attacks on page 571. 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 Access Point declares that an attack has been detected. You may modify the **Threshold** and **Period**.

9. **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.

10. Click the **Apply Config** button at the top of the configuration window to apply these changes to the Access Point. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

LED Settings

This window assigns behavior preferences for the Access Point's radio LEDs.
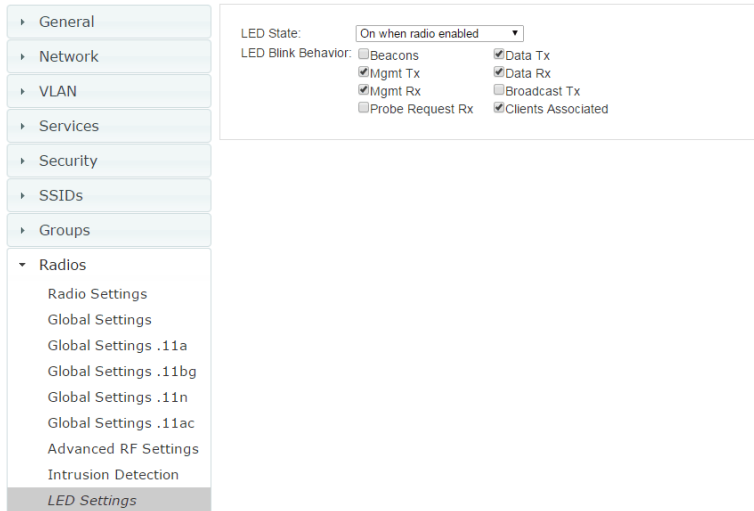
Figure 307. LED Settings

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 Access Point. 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 Access Point'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 Access Point" on page 490**.

Figure 308. 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 a Xirrus feature that helps clients roam to Access Points 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 Access Point "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 Access Point 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

Figure 309. 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 Access Point 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 Access Point'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.*

Figure 310. Filter Lists

User connections managed by the firewall are maintained statefully—once a user flow is established through the Access Point, it is recognized and passed through without application of all defined filtering rules. Stateful inspection runs automatically on the Access Point. 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 Access Point 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 XR-320 and the X2-120, 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 112**.

   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:

   a. **Filter List Name**

   b. **Access Point Filter Count**: The number of filters in this list.

   c. **Edited Filter Count**

   d. **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 Access Point. 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.

	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

Filter List: SSList

Add   Add Preset Filters   Edit   Delete   Move Up   Move Down   Select Columns

Showing: 1 to 14 of 14

Figure 311. 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 XR-320 and the X2-120, 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 Xirrus *Wireless Access Point User's Guide*.

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 Access Point 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 Access Point 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 Access Point" on page 490**.

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 Access Point" on page 490**.

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 433**). 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 112**):

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 ☐

| <All> |
| AH |
| BEETPH |
| DynGate |
| ESP |
| GRE |
| Hamachi |
| Hotspot Shield |
| IPComp |
| IPIP |
| IPsec |
| L2TP |
| OpenVPN |
| PPTP |
| RSVP Tunnel |
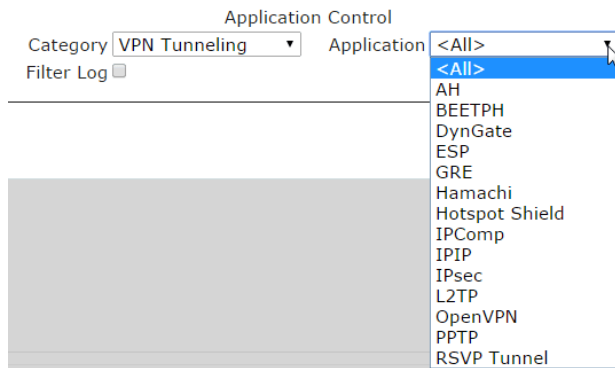
Figure 312. Filter Category/Application

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 Access Point. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

Tunnels

Xirrus Access Points offer GRE (Generic Routing Encapsulation) tunneling with VLAN support. This allows an Access Point 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:

- The Xirrus Tunnel Server (XTS)—see the Xirrus *Tunnel Server User's Guide*.
- VTS —see .

To create a tunnel, you specify the **Local Endpoint**, which should be one of the Access Point'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 Access Point 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

✎ *This feature is only available on XR Series Access Points and Access Points.*

Tunnel Management

This window allows you to create and manage tunnels.
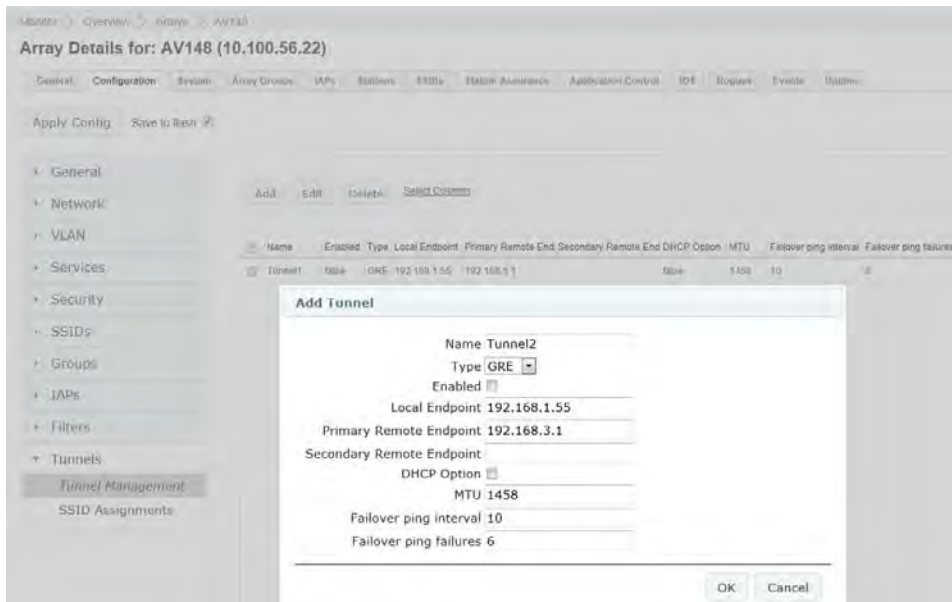
Figure 313. Tunnel Management

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 Access Point Gigabit or 10 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 Access Point snoops station DHCP requests and inserts relay agent information (option 82, in the circuit-ID sub-option) into these DHCP packets. Information inserted includes Access Point 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 Access Point 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 Access Point. 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 Access Point.

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.

Array Details for: AV148 (10.100.56.22)

| General | Configuration | System | Array Groups | IAPs | Stations | SSIDs | Station Assurance | Application Control | IDS | Rogues | Eve |

Apply Config   Save to flash ☑

- ▸ General
- ▸ Network
- ▸ VLAN
- ▸ Services
- ▸ Security
- ▸ SSIDs
- ▸ Groups
- ▸ IAPs
- ▸ Filters
- ▾ Tunnels
  - Tunnel Management
  - *SSID Assignments*

	SSID	AV148A	test	wds-21A	xirrus	
Tunnel						
Tunnel1		☑	☐	☑	☐	Clear
Tunnel2		☐	☑	☐	☑	Clear

Figure 314. Tunnel SSID Assignments

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 494**).

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 Access Point. To make these changes permanent, check **Save to flash** before using the **Apply Config** button.

XMS Administration

XMS is administered from **The XMS Web Client** with a set of special tools.

An overview of managing the server is given in the following sections:

- **"About the XMS Database" on page 595**
- **"Managing XMS on Virtual Appliances" on page 596**

About the XMS Database

The XMS database maintains the properties, status, and statistics for all the managed wireless Access Points 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 XMS is running. See **"Viewing XMS Server Status" on page 600**. 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 XMS 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 XMS provides a client option for managing backups, they can be initiated from any client.

To manage the database, see **"Database Backup Settings" on page 605**.

XMS 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 XMS on Virtual Appliances

Use the browser-based XMS web client (**Figure 315**) to manage the XMS server. There are options to perform mandatory initial configuration, to restart or reboot the server, and for server maintenance. The XMS server is started automatically when your Appliance is restarted.
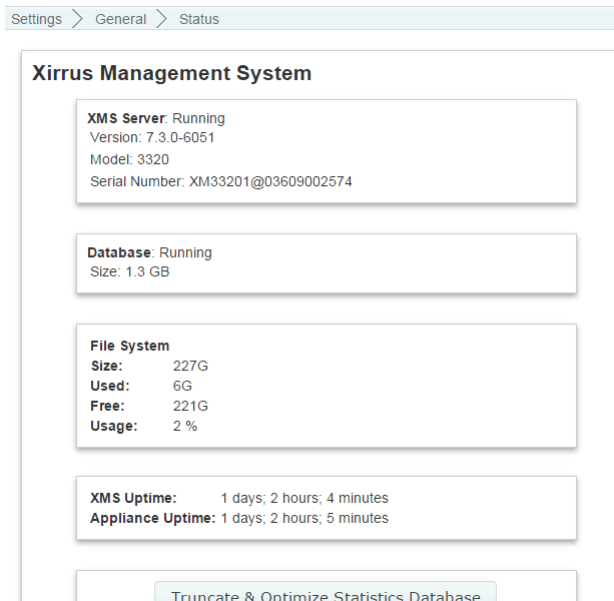
Figure 315. Server Management using the Web Client

The web client has multiple pages that manage settings for different XMS 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 597**
- **"Initial Server Setup" on page 599**
- **"Viewing XMS Server Status" on page 600**
- **"Network Settings" on page 603**
- **"Date and Time Settings" on page 604**

Accessing the Web Client

Note: Web client access to the XMS server requires access to port 9090 and 9443. Ensure that this port is open in any firewalls that exist between your browser and the XMS server.

To access the web client, set your browser's URL to the XMS server machine's IP address or host/domain name, followed by **:9090**. For example, **http://192.168.10.40:9090**.
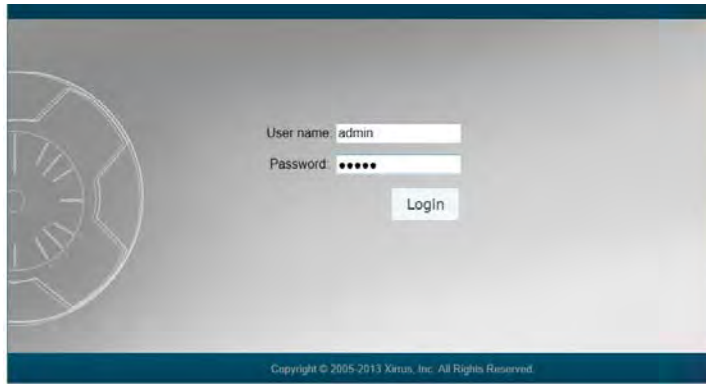
Figure 316. Starting the Web Client

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 315**) 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 XMS 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 XMS server for proper performance. If you have already completed these steps, you may skip this section.

1. **"XMS Setup Wizard" on page 639**—use the XMS Setup Wizard to enter the license for the XMS server and start discovery of the wireless network.

IMPORTANT! The XMS server does not have a default backup schedule, so you must create one after installation.

2. **"XMS Users" on page 615**—set up user accounts for XMS.

Initial Network Settings

Note: The XMS 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 XMS Server License" on page 655**.

1. Select **Settings** >**Network** to display the Network Settings window.
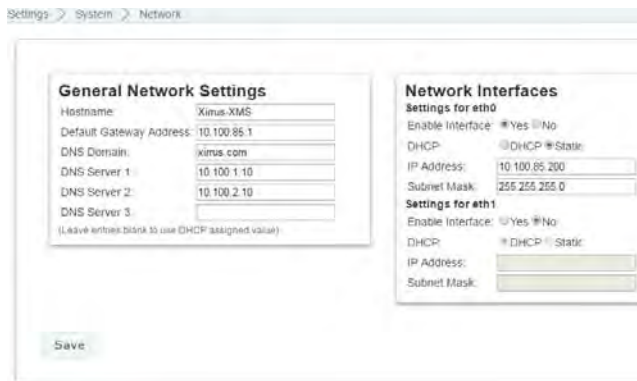
Figure 317. Changing Network Settings

Note: You may use one or both of the XMS Management Appliance's Ethernet ports. If using both, then one of the ports is typically reserved for management.

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 10.0.2.10; for eth1 it is 10.0.2.11.

3. The **Hostname** of the Appliance is set to Xirrus-**XMS** by default. If you wish to change the Appliance's DNS Hostname, please see **"General Network Settings" on page 604** for other changes that you should make to ensure proper operation of XMS in your network.

Viewing XMS Server Status

Click the **Status** link to review the status and version number of the XMS **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. XMS **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.

- **About Disk Usage Alarms**
- **Truncate & Optimize Statistics Database**

Figure 318. The Status Page

About Disk Usage Alarms

XMS checks the space available on the server's file system on an hourly basis. If more than 75% of the space has been used, XMS will issue an alarm (see **"Alarms" on page 105**) and alert you with a banner at the top of the page. If more than 90% of the space is used, it will also stop all data polling until there is more room available on the file system—i.e., no more statistics will be gathered and added to the database. In addition, no changes will be allowed on the **Polling Settings** page. You have two options to provide more file system space:

- Use **Truncate & Optimize Statistics Database**, see below.
- Contact Xirrus customer support to find out how to increase file system size.

After you have decreased the space used to under 73%, the alarm will be automatically reset within an hour, the next time XMS checks disk space. The banner will also disappear after that, when you refresh or change pages. If space used goes below 88%, polling will be re-enabled when disk space is checked.

- **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 XMS server will be shut down, statistics are deleted, and the database is optimized and compacted. When this is complete, the XMS server is rebooted.

- **Restart Application**

    If XMS is not running properly, you may click the **Restart Application** button on the lower left to restart the XMS 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 XMS related processes in an orderly manner before rebooting. Rebooting and restarting will take about two minutes on a new Management Appliance. As XMS is used and the database grows, startup integrity checks will take longer. For shutdown, see below.

Shutting down the XMS Server

Shutting down the server incorrectly can cause problems the next time you start XMS. 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.

Figure 319. Changing Network Settings

Note: You may use one or both of the XMS 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. For recommended IP addressing, please see **"Initial Network Settings" on page 599**.

- **General Network Settings**

  The **Hostname** of the Appliance is set to **xirrus-xms** by default. Note that hostnames are not case-sensitive. Xirrus Access Points send traps to the hostname Xirrus-**XMS** 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 **Xirrus-XMS** 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 XMS server host machine and all Access Points using SNMPv3. This is because SNMPv3 requires synchronization between the XMS server and the Access Points 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 Access Points from the database. This means that the Access Point will appear to be down and statistics will not be polled until the Access Point is re-discovered. A manual refresh of the Access Point should remedy the situation. See **"Add Devices" on page 183***.*

Figure 320. 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, XMS will reboot.

Database Backup Settings

The XMS server does not have a default backup schedule, so you should perform the following steps soon after you have installed the XMS 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 XMS backups:

- **"Manage Locations" on page 606**
- **"Manage Schedules or Backup Now" on page 610**
- **"Restore" on page 612**
- **"Import Backup Archive" on page 613**
- **"Backup Status" on page 614**

Note: On 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 XMS 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.

Figure 321. Backup Locations List

The XMS 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 322**)
  - 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.

Backup Location Manager

Add Backup Location

Location Name: MainBackup

Location Type: Windows File Share

Path:).54.10\10.100.54.10-share

Domain:

User Name: administrator

Password: ••••••••••••

Confirm Password: ••••••••••••

Figure 322. Backup Location—Windows File Share

- **Location Type: FTP** (**Figure 323**)

  - 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.

Figure 323. Backup Location—FTP

● **Location Type: SCP** (**Figure 324**)

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.

Figure 324. Backup Location—SCP

Click **OK** when done. XMS 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.

	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 325. 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.

Figure 326. Backup Now

To enter a schedule, click the **Schedule a Backup** button. (**Figure 327**) 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 327**) 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**.

Figure 327. 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 327** 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 328**) The most recent backup is listed first.
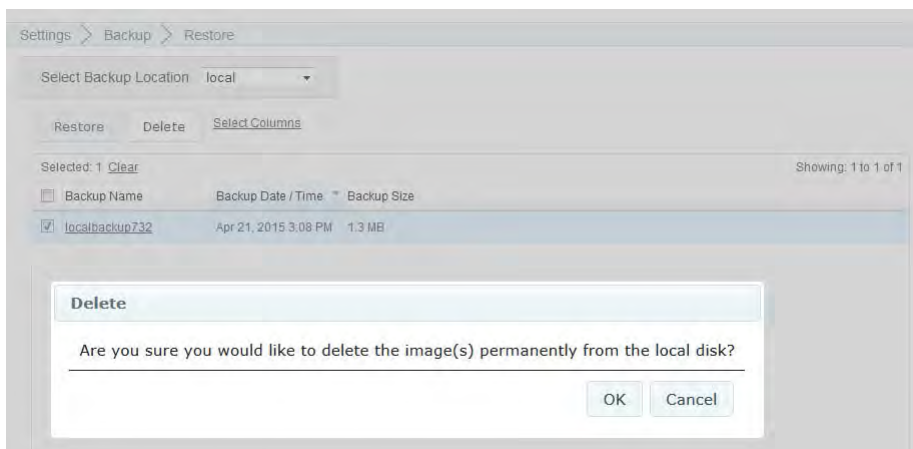
Figure 328. Restoring Backups

If you wish to restore your XMS 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 XMS client applications.
- Reboot the XMS 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 XMS server so that it can be restored. This is instead of using a backup location. For example, you can back up an XMS 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 XMS server.
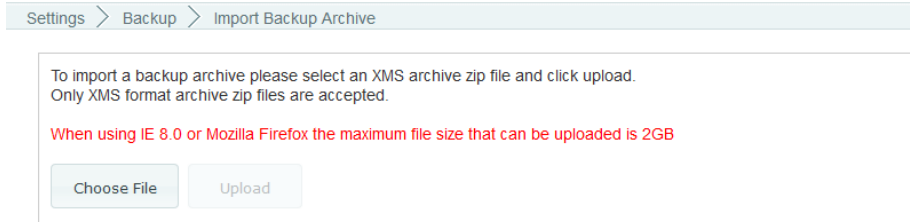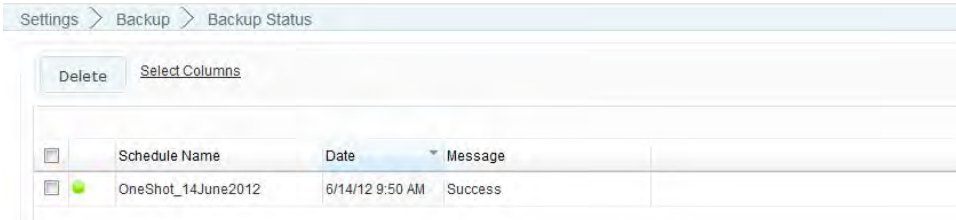
Figure 329. Import Backup Archive

Backups are archive zip files that have a specialized XMS format. Only files in this XMS-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.

Figure 330. Backup Status

XMS Users

This page manages local XMS user accounts allowing access to XMS. You may add, edit, delete, or export accounts, or change passwords. Note that XMS access may also be authenticated using RADIUS—see **"Admin RADIUS" on page 648**. If you have configured Admin RADIUS servers, then authentication will be attempted using those first. If that fails, the local XMS user accounts will be tried.

Open the XMS Users page by clicking the **Settings** link near the top of the window, then select XMS **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 66**.
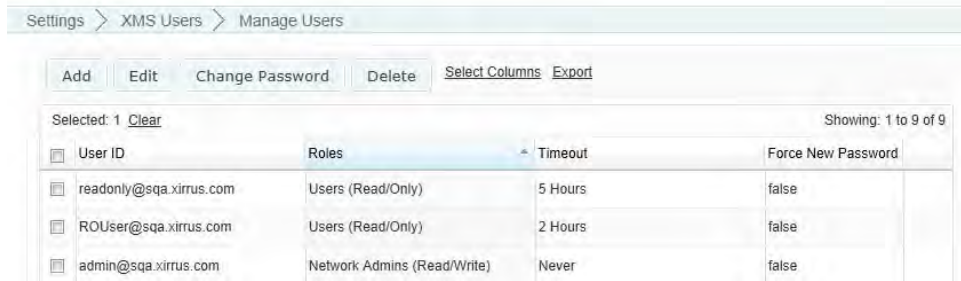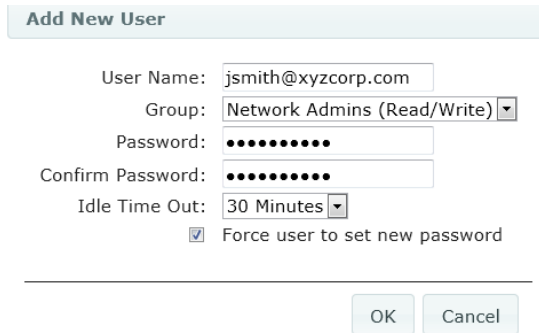
Figure 331. Managing XMS User Accounts

This page contains a list of all user accounts currently available. (**Figure 331**) To create an account for a new XMS user, click the **Add** button on the upper left. The Add New User dialog is displayed. (**Figure 332**)

Figure 332. Add an XMS 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**—it is optional for the name to be in the form of an email address.

- **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 XMS settings or to Access Point 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 XMS for Access Points. For example, you might use extra columns to add an Asset Tag to each Access Point, 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 Access Point 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 Access Points table, where you can place Access Point 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 Access Point.

Create Custom Fields

This page is used to define a new column for the Access Points 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 Access Point. For example, you might add an asset tag column, or a column for notes regarding support actions for this Access Point.

Open this page by selecting **Create Custom Fields** from the **Settings** menu near the top of the window.

Figure 333. 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 Access Points 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 F**ield 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 Access Points 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 67** for more details.

To populate the new column with data for as many Access Points as you like, see **"Import Access Point Custom Fields" on page 138** or **"Custom Field Values" on page 135**.

Create Custom Actions

This page allows you to define a custom button that adds a new function to the Access Points 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 Access Points list using the **Create Custom Fields**, and then you entered values for this field for each Access Point 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 Access Point's asset tag, using the URL:

http://track.xyzcorp.com/?assettagno=%assetTag%

Figure 334. 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 334**)

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**.

XMS 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 Xirrus 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.

Access Point Diag Log Upload

This page is provided as a utility for gathering data from Access Points in your network that are running beta release software, although it may be used with Access Points running older AOS versions as well. It provides a mechanism that can automatically upload Access Point diagnostic logs to Xirrus 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 Access Points from which to gather diagnostic logs. When an Access Point Diag Log Upload starts, all of the selected Access Points will generate diagnostic information, which is then uploaded by this utility.

Figure 335. Access Point Diagnostic Log Upload

The settings for this page are described in the following sections:

- **Set Up FTP Server**
- **Enter a Schedule (optional)**
- **Select Access Points and Test Connection**

Set Up FTP Server

Specify **Server Name** or **IP Address**, the **Directory**, and login details. Typically, if Xirrus 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 Access Points and Test Connection

Select the check boxes to the left of the Access Points whose diagnostic files are to be collected. If you are sending data for a set of Access Points that are running a particular software release, you may find it handy to sort the Access Points by clicking on the **Software Version** column header.

When you are done, click the **Test Connection** button to check that the Access Points 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 Access Points 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.

XMS API

XMS 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 XMS database. The interactive API Documentation page provides documentation for the API. Security for the XMS RESTful API is provided with tokens granted using an OAuth 2.0 mechanism.
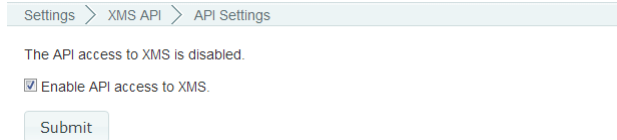
Your custom application may use the XMS API for purposes such as integrating with third party applications or creating your own applications for network analysis. Using the RESTful API eliminates the need to use SNMP which can be cumbersome for polling large amounts of data. Results are returned in JSON 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 XMS API is described in the following topics:

- **"API Settings" on page 625**
- **"Obtaining an OAuth Token" on page 625**
- **"Using the API Interface" on page 626**
- **"API Documentation" on page 627**
- **"API Documentation Toolbar" on page 631**

API Settings

The XMS RESTful API is disabled by default. Use this page to enable granting of tokens and access to the XMS API. To open this page, click **Settings** at the top of the page and then use the **API Settings** link.

Figure 336. API Settings

Make sure that the checkbox for **Enable API access to XMS** is checked, then click the **Submit** button.

Obtaining an OAuth Token

Security for the XMS RESTful API is provided with OAuth 2.0. Your custom application must request a token from an authorization server on the XMS server. That token is then presented to access the XMS 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 XMS 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://*<XMS-server hostname or IP addr>*:9443/oauth/token

- **client_id**: username of an administrator or user account on the Access Point (username and client_id must match).
- **client_secret**: password for the same account on the Access Point.
- **grant_type**: **client_credentials**

The authorization server provides a token that your application may use for read-only access the XMS 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 XMS 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://<XMS-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.

Figure 337. XMS API Documentation

The XMS 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 XMS is broken into a number of headings by type, such as: **applications, arrays,** and **profiles**. Each heading is a node that may be clicked to expand or collapse the list of corresponding API requests available in XMS. 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 **/arrays**. Click again to collapse (hide) the list. The **.json** string in the names shown, for example **GET / arrays.json/{array-name}/ssids**, indicates that the return values use JSON formatting. A parameter in brackets, e.g., **{array-name}**, indicates that information is returned for a particular item (in this case, the named Array), rather than for all Arrays.

Figure 338. 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 47**.

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 70**. For example, if you use **GET /search.json/arrays/ {search-query}** to search for "100", then the results would include Arrays 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 /arrays.json/{array-name}/ssids**. Click again to collapse (hide) the API details.

Figure 339. API — GET Request Details
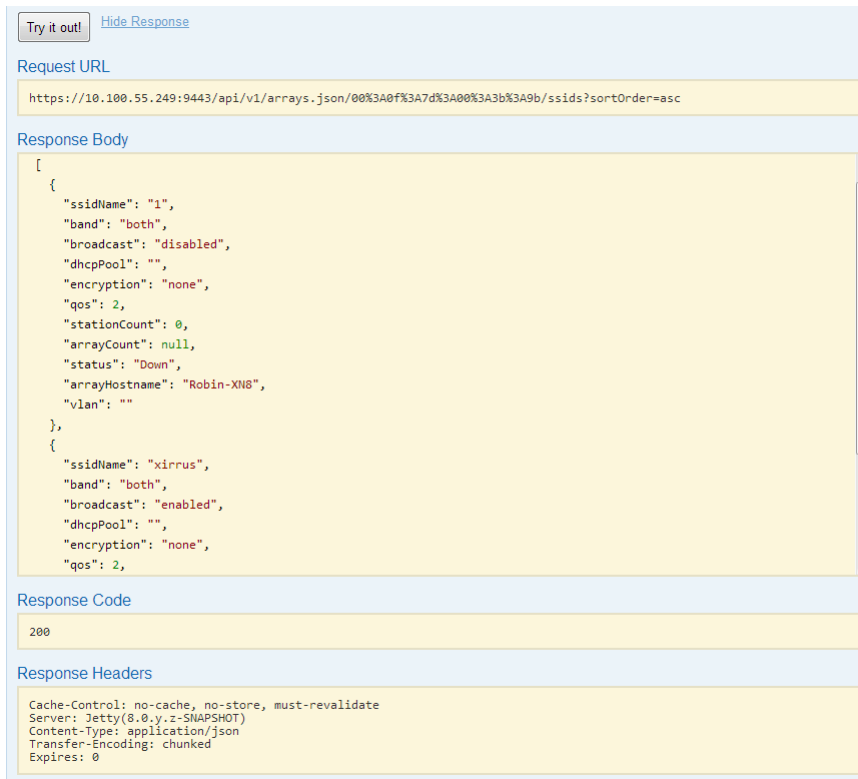
High-level details are shown, including:

- **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 /arrays.json/{array-name}** returns data for a particular Access Point, while **GET /arrays.json/** returns data for all Access Points.

Trying a GET Request

The **Try it out!** button allows you to send the GET request to the XMS API and see its response. Developers can use this feature to design and implement applications that use this response.

Figure 340. API — GET Request Response

Enter the desired **Parameters** and click the **Try it out!** button. An example is shown in **Figure 340**.

The figure above shows the response for **GET /arrays.json/{array-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 71**. 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
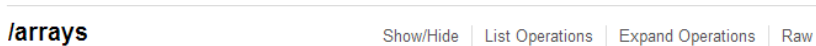
Figure 341. API Documentation Toolbar
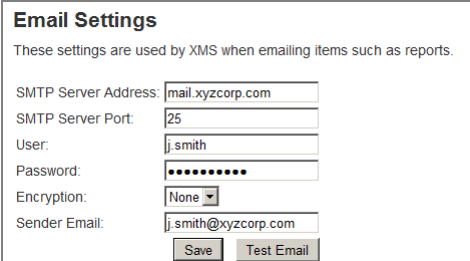
The Status and Settings sections each have a toolbar as shown above, offering the following options.

- **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 XMS to yourself or others. When XMS needs to send email, it uses an SMTP server to do so. Before XMS can send any emails, you must specify which server to use and provide authentication information.

Email Settings

These settings are used by XMS when emailing items such as reports.

SMTP Server Address:	mail.xyzcorp.com
SMTP Server Port:	25
User:	j.smith
Password:	••••••••••
Encryption:	None
Sender Email:	j.smith@xyzcorp.com

Save   Test Email

Figure 342. Changing the Email Server

To specify the SMTP server for XMS to use, click **Settings** at the top of the page and then use the **Email** link. (**Figure 342**)

Enter your **SMTP Server Address** and **SMTP Server Port**. Specify the **User** and **Password** that XMS must use to access the server. Select an **Encryption** type.

When XMS 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 XMS is able to use SMTP to successfully send an email.

Click **Save** when done.

Polling Settings

Figure 343. 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 XR-320. 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.

XMS offers a rich set of statistics in its **Dashboard**, **Reports**, and other windows. These statistics are obtained by polling the managed Access Points using SNMP. The default polling rate is **FAST**, providing near real-time data. If you have a large number of Access Points under management, we recommend that you decrease

the polling speed to enhance XMS 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
Access Point 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 Access Points
Fast	up to 100
Medium	up to 250
Slow	over 250

After you change the polling rate, each Access Point will be reconfigured for the new polling interval. Depending on the number of Access Points under management, it might take some time to process the change on all Access Points (up to 10 seconds per Access Point). You may continue to use XMS while this change is proceeding.

XMS Call-back Address

Figure 344. Changing the XMS Call-back Server

Some communication between APs and XMS, such as secured web-socket connections and **Perform or Schedule Upgrade** via SCP, use the XMS 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 XMS server's network.

The current call back address is displayed. (**Figure 344**) To provide an alternate IP address for APs to access XMS, click the **Use alternate IP address** checkbox and enter the desired **IP Address**. Click **Save** when done.
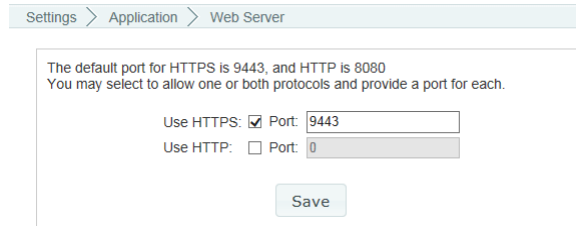
Note that Access Points will use Port 22 for SSH to the XMS server.

> *If the IP address of the XMS server is changed, you must restart the XMS server. This will automatically change the call-back address to the new IP address. Next, refresh all APs (using **"The Configure Access Points Toolbar" on page 119**) so that the new call-back IP address will be configured in the APs.*

Web Server

This page allows you to change default settings for HTTP and HTTPS access to the XMS server, including the ports used.

Figure 345. Web Server
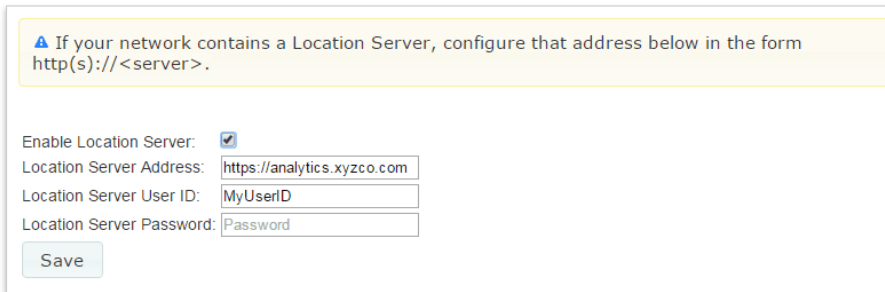
By default, only HTTPS access is enabled, and it uses port 9443.

Note that the old URL for accessing XMS at *http://<xms-server>:9090* may still be used. It will automatically redirect you to HTTPS at the port configured above.

Location Server

Xirrus Access Points offer an integrated capability for capturing and uploading visitor location data to a location server (see **"Location" on page 453** and **"Location Service Data Formats" on page 664** for details). You can use the Location Server settings on this page to set the location server globally in all APs and Profiles to the same value at once. Note that APs that run AOSLite do not provide location data.

If you are using the Xirrus Positioning System (XPS) to optimize location reporting performance for XMS-E maps or to push location data to a third party location server, you must use this page to enter location server settings. XPS is an optional service that you may obtain from Xirrus. Once you install it, its operation is automatic, invisible, and requires no user action other than the settings on this page.

Figure 346. Location Server

Procedure for Configuring Location Server

1. **Enable Location Server:** Check this box to enable the collection and upload of visitor location data for all APs under management. If you use this global setting, the **Services > Location** page for profiles configuration and for AP configuration will no longer be displayed (i.e., they are hidden). They will be displayed again if you uncheck this setting.

2. **Location Server Address**: If Location Server is enabled, enter the URL of the location server (IP address and hostname forms are both accepted). If this URL contains the string **euclid**, then the Access Point knows that data is destined for a Euclid location server.

   For a Euclid location server, use the URL that was assigned to you as a customer by Euclid. The Access Point will send JSON-formatted messages in the form required by Euclid via HTTPS.

   For any other location server, enter its URL. The Access Point will send JSON-formatted messages in the form described in **"Location Service Data Formats" on page 664**.

3. **Location Server User ID**: Enter your customer ID for the location server.

4. **Location Server Password**: Enter the password for the location server.

5. Click the **Save** button to apply these changes across the managed network. These settings will be applied to all APs (except for those that run AOSLite), overriding any previous location server settings.

SNMP Trap Receivers

Just as Access Points send SNMP traps to the XMS server, the XMS server can send traps to top-level supervisory software. Any Access Point 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.

Figure 347. 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 347**). Enter the **Host Name or IP Address** of the destination that is to receive traps sent by the XMS 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.

XMS Setup Wizard

The XMS 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 Access Points in the XMS 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 **XMS Setup Wizard** from the **Application** section.

Perform the wizard's steps as discussed in the following sections.

1.   **XMS License** (**Figure 348**)

Figure 348. XMS Setup Wizard—XMS License

Xirrus 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**—XMS 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 Access Point Count**—the server is licensed to manage a specific maximum number of Access Points. To manage additional Access Points, please contact Xirrus 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 XMS Server License" on page 655**.

2. **Community Names** (**Figure 349**)

Figure 349. XMS Setup Wizard—Community Names

This page is used to add or delete SNMPv2 community names. The XMS discovery process searches networks using both SNMPv2 and SNMPv3. XMS discovery has default SNMPv2 entries which match the factory default SNMP v2 settings in Access Points and PoGE injectors. However, for proper security on your Xirrus devices, we recommend that you change these defaults by setting your own SNMPv2 community strings

on Xirrus Access Points. Thus, you must add those community names or user names/passwords to XMS 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 187**.

3. **SSH Users** (**Figure 350**)

Figure 350. XMS Setup Wizard—SSH Users

Some actions, such as **Perform or Schedule Upgrade** and **Deploy Config Template**, require Access Points to download files. When it instructs an Access Point to fetch a file from the server, XMS needs to know a **User Name** and **Password** to gain access to the Access Point shell. Enter an Access Point's **User Name** and **Password**, and click **Add**. Repeat this for all of the accounts needed to gain access to all of your Access Points. When XMS needs access to an Access Point, 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 Access Point.

Click **Next >** to proceed to the next step. For more information, please see **"SSH Users" on page 190**.

4. **Network** (**Figure 351**)

| 1 | XMS License | 2 | Community Names | 3 | SSH Users | **4** | **Network** | 5 | Time Zone | 6 | Backup |
| 7 | Email | 8 | SNMP Trap Receivers | 9 | Discover Devices | 10 | Results | 11 | Finish |

< Previous   Next >   Cancel

Configure your network settings.

General Network Settings

Hostname:	Xirrus-XMS
Default Gateway Address:	10.100.54.1
DNS Domain:	xirrus.com
DNS Server 1:	10.100.1.10
DNS Server 2:	10.100.2.10
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:	10.100.54.14
Subnet Mask:	255.255.255.0
Auto Negotiate:	● Yes ○ No
Duplex:	● Full ○ Half

Settings for eth1

Enable Interface:	● Yes ○ No
DHCP:	○ DHCP ● Static
IP Address:	12.12.1.2
Subnet Mask:	0.0.0.0
Auto Negotiate:	● Yes ○ No
Duplex:	● Full ○ Half

Figure 351. XMS Setup Wizard—Network

This step manages IP configuration for the server. For recommended IP addressing, please see **"Initial Network Settings" on page 599**.
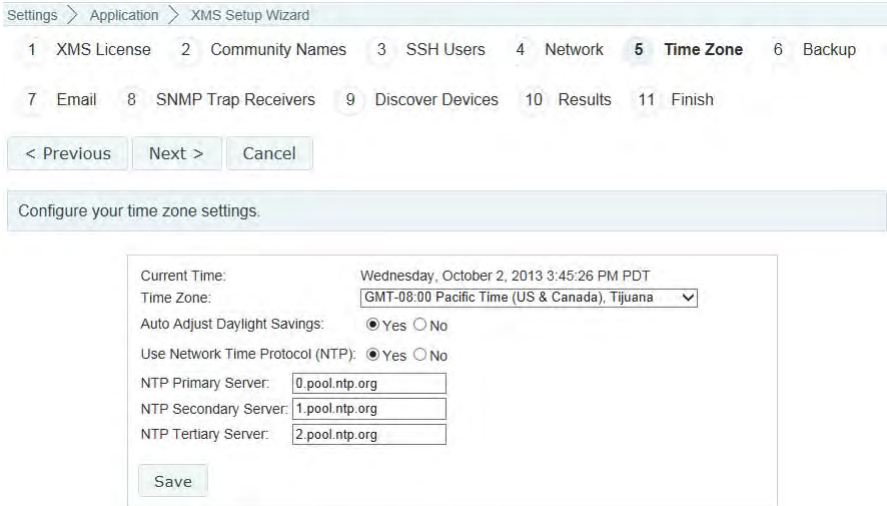
Hostname defaults to **xirrus-xms**. Xirrus Access Points send traps to **xirrus-xms** to announce their presence and speed discovery. Thus, if you change the server's Hostname, you should create an alias in your DNS server so that the server is accessible using both **xirrus-xms** and the new host name.

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 XMS 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 352**)

Figure 352. XMS Setup Wizard—Time Zone

To use SNMPv3 successfully, system time must be set using the same NTP server on both the XMS server host machine and all Access Points 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 Access Points 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 604**.

6. **Backup** (**Figure 353**)

Figure 353. XMS Setup Wizard—Backup

This page sets backup locations for the XMS database. For data protection, define and use at least one location for backups other than on the XMS server. When you are finished specifying the server type, path and account to use, XMS will verify that it is able to access the location and log in. See **"Manage Locations" on page 606** 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.
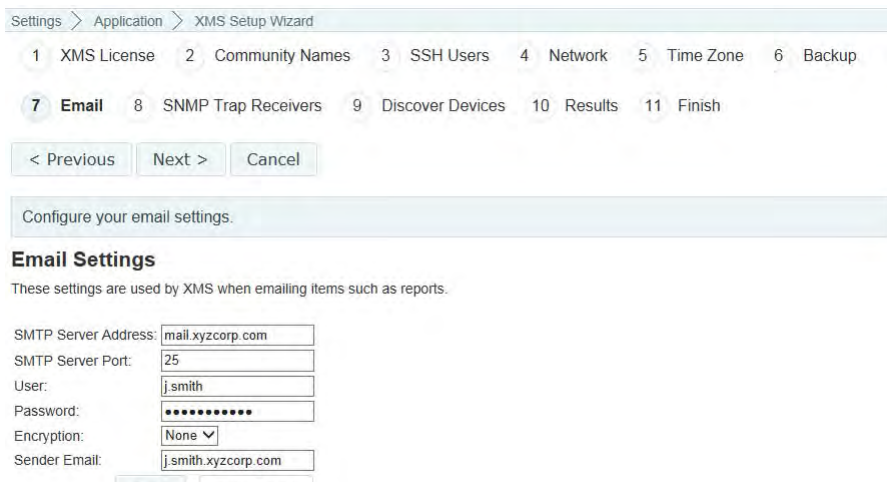
SCP (Secure Copy Protocol): specify the **SCP Server** used for backup, entering its hostname, DNS name, or IP address. Specify the **SCP**

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 610** to schedule automatic backups.

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

7. **Email** (**Figure 354**)

Figure 354. XMS Setup Wizard—Email

Some XMS features, such as reports and alarm notifications, send emails to specified recipients. XMS uses an SMTP server to send the emails. For more information, please see **"Email Settings" on page 632**.

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 355**)

Figure 355. XMS Setup Wizard—SNMP Trap Receivers

The XMS server can send traps to top-level supervisory software. Access Point 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 XMS 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 638**.

9. **Discover Devices** (**Figure 356**)
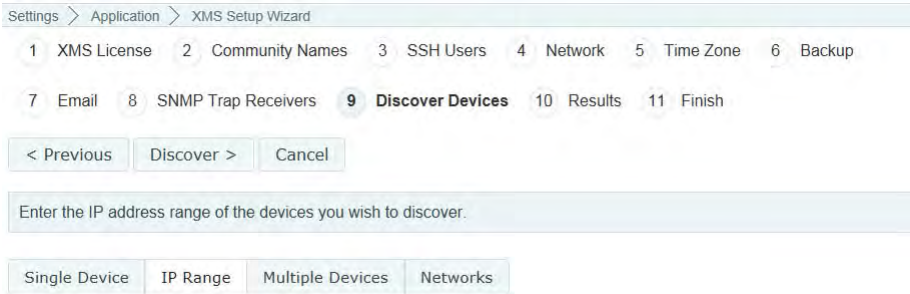
Figure 356. XMS Setup Wizard—Discover Devices

This step is used to add subnetworks or devices to XMS. You may individually add one or more Access Pointsand/or Xirrus-supplied switches or managed power injectors to XMS, or specify a network and have XMS 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 Access Points 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 Access Points, to avoid creating excess traffic by discovering a needlessly large network.

For more information, please see **"Discovery" on page 178** and **"Add Devices" on page 183**.

Click the **Discover** button to start discovery.

10. **Results** (**Figure 357**)
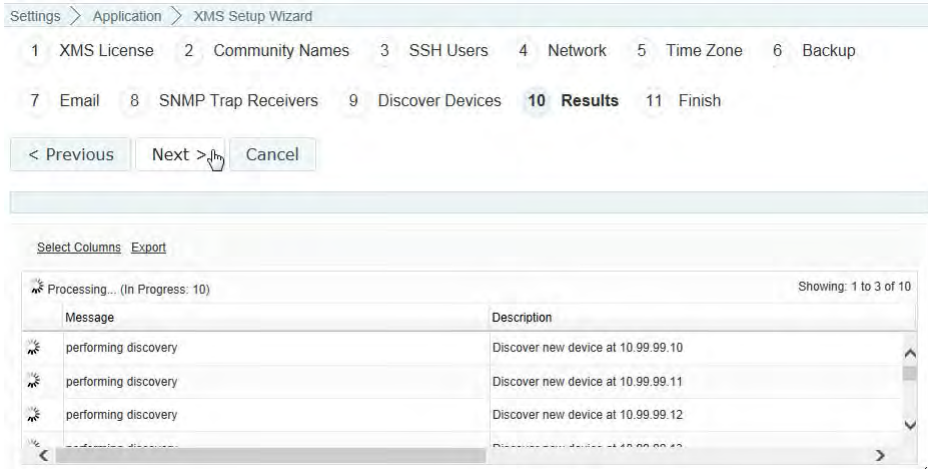
Figure 357. XMS Setup Wizard—Results

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 XMS 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 XMS users/administrators. This enables XMS 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 XMS administrator accounts configured on the **XMS 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 **XMS Users** are tried.

About Creating Admin Accounts on the RADIUS Server

Permissions for XMS administrator accounts in RADIUS are controlled by the RADIUS Vendor Specific Attribute (VSA) named **Xirrus-Admin-Role**. In the RADIUS server, set a user account's Xirrus-Admin-Role to **0** (zero) for User (read-only) privileges. Set it to **1** for Super-Admin (read-write) privileges. For more information about the RADIUS VSAs used by Xirrus, see "RADIUS Vendor Specific Attribute (VSA) for Xirrus" in the Technical Support Appendix of the Xirrus *Wireless Access Point User's Guide*.

Figure 358. Admin RADIUS

Procedure for Configuring Admin RADIUS

Use this window to enable/disable XMS 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 XMS. 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 XMS will wait for the RADIUS server to respond to the authentication request. If the request times out, XMS 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 Access Point 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 Access Points. 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 Access Point, and the **Status** of the task. (**Figure 359**)

Figure 359. Audit Log

Viewing Server Log Files

Log File	Log Size
alert_audit.txt	1 KB
ConfChange_.log	8 KB
ConfChange_.log.old	8 KB
ConfChangeErr_.log	0 KB
ConfChangeErr_.log.old	0 KB
misc.txt	231 KB
mserr.txt	2 KB
msout.txt	4 KB
mysql_repair_result.txt	17 KB
nmserr.txt	12 KB
nmsout.txt	94 KB
stderr.txt	5 KB
stdout.txt	36 KB
transactionLogs.txt	486 KB
updatemanagerlog.txt	0 KB
updatemanagerlog1.txt	0 KB
updatemanagerlog2.txt	0 KB
xirrusdiscovery.txt	6 KB
xirrusdpoller.txt	260 KB
xirrusout.txt	82 KB
xirrussched.txt	2 KB
xirrussnmp.txt	4 KB
xirruswork.txt	70 KB
xms-wmi.txt	145 KB

Figure 360. 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 XMS server while it is running. Click a link to view the contents of that file (**Figure 361**). These files journal the operation of the XMS server software, rather than reporting on the operation of the wireless network.

Log files are intended for use by Xirrus 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 XMS creates a zip file containing all of the logs. If you click **Export** on a page for a particular log file, then XMS 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.

Figure 361. 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 362**, 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 362. Multiple Log Files

Managing the XMS Server License

This section describes the license to use the XMS server. If you are looking for information regarding using XMS to manage Access Point licenses, please see **"Access Point Licenses" on page 200**.

For full operation, the XMS 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 Access Point. Thus, without an appropriate license, **Discovery** will stop at one Access Point and will not allow more Access Points to be added. If you do not have a valid license, you will be notified each time you start an XMS client.

Valid XMS licenses are typically for a particular number of radios. A two-radio AP (for example, the XR-630) consumes one license. A four-radio AP (for example, the XR-2426/2436) consumes two licenses. When XMS has discovered the maximum permitted number of radios, no additional Access Points will be discovered.

Use the following steps to enter your license.

1. Click the **Settings** button, then click **XMS License**. The XMS License Info page appears.

Figure 363. XMS Server License

2. Xirrus 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**—XMS server's product name.

- **Max Version**—the highest release number of XMS supported by this license. All incremental upgrades to the XMS release shown are also supported. For example, if Max Version is 9.0, then this license will run XMS Release 9.0.999, but Release 9.1 will require an updated license. Note that Max Version does not restrict the versions of Xirrus AP software you may run—it only applies to the XMS version.

- **Max Radio Count**—the server is licensed to manage a specific maximum number of radios. To manage additional radios, please contact Xirrus to upgrade your license.

- **Expiration Date**—the date that this license expires.

Performing Server Upgrades

Settings > Maintenance > Upgrade

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: 7.4.0-6556

Choose File   Upload
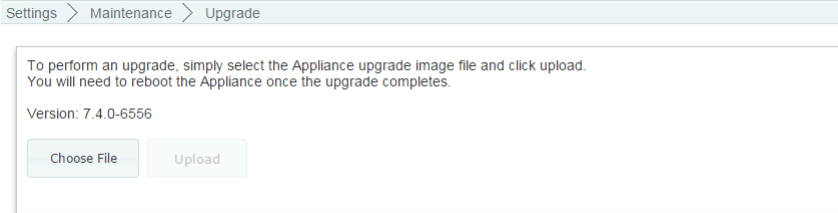
Figure 364. Upgrading XMS Software

This page is used to update the XMS server. Select the **Upgrade** link to display this page.

When you receive upgrade software from Xirrus, it comes in this form:

- For the Virtual Appliance (VMware or Hyper-V)—a .vau file. For example:

XMS-8.0.5-7407.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 Xirrus, 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 XMS server.

Resetting the XMS Server

Settings > Maintenance > Factory Reset

WARNING! This operation will delete all XMS data and settings but preserve network and date/time settings.
Perform XMS Reset
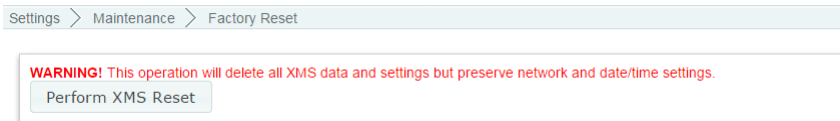
Figure 365. Resetting XMS

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 XMS database (but it does not delete backup files). It also returns the XMS server back to all of its factory default settings, except that **Network Settings** and **Date and Time Settings** are retained.

Click the **Perform XMS 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**.

Technical Support

This chapter provides valuable support information that can help you resolve technical difficulties. Before contacting Xirrus, review all sections in this chapter and try to determine if your problem resides with XMS, the server platform, or your network infrastructure. Section headings for this chapter include:

General Hints and Tips for Xirrus Management Appliances

This section provides some useful tips that will optimize the reliability and performance of XMS.

- You must terminate all applications before shutting down the server Appliance. This includes closing down the client interface and the server. For more information, go to **"Shutting Down the XMS Server" on page 33**.

- For best performance, the Management Appliance should be mounted in a dust-free and temperature-controlled environment.

- Ensure that the Management Appliance receives adequate ventilation at all times. The unit's cooling fans are mounted on the rear panel. Do not obstruct the fans.

- Never use the Management Appliance chassis as a base for heavy monitors or other equipment.

- Some Appliance management operations may take a few minutes to complete. Always be patient and wait for these operations to finish before attempting another task.

Frequently Asked Questions

This section answers some of the most frequently asked questions regarding the functions and operation of XMS.

Q. **Why won't my browser connect to the XMS server to start the XMS 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 XMS server during installation of the XMS 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 XMS. See **"Web Server" on page 636**.

Q. **Why will XMS not discover an Access Point, even though the Access Point is connected to the network and functioning correctly?**

A. SNMPv2 or v3 (Simple Network Management Protocol) must be enabled on the Access Point. Log in to the Access Point and check the SNMP settings. If the problem persists, check that the Access Point is on the same subnet as the XMS server.

For discovery of a device (Access Point or PoGE injector), 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 187**. The default SNMPv2 community string in XMS matches the Access Point default value.

When an Access Point boots up, it sends an SNMP trap to the XMS server's default hostname, **xirrus-xms**. XMS can then add it to its discovered devices list. This Phone Home feature requires DNS to resolve the hostname **xirrus-xms** correctly. Thus, if you change the host name of

the XMS server, you must configure DNS to resolve **xirrus-xms** to the actual name of the XMS server host.

Q. **XMS discovered my Access Point using SNMPv3, and the Access Point has connectivity and is running OK, but XMS reports that the Access Point is down.**

A. To use SNMPv3 successfully, system time must be set using an NTP server on both the XMS server host machine and on all Access Points using SNMPv3. This is because SNMPv3 requires synchronization between the XMS server and the Access Points 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 Access Points from the database. This means that the Access Point will appear to be down and statistics will not be polled until the Access Point is re-discovered. A manual refresh of the Access Point will remedy the situation. See **"Add Devices" on page 183**.

Q. **When managing large Access Point deployments, will the performance of the network be compromised?**

A. No. XMS 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.

XMS Default Alarms and Events

XMS alarms are generated in three ways:

- Custom alarms that you define. See **"Alarm Definitions" on page 172**.

- **Default Alarms and Events**—situations that XMS detects while monitoring the network. See the table below.

- Traps received from devices (APs or switches). See the table in **Alarms from AP Traps or Other Device Traps**.

Default Alarms and Events

Type	Description	Severity
Alarm	Xirrus 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**
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 the *Xirrus Wireless Access Points User's Guide.*

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 XMS 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
radioMixInvalid	In this software release, Wave 2 radio cards cannot be mixed with other radio types

Location Service Data Formats

Xirrus Access Points 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 453** 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.

Data Format Table

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.
- **X** indicates that this data is *only* sent if the string **xirrus** is found in the URL.
- **-X** indicates that this data is *not* sent if the string **xirrus** is found in the URL. The AP assumes that you are using location based services for stations, and reduces the size of messages by dropping unneeded fields from the output.

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 - Access Point host name
ln	Location Name	N	Header - Access Point 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 Access Point is rebooted)
ax	PositionX	X	These location coordinates are sent to the AP by XMS-Enterprise. They appear only if the AP has been placed on an XMS map. *
ay	PositionY	X	
az	PositionZ	X	
sc	PositionScale	X	
ro	PositionAngle	X	
fu	PositionMount	X	
gb	PositionGlobal	X	
mp	MapName	X	
la	GpsLatitude	X	
lo	GpsLongitude	X	
el	GpsElevation	X	
ra	GpsReference	X	

Field	Name	Use	Description
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
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 by XMS. They appear only if the AP has been placed on a map in XMS. *
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	-X	Count of frames heard from device during this window ***
ot	Origin Time	-X	Timestamp of first frame in this window (Unix time in seconds) ***

Field	Name	Use	Description
ct	Current Time	-X	Timestamp of last frame in this window (Unix time in seconds) ***
cf	Current Frequency	-X	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	-X	Minimum interval between frames (within 24 hr period) ***
ih	Interval High	-X	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
s3	Sum of Cubes	E	Sum of cubes of values for signal strength
sl	Signal Low	-X	Minimum signal strength (within 24 hr period) ***
sh	Signal High	-X	Maximum signal strength (within 24 hr period) ***
so	Signal Origin	-X	Signal strength of first frame heard ***
sc	Signal Current		Signal strength of last frame heard
am		X	List of AP MAC addresses used in location calculation
ar		X	List of AP RSSIs used in location calculation
ab		X	List of AP bias values used in location calculation
at		X	List of AP time stamps used in location calculation

Field		Name	Use	Description
	pr	Probe Request	-X	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 XMS, 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 XMS 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":{"00:0f:7d:44:03:20":-69,"00:0f:7d:44:03:30":-68,"00:0f:7d:44:03:40":-70,
"00:0f:7d:44:03:60":-60}
```

*** If the word **xirrus** is found in the URL, the AP assumes that you are using location based services for stations, and reduces the size of messages by dropping unneeded fields from the output. Specifically, the following fields will be dropped from the output for each station:

> ap (dropped for stations, but included for rogue APs)
>
> as (dropped for rogue APs, but included for stations)
>
> cn   ct   sl
>
> ot   cf   sh
>
> sm   il   so
>
> ih   pr

In addition, with **xirrus** in the URL, only those stations whose RSSI (signal strength) is highest when compared to the station's RSSI at neighboring APs will be sent. This also helps to minimize the number and size of messages, and largely

eliminates duplicate data being sent. Note that if a station's RSSI is the same at two or more APs, then they will all send data, so there is a chance of seeing duplicates.

Contact Information

Xirrus, Inc. is located in Thousand Oaks, California, just 55 minutes northwest of downtown Los Angeles and 40 minutes southeast of Santa Barbara.

Xirrus, Inc.
2101 Corporate Center Drive
Thousand Oaks, CA 91320
USA

Tel: 1.805.262.1600
         1.800.947.7871 Toll Free in the US

Fax: 1.866.462.3980

www.xirrus.com
support.xirrus.com

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.

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 XMS server resides that provides access to the client interface.

Access Point

A Xirrus proprietary high capacity wireless access point utilizing Gigabit LAN speeds and multiple wireless channels, specifically designed for high performance.

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 XMS 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.

CDP

(Cisco Discovery Protocol) CDP is a layer 2 network protocol which runs on most Cisco equipment and some other network equipment. It is used to share information with other directly connected network devices. Information such as the model, network capabilities, and IP address is shared. Wireless Access Points can both advertise their presence by sending CDP announcements, and gather and display information sent by neighbors.

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 Xirrus is: http://www.xirrus.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.

- **xirrus** 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**.

IAP

(Integrated Access Point) A configurable wireless module (radio) dedicated to the Xirrus Wireless Access Point family of products.

icon

A graphical symbol used in the XMS client interface to represent objects, such as Access Points within a map, alarms and events. See also, **map symbol**.

Intrusion Detection System

A Xirrus proprietary application that scans and monitors the XMS 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 XMS. This includes all the Access Points discovered by XMS, 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 XMS 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 Access Points in the XMS client interface maps. The symbol for an Access Point is a pictorial image of the Xirrus Wireless Access Point. 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 Access Point.

MTTR

(Mean Time To Repair) Used in reports, this shows the average time (in minutes) to restore functionality to the Access Point 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 the optional Xirrus-supplied Power over Ethernet modules that provide DC power to Access Points. 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, Access Point or group of Access Points 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.

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 Access Point

A family of Xirrus proprietary high capacity wireless access points utilizing multiple channels.

Xirrus Release 8.2   1/12/18

Index

Cambium Networks™

Wireless That Just Works

cambiumnetworks.com

USA Headquarters
3800 Golf Road, Suite 360
Rolling Meadows, IL 60008 USA

+1 888 863 5250

India Office
Cambium Networks Consulting Private Ltd
5th Floor, Quadrant 1, Umiya Business Bay, Tower 2,
Outer Ring Road,
Kadubisenahalli, Varthur Hobli Road,
Bangalore East

+91 80 67333100

UK Office
Unit B2, Linhay Business Park
Eastern Road Ashburton, United Kingdom, TQ13 7UP

+44 1364 655500

USA Thousand Oaks Office
2545 Hillcrest Dr, Suite 220
Thousand Oaks, CA 91320

USA San Jose Office
2590 N. 1st Street, Suite 220
San Jose, CA 95131 USA