Ruckus Wireless™ FlexMaster™ User Guide

Release Version 9.6

Part Number 800-70428-001 Rev B
Published November 2013

www.ruckuswireless.com

Copyright Notice and Proprietary Information

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless Bark Logo, Ruckus, Ruckus Wireless, ZoneFlex, FlexMaster, MediaFlex, SpeedFlex, and ZoneDirector are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

Contents

About This Guide

2 Installing and Upgrading FlexMaster

3 Getting Started with FlexMaster

4 Working with Device Inventory

8 Working with Reports

9 Performing Administrative Tasks

About This Guide

This guide describes how to install, configure and manage the Ruckus Wireless FlexMaster version 9.6. This guide is written for those responsible for installing and managing network equipment. Consequently, it assumes that the reader has basic working knowledge of local area networking, wireless networking, and wireless devices.

NOTE: When release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Wireless Support Web site at

http://support.ruckuswireless.com

Document Conventions

The following two tables list the text and notice conventions that are used throughout this guide.

Table 1. Text Conventions

Convention	Description	Example
`monospace`	Represents information as it appears on screen	`[Device name]>`
`monospace bold`	Represents information that you enter	`[Device name]>` **`set ipaddr 10.0.0.12`**
default font bold	Keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Screen or page names	Click **Advanced Settings**. The *Advanced Settings* page appears.

Table 2. Notice Conventions

Icon	Notice Type	Description
i	Information	Information that describes important features or instructions
!	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
⚡	Warning	Information that alerts you to potential personal injury

Related Documentation

In addition to this User Guide, each FlexMaster documentation set includes the following:

- *Online Help*: Provides instructions for performing tasks using the Access Point's Web interface. The online help is accessible from the Web interface and is searchable.
- *Release Notes*: Provide information about the current software release, including new features, enhancements and known issues.

Documentation Feedback

Ruckus Wireless is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Ruckus Wireless at

https://support.ruckuswireless.com/documents

When contacting us, please include the following information:

- Document title
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- *Ruckus Wireless FlexMaster 9.6 User Guide*
- Part number: 800-70428-001 Rev B
- Page 77

1

Introducing Ruckus Wireless FlexMaster

In This Chapter:

Ruckus Wireless FlexMaster Overview

The Ruckus Wireless FlexMaster software is an intelligent, scalable network management system designed to facilitate administration of your dispersed Ruckus Wireless Access Points and ZoneDirector devices. FlexMaster offers:

- Discovery of Ruckus Wireless devices through the "call home" feature: Ruckus Wireless devices are preconfigured with the default FlexMaster's URL (`http://flexmaster/intune/server`) to enable them to call home to FlexMaster and register for management. In addition, you can also configure your DNS server or Option 43 on your DHCP server to ensure that your managed devices can find FlexMaster on the network.
- Immediate or scheduled active firmware upgrades: Enables Ruckus Wireless AP firmware to be downloaded to multiple devices over HTTP either on-demand or according to a schedule.
- Provisioning templates for bulk configuration: Allows you to push multiple configuration settings (for example, SSID, IP addressing, login changes) to several devices simultaneously.
- Multi-level Dashboard displaying device views and events: Processes notifications received from managed Ruckus Wireless devices and displays them in an easy-to-understand and easy-to-use graphical user interface accessible via a Web browser.

FlexMaster Management Software and Server

FlexMaster is packaged as software you install on a Linux-based RHEL 5 or 6 (Red Hat Enterprise Linux) server. FlexMaster installation includes Web server and MySQL database components for communicating with and tracking your dispersed Ruckus Wireless devices. For more on FlexMaster installation in a Red Hat Enterprise Linux environment, refer to Installing the FlexMaster Software.

FlexMaster Release 9.6.1 can also be installed in a VMware/64-bit CentOS 5 and 6/ESXi (VMware) environment. FlexMaster is generally only installed on VMware/CentOS/ESXi servers for new and/or lab installations. For more on FlexMaster installation in a VMware environment, refer to the FlexMaster VMware 9.6.1 Getting Started Guide, available from

https://support.ruckuswireless.com/documents.

NOTE: Operation of FlexMaster is independent of the platform it is installed on. The operating instructions in the rest of this document apply to FM installed in Red Hat Enterprise Linux environment and in a VMware/CentOS/ESXi environment.

FlexMaster Time

FlexMaster stores all event times in Coordinated Universal Time (UTC) (and appropriate offsets). Event times that appear on the FlexMaster Web interface are automatically adjusted to the client's local time settings.

NOTE: If the FM server time is changed (for example, when corrected from a wrong time zone), then FM should be restarted to apply this change.

NOTE: When the FlexMaster server time is not synchronized with the local time, scheduled tasks may not run when expected, and reports may contain incorrect results. To ensure that scheduled tasks run when scheduled, synchronize the time on the FlexMaster server with the local time. You can do this by installing an NTP client on the FlexMaster server.

Management Protocol

FlexMaster supports the Technical Report 069 (TR-069) CPE WAN Management Protocol (CWMP) as defined by the DSL Forum (*www.dslforum.org*).

Internet Accessibility

FlexMaster requires an Internet-accessible interface to:

- *Enable remote management:* If the computer that you are using to access the FlexMaster Web interface is not on the same local network as FlexMaster, then logging into the FlexMaster Web interface remotely requires the host Linux server to be remotely accessible via HTTP or HTTPS.
- *Enable the Map View feature.* Map View data is provided by Google Maps, thus FlexMaster must be able to connect to Google Maps via the Internet to display the maps. When FlexMaster is unable to access Google Maps, gray boxes appear on the FlexMaster Web interface, instead of the map that Google Maps provides.

  If your location or network is preventing FlexMaster from accessing Google Maps, you can disable Google Maps on the *System Settings* page to hide these gray boxes. For more on Map View, refer to Text View and Map View.

NOTE: Authentication with Google Maps servers is processed via the Ruckus Wireless Web site. To ensure successful authentication, FlexMaster must be able to access *www.ruckuswireless.com* and display Google Maps data on the FlexMaster Web interface.

FlexMaster may also require Internet connectivity to manage remote Ruckus Wireless devices. Remote devices must be able to register with FlexMaster when “calling home” across the Internet. In a closed environment where managed devices are local to FlexMaster, Internet connectivity is then only required for Map View.

Potential Conflict with Ruckus Wireless ZoneDirector

If a Ruckus Wireless ZoneDirector is detected on the network, then a FlexMaster-managed AP stops communicating with FlexMaster and registers instead with ZoneDirector. If the same AP is provisioned with a firmware or configuration upgrade from FlexMaster, then the task status appears as “Started” (pending) on the task status page as FlexMaster cannot contact the AP. If the AP registers with ZoneDirector, then FlexMaster displays the status of the AP being managed by “ZD” on the *Configure > Device Registration* page.

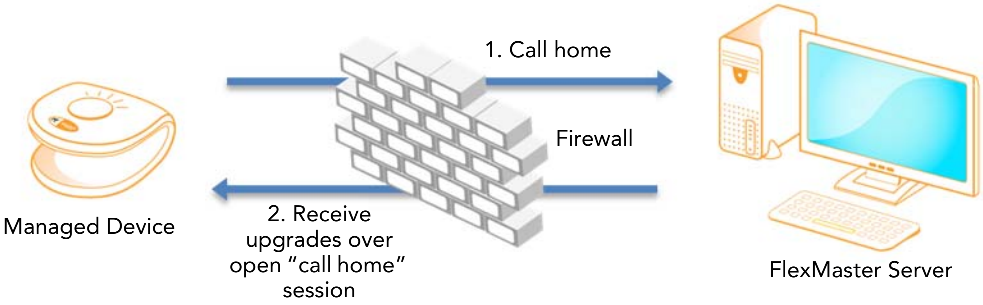
How FlexMaster Communicates with Managed Devices

FlexMaster can communicate with the devices that it manages using the Directly Accessible Method and the L2TP Tunneling Method.

Directly Accessible Method

Ruckus Wireless devices are configured to initiate the initial communication with FlexMaster by "calling home". When a supported device is shipped, the URL of your FlexMaster server is preconfigured on the device. This requires that the FlexMaster server is reachable on either HTTP port 80 or HTTPS port 443 (or the SSL port you configure). Once the device is powered on, the call home occurs.

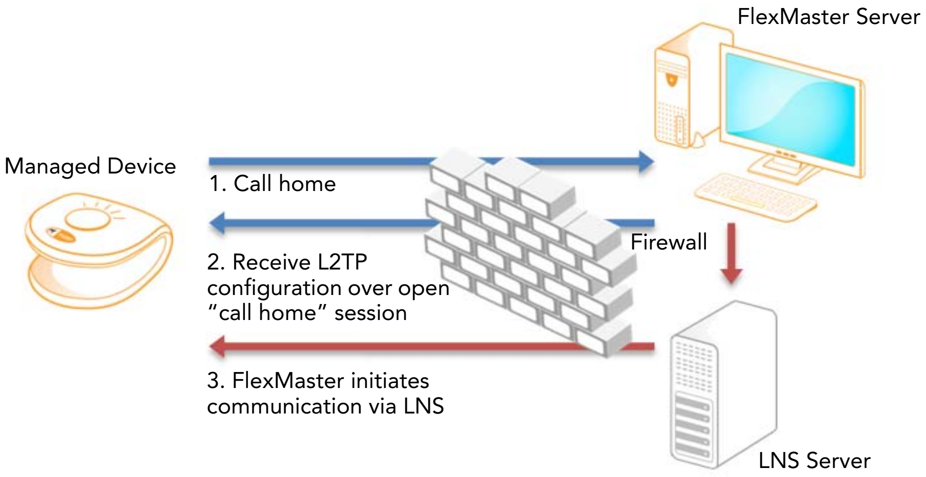
Figure 1. How a managed device calls home directly to FlexMaster



L2TP Tunneling Method

The FlexMaster connection initiation mechanism relies on the managed Ruckus Wireless AP having a routable IP address. When the Ruckus Wireless AP is behind a NAT or firewall, FlexMaster might not be able to reach the AP. In this case, FlexMaster must wait until the AP initiates a connection via the Internet. If you deploy an L2TP Network Server (LNS), then you can configure your FlexMaster to tunnel through the LNS to managed devices, thus enabling FlexMaster to initiate communication. This allows FlexMaster to check device connectivity and to push device updates proactively. For more on configuring L2TP compatibility, refer to Configuring Your Devices to Communicate with FlexMaster over L2TP.

Figure 2. How a managed device calls home to FlexMaster via an LNS server


FlexMaster Server
Managed Device
1. Call home
2. Receive L2TP configuration over open "call home" session
Firewall
3. FlexMaster initiates communication via LNS
LNS Server

Where Should You Place FlexMaster?

Since you want FlexMaster to be as available as possible to the remote devices being managed, you should place it in your network accordingly. Note the following:

- Make sure FlexMaster's IP address is reachable via HTTP/HTTPS from outside of your internal network. This allows managed devices to call home.
- Register your FlexMaster server with your DNS server. Refer to Option 1: Register FlexMaster with a DNS Server.

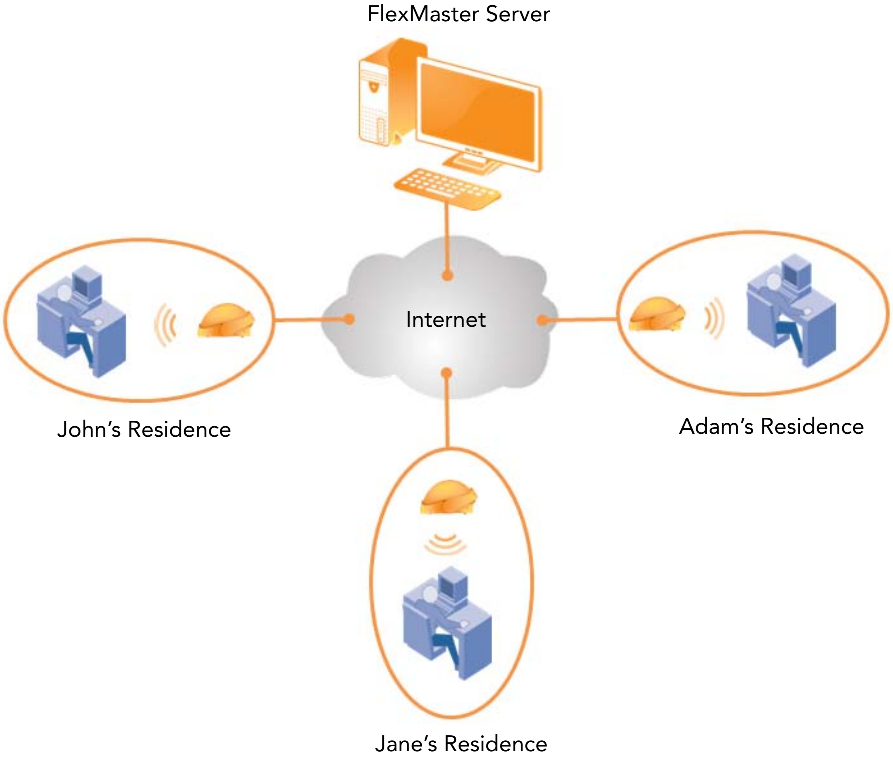
Deployment Scenarios

Since FlexMaster can manage many Ruckus Wireless devices, there are numerous scenarios that can benefit from aggregated management.

Service Provider Scenario

Service Providers can deploy FlexMaster in their Network Operations Centers (NOCs) to manage subscriber devices. The subscriber AP information can be pre-loaded to Flex-Master via inventory file, and then shipped to a subscriber, awaiting AP activation and a call home notification to FlexMaster for addition to the managed inventory. With the device information pre-loaded, you can preemptively set up a configuration to be pushed to the device when it registers after boot up.

Figure 3. Service provider scenario

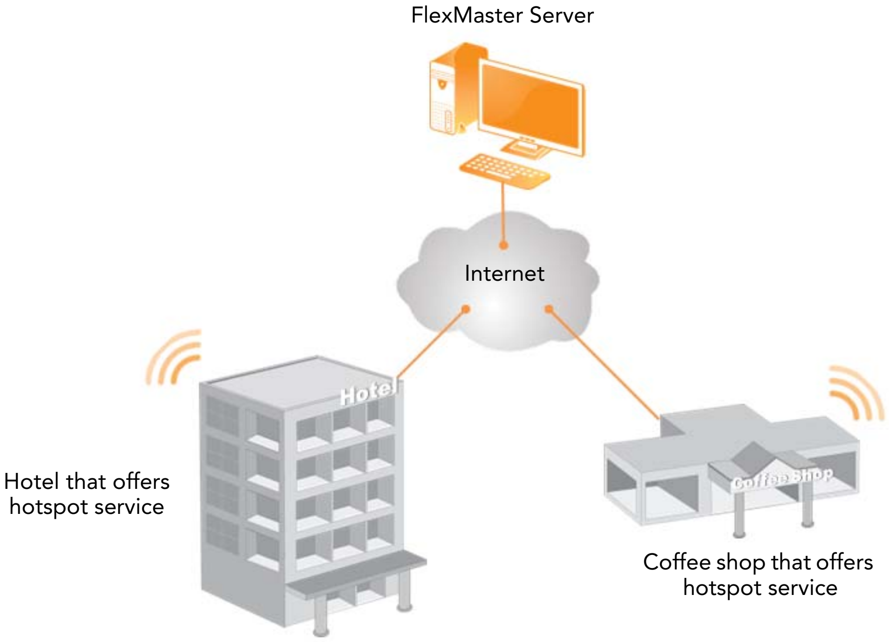


Hotspot Scenarios

Hotspots such as hotels and coffee shops offering wireless service can use FlexMaster to manage their APs. Aggregated configuration updates and firmware upgrades can be pushed out according to schedule to update one or more managed devices simultaneously. Loss of connectivity events can be monitored across the entire deployment.

Release 9.5 and later Ruckus Wireless devices also support Hotspot 2.0. APs configured for Hotspot 2.0 provide information to the client before association. This information can be used by the client to automatically select an appropriate network based on the services provided and the conditions under which the user can access them. In this way, rather than choosing from a list of SSIDs, Hotspot 2.0 clients can automatically select and authenticate to an SSID based on the client's configuration and services offered, or can allow the user to manually select an SSID for which the user has login credentials. The Ruckus Wireless Hotspot 2.0 implementation complies with the IEEE 802.11u standard and the Wi-Fi Alliance (WFA) Hotspot 2.0 Technical Specification.

Figure 4. Hotspot scenario


FlexMaster Server
Internet
Hotel
Hotel that offers hotspot service
Coffee Shop
Coffee shop that offers hotspot service

Key Terms in FlexMaster

Before using FlexMaster, Ruckus Wireless recommends that you become familiar with the key terms that are use in this Guide and on the FlexMaster Web interface. The following table lists terms that are key to full understanding and proper use of FlexMaster.

Table 1. Key terms in FlexMaster

Term	Description
Call Home	After boot up, compatible Ruckus Wireless devices attempt to register with FlexMaster. FlexMaster's URL is configured on the device.
Device View, Event View, and Audit View	*Device View:* Since FlexMaster manages many devices, you can consolidate devices with similar attributes into views. *Device views* are a powerful component within FlexMaster. Devices that are grouped into views can be: • Provisioned as one • Consolidated in reports • Quickly recalled to filter a list The grouping attributes are user customizable, and can include device type, geographic location, or any other quality that you want to use as grouping criterion. By default, FlexMaster includes two pre-configured device views: All Standalone APs and All ZoneDirectors. *All Standalone APs* is a snapshot of all APs currently managed by FlexMaster. *All ZoneDirectors* is a snapshot of all ZoneDirector devices that are currently managed by FlexMaster. Much like device views, *Event Views* can be created to quickly reference a list of events as filtered using the *Monitor > Events > New Search* tab options. You can also create an *Audit View,* which groups audit log results based on the options in *Administer > Audit Log > New Search.*
Device Registration	By default, compatible Ruckus Wireless devices attempt to register automatically with FlexMaster when they boot up. If you want to change this default approval settings, then go to the *Configure > Device Registration* page. The Device Registration option also enables you to pre-load a device inventory file before actual device registration. This enables you to stay ahead of your dispersal of Ruckus Wireless devices and keep track of each device’s details (for example, serial number and MAC address), as well as automatically permit or deny registration with FlexMaster. For more on device registration, refer to Managing Device Registration.

Table 1. Key terms in FlexMaster (Continued)

Term	**Description**
Periodic Inform Interval	This is the frequency at which managed Ruckus Wireless devices must synchronize with FlexMaster. When Ruckus Wireless devices call home periodically, FlexMaster can verify proper operation of managed devices. If a managed device does not call home at this interval, then an alert is issued by the system notifying you that the device is out of contact and therefore cannot be updated or checked for the latest operational information. To set this interval, refer to Performing an AP Configuration Upgrade.
Provisioning	Provisioning is the act of providing a specified action or configuration to a managed group, either based on a schedule or on-demand. Provisioning tasks include configuration, firmware upgrade, and reboot for both ZoneDirector devices and APs. ZoneDirector-specific tasks include configuration backup (cloning) and ZoneDirector event configuration, while AP-specific tasks include factory reset. For more on provisioning, refer to Provisioning Tasks to Managed Devices.
Device View	A dynamic group of devices filtered based on a specific criterion (for example, model number or partial serial number). Device Views should not be confused with *Device Groups,* which refers to a physical grouping of devices typically used for assigning devices for management by users.
Tag	A tag is any text that you assign to devices as another method for grouping them. For example, you can assign the tag "Lobby" to Ruckus Wireless devices that are deployed in your office lobby to identify their physical location easily. You can set a tag by editing the device details on the *Inventory* page.
Default Mail to	This phrase refers to the email address which is sent messages from the system based on various events. You enter this email address either during the FlexMaster installation procedure or in the **To** field on the *Administer > System Settings > SMTP Settings* page. You must specify an SMTP server to send email notifications to this user. Refer to SMTP Settings.

2

Installing and Upgrading FlexMaster

You normally install FlexMaster on a Linux-based RHEL 5 or 6 (Red Hat Enterprise Linux) server. FlexMaster installation includes Web server and MySQL database components for communicating with and tracking your dispersed Ruckus Wireless devices. Continue with this chapter to install FlexMaster in a Red Hat Enterprise Linux environment.

WARNING! The tasks described in this chapter should be undertaken only by an experienced network administrator or under the guidance of your service provider or technical support professional.

FlexMaster Release 9.6.1 can also be installed in a VMware/64-bit CentOS 5 and 6/ESXi (VMware) environment. FlexMaster is generally only installed on VMware servers for new and/or lab installations. For more on FlexMaster installation in a VMware environment, refer to the FlexMaster VMware 9.6.1 Getting Started Guide, available from

https://support.ruckuswireless.com/documents.

NOTE: Operation of FlexMaster is independent of the platform it is installed on. The operating instructions in the rest of this document apply to FM installed in Red Hat Enterprise Linux environment and in a VMware/CentOS/ESXi environment.

In This Chapter:

Firewall Ports that Must be Open for Communications

Depending on how your network is designed, you may need to edit the iptables file and open communication ports on any firewalls located between FlexMaster and managed ZoneDirector devices and access points. Refer to the following URLs which include information about how to edit the iptables file.

- *http://en.wikipedia.org/wiki/Iptables*
- *http://www.thegeekstuff.com/2010/07/list-and-flush-iptables-rules*
- *https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/sect-Security_Guide-IPTables.html*

The following table lists the ports that need to be open for different types of communications.

Table 2. Firewall ports that must be open for FlexMaster communications

Communication	Ports
MySQL	
FlexMaster > MySQL communications	TCP destination port 3306
ZoneDirector	
ZoneDirector > FlexMaster registration and periodic inform	TCP destination port 443 (HTTPS)
FlexMaster > ZoneDirector ZD web interface, ZD device view	TCP destination port 443 (HTTPS)
ZoneDirector > FlexMaster SNMP traps	TCP destination port 161 (SNMP)
FlexMaster > TACACS+ server *(NOTE 1)*	TCP destination port 49 (TACACS+)
TACACS+ server > FlexMaster *(NOTE 1)*	TCP destination port 49 (TACACS+)
FlexMaster > ZoneDirector wakeup, ZD device view, real-time template configuration, and real-time firmware upgrade *(NOTE 2)*	TCP destination port 8082 (ZD wakeup)
ZoneDirector > FlexMaster firmware upgrade	TCP destination port 80 (HTTP)
ZoneDirector > FlexMaster template configuration upgrade	TCP destination port 80 and 443 (HTTP and HTTPS)
ZoneDirector > FlexMaster ZD template configuration	TCP destination port 60001 through 60010 (HTTP and HTTPS)

Table 2. Firewall ports that must be open for FlexMaster communications(Continued)

Communication	Ports
Standalone AP	
Standalone AP > FlexMaster registration and periodic inform	TCP destination port 443 and/or 80 (HTTPS and/or HTTP, respectively; depends on the AP's FlexMaster URL configuration)
Standalone AP > FlexMaster SNMP traps	TCP destination port 161 (SNMP)
Standalone AP > TACACS+ server *(NOTE 1)*	TCP destination port 49 (TACACS+)
TACACS+ server > Standalone AP *(NOTE 1)*	TCP destination port 49 (TACACS+)
FlexMaster > Standalone AP Real-time template configuration upgrade, AP wakeup, AP device view, and real-time firmware upgrade *(NOTE 2)*	TCP destination port 8082 (AP wakeup)
Standalone AP > FlexMaster template configuration upgrade, AP template configuration upgrade using Auto-Provisioning	TCP destination port 80 and/or 443 (HTTP and/or HTTPS, respectively; depends on the AP's FlexMaster URL configuration)
Standalone AP > FlexMaster firmware upgrade	TCP destination port 80 (HTTP)

NOTE 1: The TACACS+ server can use a different TCP port. Refer to Configuring Your Devices to Work with TACACS+.

NOTE 2: The Ruckus Wireless device web and wakeup interfaces can be individually mapped through firewall/ NAT devices.

Administering a Linux Server

Flexmaster systems can be installed in an RHEL 5 and 6 (Red Hat Enterprise Linux) environment. Continue with this section to install FlexMaster in a Red Hat Enterprise Linux environment.

NOTE: FlexMaster Release 9.6.1 can also be installed in a VMware/64-bit CentOS 5 and 6/ESXi (VMware) environment. FlexMaster is generally only installed on VMware servers for new and/or lab installations. (Existing customers may not want to switch from FlexMaster installed on an RHEL server to a VMware server, as the data will have to be extensively modified for migration.)

For more on FlexMaster installation in a VMware environment, refer to the FlexMaster VMware 9.6.1 Getting Started Guide, available from https://support.ruckuswireless.com/documents.

Continue with the following to install FlexMaster on a Linux server:

- Preparing Your Server for FlexMaster Installation
- Ensuring That APs Can Connect to FlexMaster
- Editing the Server Hosts File
- Installing the FlexMaster Software
- Notable Files in the FlexMaster Root Directory
- Upgrading the FlexMaster Software
- Backing Up the Database from the Command Line Interface
- Restoring the Database from the Command Line Interface
- What's Next?

Preparing Your Server for FlexMaster Installation

Before installing FlexMaster, make sure your environment, including the target Linux server, meets all the requirements. This section details preparation of the host server for FlexMaster installation and operation.

What You Will Be Doing

- Preparing a clean Linux server according to the minimum system requirements.
- Placing the server on a subnet that is reachable by the Ruckus Wireless devices to be managed. This may include registering the server with your DNS server.
- Customizing your DHCP server.

Server System Requirements

When deciding on the Linux server on which to install FlexMaster, you need to consider the number of devices that your FlexMaster installation is to manage. The target server must meet the following minimum requirements:

- CPU and RAM: Depends on the number of managed ZoneDirector devices and standalone APs. Refer to Minimum Recommended RAM and CPU below for more information.
- OS:
  - Required Virtual System: VMware EXSi 5.0.0 and vSphere Client 5.0 and (Optional) Virtual System: VMware Player 4.0.4 and Workstation 8.0.5
    --OR--
  - Red Hat Enterprise Linux Edition 5.0 (64-bit)
- HDD: 30GB dedicated to FlexMaster, minimum for 10 licenses
- RAM: 8GB dedicated to FlexMaster, minimum
- CD-ROM device if you choose to use this method of installation
- Mouse
- Network adapter

WARNING! To ensure that normal FlexMaster operations run smoothly, make sure that the target Linux server has at least 160GB of free disk space dedicated to FlexMaster.

The FlexMaster disk space requirement is doubled when FlexMaster is being updated.

Database backups also consume extra disk space. The required extra disk space is determined by the number of database backups.

If FlexMaster does not have sufficient disk space, then the MySQL server for FlexMaster may encounter errors.

NOTE: When you are backing up the FlexMaster database, make sure that the Linux server has at least 10GB of available disk space. This helps ensure a successful database backup.

Minimum Recommended RAM and CPU

The amount of memory and CPU power required on the FlexMaster server depends on the number of ZoneDirector devices and standalone APs that FlexMaster is to manage. Refer to the following table for the minimum recommended RAM and CPU for managing ZoneDirector devices.

Table 3. Minimum recommended RAM and CPU for the FM 3-tier model

Managed Population	Minimum RAM	Minimum CPU
Up to 10 ZoneDirector-managed APs (for up to 10 licenses)	8GB	2.0GHz Quad Core Intel® Xeon® E5606 or equivalent
Up to 1,000 ZoneDirector-managed APs	8GB	2.0GHz Quad Core Intel® Xeon® E5606 or equivalent

Table 3. Minimum recommended RAM and CPU for the FM 3-tier model(Continued)

Managed Population	Minimum RAM	Minimum CPU
Up to 5,000 ZoneDirector-managed APs	16GB	2.5GHz Six Core Intel® Xeon® E5670 or equivalent
Up to 10,000 ZoneDirector-managed APs	32GB	2* 2.5GHz Six Core Intel® Xeon® E5670 or equivalent

When FlexMaster only manages standalone APs, the minimum recommended RAM and CPU are listed in the following table.

Table 4. Minimum recommended RAM and CPU for the FM 2-tier model

Managed Population	Minimum RAM	Minimum CPU
Less than 10 standalone APs (for up to 10 licenses)	8GB	2.5GHz Quad Core Intel® Xeon® E5606 or equivalent
Less than 1,000 standalone APs	8GB	2.5GHz Six Core Intel® Xeon® E5670 or equivalent
1,000-2,000 standalone APs	32GB	2* 2.5GHz Six Core Intel® Xeon® E5670 or equivalent

Web Browser Requirements

To access the FlexMaster Web interface, you need to use one of the following Web browsers. Ruckus Wireless recommends using the latest Firefox, Chrome or Safari browser. Although Internet Explorer 8 and IE 9 are supported, they are not recommended because of a user interface compatibility issue.

The FlexMaster Web interface is optimized for 1280 x 1024 (and higher) screen resolution.

Ensuring That APs Can Connect to FlexMaster

To enable FlexMaster to manage an AP, the AP must be able to communicate with FlexMaster when the AP performs its periodic call home procedure. To ensure successful communication between FlexMaster and the AP, the FlexMaster IP address must be reachable via HTTP or HTTPS from outside your internal network.

There are two ways you can ensure successful communication between FlexMaster and each managed AP, even when the AP is outside the internal network:

- Option 1: Register FlexMaster with a DNS Server
- Option 2: Customize Your DHCP Server
- Option 3: Set the FlexMaster Server URL Manually from the Device View

Option 1: Register FlexMaster with a DNS Server

FlexMaster's built-in Web server must be reachable by your Ruckus Wireless devices across the Internet. Hence, you may register your FlexMaster's host server with your DNS server in order for Ruckus Wireless devices calling home to register.

Option 2: Customize Your DHCP Server

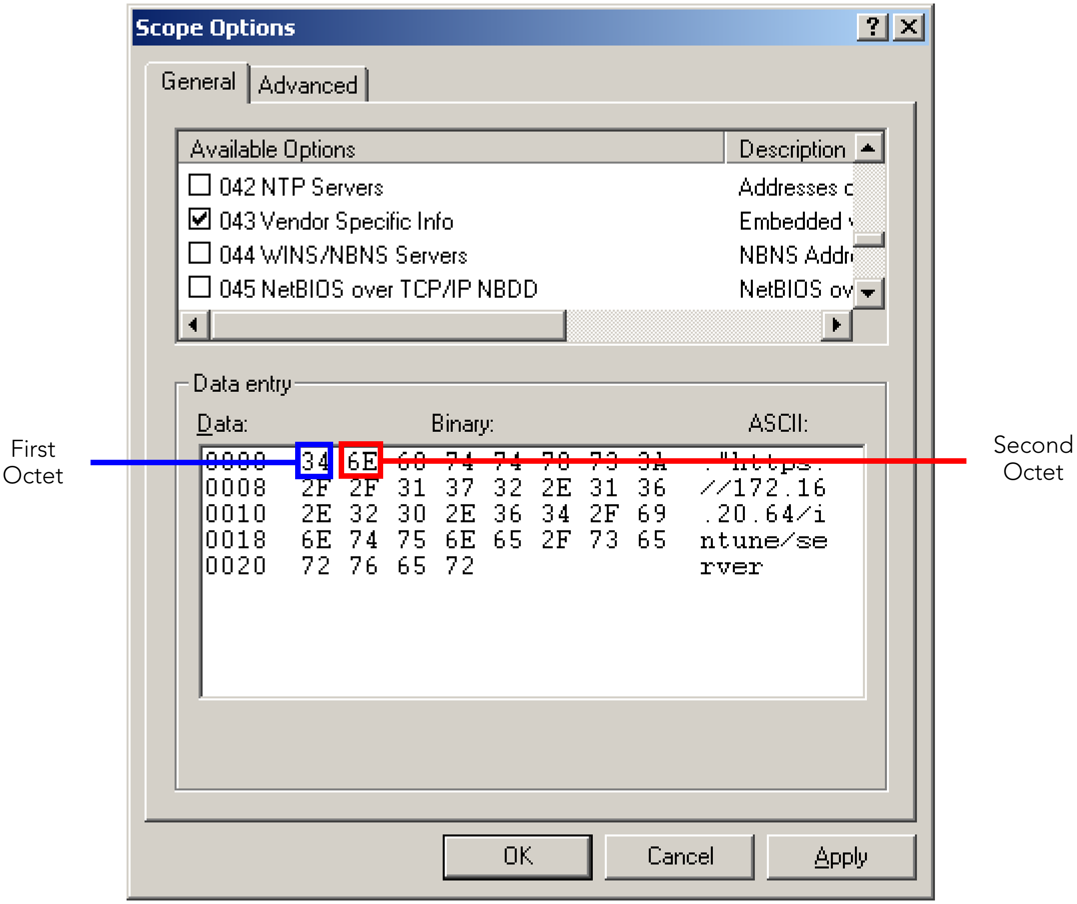
If you choose this method, then your organization's DHCP server must be configured to provide the URL of the FlexMaster server to DHCP clients. The vendor ID code on your DHCP server must be set to DHCP option 43 (043 Vendor Specific Info) discovery to enable Ruckus Wireless devices to discover and associate with FlexMaster.

NOTE: DHCP option 43 enables your DHCP server to provide the URL of the FlexMaster server to DHCP clients.

NOTE: The following procedure describes how to customize a DHCP server running on Microsoft Windows. If your DHCP server is running on a different operating system, then the procedure may be different. Refer to your DHCP server's documentation for the relevant information.

1. From the Windows Administrative Tools, open *DHCP*, and then select the DHCP server you want to configure.
2. If the *Scope* folder is collapsed, then click the plus (+) sign to expand it.
3. Right-click *Scope Options*, and then click **Configure Options**. The *General* tab of the *Scope Options* page appears.
4. Under *Available Options*, look for the **043 Vendor Specific Info** check box, and then select it.
5. Under *Data Entry*, position the cursor in the ASCII text area, and then type the URL of your FlexMaster server. The hexadecimal equivalent of the FlexMaster server URL appears in the Binary area.
6. In the *Binary* area, select the first octet, and then type `01`.

Figure 5. Selecting the first and second octets



☐ 042 NTP Servers — Addresses c
☑ 043 Vendor Specific Info — Embedded v
☐ 044 WINS/NBNS Servers — NBNS Addr
☐ 045 NetBIOS over TCP/IP NBDD — NetBIOS ov

Data: Binary: ASCII:

```
0000  34 6E 68 74 74 70 73 3A  ."https:
0008  2F 2F 31 37 32 2E 31 36  //172.16
0010  2E 32 30 2E 36 34 2F 69  .20.64/i
0018  6E 74 75 6E 65 2F 73 65  ntune/se
0020  72 76 65 72              rver
```

7. Count the total number of characters in the FlexMaster URL, including *http* or *https*, back slashes, colon, and periods. For example, if your FlexMaster URL is
   `http://flexmaster/intune/server`
   then the total number of characters in the URL is 31 (decimal value).

8. Convert the number of characters from decimal to hexadecimal. You can use an online conversion Web site, such as
   `http://www.easycalculation.com/decimal-converter.php`
   to perform the conversion.

9. Take note of the hexadecimal equivalent of the number of characters in the FlexMaster server URL. Following the example above, 24 in decimal is equivalent to 18 in hexadecimal.

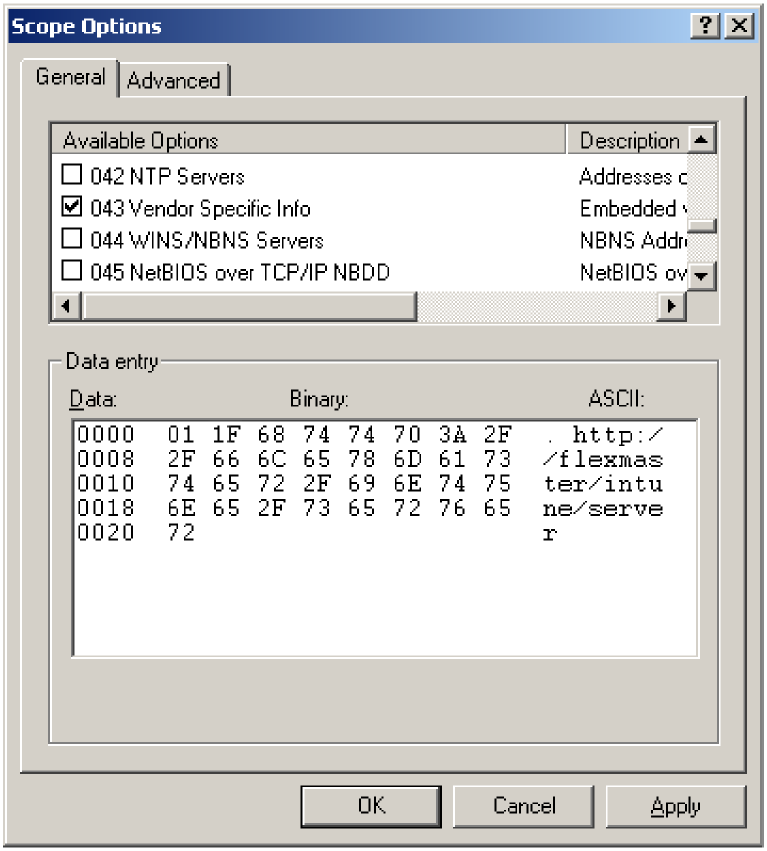
10. In the *Binary area*, select the second octet, and then type the hexadecimal equivalent of the number of characters in the FlexMaster server URL.

11. Click **Apply**, and then click **OK**.

You have completed customizing your DHCP server. The following figures show the differences in the Binary values between HTTP with a host name, HTTPS with a host name, HTTP with an IP address, and HTTPS with an IP address.

NOTE: The HEX data that you enter can be different from what is shown in the following examples if you are using a different URL.

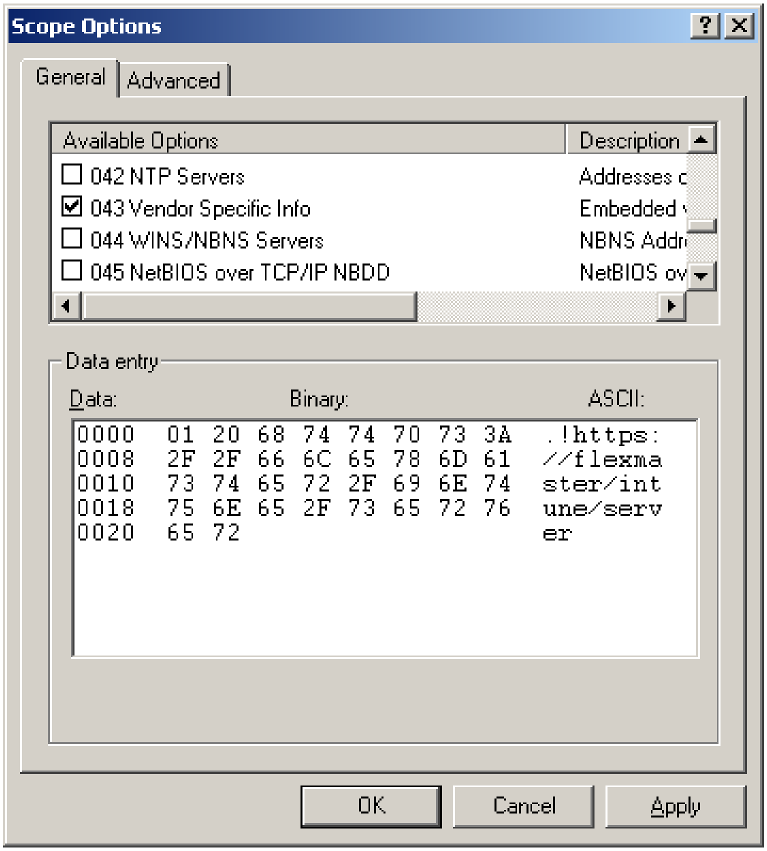
Figure 6. HTTP with a host name



Available Options	Description
□ 042 NTP Servers	Addresses c
☑ 043 Vendor Specific Info	Embedded v
□ 044 WINS/NBNS Servers	NBNS Addr
□ 045 NetBIOS over TCP/IP NBDD	NetBIOS ov

```
Data:       Binary:                      ASCII:
0000   01 1F 68 74 74 70 3A 2F   . http:/
0008   2F 66 6C 65 78 6D 61 73   /flexmas
0010   74 65 72 2F 69 6E 74 75   ter/intu
0018   6E 65 2F 73 65 72 76 65   ne/serve
0020   72                        r
```

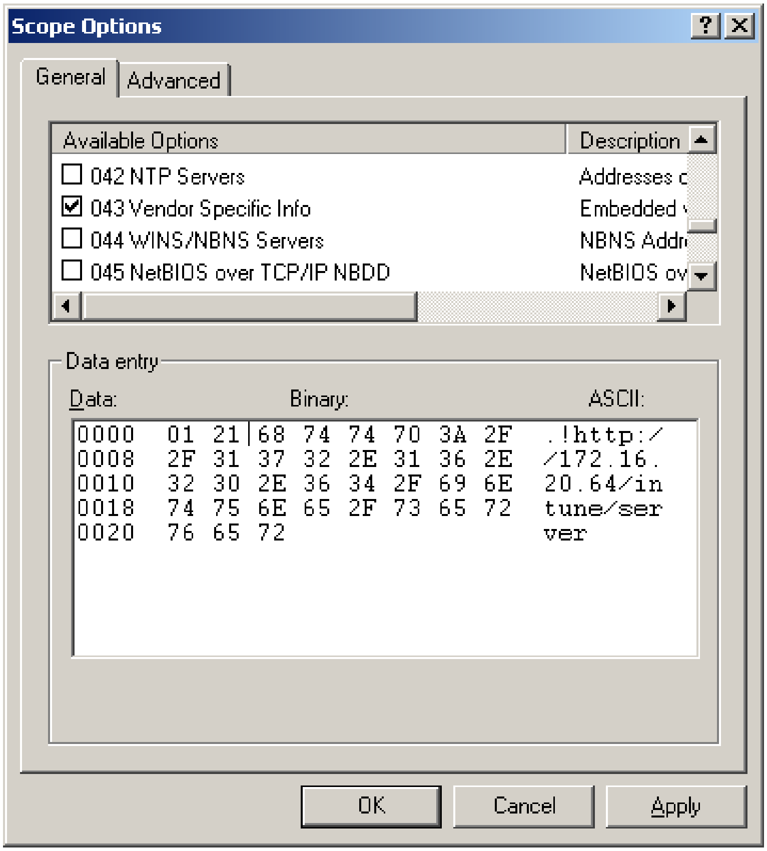
Figure 7.   HTTPS with a host name



Available Options	Description
□ 042 NTP Servers	Addresses c
☑ 043 Vendor Specific Info	Embedded v
□ 044 WINS/NBNS Servers	NBNS Addr
□ 045 NetBIOS over TCP/IP NBDD	NetBIOS ov

```
0000   01 20 68 74 74 70 73 3A   .!https:
0008   2F 2F 66 6C 65 78 6D 61   //flexma
0010   73 74 65 72 2F 69 6E 74   ster/int
0018   75 6E 65 2F 73 65 72 76   une/serv
0020   65 72                     er
```

Figure 8. HTTP with an IP address



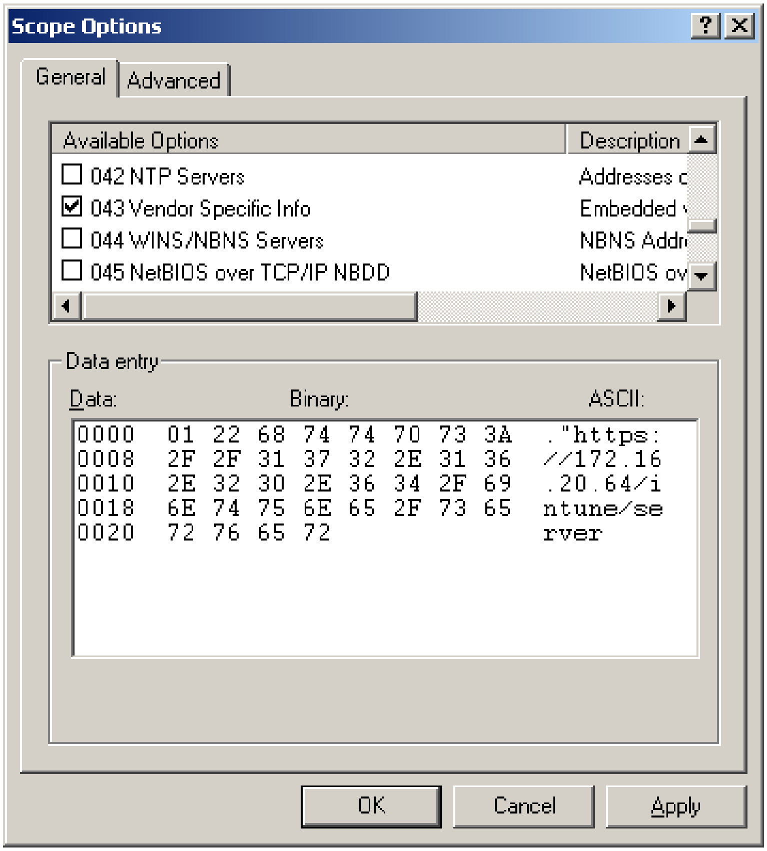
Available Options	Description
□ 042 NTP Servers	Addresses c
☑ 043 Vendor Specific Info	Embedded v
□ 044 WINS/NBNS Servers	NBNS Addr
□ 045 NetBIOS over TCP/IP NBDD	NetBIOS ov

Data entry

Data: Binary: ASCII:

```
0000   01 21 68 74 74 70 3A 2F   .!http:/
0008   2F 31 37 32 2E 31 36 2E   /172.16.
0010   32 30 2E 36 34 2F 69 6E   20.64/in
0018   74 75 6E 65 2F 73 65 72   tune/ser
0020   76 65 72                  ver
```

Figure 9. *HTTPS with an IP address*



☐ 042 NTP Servers — Addresses c
☑ 043 Vendor Specific Info — Embedded v
☐ 044 WINS/NBNS Servers — NBNS Addr
☐ 045 NetBIOS over TCP/IP NBDD — NetBIOS ov

Data: Binary: ASCII:

```
0000   01 22 68 74 74 70 73 3A   ."https:
0008   2F 2F 31 37 32 2E 31 36   //172.16
0010   2E 32 30 2E 36 34 2F 69   .20.64/i
0018   6E 74 75 6E 65 2F 73 65   ntune/se
0020   72 76 65 72               rver
```

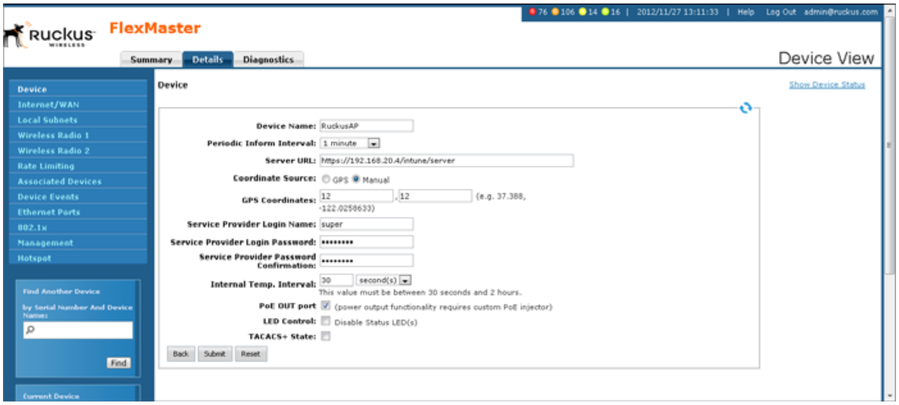
Option 3: Set the FlexMaster Server URL Manually from the Device View

You can also manually point the device to the FlexMaster server by setting the FlexMaster server URL from the Device View.

1. If not already done, then log in to the FlexMaster interface.
2. Go to the *Inventory* > *Standalone APs* > *Search* page.
3. Click the serial number of the AP that you want to configure. The *Device View* appears.
4. Click the **Details** tab.
5. Click **Edit Settings**.
6. In *Server URL*, type the URL of the FlexMaster server.
7. Click **Submit**.

You have completed setting the FlexMaster server URL manually from the Device View.

Figure 10. Setting the FlexMaster server URL from the Device View



Device

Device Name: RuckusAP

Periodic Inform Interval: 1 minute

Server URL: https://192.168.20.4/intune/server

Coordinate Source: ○ GPS ● Manual

GPS Coordinates: 12 , 12 (e.g. 37.388, -122.0258633)

Service Provider Login Name: super

Service Provider Login Password: ••••••••

Service Provider Password Confirmation: ••••••••

Internal Temp. Interval: 30 second(s)
This value must be between 30 seconds and 2 hours.

PoE OUT port ☑ (power output functionality requires custom PoE injector)

LED Control: □ Disable Status LED(s)

TACACS+ State: □

Editing the Server Hosts File

FlexMaster stores some of its configuration settings on a MySQL server database that is installed with the FlexMaster software. To ensure that FlexMaster can connect to this MySQL database after installation, you need to edit your Linux server's hosts file to include its DNS-related information.

1. Go to the `/etc` directory, and then open the `hosts` file.
2. Add the following line to the hosts file:

   ```
   127.0.0.1 fully.qualified.domain.name localhost
   ```

3. Save the hosts file.

NOTE: If you are planning to enable SMTP notification on FlexMaster, then you need to add another line in the hosts file for your SMTP server's DNS information. For more details, refer to SMTP Settings.

Installing the FlexMaster Software

You install FlexMaster software via CD-ROM to a Linux workstation that meets the system requirements listed in Server System Requirements.

WARNING! The install script, `install.sh`, must be launched from a terminal window and not from the file browser.

WARNING! If your Linux server contains an instance of MySQL before FlexMaster installation, then that MySQL instance and all dependent packages must be uninstalled before initializing FlexMaster installation.

WARNING! The FlexMaster installation script automatically selects the MySQL version to install, based on the type of CPU detected on the target server.

1. Log in to the host server as the root user.
2. Insert the FlexMaster CD into the CD-ROM drive.
3. If the FlexMaster server does not automatically mount the FlexMaster CD-ROM, then continue with Step 4. If the server automatically mounts the CD-ROM, then continue with Step 6.
4. Type the following command to create a mount point (or directory where you want to mount the CD-ROM):

   ```
   # mkdir -p /mnt/cdrom
   ```

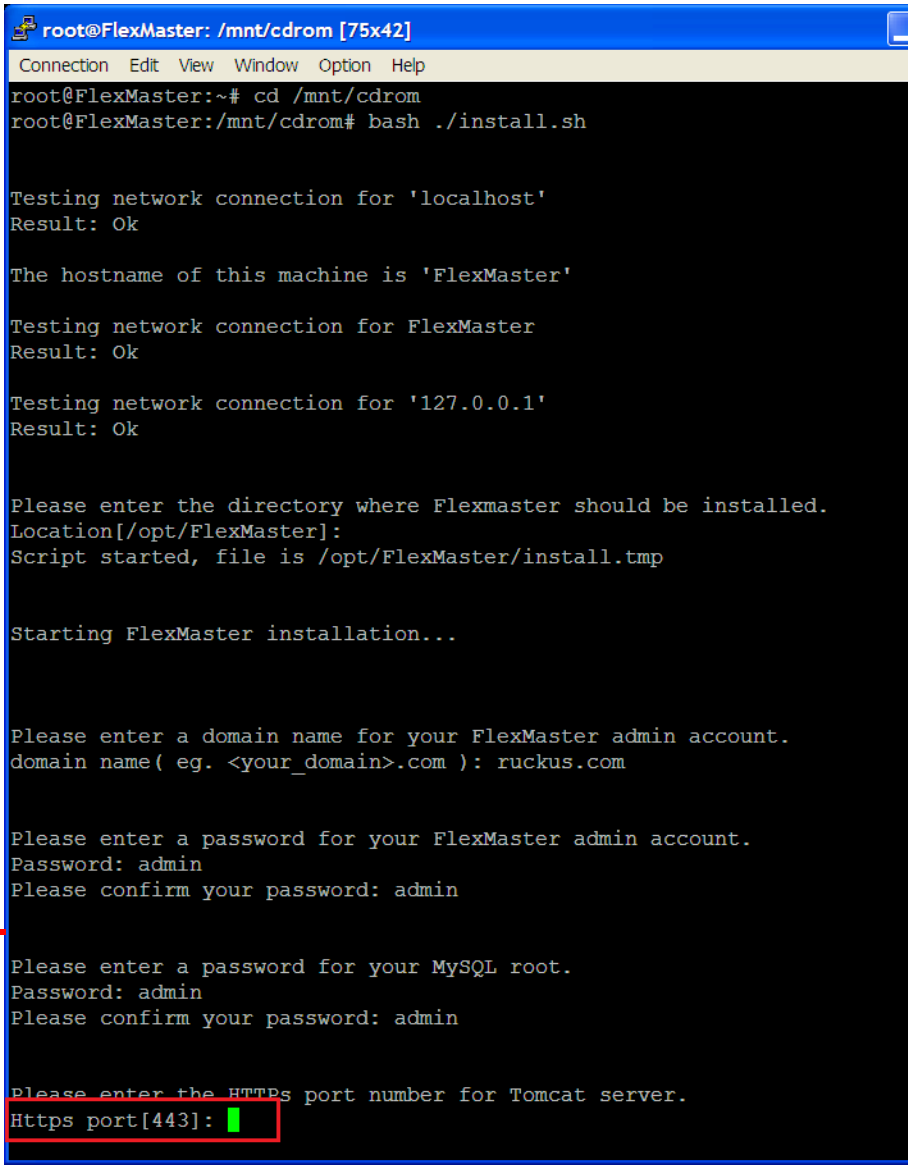
5. Type the following command to mount the CD-ROM manually to the created mount point:

   ```
   # mount /dev/cdrom /mnt/cdrom
   ```

6. Change directory (`cd`) to the mount point for the CD-ROM.
7. Execute the install script `install.sh.`

   ```
   # ./install.sh
   ```

Figure 11. FlexMaster partial installation including program location, domain identification, and admin password configuration



root@FlexMaster: /mnt/cdrom [75x42]
Connection Edit View Window Option Help

```
root@FlexMaster:~# cd /mnt/cdrom
root@FlexMaster:/mnt/cdrom# bash ./install.sh


Testing network connection for 'localhost'
Result: Ok

The hostname of this machine is 'FlexMaster'

Testing network connection for FlexMaster
Result: Ok

Testing network connection for '127.0.0.1'
Result: Ok


Please enter the directory where Flexmaster should be installed.
Location[/opt/FlexMaster]:
Script started, file is /opt/FlexMaster/install.tmp


Starting FlexMaster installation...



Please enter a domain name for your FlexMaster admin account.
domain name( eg. <your_domain>.com ): ruckus.com


Please enter a password for your FlexMaster admin account.
Password: admin
Please confirm your password: admin


Please enter a password for your MySQL root.
Password: admin
Please confirm your password: admin


Please enter the HTTPs port number for Tomcat server.
Https port[443]:
```

Tomcat Web server HTTPS port

8. You are prompted to verify the system date and time:

```
Your system time and timezone is:Thu, 16 Aug 2012 17:45:08 +0800.
yes? (Put yes to continue or program will be terminated!):yes
choose yes
```

9. The installation script performs some connection tests:

   ```
   Testing network connection for 'localhost'
   Result: Ok
   
   The hostname of this machine is 'localhost.localdomain'
   
   Testing network connection for localhost.localdomain
   Result: Ok
   
   Testing network connection for '127.0.0.1'
   Result: Ok
   ```

10. Enter the location where you want to install the FlexMaster software. A default location is provided. Press **<Enter>** to accept the default location.

    ```
    Location[/opt/FlexMaster]:
    ```

11. Enter your organization’s domain name. By default, the domain name is appended to the word “admin”, creating the default FlexMaster user account: *admin@domain*.com. The *admin@domain.com* user account is a Super User in the FlexMaster system and cannot be deleted. For more on roles, refer to Understanding User Roles and Privileges.

    ```
    domain name (e.g., <your_domain>.com): domain.com
    ```

12. Enter a password for the FlexMaster `admin@domain.com` user account.

    ```
    Password: password
    Please confirm your password: password
    ```

13. Enter a password for the MySQL root account.

    ```
    Password: password
    Please confirm your password: password
    ```

14. Enter the HTTPS port number for the Tomcat Web server. The default port is 443; press **<Enter>** to accept the default.

    ```
    Https port[443]:
    ```

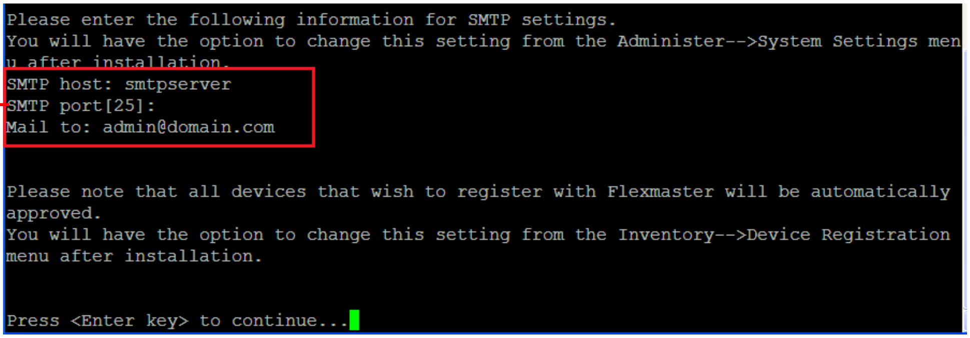
15. Enter your SMTP server host name and port number, as well as a default email address to which alerts for FlexMaster system events are sent.

    The SMTP server is the email server that FlexMaster uses to send alert notifications or system logs. You can change these settings on the *Administer > System Settings* page after installation.

    The default SMTP port is 25. Press **<Enter>** if your SMTP server is already using port 25.

    ```
    SMTP host: hostname
    
    SMTP port[25]:
    
    Mail to: username@domain.com
    ```

Figure 12. *Configuring the SMTP settings*

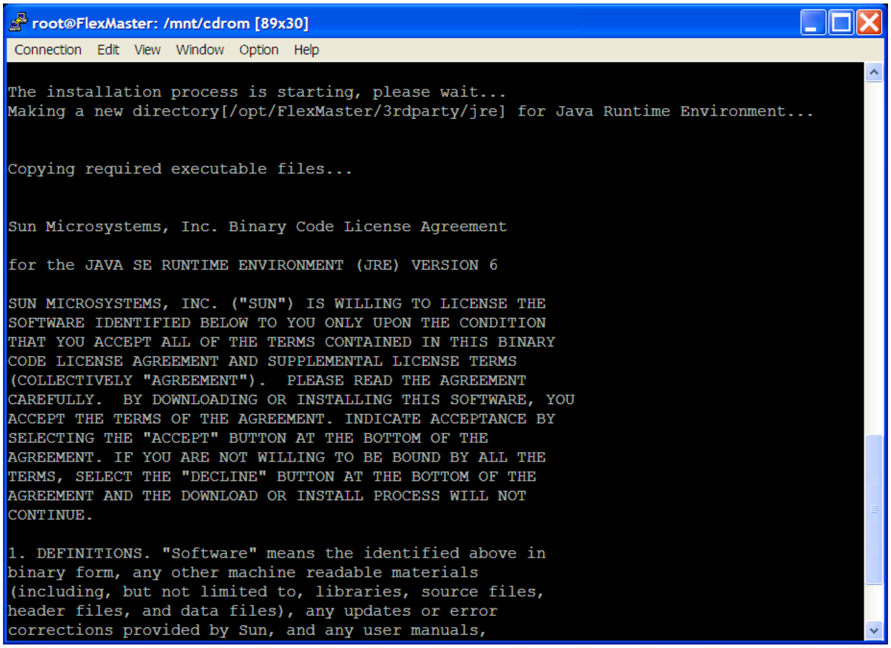


SMTP server settings

```
Please enter the following information for SMTP settings.
You will have the option to change this setting from the Administer-->System Settings men
u after installation.
SMTP host: smtpserver
SMTP port[25]:
Mail to: admin@domain.com


Please note that all devices that wish to register with Flexmaster will be automatically
approved.
You will have the option to change this setting from the Inventory-->Device Registration
menu after installation.


Press <Enter key> to continue...
```

16. Press **<Enter>** to start the installation process. Once installation begins, you are presented with a license agreement from Sun Microsystems.

Figure 13. *Sun Microsystems license agreement within the installation script*

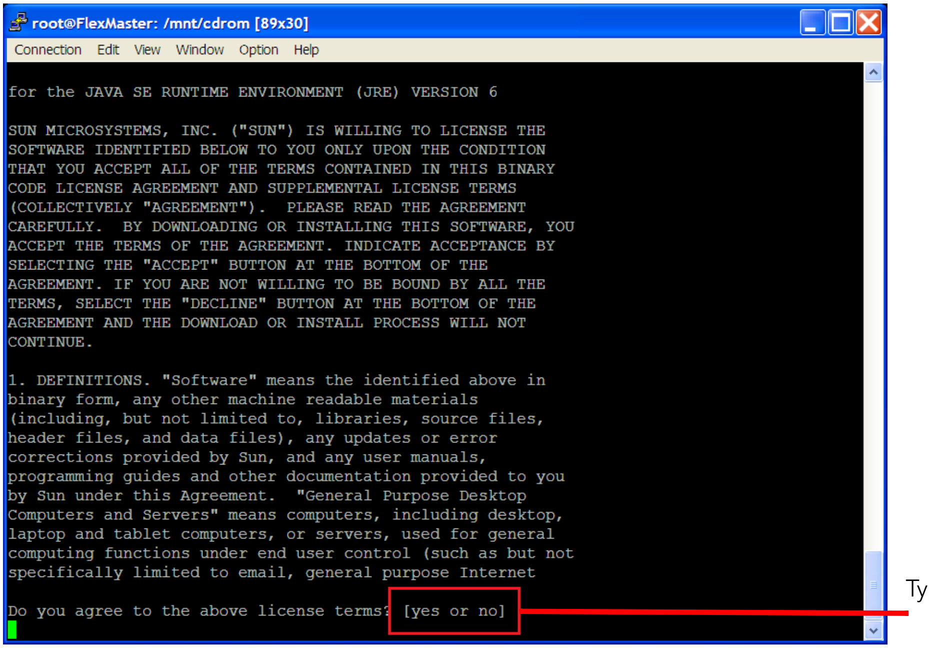


```
The installation process is starting, please wait...
Making a new directory[/opt/FlexMaster/3rdparty/jre] for Java Runtime Environment...


Copying required executable files...


Sun Microsystems, Inc. Binary Code License Agreement

for the JAVA SE RUNTIME ENVIRONMENT (JRE) VERSION 6

SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE
SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON THE CONDITION
THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY
CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS
(COLLECTIVELY "AGREEMENT").  PLEASE READ THE AGREEMENT
CAREFULLY.  BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU
ACCEPT THE TERMS OF THE AGREEMENT. INDICATE ACCEPTANCE BY
SELECTING THE "ACCEPT" BUTTON AT THE BOTTOM OF THE
AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE
TERMS, SELECT THE "DECLINE" BUTTON AT THE BOTTOM OF THE
AGREEMENT AND THE DOWNLOAD OR INSTALL PROCESS WILL NOT
CONTINUE.

1. DEFINITIONS. "Software" means the identified above in
binary form, any other machine readable materials
(including, but not limited to, libraries, source files,
header files, and data files), any updates or error
corrections provided by Sun, and any user manuals,
```

17. Read the license agreement, and accept by typing "yes" at the prompt, and then press **<Enter>.**

```
Do you agree to the above license terms? [yes or no] yes
```

Figure 14. Accepting the Sun license agreement



root@FlexMaster: /mnt/cdrom [89x30]
Connection Edit View Window Option Help

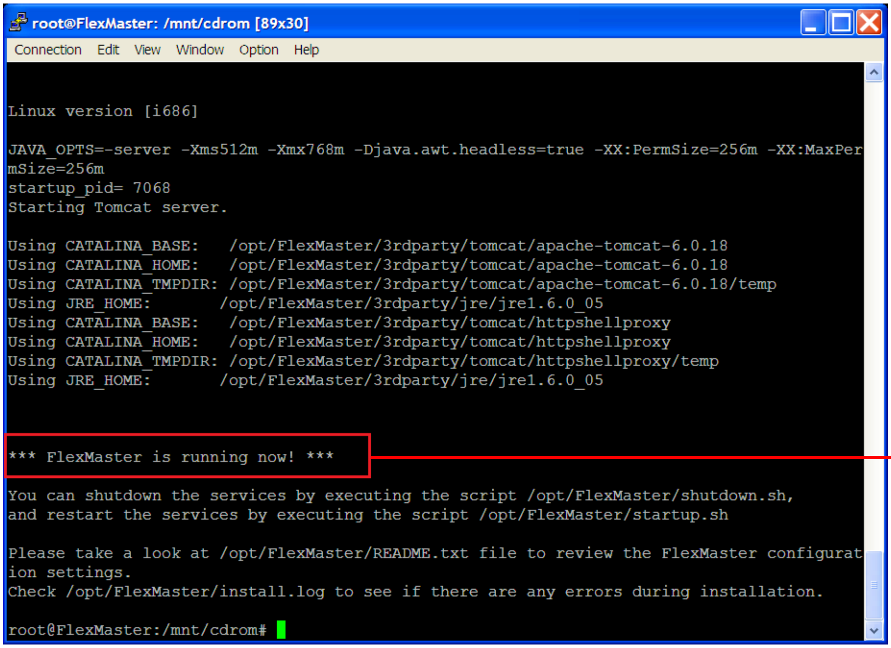
```
for the JAVA SE RUNTIME ENVIRONMENT (JRE) VERSION 6

SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE
SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON THE CONDITION
THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY
CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS
(COLLECTIVELY "AGREEMENT").  PLEASE READ THE AGREEMENT
CAREFULLY.  BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU
ACCEPT THE TERMS OF THE AGREEMENT. INDICATE ACCEPTANCE BY
SELECTING THE "ACCEPT" BUTTON AT THE BOTTOM OF THE
AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE
TERMS, SELECT THE "DECLINE" BUTTON AT THE BOTTOM OF THE
AGREEMENT AND THE DOWNLOAD OR INSTALL PROCESS WILL NOT
CONTINUE.

1. DEFINITIONS. "Software" means the identified above in
binary form, any other machine readable materials
(including, but not limited to, libraries, source files,
header files, and data files), any updates or error
corrections provided by Sun, and any user manuals,
programming guides and other documentation provided to you
by Sun under this Agreement.  "General Purpose Desktop
Computers and Servers" means computers, including desktop,
laptop and tablet computers, or servers, used for general
computing functions under end user control (such as but not
specifically limited to email, general purpose Internet

Do you agree to the above license terms? [yes or no]
```

Type 'yes' to accept the license agreement

After you accept the license agreement, the installation script installs all required packages. When the installation completes, the following message appears:

```
*** FlexMaster is running now! ***
```

Figure 15. You have completed installing FlexMaster


root@FlexMaster: /mnt/cdrom [89x30]
Connection Edit View Window Option Help

```
Linux version [i686]

JAVA_OPTS=-server -Xms512m -Xmx768m -Djava.awt.headless=true -XX:PermSize=256m -XX:MaxPer
mSize=256m
startup_pid= 7068
Starting Tomcat server.

Using CATALINA_BASE:   /opt/FlexMaster/3rdparty/tomcat/apache-tomcat-6.0.18
Using CATALINA_HOME:   /opt/FlexMaster/3rdparty/tomcat/apache-tomcat-6.0.18
Using CATALINA_TMPDIR: /opt/FlexMaster/3rdparty/tomcat/apache-tomcat-6.0.18/temp
Using JRE_HOME:       /opt/FlexMaster/3rdparty/jre/jre1.6.0_05
Using CATALINA_BASE:   /opt/FlexMaster/3rdparty/tomcat/httpshellproxy
Using CATALINA_HOME:   /opt/FlexMaster/3rdparty/tomcat/httpshellproxy
Using CATALINA_TMPDIR: /opt/FlexMaster/3rdparty/tomcat/httpshellproxy/temp
Using JRE_HOME:       /opt/FlexMaster/3rdparty/jre/jre1.6.0_05


*** FlexMaster is running now! ***

You can shutdown the services by executing the script /opt/FlexMaster/shutdown.sh,
and restart the services by executing the script /opt/FlexMaster/startup.sh

Please take a look at /opt/FlexMaster/README.txt file to review the FlexMaster configurat
ion settings.
Check /opt/FlexMaster/install.log to see if there are any errors during installation.

root@FlexMaster:/mnt/cdrom#
```

This message indicates that FlexMaster installation is complete

You have completed installing FlexMaster. You can now log in to the FlexMaster Web interface and configure the FlexMaster settings. For more information, refer to Logging into FlexMaster.

NOTE: If errors occur during installation, then details of these errors are written to the `install.log` file. Ruckus Wireless may ask you to provide the `install.log` file if you request support in troubleshooting your FlexMaster installation.

Extending the VM Hard Disk Size

The default hard disk size is 8GB. You can extend the hard disk size.

1. Before extending the hard disk size, please shut down VM.
   - If you use VMware Player, then please go to *Virtual Machine Settings* window and select **Hard Disk** from the device list. Then select *Utilities->Expand…* and then enter the new disk size.
   - If you use VMware ESXi, then please go to the VM's *Virtual Machine Properties* window and select **Hard disk** from the device list. Then in the *Disk Provisioning* tab enter the new disk size.
2. After you have changed the hard disk size, you have to create a partition for the new disk space. You could check current disk info with "df -l" shell command:

```
# df -l
Filesystem         1K-blocks Used   Available Use% Mounted on /dev/
sda3          7550352   682800 6484016   10%  /
tmpfs              961388         0  961388   0%   /dev/shm /dev/
sda1          198337     35856  152241   20%  /boot
```

NOTE: You could add a new partition **/dev/sda4**.

3. Start "fdisk" from the shell prompt:

```
# fdisk /dev/sda
```

WARNING! DOS-compatible mode is deprecated. It is strongly recommended that you switch off DOS-compatible mode (**command-c**) and change display units to sectors (**command-u**).

```
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 4
First cylinder (1045-1305, default 1045):
Using default value 1045
Last cylinder, +cylinders or +size{K,M,G} (1045-1305, default 1305):
Using default value 1305
Command (m for help): w
The partition table has been altered!
Calling ioctl() to re-read partition table.
WARNING: Re-reading the partition table failed with error 16: Device or resource
busy.
The kernel still uses the old table. The new table will be used at the next reboot
or after you run partprobe(8) or kpartx(8)
Syncing disks.
#
```

4. Reboot VM, and the new partition is added. Please check with:

```
# fdisk -l
Disk /dev/sda: 10.7 GB, 10737418240 bytes
255 heads, 63 sectors/track, 1305 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

```
Disk identifier: 0x000cdc5f
   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          26      204800   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2              26          90      512000   82  Linux swap / Solaris
Partition 2 does not end on cylinder boundary.
/dev/sda3              90        1045     7670784   83  Linux
/dev/sda4            1045        1305     2093804+  83  Linux (OPTIONAL)
```

5. Mount the new partition on a folder, for example */opt/FlexMaster*. If the folder has files, please move them into the */opt/backup* folder or some other operator-defined folder first. Then enter the mount command in the shell:

```
# mount /dev/sda4 /opt/FlexMaster/
```

6. Check the new file system with "df -h",

```
# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda3             7.3G  1.6G  5.3G  23% /
tmpfs                 939M     0  939M   0% /dev/shm
/dev/sda1             194M   36M  149M  20% /boot
/dev/sda4             2.0G   36M  1.9G   2% /opt/FlexMaster
```

   The partition sda4 has been successfully mounted on */opt/FlexMaster* folder.

7. Move the */opt/backup* folder files into */opt/FlexMaster* folder.

8. Add the mount command into the */etc/rc.d/rc.local* file, so that the mount will be automatically done on each reboot.

```
# !/bin/sh
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.
# mount /dev/sda4 /opt/FlexMaster
# touch /var/lock/subsys/local
# cd /opt/FlexMaster; bash ./startup.sh; #FlexMaster
```

9. Reboot VM.

The hard disk has been successfully extended and FlexMaster works well.

Configuring the Firewall

Root users can change the firewall settings of the iptables service for the VMware server. The firewall should be set to block all IP ports except those listed in Firewall Ports that Must be Open for Communications.

WARNING! Configuring the iptables requires that you turn off and reset your firewall rules. If your server uses its firewall as your first line of defense, it will be vulnerable while you are performing this procedure.

1. Log in as **root.**

2. Verify that iptables is installed:

```
$ rpm -q iptables
iptables-1.4.7-5.1.el6_2.x86_64
```

3. Verify that iptables is running:

```
# lsmod | grep ip_tables
ip_tables               29288  1 iptable_filter
x_tables                29192  6
ip6t_REJECT,ip6_tables,ipt_REJECT,xt_state,xt_tcpudp,ip_tables
```

4. Stop the iptables service:

```
$ service iptables stop
```

5. Refer to the iptables man pages to configure iptables to block all IP ports except those listed in Firewall Ports that Must be Open for Communications.

6. Start the iptables service:

```
$ service iptables start
```

Notable Files in the FlexMaster Root Directory

After you complete the installation, the following files are installed in the FlexMaster directory (`/opt/FlexMaster/`):

- `shutdown.sh`: Shuts down FlexMaster services.
- `startup.sh`: Restarts FlexMaster services after they have been shut down.
- `restart.sh:` Shuts down then restarts FlexMaster services.
- `upgrade.sh`: Upgrades the existing FlexMaster software.
- `backup.sh`: Backs up the FlexMaster database.
- `restore.sh`: Restores a backup of the FlexMaster database.
- `README`: Application notes.
- `install.log`: Complete record of installation, including your settings.
- `uninstall.sh`: Uninstalls FlexMaster.

Upgrading the FlexMaster Software

Ruckus Wireless releases FlexMaster software updates that contain feature enhancements or fixes for known issues. These software updates are made available on the Ruckus Wireless Support Web site or released through authorized channels. Update files typically use *{version number}.patch.tar* for their file naming convention (for example, *9.6.0.0.11.patch.tar*).

NOTE: Although the software update process has been designed to preserve all FlexMaster configuration settings, Ruckus Wireless strongly recommends that you back up the FlexMaster database, in case the update process fails for any reason. For information on how to back up the FlexMaster database, refer to Backing Up the Database from the Command Line Interface.

Beginning with release 9.4, FlexMaster upgrade files are delivered in .tar format to improve upgrade process control. The new upgrade script and patch files are contained in this tarball.

1. Log in to the host server as root.
2. Insert the FlexMaster upgrade CD into the CD-ROM drive.
3. If the FlexMaster server does not automatically mount the FlexMaster CD-ROM, then continue with Step 4. If the server automatically mounts the CD-ROM, then continue with Step 6.
4. Type the following command to create a mount point (or directory where you want to mount the CD-ROM):

```
# mkdir -p /mnt/cdrom
```

5. Type the following command to mount the CD-ROM manually to the created mount point:

```
# mount /dev/cdrom /mnt/cdrom
```

6. Upload the patch file (for example, *9.6.0.0.11.patch.tar*) to the FlexMaster server.
7. Copy the patch file to the FlexMaster folder */opt/FlexMaster/*:

```
# cp 9.6.0.0.11.patch.tar /opt/FlexMaster/
```

8. Navigate to `/opt/FlexMaster/:`

```
# cd /opt/FlexMaster/
```

9. Untar the patch file with following command:

```
# tar -vxf 9.6.0.0.11.patch.tar
```

10. Make sure that the *{version number}.patch* file, such as *9.6.0.0.11.patch*, has been extracted from the tar file.
11. Upgrade FlexMaster with following command:

```
# ./upgrade.sh 9.6.0.0.11
```

NOTE: After completing the software update, Ruckus Wireless recommends backing up the FlexMaster database so that you have a backup of the updated database schema. For instructions on how to back up the FlexMaster database, refer to Backing Up the Database from the Command Line Interface.

Uninstalling FlexMaster

1. Execute the FlexMaster uninstall script.

```
# [root@flexmaster FlexMaster]# ./uninstall.sh
```

2. After you execute the uninstall script, it performs the following steps:
   a. It shuts down the Tomcat server.
   b. It shuts down the MySQL server.
   c. It deletes the configuration files, and uninstalls the FlexMaster services.
   d. It restores the original `/etc/my.cnf` file.
   e. It finds /etc/my.cnf.ruckus, and then renames it to `/etc/my.cnf`.

f. Finally, it deletes the `/opt/FlexMaster` directory.

When the uninstall script completes deleting the `/opt/FlexMaster` directory, the uninstallation process is complete.

Backing Up the Database from the Command Line Interface

It is good practice to back up your FlexMaster database before installing a new version of any software. Although Ruckus Wireless has done its best to ensure a seamless experience when using FlexMaster, you should protect your data by creating a backup of all critical data stored on your host FlexMaster server. Ruckus Wireless recommends that you back up and reload your FlexMaster database tables from any previous version when upgrading to the next major version or patch release.

FlexMaster includes `backup.sh`, a script for backing up the FlexMaster database, which is located in the FlexMaster root directory.

Follow these steps to back up the FlexMaster database.

1. On the Linux server, go to the FlexMaster root directory (`/opt/FlexMaster`).
2. Execute the database backup script. You can either specify the file path and file name of the backup file, or you can let FlexMaster automatically set the path.
   - To back up the FlexMaster database to a specific file path and file name, enter the following command:

     ```
     # ./backup.sh {file path and file name where you want to save the backup file}
     ```

     For instance, if you want to save the backup file to the FlexMaster root directory with the file name `Mybackup.tgz`, then enter the following command:

     ```
     # ./backup.sh Mybackup.tgz
     ```

   - To back up the FlexMaster database without specifying the file path and file name, enter the following command:

     ```
     # ./backup.sh
     ```

     In this case, the backup file is created in the default backup folder, `/opt/FlexMaster/backup folder`, and the file name is automatically assigned based on the date and time when the backup script was executed (for example, `212-08-30_13h36m.tgz`).

When the backup process is completed, a message appears in the command line interface, informing you that the FlexMaster database has been backed up successfully.

Restoring the Database from the Command Line Interface

FlexMaster provides `restore.sh`, a script for restoring a backup copy of the FlexMaster database located in the FlexMaster root directory.

CAUTION! Before starting this procedure, take note of the file path and file name of the FlexMaster database backup file. You need to enter this information when you execute the restore script.

Follow these steps to restore a backup copy of the FlexMaster database.

1. On the Linux server, go to the FlexMaster root directory (`/opt/FlexMaster`).
2. Execute the database restore script by entering the following command:

   ```
   # ./restore.sh {file path and file name of the backup file that
   you want to restore}
   ```

   For example, if you want to restore a backup file named `Mybackup.tgz` that is located in the FlexMaster root directory, then enter the following command:

   ```
   # ./restore.sh Mybackup.tgz
   ```

When the restore process is completed, a message appears in the command line interface, informing you that the FlexMaster database that you specified has been restored successfully.

What’s Next?

With Ruckus Wireless FlexMaster now installed, you can log in and configure FlexMaster to manage your Ruckus Wireless devices. The chapters that follow guide you through all of these configuration tasks.

3

Getting Started with FlexMaster

In This Chapter:

Logging into FlexMaster

Use one of the Web browsers described in Web Browser Requirements to access the FlexMaster Web interface:

NOTE: When accessing the FlexMaster Web interface, Ruckus Wireless recommends using a monitor with at least 1280 x 1024 screen resolution. If you use a monitor with lower resolution, then you may not be able to see all Web interface elements at the same time and you may have to scroll through the page to see hidden elements.

1. On your computer, open a Web browser window.
2. In the browser window, type the IP address or host name (if you have set up DNS for the server) of the FlexMaster server as follows:

   ```
   http://<ipaddress>
   ```

   --OR--

   ```
   https://<ipaddress>
   ```

   --OR--

   ```
   http://flexmaster
   ```

   --OR--

   ```
   https://flexmaster
   ```

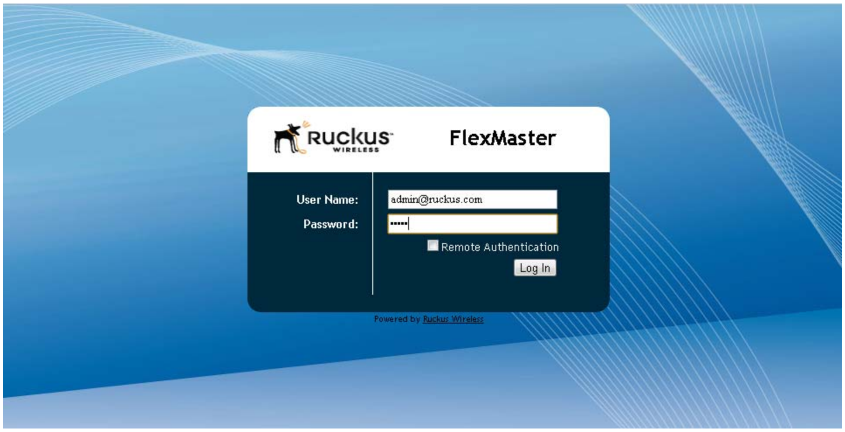
3. Press **<Enter>** to initiate the connection.

   If you are using HTTPS, then a security alert dialog box appears. Click **OK/Yes/ Proceed anyway** to continue.

NOTE: By default, FlexMaster uses a Ruckus Wireless signed security certificate that Web browsers do not recognize, causing them to display the security alert. If you want to prevent the security alerts from appearing every time you connect to FlexMaster using HTTPS, then you can install a certificate issued by a recognized certificate authority such as VeriSign. For information, refer to Managing SSL Certificates.

The *Ruckus Wireless Admin* login page appears.

Figure 16. The FlexMaster login page



User Name: admin@ruckus.com

Password: •••••

□ Remote Authentication

4. If you are not using remote authentication, then type the administrator account user name and password that you configured during installation. The full user name includes the company domain name that you specified during FlexMaster installation (refer to Installing the FlexMaster Software). For example:

   User Name: **`admin@domain.com`**

   Password: **`admin`**

5. If you are using remote authentication, then check the *Remote Authentication* check box. Then log in using the TACACS+ server configured in TACACS+ Settings.

NOTE: If you log in using the TACACS+ server, then your user name appears in the top right of the FlexMaster page followed by *(Tacacs+)*.

6. Click **Log In**. The Ruckus Wireless FlexMaster Web interface appears in the browser window. The *Dashboard* workspace appears by default.

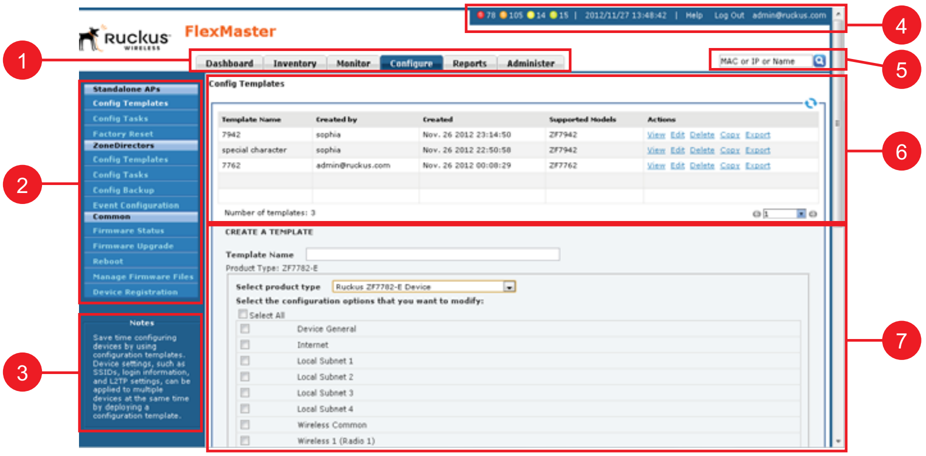
   For more on the Dashboard, refer to Getting to Know the Dashboard and Its Widgets.

NOTE: The Web interface has a session timeout mechanism that logs you out of the system automatically after 30 minutes of inactivity. This helps secure the Web interface and prevent unauthorized users from changing your FlexMaster configuration.

NOTE: If you recently upgraded the FlexMaster software, then Ruckus Wireless strongly recommends that you clear your Web browser’s cache before logging into the FlexMaster Web interface. This helps ensure that the FlexMaster Web interface shows all the changes and enhancements that were implemented in the new software version.

Features of the FlexMaster Web Interface

Figure 17. The FlexMaster Web interface has seven primary elements



Save time configuring devices by using configuration templates. Device settings, such as SSIDs, login information, and L2TP settings, can be applied to multiple devices at the same time by deploying a configuration template.

Config Templates

Template Name	Created by	Created	Supported Models	Actions
7942	sophia	Nov. 26 2012 23:14:50	ZF7942	View Edit Delete Copy Export
special character	sophia	Nov. 26 2012 22:50:58	ZF7942	View Edit Delete Copy Export
7762	admin@ruckus.com	Nov. 26 2012 00:08:29	ZF7762	View Edit Delete Copy Export

Number of templates: 3

CREATE A TEMPLATE

Template Name

Product Type: ZF7782-E

Select product type: Ruckus ZF7782-E Device

Select the configuration options that you want to modify:

□ Select All
□ Device General
□ Internet
□ Local Subnet 1
□ Local Subnet 2
□ Local Subnet 3
□ Local Subnet 4
□ Wireless Common
□ Wireless 1 (Radio 1)

Table 5. FlexMaster Web interface elements

No.	Interface Element	Description
1	Main Menu	Six tabs that group related tasks that you can perform in FlexMaster. These tabs include: • Dashboard • Inventory • Monitor • Configure • Reports • Administer
2	Submenu	On each tab are second level menu items that, when clicked, display related options in the content area to the right.
3	Page Notes	Provides brief descriptions of the tasks that you can perform on the page.

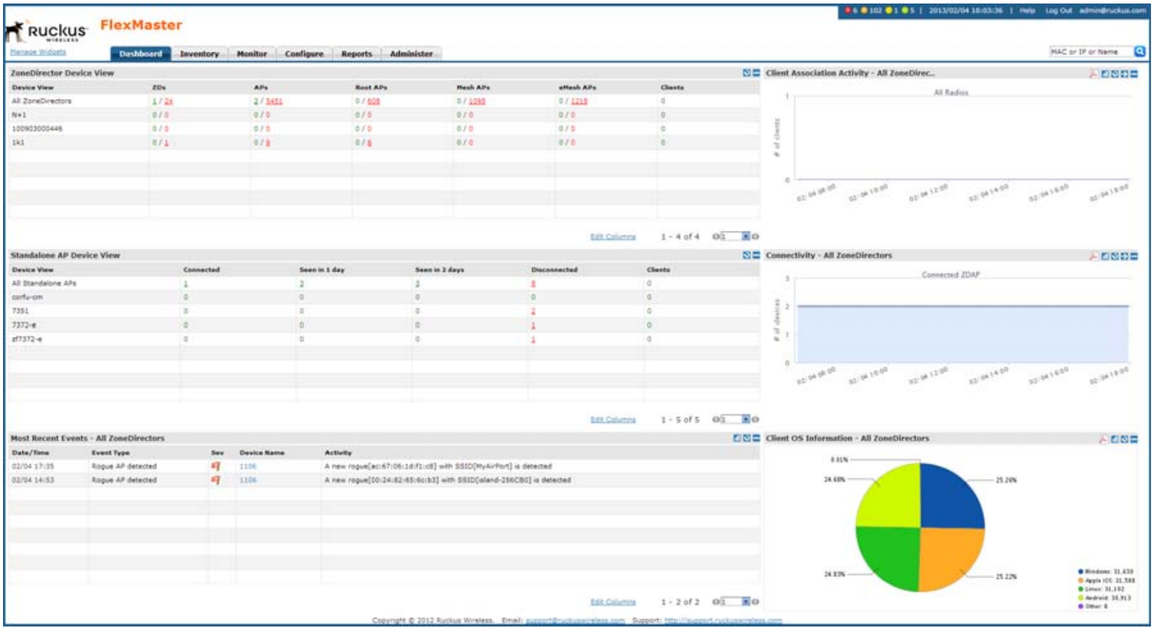
Table 5. FlexMaster Web interface elements (Continued)

No.	Interface Element	Description
4	Help and Log Out	• Shows an alarm summary (if enabled in *Monitor > Alarm Settings*). • Shows the current FlexMaster date and time. • Click the **Help** link to open the online help. • Click the **Log Out** link to log out of the FlexMaster. The user name identifies the user who is logged in.
5	Search Box	Allows you to search for a managed ZoneDirector, a standalone AP, or a client that reports to a managed AP. To search for a device, type a full or partial MAC address, IP address, or device name.
6	Content Area	This large area displays tables and configuration forms relevant to your menu choices.
7	Configuration Area	This area is populated when an action is chosen from the content area.

Getting to Know the Dashboard and Its Widgets

After you log in to the FlexMaster Web interface, the Dashboard is the first page that appears. The Dashboard provides a quick summary of what is happening on FlexMaster and its managed devices. It uses widgets to display at-a-glance information about managed devices, traffic status, connectivity status, and events that have occurred on managed devices.

Figure 18. The Dashboard



ZoneDirector Device View

Device View	ZDs	APs	Root APs	Mesh APs	eMesh APs	Clients
All ZoneDirectors	1 / 24	2 / 3431	0 / 608	0 / 1055	0 / 1218	0
N+1	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0
100903000446	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0
1k1	0 / 1	0 / 9	0 / 6	0 / 0	0 / 0	0

1 - 4 of 4

Standalone AP Device View

Device View	Connected	Seen in 1 day	Seen in 2 days	Disconnected	Clients
All Standalone APs	1	2	2	4	0
corfu-cm	0	0	0	0	0
7351	0	0	0	2	0
7372-e	0	0	0	1	0
zf7372-e	0	0	0	1	0

1 - 5 of 5

Most Recent Events - All ZoneDirectors

Date/Time	Event Type	Sev	Device Name	Activity
02/04 17:35	Rogue AP detected		1106	A new rogue[ac:67:06:1d:f1:c8] with SSID[MyAirPort] is detected
02/04 14:53	Rogue AP detected		1106	A new rogue[00:24:82:65:6c:b3] with SSID[island-256CB0] is detected

1 - 2 of 2

This section describes the information that you can find on the Dashboard and how to use widgets to display information that is most relevant to managing FlexMaster and its managed devices. Topics include:

- Widgets That You Can Display
- Available Widget Slots
- Default Widgets
- Adding a Widget
- Hiding a Widget
- Deleting a Widget

NOTE: By default, FlexMaster uses the 3-tier management mode. This means that the Web interface displays data for FlexMaster, ZoneDirector, and APs. If you do not have a ZoneDirector on the network, then you could switch to 2-tier management mode to hide data for the ZoneDirector. For more information on how to switch to a 2-tier management mode, refer to Configuring System Settings.

NOTE: Information in each of the widgets and graphs refreshes automatically based on a non-configurable time interval. To refresh the information manually, click the ↻ button that is in the same section as the widget or graph.

Widgets That You Can Display

By default, FlexMaster displays the following six standard widgets, which cannot be deleted (only minimized) from the Dashboard:

- ZoneDirector Device View Widget
- Standalone AP Device View Widget
- Most Recent Events Widget
- Client Association Activity Widget
- Connectivity Widget
- Client OS Information Widget

In addition to these standard widgets, you can also add Customized Widgets, which include the Google Maps widget and some other widgets that are related to Capacity, SLA and Troubleshooting.

For more information on each widget, refer to the following sections.

ZoneDirector Device View Widget

The ZoneDirector Device View widget displays information about ZoneDirector devices that have registered with FlexMaster. It shows the number of APs that are being managed by the ZoneDirector devices (that belong to the view) and the clients that are associated with these managed APs.

The following table describes the columns that appear on the ZoneDirector Device View widget.

NOTE: When ZoneDirector is behind a network address translation (NAT) server and port forwarding has not been configured on FlexMaster and the NAT server, the AP and client information appears as "0" (zero) on the ZoneDirector Device View widget.

Table 6. Columns on the ZoneDirector Device View Widget

Column Name	Description
Device View	Shows the name of the ZoneDirector device view. By default, a group called *All ZoneDirectors* exists, which contains all ZoneDirector devices detected on the network.
ZDs	Shows the number of ZoneDirector units that are registered with FlexMaster. There are two numbers in the *ZDs* column and they are separated by a slash symbol (for example, X / Y). • The number in green (before the slash symbol) indicates the number of ZoneDirector devices that are currently online. • The number in red (after the slash symbol) indicates the number of ZoneDirector devices that are currently offline or disconnected from FlexMaster. The sum of these two numbers is equal to the total number of ZoneDirector devices that are registered with FlexMaster. Clicking either number (hyperlink) takes you to the *Reports > Device View* page, which shows details of all these connected or disconnected ZoneDirector units.
APs	Shows the number of APs that are registered with ZoneDirector devices (which, in turn, are being managed by FlexMaster). There are two numbers in the *APs* column and they are separated by a slash symbol (for example, X / Y). • The number in green (before the slash symbol) indicates the number of APs that are currently online. • The number in red (after the slash symbol) indicates the number of APs devices that are currently offline or disconnected from ZoneDirector. The sum of these two numbers is equal to the total number of APs that are registered with ZoneDirector. Clicking either number (hyperlink) takes you to the *Reports > Device View* page, which shows details of all these connected or disconnected APs. **NOTE:** *When mesh networking is enabled on ZoneDirector, three additional columns (namely, Root APs, Mesh APs and eMesh APs) appear after the APs column. These three columns are similar to the APs column, in that they display the number of online and offline APs. Refer to* Additional AP Columns When Mesh Networking Is Enabled *for more information.*

Table 6. Columns on the ZoneDirector Device View Widget (Continued)

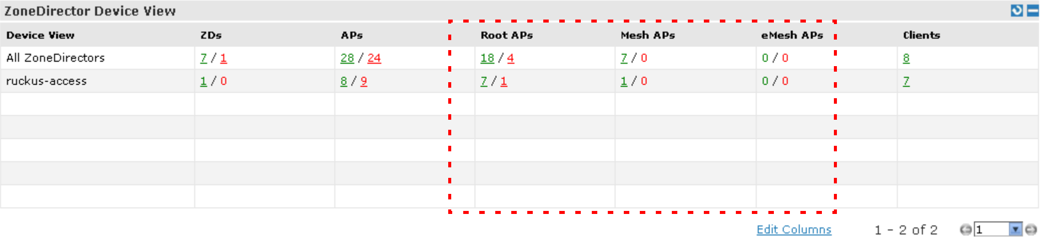
Column Name	Description
Clients	Shows the number of clients that are associated with the currently connected APs. Clicking this number (hyperlink) takes you to the *Reports > Device View* page, which shows details of all these associated clients and the APs with which they are associated.

Additional AP Columns When Mesh Networking Is Enabled

A mesh network is a peer-to-peer, multi-hop wireless network wherein participant nodes cooperate to route packets. In a Ruckus wireless mesh network, the routing nodes (that is, the Ruckus Wireless APs forming the network), or "mesh nodes", form the network's backbone. Clients (for example, laptops and other mobile devices) connect to the mesh nodes and use the backbone to communicate with one another, and if permitted, with nodes on the Internet. The mesh network enables clients to reach other systems by creating a path that "hops" between nodes.

When mesh networking is enabled, three additional columns (that display the number of APs that are part of the network) appear in the ZoneDirector *Device View* widget.

Figure 19. Root APs, Mesh APs, and eMesh APs columns on the ZoneDirector Device View widget



ZoneDirector Device View

Device View	ZDs	APs	Root APs	Mesh APs	eMesh APs	Clients
All ZoneDirectors	7 / 1	28 / 24	18 / 4	7 / 0	0 / 0	8
ruckus-access	1 / 0	8 / 9	7 / 1	1 / 0	0 / 0	7

Edit Columns   1 - 2 of 2   1

NOTE: For more information on mesh networking, refer to the *ZoneDirector User Guide*.

The additional mesh-related columns that appear in the ZoneDirector widget include:

- *Root APs:* A root AP (RAP) is mesh node that is connected to ZoneDirector through its wired Ethernet interface. There are two numbers in the *Root APs* column and they are separated by a slash symbol (for example, X / Y).
  - The number in green (before the slash symbol) indicates the number of root APs that are currently online.
  - The number in red (after the slash symbol) indicates the number of root APs that are currently offline or disconnected from ZoneDirector.
- *Mesh APs:* A mesh AP (MAP) is a mesh node that is connected to a mesh AP through its wireless interface. There are two numbers in the *Mesh APs* column and they are separated by a slash symbol (for example, X / Y).

  - The number in green (before the slash symbol) indicates the number of mesh APs that are currently online.
  - The number in red (after the slash symbol) indicates the number of mesh APs that are currently offline or disconnected from ZoneDirector.
- *eMesh APs:* An eMesh AP is a mesh node that is connected to a mesh AP through its wired Ethernet interface. If the MAP to which the LAP is connected goes offline, then the eMesh AP can turn into a MAP if it is able to find a RAP.
  - The number in green (before the slash symbol) indicates the number of eMesh APs that are currently online.
  - The number in red (after the slash symbol) indicates the number of eMesh APs that are currently offline or disconnected from ZoneDirector.

Standalone AP Device View Widget

The Standalone AP Device View Widget provides a quick glance of all existing AP device views, including the default and custom AP device views, listing them by default in alphabetical order.

NOTE: For more on creating device views, refer to Creating a Standalone AP View.

NOTE: The *Dashboard > Standalone AP Device View* is updated every 15 minutes, while the *Report > Device View* is a real time report. Therefore, there are differences between the two views.

Table 7. Columns on the Standalone AP Device View widget

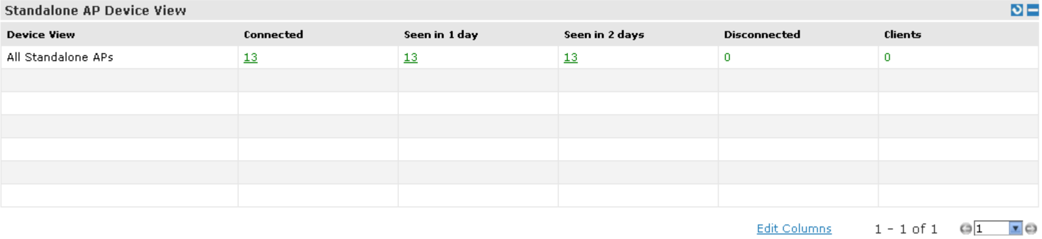
Column Name	Description
Device View	Shows the name of the AP device view. A default device view named *All Standalone APs* exists. Clicking this number (hyperlink) takes you to the *Reports > Device View* page, which shows details of these APs.
Connected	Shows the number of APs that are currently connected to FlexMaster. Clicking this number (hyperlink) takes you to the *Reports > Device View* page, which shows details of all these connected APs.
Seen in 1 day	Shows the number of devices seen in the last 24 hours. Click the link to go to *Reports > Device View* page for a view of the devices that reported in during the last 24 hours.
Seen in 2 days	Shows the number of devices seen in the last 48 hours. Click the link to go to *Reports > Device View* page for a view of the devices that reported in within during the last 48 hours.
Disconnected	Shows the number of APs that are reporting to FlexMaster, but are currently disconnected. Clicking this number (hyperlink) takes you to the *Reports > Device View* page, which shows details of all these disconnected APs.

Table 7. Columns on the Standalone AP Device View widget (Continued)

Column Name	Description
Clients	Shows the number of clients that are associated with the currently connected APs. Clicking this number (hyperlink) takes you to the *Reports > Device View* page, which shows details of all these associated clients and the APs with which they are associated.

NOTE: To determine the total number of APs that are reporting to FlexMaster, add the numbers in the *Connected* and *Disconnected* columns.

Figure 20. The Standalone AP Device View widget



Standalone AP Device View

Device View	Connected	Seen in 1 day	Seen in 2 days	Disconnected	Clients
All Standalone APs	13	13	13	0	0

Edit Columns 1 - 1 of 1 1

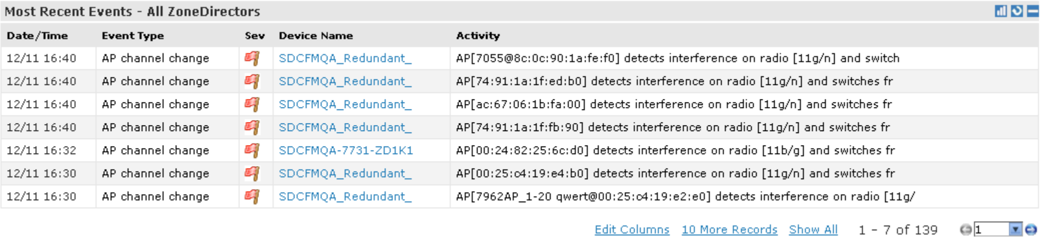
Most Recent Events Widget

The Most Recent Events widget displays events that have occurred on FlexMaster, on managed ZoneDirector devices and standalone APs, and on clients that report to managed APs. The following table describes the information that you can find on the Events widgets.

Table 8. Columns on the Most Recent Events widget

Column Name	Description
Event Type	Displays the name of the event (as assigned by Ruckus Wireless)
Sev (Severity)	Indicates the importance of an events. There are three event severity levels in FlexMaster: • *Error* (high importance): These are events that you should check. For example, if you see `Rogue AP detected` in the Event Type column, then you might want to check whether it is an AP that should authorized or if someone is attempting to spoof authorized APs. • *Warning* (medium importance): These are events that may require your attention. For example, if you see `Connectivity problem`, then you might want to check what is causing the connectivity issue. When a significant number of devices are experiencing this issue, it might indicate a network issue that needs to be resolved. • *Info* (low importance): These are informational events that typically do not require your attention (for example, `Device rebooted`).
Device Name	Name of AP reporting the event. Click this link to go to an *Inventory > Reports* view of the devices reporting the specific event.
Activity	Events description.
Device Events	Displays the number of events generated by all Standalone APs.

Figure 21. Columns on the Most Recent Events widget



Most Recent Events - All ZoneDirectors

Date/Time	Event Type	Sev	Device Name	Activity
12/11 16:40	AP channel change	🚩	SDCFMQA_Redundant_	AP[7055@8c:0c:90:1a:fe:f0] detects interference on radio [11g/n] and switch
12/11 16:40	AP channel change	🚩	SDCFMQA_Redundant_	AP[74:91:1a:1f:ed:b0] detects interference on radio [11g/n] and switches fr
12/11 16:40	AP channel change	🚩	SDCFMQA_Redundant_	AP[ac:67:06:1b:fa:00] detects interference on radio [11g/n] and switches fr
12/11 16:40	AP channel change	🚩	SDCFMQA_Redundant_	AP[74:91:1a:1f:fb:90] detects interference on radio [11g/n] and switches fr
12/11 16:32	AP channel change	🚩	SDCFMQA-7731-ZD1K1	AP[00:24:82:25:6c:d0] detects interference on radio [11b/g] and switches fr
12/11 16:30	AP channel change	🚩	SDCFMQA_Redundant_	AP[00:25:c4:19:e4:b0] detects interference on radio [11g/n] and switches fr
12/11 16:30	AP channel change	🚩	SDCFMQA_Redundant_	AP[7962AP_1-20 qwert@00:25:c4:19:e2:e0] detects interference on radio [11g/

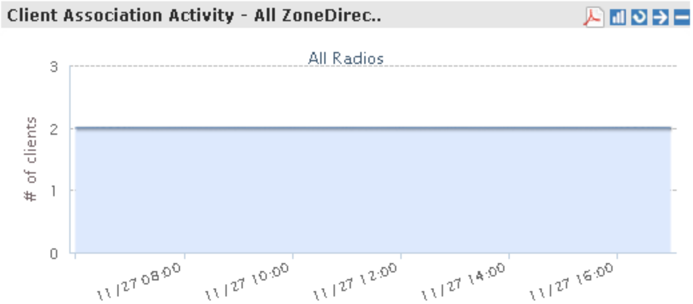
Client Association Activity Widget

The Client Association Activity widget shows the number of clients that have associated with managed APs. The default Client Association Activity widget displays connectivity information for the All ZoneDirectors device view and on all radios on the managed APs.

When you want to view a tabular version of the information on the widget, click the ➔ (Navigate) icon in the upper-right corner of the widget. This takes you to the *Client Association* page on the *Reports* tab, where you can view detailed client association information for the selected device view.

NOTE: Information on the *Client Association Activity* widget is updated automatically every hour.

Figure 22. The Client Association Activity widget for the All ZoneDirectors device view



You can customize the information that appears on the widget. For example, you can switch to a different device view or view association activity for a specific radio only.

1. Click the 📊 (Edit) icon in the upper-right corner of the widget. The *Customize Trend Graph* window appears.
2. Configure the options under Report Criteria to show information that you want to appear on the widget. These options include:
   - *Device View:* Select the device view that you want to display.
   - *Radio Type:* Select the radio for which you want to display association information. Options include **All Radios**, **11b/g**, **11a/n**, **11g/n**, and **11a**.
   - *Display Period:* Select the time period for which you want to display connectivity information. Options range from 4 hours to one week. You can also specify a date range (maximum of seven days).
   - *Serial Number OR Name:* When you want to display association information for a specific AP only, type a partial or full serial number or device name in the box. When results appear under the box, click the AP for which you want to display information on the widget.
3. Click **Apply** to save your changes.

You have completed customizing the widget.

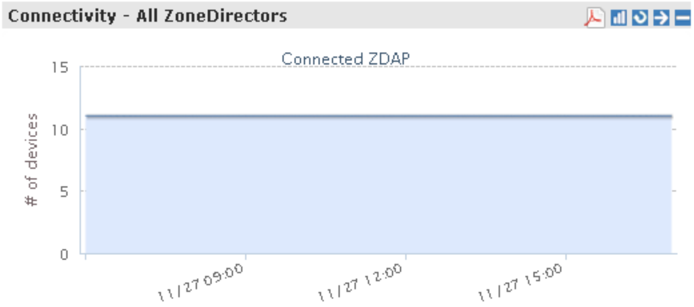
Connectivity Widget

The Connectivity widget displays (in an interactive volume graph) the number of connectivity or loss-of-connectivity events on devices. The default Connectivity widget displays connectivity information for the All ZoneDirectors device view.

When you want to view a tabular version of the information on the widget, click the ➔ (Navigate) icon in the upper-right corner of the widget. This takes you to the Historical *Connectivity* page on the *Reports* tab, where you can view detailed connectivity information for the selected device view.

NOTE: Information on the *Connectivity* widget is updated automatically every hour.

Figure 23. The Connectivity widget for the All ZoneDirectors device view



You can customize the information that appears on the widget. For example, you can switch to a different ZoneDirector device view or view connectivity information of managed APs.

Follow these steps to customize the *Connectivity* widget.

1. Click the 📶 (Edit) icon in the upper-right corner of the widget. The *Customize Trend Graph* window appears.
2. Configure the options under *Report Criteria* to show information that you want to appear on the widget. These options include:
   - *Device View:* Select the device view that you want to display.
   - *Device Type:* Select whether you want to display connectivity information on ZoneDirector devices or its managed APs.
   - *Status:* Select whether you want to show connectivity or loss of connectivity information.
   - *Display Period:* Select the time period for which you want to display connectivity information. Options range from 4 hours to one week. You can also specify a date range (maximum of seven days).
3. Click **Apply** to save your changes.

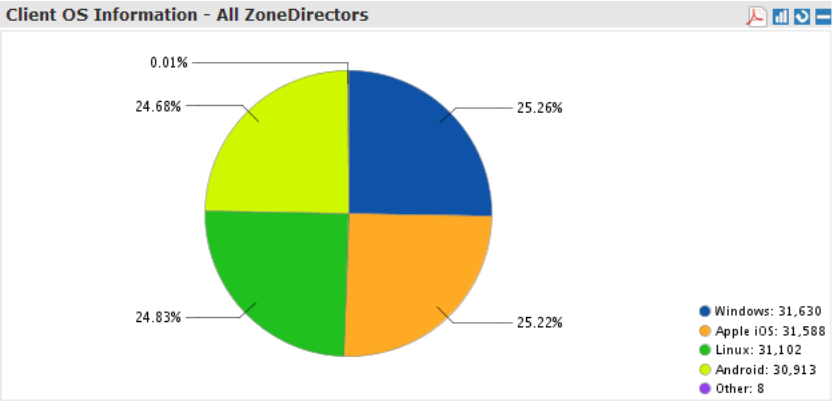
You have completed customizing the widget.

Client OS Information Widget

The Client OS Information widget displays a pie chart of wireless clients based on the operating systems (Windows, Mac OS, Android, and others) that they are running on.

By default, client OS information is retrieved from the *All ZoneDirectors* device view. You can customize the widget to display client OS information from other ZoneDirector device views.

Figure 24. The Client OS Information widget for All ZoneDirectors



1. Click the 📊 (Edit) icon in the upper-right corner of the widget. The *Customize Trend Graph* window appears.
2. In *Device View*, select the ZoneDirector device view for which you want to display the client OS information.
3. Click **Apply** to save your changes.

You have completed customizing the widget.

Customized Widgets

In addition to the six default FlexMaster widgets, you can also display the following custom widgets on the Dashboard.

- Capacity Widget
- SLA Widget
- Troubleshooting Widget

NOTE: For instructions on how to add these widgets, refer to Adding a Widget.

Capacity Widget

The *Capacity* widget can show client population, traffic and throughput information. See the following table for the types of information that you can show on the *Capacity* widget.

Table 9. Information that you can show on the Capacity widget

Information	Device
# of Associated Clients	ZoneDirector
Air-Time Utilization - 802.11b/g	ZoneDirector
Air-Time Utilization - 802.11a/n	ZoneDirector
Air-Time Utilization - 802.11g/n	ZoneDirector
AP Actual Throughput - Tx	ZoneDirector
AP Actual Throughput - Rx	ZoneDirector
AP Traffic - Tx	ZoneDirector
AP Traffic - Rx	ZoneDirector
Client Actual Throughput - TX	ZoneDirector
Client Actual Throughput - Rx	ZoneDirector
Client Traffic - Tx	ZoneDirector
Client Traffic - Rx	ZoneDirector
Backhaul Throughput	Standalone AP

SLA Widget

The *SLA* (service level agreement) widget can show uptime, downtime and potential throughput information. See the following table for the types of information that you can show on the *SLA* widget.

Table 10. Information that you can show on the SLA widget

Information	Device
AP Downtime	ZoneDirector and Standalone AP
AP Uptime	ZoneDirector and Standalone AP
Client Potential Throughput	ZoneDirector
Client Associated Time	ZoneDirector
Backhaul Link Uptime	Standalone AP

Troubleshooting Widget

The *Troubleshooting* widget can show information that may be helpful in resolving connectivity issues on the network. See the following table for the types of information that you can show on the *Troubleshooting* widget.

Table 11. Information that you can show on the Troubleshooting widget

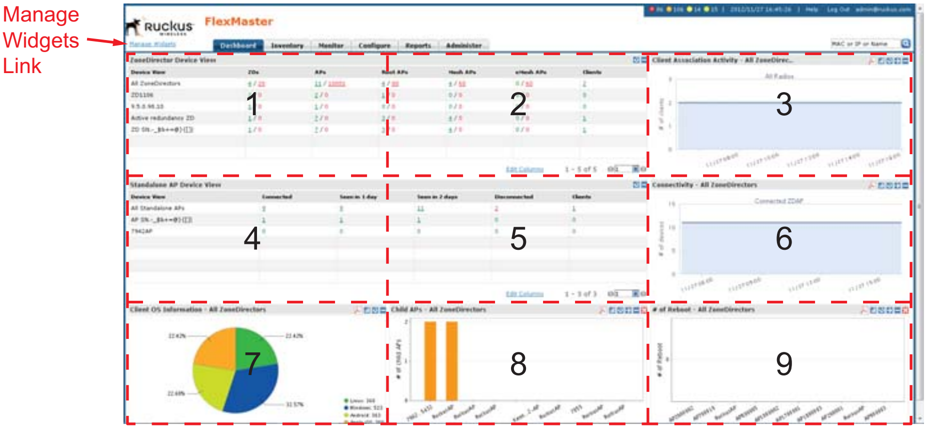
Information	Device
# of Child APs	ZoneDirector
# of Hops	ZoneDirector
Change of Topology of Mesh	ZoneDirector
Client Phy Rate	ZoneDirector
Client RSSI	ZoneDirector
Mesh RSSI	ZoneDirector
# of Reboot	ZoneDirector
Physical Link Distance	ZoneDirector
Backhaul Change of State	Standalone AP

Available Widget Slots

FlexMaster provides nine slots on the Dashboard for placing widgets.

Note that some widgets are wider (for example, the ZoneDirector Device View widget) and require two widget slots. Make sure there are enough empty slots on the Dashboard before you add a widget.

Figure 25. Nine widget slots on the Dashboard



Default Widgets

By default, FlexMaster displays the following widgets on the Dashboard:

- ZoneDirector Device View
- Standalone AP Device View
- Most Recent Events View
- Client Association Activity View
- Client OS Information
- Connectivity View

These default widgets cannot be deleted, but you can hide or minimize them so you can place other widgets if you want.

Adding a Widget

You can add widgets to the Dashboard as long as there are available slots. The Dashboard provides nine slots for widgets.

1. Click the **Manage Widgets** link at the bottom of the Dashboard. A mini sidebar appears on the left side of the Dashboard and displays widgets that you can add.

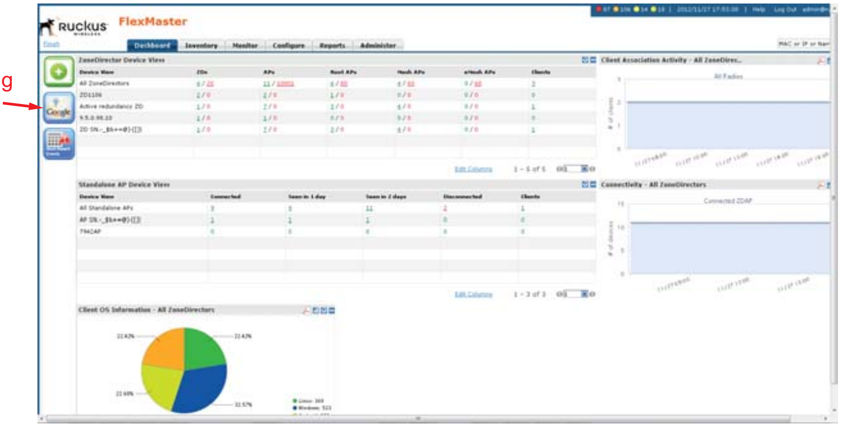
2. Click-and-hold the widget that you want to add, and then drag it to an empty slot where you want to place it. There are nine slots on the Dashboard.
3. Release the mouse button to place the widget.

The page refreshes, and the widget that you added appears in the slot where you placed it.

NOTE: When you are unable to place a widget in a slot, verify that the slot is empty. Also, some widgets (for example, the ZoneDirector Device View widget) are wider and require more than one slot. Make sure that are enough slots for the widget that you are adding.

Figure 26. A mini sidebar appears on the left side

Mini sidebar displaying widgets you can add


Ruckus
FlexMaster
Dashboard
Inventory
Monitor
Configure
Reports
Administer
ZoneDirector Device View
Client Association Activity - All ZoneDirec...
Standalone AP Device View
Connectivity - All ZoneDirectors
Client OS Information - All ZoneDirectors

Hiding a Widget

Default widgets cannot be deleted, but you can hide or minimize them. For a list of default widgets, refer to Default Widgets.

- Click the ▬ (Minimize) icon in the upper-right corner of the default widget that you want to minimize. The widget disappears from the Dashboard as it is minimized to the widget sidebar.
- To show the widget again, refer to Adding a Widget.

Deleting a Widget

When you no longer want the customized widgets that you have added, you can delete them.

- Click the ☒ (Delete) icon that is in the upper-right corner of the customized widget that you want to delete. The widget disappears from the Dashboard.
- To show the widget again, refer to Adding a Widget.

Getting Started Tasks

Before configuring FlexMaster to manage your AP and ZoneDirector devices, Ruckus Wireless recommends performing the following tasks:

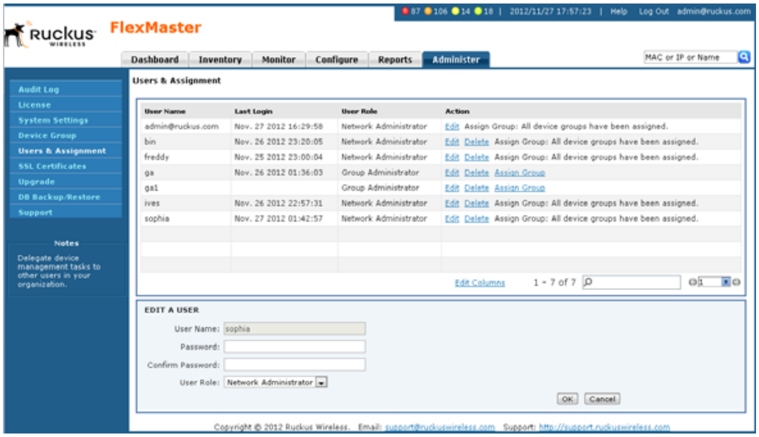
- Changing the Default Password
- Pointing Your Ruckus Wireless AP to FlexMaster
- Pointing A ZoneDirector to FlexMaster
- Checking Your FlexMaster License
- Configuring Your Devices to Work with TACACS+
- Configuring Your Devices to Communicate with FlexMaster over L2TP

Changing the Default Password

Ruckus Wireless recommends that you change the default administrative password as soon as possible to prevent unauthorized users from accessing the FlexMaster Web interface and modifying the settings you have configured.

1. After logging in to the FlexMaster Web interface, go to *Administer > Users & Assignment.*
2. In the *Users* table, look for the network administrator user account that you used to log in to the FlexMaster Web interface.
3. Click the **Edit** link (in the *Action* column) that is in the same row as the user account name. The *EDIT A USER* form appears below the table.

Figure 27. The Edit a User form appears at the bottom of the page



Users & Assignment

User Name	Last Login	User Role	Action
admin@ruckus.com	Nov. 27 2012 16:29:58	Network Administrator	Edit Assign Group: All device groups have been assigned.
bin	Nov. 26 2012 23:20:05	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
freddy	Nov. 25 2012 23:00:04	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
ga	Nov. 26 2012 01:36:03	Group Administrator	Edit Delete Assign Group
ga1		Group Administrator	Edit Delete Assign Group
ives	Nov. 26 2012 22:57:31	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
sophia	Nov. 27 2012 01:42:57	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.

Edit Columns 1 - 7 of 7

EDIT A USER

User Name: sophia
Password:
Confirm Password:
User Role: Network Administrator

OK Cancel

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

4. Type a new password in the **Password** field.
   - Passwords must be between 6 and 32 characters long, and must be comprised of letters and numbers only.
   - Passwords are case-sensitive.

- Do not use spaces.

NOTE: Make sure you remember your new password. You will use this new password the next time you want to log in to the FlexMaster Web interface.

5. Retype the new password in the **Confirm Password** field.
6. Click **OK**.

Pointing Your Ruckus Wireless AP to FlexMaster

Your Ruckus Wireless APs are required to call home to register with FlexMaster; FlexMaster does not initiate initial contact. To register with FlexMaster, Ruckus Wireless APs must know the FlexMaster server URL, thus requiring that URL is available over the Internet.

Take note of the following:

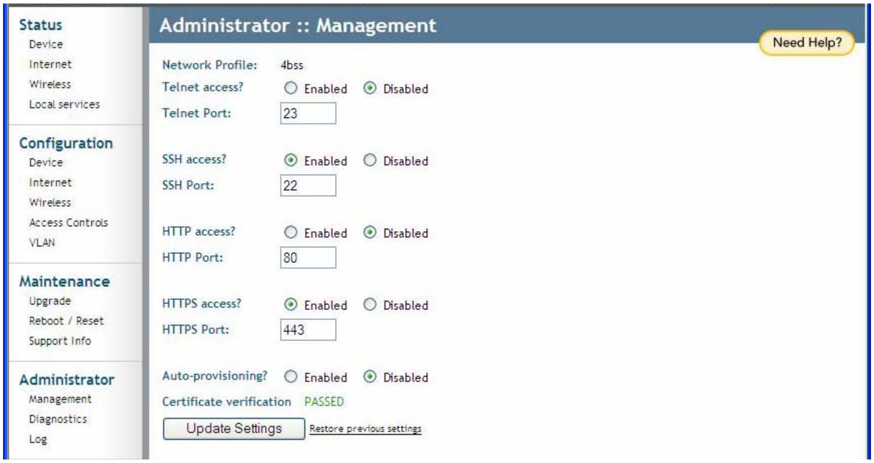
- ZoneFlex APs shipped with this version are preconfigured with the URL of your FlexMaster server, so you only need to set up your DHCP or DNS settings as described previously in this chapter.
- ZoneFlex APs running on earlier software versions must be upgraded to this version before they can register with FlexMaster. Once upgraded, perform the steps below.

  In most cases, you can supply the FlexMaster URL using either DNS or DHCP as described earlier in this chapter. If these methods are not available to you, then you can manually set the URL as described in the procedure that follows.

NOTE: The FlexMaster server URL must be assigned on each Ruckus Wireless device you want to register with FlexMaster.

NOTE: Make sure that the required communication ports are open between the APs and FlexMaster as described in Firewall Ports that Must be Open for Communications.

Figure 28. ZF2942 Administrator > Management page with pre-5.0 code



Administrator :: Management

Network Profile: 4bss
Telnet access? ○ Enabled ● Disabled
Telnet Port: 23

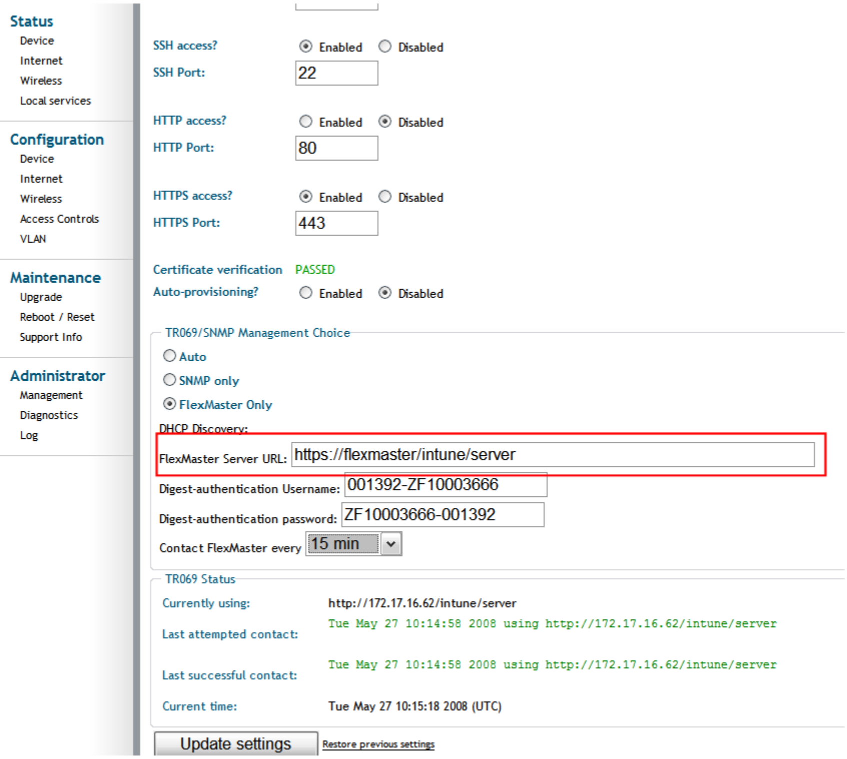
SSH access? ● Enabled ○ Disabled
SSH Port: 22

HTTP access? ○ Enabled ● Disabled
HTTP Port: 80

HTTPS access? ● Enabled ○ Disabled
HTTPS Port: 443

Auto-provisioning? ○ Enabled ● Disabled
Certificate verification PASSED

Figure 29. ZF2942 Administration > Management page after upgrading to 6.0



SSH access? ● Enabled ○ Disabled
SSH Port: 22

HTTP access? ○ Enabled ● Disabled
HTTP Port: 80

HTTPS access? ● Enabled ○ Disabled
HTTPS Port: 443

Certificate verification PASSED
Auto-provisioning? ○ Enabled ● Disabled

TR069/SNMP Management Choice
○ Auto
○ SNMP only
● FlexMaster Only
DHCP Discovery:
FlexMaster Server URL: https://flexmaster/intune/server
Digest-authentication Username: 001392-ZF10003666
Digest-authentication password: ZF10003666-001392
Contact FlexMaster every 15 min

TR069 Status
Currently using: http://172.17.16.62/intune/server
Last attempted contact: `Tue May 27 10:14:58 2008 using http://172.17.16.62/intune/server`
Last successful contact: `Tue May 27 10:14:58 2008 using http://172.17.16.62/intune/server`
Current time: Tue May 27 10:15:18 2008 (UTC)

When it is necessary to manually configure your Ruckus Wireless AP to communicate with FlexMaster, do the following:

1. Log in to your Ruckus Wireless AP's Web interface.
2. Go to *Administrator > Management*.
3. Under *TR069/SNMP Management Choice*, click the **Auto** option.
4. In *FlexMaster Server URL*, type the FlexMaster server URL. This must be a correctly formed URL that starts with either **`http://`** or **`https://`**.
5. Toggle the *Contact FlexMaster every* drop-down list to select how frequently the device should "call home" to FlexMaster. In FlexMaster, this field is referred to as the *Periodic Inform Interval.*
6. Click **Update Settings** to save your settings. Once the AP registers with FlexMaster, this *Administer > Management* page displays the contact status between the AP and FlexMaster.

After the AP has registered with FlexMaster, you can use the Configure options to change these settings. Refer to Creating an AP Configuration Task.

Pointing A ZoneDirector to FlexMaster

If you want to use FlexMaster to monitor and administer ZoneDirectors, then follow the procedures listed in the *Enabling Management via FlexMaster* section in the ZoneDirector User Guide.

NOTE: Make sure that the required communication ports are open between the ZoneDirector and FlexMaster as described in Firewall Ports that Must be Open for Communications.

Checking Your FlexMaster License

A FlexMaster installation provides 100 license seats by default. This means that your FlexMaster server can support up to 100 APs without requiring additional licenses. When you are also managing ZoneDirector using FlexMaster, note that the number of license seats that ZoneDirector consumes depends on the maximum number of APs that it can support. ZoneDirector 3250 (which supports up to 250 clients), for example, consumes 250 license seats.

NOTE: When the Smart Redundancy™ feature is enabled, the Smart Redundant pair of ZDs consume one extra ZoneDirector license. Refer to ZoneDirector Inventory Pages for more information on the Smart Redundancy feature.

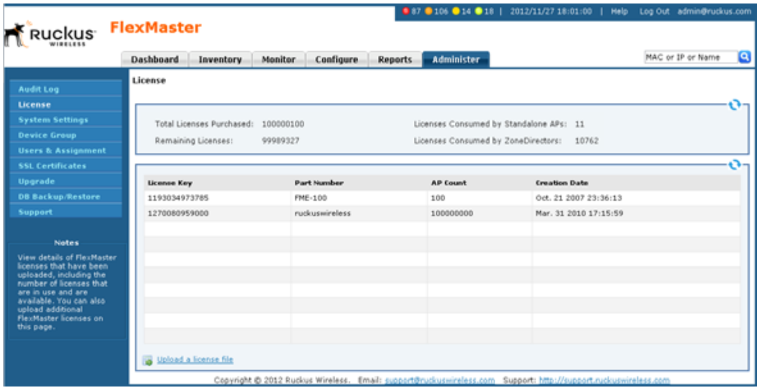
When this seat limit is reached, no additional devices are able to register with FlexMaster until a license file that provides additional license seats is uploaded. FlexMaster shows the following message on the Dashboard to inform you that the seat limit has been reached:

```
License file is not found. Please upload a valid license file
in the Administer > License page.
```

Before using FlexMaster to manage Ruckus Wireless devices, Ruckus Wireless recommends that you check how many ZoneDirector devices and standalone APs can be supported by your current license. You can do this by going to the *Administer > License* page. The total number of devices supported by your license and the seats consumed are shown on the page, as well as the number of license seats consumed by ZoneDirector devices and standalone APs.

If the number of devices that you plan to manage exceeds the number of devices supported by the license file, then you need to contact Ruckus Wireless Support, obtain a license file for additional devices, and upload it to FlexMaster.

Figure 30. The Administer > License page



License

Total Licenses Purchased: 100000100
Remaining Licenses: 99989327
Licenses Consumed by Standalone APs: 11
Licenses Consumed by ZoneDirectors: 10762

License Key	Part Number	AP Count	Creation Date
1193034973785	FME-100	100	Oct. 21 2007 23:36:13
1270080959000	ruckuswireless	100000000	Mar. 31 2010 17:15:59

Notes

View details of FlexMaster licenses that have been uploaded, including the number of licenses that are in use and are available. You can also upload additional FlexMaster licenses on this page.

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Configuring Your Devices to Work with TACACS+

TACACS+ (Terminal Access Controller Access-Control System Plus) is an access control network protocol that provides separate authentication, authorization and accounting services. If your Ruckus Wireless devices are going to use TACACS+, then you must configure the devices to communicate with the TACACS+ server.

To do this, you create a configuration template specifying your TACACS+ settings, and then create a configuration task to push the update with the TACACS+ settings to your managed devices. When the devices next call home, they receive this update and work with the TACACS+ server.

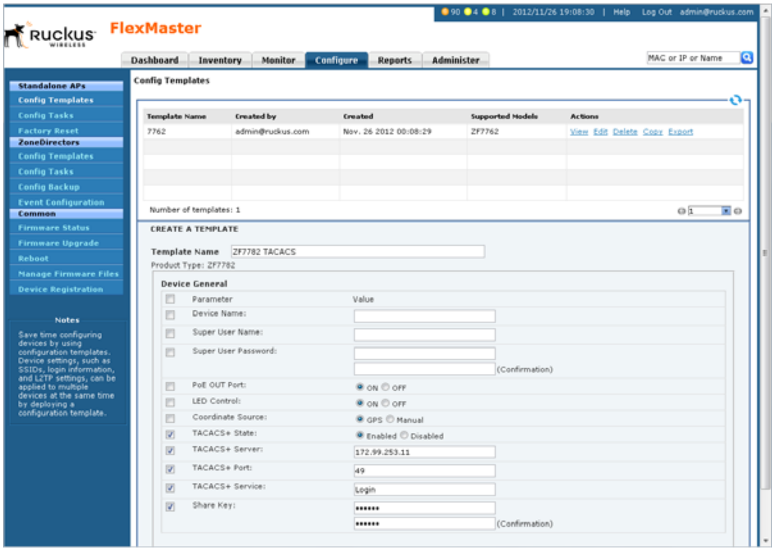
NOTE: If the Ruckus Wireless ZD is behind a firewall/NAT device, then port 49 (TACACS+ port) may need to be forwarded through the firewall/NAT device for FM to communicate with the ZD and AP devices. For more information, refer to Firewall Ports that Must be Open for Communications.

This procedure allows you to configure an AP to communicate with the TACACS+ server. Configuring other Ruckus Wireless devices to communicate with the TACACS+ server is similar.

Creating the TACACS+ Configuration Template

1. Go to *Configure > Standalone APs > Config Templates.*
2. Click **Create a template**. The *Create a Template* configuration form opens at the bottom of the page.
3. In *Template Name*, type a name for this TACACS+-specific template. For example, when you are creating a TACACS+ configuration template for ZoneFlex 7782, you can type **`ZF7782 TACACS+`**.
4. In *Select Product Type*, select the product model for which you are creating a TACACS+ configuration template (**`Ruckus ZF7782 Device`**).
5. Under *Select the configuration options that you want to modify,* select the **Device General** check box.
6. Click **Next**. The *Device General* page appears.
7. Click the **Enabled** *TACACS+ State* button. FlexMaster displays the remaining TACACS+ parameters.
8. Enter the TACACS+ parameters:
   - *TACACS+ Server* - IPv4 or IPv6 server address.
   - *TACACS+ Port* - 49 is the default, but it can be set to any available TCP port.
   - *TACACS+ Service* - Login.
   - *Share Key* - TACACS+ Password.

Figure 31. Required TACACS+ settings



Config Templates

Template Name	Created by	Created	Supported Models	Actions
7762	admin@ruckus.com	Nov. 26 2012 00:08:29	ZF7762	View Edit Delete Copy Export

Number of templates: 1

CREATE A TEMPLATE

Template Name: ZF7782 TACACS
Product Type: ZF7782

Device General

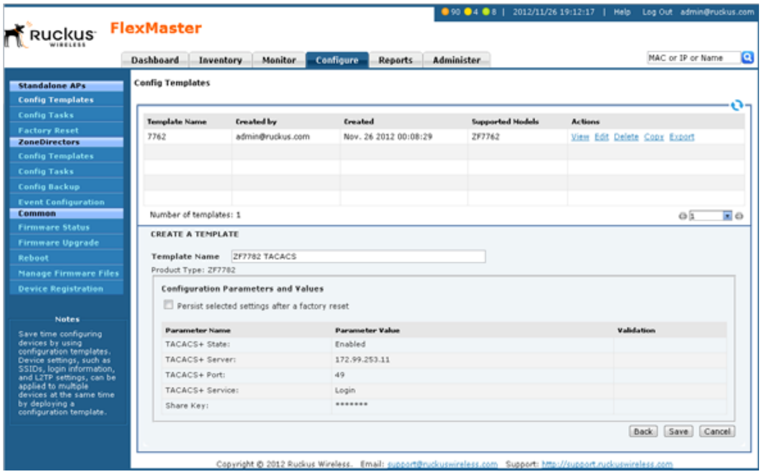
☐	Parameter	Value
☐	Device Name:	
☐	Super User Name:	
☐	Super User Password:	 (Confirmation)
☐	PoE OUT Port:	● ON ○ OFF
☐	LED Control:	● ON ○ OFF
☐	Coordinate Source:	● GPS ○ Manual
☑	TACACS+ State:	● Enabled ○ Disabled
☑	TACACS+ Server:	172.99.253.11
☑	TACACS+ Port:	49
☑	TACACS+ Service:	Login
☑	Share Key:	•••••• •••••• (Confirmation)

9. Click **Next**.

10. When you reach the *Configuration Parameters and Values* page, a summary of the TACACS+ settings are displayed.

    Also on this summary page is the *Persist selected settings after a factory reset* check box. If this check box is selected when the template is provisioned to a group of devices via a configuration task, then the devices retain these template settings even after a factory reset. If this box is left unchecked, then the parameters provisioned in this template revert to factory defaults after a factory reset.

Figure 32. Verify that the TACACS+ settings are correct


● 90 ● 4 ● 8 | 2012/11/26 19:12:17 | Help Log Out admin@ruckus.com
FlexMaster
Dashboard
Inventory
Monitor
Configure
Reports
Administer
MAC or IP or Name
Standalone APs
Config Templates
Config Tasks
Factory Reset
ZoneDirectors
Config Templates
Config Tasks
Config Backup
Event Configuration
Common
Firmware Status
Firmware Upgrade
Reboot
Manage Firmware Files
Device Registration
Notes
Save time configuring devices by using configuration templates. Device settings, such as SSIDs, login information, and L2TP settings, can be applied to multiple devices at the same time by deploying a configuration template.
Back
Save
Cancel
Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Config Templates

Template Name	Created by	Created	Supported Models	Actions
7762	admin@ruckus.com	Nov. 26 2012 00:08:29	ZF7762	View Edit Delete Copy Export

Number of templates: 1

CREATE A TEMPLATE

Template Name: ZF7782 TACACS
Product Type: ZF7782

Configuration Parameters and Values

☐ Persist selected settings after a factory reset

Parameter Name	Parameter Value	Validation
TACACS+ State:	Enabled	
TACACS+ Server:	172.99.253.11	
TACACS+ Port:	49	
TACACS+ Service:	Login	
Share Key:	*******	

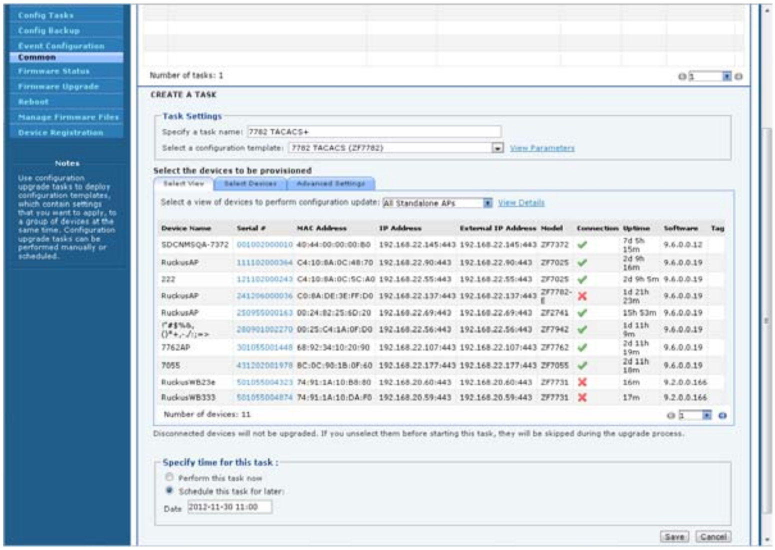
11. On the *Configuration Parameters and Values* page, click **Save** to save the template. FlexMaster returns you to the *Configure > Config Templates* page.

Continue with Creating the TACACS+ Configuration Task.

Creating the TACACS+ Configuration Task

1. Go to *Configure > Config Tasks.*
2. Click **Create a task**. The *CREATE A TASK* form appears at the bottom of the page.

Figure 33. Creating the TACACS+ configuration task



Notes

Use configuration upgrade tasks to deploy configuration templates, which contain settings that you want to apply, to a group of devices at the same time. Configuration upgrade tasks can be performed manually or scheduled.

Number of tasks: 1

CREATE A TASK

Task Settings

Specify a task name: 7782 TACACS+

Select a configuration template: 7782 TACACS (ZF7782) View Parameters

Select the devices to be provisioned

Select a view of devices to perform configuration update: All Standalone APs View Details

Device Name	Serial #	MAC Address	IP Address	External IP Address	Model	Connection	Uptime	Software	Tag
SDCNMSQA-7372	001002000010	40:44:00:00:00:B0	192.168.22.145:443	192.168.22.145:443	ZF7372	✓	7d 5h 15m	9.6.0.0.12	
RuckusAP	111102000364	C4:10:8A:0C:48:70	192.168.22.90:443	192.168.22.90:443	ZF7025	✓	2d 9h 16m	9.6.0.0.19	
222	121102000243	C4:10:8A:0C:5C:A0	192.168.22.55:443	192.168.22.55:443	ZF7025	✓	2d 9h 5m	9.6.0.0.19	
RuckusAP	241206000036	C0:8A:DE:3E:FF:D0	192.168.22.137:443	192.168.22.137:443	ZF7782-E	✗	1d 21h 23m	9.6.0.0.19	
RuckusAP	250955000163	00:24:82:25:6D:20	192.168.22.69:443	192.168.22.69:443	ZF2741	✓	15h 53m	9.6.0.0.19	
"#$%&, ()*+,-./:;=>	280901002270	00:25:C4:1A:0F:D0	192.168.22.56:443	192.168.22.56:443	ZF7942	✓	1d 11h 9m	9.6.0.0.19	
7762AP	301055001448	68:92:34:10:20:90	192.168.22.107:443	192.168.22.107:443	ZF7762	✓	2d 11h 19m	9.6.0.0.19	
7055	431202001978	8C:0C:90:1B:0F:60	192.168.22.177:443	192.168.22.177:443	ZF7055	✓	2d 11h 18m	9.6.0.0.19	
RuckusWB23e	501055004323	74:91:1A:10:B8:80	192.168.20.60:443	192.168.20.60:443	ZF7731	✗	16m	9.2.0.0.166	
RuckusWB333	501055004874	74:91:1A:10:DA:F0	192.168.20.59:443	192.168.20.59:443	ZF7731	✗	17m	9.2.0.0.166	

Number of devices: 11

Disconnected devices will not be upgraded. If you unselect them before starting this task, they will be skipped during the upgrade process.

Specify time for this task :

○ Perform this task now

● Schedule this task for later:

Date 2012-11-30 11:00

3. In *Specify a task name*, type a name for this TACACS+ configuration task. For example, when this TACACS+ configuration task is for ZoneFlex 7782 APs, you can type **`7782 TACACS+`**.
4. Select the previously-configured TACACS+ configuration template from the *Select a configuration template* drop-down list.
5. (Optional) Under the *Select View* tab, toggle the *Select a view of devices to perform configuration update* drop-down list to filter the list of devices based on a device view. For example, when the configuration template is for ZoneFlex 7782, select the device view that contains ZF7782 models.
6. Under *Specify time for the task*, click when you want to perform this task:
   - Perform this task now
   - Schedule this task for later: Specify the desired Date and Time
7. Click **Save**.

Configuring Your Devices to Communicate with FlexMaster over L2TP

If your network prevents FlexMaster from initiating communication across the Internet to managed devices, then you can use your L2TP Network Server (LNS) to tunnel through to managed devices. For example, if a device behind a NAT server or firewall is not reachable by FlexMaster, then you can use L2TP to solve this problem.

To do this, you create a configuration template specifying your L2TP settings, and then create a configuration task to push the update with the L2TP settings to your managed devices. When the devices next call home, they receive this update and register with the LNS. This allows FlexMaster to initiate future connections.

NOTE: If the Ruckus Wireless ZD is behind a firewall/NAT device, then port 49 (TACACS+ port) may need to be forwarded through the firewall/NAT device for FM to communicate with the ZD and AP devices. For more information, refer to Firewall Ports that Must be Open for Communications.

Creating the L2TP Configuration Template

1. Go to *Configure > Standalone APs > Config Templates.*
2. Click **Create a template**. The *CREATE A TEMPLATE* configuration form opens at the bottom of the page.
3. In *Template Name,* type a name for this L2TP-specific template. For example, when you are creating an L2TP configuration template for ZoneFlex 7782, you can type **`L2TP for 7782`**.
4. In *Select product type,* select the product model for which you are creating an L2TP configuration template.
5. Under *Select the configuration options you would like to modify,* select the **Internet** and **VLAN & LAN Port Setting** check boxes.

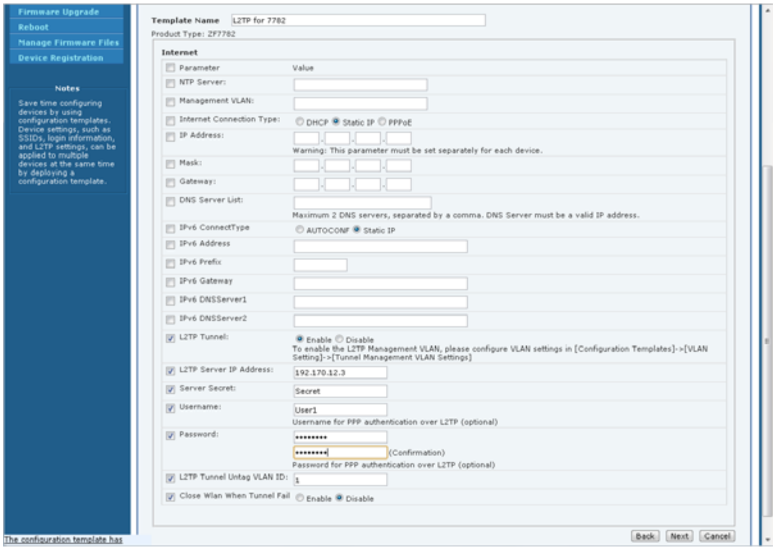
NOTE: You must select both the *Internet* and *VLAN & LAN Port Setting* check boxes to create an L2TP configuration template successfully. If you only select the *Internet* check box, then you are able to create the configuration template, but it is not applied.

6. Click **Next**. The *Internet* settings page appears.
7. In the *L2TP Tunnel* parameter, click the **Enable** option. After you enable L2TP, additional L2TP configuration parameters appear.

   The following L2TP values are required:
   - L2TP Server IP Address
   - Server Secret
   - L2TP Username

- L2TP Password (appropriate to the User Name account)
- L2TP Tunnel Untag VLAN ID
- Close WLAN When Tunnel Fail (options include **Enable** and **Disable**)

Figure 34. Required L2TP settings



Notes

Save time configuring devices by using configuration templates. Device settings, such as SSIDs, login information, and L2TP settings, can be applied to multiple devices at the same time by deploying a configuration template.

The configuration template has

Template Name L2TP for 7782
Product Type: ZF7782

Internet

□ Parameter	Value
□ NTP Server:	
□ Management VLAN:	
□ Internet Connection Type:	○ DHCP ● Static IP ○ PPPoE
□ IP Address:	. . . Warning: This parameter must be set separately for each device.
□ Mask:	. . .
□ Gateway:	. . .
□ DNS Server List:	 Maximum 2 DNS servers, separated by a comma. DNS Server must be a valid IP address.
□ IPv6 ConnectType	○ AUTOCONF ● Static IP
□ IPv6 Address	
□ IPv6 Prefix	
□ IPv6 Gateway	
□ IPv6 DNSServer1	
□ IPv6 DNSServer2	
☑ L2TP Tunnel:	● Enable ○ Disable To enable the L2TP Management VLAN, please configure VLAN settings in [Configuration Templates]->[VLAN Setting]->[Tunnel Management VLAN Settings]
☑ L2TP Server IP Address:	192.170.12.3
☑ Server Secret:	Secret
☑ Username:	User1 Username for PPP authentication over L2TP (optional)
☑ Password:	•••••••• •••••••• (Confirmation) Password for PPP authentication over L2TP (optional)
☑ L2TP Tunnel Untag VLAN ID:	1
☑ Close Wlan When Tunnel Fail	○ Enable ● Disable

8. Click **Next**.

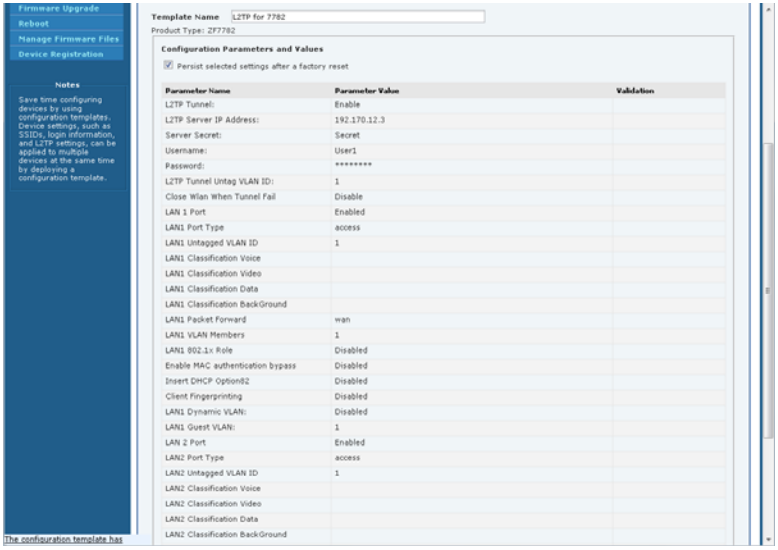
9. On the *VLAN & LAN Port Setting* page, select and configure the parameters according to your required settings. When you do not use VLANs, you do not need to configure these settings.

10. Click **Next**.

11. When you reach the *Configuration Parameters and Values* page, a summary of the L2TP settings are displayed.

Also on this summary page is the *Persist selected settings after a factory reset check* box. If this check box is selected when the template is provisioned to a group of devices via a configuration task, then the devices retain these template settings even after a factory reset. If this box is left unchecked, then the parameters provisioned in this template revert to factory defaults after a factory reset.

Figure 35. Verify that the L2TP settings are correct


Firmware Upgrade
Reboot
Manage Firmware Files
Device Registration
Notes
Save time configuring devices by using configuration templates. Device settings, such as SSIDs, login information, and L2TP settings, can be applied to multiple devices at the same time by deploying a configuration template.
The configuration template has

Template Name: L2TP for 7782

Product Type: ZF7782

Configuration Parameters and Values

☑ Persist selected settings after a factory reset

Parameter Name	Parameter Value	Validation
L2TP Tunnel:	Enable	
L2TP Server IP Address:	192.170.12.3	
Server Secret:	Secret	
Username:	User1	
Password:	********	
L2TP Tunnel Untag VLAN ID:	1	
Close Wlan When Tunnel Fail	Disable	
LAN 1 Port	Enabled	
LAN1 Port Type	access	
LAN1 Untagged VLAN ID	1	
LAN1 Classification Voice		
LAN1 Classification Video		
LAN1 Classification Data		
LAN1 Classification BackGround		
LAN1 Packet Forward	wan	
LAN1 VLAN Members	1	
LAN1 802.1x Role	Disabled	
Enable MAC authentication bypass	Disabled	
Insert DHCP Option82	Disabled	
Client Fingerprinting	Disabled	
LAN1 Dynamic VLAN:	Disabled	
LAN1 Guest VLAN:	1	
LAN 2 Port	Enabled	
LAN2 Port Type	access	
LAN2 Untagged VLAN ID	1	
LAN2 Classification Voice		
LAN2 Classification Video		
LAN2 Classification Data		
LAN2 Classification BackGround		

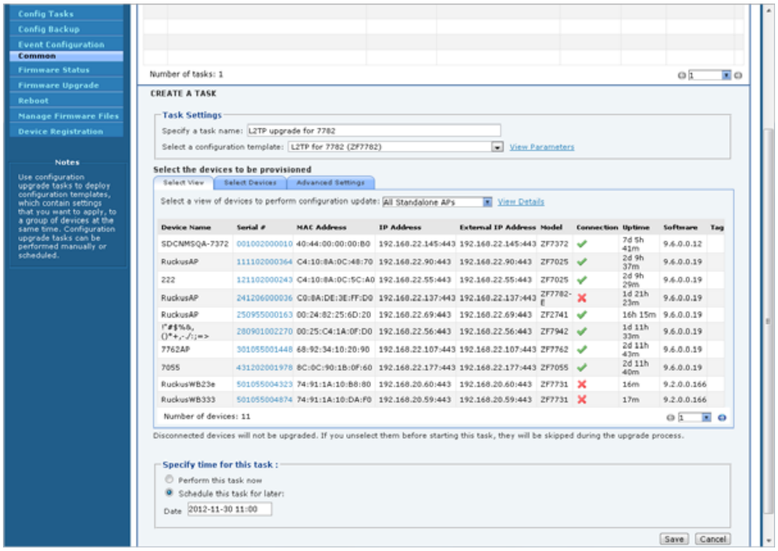
12. On the *Configuration Parameters and Values* page, click **Save** to save the template.

Continue with Creating the L2TP Configuration Task.

Creating the L2TP Configuration Task

1. Go to *Configure > Config Tasks.*
2. Click **Create a task**. The *CREATE A TASK* form appears at the bottom of the page.
3. In *Specify a task name*, type a name for this L2TP configuration task. For example, when this L2TP configuration task is for ZoneFlex 7782 APs, you can type **`L2TP Upgrade for 7782`**.
4. Toggle the *Select a configuration template* drop-down list to select the previously configured L2TP configuration template.
5. (Optional) Under the *Select View* tab, toggle the *Select a view of devices to perform configuration update* drop-down list to filter the list of devices based on a device view. For example, when the configuration template is for ZoneFlex 7782, select the device view that contains ZF7782 models.
6. Under *Specify time for the task*, click when you want to perform this task:
   - Perform this task now
   - Schedule this task for later: Specify the desired Date and Time
7. Click **Save**.

Figure 36. Creating the L2TP configuration task



Notes

Use configuration upgrade tasks to deploy configuration templates, which contain settings that you want to apply, to a group of devices at the same time. Configuration upgrade tasks can be performed manually or scheduled.

Number of tasks: 1

CREATE A TASK

Task Settings

Specify a task name: L2TP upgrade for 7782

Select a configuration template: L2TP for 7782 (ZF7782) View Parameters

Select the devices to be provisioned

Select a view of devices to perform configuration update: All Standalone APs View Details

Device Name	Serial #	MAC Address	IP Address	External IP Address	Model	Connection	Uptime	Software	Tag
SDCNMSQA-7372	001002000010	40:44:00:00:00:B0	192.168.22.145:443	192.168.22.145:443	ZF7372	✓	7d 5h 41m	9.6.0.0.12	
RuckusAP	111102000364	C4:10:8A:0C:48:70	192.168.22.90:443	192.168.22.90:443	ZF7025	✓	2d 9h 37m	9.6.0.0.19	
222	121102000243	C4:10:8A:0C:5C:A0	192.168.22.55:443	192.168.22.55:443	ZF7025	✓	2d 9h 29m	9.6.0.0.19	
RuckusAP	241206000036	C0:8A:DE:3E:FF:D0	192.168.22.137:443	192.168.22.137:443	ZF7782-E	✗	1d 21h 23m	9.6.0.0.19	
RuckusAP	250955000163	00:24:82:25:6D:20	192.168.22.69:443	192.168.22.69:443	ZF2741	✓	16h 15m	9.6.0.0.19	
!"#$%&,()*+,-./:;=>	280901002270	00:25:C4:1A:0F:D0	192.168.22.56:443	192.168.22.56:443	ZF7942	✓	1d 11h 33m	9.6.0.0.19	
7762AP	301055001448	68:92:34:10:20:90	192.168.22.107:443	192.168.22.107:443	ZF7762	✓	2d 11h 43m	9.6.0.0.19	
7055	431202001978	8C:0C:90:1B:0F:60	192.168.22.177:443	192.168.22.177:443	ZF7055	✓	2d 11h 40m	9.6.0.0.19	
RuckusWB23e	501055004323	74:91:1A:10:B8:80	192.168.20.60:443	192.168.20.60:443	ZF7731	✗	16m	9.2.0.0.166	
RuckusWB333	501055004874	74:91:1A:10:DA:F0	192.168.20.59:443	192.168.20.59:443	ZF7731	✗	17m	9.2.0.0.166	

Number of devices: 11

Disconnected devices will not be upgraded. If you unselect them before starting this task, they will be skipped during the upgrade process.

Specify time for this task :

○ Perform this task now

● Schedule this task for later:

Date 2012-11-30 11:00

4

Working with Device Inventory

In This Chapter:

About the Inventory Page

The *Inventory* page of the FlexMaster Web interface displays information about devices that FlexMaster is directly and indirectly managing. These devices include:

- ZoneDirectors (reporting to FlexMaster)
- Standalone APs (reporting directly to FlexMaster)
- Clients (reporting to Standalone APs)

This chapter provides information on how to use the options on the *Inventory* tab to view and search for managed devices and to create views.

ZoneDirector Inventory Pages

The following two tables list the fields and table columns that appear by default in the *ZoneDirectors* section of the *Inventory* page.

Table 12. Information that appears in the ZoneDirectors section of the Inventory page

Field/Column	Description
ZD Search Criteria section	Use these filters to search for specific ZoneDirector devices. You can save the search results as a new ZoneDirector view. Refer to Searching for ZoneDirector Devices.
Text View/Map View	By default, the page displays a **Text View** of devices (in a tabular form). When you want to display the geographical location of devices in the current view (whose GPS coordinates have been configured), click **Map View**. Refer to Text View and Map View.
List of ZDs	By default, this table lists all managed ZoneDirector devices. When you search for devices using the *ZD Search Criteria* section, the devices that match the search criteria appear in this table. For information on the columns that appear in this table, refer to the following table.
Export As XLS File or CSV File	When you want to save the devices that currently appear in the table to an XLS file, click **XLS File**. To save them to a CSV file, click **CSV File**.
Search box	Type a word or phrase that you want to search for, and then wait for a second or two. FlexMaster refreshes the page and displays devices with attributes that matched your search keyword or keyphrase. The matching attributes are highlighted in yellow. FlexMaster displays up to ten search results on each page. When your search generates more than ten results, use the left arrow and right arrow icons after the search box to display the previous page or next page, respectively.
Save As View	Use this section to save the search results as a device view. Refer to Search Using the ZD Search Criteria.

The following table describes the columns that appear in the *List of ZDs* table.

NOTE: By default, ZoneDirector only displays a few of the available columns on the ZoneDirector *Inventory* page. When you want to display additional columns, refer to Displaying and Hiding Columns on the ZoneDirector Inventory Page for information.

Table 13. Columns that appear in the List of ZDs table

Column	Description
ZD Name	Name assigned to the device.
Serial Number	Serial number of the device. Clicking this link opens a new browser window specific to the device. This is the device view as if you logged into the device's Web interface. **NOTE:** *Use the opened ZoneDirector web interface to configure features such as Hotspot 2.0.* Refer to the *Ruckus Wireless ZoneDirector User Guide* to create a Hotspot 2.0 service on a ZoneDirector.
MAC Address	MAC address of the device.
IP Address	IP address assigned to the device. **NOTE:** *The port number after the IP address indicates the protocol that you can use to gain access to the device's Web interface.* • If :443 appears after the port number, you can access the device's Web interface using `https://{device-IP-address}`. • If :80 appears after the IP address, you can access the device's Web interface using `http://{device-IP-address}`. When both HTTPS and HTTP management options are enabled, only :443 appears after the IP address.
External IP	When the device is behind a NAT server, this is the IP address and port number that FlexMaster uses to communicate with the device. **NOTES:** • *When the device is not behind a NAT server, the values for IP Address (above) and External IP Address are the same.* • *When the device is behind a NAT server, make sure that you configure port forwarding for the device on the NAT server. Then, click the* **Edit** *link on this page that is in the same row as the device name, and then enter the port number that you assigned to the device on the NAT server.*
Model	Model of the managed Ruckus Wireless device.
Location	Location of the device (if provided).

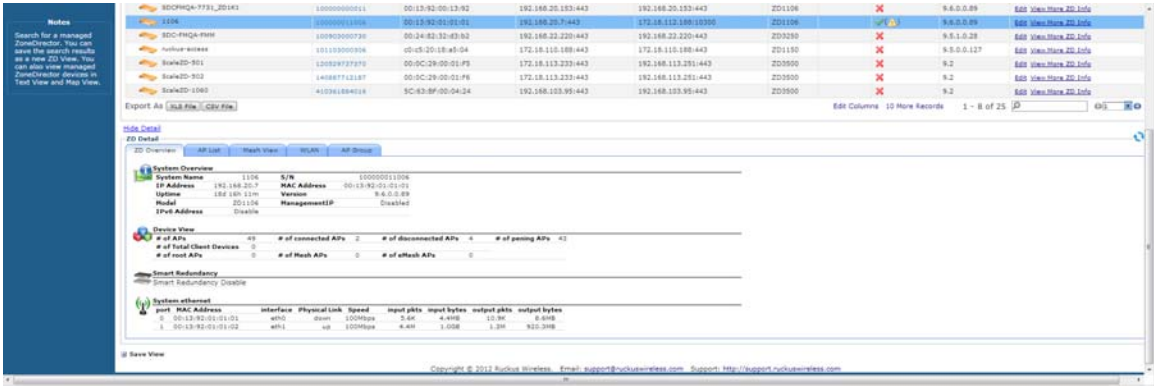
Table 13. Columns that appear in the List of ZDs table (Continued)

Column	Description
Connection	Indicates whether the device is currently online (✅) or offline (❌).
Software	Shows the software version that is installed on the device.
Actions	• **Edit**: Allows you change the *Device Tag* name, as well as its *Location* and *GPS coordinates.* • **View More ZD Info**: Clicking this link displays the *ZD Detail* table below the *List of ZDs* table. Refer to Viewing the ZD Detail Section.

Viewing the ZD Detail Section

The *ZD Detail* section displays additional information about the selected ZoneDirector device. This section is hidden by default. To display the *ZD Detail* section, in the *List of ZDs* table, click the desired **View More ZD Info** link.

Figure 37. The ZD Detail section



Notes

Search for a managed ZoneDirector. You can save the search results as a new ZD View. You can also view managed ZoneDirector devices in Text View and Map View.

SDCFMQA-7731_ZD1K1	100000000011	00:13:92:00:13:92	192.168.20.153:443	192.168.20.153:443	ZD1106	✗	9.6.0.0.89	Edit View More ZD Info
1106	100000011006	00:13:92:01:01:01	192.168.20.7:443	172.18.112.188:10300	ZD1106	✓ ⚠	9.6.0.0.89	Edit View More ZD Info
SDC-FMQA-FMM	100903000730	00:24:82:32:d3:b2	192.168.22.220:443	192.168.22.220:443	ZD3250	✗	9.5.1.0.28	Edit View More ZD Info
ruckus-access	101103000306	c0:c5:20:18:a5:04	172.18.110.188:443	172.18.110.188:443	ZD1150	✗	9.5.0.0.127	Edit View More ZD Info
ScaleZD-501	120329737370	00:0C:29:00:01:F5	172.18.113.233:443	192.168.113.251:443	ZD3500	✗	9.2	Edit View More ZD Info
ScaleZD-502	140887712187	00:0C:29:00:01:F6	172.18.113.233:443	192.168.113.251:443	ZD3500	✗	9.2	Edit View More ZD Info
ScaleZD-1060	410361884018	5C:63:BF:00:04:24	192.168.103.95:443	192.168.103.95:443	ZD3500	✗	9.2	Edit View More ZD Info

Export As XLS File CSV File   Edit Columns 10 More Records 1 - 8 of 25

Hide Detail

ZD Detail

ZD Overview | AP List | Mesh View | WLAN | AP Group

System Overview

System Name	1106	**S/N**	100000011006
IP Address	192.168.20.7	**MAC Address**	00:13:92:01:01:01
Uptime	18d 16h 11m	**Version**	9.6.0.0.89
Model	ZD1106	**ManagementIP**	Disabled
IPv6 Address	Disable		

Device View

# of APs	49	**# of connected APs**	2	**# of disconnected APs**	4	**# of pening APs**	43
# of Total Client Devices	0						
# of root APs	0	**# of Mesh APs**	0	**# of eMesh APs**	0		

Smart Redundancy

Smart Redundancy Disable

System ethernet

port	MAC Address	interface	Physical Link	Speed	input pkts	input bytes	output pkts	output bytes
0	00:13:92:01:01:01	eth0	down	100Mbps	5.6K	4.4MB	10.9K	8.6MB
1	00:13:92:01:01:02	eth1	up	100Mbps	4.4M	1.0GB	1.2M	920.3MB

☑ Save View

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

The *ZD Detail* section displays five tabs described in the following table.

Table 14. Information that appears in the ZD Detail table

Tab	Description
ZD Overview	Displays summary information about the ZoneDirector device, including its system overview, devices summary (AP and client information), Smart Redundancy status, and system ethernet statistics.
AP List	Displays a table that lists the APs reporting to the ZoneDirector device.
Mesh View	Displays a table that lists the mesh details of the ZoneDirector device.
WLAN	Displays a table that lists the WLANs configured on the ZoneDirector device, including the WLAN names, ESSIDs, authentication and encryption methods, and the number of clients associated with each WLAN.
AP Group	Displays a tree of AP groups that have been created on the ZoneDirector device. By default, an AP group named *System Default* exists. When there are additional AP groups, they also appear in this tree. AP group details include the device MAC address, name of each member device, description, model number, and connection status.

Displaying and Hiding Columns on the ZoneDirector Inventory Page

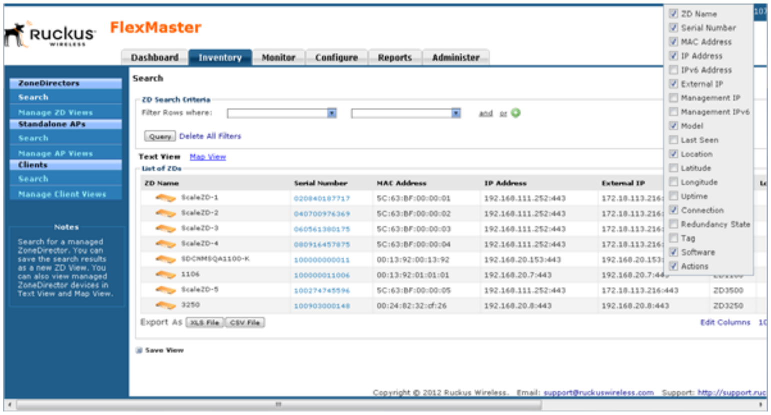
By default, FlexMaster displays only a few of the available columns on the ZoneDirector *Inventory* page. When you want to display additional columns, do the following:

1. Click the **Edit Columns** link at the bottom of the table. A box appears and displays check boxes for the table columns. The checked boxes indicate the columns that are currently visible in the table.
2. To display a hidden column, select the check box for the column. For example, when your network supports IPv6 and you want to display ZoneDirector's IPv6 settings, select the check box for **IPv6 Address** and **Management IPv6**.

   To hide a visible column, clear or uncheck the check box.
3. When you are done, click anywhere outside of the box.

You have completed displaying columns on the ZoneDirector *Inventory* page.

Figure 38. Click the Edit Columns link to select which columns to hide or display



Notes

Search for a managed ZoneDirector. You can save the search results as a new ZD View. You can also view managed ZoneDirector devices in Text View and Map View.

Search

ZD Search Criteria

Filter Rows where: and or

List of ZDs

ZD Name	Serial Number	MAC Address	IP Address	External IP	
ScaleZD-1	020840187717	5C:63:BF:00:00:01	192.168.111.252:443	172.18.113.216:	
ScaleZD-2	040700976369	5C:63:BF:00:00:02	192.168.111.252:443	172.18.113.216:	
ScaleZD-3	060561380175	5C:63:BF:00:00:03	192.168.111.252:443	172.18.113.216:	
ScaleZD-4	080916457875	5C:63:BF:00:00:04	192.168.111.252:443	172.18.113.216:	
SDCNMSQA1100-K	100000000011	00:13:92:00:13:92	192.168.20.153:443	192.168.20.153:	
1106	100000011006	00:13:92:01:01:01	192.168.20.7:443	192.168.20.7:44	
ScaleZD-5	100274745596	5C:63:BF:00:00:05	192.168.111.252:443	172.18.113.216:443	ZD3500
3250	100903000148	00:24:82:32:cf:26	192.168.20.8:443	192.168.20.8:443	ZD3250

- ☑ ZD Name
- ☑ Serial Number
- ☑ MAC Address
- ☑ IP Address
- ☐ IPv6 Address
- ☑ External IP
- ☐ Management IP
- ☐ Management IPv6
- ☑ Model
- ☐ Last Seen
- ☑ Location
- ☐ Latitude
- ☐ Longitude
- ☐ Uptime
- ☑ Connection
- ☐ Redundancy State
- ☐ Tag
- ☑ Software
- ☑ Actions

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruc

Standalone APs Inventory Pages

The following two tables list the fields and table columns that appear in the *Standalone APs* section of the *Inventory* tab.

Table 15. Information that appears in the Standalone APs section of the Inventory page

Field/Column	**Description**
AP Search Criteria	Use these filters to search for specific standalone APs. You can save the search results as a new AP view. Refer to Searching for Standalone APs.
Text View/Map View	By default, the page displays a **Text View** of devices (in a tabular form). When you want to display the geographical location of devices in the current view (whose GPS coordinates have been configured), click **Map View**. Refer to Text View and Map View.
List of APs	By default, this table lists all standalone APs. When you search for devices using the *AP Search Criteria* section, the devices that match the search criteria appear in this table. For information on the columns that appear in this table, refer to the following table.
Export as XLS File or CSV File	When you want to save the devices that currently appear in the table to an XLS file, click **XLS File**. To save them to a CSV file, click **CSV File**.
Search box	Type a word or phrase that you want to search for, and then wait for a second or two. FlexMaster refreshes the page and displays devices with attributes that matched your search keyword or keyphrase. The matching attributes are highlighted in yellow. FlexMaster displays up to ten search results on each page. When your search generates more than ten results, use the left arrow and right arrow icons after the search box to display the previous page or next page, respectively.
Save As View	Use this section to save the search results as a device view. Refer to Search Using the AP Search Criteria.

Table 16. Columns that appear in the List of APs table

Column	Description
AP Name	Name assigned to the device.
Serial Number	Serial number of the device. Clicking this link opens a new browser window specific to the device. This is the device view as if you logged into the device's Web interface.
MAC Address	AP network interface Media Access Control address.
IP Address	IP address assigned to the device **NOTE:** *The port number after the IP address indicates the protocol that you can use to gain access to the device's Web interface.* • When :443 appears after the port number, you can access the device's Web interface using `https://{device-IP-address}`. • When :80 appears after the IP address, you can access the device's Web interface using `http://{device-IP-address}`. When both HTTPS and HTTP management options are enabled, only :443 appears after the IP address.
IPv6 Address	If the network supports IPv6, then this is the IPv6 address that is assigned to the AP.
External IP	When the device is behind a NAT server, this is the IP address and port number that FlexMaster uses to communicate with the device. **NOTES:** • *When the device is not behind a NAT server, the values for IP Address (above) and External IP Address are the same.* • *When the device is behind a NAT server, make sure that you configure port forwarding for the device on the NAT server. Then, click the* **Edit** *link on this page that is in the same row as the device name, and then enter the port number that you assigned to the device on the NAT server.*
Model	Model of the managed Ruckus Wireless device.
Last Seen	Date and time when FlexMaster last communicated with the device.
Location	When configured, this column shows the location name of the device.
Latitude	When configured, this column shows the latitude (North-South position) of the device.
Longitude	When configured, this column shows the latitude (East-West position) of the device.
Uptime	Shows how long since the device was last rebooted.

Table 16. Columns that appear in the List of APs table (Continued)

Column	Description
Connection	Indicates whether the device is currently online (✅) or offline (❎).
Tag	When configured, this column shows a generic attribute (Device Tag) that can be used to identify the device. For example, when this AP device is located in main office, you can assign the tag "Main" to it. To assign a device tag to one device, edit the device details on the *Inventory* page. To assign a device tag to multiple devices using the same Device View, edit the device details on the *Manage ZD Views* page.
Software	Shows the software version that is installed on the device.
Actions	Clicking **Edit** allows you change the tag name assigned to the device, as well as its location, GPS coordinates, and Web port mapping. Clicking **Link** allows you assign a 7731 Bridge to report to a particular ZoneDirector device.

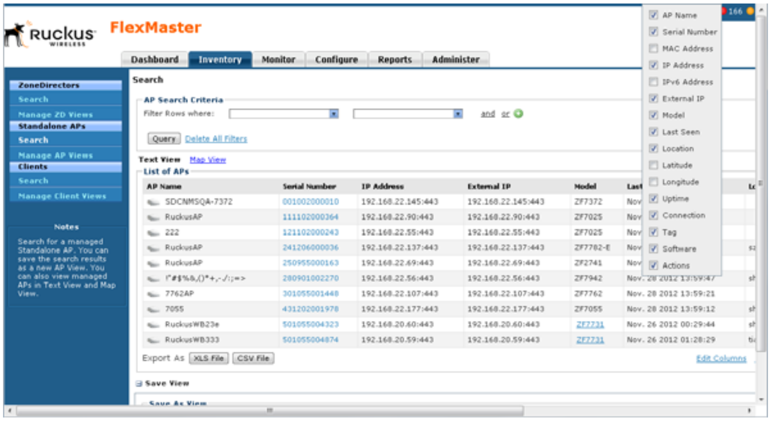
Displaying and Hiding Columns on the Standalone AP Inventory Page

By default, FlexMaster displays only a few of the available columns on the Standalone AP *Inventory* page. When you want to display additional columns, do the following:

1. Click the **Edit Columns** link at the bottom of the table. A box appears and displays check boxes for the table columns. The checked boxes indicate the columns that are currently visible in the table.
2. To display a hidden column, select the check box for the column. For example, if your network supports IPv6 and you want to display the IPv6 address of standalone APs, then select the check box for **IPv6 Address**.
3. When you are done, click anywhere outside of the box to close the box.

You have completed displaying columns on the Standalone AP *Inventory* page. To hide a visible column, clear or uncheck the check box.

Figure 39. Click the Edit Columns link to select which columns to hide or display



Search

AP Search Criteria

Filter Rows where:

Text View Map View

List of APs

AP Name	Serial Number	IP Address	External IP	Model	Last	Lc
SDCNMSQA-7372	001002000010	192.168.22.145:443	192.168.22.145:443	ZF7372	Nov	
RuckusAP	111102000364	192.168.22.90:443	192.168.22.90:443	ZF7025	Nov	
222	121102000243	192.168.22.55:443	192.168.22.55:443	ZF7025	Nov	
RuckusAP	241206000036	192.168.22.137:443	192.168.22.137:443	ZF7782-E	Nov	sz
RuckusAP	250955000163	192.168.22.69:443	192.168.22.69:443	ZF2741	Nov	
!"#$%&,()*+,-./:;=>	280901002270	192.168.22.56:443	192.168.22.56:443	ZF7942	Nov. 28 2012 13:59:47	sh
7762AP	301055001448	192.168.22.107:443	192.168.22.107:443	ZF7762	Nov. 28 2012 13:59:21	
7055	431202001978	192.168.22.177:443	192.168.22.177:443	ZF7055	Nov. 28 2012 13:59:12	sh
RuckusWB23e	501055004323	192.168.20.60:443	192.168.20.60:443	ZF7731	Nov. 26 2012 00:29:44	sh
RuckusWB333	501055004874	192.168.20.59:443	192.168.20.59:443	ZF7731	Nov. 26 2012 01:28:29	ti

Notes

Search for a managed Standalone AP. You can save the search results as a new AP View. You can also view managed APs in Text View and Map View.

☑ AP Name
☑ Serial Number
□ MAC Address
☑ IP Address
□ IPv6 Address
☑ External IP
☑ Model
☑ Last Seen
☑ Location
□ Latitude
□ Longitude
☑ Uptime
☑ Connection
☑ Tag
☑ Software
☑ Actions

Client Inventory Pages

The following two tables list the fields and table columns that appear in the *Clients* section of the *Inventory* tab.

Table 17. Information that appears in the Clients section of the Inventory page

Field/Column	Description
Clients Search Criteria section	Use these filters to search for specific clients. You can save the search results as a new client view. Refer to Searching for Clients.
List of Clients	By default, this table lists all clients. When you search for devices using the *Clients Search Criteria* section, the devices that match the search criteria appear in this table. For information on the columns that appear in this table, refer to the following table.
Export as XLS File or CSV File	When you want to save the devices that currently appear in the table to an XLS file, click **XLS File**. To save them to a CSV file, click **CSV File**.
Search box	Type a word or phrase that you want to search for, and then wait for a second or two. FlexMaster refreshes the page and displays devices with attributes that matched your search keyword or keyphrase. The matching attributes are highlighted in yellow. FlexMaster displays up to ten search results on each page. When your search generates more than ten results, use the left arrow and right arrow icons after the search box to display the previous page or next page, respectively.
Save As View	Use this section to save the search results as a device view. Refer to Search Using the Client Search Criteria.

Table 18. Columns that appear in the List of Clients table

Column	Description
ZD Name	Name of the ZoneDirector device that is managing the AP with which this client is associated.
AP Name	Name of the AP with which this client is associated.
Description	Optional description of the wireless client AP.
Client MAC	MAC address of the wireless client.
Client IP Address	IPv4 address assigned to the client.
Client IPv6 Address	IPv6 address assigned to the client.

Table 18. Columns that appear in the List of Clients table (Continued)

Column	Description
Client Model	Model name of the client.
User Name	User name assigned to the client.
WLAN	WLAN name with which this client is associated.
Device Info	Icon designating the client device operating system.
Host Name	Name of the client host.
Vendor	Client vendor name, if reported.
On Time	When the client first logged on.
Associated Time	Time that the client has been associated.
Channel	Radio channel that the client is using.
Radio Type	Type of radio that the client is using.
Signal	Strength of wireless signal.
Rx	Number of bytes that the client has received.
Tx	Number of bytes that the client has transmitted.
Vlan	Client VLAN, if assigned.
Retries	Number of retries for this client.
Connection	Indicates whether the client is currently online (✅) or offline (❌).
Authentication	Indicates whether the client has been authenticated (✅) or not authenticated (❌).

Displaying and Hiding Columns on the Client Inventory Page

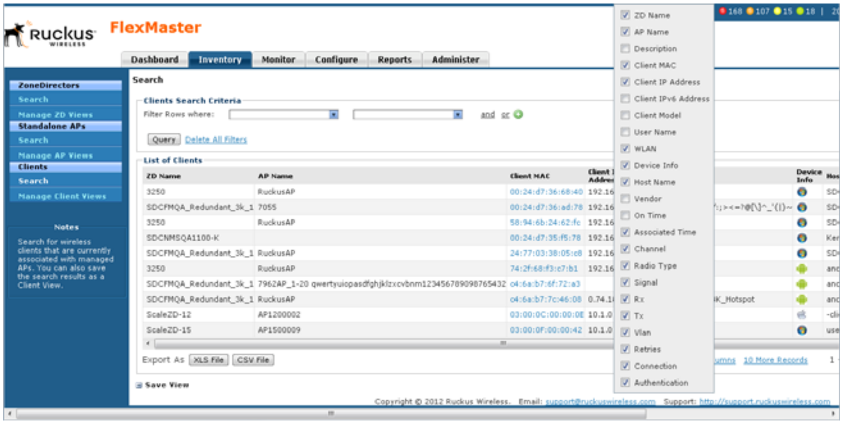
By default, FlexMaster displays all the available columns on the Client *Inventory* page. When you want to hide some of these columns, do the following:

1. Click the **Edit Columns** link at the bottom of the table. A box appears and displays check boxes for the table columns. By default, all check boxes are selected, which means all available columns are visible in the table.
2. To hide a column, clear the check box for that column. For example, if your network does not support IPv6, then you can hide the *User IPv6 Address* column by clearing or unchecking the **User IPv6 Address** check box.
3. When you are done, click anywhere outside of the box to close the box.

You have completed hiding columns from the Client *Inventory* page.

To display a hidden column, click the **Edit Column** link, and then select the check box for the column that you want to display.

Figure 40. To hide a column, clear or uncheck the check box for that column



Notes

Search for wireless clients that are currently associated with managed APs. You can also save the search results as a Client View.

Search

Clients Search Criteria

Filter Rows where: and or

Query Delete All Filters

List of Clients

ZD Name	AP Name	Client MAC	Client I Addre		Hos
3250	RuckusAP	00:24:d7:36:68:40	192.16		SD
SDCFMQA_Redundant_3k_1	7055	00:24:d7:36:ad:78	192.16	'/:;>‹=?@[\]^_'{|}~	SD
3250	RuckusAP	58:94:6b:24:62:fc	192.16		SD
SDCNMSQA1100-K		00:24:d7:35:f5:78	192.16		Ker
SDCFMQA_Redundant_3k_1	RuckusAP	24:77:03:38:05:c8	192.16		SD
3250	RuckusAP	74:2f:68:f3:c7:b1	192.16		and
SDCFMQA_Redundant_3k_1	7962AP_1-20 qwertyuiopasdfghjklzxcvbnm123456789098765432	c4:6a:b7:6f:72:a3			and
SDCFMQA_Redundant_3k_1	RuckusAP	c4:6a:b7:7c:46:08	0.74.1	K_Hotspot	and
ScaleZD-12	AP1200002	03:00:0C:00:00:0E	10.1.0		-cli
ScaleZD-15	AP1500009	03:00:0F:00:00:42	10.1.0		use

Export As XLS File CSV File

umns 10 More Records 1

Save View

- ☑ ZD Name
- ☑ AP Name
- ☐ Description
- ☑ Client MAC
- ☑ Client IP Address
- ☐ Client IPv6 Address
- ☐ Client Model
- ☐ User Name
- ☑ WLAN
- ☑ Device Info
- ☑ Host Name
- ☐ Vendor
- ☐ On Time
- ☑ Associated Time
- ☑ Channel
- ☑ Radio Type
- ☑ Signal
- ☑ Rx
- ☑ Tx
- ☑ Vlan
- ☑ Retries
- ☑ Connection
- ☑ Authentication

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Text View and Map View

The Map View displays the geographical location of devices whose GPS coordinates have been configured. The device GPS coordinates can be configured either its their native Web interface (for standalone APs) or from the FlexMaster Web interface.

The Map View shows the connection status of each managed device – green icons indicate online devices, and red markers indicate offline devices. Yellow ZD icons indicate that some of the associated APs are offline.

When multiple devices have the same GPS coordinates, FlexMaster shows a single multiple-device icon in that location.

NOTE: The GPS coordinates of standalone APs can be set either from their native Web interface or from the FlexMaster Web interface. The GPS coordinates of ZoneDirector devices, on the other hand, can only be configured from the FlexMaster Web interface. GPS coordinates cannot be assigned to clients.

To set the coordinates of a standalone AP or ZoneDirector from the FlexMaster Web interface, search for the device on the *Inventory* page, and then click the **Edit** link in the *Actions* column. When the *Edit Tag* form appears, enter the GPS coordinates of the device, and then click **OK**.

By default, the Text View is displayed and the Map View is hidden. To display the ZD Map View, click **Map View** on the *Inventory* > *ZoneDirectors* > *Search* page. To display the AP Map View, click **Map View** on the *Inventory* > *Standalone APs* > *Search* page.

When the selected Map View appears, you can switch to either of the following views:

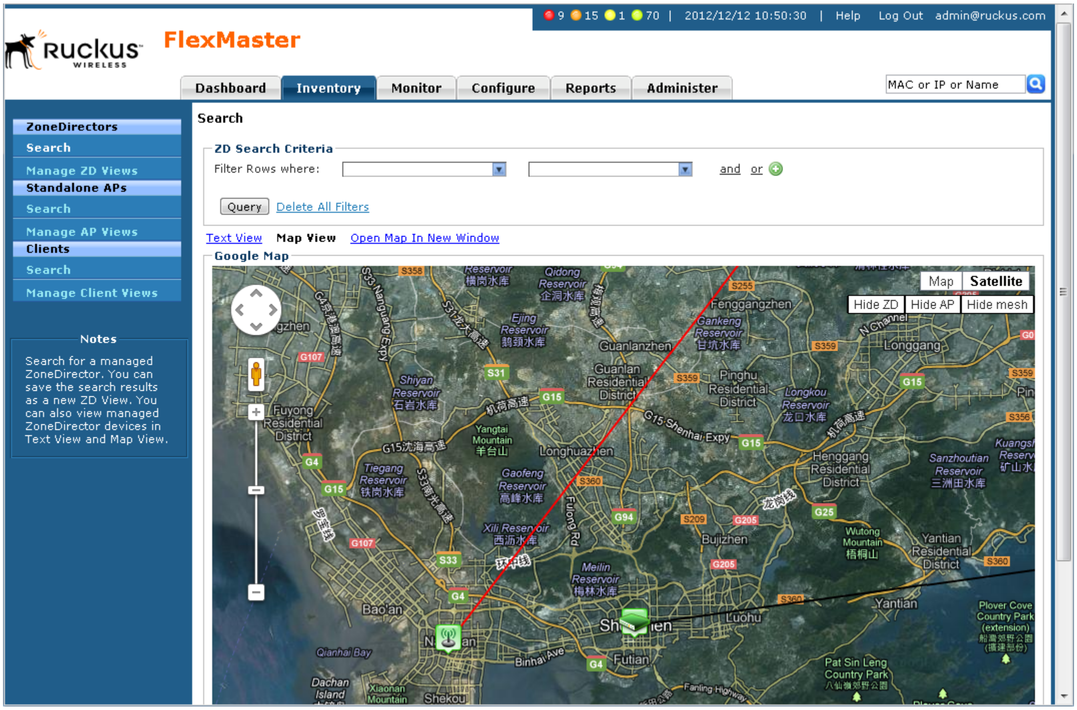
- *Map*: Standard view of roads, cities and bodies of water
- *Satellite*: Satellite map including geographical features; select *Labels* to show street and city names and other information

NOTE: When a device changes status (online or offline), its status is not updated on the Map View. Click the ↻ (Refresh) button in the upper-right corner of the page to show the updated device status on the Map View.

The ZD Map View includes three buttons in the top-right corner:

- **Show ZD/Hide ZD**: Click to show or hide all ZoneDirector devices
- **Show AP/Hide AP**: Click to show or hide all ZoneDirector-managed APs
- **Show Mesh/Hide Mesh**: Click to show or hide all ZoneDirector-managed mesh network links

Figure 41. Map View showing AP, ZD and mesh links (red) using satellite view



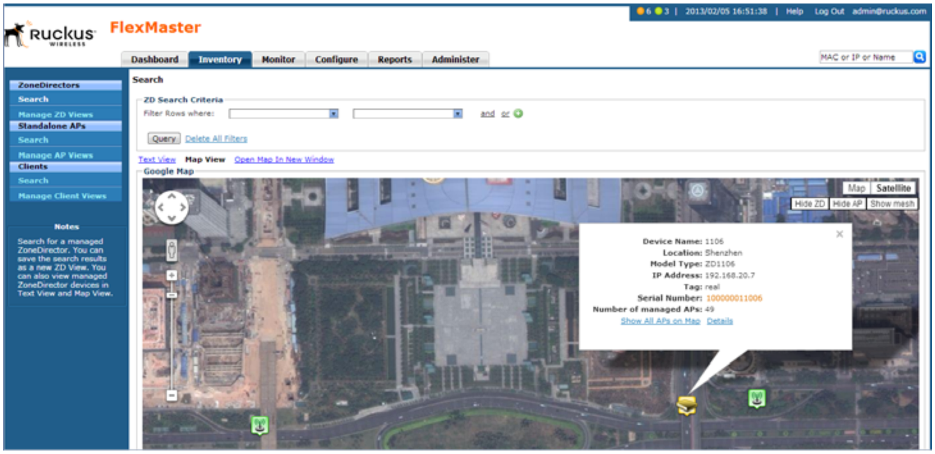
Search for a managed ZoneDirector. You can save the search results as a new ZD View. You can also view managed ZoneDirector devices in Text View and Map View.

ZD Icons

- When you hover the cursor over a single-ZD icon, FlexMaster displays the ZD device name.
- When you hover the cursor over a multiple-ZD icon, FlexMaster displays the all ZD device names.
- When you click a single-ZD icon, FlexMaster displays a basic information box that includes the ZD device name, location, and other basic information. Click the *Serial Number* link to display the ZD native Web interface in a new tab. The information box includes a *Show All APs on Map* link; click this link to display the managed AP icons on the ZD Map View. The information box also includes a *Details* link; click this link to display the managed AP and mesh data.

  When you click a multiple-ZD icon, FlexMaster displays an information box that includes the same information and links for each ZD device at that location.

Figure 42. Map View showing ZD basic information



Search for a managed ZoneDirector. You can save the search results as a new ZD View. You can also view managed ZoneDirector devices in Text View and Map View.

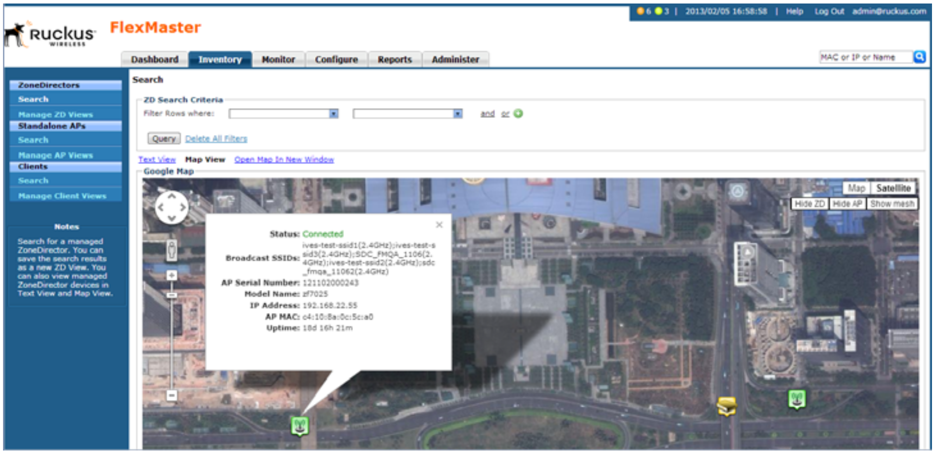
Device Name: 1106
Location: Shenzhen
Model Type: ZD1106
IP Address: 192.168.20.7
Tag: real
Serial Number: 100000011006
Number of managed APs: 49
Show All APs on Map Details

AP Icons

- When you hover the cursor over a single-AP icon, FlexMaster displays the AP device name and available channel.
- When you hover the cursor over a multiple-AP icon, FlexMaster displays the AP device names and available channels.
- When you click a single-AP icon, FlexMaster displays the AP device name, broadcast SSIDs, and other basic information.

  When you click a multiple-AP icon, FlexMaster displays a basic information box that includes the same information and links for each AP device at that location.

Figure 43. Map View showing AP basic information



Search for a managed ZoneDirector. You can save the search results as a new ZD View. You can also view managed ZoneDirector devices in Text View and Map View.

Status: Connected
Broadcast SSIDs: ives-test-ssid1(2.4GHz);ives-test-ssid3(2.4GHz);SDC_FMQA_1106(2.4GHz);ives-test-ssid2(2.4GHz);sdc_fmqa_11062(2.4GHz)
AP Serial Number: 121102000243
Model Name: zf7025
IP Address: 192.168.22.55
AP MAC: c4:10:8a:0c:5c:a0
Uptime: 18d 16h 21m

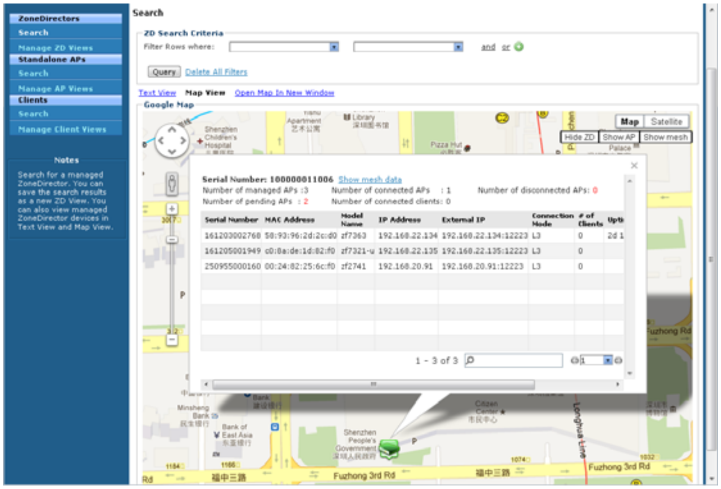
Viewing ZoneDirector Devices on the Map View

When viewing a ZoneDirector device on the Map View, you have several options for displaying additional information about the ZoneDirector device. Click the ZoneDirector icon on the Map View to display the following information:

- Device name
- Location (if configured)
- Model type
- IP address
- Tag (if configured)
- Serial number (hyperlink): Clicking this link opens the ZoneDirector Web interface.
- Number of managed APs
- **Show All APs on Map** (hyperlink): Clicking this link displays the Ruckus Wireless APs on the Map View. After clicking this link, the **Show/Hide ZD, Show/Hide AP**, and **Show/Hide Mesh** buttons appear in the upper-right corner of the Map View.
- **Details** (hyperlink): Clicking this link displays associated AP details in a pop-up table.

  When mesh networking is enabled on ZoneDirector, you can click **Show mesh data** to view the ZD's mesh tree. After that you can click **Show AP data** and **Show mesh data** to toggle between the ZD's mesh tree and the associated AP details table.

Figure 44. Map View showing associated AP details pop-up using map view



Notes

Search for a managed ZoneDirector. You can save the search results as a new ZD View. You can also view managed ZoneDirector devices in Text View and Map View.

Serial Number: 100000011006

Number of managed APs :3   Number of connected APs : 1   Number of disconnected APs: 0

Number of pending APs : 2   Number of connected clients: 0

Serial Number	MAC Address	Model Name	IP Address	External IP	Connection Mode	# of Clients	Upti
161203002760	58:93:96:2d:2c:d0	zf7363	192.168.22.134	192.168.22.134:12223	L3	0	2d 1
161205001949	c0:8a:de:1d:82:f0	zf7321-u	192.168.22.135	192.168.22.135:12223	L3	0	
250955000160	00:24:82:25:6c:f0	zf2741	192.168.20.91	192.168.20.91:12223	L3	0	

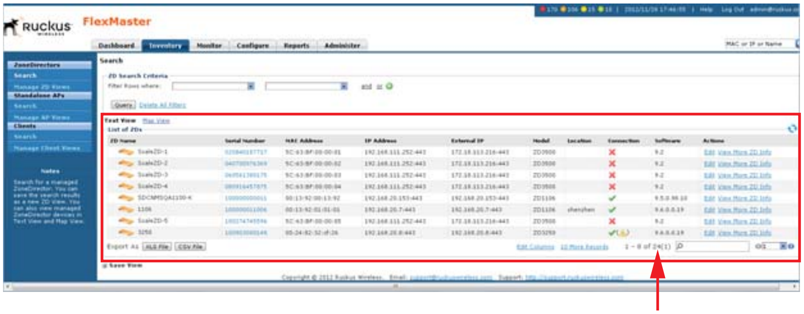
Working with ZoneDirector Inventory

The ZoneDirector *Inventory* page displays a list of ZoneDirector devices that have registered with FlexMaster. It also provides options for searching for specific ZoneDirector devices (especially helpful when you are managing a large number of ZoneDirector devices), creating views, and viewing devices in *Text View* and *Map View*.

Viewing a Summary of ZoneDirector Devices

To view ZoneDirector devices that have registered with FlexMaster, click the **Inventory** tab. A list of ZoneDirector devices appears in the *List of ZDs* section. The total number of managed ZoneDirector devices is indicated below the table, right next to the device search box.

Figure 45. A list of ZoneDirector devices that have registered with FlexMaster appears in the List of ZDs section



Search

ZD Search Criteria

Filter Rows where:

List of ZDs

ZD Name	Serial Number	MAC Address	IP Address	External IP	Model	Location	Connection	Software	Actions
ScaleZD-1	[illegible]	5C:63:BF:00:00:01	192.168.111.252:443	172.18.113.216:443	ZD3500		✗	9.2	Edit View More ZD Info
ScaleZD-2	[illegible]	5C:63:BF:00:00:02	192.168.111.252:443	172.18.113.216:443	ZD3500		✗	9.2	Edit View More ZD Info
ScaleZD-3	[illegible]	5C:63:BF:00:00:03	192.168.111.252:443	172.18.113.216:443	ZD3500		✗	9.2	Edit View More ZD Info
ScaleZD-4	[illegible]	5C:63:BF:00:00:04	192.168.111.252:443	172.18.113.216:443	ZD3500		✗	9.2	Edit View More ZD Info
SDCNMSQA1100-K	100000000011	00:13:92:00:13:92	192.168.20.153:443	192.168.20.153:443	ZD1106		✓	9.5.0.98.10	Edit View More ZD Info
1106	100000001006	00:13:92:01:01:01	192.168.20.7:443	192.168.20.7:443	ZD1106	shenzhen	✓	9.4.0.0.19	Edit View More ZD Info
ScaleZD-5	[illegible]	5C:63:BF:00:00:05	192.168.111.252:443	172.18.113.216:443	ZD3500		✗	9.2	Edit View More ZD Info
3250	[illegible]	00:24:82:32:df:26	192.168.20.8:443	192.168.20.8:443	ZD3250		✓	9.4.0.0.19	Edit View More ZD Info

1 - 8 of 24(1)

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Total ZoneDirector devices

The *List of ZDs* section can show up to 10 ZoneDirector devices at a time. When FlexMaster is managing more than 10 ZoneDirector devices, you can view the succeeding pages that list the remaining ZoneDirector devices by clicking the left and right arrows at the bottom of the page.

Alternatively, you can also use the search box at the bottom of the page to search for specific ZoneDirector devices.

Searching for ZoneDirector Devices

There are two ways to search for ZoneDirector devices:

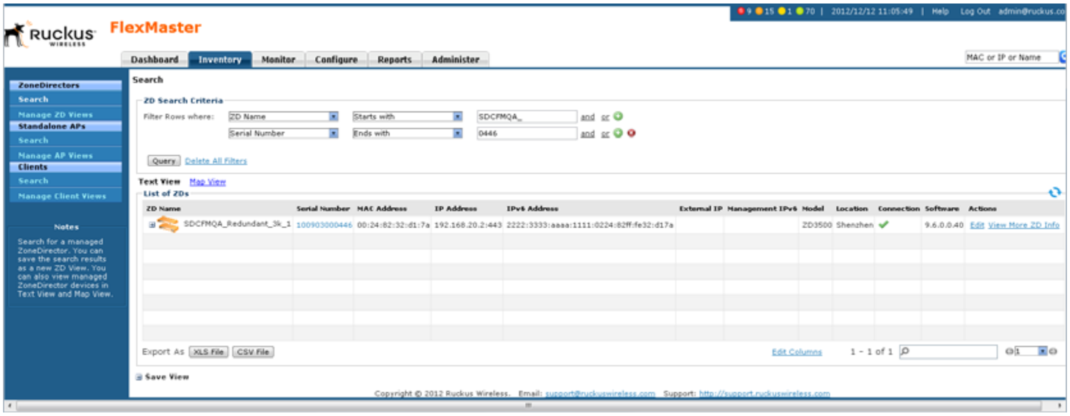
- Search Using the ZD Search Criteria
- Search Using the Search Box

Search Using the ZD Search Criteria

1. Go to *Inventory* > *ZoneDirectors* > *Search.*
2. Go to the *ZD Search Criteria* section. To search for ZoneDirector devices, you need to specify the criteria of the devices that you are looking for.
3. In the first drop-down list box after *Filter Rows where,* select the search attribute that you want to use. Options include name, serial number, MAC address, IP address, external IP address, model, last seen, and others.
4. In the second drop-down list box, select the search operator that you want to use. Available search operators include:
   - *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered 172.17.16.176 as the search parameter, then only devices with this IP address appears in the search results.
   - *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered 100 as the search parameter, then all devices with "100" in the IP address (for example, 172.17.16.**100** and **100**.1.10.13) appears in the search results.
   - *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered 3208 as the query parameter, then only devices with serial numbers that begin with "3208" (for example, 320833000219 appear in the search results.
   - *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected **IP address** as the attribute and you entered 13 as the query parameter, then only devices with model names that end in "13" (for example, 100.1.10.**13**) appear in the search results.

   After you select a search operator, a third (text) box appears.
5. In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
6. If you want to add another search filter, then click ⊕. A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.
7. When you complete setting up the search filters, click **Query**. FlexMaster displays the devices that match the search criteria.

Figure 46. Using Search Criteria to search for a ZoneDirector device



Notes

Search for a managed ZoneDirector. You can save the search results as a new ZD View. You can also view managed ZoneDirector devices in Text View and Map View.

Search

ZD Search Criteria

Filter Rows where: ZD Name | Starts with | SDCFMQA_ and or
Serial Number | Ends with | 0446 and or

List of ZDs

ZD Name	Serial Number	MAC Address	IP Address	IPv6 Address	External IP	Management IPv6	Model	Location	Connection	Software	Actions
SDCFMQA_Redundant_3k_1	100903000446	00:24:82:32:d1:7a	192.168.20.2:443	2222:3333:aaaa:1111:0224:82ff:fe32:d17a			ZD3500	Shenzhen	✓	9.6.0.0.40	Edit View More ZD Info

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

NOTE: If you save your query parameters as a view, then any new devices that later register with FlexMaster and meet the query criteria are automatically added to the saved view.

Additional Tasks That You Can Perform

After the search results appear, you can perform the following tasks:

- Save the search results as XLS (Microsoft® Excel® file format): In *Export As*, click **XLS File**. When the *Save As* dialog box appears, click **Save File**, and then click **OK**. Use Microsoft Excel to open the file.
- Save the search results as CSV (comma-separated value file): In *Export As*, click **CSV File**. When the *Save As* dialog box appears, click **Save File**, and then click **OK**. You can use any spreadsheet application (such as Microsoft Excel) to open the file.
- Save the results as a ZD view: Refer to Creating a ZD View for more information.

Search Using the Search Box

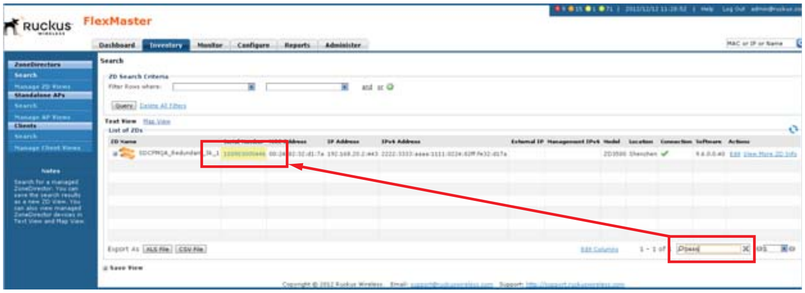
A search box exists at the bottom right area of the *List of ZDs* section. You can use this search box to search for ZoneDirector devices that are reporting to FlexMaster.

NOTE: If you save your query parameters as a view, then any new devices that later register with FlexMaster and meet the query criteria are automatically added to the saved view.

1. Type a search string into the box. The search string could be a partial or full string and can consist of numbers or letters or a combination of both.
2. Press **<Enter>** on your keyboard.

FlexMaster searches all its database columns for a match to the string that you entered, and then displays the results in the *List of ZDs* table. The device property that matches the search string is highlighted in yellow.

Figure 47. The device property that matches the search string is highlighted in the search results



Notes

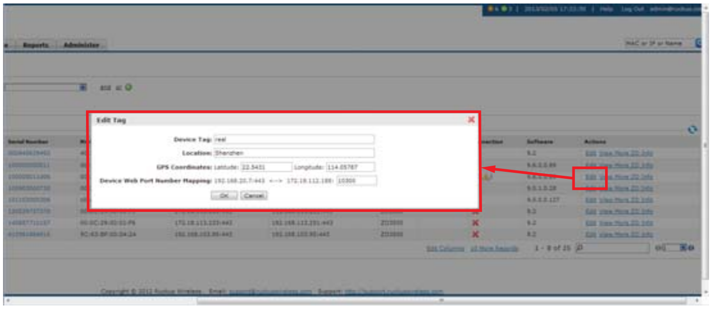
Search for a managed ZoneDirector. You can save the search results as a new ZD View. You can also view managed ZoneDirector devices in Text View and Map View.

Editing a ZoneDirector Tag

You can edit a ZoneDirector device's tag name, location and GPS coordinates:

1. In the *List of ZDs* table, display the device you want to edit. When the device you want to edit does not appear on the table, search for it using the search box.
2. When the device appears, click the **Edit** link. FlexMaster displays the *Edit Tag* pop-up menu.
3. Edit the ZD device tag properties that you want to update. Properties that you can edit include:
   - *Device Tag* name
   - *Location* -- text string that appears in the *Text View* and the *Map View*
   - *GPS Coordinates* (Latitude and Longitude) -- FlexMaster uses these to position the ZD icon on the *Map View*
   - *Device Web Port Number Mapping* -- Maps the device wakeup port for this ZD; normally 10300.
4. After you make changes, click **OK**.

Figure 48. Editing ZoneDirector tag details



Edit Tag

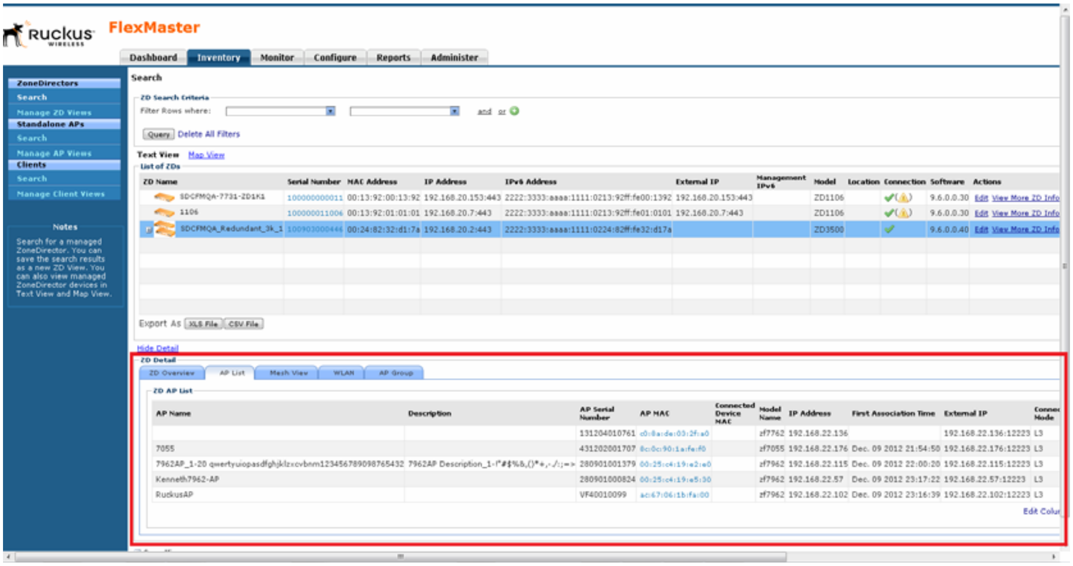
Device Tag: real
Location: Shenzhen
GPS Coordinates: Latitude: 22.5431 Longitude: 114.05787
Device Web Port Number Mapping: 192.168.20.7:443 <--> 172.18.112.188: 10300

Viewing ZoneDirector APs

Follow these steps to view a list of APs reporting to a ZoneDirector device.

1. On the *List of ZDs* table, display the ZD device that includes the APs you want to view. When the ZD device does not appear on the table, search for it as described in Searching for ZoneDirector Devices.
2. In the *List of ZDs* table, click the **View More ZD Info** link. FlexMaster displays the *ZD Detail* section at the bottom of the window.
3. In the *ZD Detail* section, click the **AP List** tab. FlexMaster displays the following information for the associated APs:
   - AP name
   - Description (optional)
   - Serial number
   - MAC address
   - Connected device MAC address
   - Model name
   - IP address
   - First association time
   - External IP
   - Connection mode
   - # of clients
   - Uptime
   - Connection status

Figure 49. The AP List shows a list of APs reporting to the ZoneDirector device



Notes

Search for a managed ZoneDirector. You can save the search results as a new ZD View. You can also view managed ZoneDirector devices in Text View and Map View.

List of ZDs

ZD Name	Serial Number	MAC Address	IP Address	IPv6 Address	External IP	Management IPv6	Model	Location	Connection	Software	Actions
SDCFMQA-7731-ZD1K1	100000000011	00:13:92:00:13:92	192.168.20.153:443	2222:3333:aaaa:1111:0213:92ff:fe00:1392	192.168.20.153:443		ZD1106		✓(⚠)	9.6.0.0.30	Edit View More ZD Info
1106	100000011006	00:13:92:01:01:01	192.168.20.7:443	2222:3333:aaaa:1111:0213:92ff:fe01:0101	192.168.20.7:443		ZD1106		✓(⚠)	9.6.0.0.30	Edit View More ZD Info
SDCFMQA_Redundant_3k_1	100903000446	00:24:82:32:d1:7a	192.168.20.2:443	2222:3333:aaaa:1111:0224:82ff:fe32:d17a			ZD3500		✓	9.6.0.0.40	Edit View More ZD Info

ZD AP List

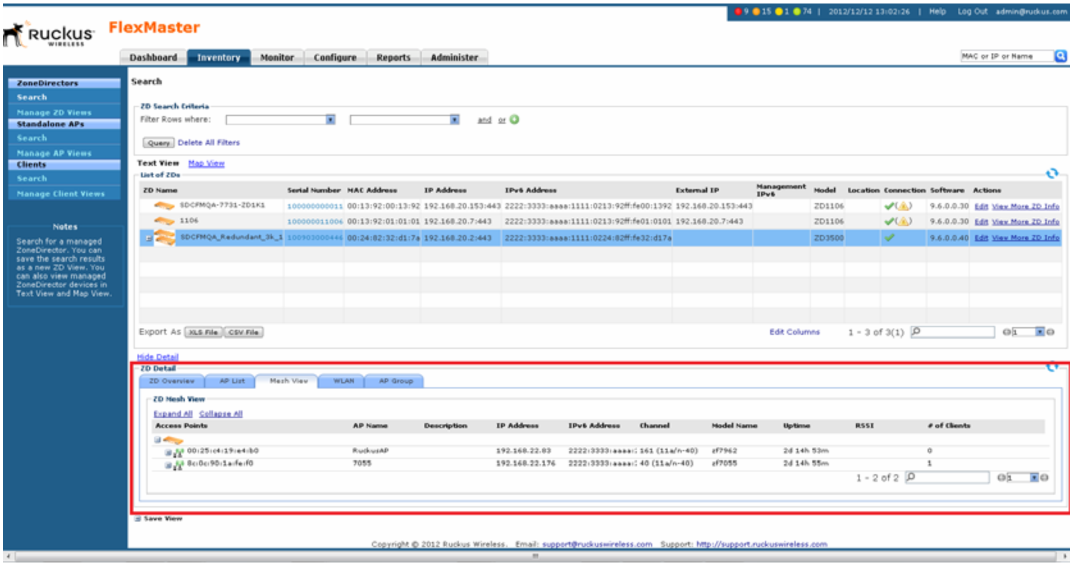
AP Name	Description	AP Serial Number	AP MAC	Connected Device MAC	Model Name	IP Address	First Association Time	External IP	Connec Mode
		131204010761	c0:8a:de:03:2f:a0		zf7762	192.168.22.136		192.168.22.136:12223	L3
7055		431202001707	8c:0c:90:1a:fe:f0		zf7055	192.168.22.176	Dec. 09 2012 21:54:50	192.168.22.176:12223	L3
7962AP_1-20 qwertyuiopasdfghjklzxcvbnm123456789098765432	7962AP Description_1-!"#$%&,()*+,-./:;=>	280901001379	00:25:c4:19:e2:e0		zf7962	192.168.22.115	Dec. 09 2012 22:00:20	192.168.22.115:12223	L3
Kenneth7962-AP		280901000824	00:25:c4:19:e5:30		zf7962	192.168.22.57	Dec. 09 2012 23:17:22	192.168.22.57:12223	L3
RuckusAP		VF40010099	ac:67:06:1b:fa:00		zf7962	192.168.22.102	Dec. 09 2012 23:16:39	192.168.22.102:12223	L3

Viewing ZoneDirector Mesh Connections

If a ZoneDirector device is part of a mesh network, then follow these steps to view mesh details.

1. On the *List of ZDs* table, display the ZD device that you want to view. When the ZD device does not appear on the table, search for it as described in Searching for ZoneDirector Devices.
2. In the *List of ZDs* table, click the **View More ZD Info** link. FlexMaster displays the *ZD Detail* section at the bottom of the window.
3. In the *ZD Detail* section, click the **Mesh View** tab. FlexMaster displays the following mesh details:
   - AP MAC address
   - AP name
   - Description
   - IP address
   - IPv6 address
   - Channel
   - Model name
   - Uptime
   - RSSI
   - # of clients

Figure 50. ZoneDirector Mesh View



Search for a managed ZoneDirector. You can save the search results as a new ZD View. You can also view managed ZoneDirector devices in Text View and Map View.

ZD Name	Serial Number	MAC Address	IP Address	IPv6 Address	External IP	Management IPv6	Model	Location	Connection	Software	Actions
SDCFMQA-7731-ZD1K1	100000000011	00:13:92:00:13:92	192.168.20.153:443	2222:3333:aaaa:1111:0213:92ff:fe00:1392	192.168.20.153:443		ZD1106		✓(⚠)	9.6.0.0.30	Edit View More ZD Info
1106	100000011006	00:13:92:01:01:01	192.168.20.7:443	2222:3333:aaaa:1111:0213:92ff:fe01:0101	192.168.20.7:443		ZD1106		✓(⚠)	9.6.0.0.30	Edit View More ZD Info
SDCFMQA_Redundant_3k_1	100903000446	00:24:82:32:d1:7a	192.168.20.2:443	2222:3333:aaaa:1111:0224:82ff:fe32:d17a			ZD3500		✓	9.6.0.0.40	Edit View More ZD Info

Access Points	AP Name	Description	IP Address	IPv6 Address	Channel	Model Name	Uptime	RSSI	# of Clients
00:25:c4:19:e4:b0	RuckusAP		192.168.22.83	2222:3333:aaaa::	161 (11a/n-40)	zf7962	2d 14h 53m		0
8c:0c:90:1a:fe:f0	7055		192.168.22.176	2222:3333:aaaa::	40 (11a/n-40)	zf7055	2d 14h 55m		1

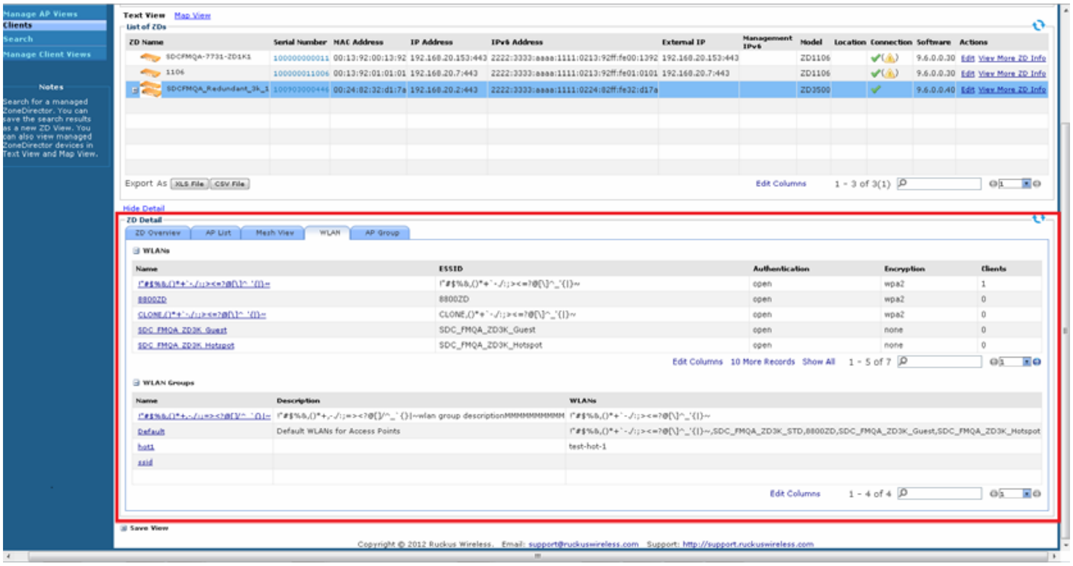
Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Viewing ZoneDirector WLANs and WLAN Groups

Follow these steps to view ZD WLAN and WLAN group details.

1. On the *List of ZDs* table, display the ZD device that you want to view. When the ZD device does not appear on the table, search for it as described in Searching for ZoneDirector Devices.
2. In the *List of ZDs* table, click the **View More ZD Info** link. FlexMaster displays the *ZD Detail* section at the bottom of the window.
3. In the *ZD Detail* section, click the **WLAN** tab. FlexMaster displays the following WLAN and WLAN group details:
   - WLAN name
   - WLAN ESSID
   - WLAN authentication type
   - WLAN encryption type
   - WLAN number of connected clients
   - WLAN group name
   - WLAN group description
   - WLAN group members

Figure 51.   ZoneDirector WLANs and WLAN groups



Search for a managed ZoneDirector. You can save the search results as a new ZD View. You can also view managed ZoneDirector devices in Text View and Map View.

List of ZDs

ZD Name	Serial Number	MAC Address	IP Address	IPv6 Address	External IP	Management IPv6	Model	Location	Connection	Software	Actions
SDCFMQA-7731-ZD1K1	100000000011	00:13:92:00:13:92	192.168.20.153:443	2222:3333:aaaa:1111:0213:92ff:fe00:1392	192.168.20.153:443		ZD1106		✓(⚠)	9.6.0.0.30	Edit View More ZD Info
1106	100000011006	00:13:92:01:01:01	192.168.20.7:443	2222:3333:aaaa:1111:0213:92ff:fe01:0101	192.168.20.7:443		ZD1106		✓(⚠)	9.6.0.0.30	Edit View More ZD Info
SDCFMQA_Redundant_3k_1	100903000446	00:24:82:32:d1:7a	192.168.20.2:443	2222:3333:aaaa:1111:0224:82ff:fe32:d17a			ZD3500		✓	9.6.0.0.40	Edit View More ZD Info

ZD Detail

WLANs

Name	ESSID	Authentication	Encryption	Clients
!"#$%&,()*+`-./:;><=?@[\]^_'{|}~	!"#$%&,()*+`-./:;><=?@[\]^_'{|}~	open	wpa2	1
8800ZD	8800ZD	open	wpa2	0
CLONE,()*+`-./:;><=?@[\]^_'{|}~	CLONE,()*+`-./:;><=?@[\]^_'{|}~	open	wpa2	0
SDC_FMQA_ZD3K_Guest	SDC_FMQA_ZD3K_Guest	open	none	0
SDC_FMQA_ZD3K_Hotspot	SDC_FMQA_ZD3K_Hotspot	open	none	0

WLAN Groups

Name	Description	WLANs
!"#$%&,()*+,-./:;=><?@[]/^_'{}|~	!"#$%&,()*+,-./:;=><?@[]/^_`{}|~wlan group descriptionMMMMMMMMMM	!"#$%&,()*+`-./:;><=?@[\]^_'{|}~
Default	Default WLANs for Access Points	!"#$%&,()*+`-./:;><=?@[\]^_'{|}~,SDC_FMQA_ZD3K_STD,8800ZD,SDC_FMQA_ZD3K_Guest,SDC_FMQA_ZD3K_Hotspot
hot1		test-hot-1
ssid		

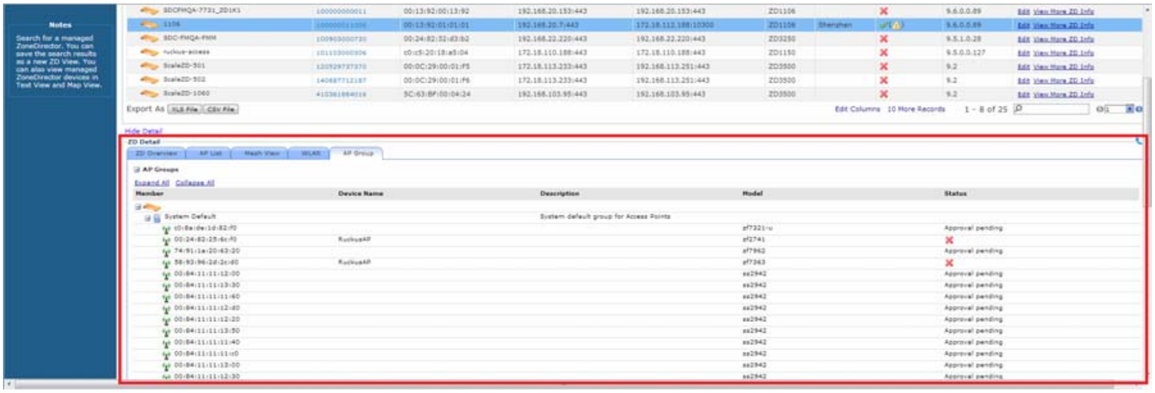
Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Viewing ZoneDirector AP Groups

Follow these steps to view a list of AP groups reporting to a ZoneDirector device.

1. On the *List of ZDs* table, display the ZD device that includes the AP group you want to view. When the ZD device does not appear on the table, search for it as described in Searching for ZoneDirector Devices.
2. In the *List of ZDs* table, click the **View More ZD Info** link. FlexMaster displays the *ZD Detail* section at the bottom of the window.
3. In the *ZD Detail* section, click the **AP Group** tab. FlexMaster displays the following information for the associated AP groups:
   - AP group name (default = *System Default*)
   - Device MAC address
   - Device name (optional)
   - Description (optional)
   - Device model
   - Connection status

Figure 52. The AP Groups shows a list of APs reporting to the ZoneDirector AP group



Notes

Search for a managed ZoneDirector. You can save the search results as a new ZD View. You can also view managed ZoneDirector devices in Text View and Map View.

SDCFMQA-7731_ZD1K1	100000000011	00:13:92:00:13:92	192.168.20.153:443	192.168.20.153:443	ZD1106		✗	9.6.0.0.89	Edit View More ZD Info
1106	100000011106	00:13:92:01:01:01	192.168.20.7:443	172.18.112.188:10300	ZD1106	Shenzhen	✓(⚠)	9.6.0.0.89	Edit View More ZD Info
SDC-FMQA-FMM	100903000720	00:24:82:32:d3:b2	192.168.22.220:443	192.168.22.220:443	ZD3250		✗	9.5.1.0.28	Edit View More ZD Info
ruckus-access	101103000306	c0:c5:20:18:a5:04	172.18.110.188:443	172.18.110.188:443	ZD1150		✗	9.5.0.0.127	Edit View More ZD Info
ScaleZD-501	120529737370	00:0C:29:00:01:F5	172.18.113.233:443	192.168.113.251:443	ZD3500		✗	9.2	Edit View More ZD Info
ScaleZD-502	140687712187	00:0C:29:00:01:F6	172.18.113.233:443	192.168.113.251:443	ZD3500		✗	9.2	Edit View More ZD Info
ScaleZD-1060	410361864016	5C:63:BF:00:04:24	192.168.103.95:443	192.168.103.95:443	ZD3500		✗	9.2	Edit View More ZD Info

Export As XLS File CSV File

Edit Columns 10 More Records 1 - 8 of 25

Hide Detail

ZD Detail

AP Groups

Expand All Collapse All

Member	Device Name	Description	Model	Status
System Default		System default group for Access Points		
c0:8a:de:1d:82:f0			zf7321-u	Approval pending
00:24:82:25:6c:f0	RuckusAP		zf2741	✗
74:91:1a:20:63:20			zf7962	Approval pending
58:93:96:2d:2c:40	RuckusAP		zf7363	✗
00:84:11:11:12:00			ss2942	Approval pending
00:84:11:11:13:30			ss2942	Approval pending
00:84:11:11:11:60			ss2942	Approval pending
00:84:11:11:12:d0			ss2942	Approval pending
00:84:11:11:12:20			ss2942	Approval pending
00:84:11:11:13:50			ss2942	Approval pending
00:84:11:11:11:40			ss2942	Approval pending
00:84:11:11:11:c0			ss2942	Approval pending
00:84:11:11:13:00			ss2942	Approval pending
00:84:11:11:12:30			ss2942	Approval pending

Creating a ZD View

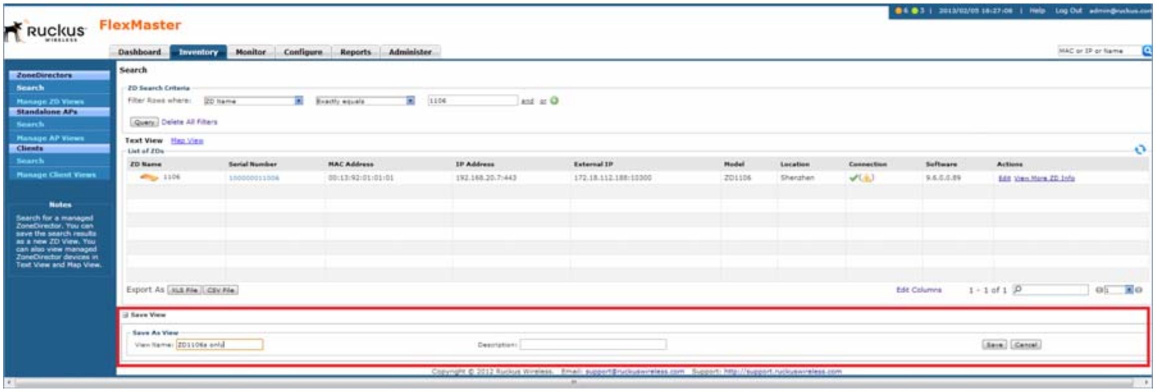
A *view* in FlexMaster is a manually configured grouping of devices with similar characteristics. For example, you can create a view that contains ZoneDirector (ZD) devices of the same model. Views are useful when want to deploy tasks to a group of devices.

A default view called *All ZoneDirectors*, which contains all ZoneDirector devices reporting to FlexMaster, exists. You can create additional or more specific views, depending on your management requirements.

1. Perform a search for clients using one of these search methods:
   - Search Using the ZD Search Criteria, or
   - Search Using the Search Box
2. When the search results appear, scroll down to the *Save as View* section.
3. In *View Name*, type a name that you want to assign to the view.
4. In *Description*, type an optional description for the view that you are saving. For example, when the view contains only ZoneDirector 1106 devices, you can type **`ZD1106s only`**.
5. Click **Save**.

The *Manage ZD Views* page appears, displaying the ZD view that you have saved along with other saved ZD views.

Figure 53. Creating a ZD view that contains only ZoneDirector 1106 devices



Search for a managed ZoneDirector. You can save the search results as a new ZD View. You can also view managed ZoneDirector devices in Text View and Map View.

Search

ZD Search Criteria

Filter Rows where: ZD Name | Exactly equals | 1106 | and or

List of ZDs

ZD Name	Serial Number	MAC Address	IP Address	External IP	Model	Location	Connection	Software	Actions
1106	100000011006	00:13:92:01:01:01	192.168.20.7:443	172.18.112.188:10300	ZD1106	Shenzhen	✓ (⚠)	9.6.0.0.89	Edit View More ZD Info

1 - 1 of 1

Save View

Save As View

View Name: ZD1106s only

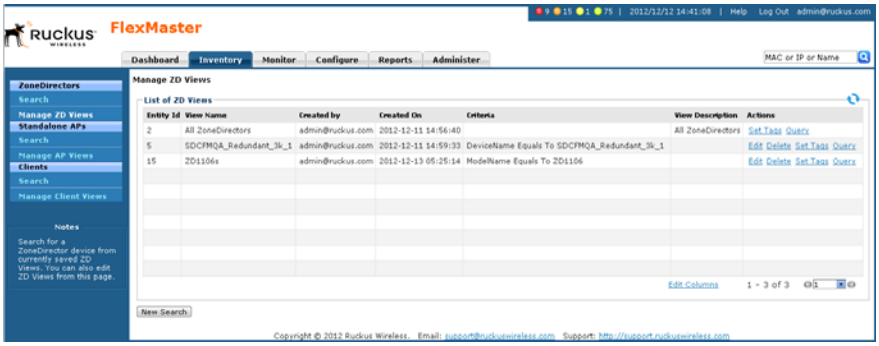
Description:

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Managing ZD Views

Use the *Manage ZD Views* page to view list of existing ZoneDirector views, assign tags to a view, run a query, and edit or delete a view.

Figure 54. The Manage ZD View page lists all existing ZoneDirector views



Search for a ZoneDirector device from currently saved ZD Views. You can also edit ZD Views from this page.

Manage ZD Views

List of ZD Views

Entity Id	View Name	Created by	Created On	Criteria	View Description	Actions
2	All ZoneDirectors	admin@ruckus.com	2012-12-11 14:56:40		All ZoneDirectors	Set Tags Query
5	SDCFMQA_Redundant_3k_1	admin@ruckus.com	2012-12-11 14:59:33	DeviceName Equals To SDCFMQA_Redundant_3k_1		Edit Delete Set Tags Query
15	ZD1106s	admin@ruckus.com	2012-12-13 05:25:14	ModelName Equals To ZD1106		Edit Delete Set Tags Query

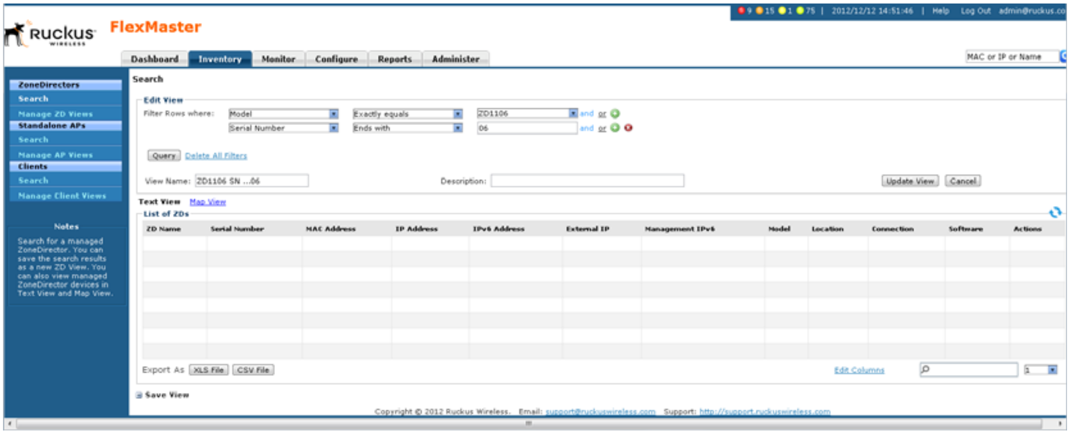
Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Editing a ZD View

Editing a ZD view is very similar to the process of creating a ZD view.

1. Go to the *Inventory* > *ZoneDirectors* > *Manage ZD Views* page. All existing ZD Views appear in the *Manage ZD Views* section.
2. Look for the ZD view that you want to edit, and then click its **Edit** link. FlexMaster displays the *Edit View* section.
3. Update any of the following to edit the view:
   - The search filter that you configured when you created the view
   - The view name
   - The optional description
4. To view devices that match the search filter that you updated, click **Query**.
5. To save the changes that you made, click **Update View**.

Figure 55. Editing a ZD view



Notes

Search for a managed ZoneDirector. You can save the search results as a new ZD View. You can also view managed ZoneDirector devices in Text View and Map View.

Filter Rows where: Model | Exactly equals | ZD1106 and or
Serial Number | Ends with | 06 and or

View Name: ZD1106 SN ...06

Description:

ZD Name	Serial Number	MAC Address	IP Address	IPv6 Address	External IP	Management IPv6	Model	Location	Connection	Software	Actions

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Deleting a ZD View

1. Go to the *Inventory* > *ZoneDirectors* > *Manage ZD Views* page.
2. Look for the ZD view that you want to delete.
3. Click the **Delete** link that is in the same row as the view name. A confirmation message appears.
4. Click **OK** to confirm.

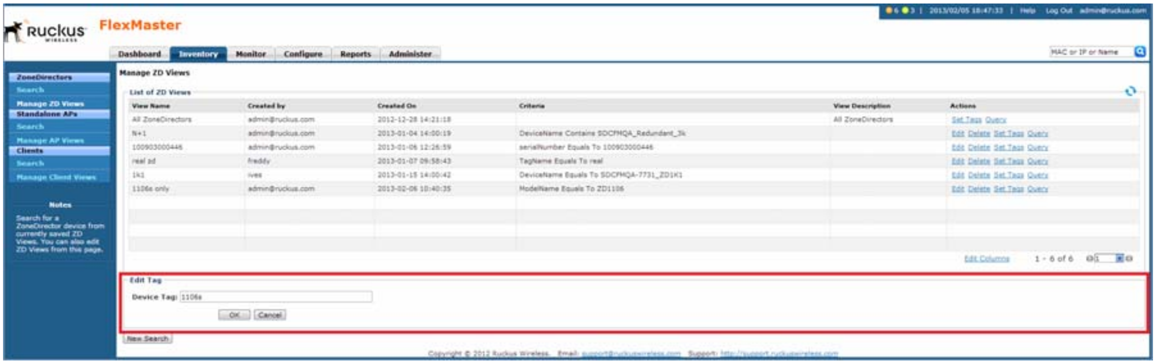
The *Manage Views* page refreshes, and then FlexMaster removes the view that you deleted.

Editing a ZD View Device Tag

You can create an optional ZD device tag for all the devices included in the device view.

1. In the *List of ZD Views* table, display the ZD view you want to edit. If the ZD view you want to edit does not appear on the table, then search for it using the search box.
2. Click the ZD view **Set Tags** link. FlexMaster displays the *Edit Tag* menu at the bottom of the window.
3. Edit the ZD view device tag name.
4. After you make changes, click **OK**.

Figure 56. Editing ZoneDirector view device tag details



Notes

Search for a ZoneDirector device from currently saved ZD Views. You can also edit ZD Views from this page.

Manage ZD Views

List of ZD Views

View Name	Created by	Created On	Criteria	View Description	Actions
All ZoneDirectors	admin@ruckus.com	2012-12-28 14:21:18		All ZoneDirectors	Set Tags Query
N+1	admin@ruckus.com	2013-01-04 14:00:19	DeviceName Contains SDCFMQA_Redundant_3k		Edit Delete Set Tags Query
100903000446	admin@ruckus.com	2013-01-06 12:26:59	serialNumber Equals To 100903000446		Edit Delete Set Tags Query
real zd	freddy	2013-01-07 09:58:43	TagName Equals To real		Edit Delete Set Tags Query
1k1	ives	2013-01-15 14:00:42	DeviceName Equals To SDCFMQA-7731_ZD1K1		Edit Delete Set Tags Query
1106a only	admin@ruckus.com	2013-02-06 10:40:35	ModelName Equals To ZD1106		Edit Delete Set Tags Query

Edit Columns 1 - 6 of 6

Edit Tag

Device Tag: 1106a

OK Cancel

New Search

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Viewing Devices That Belong to a ZD View

Use the **Query** link on the *Manage Views* page to display the devices that belong to a view.

1. Go to the *Inventory* > *ZoneDirectors* > *Manage ZD Views* page.
2. Look for the ZD view on which you want to run a query.
3. Click the ZD view **Query** link. The ZoneDirector *Search* page appears, and the devices that belong to the ZD view appear in the *List of ZDs* section.

Working with Standalone APs Inventory

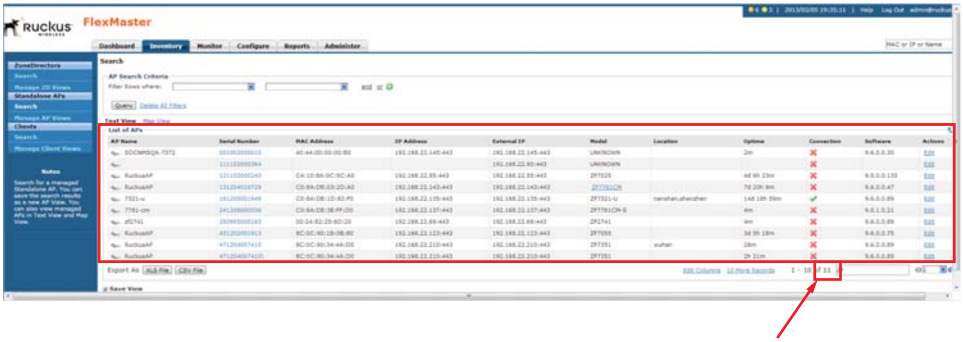
The Standalone APs *Inventory* page displays a list of APs that are reporting *directly* to FlexMaster. It also provides options for searching for specific standalone APs (especially helpful when you are managing a large number of APs), creating views, and viewing devices in *Text View* and *Map View*.

NOTE: To view a list of APs that are reporting to managed ZoneDirector devices, refer to Viewing ZoneDirector APs.

Viewing a Summary of Standalone APs

To view APs that have registered with FlexMaster, click *Inventory* > *Standalone APs* > *Search.* A list of APs appears in the *List of APs* section. The total number of managed APs is indicated below the table, right next to the device search box.

Figure 57. A list of APs that have registered with FlexMaster appears in the List of APs section



AP Name	Serial Number	MAC Address	IP Address	External IP	Model	Location	Uptime	Connection	Software	Actions
SOCMPSQA-7372	101002000010	40:44:00:00:00:B0	192.168.22.145:443	192.168.22.145:443	UNKNOWN		2m	✗	9.6.0.0.30	Edit
	111102000384			192.168.22.90:443	UNKNOWN			✗		Edit
RuckusAP	121102000243	C4:10:8A:0C:5C:A0	192.168.22.55:443	192.168.22.55:443	ZF7025		4d 6h 23m	✗	9.5.0.0.133	Edit
RuckusAP	131204010729	C0:8A:DE:03:2D:A0	192.168.22.143:443	192.168.22.143:443	ZF7761CM		7d 20h 9m	✗	9.6.0.0.47	Edit
7321-u	181205001949	C0:8A:DE:1D:82:F0	192.168.22.135:443	192.168.22.135:443	ZF7321-U	nanshan,shenzhen	14d 18h 59m	✓	9.6.0.0.89	Edit
7781-cm	241206000036	C0:8A:DE:3E:FF:D0	192.168.22.137:443	192.168.22.137:443	ZF7781CM-S		4m	✗	9.6.1.0.21	Edit
zf2741	150905000143	00:24:82:25:6D:20	192.168.22.69:443	192.168.22.69:443	ZF2741		4m	✗	9.6.0.0.89	Edit
RuckusAP	431202001813	8C:0C:90:1B:0B:80	192.168.22.123:443	192.168.22.123:443	ZF7055		3d 5h 18m	✗	9.6.0.0.75	Edit
RuckusAP	471204007410	8C:0C:90:34:4A:D0	192.168.22.210:443	192.168.22.210:443	ZF7351	wuhan	18m	✗	9.6.0.0.89	Edit
RuckusAP	471204007410	8C:0C:90:34:4A:D0	192.168.22.210:443	192.168.22.210:443	ZF7351		2h 21m	✗	9.6.0.0.89	Edit

Search for a managed Standalone AP. You can save the search results as a new AP View. You can also view managed APs in Text View and Map View.

The *List of APs* section can show up to 10 APs at a time. When FlexMaster is managing more than 10 APs, you can view the succeeding pages that list the remaining APs by clicking the left and right arrows at the bottom of the page.

Alternatively, you can also use the search box at the bottom of the page to search for specific APs.

Searching for Standalone APs

There are two ways to search for APs:

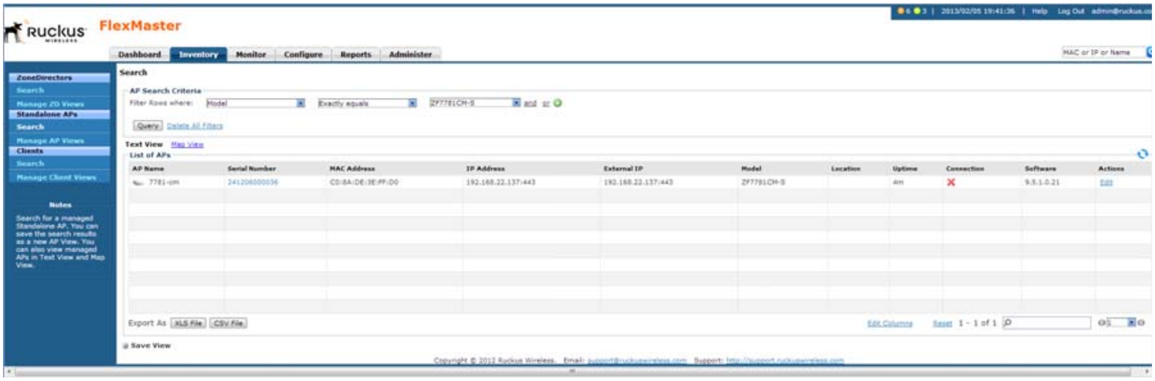
- Search Using the AP Search Criteria
- Search Using the Search Box

Search Using the AP Search Criteria

1. Go to *Inventory* > *Standalone APs* > *Search*.
2. Look for the *AP Search Criteria* section. To search for APs, you need to specify the criteria of the devices that you are looking for.
3. In the first drop-down list box after **Filter Rows where**, select the search attribute that you want to use. Options include AP name, serial number, MAC address, IP address, external IP address, model, and last seen (among others).
4. In the second drop-down list box, select the search operator that you want to use. Available search operators include:
   - *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered `172.17.16.176` as the search parameter, then only devices with this IP address appear in the search results.
   - *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered `100` as the search parameter, then all devices with "100" in the IP address (for example, `172.17.16.`**`100`** and **`100`**`.1.10.13`) appear in the search results.
   - *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered `3908` as the query parameter, then only devices with serial numbers that begin with "3908" (for example, `390801005202`) appear in the search results.
   - *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected **IP address** as the attribute and you entered `13` as the query parameter, then only devices with model names that end in "13" (for example, `100.1.10.`**`13`**) appear in the search results.

   After you select a search operator, a third (text) box appears.
5. In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
6. If you want to add another search filter, then click ⊕. A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.
7. When you complete setting up the search filters, click **Query**. FlexMaster displays the devices that match the search criteria.

Figure 58. Using Search Criteria to search for an AP



Notes

Search for a managed Standalone AP. You can save the search results as a new AP View. You can also view managed APs in Text View and Map View.

Filter Rows where: Model | Exactly equals | ZF7781CM-S and or

List of APs

AP Name	Serial Number	MAC Address	IP Address	External IP	Model	Location	Uptime	Connection	Software	Actions
7781-cm	241206000036	C0:8A:DE:3E:FF:D0	192.168.22.137:443	192.168.22.137:443	ZF7781CM-S		4m	✗	9.5.1.0.21	Edit

NOTE: If you save your query parameters as a view, then any new devices that later register with FlexMaster and meet the query criteria are automatically added to the saved view.

Additional Tasks That You Can Perform

After the search results appear, you can perform the following tasks:

- Save the search results as XLS (Microsoft® Excel® file format): In *Export As*, click **XLS File**. When the *Save As* dialog box appears, click **Save File**, and then click **OK**. Use Microsoft Excel to open the file.
- Save the search results as CSV (comma-separated value file): In *Export As*, click **CSV File**. When the *Save As* dialog box appears, click **Save File**, and then click **OK**. You can use any spreadsheet application (such as Microsoft Excel) to open the file.
- Save the results as an AP view: Refer to Creating a Standalone AP View for more information.

Search Using the Search Box

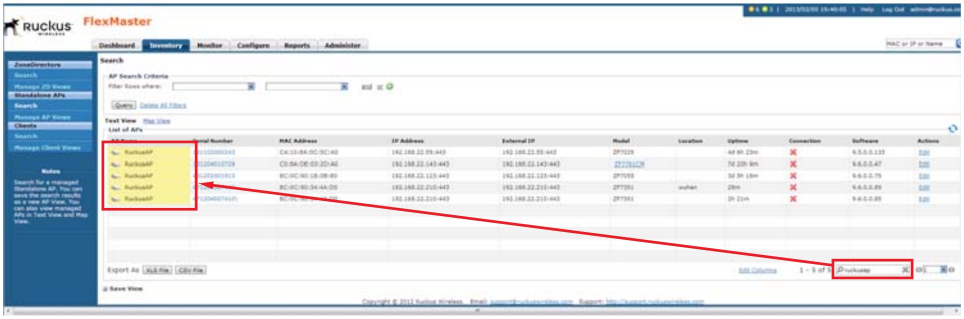
A search box exists at the bottom right area of the *List of APs* section. You can use this search box to search for APs that are directly reporting to FlexMaster.

NOTE: If you save your query parameters as a view, then any new devices that later register with FlexMaster and meet the query criteria are automatically added to the saved view.

1. Type a search string into the box. The search string could be a partial or full string and can consist of numbers or letters or a combination of both.
2. Press **<Enter>** on your keyboard.

FlexMaster searches all its database columns for a match to the string that you entered, and then displays the results in the *List of APs* table. The device property that matches the search string is highlighted in the table.

Figure 59. The device property that matches the search string is highlighted in the search results



AP Name	Serial Number	MAC Address	IP Address	External IP	Model	Location	Uptime	Connection	Software	Actions
RuckusAP	[illegible]	C4:10:8A:0C:5C:A0	192.168.22.55:443	192.168.22.55:443	ZF7025		4d 6h 23m	✗	9.5.0.0.133	Edit
RuckusAP	[illegible]	C0:8A:DE:03:2D:A0	192.168.22.143:443	192.168.22.143:443	ZF7761CM		7d 20h 9m	✗	9.6.0.0.47	Edit
RuckusAP	[illegible]	8C:0C:90:18:0B:80	192.168.22.123:443	192.168.22.123:443	ZF7055		3d 3h 18m	✗	9.6.0.0.75	Edit
RuckusAP	[illegible]	8C:0C:90:34:4A:D0	192.168.22.210:443	192.168.22.210:443	ZF7351	wuhan	28m	✗	9.6.0.0.89	Edit
RuckusAP	[illegible]	[illegible]	192.168.22.210:443	192.168.22.210:443	ZF7351		1h 21m	✗	9.6.0.0.85	Edit

Editing a Standalone AP Tag

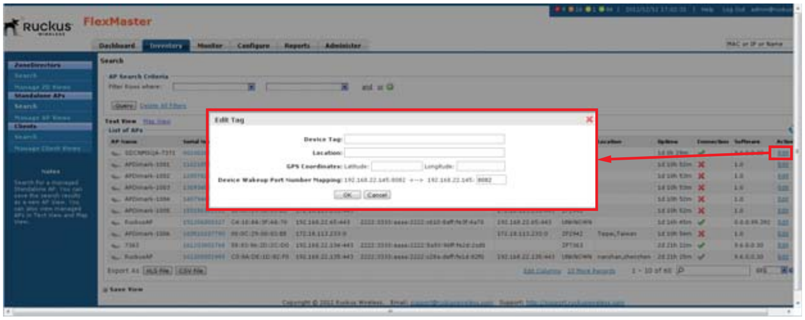
You can edit an AP's tag name, location, GPS coordinates, and wakeup port number mapping (for devices behind a NAT server).

1. On the *List of APs* table, look for the device that you want to edit. When the device that you want to edit does not appear on the table, search for it using the search box.
2. When the device appears, click the **Edit** link that is in the same row as the device name. The *Edit Tag* section appears at the bottom of the page.
3. Edit the tag properties that you want to update. Properties that you can edit include:
   - Standalone AP *device tag* name.
   - *Location* -- Text string that appears in the *Text View* and the *Map View*.
   - *GPS Coordinates (Latitude and Longitude)* -- FlexMaster uses these to position the standalone AP icon on the *Map View*.
   - *Device Wakeup Port Number Mapping* -- Maps the device wakeup port for this standalone AP; normally 8082.

NOTE: If you edit the GPS coordinates from the AP's native Web interface, then the GPS coordinates are synchronized with the FlexMaster database the next time the AP calls home.

4. After you make changes, click **OK**.

Figure 60. Editing standalone AP tag details



Edit Tag

Device Tag:

Location:

GPS Coordinates: Latitude: Longitude:

Device Wakeup Port Number Mapping: 192.168.22.145:8082 <--> 192.168.22.145: 8082

OK Cancel

Creating a Standalone AP View

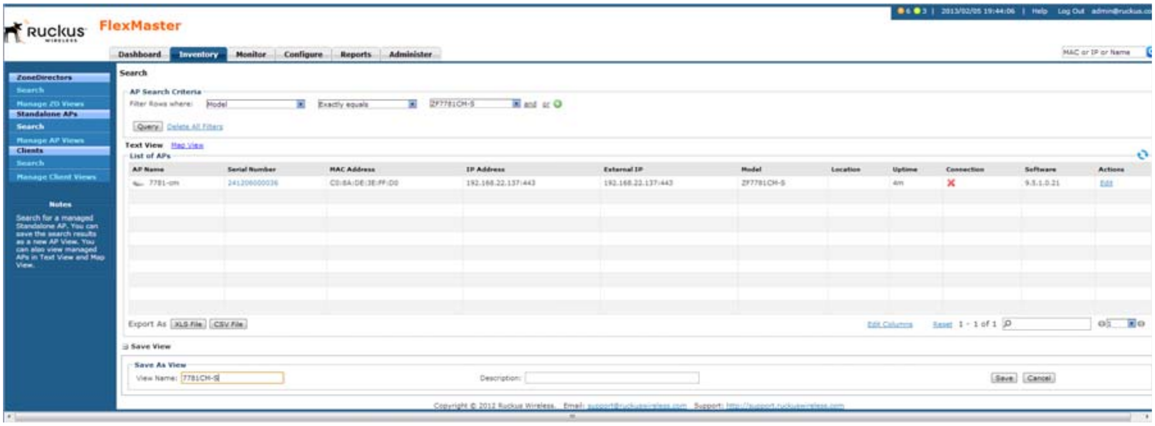
A *view* in FlexMaster is a manually configured grouping of devices with similar characteristics. For example, you can create a view that contains access points (AP) devices of the same model. Views are useful when want to deploy tasks to a group of devices.

A default view called *All Standalone APs*, which contains all APs that reporting directly to FlexMaster, exists. You can create additional or more specific views, depending on your management requirements.

1. Perform a search for clients through one of these search methods
   - Search Using the AP Search Criteria, or
   - Search Using the Search Box
2. When the search results appear, scroll down to the *Save as View* section.
3. In **View Name**, type a name that you want to assign to the view.
4. In **Description**, type a description for the view that you are saving. For example, when the view contains only 7781CM-S AP devices, you can type **`7781CM-Ss`**.
5. Click **Save**.

The *Manage AP Views* page appears, displaying the AP view that you have saved along with other saved AP views.

Figure 61. Creating an AP view that contains only ZF7781CM-S APs



Notes

Search for a managed Standalone AP. You can save the search results as a new AP View. You can also view managed APs in Text View and Map View.

Search

AP Search Criteria

Filter Rows where: Model | Exactly equals | ZF7781CM-S and or

Query Delete All Filters

Text View Map View

List of APs

AP Name	Serial Number	MAC Address	IP Address	External IP	Model	Location	Uptime	Connection	Software	Actions
7781-cm	241206000036	C0:8A:DE:3E:FF:D0	192.168.22.137:443	192.168.22.137:443	ZF7781CM-S		4m	✗	9.5.1.0.21	Edit

Export As XLS File CSV File

Edit Columns Reset 1 - 1 of 1

Save View

Save As View

View Name: 7781CM-S

Description:

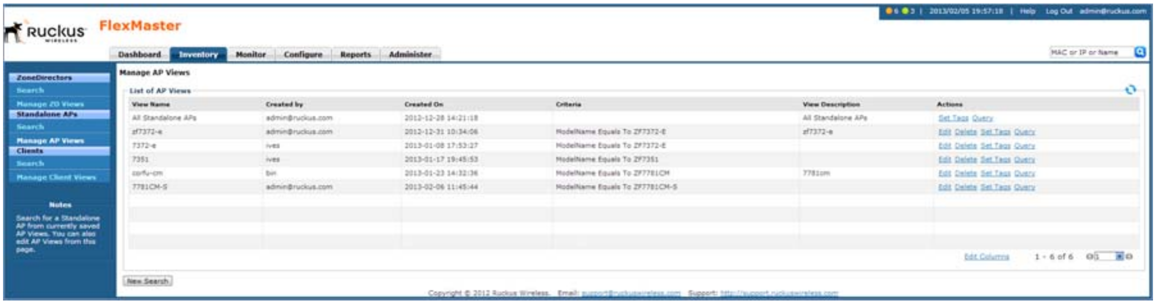
Save Cancel

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Managing Standalone AP Views

Use the *Manage AP Views* page to view list of existing AP views, assign tags to a view, run a query, and edit or delete an AP view.

Figure 62. The Manage AP Views page lists all existing AP views



Search for a Standalone AP from currently saved AP Views. You can also edit AP Views from this page.

Manage AP Views

List of AP Views

View Name	Created by	Created On	Criteria	View Description	Actions
All Standalone APs	admin@ruckus.com	2012-12-28 14:21:18		All Standalone APs	Set Tags Query
zf7372-e	admin@ruckus.com	2012-12-31 10:34:06	ModelName Equals To ZF7372-E	zf7372-e	Edit Delete Set Tags Query
7372-e	ives	2013-01-08 17:53:27	ModelName Equals To ZF7372-E		Edit Delete Set Tags Query
7351	ives	2013-01-17 19:45:53	ModelName Equals To ZF7351		Edit Delete Set Tags Query
corfu-cm	bin	2013-01-23 14:32:36	ModelName Equals To ZF7781CM	7781cm	Edit Delete Set Tags Query
7781CM-S	admin@ruckus.com	2013-02-06 11:45:44	ModelName Equals To ZF7781CM-S		Edit Delete Set Tags Query

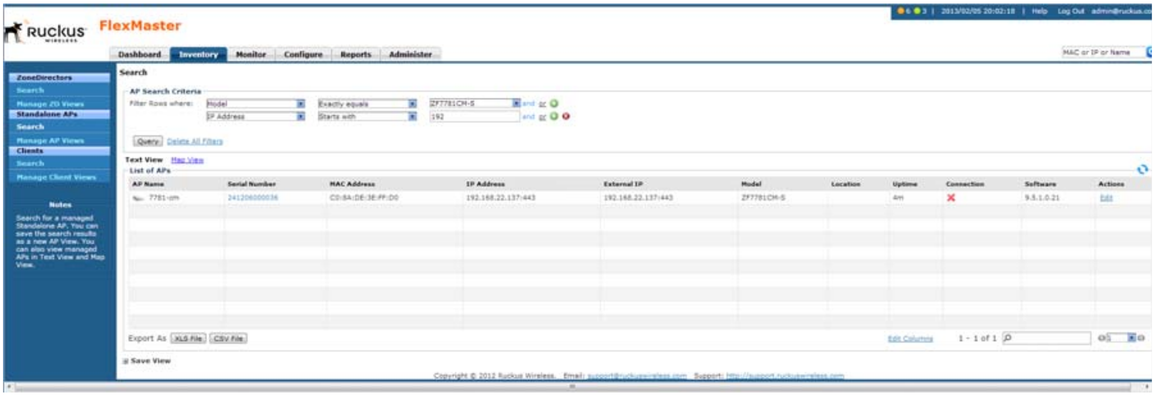
Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Editing an AP View

Editing an AP view is very similar to the process of creating an AP view.

1. Go to *Inventory* > *Standalone APs* > *Manage AP Views.* All existing AP Views appear in the *Manage AP Views* section.
2. Look for the AP view that you want to edit, and then click the AP view **Edit** link. The *Edit View* section appears.
3. Update any of the following to edit the view:
   - The search filter that you configured when you created the view
   - The view name
   - The description
4. To view devices that match the search filter that you updated, click **Query**.
5. To save the changes that you made, click **Update View**.

Figure 63. Editing an AP view



Search for a managed Standalone AP. You can save the search results as a new AP View. You can also view managed APs in Text View and Map View.

Search

AP Search Criteria

Filter Rows where: Model | Exactly equals | ZF7781CM-S and or
IP Address | Starts with | 192 and or

List of APs

AP Name	Serial Number	MAC Address	IP Address	External IP	Model	Location	Uptime	Connection	Software	Actions
7781-cm	241206000036	C0:8A:DE:3E:FF:D0	192.168.22.137:443	192.168.22.137:443	ZF7781CM-S		4m	✗	9.5.1.0.21	Edit

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Deleting an AP View

1. Go to the *Inventory* > *Standalone APs* > *Manage Views* page.
2. Look for the AP view that you want to delete.
3. Click the **Del** link that is in the same row as the view name. A confirmation message appears.
4. Click **OK** to confirm.

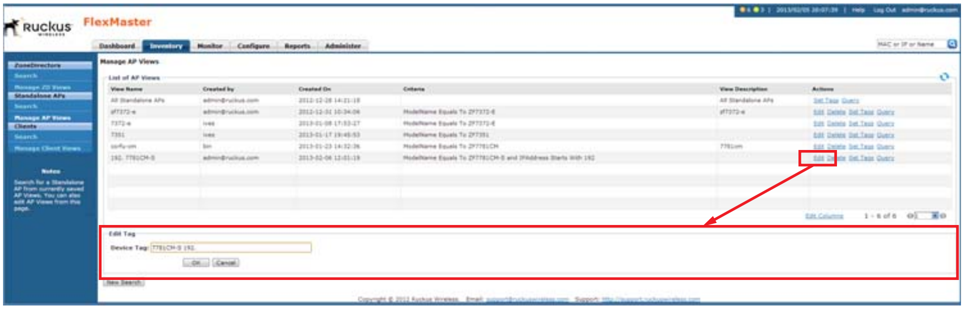
The *Manage Views* page refreshes, and then the view that you deleted disappears from the page.

Setting AP View Device Tags

You can set device tags for all devices included in an existing AP View.

1. Go to the *Inventory* > *Standalone APs* > *Manage Views* page.
2. Look for the to which you want to assign a tag.
3. Click the AP view **Set Tags** link. The *Edit Tag* section appears at the bottom of the page.
4. In **Device Tag**, type the tag name that you want to assign to the AP view devices.
5. Click **OK** to save your changes.

Figure 64. Assigning a device tag to an AP view



Notes
Search for a Standalone AP from currently saved AP Views. You can also edit AP Views from this page.

Manage AP Views

List of AP Views

View Name	Created by	Created On	Criteria	View Description	Actions
All Standalone APs	admin@ruckus.com	2012-12-28 14:21:18		All Standalone APs	Set Tags Query
zf7372-e	admin@ruckus.com	2012-12-31 10:34:06	ModelName Equals To ZF7372-E	zf7372-e	Edit Delete Set Tags Query
7372-e	ivee	2013-01-08 17:53:27	ModelName Equals To ZF7372-E		Edit Delete Set Tags Query
7351	ivee	2013-01-17 19:45:53	ModelName Equals To ZF7351		Edit Delete Set Tags Query
corfu-cm	bin	2013-01-23 14:32:36	ModelName Equals To ZF7781CM	7781cm	Edit Delete Set Tags Query
192. 7781CM-S	admin@ruckus.com	2013-02-06 12:01:19	ModelName Equals To ZF7781CM-S and IPAddress Starts With 192		Edit Delete Set Tags Query

Edit Columns 1 - 6 of 6

Edit Tag

Device Tag: 7781CM-S 192

OK
Cancel
New Search
Copyright © 2013 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Viewing Devices That Belong to an AP View

Use the **Query** link on the *Manage Views* page to display the devices that belong to a view.

1. Go to the *Inventory* > *Standalone APs* > *Manage AP Views* page.
2. Look for the AP view on which you want to run a query.
3. Click the **Query** link that is in the same row as the view name. The Standalone AP *Search* page appears, and then devices that belong to the view appears in the *List of APs* section.

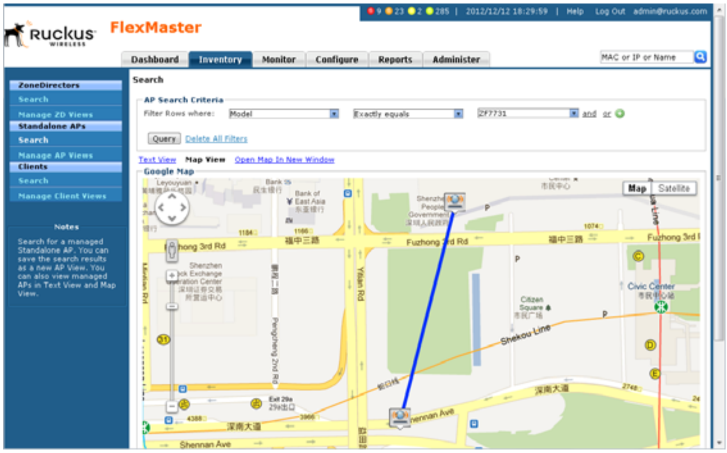
Viewing 7731 Bridge Relationships

When you have ZoneFlex 7731 Bridge devices that are being managed by FlexMaster, you can view the relationships (point-to-point or point-to-multipoint) of these bridge devices on the *Inventory* page.

1. Go to the *Inventory* page.
2. Under *Standalone APs*, click **Search**.
3. In *Filter Rows where*, select the following:
   - First drop-down menu: **Model**
   - Second drop-down menu: **Exactly equals**
   - Third drop-down menu: **ZF7731**
4. Click **Query**. The 7731 devices on the network appear under *List of APs*.
5. Click the **Map View** link to view the locations of the 7731 devices on the map. If the 7731 devices have had GPS coordinates set as described in Editing a Standalone AP Tag, then the map view displays the 7731 devices (denoted by icons) on the map.

The Map View also displays the bridge relationships of these 7731 devices, and can also display the ZoneDirector device (denoted by an icon) to which they report.

Figure 65. The map view shows the relationships of the 7731 Bridge devices



Search for a managed Standalone AP. You can save the search results as a new AP View. You can also view managed APs in Text View and Map View.

Filter Rows where: Model | Exactly equals | ZF7731 | and or

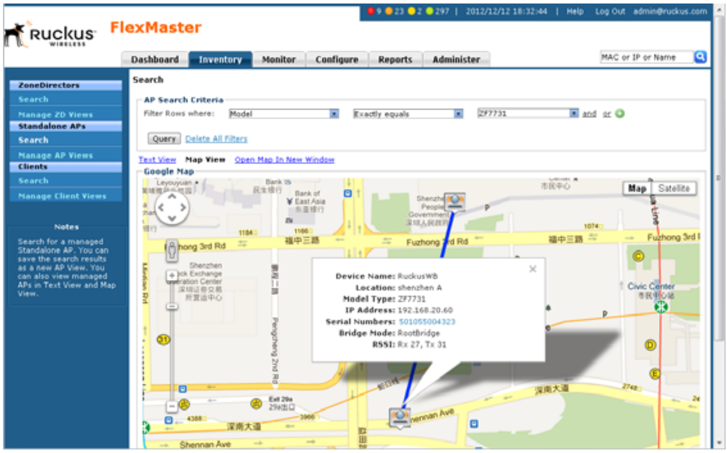
Viewing 7731 AP Bridge Summary Information

To view summary information about a 7731 Bridge device (or any device) that appears on the map, click the icon for the device. A text bubble appears and displays the following information:

- *Device Name*
- *Location*

- *Model Type*
- *IP Address*
- *Serial Numbers*
- *Bridge Mode*
- *RSSI*

Figure 66. Click the device icon to view summary information about the device



Filter Rows where: Model | Exactly equals | ZF7731 and or

Notes

Search for a managed Standalone AP. You can save the search results as a new AP View. You can also view managed APs in Text View and Map View.

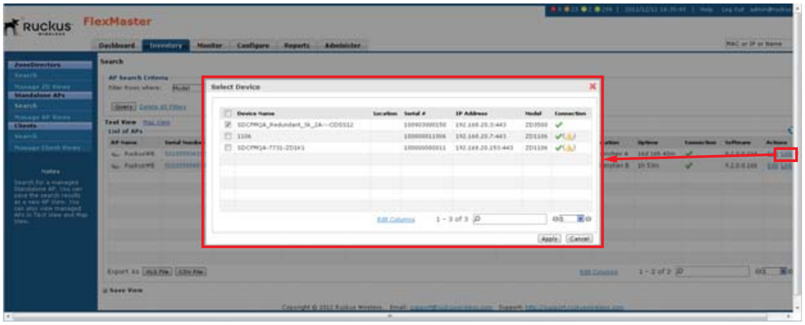
Device Name: RuckusWB
Location: shenzhen A
Model Type: ZF7731
IP Address: 192.168.20.60
Serial Numbers: 501055004323
Bridge Mode: RootBridge
RSSI: Rx 27, Tx 31

Updating the Parent ZoneDirector of a 7731 Bridge Device

You can also update or change the parent ZoneDirector of a 7731 Bridge device from the *Inventory* page.

1. Click the **Text View** link. The 7731 devices that you searched for earlier in Viewing 7731 Bridge Relationships appears on the page. If they are not visible, then run the search for 7731 devices again.
2. Click **Link** (in the *Actions* column) for the 7731 device that you want to update. The *Select Device* page appears, displaying a list of ZoneDirector devices to which the 7731 Bridge could report.
3. Select the check box for the ZoneDirector devices to which you want the 7731 Bridge to report. Before selecting a check box, verify that the ZoneDirector device that you are about to select is online (denoted by ✓ in the *Connection* column).
4. Click **Apply**.

Figure 67. Select the check box for the ZoneDirector device to which you want the 7731 Bridge to report



☐	Device Name	Location	Serial #	IP Address	Model	Connection
☑	SDCPMQA_Redundant_3k_2A---CDS312		100903000150	192.168.20.3:443	ZD3500	✓
☐	1106		100000011006	192.168.20.7:443	ZD1106	✓
☐	SDCPMQA-7731-ZD1K1		100000000011	192.168.20.153:443	ZD1106	✓

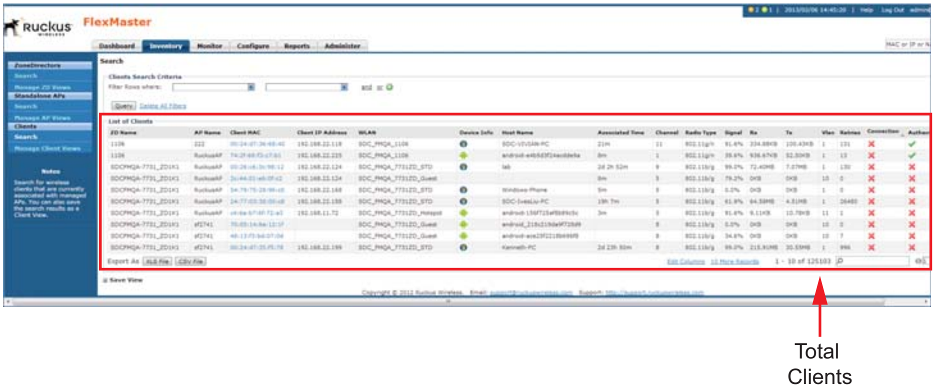
Working with Client Inventory

The Client *Inventory* page displays a list of wireless clients that are associated with APs reporting to managed ZoneDirector devices. It also provides options for searching for specific clients (especially helpful when you have a large number of clients on the network), creating views, and viewing devices in *Text View* and *Map View*.

Viewing a Summary of Clients

To view clients that are associated with clients, click the **Inventory** tab, and then click **Search** under **Clients**. A list of clients appears in the *List of Clients* section. The total number of clients (associated with APs reporting to managed ZoneDirector devices) is indicated below the table, right next to the device search box.

Figure 68. A list of clients appears in the List of Clients section



Search

Clients Search Criteria

Filter Rows where: and or

Search for wireless clients that are currently associated with managed APs. You can also save the search results as a Client View.

List of Clients

ZD Name	AP Name	Client MAC	Client IP Address	WLAN	Device Info	Host Name	Associated Time	Channel	Radio Type	Signal	Rx	Tx	Vlan	Retries	Connection	Authen
1106	222	00:24:d7:36:48:4c	192.168.22.118	SDC_FMQA_1106	●	SDC-VIVIAN-PC	21m	11	802.11g/n	81.6%	334.88KB	100.43KB	1	131	✗	✓
1106	RuckusAP	74:2f:68:f3:c7:61	192.168.22.225	SDC_FMQA_1106	●	android-e4b5d3f24acddeba	8m	1	802.11g/n	38.6%	936.67KB	52.30KB	1	13	✗	✓
SDCFMQA-7731_ZD1K1	RuckusAP	00:26:c6:3c:98:12	192.168.22.124	SDC_FMQA_7731ZD_STD	●	lab	2d 2h 52m	9	802.11b/g	99.0%	72.40MB	7.07MB	1	130	✗	✗
SDCFMQA-7731_ZD1K1	RuckusAP	2c:44:01:eb:0f:c2	192.168.22.124	SDC_FMQA_7731ZD_Guest			8m	5	802.11b/g	79.2%	0KB	0KB	10	0	✗	✗
SDCFMQA-7731_ZD1K1	RuckusAP	54:79:75:28:98:c0	192.168.22.168	SDC_FMQA_7731ZD_STD	●	Windows-Phone	5m	5	802.11b/g	0.0%	0KB	0KB	1	0	✗	✗
SDCFMQA-7731_ZD1K1	RuckusAP	24:77:03:38:00:c8	192.168.22.188	SDC_FMQA_7731ZD_STD	●	SDC-IvesLiu-PC	19h 7m	5	802.11b/g	61.8%	64.59MB	4.31MB	1	26480	✗	✗
SDCFMQA-7731_ZD1K1	RuckusAP	c4:6a:b7:4f:72:a0	192.168.11.72	SDC_FMQA_7731ZD_Hotspot	●	android-156f725af8b89c5c	3m	3	802.11b/g	81.6%	9.11KB	10.78KB	11	1	✗	✗
SDCFMQA-7731_ZD1K1	af2741	70:05:14:8a:12:1f		SDC_FMQA_7731ZD_Guest	●	android_218c219da9f728d9		8	802.11b/g	0.0%	0KB	0KB	10	0	✗	✗
SDCFMQA-7731_ZD1K1	af2741	48:13:f3:8d:07:0d		SDC_FMQA_7731ZD_Guest	●	android-ace23f2218b69bf8		8	802.11b/g	34.8%	0KB	0KB	10	7	✗	✗
SDCFMQA-7731_ZD1K1	af2741	00:24:d7:35:f5:78	192.168.22.199	SDC_FMQA_7731ZD_STD	●	Kenneth-PC	2d 23h 50m	8	802.11b/g	99.0%	215.91MB	30.55MB	1	996	✗	✗

1 - 10 of 125103

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

The *List of Clients* section can show up to 10 clients at a time. If there are more than 10 managed clients on the network, you can view the succeeding pages that list the remaining clients by clicking the left and right arrows at the bottom of the page.

Alternatively, you can also use the search box at the bottom of the page to search for specific clients.

Searching for Clients

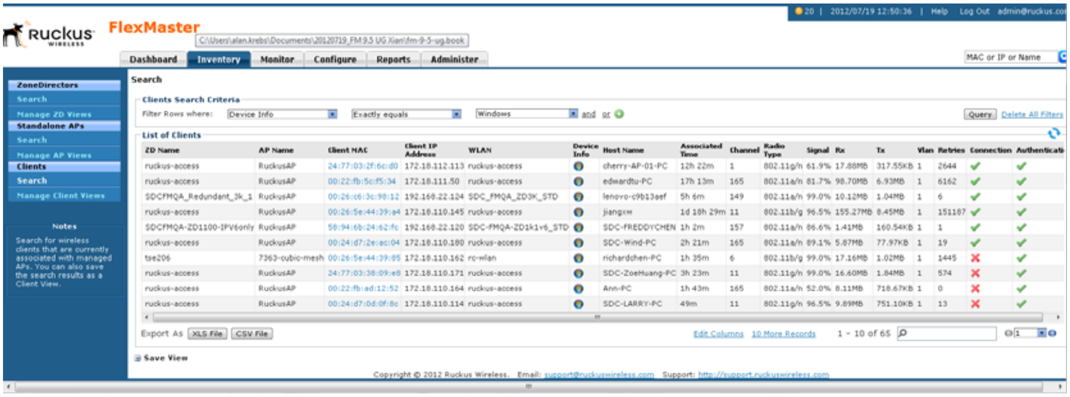
There are two ways to search for clients:

- Search Using the AP Search Criteria
- Search Using the Search Box

Search Using the Client Search Criteria

1. Go to the *Inventory* > *Clients* > *Search*.
2. Go to the *Clients Search Criteria* section. To search for clients, you need to specify the criteria of the devices that you are looking for.

Figure 69. Using Search Criteria to search for a client



Notes

Search for wireless clients that are currently associated with managed APs. You can also save the search results as a Client View.

Search

Clients Search Criteria

Filter Rows where: Device Info | Exactly equals | Windows and or

List of Clients

ZD Name	AP Name	Client MAC	Client IP Address	WLAN	Device Info	Host Name	Associated Time	Channel	Radio Type	Signal	Rx	Tx	Vlan	Retries	Connection	Authenticati
ruckus-access	RuckusAP	24:77:03:2f:6c:d0	172.18.112.113	ruckus-access	●	cherry-AP-01-PC	12h 22m	1	802.11g/n	61.9%	17.88MB	317.55KB	1	2644	✓	✓
ruckus-access	RuckusAP	00:22:fb:5c:f5:34	172.18.111.50	ruckus-access	●	edwardtu-PC	17h 13m	165	802.11a/n	81.7%	98.70MB	6.93MB	1	6162	✓	✓
SDCFMQA_Redundant_3k_1	RuckusAP	00:26:c6:3c:98:12	192.168.22.124	SDC_FMQA_ZD3K_STD	●	lenovo-c9b13aef	5h 6m	149	802.11a/n	99.0%	10.12MB	1.04MB	1	6	✓	✓
ruckus-access	RuckusAP	00:26:5e:44:39:a4	172.18.110.145	ruckus-access	●	jiangxw	1d 18h 29m	11	802.11b/g	96.5%	155.27MB	8.45MB	1	151187	✓	✓
SDCFMQA-ZD1100-IPV6only	RuckusAP	58:94:6b:24:62:fc	192.168.22.120	SDC-FMQA-ZD1k1v6_STD	●	SDC-FREDDYCHEN	1h 2m	157	802.11a/n	86.6%	1.41MB	160.54KB	1	1	✓	✓
ruckus-access	RuckusAP	00:24:d7:2e:ac:04	172.18.110.180	ruckus-access	●	SDC-Wind-PC	2h 21m	165	802.11a/n	89.1%	5.87MB	77.97KB	1	19	✓	✓
tse206	7363-cubic-mesh	00:26:5e:44:39:85	172.18.110.162	rc-wlan	●	richardchen-PC	1h 35m	6	802.11b/g	99.0%	17.16MB	1.02MB	1	1445	✗	✓
ruckus-access	RuckusAP	24:77:03:38:09:e8	172.18.110.171	ruckus-access	●	SDC-ZoeHuang-PC	3h 23m	11	802.11g/n	99.0%	16.60MB	1.84MB	1	574	✗	✓
ruckus-access	RuckusAP	00:22:fb:ad:12:52	172.18.110.164	ruckus-access	●	Ann-PC	1h 43m	165	802.11a/n	52.0%	8.11MB	718.67KB	1	0	✗	✓
ruckus-access	RuckusAP	00:24:d7:0d:0f:8c	172.18.110.114	ruckus-access	●	SDC-LARRY-PC	49m	11	802.11g/n	96.5%	9.89MB	751.10KB	1	13	✗	✓

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

3. In the first drop-down list box after *Filter Rows where,* select the search attribute that you want to use. Options include (parent) ZoneDirector name, AP name, client MAC address, client IP address, WLAN, and channel (among others).
4. In the second drop-down list box, select the search operator that you want to use. Available search operators include:
   - *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **Client IP Address** as the attribute and you entered `172.17.16.176` as the search parameter, then only devices with this IP address appear in the search results.
   - *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **Client IP Address** as the attribute and you entered `100` as the search parameter, then all devices with “100” in the IP address (for example, `172.17.16.`**`100`** and **`100`**`.1.10.13`) appear in the search results.

- *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Client MAC** as the attribute and you entered `00:16` as the query parameter, then only devices with serial numbers that begin with "00:16" (for example, `00:16:ea:49:6e:d8` appear in the search results.
- *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected **Client IP Address** as the attribute and you entered `13` as the query parameter, then only devices with model names that end in "13" (for example, `100.1.10.`**13**) appear in the search results.

After you select a search operator, a third (text) box appears.

5. In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
6. If you want to add another search filter, then click ⊕. A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.
7. When you complete setting up the search filters, click **Query**. FlexMaster displays the devices that match the search criteria.

NOTE: If you save your query parameters as a view, then any new devices that later register with FlexMaster and meet the query criteria are automatically added to the saved view.

Additional Tasks That You Can Perform

After the search results appear, you can perform the following tasks:

- Save the search results as XLS (Microsoft® Excel® file format): In *Export As*, click **XLS File**. When the *Save As* dialog box appears, click **Save File**, and then click **OK**. Use Microsoft Excel to open the file.
- Save the search results as CSV (comma-separated value file): In *Export As*, click **CSV File**. When the *Save As* dialog box appears, click **Save File**, and then click **OK**. You can use any spreadsheet application (such as Microsoft Excel) to open the file.
- Save the results as a client view: Refer to Creating a Client View for more information.

Search Using the Search Box

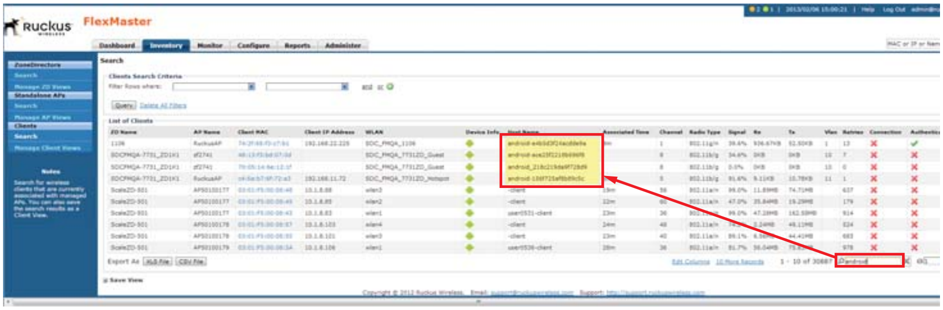
A search box exists at the bottom right area of the *List of Clients* section. You can use this search box to search for clients.

NOTE: If you save your query parameters as a view, then any new devices that later register with FlexMaster and meet the query criteria are automatically added to the saved view.

1. Type a search string into the box. The search string could be a partial or full string and can consist of numbers or letters or a combination of both.
2. Press **<Enter>** on your keyboard.

FlexMaster searches all its database columns for a match to the string that you entered, and then displays the results in the *List of Clients* table. The device property that matches the search string is highlighted in the table. In Figure 70, the search string `android` matched part of a host name and is highlighted in yellow.

Figure 70. The device property that matches the search string is highlighted in the search results



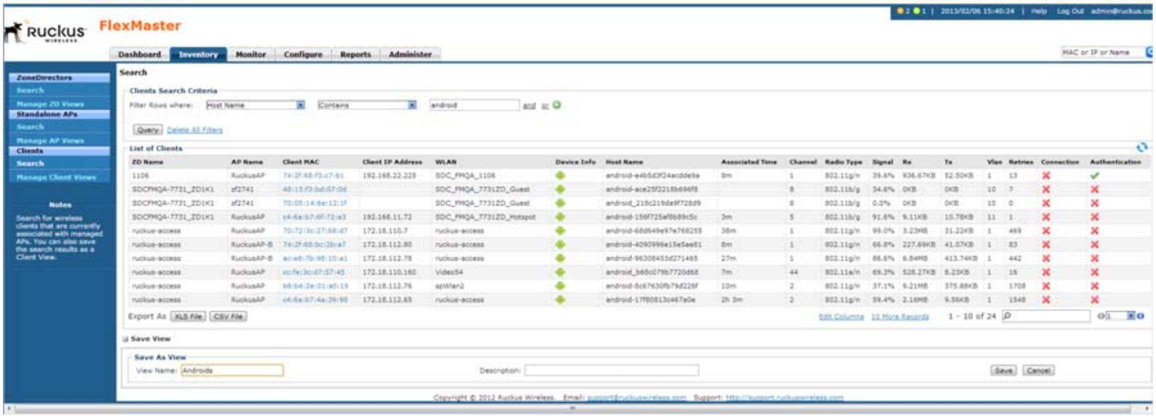
Creating a Client View

A *view* in FlexMaster is a manually configured grouping of devices with similar characteristics. For example, you can create a view that contains clients that belong to the same company department. Views are useful when want to deploy tasks to a group of devices.

1. Perform a search for clients through one of these search methods:
   - Search Using the Client Search Criteria, or
   - Search Using the Search Box
2. When the search results appear, scroll down to the *Save as View* section.
3. In **View Name**, type a name that you want to assign to the view.
4. In **Description**, type a description for the view that you are saving. For example, when the view contains only clients with "android" as a search string, you could enter **Androids**.
5. Click **Save**.

The *Manage Clients Views* page appears, displaying the client view that you have saved along with other saved client views.

Figure 71. Creating a client view that consists of clients where android starts the Host Name



Search

Clients Search Criteria

Filter Rows where: Host Name | Contains | android and or

Query Delete All Filters

List of Clients

ZD Name	AP Name	Client MAC	Client IP Address	WLAN	Device Info	Host Name	Associated Time	Channel	Radio Type	Signal	Rx	Tx	Vlan	Retries	Connection	Authentication
1106	RuckusAP	74:2f:68:f3:c7:61	192.168.22.225	SDC_FMQA_1106	●	android-e4b5d3f24acdde9a	8m	1	802.11g/n	39.6%	936.67KB	52.50KB	1	13	✗	✓
SDCFMQA-7731_ZD1K1	zf2741	48:13:f3:bd:07:0d		SDC_FMQA_7731ZD_Guest	●	android-ace25f2218b696f8		8	802.11b/g	34.6%	0KB	0KB	10	7	✗	✗
SDCFMQA-7731_ZD1K1	zf2741	70:05:14:6e:12:1f		SDC_FMQA_7731ZD_Guest	●	android_218c219da9f728d9		8	802.11b/g	0.0%	0KB	0KB	10	0	✗	✗
SDCFMQA-7731_ZD1K1	RuckusAP	c4:6a:b7:6f:72:a3	192.168.11.72	SDC_FMQA_7731ZD_Hotspot	●	android-156f725af8b89c5c	3m	5	802.11b/g	91.6%	9.11KB	10.78KB	11	1	✗	✗
ruckus-access	RuckusAP	70:72:3c:27:68:d7	172.18.110.7	ruckus-access	●	android-68d649e97e768255	38m	1	802.11g/n	99.0%	3.23MB	31.22KB	1	469	✗	✗
ruckus-access	RuckusAP-B	74:2f:68:bc:2b:a7	172.18.112.80	ruckus-access	●	android-4090996e15e5ae81	8m	1	802.11g/n	66.8%	227.69KB	41.07KB	1	83	✗	✗
ruckus-access	RuckusAP-B	ac:e8:7b:98:10:a1	172.18.112.78	ruckus-access	●	android-96308453d271465	27m	1	802.11g/n	86.6%	6.84MB	413.74KB	1	442	✗	✗
ruckus-access	RuckusAP	cc:fe:3c:d7:57:45	172.18.110.160	Video54	●	android_b68c079b7720d68	7m	44	802.11a/n	69.3%	528.27KB	8.23KB	1	16	✗	✗
ruckus-access	RuckusAP	b8:b4:2e:01:a0:19	172.18.112.76	apWlan2	●	android-8c67630fb79d226f	10m	2	802.11g/n	37.1%	9.21MB	375.88KB	1	1708	✗	✗
ruckus-access	RuckusAP	c4:6a:b7:4a:39:98	172.18.112.65	ruckus-access	●	android-17f80813c467a0e	2h 3m	2	802.11g/n	59.4%	2.16MB	9.56KB	1	1548	✗	✗

Export As XLS File CSV File Edit Columns 10 More Records 1 - 10 of 24

Save View

Save As View

View Name: Androids Description:

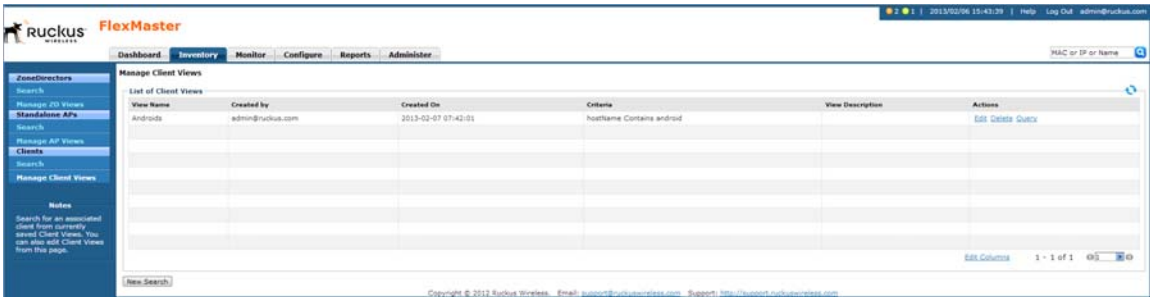
Save Cancel

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Managing Client Views

Use the *Manage Client Views* page to view list of existing client views, run a query, and edit or delete a view.

Figure 72. The Manage Client View page lists all existing client views



Notes

Search for an associated client from currently saved Client Views. You can also edit Client Views from this page.

Manage Client Views

List of Client Views

View Name	Created by	Created On	Criteria	View Description	Actions
Androids	admin@ruckus.com	2013-02-07 07:42:01	hostName Contains android		Edit Delete Query

Viewing Clients That Belong to a View

Use the **Query** link on the *Manage Views* page to display clients that belong to a view.

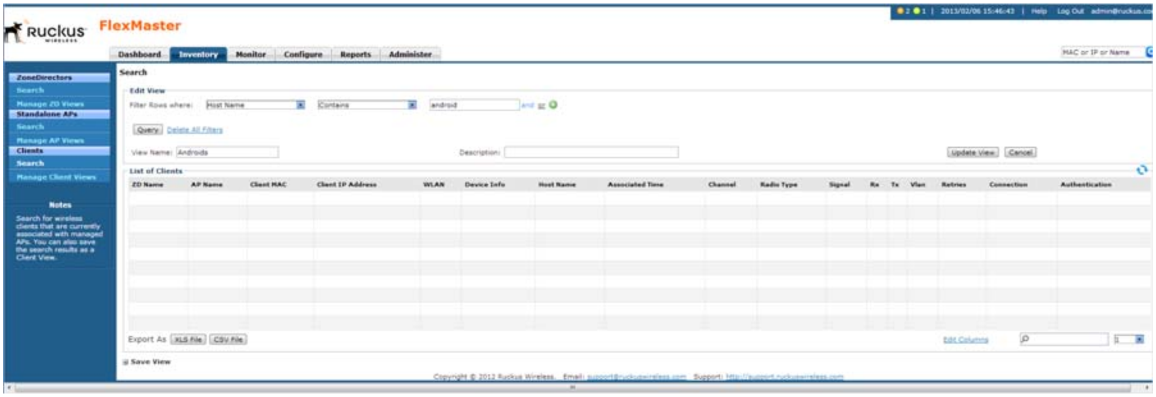
1. Go to the *Inventory* > *Clients* > *Manage Client Views* page.
2. Look for the client view on which you want to run a query.
3. Click the **Query** link that is in the same row as the view name. The Client *Search* page appears, and then clients that belong to the view appears in the *List of Clients* section.

Editing a Client View

Editing a client view is very similar to the process of creating a client view.

1. Go to the *Inventory* > *Clients* > *Manage Client Views* page. All existing client views appear in the *Manage Client Views* section.
2. Look for the client view that you want to edit, and then click the **Edit** link that is in the same row as the client view name. The *Edit View* section appears.

Figure 73. Editing a client view



Edit View

Filter Rows where: Host Name | Contains | android

View Name: Androids

Description:

3. Update any of the following to edit the view:
   - The search filter that you configured when you created the view
   - The view name
   - The description
4. To view devices that match the search filter that you updated, click **Query**.
5. To save the changes that you made, click **Update View**.

Deleting a Client View

1. Go to the *Inventory* > *Clients* > *Manage Client Views* page.
2. Look for the client view that you want to delete.
3. Click the **Delete** link that is in the same row as the view name. A confirmation message appears.
4. Click **OK** to confirm.

The *Manage Client Views* page refreshes, and then the view that you deleted disappears from the page.

5

Managing a Single Standalone Access Point

In This Chapter:

NOTE: Unlike standalone APs, ZoneDirector devices do not have a Device View. Clicking a ZoneDirector device's serial number opens its native Web interface, instead of Device View.

Device View

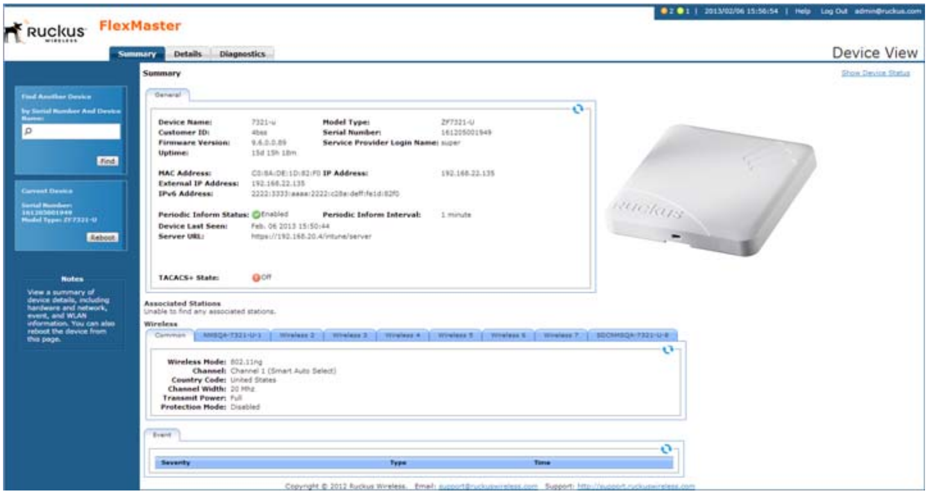
When you click a standalone AP's serial number link on any page of the FlexMaster Web interface, a new window called *Device View* appears. Device View allows you to manage a single standalone AP without having to provision tasks.

NOTE: If the Ruckus Wireless AP is behind a firewall/NAT device, then ports 49 (TACACS+ port) and 8082 (default AP wakeup port) may need to be forwarded through the firewall/NAT device for FM to communicate with the standalone AP. For more information, refer to Firewall Ports that Must be Open for Communications.

NOTE: To manage a Ruckus Wireless AP with FlexMaster, the management server URL must be configured on the AP. The default URL is https://flexmaster/intune/server.

To change the URL, a provisioning template must be used. Another way to configure this URL is from the device's embedded Web management user interface. For more information, refer to Ensuring That APs Can Connect to FlexMaster.

Figure 74. The AP Device View opens in a new browser window



Current Device
Serial Number: 161205001949
Model Type: ZF7321-U

Notes
View a summary of device details, including hardware and network, event, and WLAN information. You can also reboot the device from this page.

Summary

Device Name: 7321-u
Customer ID: 4bes
Firmware Version: 9.6.0.0.89
Uptime: 15d 15h 18m
Model Type: ZF7321-U
Serial Number: 161205001949
Service Provider Login Name: super

MAC Address: C0:8A:DE:1D:82:F0
IP Address: 192.168.22.135
External IP Address: 192.168.22.135
IPv6 Address: 2222:3333:aaaa:2222:c28a:deff:fe1d:82f0

Periodic Inform Status: ● Enabled
Periodic Inform Interval: 1 minute
Device Last Seen: Feb. 06 2013 15:50:44
Server URL: https://192.168.20.4/intune/server

TACACS+ State: ● Off

Associated Stations
Unable to find any associated stations.

Wireless

Wireless Mode: 802.11ng
Channel: Channel 1 (Smart Auto Select)
Country Code: United States
Channel Width: 20 Mhz
Transmit Power: Full
Protection Mode: Disabled

Severity	Type	Time

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

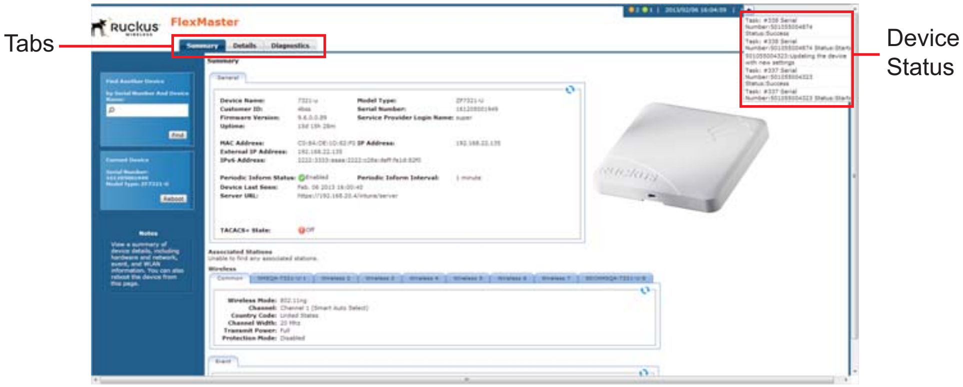
Device View Tabs and Status Boxes

The Device View contains three tabs that you can use to view information about the standalone AP, configure its settings, and run diagnostic tests on it. The following table lists the tabs that are available on the *Device View.*

Table 19. Tabs on the Device View

Tab Name	Description
Summary	Displays information about the device, including its system settings, available SSIDs, and associated clients. For more information, refer to Viewing Device Summary.
Details	Displays network configuration information and provides options for editing these settings. For more information, refer to Viewing and Editing Device Details.
Diagnostics	Provides options for running a PING test from the device and for viewing logs. For more information, refer to Performing Device Diagnostics.

Figure 75. Typical ZoneFlex Device View



There is also a status box located in the lower-left corner of the page. The status box displays statuses related to device operations. For example, when you apply a provisioning task to the device, the task number and task status appear in this box.

This status box is hidden by default. To display the box, click the **Show Device Status** link at the top-right corner of the page. The device status is updated every 30 seconds to present the most up-to-date device information. If a device change is in progress, then this status box displays the requested change and the user who initiated the change.

Viewing Device Summary

The *Summary* tab offers a quick look at general details of the device, including a picture of the device, the device name, IP address, and available SSIDs. The following table lists the tasks that you can perform on the *Summary* tab.

Table 20. Tasks you can perform on the Summary tab

Task	How To Do It
Find another device	In the *Find Another Device* box in the upper left corner of the page, type the serial number or MAC address of another device, and then click **Find** to find matching devices.
Reboot the device	Under *Current Device*, click **Reboot** to reboot the device.
View device details	(Default View) Shows a picture of the device model and high-level device details.
View device events	Clicking the **Events** tab opens a summary of device events.
NOTE: *Some APs have two built-in radios. In those Summary pages, details are shown for the two radios.*	

Viewing Statistics for Cable Modems

The Device View for Ruckus Wireless APs with cable modems, such as for the ZF7761-CM and ZF7781-CM Cable Modem APs, displays basic cable modem information. This basic cable modem information includes:

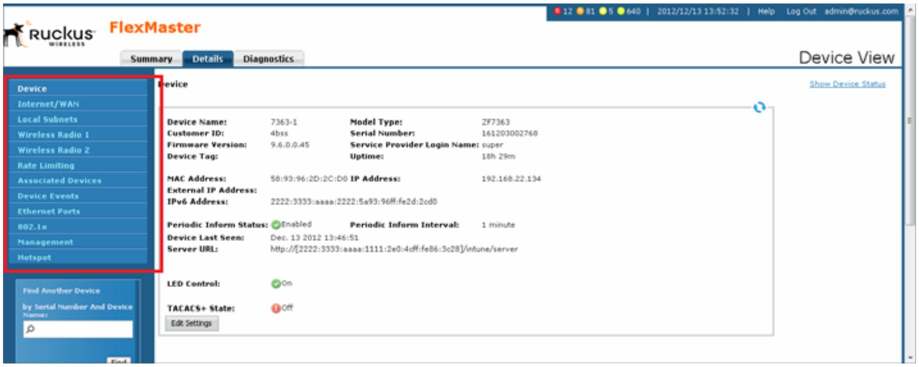
- MAC address
- Software version
- WAN IP address
- Uptime
- Connection status
- Downstream channel information
- Upstream channel information

Viewing and Editing Device Details

The **Details** tab provides view/edit capabilities on the specific settings of the selected device (options vary depending on Ruckus Wireless device type).

For each left-side menu option you click in the *Details* tab, the page that displays is a view-only static view of the details for that option. Click the **Edit Settings** button to edit option details.

Figure 76. Typical Details Menu Options



Device

Device Name: 7363-1
Customer ID: 4bss
Firmware Version: 9.6.0.0.45
Device Tag:
Model Type: ZF7363
Serial Number: 161203002768
Service Provider Login Name: super
Uptime: 18h 29m

MAC Address: 58:93:96:2D:2C:D0
External IP Address:
IPv6 Address: 2222:3333:aaaa:2222:5a93:96ff:fe2d:2cd0
IP Address: 192.168.22.134

Periodic Inform Status: ✓ Enabled
Periodic Inform Interval: 1 minute
Device Last Seen: Dec. 13 2012 13:46:51
Server URL: http://[2222:3333:aaaa:1111:2e0:4cff:fe86:3c28]/intune/server

LED Control: ✓ On

TACACS+ State: ! Off

Edit Settings

NOTE: Managed devices allow you to configure many advanced features and functions, such as 802.1x rate limiting. Please refer to the associated device *User Guide* for configuration instructions.

Note the following FlexMaster-related parameters on the *Details > Device* page:

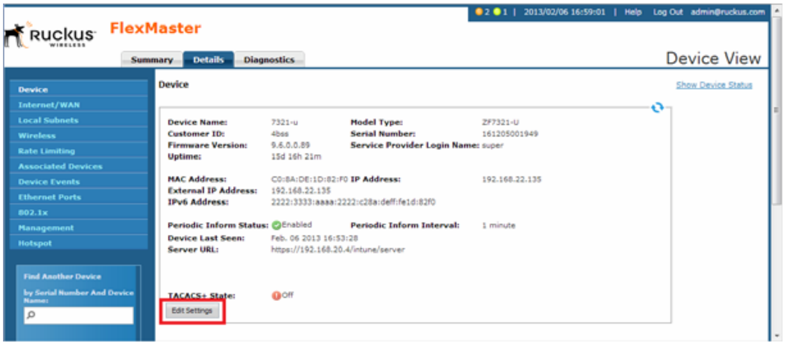
- Periodic Inform Status: Status of the Periodic Inform feature
- Server URL: the URL of FlexMaster
- Periodic Inform Interval: the interval at which the device "calls home" to FlexMaster
- Associated Clients Monitoring Mode (some APs): when enabled, the device periodically sends information on associated clients to FlexMaster

NOTE: Managed devices attempt to contact FlexMaster at the specified inform interval. When an AP is unable to contact FlexMaster after one hour, then it automatically extends the periodic inform interval by a random number of minutes.

For example, if you set the inform interval to 5 minutes and the AP is unable to contact FlexMaster, then it may extend the inform interval to 15 minutes. The AP continues to extend the interval until it is able to contact FlexMaster successfully (in which case the periodic inform interval reverts to the original setting) or it stops attempting to contact FlexMaster.

NOTE: On ZoneFlex 7942 and 7811 APs, the radio channel is not configurable on the *Device View* page of FlexMaster; the only option that appears is **SmartSelect**. To ensure that the AP is using an authorized radio channel, make sure that you select the correct country code and the correct wireless mode.

Figure 77. To change the device settings, click Edit Settings



Device

Device Name: 7321-u
Model Type: ZF7321-U
Customer ID: 4bss
Serial Number: 161205001949
Firmware Version: 9.6.0.0.89
Service Provider Login Name: super
Uptime: 15d 16h 21m

MAC Address: C0:8A:DE:1D:82:F0
IP Address: 192.168.22.135
External IP Address: 192.168.22.135
IPv6 Address: 2222:3333:aaaa:2222:c28a:deff:fe1d:82f0

Periodic Inform Status: Enabled
Periodic Inform Interval: 1 minute
Device Last Seen: Feb. 06 2013 16:53:28
Server URL: https://192.168.20.4/intune/server

TACACS+ State: Off

NOTE: For all **Device View** > **Details** configuration options, refer to the user guide for the Ruckus Wireless device.

Configuring Replacement Options for ZoneFlex 7731 Wireless Bridge

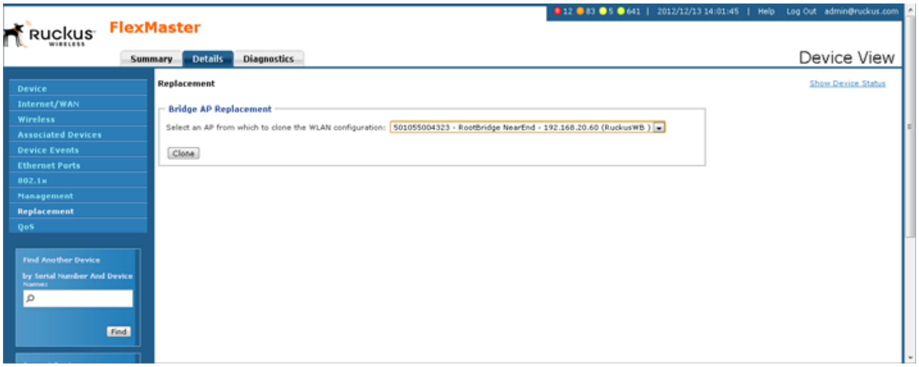
When you have a pair of ZoneFlex 7731 Wireless Bridge devices being managed by FlexMaster and one of them needs to be replaced (for example, it is experiencing hardware issues), you can export the settings of the Wireless Bridge to a replacement easily from the Device View.

NOTE: This option is only available on the Device View of ZoneFlex 7731 Wireless Bridge.

Follow these steps to export or clone the settings of a 7731 Wireless Bridge to a replacement unit.

1. Register the new ZoneFlex 7731 Wireless Bridge (replacement unit) with FlexMaster.
2. Access the *Device View* of the new ZoneFlex 7731 Wireless Bridge.
3. Click the **Details** tab, and then click the **Replacement** option on the left-side menu.
4. In *Select one AP to clone WLAN configurations*, select the wireless bridge that you are replacing.
5. Click **Clone**. FlexMaster queries its database for the settings of wireless bridge for replacement, and them copies them to the replacement unit.

Figure 78. The Replacement page for ZoneFlex 7731 Wireless Bridge



Select an AP from which to clone the WLAN configuration: 501055004323 - RootBridge NearEnd - 192.168.20.60 (RuckusWB)

When the settings have been copied successfully to the replacement unit, the status window notifies you that the process has been completed.

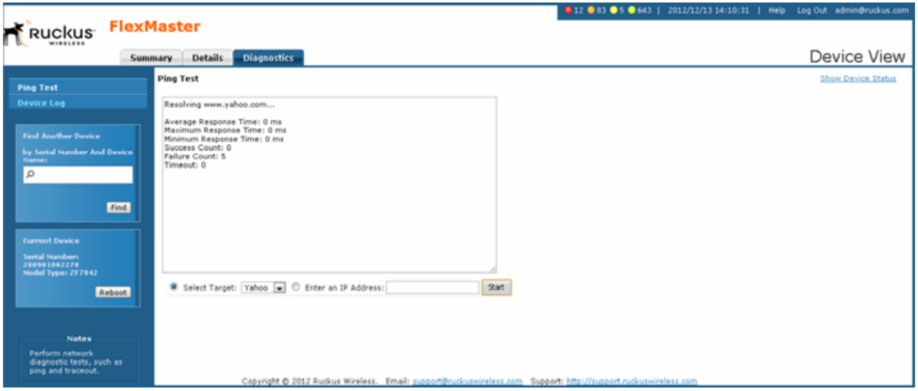
Performing Device Diagnostics

The **Diagnostics** tab enables you to perform a ping test (to test connectivity) and to retrieve the device's system log.

Running a Ping Test

Click the **Select Target** option and toggle the provided target (Yahoo or Google) from the drop-down list, or click the **Enter an IP address** option and enter an IP address in the accompanying text field. Ping the destination address by clicking **Start**. When the test is completed, FlexMaster displays the results in the *Ping Test* box.

Figure 79. Typical ping test



Ping Test

```
Resolving www.yahoo.com....

Average Response Time: 0 ms
Maximum Response Time: 0 ms
Minimum Response Time: 0 ms
Success Count: 0
Failure Count: 5
Timeout: 0
```

● Select Target: Yahoo ○ Enter an IP Address:

Current Device
Serial Number: 200901002270
Model Type: ZF7942

Perform network diagnostic tests, such as ping and traceout.

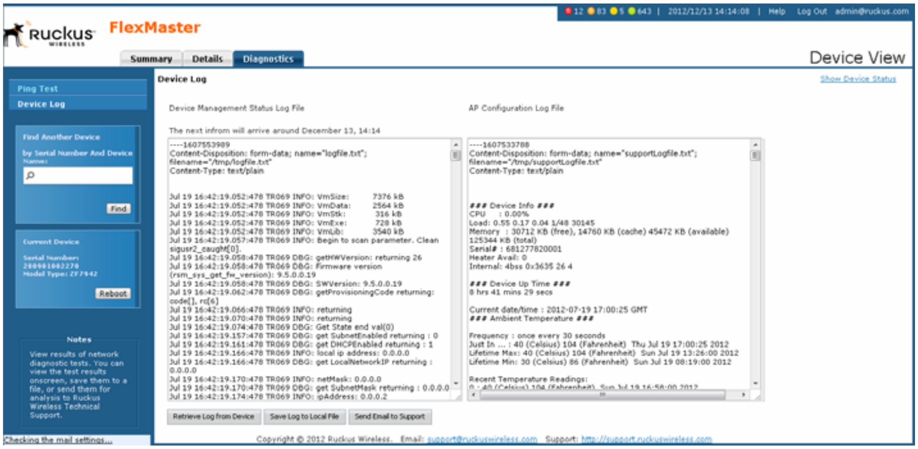
Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Viewing the Device Log

Click the left-hand menu **Device Log** option to have FlexMaster display the *Device Log* page. On the *Device Log* page:

1. click **Retrieve Log from Device** to retrieve the device's log,
2. and then click **Save Log to Local File** to save it to your client,
3. and/or click **Send Email to Support** to email it to Ruckus Wireless Technical Support.

Figure 80. The Device Log page



View results of network diagnostic tests. You can view the test results onscreen, save them to a file, or send them for analysis to Ruckus Wireless Technical Support.

Device Log

Device Management Status Log File

The next infrom will arrive around December 13, 14:14

```
----1607553989
Content-Disposition: form-data; name="logfile.txt";
filename="/tmp/logfile.txt"
Content-Type: text/plain


Jul 19 16:42::19.052:478 TR069 INFO: VmSize:        7376 kB
Jul 19 16:42::19.052:478 TR069 INFO: VmData:        2564 kB
Jul 19 16:42::19.052:478 TR069 INFO: VmStk:          316 kB
Jul 19 16:42::19.052:478 TR069 INFO: VmExe:          728 kB
Jul 19 16:42::19.052:478 TR069 INFO: VmLib:         3540 kB
Jul 19 16:42::19.057:478 TR069 INFO: Begin to scan parameter. Clean
sigusr2_caught[0].
Jul 19 16:42::19.058:478 TR069 DBG: getHWVersion: returning 26
Jul 19 16:42::19.058:478 TR069 DBG: Firmware version
(rsm_sys_get_fw_version): 9.5.0.0.19
Jul 19 16:42::19.058:478 TR069 DBG: SWVersion: 9.5.0.0.19
Jul 19 16:42::19.062:478 TR069 DBG: getProvisioningCode returning:
code[], rc[6]
Jul 19 16:42::19.066:478 TR069 INFO: returning
Jul 19 16:42::19.070:478 TR069 INFO: returning
Jul 19 16:42::19.074:478 TR069 DBG: Get State end val(0)
Jul 19 16:42::19.157:478 TR069 DBG: get SubnetEnabled returning : 0
Jul 19 16:42::19.161:478 TR069 DBG: get DHCPEnabled returning : 1
Jul 19 16:42::19.166:478 TR069 INFO: local ip address: 0.0.0.0
Jul 19 16:42::19.166:478 TR069 DBG: get LocalNetworkIP returning :
0.0.0.0
Jul 19 16:42::19.170:478 TR069 INFO: netMask: 0.0.0.0
Jul 19 16:42::19.170:478 TR069 DBG: get SubnetMask returning : 0.0.0.0
Jul 19 16:42::19.174:478 TR069 INFO: ipAddress: 0.0.0.2
```

AP Configuration Log File

```
----1607533788
Content-Disposition: form-data; name="supportLogfile.txt";
filename="/tmp/supportLogfile.txt"
Content-Type: text/plain



### Device Info ###
CPU      : 0.00%
Load: 0.55 0.17 0.04 1/48 30145
Memory  : 30712 KB (free), 14760 KB (cache) 45472 KB (available)
125344 KB (total)
Serial# : 681277820001
Heater Avail: 0
Internal: 4bss 0x3635 26 4

### Device Up Time ###
8 hrs 41 mins 29 secs

Current date/time : 2012-07-19 17:00:25 GMT
### Ambient Temperature ###

Frequency : once every 30 seconds
Just In ... : 40 (Celsius) 104 (Fahrenheit)  Thu Jul 19 17:00:25 2012
Lifetime Max: 40 (Celsius) 104 (Fahrenheit)  Sun Jul 19 13:26:00 2012
Lifetime Min: 30 (Celsius) 86 (Fahrenheit)  Sun Jul 19 08:19:00 2012

Recent Temperature Readings:
0 : 40 (Celsius) 104 (Fahrenheit)  Sun Jul 19 16:58:00 2012
```

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

FlexMaster retrieves two types of logs from the device:

- *Device Management Status Log File*: Shows communication logs between FlexMaster and the device. This is the same log information that appears on the device's *Administer > Log* page.
- *AP Configuration Log File*: Shows the device's system information and its current network, wireless, and system settings. This is the same log information that appears on the device's *Support Info* page.

NOTE: Attempts to retrieve device logs from APs running on earlier software versions time out. Ruckus Wireless recommends upgrading all FlexMaster managed APs to the latest version to retrieve logs successfully.

NOTE: When you are retrieving logs from a managed AP that is behind a NAT server and you have not configured L2TP, FlexMaster is unable to wake up AP and retrieve logs.

NOTE: When a managed AP is behind a NAT server and you click the Retrieve Log from Device button, FlexMaster is able to retrieve the log from the managed AP only at the next inform interval. To determine if a managed AP is behind a NAT server, then go to the *Summary* tab and check if the following message appears at the bottom of the page: **This device is not directly reachable; it might be offline or behind a firewall.*

6

Provisioning Tasks to Managed Devices

In This Chapter:

About Provisioning Tasks

Provisioning is creating tasks that update the configuration, upgrade the firmware, or reboot a group (one or more) of your managed Ruckus Wireless devices according to a schedule. These tasks allow you to manage the provisioning of all or a subset of devices based on requirements such as change management rules, geographical locations, time zones, and more.

As FlexMaster can manage many Ruckus Wireless devices, creating configuration or upgrade tasks to configure or upgrade multiple sets of devices at a time consolidates and simplifies deployment and management of your devices.

To perform provisioning, click the **Configure** tab on the Web interface, and then create or deploy provisioning tasks to target device views. Some examples of provisioning tasks include:

- Configuring the settings of standalone APs
- Resetting standalone APs to factory default
- Configuring the settings of ZoneDirector devices
- Backing up the settings of a ZoneDirector device
- Upgrade the firmware of specific ZoneDirector or standalone AP models
- Managing device registration settings

Provisioning Conventions and Recommended Practices

The following conventions and best practices are common across all options on the *Configure* tab:

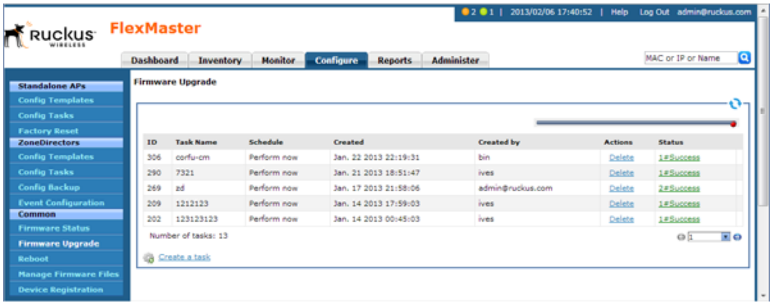
- Configuration Upgrade, Firmware Upgrade, Reboot and Factory Reset tasks are assigned to device views. For each of these tasks, you can select from either of the two default devices views or any device view that you have created.
- If your Change Management Policy or Service Level Agreement (SLA) calls for particular days and times of the week/month when service can be momentarily disrupted for maintenance purposes, then you may want to schedule Configure tasks during such a time.

NOTE: When scheduling tasks, make sure that there is adequate time interval between tasks that target the same devices. For example, when you are provisioning a firmware upgrade or reboot task for a device view and you have another task that target the same view, schedule the second task in a way that allows for the upgrade or reboot process to complete first. Otherwise, the second task fails or expires.

Understanding the Status of a Task

When you deploy a configuration upgrade, firmware upgrade, or reboot task, the task status appears in the task table, in the *Status* column. Check this column to determine if the task that you deployed has been completed successfully.

Figure 81. The task status column on the Firmware Upgrade page



Firmware Upgrade

ID	Task Name	Schedule	Created	Created by	Actions	Status
306	corfu-cm	Perform now	Jan. 22 2013 22:19:31	bin	Delete	1#Success
290	7321	Perform now	Jan. 21 2013 18:51:47	ives	Delete	1#Success
269	zd	Perform now	Jan. 17 2013 21:58:06	admin@ruckus.com	Delete	2#Success
209	1212123	Perform now	Jan. 14 2013 17:59:03	ives	Delete	1#Success
202	123123123	Perform now	Jan. 14 2013 00:45:03	ives	Delete	1#Success

Number of tasks: 13

Create a task

Task status is shown in the format `{number}#{status}`, where:

- `{number}` indicates the number of devices that have this status
- `{status}` indicates the outcome of the task

Note that when the task is being provisioned to multiple devices, multiple tasks statuses can appear in the *Status* column. When you provision a reboot task to 10 APs, for example, and this task succeeded on 8 APs but failed on 2 APs, you see the following statuses (hyperlinks):

```
8#Success 2#Failed
```

Clicking the link opens a table below that lists details about the task, including its target devices, their serial numbers, and their model names (among others).

The following table lists all possible task statuses that can appear in the *Status* column.

Table 21. Task status descriptions

Task Status	Description
Started	The task has started successfully on these devices. When it is a scheduled task, this status indicates that the task has been triggered because the run schedule has arrived.
Applied	The task has been applied on these devices. FlexMaster is retrieving the status on the devices (success or fail). When this is a firmware upgrade task, the next successful status is Downloaded (see below).
Downloaded	Applies only to firmware upgrade tasks. The status indicates that the firmware has already been downloaded on these devices. Note that, at this point, the firmware has not been installed yet.

Table 21. Task status descriptions (Continued)

Task Status	**Description**
Expired	The task expired on these devices. Task expiration occurs when FlexMaster is unable to provision that task to a target device (for any reason, including the device being offline) after three (3) inform intervals. To restart this task on the devices that expired, click the **Restart** link in the *Actions* column.
Cancelled	The scheduled task has been cancelled.
Success	The task has completed successfully.
Failed	The task failed because these devices did not respond to FlexMaster. To see which target devices failed to complete the task, click the failed status link. To restart this task on the devices that failed, click the **Restart** link in the *Actions* column.

Provisioning Tasks to Standalone APs

This section describes AP configuration templates and how you can use them to define the settings that you want to deploy to a group of APs.

Working with AP Configuration Templates

Configuration templates allow you to provision changes in bulk to a group of devices. Attributes, such as SSIDs, login info, and L2TP settings, can be applied in bulk by simply deploying a configuration template. For example, you can change the SSIDs or L2TP settings of a group of ZoneFlex 2942 APs.

Configuration templates are a useful way to ensure all or a subset of managed devices share the same configuration. For instance, you may not want all devices to have the same login information, but you may want them to have the same wireless settings.

Provisioning configuration is a two-step process. First, in Creating an AP Configuration Template, you select the parameters and corresponding values to configure. Once you have created the configuration template, you can then provision the settings within that template to multiple managed devices via the configuration task (refer to Creating an AP Configuration Task). Once a template's settings have been provisioned to a device, those parameters override previous device settings, but can be changed in the future from either the device's Web interface or from FlexMaster.

Creating an AP Configuration Template

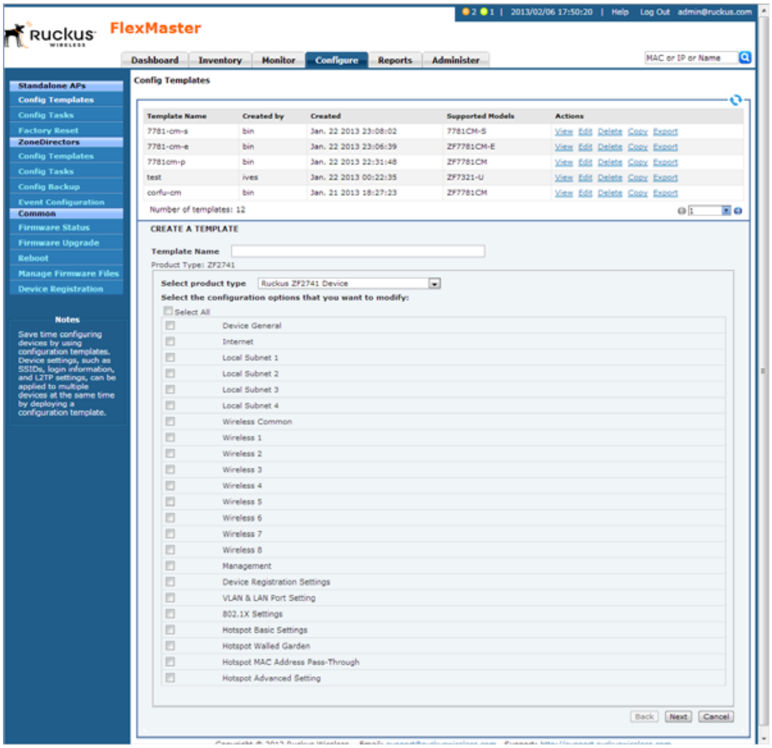
NOTE: Provisioning settings to some APs that are running software version 5.1 or earlier may be unsuccessful. To help ensure successful provisioning to all APs, Ruckus Wireless strongly recommends upgrading all FlexMaster managed devices to the latest software version.

NOTE: If you need to provision wireless settings to ZoneFlex 2942 APs running software version 5.1, then you must configure the wireless settings for BSSID 1 to BSSID 4 only in the configuration template (leave the settings for BSSIDs 5 to 8 blank). Although the current FlexMaster configuration template supports BSSID 1 to BSSID 8, provisioning to ZoneFlex 2942 APs is unsuccessful if you configure BSSIDs 5 to 8.

NOTE: When you create configuration templates, and then upgrade your FlexMaster server to a newer version, some of the templates that you created using the previous version may no longer provision successfully. To help ensure successful provisioning, recreate the templates using the new FlexMaster version and delete the old templates.

1. Go to *Configure > Standalone APs > Config Templates.*
2. Click **Create a template**. The *CREATE A TEMPLATE* configuration wizard opens at the bottom of the page.

Figure 82. Select the check boxes for the options that you want to configure



Notes

Save time configuring devices by using configuration templates. Device settings, such as SSIDs, login information, and L2TP settings, can be applied to multiple devices at the same time by deploying a configuration template.

Config Templates

Template Name	Created by	Created	Supported Models	Actions
7781-cm-s	bin	Jan. 22 2013 23:08:02	7781CM-S	View Edit Delete Copy Export
7781-cm-e	bin	Jan. 22 2013 23:06:39	ZF7781CM-E	View Edit Delete Copy Export
7781cm-p	bin	Jan. 22 2013 22:31:48	ZF7781CM	View Edit Delete Copy Export
test	ives	Jan. 22 2013 00:22:35	ZF7321-U	View Edit Delete Copy Export
corfu-cm	bin	Jan. 21 2013 18:27:23	ZF7781CM	View Edit Delete Copy Export

Number of templates: 12

CREATE A TEMPLATE

Template Name

Product Type: ZF2741

Select product type: Ruckus ZF2741 Device

Select the configuration options that you want to modify:

□ Select All

□ Device General
□ Internet
□ Local Subnet 1
□ Local Subnet 2
□ Local Subnet 3
□ Local Subnet 4
□ Wireless Common
□ Wireless 1
□ Wireless 2
□ Wireless 3
□ Wireless 4
□ Wireless 5
□ Wireless 6
□ Wireless 7
□ Wireless 8
□ Management
□ Device Registration Settings
□ VLAN & LAN Port Setting
□ 802.1X Settings
□ Hotspot Basic Settings
□ Hotspot Walled Garden
□ Hotspot MAC Address Pass-Through
□ Hotspot Advanced Setting

3. In *Template Name,* type a name for the template that you are creating. Ruckus Wireless recommends using a descriptive name that identifies the task to be accomplished, including device type, if appropriate.

4. Toggle the *Select product type* drop-down list, and then select a specific Ruckus Wireless product model.

   - For the Management Server Configuration Settings option, refer to Creating an AP Configuration Task.
   - For L2TP Settings, refer to Configuring Your Devices to Communicate with FlexMaster over L2TP.
   - For TACACS+ settings, refer to Configuring Your Devices to Work with TACACS+.

5. Under **Select the configuration options that you want to modify**, select the check boxes for the configuration categories that you want the template to cover. Each category covers multiple parameters.

Table 22. Configuration categories and example parameters

Category	**Example Parameters**
Device General	Device Name, Super User Name, Super User Password, TACACS+ State, Internal Heater, Temperature Update Interval
Internet	NTP Server, Management VLAN, Internet Connection Type, IP address, Mask, Gateway, DNS Server List, IPv6 settings, L2TP Tunnel
Local Subnet(s)	Subnet, Access VLAN, Local IP Address, Subnet Mask, DHCP Server, Starting Address, Maximum DHCP Users
Wireless Common	Country Code, Wireless Radio Mode, Radio Channel Width, Channel, Radio Transmit Power, Radio Protection Mode, 5.8 GHz Channels, Data Rate, External Antenna Gain
Wireless setting (wireless bridge only)	Enable Pairing, Wireless Bridge Availability, Wireless Bridge Broadcast SSID, Wireless Bridge Name, Wireless Bridge SSID, Wireless Bridge Encryption Method, Country Code, Wireless Radio Mode, Radio Channel Width, Channel, Radio Transmit Power, Radio Protection Mode, Antenna
Wireless (number)	Wireless Availability, Broadcast SSID, Client Isolation, Name, SSID, RTS/CTS Threshold, Rate limiting, Encryption Method, Packet Forwarding, Hotspot Service, Access VLAN, Insert DHCP option 82, Client Fingerprinting
Management	SSH Access, HTTP/HTTPS Access, Telnet Access, Telnet Port, SSH Access, SSH Port, HTTP Access, HTTP Port, HTTPS Access, HTTPS Port, System Log Access, Log Server IP, Log Server Port, Remote Management Mode
Device Registration Settings	Server URL, Server Registration User Name, Server Registration Password, Periodic Inform Interval (for more on these settings, refer to Creating an AP Configuration Task)
QoS Global, Ethernet, and Wireless Configuration (wireless bridge only)	TOS settings, Dot1p settings, QoS settings
VLAN & LAN Port Setting	LAN port and WLAN settings, VLAN based QoS settings

Table 22. Configuration categories and example parameters (Continued)

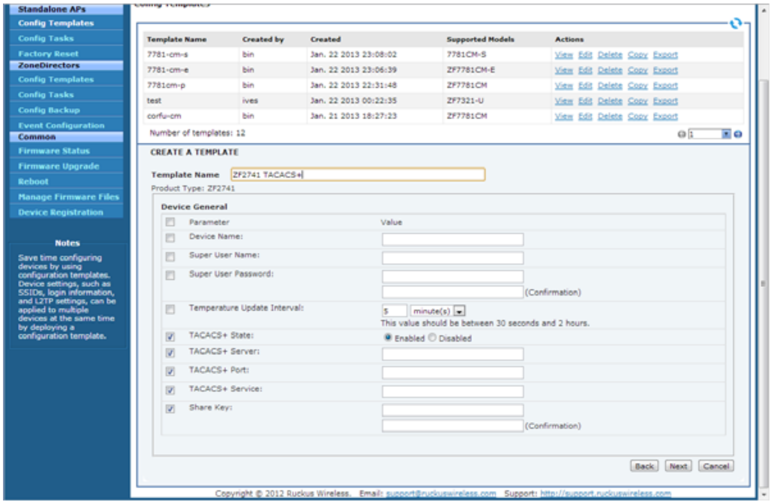
Category	**Example Parameters**
802.1X Settings	LAN1 802.1X settings
Hotspot Basic Settings, Walled Garden, MAC Address Pass-Through, Advanced Setting	Hotspot Service, UAM IP Address, Redirect URL, After Login, Primary RADIUS Server, Secondary RADIUS Server, RADIUS Shared Secret, Set Host List, Set MAC Address List, Login Retry Times, Blocked User URL, MAC Authentication, NAS ID, WISPr Location ID, WISPr Location Name, Location Description, Accounting Update Interval (minute(s), Interim Redirection Frequency (minute(s), Maximum Session Time (minute(s), Grace Period (minute(s), COA Port, Swap Input and Output Counters, Encode User Password, UAM Server Secret
LED Diagnostics	(per device)

NOTE: To configure VLANs, you must do so on a per-device basis from the Device View. You cannot completely configure VLAN settings through the template options. For more on the Device View, refer to Managing a Single Standalone Access Point.

6. Click **Next**.
7. Depending on the check boxes you selected in Step 5, selection and configuration parameters appear based on the category. Select the *Checked* column check box for a parameter and configure the value (for example, type an IP address or click an **Enable** button) for that parameter as part of the template. When the check box in the *Checked* column is not selected, then that parameter is not provisioned as part of the template.

NOTE: If you modify any of the values in the template or click any option or text box, then FlexMaster assumes that you want to change this parameter and automatically selects the check box in the *Checked* column.

Figure 83. Enter the values for the parameters that you want to modify



Template Name	Created by	Created	Supported Models	Actions
7781-cm-s	bin	Jan. 22 2013 23:08:02	7781CM-S	View Edit Delete Copy Export
7781-cm-e	bin	Jan. 22 2013 23:06:39	ZF7781CM-E	View Edit Delete Copy Export
7781cm-p	bin	Jan. 22 2013 22:31:48	ZF7781CM	View Edit Delete Copy Export
test	ives	Jan. 22 2013 00:22:35	ZF7321-U	View Edit Delete Copy Export
corfu-cm	bin	Jan. 21 2013 18:27:23	ZF7781CM	View Edit Delete Copy Export

Number of templates: 12

CREATE A TEMPLATE

Template Name ZF2741 TACACS+

Product Type: ZF2741

Device General

	Parameter	Value
□	Device Name:	
□	Super User Name:	
□	Super User Password:	(Confirmation)
□	Temperature Update Interval:	5 minute(s) This value should be between 30 seconds and 2 hours.
☑	TACACS+ State:	● Enabled ○ Disabled
☑	TACACS+ Server:	
☑	TACACS+ Port:	
☑	TACACS+ Service:	
☑	Share Key:	(Confirmation)

Notes

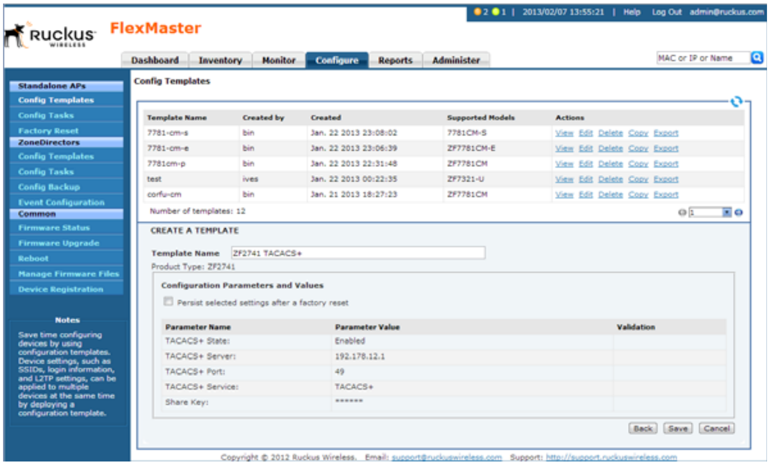
Save time configuring devices by using configuration templates. Device settings, such as SSIDs, login information, and L2TP settings, can be applied to multiple devices at the same time by deploying a configuration template.

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

8. Click **Next** after each category selection and configuration.
9. When you reach the *Configuration Parameters and Values* page, a summary of the configurations you have specified are displayed. If FlexMaster detected any errors, then the corresponding fields are flagged in red.

   Also on this summary page is the *Persist selected settings after a factory reset* check box. When this check box is selected, all attributes that are provisioned to one or more devices have precedence over the factory default settings, even if the device is reset to factory defaults. When this check box is cleared, the parameters provisioned in this template revert to factory defaults after a factory reset.
10. Click **Save** to save your configuration template.

Figure 84. *Click Save to save the configuration template that you are creating*



Notes

Save time configuring devices by using configuration templates. Device settings, such as SSIDs, login information, and L2TP settings, can be applied to multiple devices at the same time by deploying a configuration template.

Config Templates

Template Name	Created by	Created	Supported Models	Actions
7781-cm-s	bin	Jan. 22 2013 23:08:02	7781CM-S	View Edit Delete Copy Export
7781-cm-e	bin	Jan. 22 2013 23:06:39	ZF7781CM-E	View Edit Delete Copy Export
7781cm-p	bin	Jan. 22 2013 22:31:48	ZF7781CM	View Edit Delete Copy Export
test	ives	Jan. 22 2013 00:22:35	ZF7321-U	View Edit Delete Copy Export
corfu-cm	bin	Jan. 21 2013 18:27:23	ZF7781CM	View Edit Delete Copy Export

Number of templates: 12

CREATE A TEMPLATE

Template Name: ZF2741 TACACS+

Product Type: ZF2741

Configuration Parameters and Values

□ Persist selected settings after a factory reset

Parameter Name	Parameter Value	Validation
TACACS+ State:	Enabled	
TACACS+ Server:	192.178.12.1	
TACACS+ Port:	49	
TACACS+ Service:	TACACS+	
Share Key:	******	

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

NOTE: After you click **Save**, if any of the values that you entered in the configuration template is invalid, then an error message appears in the *Validation* column. You need to correct invalid values before the template can be saved.

The only configuration template that does not provide the validation feature is the VLAN Settings template. This is because there is no way for FlexMaster to check if the VLAN settings you configured are correct. To view the status of a VLAN configuration template, check the *Configuration Upgrade* page.

Since multiple templates with varying attributes can be applied to a given device and the persist flag can be set on a per template basis, the last template that is applied overwrites the previous persist flag. Furthermore, if the same parameters are set in multiple templates, then the value set in the last template takes precedence.

Viewing the Settings of an AP Configuration Template

1. Go to *Configure* > *Standalone APs* > *Config Templates*. A list of templates that you have created appears on the page.
2. Look for the template you want to view.
3. Click the **View** link that is in the same row as the template name.

The *VIEW* pane appears at the bottom of the page, displaying the parameters that are included in the template and the current parameter settings.

Editing an AP Configuration Template

1. Go to *Configure > Standalone APs > Config Templates.* A list of templates that you have created appears on the page.
2. Look for the configuration template that you want to edit.
3. Click the **Edit** link that is in the same row as the template name. The *EDIT* pane appears at the bottom of the page, displaying the parameters that you can modify.
4. Select the check box for the parameters that you want to modify, and then click **Next**. The related options for the selected parameters appear.
5. Edit the options as needed. If you selected multiple parameters for editing, then related options appear on several screens. To move to the next screen, click the **Next** button at the bottom of the screen.

   When you reach the last configuration screen, a summary of the settings that you are configuring appears.
6. Verify that the settings you have configured are correct. To make changes, click **Back** until you reach the screen where you can edit the settings. When you have finished editing the settings, click **Next** again until you reach the summary screen.
7. If you want managed devices to retain these settings even after they are reset to factory defaults, then select the *Persist selected settings after a factory reset* check box.
8. Click **Save** to save your changes.

Deleting an AP Configuration Template

1. Go to *Configure > Standalone APs > Config Templates.* A list of templates that you have created appears on the page.
2. Look for the configuration template that you want to delete.
3. Click the **Delete** link that is in the same row as the template name. A confirmation message appears.
4. Click **OK**.

The page refreshes and the configuration task that you deleted disappears from the list.

Copying an AP Configuration Template

In addition to creating and editing configuration templates, you can also copy an existing template and save it under a different template name. This feature is useful when you want to apply a similar set of configuration settings to another group of devices. Note that when you copy or clone a template, you can only apply it to devices of the same model.

1. Go to *Configure > Standalone APs > Config Templates.* A list of templates that you have created appears on the page.
2. Look for the configuration template that you want to copy.
3. Click the **Copy** link that is in the same row as the template name. The *COPY* pane appears at the bottom of the page.
4. In **New template name**, type the name that you want to assign to the new configuration template.
5. Click **Copy** to finish copying the configuration template.

The new template you have copied appears in the list of configuration templates. After you copy a template successfully, you can edit or fine-tune it before using it to create a provisioning task.

Exporting an AP Configuration Template

1. Go to *Configure > Standalone APs > Config Templates.* A list of templates that you have created appears on the page.
2. Look for the configuration template that you want to export to Excel.
3. Click the **Export** link that is in the same row as the template name. A *File Download* dialog box appears.
4. If the download location is not already set in your web browser, then click **Save**, select the location where you want to save the file, and click **OK**.
5. When the download is complete, go to the location where you saved the file, and then verify that it has been saved successfully.

To open the file that you saved, use Microsoft Excel 97 or later.

Configuring a Management Server Configuration Template

Use the Management Server Configuration Settings option within Configuration Templates to:

- change the FlexMaster URL that managed devices use to "call home", and
- change the interval at which a managed device "calls home".

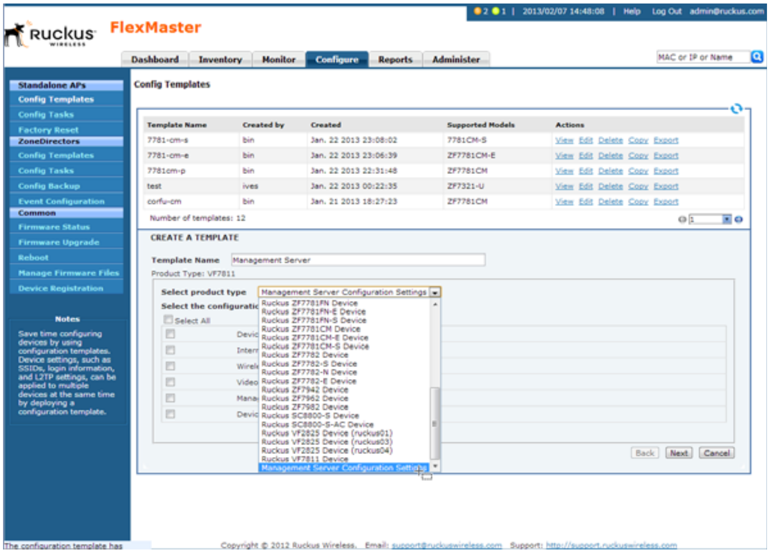
When configured, these settings are provisioned to *all* managed standalone APs, regardless of the product model.

The *Periodic Inform Interval* is the frequency at which devices attempt to connect to FlexMaster. If the interval for a device arrives and it does not call FlexMaster, then this could indicate a device issue. To learn how to receive notifications for devices that do not call home at the inform interval, refer to Configuring Alert Properties.

Follow these steps to create a management server configuration template.

1. Go to *Configure* > *Standalone APs* > *Config Templates.*
2. Click **Create a template**. The *CREATE A TEMPLATE* configuration form appears at the bottom of the page.
3. In *Template Name*, type a name for the template that you are creating.
4. (Optional) Toggle the *Select product type* drop-down list to select the **Management Server Configuration Settings** option.

Figure 85. Select the target product type



Save time configuring devices by using configuration templates. Device settings, such as SSIDs, login information, and L2TP settings, can be applied to multiple devices at the same time by deploying a configuration template.

Config Templates

Template Name	Created by	Created	Supported Models	Actions
7781-cm-s	bin	Jan. 22 2013 23:08:02	7781CM-S	View Edit Delete Copy Export
7781-cm-e	bin	Jan. 22 2013 23:06:39	ZF7781CM-E	View Edit Delete Copy Export
7781cm-p	bin	Jan. 22 2013 22:31:48	ZF7781CM	View Edit Delete Copy Export
test	ives	Jan. 22 2013 00:22:35	ZF7321-U	View Edit Delete Copy Export
corfu-cm	bin	Jan. 21 2013 18:27:23	ZF7781CM	View Edit Delete Copy Export

Number of templates: 12

CREATE A TEMPLATE

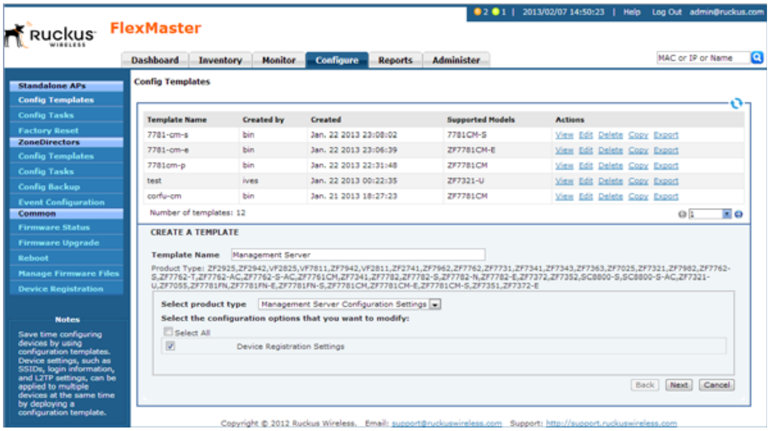
Template Name: Management Server

Product Type: VF7811

Select product type: Management Server Configuration Settings

5. Under *Select the configuration options you would like to modify,* select the **Device Registration Settings** check box.

Figure 86. Select Device Registration Settings



Config Templates

Template Name	Created by	Created	Supported Models	Actions
7781-cm-s	bin	Jan. 22 2013 23:08:02	7781CM-S	View Edit Delete Copy Export
7781-cm-e	bin	Jan. 22 2013 23:06:39	ZF7781CM-E	View Edit Delete Copy Export
7781cm-p	bin	Jan. 22 2013 22:31:48	ZF7781CM	View Edit Delete Copy Export
test	ives	Jan. 22 2013 00:22:35	ZF7321-U	View Edit Delete Copy Export
corfu-cm	bin	Jan. 21 2013 18:27:23	ZF7781CM	View Edit Delete Copy Export

Number of templates: 12

CREATE A TEMPLATE

Template Name: Management Server

Product Type: ZF2925,ZF2942,VF2825,VF7811,ZF7942,VF2811,ZF2741,ZF7962,ZF7762,ZF7731,ZF7341,ZF7343,ZF7363,ZF7025,ZF7321,ZF7982,ZF7762-S,ZF7762-T,ZF7762-AC,ZF7762-S-AC,ZF7761CM,ZF7341,ZF7782,ZF7782-S,ZF7782-N,ZF7782-E,ZF7372,ZF7352,SC8800-S,SC8800-S-AC,ZF7321-U,ZF7055,ZF7781FN,ZF7781FN-E,ZF7781FN-S,ZF7781CM,ZF7781CM-E,ZF7781CM-S,ZF7351,ZF7372-E

Select product type: Management Server Configuration Settings

Select the configuration options that you want to modify:

□ Select All

☑ Device Registration Settings

Save time configuring devices by using configuration templates. Device settings, such as SSIDs, login information, and L2TP settings, can be applied to multiple devices at the same time by deploying a configuration template.

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

6. Click **Next**.

7. Under *Device Registration Settings*, change the required parameters.

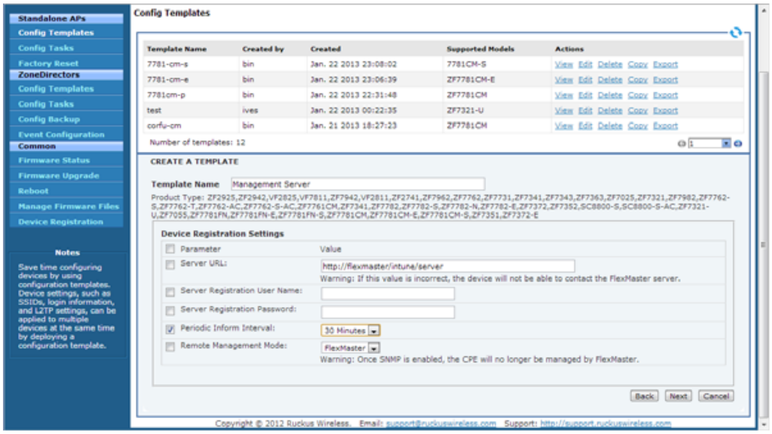
Table 23. Parameters included in registration settings

Parameter	**Description**
Server URL	Type the URL to FlexMaster's management service. The URL value must be a full URL starting with "http://" or "https://" followed by the FlexMaster server host name or IP address, and must end with "/intune/server". The default value is "http://flexmaster/intune/server".
Server Registration User Name	Type the user name for logging into the FlexMaster server
Server Registration Password	Type the password appropriate to the user name for logging into the FlexMaster server
Periodic Inform Interval	Select the time interval at which the device must synchronize with FlexMaster **NOTE:** *The shortest inform interval that APs with 7.0 and later software support is one (1) minute, while APs with pre-7.0 software support five (5) minutes. If you set 1 minute as the periodic inform interval in your template, then it is provisioned successfully to APs running on pre-7.0 software, but the interval that they use is 5 minutes (the shortest interval that they can support).*

Table 23. Parameters included in registration settings (Continued)

Parameter	Description
Remote Management Mode	Select the remote management option that you want to apply to the device: • **AUTO** to allow the device to be managed via SNMP or TR-69 (FlexMaster) • **FlexMaster** (default) to allow only FlexMaster management • **SNMP** to allow only SNMP management **NOTE:** *If you enable SNMP management, then FlexMaster is no longer able to manage the device.*

Figure 87. Configure the parameters that you want to modify



Notes

Save time configuring devices by using configuration templates. Device settings, such as SSIDs, login information, and L2TP settings, can be applied to multiple devices at the same time by deploying a configuration template.

Config Templates

Template Name	Created by	Created	Supported Models	Actions
7781-cm-s	bin	Jan. 22 2013 23:08:02	7781CM-S	View Edit Delete Copy Export
7781-cm-e	bin	Jan. 22 2013 23:06:39	ZF7781CM-E	View Edit Delete Copy Export
7781cm-p	bin	Jan. 22 2013 22:31:48	ZF7781CM	View Edit Delete Copy Export
test	ives	Jan. 22 2013 00:22:35	ZF7321-U	View Edit Delete Copy Export
corfu-cm	bin	Jan. 21 2013 18:27:23	ZF7781CM	View Edit Delete Copy Export

Number of templates: 12

CREATE A TEMPLATE

Template Name: Management Server

Product Type: ZF2925,ZF2942,VF2825,VF7811,ZF7942,VF2811,ZF2741,ZF7962,ZF7762,ZF7731,ZF7341,ZF7343,ZF7363,ZF7025,ZF7321,ZF7982,ZF7762-S,ZF7762-T,ZF7762-AC,ZF7762-S-AC,ZF7761CM,ZF7341,ZF7782,ZF7782-S,ZF7782-N,ZF7782-E,ZF7372,ZF7352,SC8800-S,SC8800-S-AC,ZF7321-U,ZF7055,ZF7781FN,ZF7781FN-E,ZF7781FN-S,ZF7781CM,ZF7781CM-E,ZF7781CM-S,ZF7351,ZF7372-E

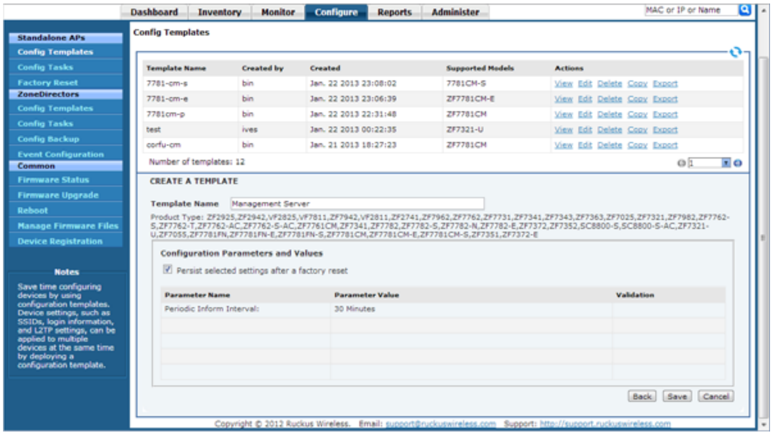
Device Registration Settings

	Parameter	Value
□	Server URL:	http://flexmaster/intune/server Warning: If this value is incorrect, the device will not be able to contact the FlexMaster server.
□	Server Registration User Name:	
□	Server Registration Password:	
☑	Periodic Inform Interval:	30 Minutes
□	Remote Management Mode:	FlexMaster Warning: Once SNMP is enabled, the CPE will no longer be managed by FlexMaster.

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

8. Click **Next**.

Figure 88. Review your configuration settings, and then click Save



Save time configuring devices by using configuration templates. Device settings, such as SSIDs, login information, and L2TP settings, can be applied to multiple devices at the same time by deploying a configuration template.

Config Templates

Template Name	Created by	Created	Supported Models	Actions
7781-cm-s	bin	Jan. 22 2013 23:08:02	7781CM-S	View Edit Delete Copy Export
7781-cm-e	bin	Jan. 22 2013 23:06:39	ZF7781CM-E	View Edit Delete Copy Export
7781cm-p	bin	Jan. 22 2013 22:31:48	ZF7781CM	View Edit Delete Copy Export
test	ives	Jan. 22 2013 00:22:35	ZF7321-U	View Edit Delete Copy Export
corfu-cm	bin	Jan. 21 2013 18:27:23	ZF7781CM	View Edit Delete Copy Export

Number of templates: 12

CREATE A TEMPLATE

Template Name: Management Server

Product Type: ZF2925,ZF2942,VF2825,VF7811,ZF7942,VF2811,ZF2741,ZF7962,ZF7762,ZF7731,ZF7341,ZF7343,ZF7363,ZF7025,ZF7321,ZF7982,ZF7762-S,ZF7762-T,ZF7762-AC,ZF7762-S-AC,ZF7761CM,ZF7341,ZF7782,ZF7782-S,ZF7782-N,ZF7782-E,ZF7372,ZF7352,SC8800-S,SC8800-S-AC,ZF7321-U,ZF7055,ZF7781FN,ZF7781FN-E,ZF7781FN-S,ZF7781CM,ZF7781CM-E,ZF7781CM-S,ZF7351,ZF7372-E

Configuration Parameters and Values

☑ Persist selected settings after a factory reset

Parameter Name	Parameter Value	Validation
Periodic Inform Interval:	30 Minutes	

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

9. After saving the template, create an AP configuration task that provisions this configuration template to all managed devices. Refer to Creating an AP Configuration Task.

]

Performing an AP Configuration Upgrade

An AP Configuration Upgrade is a task that upgrades the configuration settings of managed devices either on-demand or at a specified time. As FlexMaster can manage many Ruckus Wireless devices, creating configuration upgrade tasks consolidates necessary configurations across one or more devices as defined by a device view.

AP Configuration Upgrade tasks require a configuration template that specifies the settings to be updated. Since configuration templates are specific to a product model, it is possible that not all devices in a device view are provisioned based on product model. For example, if you grouped multiple devices according to their common location (for example, Los Angeles, CA) and called that view "LA Devices", and the view consisted of three ZF 7782s and two VF 2825s, then you need to create two (or more) separate configuration templates and configuration upgrade tasks to configure all of the devices in the view.

WARNING! Deploying a template that changes the device's country code or 802.11 radio mode settings causes the Ruckus Wireless device to reboot. The reboot may take up to two minutes. Ruckus Wireless recommends applying such configuration changes during periods when service level agreement (SLA) downtime is permitted.

NOTE: Before you create a configuration upgrade task, you need to create a configuration template. To create a configuration template, refer to Creating an AP Configuration Template.

Creating an AP Configuration Task

An AP configuration task enables FlexMaster to deploy a configuration template that you have already created.

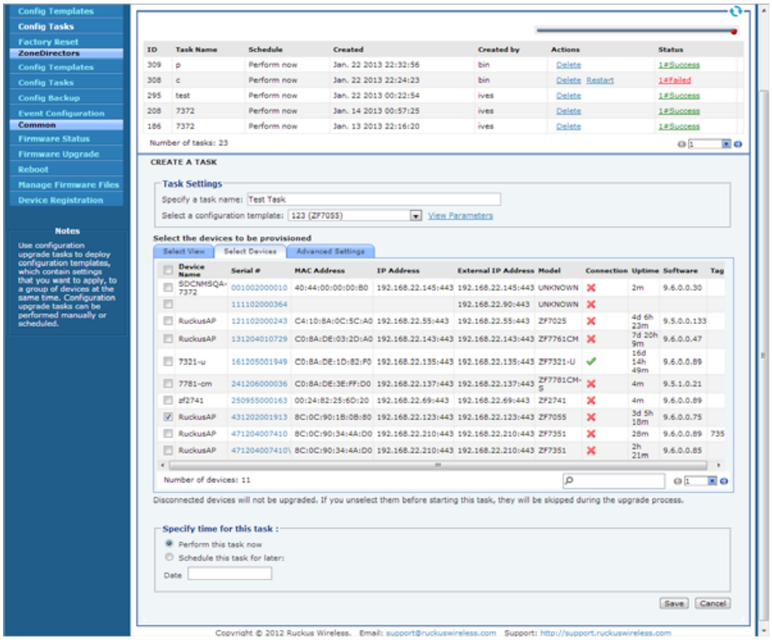
NOTE: Configuration, firmware, reboot and factory reset tasks cannot be deleted. Tasks that have not yet started, however, can be cancelled, although they remain in the FlexMaster database. By keeping all of the user actions in the database, FlexMaster can produce accurate audit logs of system configuration activities.

1. Go to *Configure* > *Standalone APs* > *Config Tasks.*
2. Click **Create a task**. The *CREATE A TASK* form appears at the bottom of the page.
3. In the *Task Settings* section, do the following:
   - In *Specify a task name*, type a name that you want to assign to this configuration upgrade task.
   - In *Select a configuration template*, select the configuration template that you want to use. If you want to view the parameters and settings that are included in the configuration template, select the template, and then click the *View Parameters* link.

4. In *Select the devices to be provisioned,* choose the target devices.

- To apply the selected configuration template to all standalone APs, select **All Standalone APs**.
- To apply the selected configuration template to an existing AP view, select the *AP View* name.
  Note that when the template is model-specific, the settings in the template are only applied to devices that match the model.
- To apply all settings in the configuration template to a device group or to specific devices,
  – Click the **Select Devices** tab.
  – In the **Select Devices** tab, search for and select the target devices.
  Note that when the template is model-specific, the settings in the template are only applied to devices that match the model.

Figure 89. Selecting the configuration template and target devices



Notes

Use configuration upgrade tasks to deploy configuration templates, which contain settings that you want to apply, to a group of devices at the same time. Configuration upgrade tasks can be performed manually or scheduled.

ID	Task Name	Schedule	Created	Created by	Actions	Status
309	p	Perform now	Jan. 22 2013 22:32:56	bin	Delete	1#Success
308	c	Perform now	Jan. 22 2013 22:24:23	bin	Delete Restart	1#Failed
295	test	Perform now	Jan. 22 2013 00:22:54	ives	Delete	1#Success
208	7372	Perform now	Jan. 14 2013 00:57:25	ives	Delete	1#Success
186	7372	Perform now	Jan. 13 2013 22:16:20	ives	Delete	1#Success

Number of tasks: 23

CREATE A TASK

Task Settings

Specify a task name: Test Task

Select a configuration template: 123 (ZF7055) View Parameters

Select the devices to be provisioned

□	Device Name	Serial #	MAC Address	IP Address	External IP Address	Model	Connection	Uptime	Software	Tag
□	SDCNMSQA-7372	001002000010	40:44:00:00:00:B0	192.168.22.145:443	192.168.22.145:443	UNKNOWN	✗	2m	9.6.0.0.30	
□		111102000364			192.168.22.90:443	UNKNOWN	✗			
□	RuckusAP	121102000243	C4:10:8A:0C:5C:A0	192.168.22.55:443	192.168.22.55:443	ZF7025	✗	4d 6h 23m	9.5.0.0.133	
□	RuckusAP	131204010729	C0:8A:DE:03:2D:A0	192.168.22.143:443	192.168.22.143:443	ZF7761CM	✗	7d 20h 9m	9.6.0.0.47	
□	7321-u	161205001949	C0:8A:DE:1D:82:F0	192.168.22.135:443	192.168.22.135:443	ZF7321-U	✓	16d 14h 49m	9.6.0.0.89	
□	7781-cm	241206000036	C0:8A:DE:3E:FF:D0	192.168.22.137:443	192.168.22.137:443	ZF7781CM-S	✗	4m	9.5.1.0.21	
□	zf2741	250955000163	00:24:82:25:6D:20	192.168.22.69:443	192.168.22.69:443	ZF2741	✗	4m	9.6.0.0.89	
☑	RuckusAP	431202001913	8C:0C:90:1B:0B:80	192.168.22.123:443	192.168.22.123:443	ZF7055	✗	3d 5h 18m	9.6.0.0.75	
□	RuckusAP	471204007410	8C:0C:90:34:4A:D0	192.168.22.210:443	192.168.22.210:443	ZF7351	✗	28m	9.6.0.0.89	735
□	RuckusAP	471204007410\	8C:0C:90:34:4A:D0	192.168.22.210:443	192.168.22.210:443	ZF7351	✗	2h 21m	9.6.0.0.85	

Number of devices: 11

Disconnected devices will not be upgraded. If you unselect them before starting this task, they will be skipped during the upgrade process.

Specify time for this task :

● Perform this task now
○ Schedule this task for later:

Date

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

NOTE: In addition to the default device view (All Standalone APs), device views that you manually created from search results also appears on the **Select View** tab. When you deploy an upgrade task to a manually-created device view, only the current members of that view are marked for provisioning. New devices that match the view criteria but that registered with FlexMaster after the upgrade task is saved is not provisioned. You need to create a new upgrade task to include these new devices.

- To apply different parameter settings to target devices, click the **Advanced Settings** tab, and then do the following:
  - In *Serial Number*, enter the serial number of the device that you want to configure.
  - Select the check boxes for the parameters that you want to configure for the device, and then configure the settings.
    For example, if the configuration template includes IP address settings and you want to assign the IP address `192.68.100.13` to this device, select the *IP Address* check box, and then type `192.68.100.13` in the box provided.
  - Click the **Add** link to add this configuration to the task.
    NOTE: *Clicking Add does not save the task itself. To save the configuration upgrade task, after you done configuring the task, click the* **Save** *button at the bottom of the page.*
  - Repeat these steps for each device that you want to configure.

5. In *Specify time for this task*, specify when you want the task to run.
   - To run the task immediately, click **Perform this task now**.
   - To schedule the task, click **Schedule this task for later**, and then enter the date and time.
6. Click **Save** to save the configuration upgrade task.

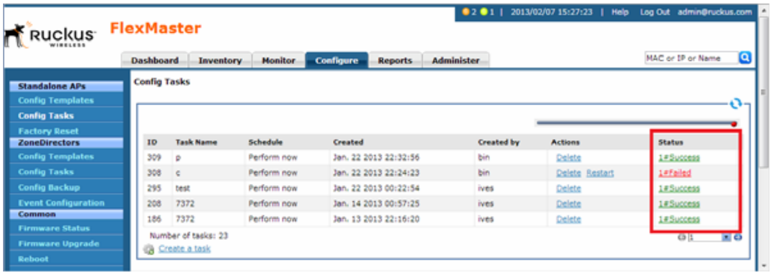
NOTE: If FlexMaster detects a problem in the configuration upgrade task that you are saving, then an error message appears.

To cancel a configuration upgrade task, refer to Canceling a Scheduled Configuration Upgrade Task.

Viewing the Status of an AP Configuration Upgrade Task

1. Go to *Configure* > *Standalone APs* > *Config Tasks*. A list of upgrade tasks that you have created appears on the page.
2. Look for the upgrade task for which status you want to view.
3. In the *Status* column, check the value that appears on the same row as the task name:
   - *n#Success*: Indicates that the configuration task has been provisioned successfully to n number of devices. To view the list of devices that have been provisioned successfully, click **n#Success** (hyperlink). The *Device Status* pane appears at the bottom of the page, displaying task details, device details, and task status.
   - *n#Fail:* Indicates that the configuration task failed on n number of devices. To view the list of devices on which provisioning failed, click **n#Fail** (hyperlink). The *Device Status* pane appears at the bottom of the page, displaying task details, device details, and task status. If the task failed, then click the *Detail* link in the *Failure* column to see what may have caused the task failure.
   - Other statuses can appear in the *Status* column. For a complete list of all statuses, refer to Understanding the Status of a Task.

Figure 90. Viewing the status of a configuration upgrade task



Config Tasks

ID	Task Name	Schedule	Created	Created by	Actions	Status
309	p	Perform now	Jan. 22 2013 22:32:56	bin	Delete	1#Success
308	c	Perform now	Jan. 22 2013 22:24:23	bin	Delete Restart	1#Failed
295	test	Perform now	Jan. 22 2013 00:22:54	ives	Delete	1#Success
208	7372	Perform now	Jan. 14 2013 00:57:25	ives	Delete	1#Success
186	7372	Perform now	Jan. 13 2013 22:16:20	ives	Delete	1#Success

Number of tasks: 23

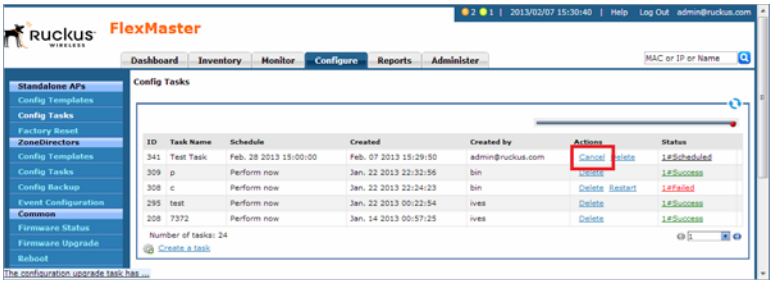
Create a task

Canceling a Scheduled Configuration Upgrade Task

Provisioning tasks that have not yet started can be cancelled. For all cancelled tasks, the record of their creation and scheduling remain in the FlexMaster database.

1. Go to *Configure* > *Standalone APs* > *Config Tasks.*
2. Locate the upgrade task you want to cancel in the *Config Tasks* table.
3. Click **Cancel** in the *Actions* column.

Figure 91. Click Cancel to cancel a scheduled task



Config Tasks

ID	Task Name	Schedule	Created	Created by	Actions	Status
341	Test Task	Feb. 28 2013 15:00:00	Feb. 07 2013 15:29:50	admin@ruckus.com	Cancel Delete	1#Scheduled
309	p	Perform now	Jan. 22 2013 22:32:56	bin	Delete	1#Success
308	c	Perform now	Jan. 22 2013 22:24:23	bin	Delete Restart	1#Failed
295	test	Perform now	Jan. 22 2013 00:22:54	ives	Delete	1#Success
208	7372	Perform now	Jan. 14 2013 00:57:25	ives	Delete	1#Success

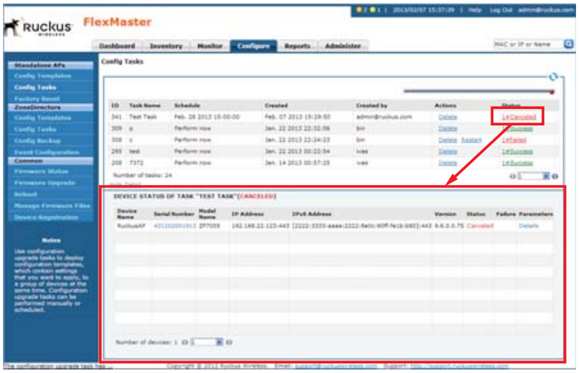
Number of tasks: 24

Create a task

The configuration upgrade task has ...

4. In the pop-up window that appears, click **OK** to confirm the cancellation. The cancelled upgrade displays “Cancelled” in the *Status* column.
5. Click the **Cancelled** link for the cancelled upgrade to view all task details.

Figure 92. Viewing details of the cancelled task



Config Tasks

ID	Task Name	Schedule	Created	Created by	Actions	Status
341	Test Task	Feb. 28 2013 15:00:00	Feb. 07 2013 15:29:50	admin@ruckus.com	Delete	1#Canceled
309	p	Perform now	Jan. 22 2013 22:32:56	bin	Delete	1#Success
308	c	Perform now	Jan. 22 2013 22:24:23	bin	Delete Restart	1#Failed
295	test	Perform now	Jan. 22 2013 00:22:54	ives	Delete	1#Success
208	7372	Perform now	Jan. 14 2013 00:57:25	ives	Delete	1#Success

Number of tasks: 24

DEVICE STATUS OF TASK "TEST TASK"(CANCELED)

Device Name	Serial Number	Model Name	IP Address	IPv6 Address	Version	Status	Failure	Parameters
RuckusAP	431202001313	ZF7055	192.168.22.123:443	[2222:3333:aaaa:2222:6e0c:90ff:fe1b:0802]:443	9.6.3.0.75	Canceled		Details

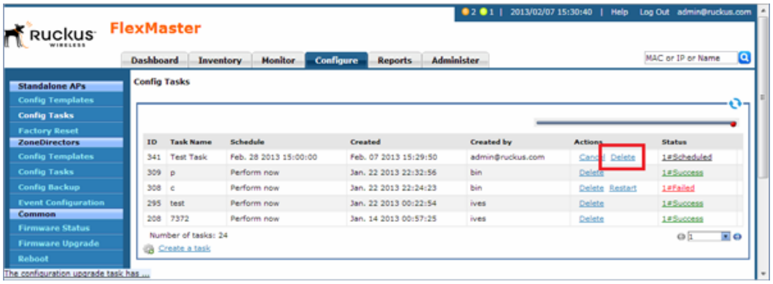
Number of devices: 1

Deleting a Configuration Upgrade Task

1. Go to *Configure* > *Standalone APs* > *Config Tasks.*
2. Locate the task you want to delete.
3. Click the **Delete** link that is in the same row as the task name. A confirmation message appears.
4. Click **OK** to delete the scheduled task.

The page refreshes, and then the task that you deleted disappears from the list of configuration upgrade tasks.

Figure 93. Click Delete to delete the configuration upgrade task



Config Tasks

ID	Task Name	Schedule	Created	Created by	Actions	Status
341	Test Task	Feb. 28 2013 15:00:00	Feb. 07 2013 15:29:50	admin@ruckus.com	Cancel Delete	1#Scheduled
309	p	Perform now	Jan. 22 2013 22:32:56	bin	Delete	1#Success
308	c	Perform now	Jan. 22 2013 22:24:23	bin	Delete Restart	1#Failed
295	test	Perform now	Jan. 22 2013 00:22:54	ives	Delete	1#Success
208	7372	Perform now	Jan. 14 2013 00:57:25	ives	Delete	1#Success

Number of tasks: 24

Restarting a Configuration Upgrade Task

If a configuration task that you deployed fails for any reason, then you can manually restart the task from the *Configuration Upgrade* page.

NOTE: Before restarting a failed task, Ruckus Wireless recommends that you first check the reason the task failed. You can do this by clicking the View link for the task to open the task status pane. In the *Failure* column, click the **Details** link to display the reason the task failed. If the upgrade task includes settings that need to be corrected, then you should correct these settings first before restarting the task.

NOTE: Restart tasks are only applied to devices on which provisioning failed. Devices that have been provisioned successfully are not affected by the restart task option.

1. Go to *Configure > Standalone APs > Config Tasks.*
2. Locate the task you want to restart.
3. Click the **Restart** link that is in the same row as the task name. A confirmation message appears.
4. Click **OK** to restart the task.

The page refreshes and the *Status* column for the task shows *Started.*

NOTE: In addition to restarting a single task manually, FlexMaster provides a way to automatically restart all failed tasks. To configure this setting, go to *Administer > System Settings,* and then click the **Yes** option in *Task Restart Services.*

Performing an AP Factory Reset

The Factory Reset option resets devices to their factory defaults, immediately or at the specified time. Resetting to factory defaults may be necessary when repurposing devices, thus requiring a new configuration for each device. A reset causes a reboot; thus, the devices go out of service for a period of time (approximately one to two minutes).

Note that FlexMaster can reset APs to factory defaults, but not ZoneDirector devices. This is because resetting ZoneDirector to factory defaults affects all APs that are connected to it and may cause parts of (if not the entire) network to go offline.

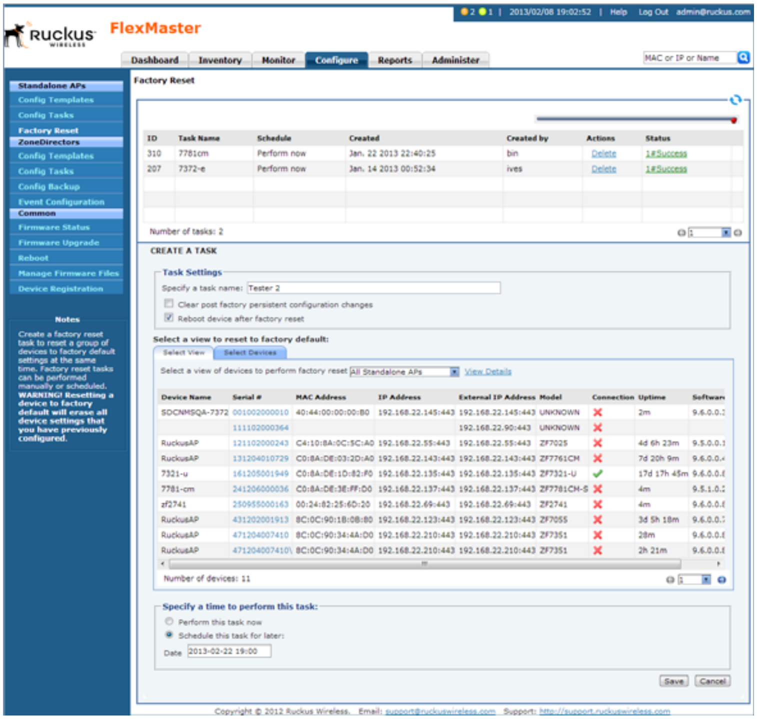
WARNING! *If* you changed the Management Server Configuration Settings (refer to Creating an AP Configuration Task) but you did not persist the configuration across factory resets, then provisioning a factory reset can result in managed APs being unable to find FlexMaster after they are reset to factory default.

WARNING! Resetting an AP to factory default erases all configuration settings, except those that you chose to make persistent. When you create a new configuration template, you can make the settings in the template persistent by selecting the Persist selected settings after a factory reset check box. For more information, refer to Creating an AP Configuration Task.

Creating an AP Factory Reset Task

1. Go to *Configure* > *Standalone APs* > *Factory Reset.*
2. Click **Create a task**. The *CREATE A TASK* form appears at the bottom of the page.

Figure 94. Creating a factory reset task



Notes

Create a factory reset task to reset a group of devices to factory default settings at the same time. Factory reset tasks can be performed manually or scheduled. **WARNING! Resetting a device to factory default will erase all device settings that you have previously configured.**

Factory Reset

ID	Task Name	Schedule	Created	Created by	Actions	Status
310	7781cm	Perform now	Jan. 22 2013 22:40:25	bin	Delete	1#Success
207	7372-e	Perform now	Jan. 14 2013 00:52:34	ives	Delete	1#Success

Number of tasks: 2

CREATE A TASK

Task Settings

Specify a task name: Tester 2

□ Clear post factory persistent configuration changes

☑ Reboot device after factory reset

Select a view to reset to factory default:

Select a view of devices to perform factory reset All Standalone APs View Details

Device Name	Serial #	MAC Address	IP Address	External IP Address	Model	Connection	Uptime	Software
SDCNMSQA-7372	001002000010	40:44:00:00:00:B0	192.168.22.145:443	192.168.22.145:443	UNKNOWN	✗	2m	9.6.0.0.
	111102000364			192.168.22.90:443	UNKNOWN	✗		
RuckusAP	121102000243	C4:10:8A:0C:5C:A0	192.168.22.55:443	192.168.22.55:443	ZF7025	✗	4d 6h 23m	9.5.0.0.
RuckusAP	131204010729	C0:8A:DE:03:2D:A0	192.168.22.143:443	192.168.22.143:443	ZF7761CM	✗	7d 20h 9m	9.6.0.0.
7321-u	161205001949	C0:8A:DE:1D:82:F0	192.168.22.135:443	192.168.22.135:443	ZF7321-U	✓	17d 17h 45m	9.6.0.0.
7781-cm	241206000036	C0:8A:DE:3E:FF:D0	192.168.22.137:443	192.168.22.137:443	ZF7781CM-S	✗	4m	9.5.1.0.
zf2741	250955000163	00:24:82:25:6D:20	192.168.22.69:443	192.168.22.69:443	ZF2741	✗	4m	9.6.0.0.
RuckusAP	431202001913	8C:0C:90:1B:0B:80	192.168.22.123:443	192.168.22.123:443	ZF7055	✗	3d 5h 18m	9.6.0.0.
RuckusAP	471204007410	8C:0C:90:34:4A:D0	192.168.22.210:443	192.168.22.210:443	ZF7351	✗	28m	9.6.0.0.
RuckusAP	471204007410\	8C:0C:90:34:4A:D0	192.168.22.210:443	192.168.22.210:443	ZF7351	✗	2h 21m	9.6.0.0.

Number of devices: 11

Specify a time to perform this task:

○ Perform this task now

● Schedule this task for later:

Date 2013-02-22 19:00

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

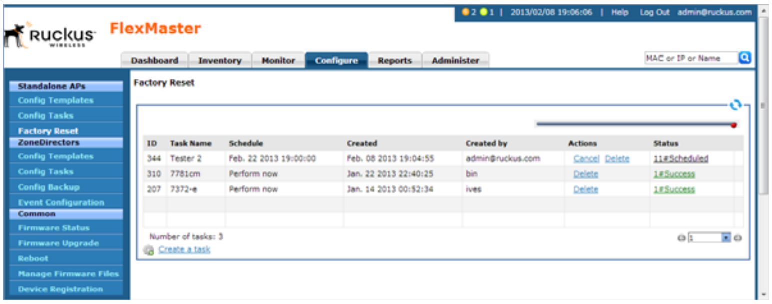
3. In *Specify a task name*, type a name for your reboot task.
4. If you want this task that you are creating to reset all settings on the target devices to factory default, including those settings that have been made persistent, then select the *Clear post factory persistent configuration changes* check box.
5. Select the *Reboot device after factory reset* check box to reboot all group devices after sending the factory reset task. A reboot is required to complete the factory reset process, therefore Ruckus Wireless recommends selecting this check box.

6. Under *Select a view of devices to perform factory default*, select the target devices. Do one of the following:
   - On the *Select View* tab, select an existing device view.
   - On the *Select Devices* tab, select the check box for each device that you want to reset to factory default.
7. Under *Specify a time to perform this task*, click when you want to perform this task:
   - **Perform this task now**: Run the task immediately after clicking **Save**.
   - **Schedule this task for later**: Specify the Date (yyyy-mm-dd) and Time (hh:mm:ss [AM|PM]) on which the task should run.
8. Click **Save**.

Viewing Existing AP Factory Reset Tasks

Go to *Configure* > *Standalone APs* > *Factory Reset*. The *Factory Reset* page appears and lists that factory reset tasks that have been created.

Figure 95. The Factory Reset page lists that factory reset tasks that have been created



Factory Reset

ID	Task Name	Schedule	Created	Created by	Actions	Status
344	Tester 2	Feb. 22 2013 19:00:00	Feb. 08 2013 19:04:55	admin@ruckus.com	Cancel Delete	11#Scheduled
310	7781cm	Perform now	Jan. 22 2013 22:40:25	bin	Delete	1#Success
207	7372-e	Perform now	Jan. 14 2013 00:52:34	ives	Delete	1#Success

Number of tasks: 3

Create a task

Canceling an AP Factory Reset Task

1. Go to *Configure* > *Standalone APs* > *Factory Reset*. The *Factory Reset* page displays the factory reset tasks that have been created.
2. Look for the factory reset task that you want to cancel, and then click the **Cancel** link that is in the same row as the task name. A confirmation dialog appears.
3. Click **OK** to continue.

The page refreshes, and then the *Status* column for the task now display `#Cancelled`. You have cancelled the AP factory reset task.

Deleting an AP Factory Reset Task

1. Go to *Configure > Standalone APs > Factory Reset.* The *Factory Reset* page displays the factory reset tasks that have been created.
2. Look for the factory reset task that you want to delete, and then click the **Delete** link that is in the same row as the task name. A confirmation dialog appears.
3. Click **OK** to continue.

The page refreshes, and then the task disappears from the Factory Reset table. You have completed deleting the AP factory reset task.

Creating an Auto Configuration Task

New devices that are registering with FlexMaster can also be automatically provisioned with settings preconfigured by the administrator for a specific group of devices (for example, all ZoneFlex 2942 devices). Auto configuration enables you to ensure that newly registered devices can be made operational immediately, without having to wait for you to configure them.

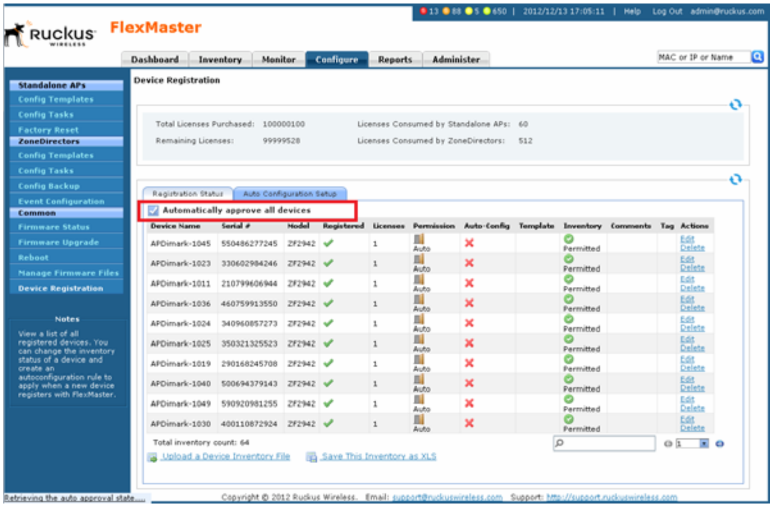
Note that auto configuration is only for devices that have not registered with FlexMaster. When a device is already registered with FlexMaster, its settings are not updated by the auto configuration task, even if it is part of the target device view for auto configuration.

Step A: Before You Begin

Before creating an auto configuration task, verify that device registration is set to Auto (this is the default setting). Follow these steps to check if device registration is set to auto approve.

1. Go to *Configure* > *Common* > *Device Registration.*
2. In the *Registration Status* tab, make sure that the **Automatically approve all devices** check box is selected.
   If the check box is clear, then select it. A popup message appears, prompting you to confirm that you want to enable automatic approval of devices. Click **Yes** to enable automatic approval of devices.

Figure 96. Verify that device registration is set to Auto



Device Registration

Total Licenses Purchased: 100000100
Remaining Licenses: 99999528
Licenses Consumed by Standalone APs: 60
Licenses Consumed by ZoneDirectors: 512

☑ Automatically approve all devices

Device Name	Serial #	Model	Registered	Licenses	Permission	Auto-Config	Template	Inventory	Comments	Tag	Actions
APDimark-1045	550486277245	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
APDimark-1023	330602984246	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
APDimark-1011	210799606944	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
APDimark-1036	460759913550	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
APDimark-1024	340960857273	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
APDimark-1025	350321325523	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
APDimark-1019	290168245708	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
APDimark-1040	500694379143	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
APDimark-1049	590920981255	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
APDimark-1030	400110872924	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete

Total inventory count: 64

Notes

View a list of all registered devices. You can change the inventory status of a device and create an autoconfiguration rule to apply when a new device registers with FlexMaster.

Retrieving the auto approval state....

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

If you intentionally disabled automatic device registration, then you can still run auto configuration tasks, but you need to list the devices that you want to auto configure in an inventory file. For instructions on how to create an inventory file, refer to Option 2: Upload an Inventory File of Devices to Auto Configure.

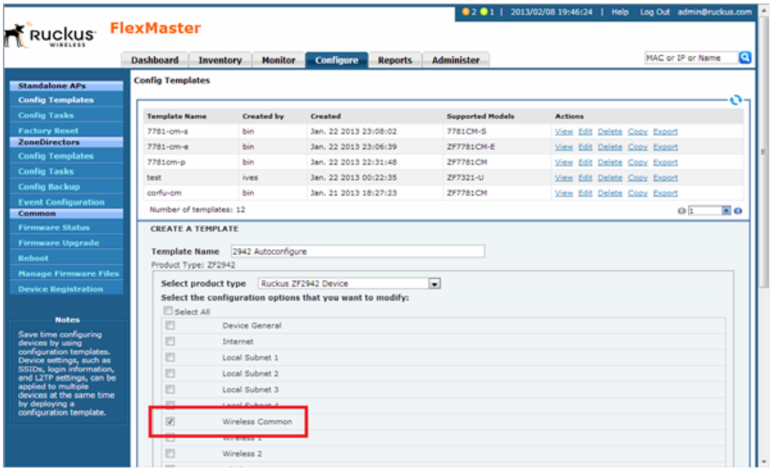
Step B: Create a Configuration Template

Create a configuration template that defines the settings that you want to provision to new devices. For more information on creating templates, refer to Creating an AP Configuration Template.

For example, when you want to auto configure the Wireless Common settings of all ZoneFlex 2942 access points that register with FlexMaster:

1. Go to *Configure > Standalone APs > Config Templates.*
2. Click **Create a template**. The *CREATE A TEMPLATE* configuration wizard opens at the bottom of the page.
3. In *Template Name,* type a name for the template, such as **`2942 Autoconfigure`**.
4. Select **Ruckus ZF2942 Device** in *Select product type.*
5. Select the **Wireless Common** check box when you create it.

Figure 97. Example: Creating a basic Wireless Common auto configuration template for ZoneFlex 2942 access points



Save time configuring devices by using configuration templates. Device settings, such as SSIDs, login information, and L2TP settings, can be applied to multiple devices at the same time by deploying a configuration template.

Config Templates

Template Name	Created by	Created	Supported Models	Actions
7781-cm-s	bin	Jan. 22 2013 23:08:02	7781CM-S	View Edit Delete Copy Export
7781-cm-e	bin	Jan. 22 2013 23:06:39	ZF7781CM-E	View Edit Delete Copy Export
7781cm-p	bin	Jan. 22 2013 22:31:48	ZF7781CM	View Edit Delete Copy Export
test	ives	Jan. 22 2013 00:22:35	ZF7321-U	View Edit Delete Copy Export
corfu-cm	bin	Jan. 21 2013 18:27:23	ZF7781CM	View Edit Delete Copy Export

Number of templates: 12

CREATE A TEMPLATE

Template Name: 2942 Autoconfigure

Product Type: ZF2942

Select product type: Ruckus ZF2942 Device

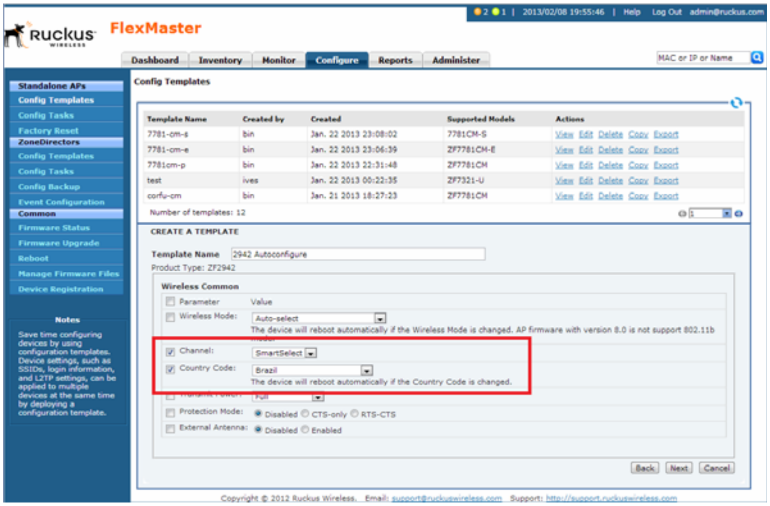
Select the configuration options that you want to modify:

□ Select All

□ Device General
□ Internet
□ Local Subnet 1
□ Local Subnet 2
□ Local Subnet 3
□ Local Subnet 4
☑ Wireless Common
□ Wireless 1
□ Wireless 2

6. Click **Next**. FlexMaster displays the *Create a Template Wireless Common* page.

Figure 98. Example: Enter the Wireless Common values for the parameters that you want to auto configure



Notes

Save time configuring devices by using configuration templates. Device settings, such as SSIDs, login information, and L2TP settings, can be applied to multiple devices at the same time by deploying a configuration template.

Config Templates

Template Name	Created by	Created	Supported Models	Actions
7781-cm-s	bin	Jan. 22 2013 23:08:02	7781CM-S	View Edit Delete Copy Export
7781-cm-e	bin	Jan. 22 2013 23:06:39	ZF7781CM-E	View Edit Delete Copy Export
7781cm-p	bin	Jan. 22 2013 22:31:48	ZF7781CM	View Edit Delete Copy Export
test	ives	Jan. 22 2013 00:22:35	ZF7321-U	View Edit Delete Copy Export
corfu-cm	bin	Jan. 21 2013 18:27:23	ZF7781CM	View Edit Delete Copy Export

Number of templates: 12

CREATE A TEMPLATE

Template Name: 2942 Autoconfigure

Product Type: ZF2942

Wireless Common

	Parameter	Value
□	Wireless Mode:	Auto-select The device will reboot automatically if the Wireless Mode is changed. AP firmware with version 8.0 is not support 802.11b mode.
☑	Channel:	SmartSelect
☑	Country Code:	Brazil The device will reboot automatically if the Country Code is changed.
□	Transmit Power:	Full
□	Protection Mode:	● Disabled ○ CTS-only ○ RTS-CTS
□	External Antenna:	● Disabled ○ Enabled

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

7. In *Wireless Common*, change the required parameters.

NOTE: When you are creating a configuration template that includes wireless radio settings, make sure that the radio channel you select is authorized in your country. To ensure that you are using an authorized radio channel, select the correct *Country Code* for the location in which you operate the access points, and then select **SmartSelect** for the channel.

NOTE: To configure VLANs, you must do so on a per-device basis from the Device View. You cannot completely configure VLAN settings through the template options. For more on the Device View, refer to Managing a Single Standalone Access Point.

8. Click **Next**.
9. When you reach the *Configuration Parameters and Values* page, a summary of the configurations you have specified are displayed. If FlexMaster detected any errors, then the corresponding fields are flagged in red.

   Also on this page is the *Persist selected settings after a factory reset* check box. If this check box is selected, then all attributes that are provisioned to one or more devices have precedence over the factory default settings, even if the device is reset to factory defaults. If this check box is cleared, then the parameters provisioned in this template reverts to factory defaults after a factory reset.
10. Click **Save** to save your configuration template.

Step C: Define the Target Devices for Auto Configuration

The next step is to specify the devices that are automatically configured when they register with FlexMaster. You can either create a device view and use that as the target group for auto configuration, or upload an inventory file that lists the target devices.

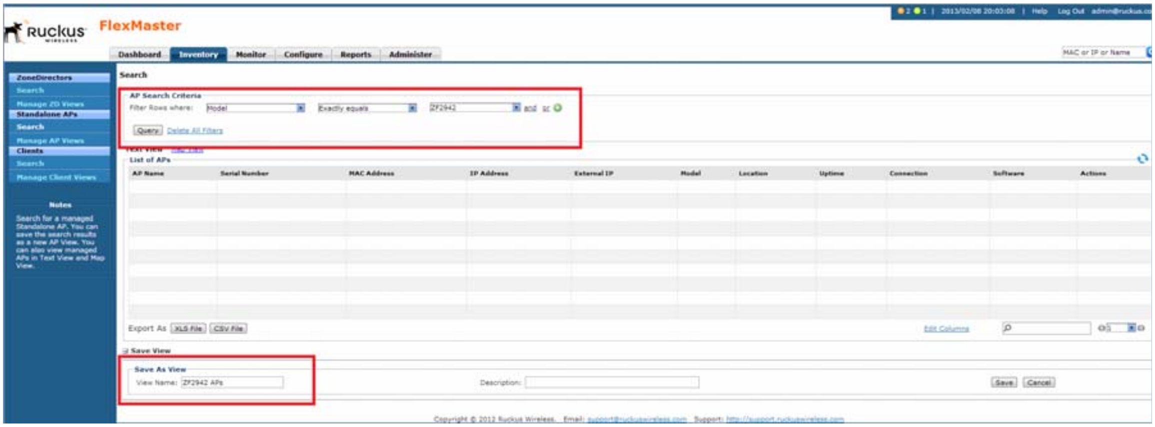
Option 1: Search and Save As a Device View

The easiest way to create a device view is to perform a search based on a specific attribute, and then save the search results as a device group.

For example, when you want to create a group consisting of ZoneFlex 2942 devices only, select Standalone APs in Select a Device Category, run a search using *Model* > *Exactly Equals* > *ZF2942*, and then save the results as a device view. Use a descriptive name for the view; you select this name as the target view later when you create an auto configuration task.

For instructions on how to run a search and save the results as a view, refer to Creating a Standalone AP View and Creating a ZD View.

Figure 99. Running a search for ZoneFlex 2942 devices



Filter Rows where: Model | Exactly equals | ZF2942 and or

View Name: ZF2942 APs

Description:

Copyright © 2012 Ruckus Wireless.

Option 2: Upload an Inventory File of Devices to Auto Configure

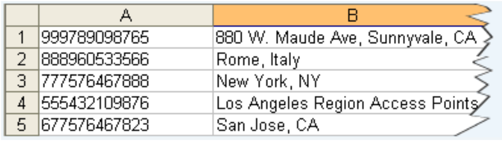
When you have a specific list of devices that you want to auto configure, you can create an inventory file using Microsoft Excel and list the serial numbers of these devices. In addition to the serial numbers, you must also specify a "tag" for each device in the list. These tags function as "group names" that you can use as target groups when you create an auto configuration task.

NOTE: If you disabled auto approval of devices on the *Registration Status* tab of the *Configure* > *Common* > *Device Registration* page, then you need to upload an inventory file for FlexMaster to auto configure devices.

Follow these steps to create and upload an inventory file.

1. Open a blank Microsoft Excel sheet.
2. In Column A, type the serial numbers of all Ruckus Wireless devices that you want to include in the inventory file.
3. In Column B, assign a tag to each device in the list. These tags function as the group names for the devices in the list.

Figure 100. Sample inventory file



	A	B
1	999789098765	880 W. Maude Ave, Sunnyvale, CA
2	888960533566	Rome, Italy
3	777576467888	New York, NY
4	555432109876	Los Angeles Region Access Points
5	677576467823	San Jose, CA

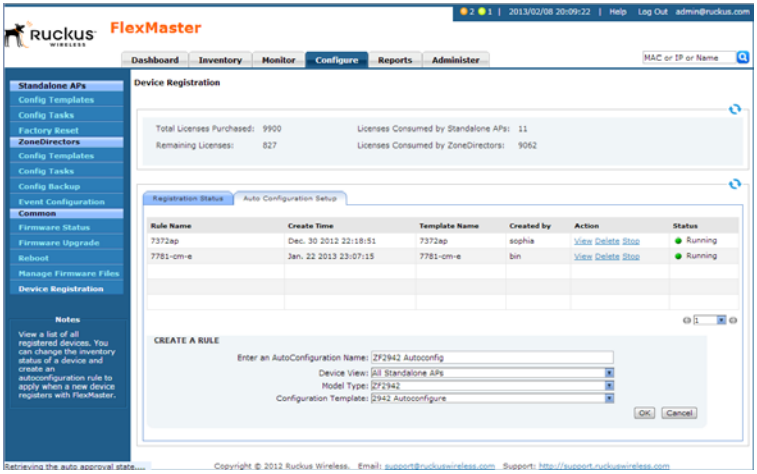
4. Save the file in .XLS format.
5. On the FlexMaster Web interface, go to the *Configure* > *Common* > *Device Registration* page.
6. On the *Registration Status* tab, click the **Upload a Device Inventory File** link at the bottom of the page.
7. In *Pre-Registration Data,* click **Choose File**.
8. Go to the location of the inventory file (in .XLS format) that you saved earlier, and then click **Open**.
9. Click **OK**.

The Web interface refreshes and a message appears at the top of the page, informing you that the inventory file has been uploaded successfully. The tags that you assigned to each device appear in the *Auto-Config* column on the *Registration Status* tab.

Step D: Create the Auto Configuration Task

1. Go to the *Configure* > *Common* > *Device Registration* page.
2. On the *Device Registration* page, click the **Auto Configuration Setup** tab.
3. Click **Create a rule**.
4. In *Enter an AutoConfiguration Name,* type a name that you want to assign to the auto configuration task.
5. In *Device View,* select the device view to which you want to deploy the auto configuration task. Options include the default device view, *All Standalone APs*, as well any device views you have created. If you uploaded an inventory file, then the tag names that you assigned to the devices in the group function as group names.

Figure 101.   Creating an auto configuration task for ZoneFlex 2942 access points



Device Registration

Total Licenses Purchased: 9900
Remaining Licenses: 827
Licenses Consumed by Standalone APs: 11
Licenses Consumed by ZoneDirectors: 9062

Rule Name	Create Time	Template Name	Created by	Action	Status
7372ap	Dec. 30 2012 22:18:51	7372ap	sophia	View Delete Stop	● Running
7781-cm-e	Jan. 22 2013 23:07:15	7781-cm-e	bin	View Delete Stop	● Running

CREATE A RULE

Enter an AutoConfiguration Name: ZF2942 Autoconfig
Device View: All Standalone APs
Model Type: ZF2942
Configuration Template: 2942 Autoconfigure

Notes

View a list of all registered devices. You can change the inventory status of a device and create an autoconfiguration rule to apply when a new device registers with FlexMaster.

Retrieving the auto approval state....

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

6. In *Model Type*, select the model number of the target device. Available options include:

- VF2811 (MediaFlex 2811 Adapter)
- VF2825 (MediaFlex 2825 AP)
- VF7811 (MediaFlex 7811 Adapter)
- ZF2741 (ZoneFlex 2741 Outdoor AP)
- ZF2925 (ZoneFlex 2925 802.11g AP)
- ZF2942 (ZoneFlex 2942 802.11g AP)
- ZF7025 (ZoneFlex 7025 Multiservice 802.11n Wired/Wireless Wall Switch)
- ZF7055 (ZoneFlex 7055 Dual-Band Multimedia Wi-Fi Wall Switch)
- ZF7321 (ZoneFlex Smart Dual-Band Selectable 802.11n Access Point)
- ZF7321-U (ZoneFlex Smart Dual-Band Selectable 802.11n AP with USB)
- ZF7341 (ZoneFlex 7341 2.4GHz 802.11n Smart Wi-Fi AP)
- ZF7341-U (ZoneFlex 7300 Series Dual Band 802.11n Indoor AP with USB)
- ZF7343 (ZoneFlex 7363 802.11n Indoor Single-Band AP)
- ZF7343-U (ZoneFlex 7300 Series Dual Band 802.11n Indoor AP with USB)
- ZF7351 (ZoneFlex 7351 802.11n Multimedia Wi-Fi Access Point)
- ZF7351-U (ZoneFlex 7351 802.11n Multimedia Wi-Fi Access Point with USB)
- ZF7352 (ZoneFlex 7352 Indoor Single-Band AP)
- ZF7363 (ZoneFlex 7363 802.11n Indoor Dual-Band AP)
- ZF7363-U (ZoneFlex 7300 Series Dual Band 802.11n Indoor AP with USB)
- ZF7372 (ZoneFlex 7372 Indoor Dual-Band AP)
- ZF7372-E (ZoneFlex 7372-E Indoor Dual-Band AP)
- ZF7731 (ZoneFlex 7731 802.11n Bridge AP)
- ZF7761CM (ZoneFlex 7761-CM Cable Modem AP)
- ZF7762 (ZoneFlex 7762 802.11n Outdoor AP)
- ZF7762-AC (ZoneFlex 7762-AC 802.11n Outdoor AP)

- ZF7762-N (ZoneFlex 7762-N 802.11n Outdoor AP)
- ZF7762-S (ZoneFlex 7762-S 802.11n Outdoor Sector AP)
- ZF7762-S-AC (ZoneFlex 7762-S-AC 802.11n Outdoor Sector AP)
- ZF7762-T (ZoneFlex 7762-T Dual Band 802.11n Outdoor AP)
- ZF7781CM (ZoneFlex 7781CM AP with Cable Modem)
- ZF7781CM-E (ZoneFlex 7781CM-E AP with Cable Modem)
- ZF7781CM-S (ZoneFlex 7781CM-S AP with Cable Modem)
- ZF7781FN (ZoneFlex 7781FN AP with Fiber Node)
- ZF7781FN-E (ZoneFlex 7781FN-E AP with Fiber Node)
- ZF7781FN-S (ZoneFlex 7781FN-S AP with Fiber Node)
- ZF7781-M (ZoneFlex 7781-M AP)
- ZF7782 (ZoneFlex 7782 Dual Band 802.11n Outdoor Omni AP)
- ZF7782-E (ZoneFlex 7782-E Dual Band 802.11n Outdoor External Antenna AP)
- ZF7782-N (ZoneFlex 7782-T Dual Band 802.11n 30-Degree Narrow Sector Outdoor AP)
- ZF7782-S (ZoneFlex 7782-S Dual Band 802.11n Outdoor 120-Degree Sector AP)
- ZF7942 (ZoneFlex 7942 Smart Wi-Fi 802.11n AP)
- ZF7962 (ZoneFlex 7962 Dual-Band 802.11n Smart Wi-Fi AP)
- ZF7982 (ZoneFlex 7982 Dual-Band 802.11n Smart Wi-Fi AP)
- SC8800-S (Small Cell 8800 AP)
- SC8800-S-AC (Small Cell 8800 AP)

7. In **Configuration Template**, select the configuration template that you want to use to auto configure the target device view.

NOTE: The target device model and the configuration template must match. For example, if the target device view consists of ZoneFlex 2942, then the configuration template must be configured for ZoneFlex 2942. If these do not match, then you are unable to save the auto configuration task.

8. Click **OK**.

The Web interface refreshes and the auto configuration task appears in the *Auto Configuration Setup* table.

Note that an auto configuration task cannot be edited once you create it. You can only view the task status, stop the task, or delete the task.

- To view the task status, click the **View** link on the *Device Registration* page.
- To stop the task, click the **Stop** link. The page refreshes, and the task status changes from *Running* to *Cancelled.* To start the task again, click the **Restart** link.
- To delete the task, click the **Delete** link. The page refreshes, and the task status changes to *Cancelled.* To start the task again, click the **Restart** link.

You have completed creating an auto configuration task. To create another auto configuration task (for example, for a different device view or with a different set of settings), repeat the same procedure.

How to Tell Which Devices Were Auto Configured

When the auto configuration template that you created and deployed only covers basic device settings, it is important to be able to tell which devices were auto configured. This way, you can configure additional settings later on, if necessary.

To check which devices were auto configured, go to the *Registration Status* tab (under *Configure > Common > Device Registration*). The *Auto-Config* column shows two types of icons that indicate the auto registration status of a device:

- ✓ means auto configured
- ✗ means not auto configured

If a template was used to auto-configure a device, then the Template Name appears in the *Template* column.

Provisioning Tasks to ZoneDirector Devices

This section describes how to create ZoneDirector configuration templates and provision these to ZoneDirector devices. It also describes how to back up ZoneDirector settings and restore them to the original ZoneDirector device or another ZoneDirector device of the same model.

Working with ZoneDirector Configuration Templates

ZoneDirector configuration templates as similar to AP configuration templates, only this time, the target devices are managed ZoneDirector devices and the configuration settings that need to be upgraded are different.

NOTE: When redundant ZoneDirector devices (one active ZoneDirector and one standby ZoneDirector) exist on the network, note that FlexMaster only provisions configuration templates to the active ZoneDirector. When you select the target ZoneDirector devices to provision with a template, standby ZoneDirector devices are automatically filtered from the list. Once the active ZoneDirector device is provisioned, it automatically synchronizes its settings with the standby ZoneDirector device.

Creating a ZoneDirector Configuration Template

NOTE: Before creating a ZoneDirector configuration template, you must have saved at least one configuration file for the target ZoneDirector. For information on how to back up ZoneDirector configuration, refer to Immediately Backing Up ZoneDirector Configurations.

1. Go to *Configure* > *ZoneDirectors* > *Config Templates.*
2. Click **Create a template**. The *CREATE A TEMPLATE* configuration form opens at the bottom of the page.
3. In *Template Name,* type a name for the configuration template that you are creating.
4. In *ZoneDirector Database Backup Configuration,* select a backup configuration that you use as base configuration for the template that you are creating. You need to make modifications to the backup configuration to create your ZoneDirector configuration template.
5. Click **Next**. FlexMaster displays the *WLANs*, *Access Point Policies*, *Hotspot Services*, *AAA Servers*, and *System* tabs.
6. Under each of the *WLANs*, *Access Point Policies*, *Hotspot Services*, *AAA Servers*, and *System* tabs, make required changes to the device parameters. After making changes, click **Apply** or **OK** to save your changes to the template.

NOTE: For instructions on how to configure the ZoneDirector settings (for example, WLAN settings), refer to the *ZoneDirector User Guide* or *ZoneDirector Online Help.*

7. After you have made all required changes, click **Save** to finish creating the ZoneDirector configuration template.

The page refreshes, and the ZoneDirector configuration template that you created appears in the list of available templates.

Editing a ZoneDirector Configuration Template

1. Go to *Configure > ZoneDirectors > Config Templates.* A list of templates that you have created appears on the page.
2. Click the ZoneDirector configuration template **Edit** link. The *EDIT* pane appears at the bottom of the page, displaying the *WLANs*, *Access Point Policies*, *Hotspot Services*, *AAA Servers*, and *System* tabs.
3. Under each of the *WLANs*, *Access Point Policies*, *Hotspot Services*, *AAA Servers*, and *System* tabs, make changes to the device parameters as required. After making changes, click **OK** and/or **Apply** to save your changes to the template.

NOTE: For instructions on how to configure the ZoneDirector settings (for example, WLAN settings), refer to the *ZoneDirector User Guide* or *ZoneDirector Online Help.*

4. After you have made all required changes, click **Save** to finish creating the ZoneDirector configuration template.

Deleting a ZoneDirector Configuration Template

1. Go to *Configure > ZoneDirectors > Config Templates.* A list of templates that you have created appears on the page.
2. Click the ZoneDirector configuration template **Delete** link. A confirmation message appears.
3. Click **OK**.

The page refreshes, and the configuration task that you deleted disappears from the list.

Working with ZoneDirector Event Configuration

Managed ZoneDirector devices generate a significant number of events, which makes the task of monitoring critical ZoneDirector events challenging. To ensure that you are notified about ZoneDirector events that are critical to your organization, you can define the events that you want to show on the Events widget on the Dashboard.

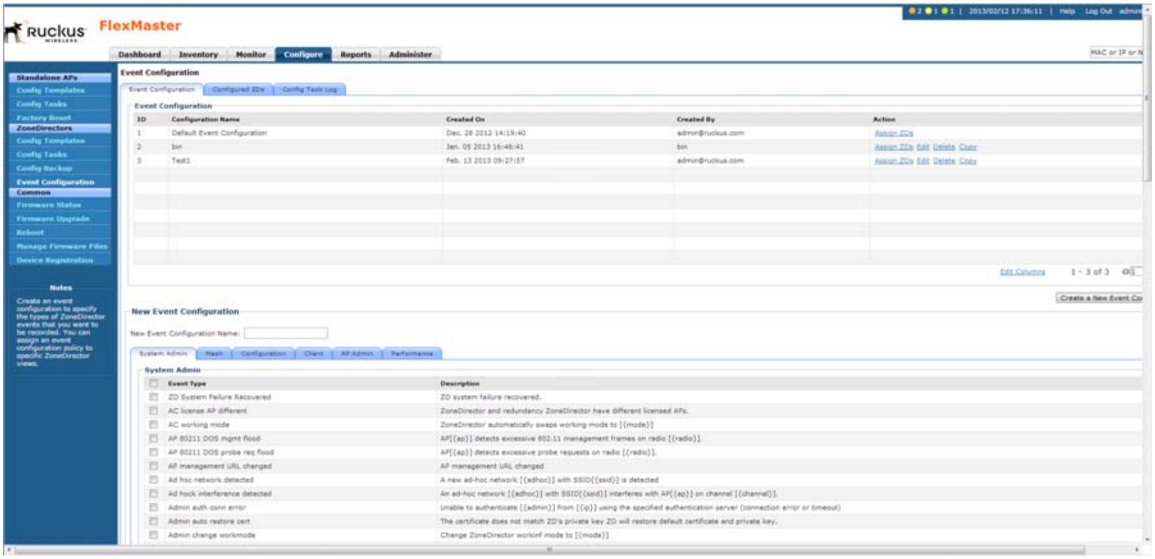
Creating a ZoneDirector Event Configuration

A ZoneDirector event configuration named *Default Event Configuration* exists. This default event configuration includes all important ZoneDirector events defined by Ruckus Wireless.

When you want to a smaller set of events (for example, critical-only) to appear on the *Events* widget, you can create a custom event configuration and assign it to managed ZoneDirector devices.

1. Go to *Configure > ZoneDirectors > Event Configuration*. The *Event Configuration* tab displays the event configurations that have been created.
2. Click the **Create a New Event Configuration** button at the bottom-right corner of the page. The *New Event Configuration* form appears, displaying six tabs that categorize the different types of ZoneDirector events. These tabs include:
   - *System Admin*: Includes administration and security related events, such as administrator logins and rogue AP detection, among others.
   - *Mesh:* Includes mesh related events, such as mesh activation on an AP and mesh isolation detection, among others.
   - *Configuration:* Includes configuration events, such as changing management IP address, changing password, and enabling the built-in DHCP, among others.
   - *Client:* Includes client events, such as client join, disconnection, and session expiration, among others
   - *AP Admin:* Includes AP events that may need your attention, such as failed authorization, failed image upgrade, and AP reset, among others.
   - *Performance:* Includes the results of SpeedFlex tests that have been performed.

Figure 102. The New Event Configuration form appears at the bottom of the page



Create an event configuration to specify the types of ZoneDirector events that you want to be recorded. You can assign an event configuration policy to specific ZoneDirector views.

Event Configuration

ID	Configuration Name	Created On	Created By	Action
1	Default Event Configuration	Dec. 28 2012 14:19:40	admin@ruckus.com	Assign ZDs
2	bin	Jan. 05 2013 16:46:41	bin	Assign ZDs Edit Delete Copy
3	Test1	Feb. 13 2013 09:27:57	admin@ruckus.com	Assign ZDs Edit Delete Copy

New Event Configuration

New Event Configuration Name:

System Admin

☐	Event Type	Description
☐	ZD System Failure Recovered	ZD system failure recovered.
☐	AC license AP different	ZoneDirector and redundancy ZoneDirector have different licensed APs.
☐	AC working mode	ZoneDirector automatically swaps working mode to [{mode}]
☐	AP 80211 DOS mgmt flood	AP[{ap}] detects excessive 802.11 management frames on radio [{radio}].
☐	AP 80211 DOS probe req flood	AP[{ap}] detects excessive probe requests on radio [{radio}].
☐	AP management URL changed	AP management URL changed
☐	Ad hoc network detected	A new ad-hoc network [{adhoc}] with SSID[{ssid}] is detected
☐	Ad hock interference detected	An ad-hoc network [{adhoc}] with SSID[{ssid}] interferes with AP[{ap}] on channel [{channel}].
☐	Admin auth conn error	Unable to authenticate [{admin}] from [{ip}] using the specified authentication server (connection error or timeout)
☐	Admin auto restore cert	The certificate does not match ZD's private key ZD will restore default certificate and private key.
☐	Admin change workmode	Change ZoneDirector workinf mode to [{mode}]

3. In *New Event Configuration Name*, type a name that you want to assign to this event configuration. For example, when you are including only critical ZoneDirector events in this event configuration, you can type **`Critical ZD Events`**.

NOTE: The default settings in the *New Event Configuration* form are exactly the same as the settings in *Default Event Configuration*.
To ensure that only events that you consider important are included in the event configuration that you are creating, clear all the check boxes on all tabs before selecting those that you want to include in the new event configuration. You can clear or unselect all check boxes on each tab the clicking the check box next to *Event Type* twice – the first click selects all check boxes and the second click clears them all.

4. Click each of the event type tabs, and then select the check boxes for the ZoneDirector events that you want to include in the new event configuration.
5. Click **Save**. The event configuration that you created appears in the *Event Configuration* table.

You have completed creating a new ZoneDirector event configuration. To apply this event configuration to ZoneDirector devices, refer to Assigning an Event Configuration to ZoneDirector Devices.

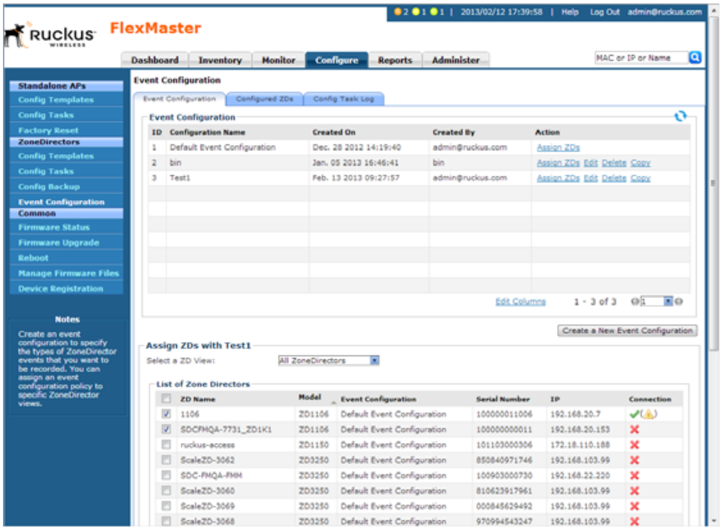
Assigning an Event Configuration to ZoneDirector Devices

After you create an event configuration, you need to assign it to the ZoneDirector devices that you want to send notifications for the events that you defined in the event configuration template. Assigning an event configuration creates a provisioning task that deploys that particular event configuration to the target ZoneDirector devices.

NOTE: You can only assign one event configuration to each ZoneDirector device.

1. Go to *Configure* > *ZoneDirectors* > *Event Configuration.*
2. On the *Event Configuration* tab, look for the event configuration that you want to assign to ZoneDirector devices.
3. Click the **Assign ZDs** link that is in the same row as the event configuration that you want to assign. The *Assign ZDs with {Event Configuration Name}* form appears at the bottom of the page.

Figure 103. Assigning an event configuration to ZoneDirector devices



Notes

Create an event configuration to specify the types of ZoneDirector events that you want to be recorded. You can assign an event configuration policy to specific ZoneDirector views.

Event Configuration

ID	Configuration Name	Created On	Created By	Action
1	Default Event Configuration	Dec. 28 2012 14:19:40	admin@ruckus.com	Assign ZDs
2	bin	Jan. 05 2013 16:46:41	bin	Assign ZDs Edit Delete Copy
3	Test1	Feb. 13 2013 09:27:57	admin@ruckus.com	Assign ZDs Edit Delete Copy

1 - 3 of 3

Assign ZDs with Test1

Select a ZD View: All ZoneDirectors

List of Zone Directors

□	ZD Name	Model	Event Configuration	Serial Number	IP	Connection
☑	1106	ZD1106	Default Event Configuration	100000011006	192.168.20.7	✓(⚠)
☑	SDCFMQA-7731_ZD1K1	ZD1106	Default Event Configuration	100000000011	192.168.20.153	✗
□	ruckus-access	ZD1150	Default Event Configuration	101103000306	172.18.110.188	✗
□	ScaleZD-3062	ZD3250	Default Event Configuration	850840971746	192.168.103.99	✗
□	SDC-FMQA-FMM	ZD3250	Default Event Configuration	100903000730	192.168.22.220	✗
□	ScaleZD-3060	ZD3250	Default Event Configuration	810623917961	192.168.103.99	✗
□	ScaleZD-3069	ZD3250	Default Event Configuration	000845629492	192.168.103.99	✗
□	ScaleZD-3068	ZD3250	Default Event Configuration	970994543247	192.168.103.99	✗

4. In *Select a ZD View,* select the ZoneDirector view from which you want to select ZoneDirector devices. The default *All ZoneDirectors* view and all custom ZoneDirector views appear in the list.

   The List of ZoneDirectors table refreshes, and then displays the ZoneDirector devices that belong to the selected view.
5. Select the check boxes for the ZoneDirector devices to which you want to assign the event configuration. To select all ZoneDirector devices that are currently displayed on the page, click the check box next to the *ZD Name* column header.

Note that this only selects the devices on the current page. When there are devices listed on other pages, you need to go to those pages to select the devices.

NOTE: The *List of ZoneDirectors* table can show up to ten ZoneDirector devices at a time. When the selected view has more than ten ZoneDirector devices, you can view the succeeding pages that list the remaining devices by clicking the left and right arrows at the bottom of the page.

6. After you select the check boxes for all the ZoneDirector devices to which you want to assign the event configuration, click **Save** to save your changes.

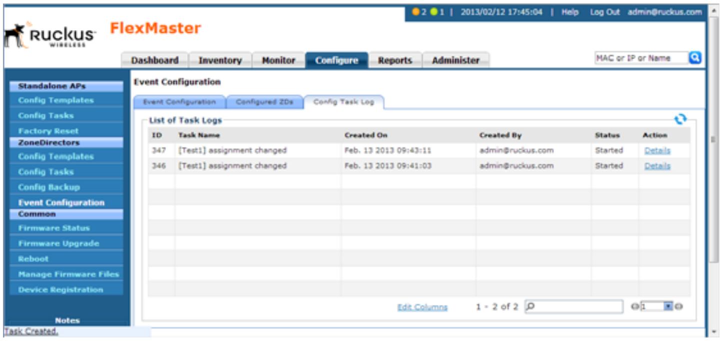
You have completed assigning ZoneDirector devices to the event configuration. To view the status of the task, refer to Viewing the Status of an Event Configuration Task.

Viewing the Status of an Event Configuration Task

After you assign ZoneDirector devices to an event configuration task, you can check the provisioning status of the task by going to the **Config Task Log** tab.

1. Go to *Configure* > *ZoneDirectors* > *Event Configuration*.
2. Click the **Config Task Log** tab.

Figure 104. Check the Status column for the status of the event configuration task



ID	Task Name	Created On	Created By	Status	Action
347	[Test1] assignment changed	Feb. 13 2013 09:43:11	admin@ruckus.com	Started	Details
346	[Test1] assignment changed	Feb. 13 2013 09:41:03	admin@ruckus.com	Started	Details

3. In the *List of Task Logs* table, look for the event configuration task that you want to view.
4. Check the *Status* column to determine the status of the task.

Typically, the *Status* column shows `Started` after you assign ZoneDirector devices to the event configuration. The status changes to `Success` when all target ZoneDirector devices have received and applied the event configuration task.

Viewing the Event Configuration Assigned to a ZoneDirector Device

1. Go to *Configure* > *ZoneDirectors* > *Event Configuration*.
2. Click the *Configured ZDs* tab.

3. In *Select a ZD View,* select the view from which to search for ZoneDirector devices.
4. View all devices in the view or create a filter to search for specific ZoneDirector devices.
   - To display all ZoneDirector devices within the selected view, click **Query**. The *List of ZDs* table appears and lists ZoneDirector details. The *Configuration* column displays the event configuration that is currently assigned to each ZoneDirector device.
   - To search for specific ZoneDirector devices, configure the filter settings by doing the following:

     i. In the first drop-down list box after *Filter Rows where,* select the search attribute that you want to use. Options include name, serial number, IP address, external IP address, model, and last seen (among others).

     ii. In the second drop-down list box, select the search operator that you want to use. Available search operators include:

     – *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered `172.17.16.176` as the search parameter, then only devices with this IP address appear in the search results.

     – *Contains:* Search for devices with attributes that include the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered `100` as the search parameter, then all devices with "100" in the IP address (for example, `172.17.16.`**`100`** and **`100`**`.1.10.13`) appear in the search results.

     – *Starts with:* Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered `3208` as the query parameter, then only devices with serial numbers that begin with "3208" (for example, `320833000219)` appear in the search results.

     – *Ends with:* Search for devices with attributes that end with the query parameter you entered. For example, if you selected **IP address** as the attribute and you entered `13` as the query parameter, then only devices with model names that end in "13" (for example, `100.1.10.`**`13`**) appear in the search results.

     After you select a search operator, a third text box appears.

     iii. In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.

     iv. If you want to add another search filter, then click ⊕. A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.

     v. When you complete setting up the search filters, click **Query**. The *List of ZDs* table appears and lists ZoneDirector details. The *Configuration* column displays the event configuration that is currently assigned to each ZoneDirector device.

Performing a ZoneDirector Configuration Upgrade

Performing a ZoneDirector configuration upgrade refers to provisioning a ZoneDirector configuration template to a single or a group of ZoneDirector devices (similar to creating a configuration upgrade task for APs).

Before you can deploy a ZoneDirector configuration template, you must have already created a ZoneDirector configuration template. For instructions on how to create a ZoneDirector template, refer to Creating a ZoneDirector Configuration Template.

NOTE: Configuration, firmware, reboot, and factory reset tasks can be deleted. Tasks that have not yet started, however, can be cancelled, although they remain on the FlexMaster database. By keeping all user actions on the database, FlexMaster can produce accurate audit logs of system configuration activities.

Creating a ZoneDirector Configuration Upgrade Task

1. Go to *Configure > ZoneDirectors > Config Tasks.*
2. Click **Create a task**. The *CREATE A TASK* pane opens at the bottom of the page.
3. In the *Task Settings* section, do the following:
   - In *Specify a task name,* type a name that you want to assign to this ZoneDirector configuration task.
   - In *Select configuration type,* click **Configuration**.

NOTE: A **Restore** option, which allows you to restore the backup settings to a ZoneDirector device, appears next to **Configuration**. For information on how to use the Restore option, refer to Restoring a ZoneDirector Configuration.

   - In *Select configuration file,* select the ZoneDirector configuration template that you want to deploy.
4. In *Select ZoneDirectors to restore,* choose the target ZoneDirector devices.
   - When you want to apply the template to a group of ZoneDirector devices, click the **Select View** tab, and then select the target ZoneDirector view from the drop-down list. All default and custom ZoneDirector views appear in the drop-down list. Note that when the template is model-specific, the settings in the template are only applied to ZoneDirector devices that match the model.
   - When you want to apply the template to specific ZoneDirector devices, click the **Select Devices** tab, and then select the check boxes for the devices to which you want to deploy the configuration template. Note that when the template is model-specific, the settings in the template are only applied to ZoneDirector devices that match the model. If you select a device of a different model, then an error message appears when you save the configuration upgrade task.

NOTE: In addition to the default ZoneDirector device view (*All ZoneDirectors*), ZoneDirector device views that you manually created from search results also appear on the *Select View* tab. When you deploy a configuration template to a manually-created device view, only the current members of that view are marked for provisioning.

New ZoneDirector devices that match the view criteria but that registered with FlexMaster after the configuration task is created are not provisioned. You need to create a new configuration task to include these new devices.

5. In *Specify a time to perform this task*, specify when you want the task to run.
   - To run the task immediately, click **Perform this task now**.
   - To schedule the task, click **Schedule this task for later**, and then select the date and time.
6. Click **Save** to save the ZoneDirector configuration task.

   If FlexMaster detects a problem in the configuration upgrade task that you are saving, then an error message appears.

Backing Up and Restoring ZoneDirector Configuration

This section describes how to create and restore ZoneDirector device configuration backup files. The backup files can be created for single or multiple ZoneDirector devices. The following sections detail how to schedule automatic backups, create an immediate backup, and how to restore backups.

Ruckus Wireless strongly recommends that you periodically back up the settings of your ZoneDirector devices, to make sure that you can easily recover the configuration settings if they ever become corrupted.

NOTE: If your ZoneDirector device is behind a NAT server, then you need to set up port forwarding on the *Inventory* > *ZoneDirectors* > *Search* page. Click the ZoneDirector device **Edit** link, and then type the port forwarding settings in the *Device Web Port Number Mapping* box.

Continue with the following:

- Configuring the Number of ZoneDirector Configuration Backups
- Scheduling Automatic ZoneDirector Configuration Backups
- Immediately Backing Up ZoneDirector Configurations
- Restoring a ZoneDirector Configuration

Configuring the Number of ZoneDirector Configuration Backups

Operators can define the number of (between 10 and 100) ZoneDirector (ZD) configuration backups to retain in the FlexMaster database for each ZD. Note that saving more configuration backups requires more hard drive storage space.

1. Go to *Configure* > *ZoneDirectors* > *Config Backup*.
2. In the *Config Backup* window, change the entry in *Max number of backup files for each ZD:* to any number between 10 and 100 (default = 10).
3. Click **Update**.

Scheduling Automatic ZoneDirector Configuration Backups

1. Go to *Configure* > *ZoneDirectors* > *Config Backup*.
2. On the *Config Backup* page, click **Create a task**. FlexMaster displays the *Saved Views* tab.
3. Select the *Actions* check box(es) for the ZoneDirector device(s) to be backed up. The names of the targeted ZoneDirectors appear in the *Selected ZoneDirector* list at the bottom of the screen.

4. When you have completed the list of targeted ZoneDirector devices, type a name for the backup task in the *Enter a description for the Configuration* box. Use a descriptive name that helps you identify this backup configuration (especially if you are backing up multiple ZoneDirector configurations).
5. Select the *Schedule BackUp* check box. FlexMaster displays the *Schedule* dialog at the bottom of the screen.
6. In the *Schedule* dialog, select the **Frequency** and **Time of Day** for the automatic backups.
7. Click **Save**. FlexMaster saves your selections, and performs your backups as scheduled.
8. At any time, you can check your backup task in the *List of Backup Results* at the bottom of the screen. The list displays the status of your backup task.

Immediately Backing Up ZoneDirector Configurations

1. Go to *Configure > ZoneDirectors > Config Backup.*
2. On the *Config Backup* page, click **Create a task**. FlexMaster displays the *Saved Views* tab.
3. Select the *Actions* check box(es) for the ZoneDirector device(s) to be backed up. The names of the targeted ZoneDirectors appear in the *Selected ZoneDirector* list at the bottom of the screen.
4. When you have completed the list of targeted ZoneDirector devices, type a name for the backup task in the *Enter a description for the Configuration* box. Use a descriptive name that helps you identify this backup configuration (especially if you are backing up multiple ZoneDirector configurations).
5. Click **Save**. FlexMaster saves your selections, and immediately performs your backup.
6. After a few moments, check the *List of Backup Results* for your backup task. The list displays the status of your backup task.

Restoring a ZoneDirector Configuration

FlexMaster enables you to restore ZoneDirector settings easily from a backup file. You have the option to perform full or partial restore, and to restore to a group of ZoneDirector devices or a single ZoneDirector device.

Supported ZoneDirector Restore Types

FlexMaster supports three types of configuration restoration:

- *Full Restore:* Restores all settings from the backup file, including the IP address, system name, user name, and password. Use this restore type to overwrite all current settings of a ZoneDirector device with those from the backup file. For example, if the configuration file of a ZoneDirector device becomes corrupted, then you can use full restore to recover the ZoneDirector device.

- *Failover Restore:* Restores all settings from the backup file, except the system name, IP address, user name, and password. Use this restore type when you want to configure a secondary ZoneDirector device as a failover unit. After configuring the secondary ZoneDirector device, deploy it to the same network as the primary ZoneDirector device.

  If the primary ZoneDirector device fails for any reason, then all APs managed by the primary ZoneDirector device are able to report to the secondary ZoneDirector device automatically. If you choose this restore type, then you need to manually configure the IP address, system name, user name and password of the secondary ZoneDirector device.
- *Policy Restore:* Restores only the wireless, access control, role, and user settings from the backup file. Use this restore type when you want to apply the same set of common settings to multiple ZoneDirector devices. You need to first configure one ZoneDirector device with your preferred wireless, access control, role, and user settings, back up these settings, and then restore them onto the target ZoneDirector devices. Note that guest access settings and dynamic pre-shared key (PSK) data is not exported to the target devices. The target devices also retain their original IP address, system name, user name and password.

Performing the Restore Procedure

Before performing a restore procedure for ZoneDirector, make sure that you have at least one backup file that you can use to restore the ZoneDirector settings. If you have not created a backup file, then refer to Backing Up and Restoring ZoneDirector Configuration for more information.

Restoring ZoneDirector settings from a backup file overwrites the current settings with those contained in the backup file. When performing the restore procedure, make sure that:

- You are restoring the correct backup file.
- You are selecting the appropriate restore type. For example, when you only want to restore the wireless, access control, and user settings, make sure you select *Policy Restore*. Selecting *Full Restore* overwrites all existing ZoneDirector settings, including the IP address, system name, user name, and password.

Follow these steps to restore ZoneDirector settings from a backup file.

1. Go to *Configure > ZoneDirectors > Config Tasks.*
2. Click **Create a task**. The *CREATE A TASK* pane opens at the bottom of the page.
3. In the *Task Settings* section, do the following:
   - In *Specify a task name,* type a name that you want to assign to this ZoneDirector configuration task.
   - In *Select configuration type,* click **Restore**.
   - In *Select a configuration file*, select the ZoneDirector backup file that you want to use for the restore procedure. The settings (partial or complete, depending on the restore type) in this backup file are copied to the target ZoneDirector devices.

- In *Specify restore type*, select the type of restore that you want to perform. FlexMaster provides three restore types: **Full Restore**, **Failover Restore**, and **Policy Restore**. For help in deciding which restore type to choose, refer to Supported ZoneDirector Restore Types.

4. In *Select ZoneDirector to restore*, choose the target ZoneDirector devices.
    - When you want to apply the template to a group of ZoneDirector devices, click the **Select View** tab, and then select the target ZoneDirector view from the drop-down list. All default and custom ZoneDirector views appear in the drop-down list. Note that when the template is model-specific, the settings in the template are only applied to ZoneDirector devices that match the model.
    - When you want to apply the template to specific ZoneDirector devices, click the **Select Devices** tab, and then select the check boxes for the devices to which you want to deploy the configuration template. Note that when the template is model-specific, the settings in the template are only applied to ZoneDirector devices that match the model. If you select a device of a different model, then an error message appears when you save the configuration upgrade task.

NOTE: In addition to the default ZoneDirector device view (*All ZoneDirectors*), ZoneDirector device views that you manually created from search results also appear on the *Select View* tab. When you deploy a configuration template to a manually-created device view, only the current members of that group are marked for provisioning.

New ZoneDirector devices that match the view criteria but that registered with FlexMaster after the configuration task is created are not provisioned. You need to create a new configuration task to include these new devices.

5. In *Specify time for this task*, specify when you want the task to run.
    - To run the task immediately, click **Perform this task now**.
    - To schedule the task, click **Schedule this task for later**, and then select the date and time.
6. Click **Save** to save the ZoneDirector restore task, and then click **Confirm.** If FlexMaster detects a problem in the restore task that you are saving, then an error message appears.

To view the status of the task, check the Status column. For information on the possible tasks statuses, refer to Understanding the Status of a Task. When you are deploying the restore task to multiple devices (either to a device view or select ZoneDirector devices), click the **View** link in the *Actions* column to view the task status for each target device.

Provisioning Common Tasks

This section describes provisioning tasks that are common to ZoneDirector devices and standalone APs. Topics include:

- Working with Device Firmware
- Working with Reboot Tasks
- Managing Firmware Files
- Managing Device Registration
- Uploading a Device Inventory File
- Releasing Device Licenses

Working with Device Firmware

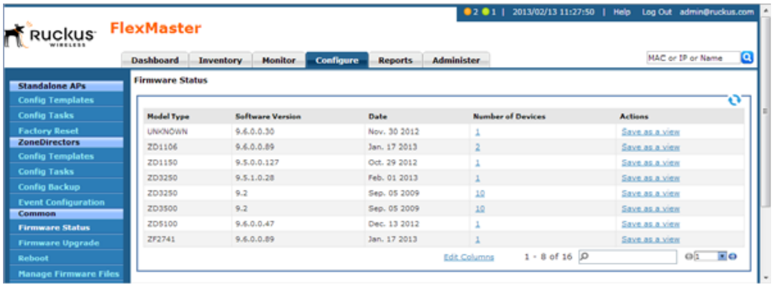
This section describes how to view firmware that is currently installed on managed devices and how to upgrade firmware on these devices.

NOTE: When redundant ZoneDirector devices (one active ZoneDirector and one standby ZoneDirector) exist on the network, note that FlexMaster only provisions firmware upgrades to the active ZoneDirector. When you select the target ZoneDirector devices to which to provision a firmware upgrade, standby ZoneDirector devices are automatically filtered from the list. Once the active ZoneDirector device is provisioned, it synchronizes its firmware automatically with the standby ZoneDirector device.

Viewing Firmware Installed on Managed Devices

To view the firmware versions that are currently installed on managed devices, go to the *Configure > Common > Firmware Status* page. The *Firmware Status* page displays the firmware versions that are installed on the managed devices based on the device models. See the following table for descriptions of the columns that appear on the page.

Figure 105. The Firmware Status page displays the firmware versions that are installed on managed devices



Firmware Status

Model Type	Software Version	Date	Number of Devices	Actions
UNKNOWN	9.6.0.0.30	Nov. 30 2012	1	Save as a view
ZD1106	9.6.0.0.89	Jan. 17 2013	2	Save as a view
ZD1150	9.5.0.0.127	Oct. 29 2012	1	Save as a view
ZD3250	9.5.1.0.28	Feb. 01 2013	1	Save as a view
ZD3250	9.2	Sep. 05 2009	10	Save as a view
ZD3500	9.2	Sep. 05 2009	10	Save as a view
ZD5100	9.6.0.0.47	Dec. 13 2012	1	Save as a view
ZF2741	9.6.0.0.89	Jan. 17 2013	1	Save as a view

NOTE: The table can show up to eight rows. If it has more than eight rows, then click the ➲ button at the bottom-right corner of the table to show the next eight rows.

Table 24. Columns on the Firmware Status table

Column Name	Description
Model Type	Model of the device.
Software Version	Version of the software/firmware that is currently installed on a device.
Date	Date when the firmware was uploaded to FlexMaster.
Number of Devices	Number of devices that are using this firmware.

Table 24. Columns on the Firmware Status table (Continued)

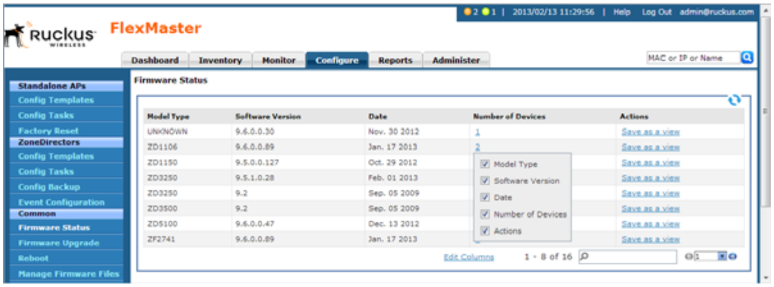
Column Name	Description
Actions	Shows the **Save as a view** link. Clicking this link shows options for saving devices in this group as a view, based on their firmware version.

Displaying and Hiding Columns

By default, FlexMaster displays all the available columns on the *Firmware Status* page. When you want to hide some of these columns, do the following:

1. Click the **Edit Columns** link at the bottom of the table. A box appears and displays check boxes for the table columns. By default, all check boxes are selected, which means all available columns are visible in the table.

Figure 106. To hide a column, clear or uncheck the check box for that column



Model Type	Software Version	Date	Number of Devices	Actions
UNKNOWN	9.6.0.0.30	Nov. 30 2012	1	Save as a view
ZD1106	9.6.0.0.89	Jan. 17 2013	2	Save as a view
ZD1150	9.5.0.0.127	Oct. 29 2012		Save as a view
ZD3250	9.5.1.0.28	Feb. 01 2013		Save as a view
ZD3250	9.2	Sep. 05 2009		Save as a view
ZD3500	9.2	Sep. 05 2009		Save as a view
ZD5100	9.6.0.0.47	Dec. 13 2012		Save as a view
ZF2741	9.6.0.0.89	Jan. 17 2013		Save as a view

☑ Model Type
☑ Software Version
☑ Date
☑ Number of Devices
☑ Actions

Edit Columns 1 - 8 of 16

2. To hide a column, clear the check box for that column. For example, to hide the date column, clear (or uncheck) the **Date** check box.
3. Click anywhere outside the box with check boxes when you are done.

You have completed hiding columns from the *Firmware Status* page.

To display a hidden column, click the **Edit Column** link, and then select the check box for the column that you want to display.

Creating a Firmware Upgrade Task

The Firmware Upgrade option enables the creation of tasks that upgrade the firmware of managed devices at a specified time. The task defines the devices to be upgraded, the firmware files to provision, and the time at which to perform the upgrade.

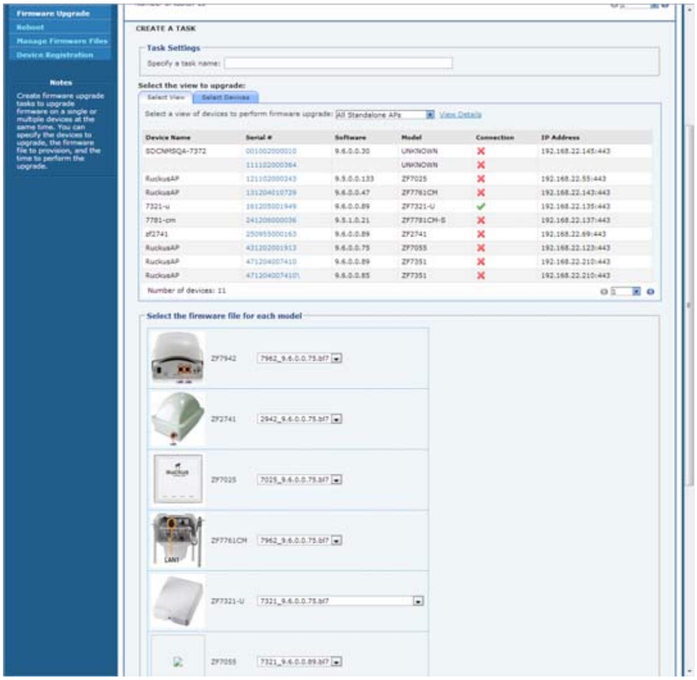
NOTE: Before creating a firmware upgrade task, you first need to upload one or more firmware files to FlexMaster by following the steps in Uploading a Firmware File.

NOTE: You need not accompany a firmware upgrade task with a reboot task. However, the new firmware does not become active until the next reboot. For more on rebooting, refer to Working with Reboot Tasks.

NOTE: Configuration, firmware, reboot, and factory reset tasks cannot be deleted. However, tasks that have not yet started can be cancelled, but they remain on the FlexMaster database. By keeping all user actions in the database, FlexMaster can produce accurate audit logs of system configuration activities.

1. Go to *Configure > Common > Firmware Upgrade.*
2. Click **Create a task**. The *CREATE A TASK* form appears at the bottom of the page.

Figure 107. Creating a firmware upgrade task



Notes

Create firmware upgrade tasks to upgrade firmware on a single or multiple devices at the same time. You can specify the devices to upgrade, the firmware file to provision, and the time to perform the upgrade.

CREATE A TASK

Task Settings

Specify a task name:

Select the view to upgrade:

Select a view of devices to perform firmware upgrade: All Standalone APs

Device Name	Serial #	Software	Model	Connection	IP Address
SDCNMSQA-7372	001002000010	9.6.0.0.30	UNKNOWN	✗	192.168.22.145:443
	111102000364		UNKNOWN	✗	
RuckusAP	121102000243	9.5.0.0.133	ZF7025	✗	192.168.22.55:443
RuckusAP	131204010729	9.6.0.0.47	ZF7761CM	✗	192.168.22.143:443
7321-u	161205001949	9.6.0.0.89	ZF7321-U	✓	192.168.22.135:443
7781-cm	241206000036	9.5.1.0.21	ZF7781CM-S	✗	192.168.22.137:443
zf2741	250955000163	9.6.0.0.89	ZF2741	✗	192.168.22.69:443
RuckusAP	431202001913	9.6.0.0.75	ZF7055	✗	192.168.22.123:443
RuckusAP	471204007410	9.6.0.0.89	ZF7351	✗	192.168.22.210:443
RuckusAP	4712040074101\	9.6.0.0.85	ZF7351	✗	192.168.22.210:443

Number of devices: 11

Select the firmware file for each model

ZF7942	7962_9.6.0.0.75.bl7
ZF2741	2942_9.6.0.0.75.bl7
ZF7025	7025_9.6.0.0.75.bl7
ZF7761CM	7962_9.6.0.0.75.bl7
ZF7321-U	7321_9.6.0.0.75.bl7
ZF7055	7321_9.6.0.0.89.bl7

3. In *Specify a task name,* type a name for the firmware upgrade task that you are creating.
4. Under *Select the view to upgrade,* do one of the following:
   - Click the **Select View** tab, and then toggle the *Select a view of devices to perform firmware upgrade* drop-down list to filter the list of devices based on a device view.
   - Click the **Select Devices** tab. And then, in the *Select* column, select the check box for each device you want to update.
5. Under *Select the firmware file for each model*, select the firmware file for each device type by selecting the desired firmware file from the drop-down list. Different types of devices require different firmware files. If a device in the group does not have a suitable firmware file, then that device is not updated.
6. (Optional) Mark the **Reboot the devices after upgrading the firmware** check box to reboot all groups of devices after firmware upgrade. You may choose to upgrade devices without immediate reboot, and then reboot them later, such as during an SLA-defined maintenance interval.

NOTE: You do not need to force a reboot with a firmware upgrade. However, the new firmware does not become active until the devices are rebooted.

7. Under *Specify a time to perform this task*, click when you want to perform this task:
   - **Perform this task now**: Run the task immediately after clicking **Save**.
   - **Schedule this task for later**: Specify the *Date* (yyyy-mm-dd) and *Time* (hh:mm) when the task should run.
8. Click **Save**. A pop-up window appears.
9. Click **OK** in the pop-up window to confirm the task.

NOTE: There may be a warning message when the Firmware Upgrade task is performed. For instance, when upgrading from 9.3 or 9.4 to 9.5, ZoneDirector may need more memory to upgrade.
You can either upgrade to the latest 9.4.2.0 or 9.3.4.0 first and then upgrade to 9.5. Or you can disconnect all the ZoneDirector APs and reboot the ZoneDirector to save memory.

Deleting a Firmware Upgrade Task

When you no longer use an existing firmware upgrade task, you can delete it.

1. Go to the *Configure > Common > Firmware Upgrade* page.
2. Look for the firmware upgrade task that you want to delete.
3. Click the **Delete** link that is in the same row as the task name. A confirmation message appears.
4. Click **OK** to continue.

The page refreshes, and the task that you deleted disappears from the list.

Working with Reboot Tasks

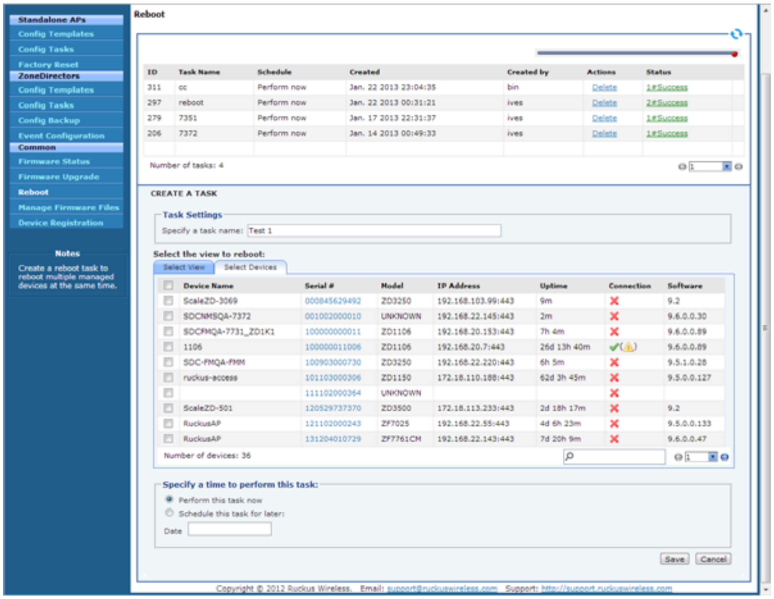
The Reboot option enables creation of tasks that reboot devices at a specified time. For example, your Change Management Policy may require a specific time window within which devices can be rebooted. Your service agreement specifies that on Sundays at 3:00 AM devices may be taken out of service for maintenance tasks, such as configuration changes, firmware upgrades, and rebooting. Since the device cannot forward end-user traffic during reboot, it goes out of service during the reboot, which takes approximately two minutes.

NOTE: Configuration, firmware, reboot, and factory reset tasks cannot be deleted. However, tasks that have not yet started can be cancelled, but they remain on the FlexMaster database. By keeping all of the user actions on the database, FlexMaster can produce accurate audit logs of system configuration activities.

Creating a Reboot Task

1. Go to *Configure* > *Common* > *Reboot.*
2. Click **Create a task**. The *CREATE A TASK* form appears at the bottom of the page.

Figure 108. Creating a reboot task



ID	Task Name	Schedule	Created	Created by	Actions	Status
311	cc	Perform now	Jan. 22 2013 23:04:35	bin	Delete	1#Success
297	reboot	Perform now	Jan. 22 2013 00:31:21	ives	Delete	2#Success
279	7351	Perform now	Jan. 17 2013 22:31:37	ives	Delete	1#Success
206	7372	Perform now	Jan. 14 2013 00:49:33	ives	Delete	1#Success

Number of tasks: 4

CREATE A TASK

Task Settings

Specify a task name: Test 1

Select the view to reboot:

Select View | Select Devices

□	Device Name	Serial #	Model	IP Address	Uptime	Connection	Software
□	ScaleZD-3069	000845629492	ZD3250	192.168.103.99:443	9m	✗	9.2
□	SDCNMSQA-7372	001002000010	UNKNOWN	192.168.22.145:443	2m	✗	9.6.0.0.30
□	SDCFMQA-7731_ZD1K1	100000000011	ZD1106	192.168.20.153:443	7h 4m	✗	9.6.0.0.89
□	1106	100000011006	ZD1106	192.168.20.7:443	26d 13h 40m	✓(⚠)	9.6.0.0.89
□	SDC-FMQA-FMM	100903000730	ZD3250	192.168.22.220:443	6h 5m	✗	9.5.1.0.28
□	ruckus-access	101103000306	ZD1150	172.18.110.188:443	62d 3h 45m	✗	9.5.0.0.127
□		111102000364	UNKNOWN			✗	
□	ScaleZD-501	120529737370	ZD3500	172.18.113.233:443	2d 18h 17m	✗	9.2
□	RuckusAP	121102000243	ZF7025	192.168.22.55:443	4d 6h 23m	✗	9.5.0.0.133
□	RuckusAP	131204010729	ZF7761CM	192.168.22.143:443	7d 20h 9m	✗	9.6.0.0.47

Number of devices: 36

Specify a time to perform this task:

● Perform this task now
○ Schedule this task for later:

Date

Save | Cancel

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

3. Type a name for your reboot task at *Specify a task name*.
4. Under *Select the view to reboot*, do the following:
   - Click the **Select View** tab, and then toggle the *Select a view of devices to perform reboot* drop-down list to filter the list of devices based on a device view. Default view include *All Standalone APs and All ZoneDirectors.*
   - Click the **Select Devices** tab, and then select the check box in the *Select* column for each device you want to update.
5. Under *Specify time to perform this task*, click when you want to perform this task:
   - **Perform this task now**: Run the task immediately after clicking **Save**.
   - **Schedule this task for later**: Specify the *Date* (yyyy-mm-dd) and *Time* (hh:mm) when the task should run.
6. Click **Save**.

Viewing the Status of a Reboot Task

View the status of the reboot task to check if it has started, completed successfully, or failed.

1. Go to *Configure* > *Common* > *Reboot.* A list of reboot tasks that you have created appears on the page.
2. In the *Status* column, check the value that appears on the same row as the task name:
   - *n#Scheduled*: Indicates that the configuration task has been successfully scheduled for *n* number of devices.

     To view the list of devices that have been scheduled, click **n#Scheduled** (hyperlink). The *Device Status* pane appears at the bottom of the page, displaying scheduled task information.
   - *n#Success*: Indicates that the configuration task has been provisioned successfully to *n* number of devices that have this status.

     To view the list of devices that have been provisioned successfully, click **n#Success** (hyperlink). The *Device Status* pane appears at the bottom of the page, displaying task details, device details, and task status.
   - *n#Fail*: Indicates that the configuration task failed on *n* number of devices.

     To view the list of devices on which provisioning failed, click **n#Fail** (hyperlink). The *Device Status* pane appears at the bottom of the page, displaying task details, device details, and task status. If the task failed, then click the **Detail** link in the *Failure* column to see what may have caused the task failure.

A few other statuses can appear in the *Status* column. For a complete list of possible statuses, refer to Understanding the Status of a Task.

Deleting a Reboot Task

1. Go to the *Configure* > *Common* > *Reboot* page.
2. Click the reboot task **Delete** link. A confirmation message appears.
3. Click **OK** to continue. The page refreshes, and the task that you deleted disappears.

Managing Firmware Files

The Manage Firmware Files option provides storage and management of Ruckus Wireless firmware files and packages. Firmware files and packages must be uploaded to FlexMaster for firmware upgrade tasks.

Once a firmware file or package has been uploaded to FlexMaster, the file or package can be provisioned to managed Ruckus Wireless devices as scheduled according to a firmware upgrade task. Each device model requires its own firmware; thus, firmware files and device models must be matched.

NOTE: You cannot delete a firmware file or package if it is being used by an existing scheduled firmware upgrade task.

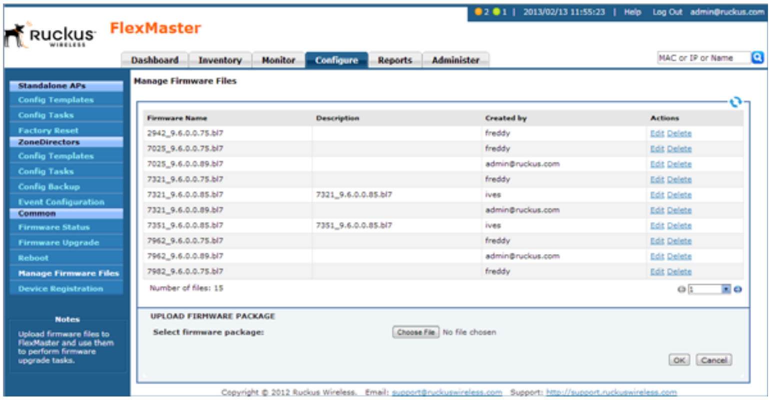
Each device model requires its own firmware; thus, firmware files and packages and device models must be matched.

Uploading a Firmware Package

Follow these steps to upload a firmware package to FlexMaster.

1. Go to *Configure > Common > Manage Firmware Files.*
2. Click **Upload firmware package**. The *UPLOAD FIRMWARE PACKAGE* form appears at the bottom of the page.

Figure 109. Uploading a firmware package



Manage Firmware Files

Firmware Name	Description	Created by	Actions
2942_9.6.0.0.75.bl7		freddy	Edit Delete
7025_9.6.0.0.75.bl7		freddy	Edit Delete
7025_9.6.0.0.89.bl7		admin@ruckus.com	Edit Delete
7321_9.6.0.0.75.bl7		freddy	Edit Delete
7321_9.6.0.0.85.bl7	7321_9.6.0.0.85.bl7	ives	Edit Delete
7321_9.6.0.0.89.bl7		admin@ruckus.com	Edit Delete
7351_9.6.0.0.85.bl7	7351_9.6.0.0.85.bl7	ives	Edit Delete
7962_9.6.0.0.75.bl7		freddy	Edit Delete
7962_9.6.0.0.89.bl7		admin@ruckus.com	Edit Delete
7982_9.6.0.0.75.bl7		freddy	Edit Delete

Number of files: 15

UPLOAD FIRMWARE PACKAGE

Select firmware package: No file chosen

Notes

Upload firmware files to FlexMaster and use them to perform firmware upgrade tasks.

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

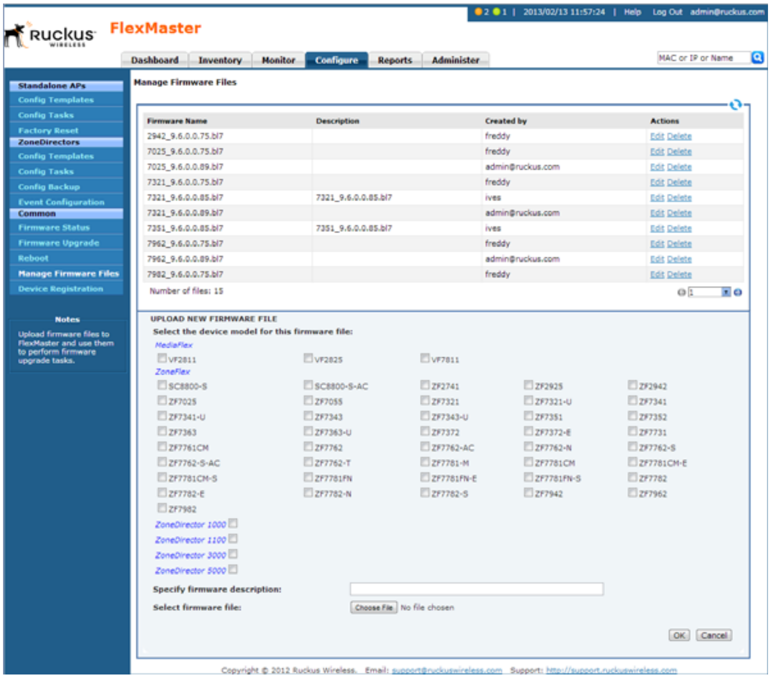
3. In *Select firmware package*, click **Choose File** to search your client workstation or other reachable location for the firmware package.
4. Click **OK** to upload the firmware package for storage on FlexMaster.

Uploading a Firmware File

Follow these steps to upload a firmware file to FlexMaster.

1. Go to *Configure* > *Common* > *Manage Firmware Files.*
2. Click **Upload new firmware file**. The *UPLOAD NEW FIRMWARE FILE* form appears at the bottom of the page.

Figure 110. Uploading a firmware file



Manage Firmware Files

Firmware Name	Description	Created by	Actions
2942_9.6.0.0.75.bl7		freddy	Edit Delete
7025_9.6.0.0.75.bl7		freddy	Edit Delete
7025_9.6.0.0.89.bl7		admin@ruckus.com	Edit Delete
7321_9.6.0.0.75.bl7		freddy	Edit Delete
7321_9.6.0.0.85.bl7	7321_9.6.0.0.85.bl7	ives	Edit Delete
7321_9.6.0.0.89.bl7		admin@ruckus.com	Edit Delete
7351_9.6.0.0.85.bl7	7351_9.6.0.0.85.bl7	ives	Edit Delete
7962_9.6.0.0.75.bl7		freddy	Edit Delete
7962_9.6.0.0.89.bl7		admin@ruckus.com	Edit Delete
7982_9.6.0.0.75.bl7		freddy	Edit Delete

Number of files: 15

UPLOAD NEW FIRMWARE FILE

Select the device model for this firmware file:

MediaFlex

□ VF2811 □ VF2825 □ VF7811

ZoneFlex

□ SC8800-S □ SC8800-S-AC □ ZF2741 □ ZF2925 □ ZF2942
□ ZF7025 □ ZF7055 □ ZF7321 □ ZF7321-U □ ZF7341
□ ZF7341-U □ ZF7343 □ ZF7343-U □ ZF7351 □ ZF7352
□ ZF7363 □ ZF7363-U □ ZF7372 □ ZF7372-E □ ZF7731
□ ZF7761CM □ ZF7762 □ ZF7762-AC □ ZF7762-N □ ZF7762-S
□ ZF7762-S-AC □ ZF7762-T □ ZF7781-M □ ZF7781CM □ ZF7781CM-E
□ ZF7781CM-S □ ZF7781FN □ ZF7781FN-E □ ZF7781FN-S □ ZF7782
□ ZF7782-E □ ZF7782-N □ ZF7782-S □ ZF7942 □ ZF7962
□ ZF7982

ZoneDirector 1000 □
ZoneDirector 1100 □
ZoneDirector 3000 □
ZoneDirector 5000 □

Specify firmware description:

Select firmware file: Choose File No file chosen

OK Cancel

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

3. Under *Select the device model for this firmware file*, select the check box before the Ruckus Wireless device to specify the product and model to which the firmware applies. Device models are grouped according to product names: MediaFlex, ZoneFlex, and ZoneDirector.
4. In *Specify firmware description*, type a description of the firmware file. Ruckus Wireless recommends using a name that readily identifies the firmware.
5. In *Select firmware* file, click **Choose File** to search your client workstation or other reachable location for the firmware file.
6. Click **OK** to upload the firmware file for storage on FlexMaster.

Editing a Firmware File

After you upload a firmware file, you can edit it to define the product models on which the firmware is installed.

NOTE: When you assign a firmware to an unsupported product model (on which the firmware cannot be installed), you are still able to edit and save the firmware file, but the firmware is not installed on that product model.

1. Go to *Configure > Common > Manage Firmware Files.*
2. Click a firmware file **Edit** link. The *EDIT* form appears below the table.
3. Edit the firmware details as required. You can select the product models on which FlexMaster attempts to provision the firmware. You can also edit the firmware description.
4. Click **OK** to save your changes.

The page refreshes. You have completed editing the firmware file.

Deleting a Firmware File

1. Go to *Configure > Common > Manage Firmware Files.*
2. Look for the firmware file that you want to delete.
3. Click the **Delete** link that is in the same row as the firmware name. A confirmation message appears.
4. Click **OK** to confirm.

The page refreshes, and then the firmware file that you deleted disappears from the list.

Managing Device Registration

By default, compatible Ruckus Wireless devices attempt to register with FlexMaster upon boot up. The Device Registration option offers management of each join request sent by your devices. Thus, you can permit or deny devices from joining FlexMaster. All device registration requests are accepted by default.

A key feature of Device Registration is the ability to import a list of devices into the FlexMaster inventory before actual device registration, which occurs when the devices boot up. This enables you to stay ahead of your dispersal of Ruckus Wireless APs and keep track of each device's details (for example, serial number and MAC address), as well as automatically permit or deny the device to register with FlexMaster upon power up.

The following table shows the approval matrix for devices, based on the registration method, the auto approval setting, and the device status in Inventory.

Table 25. Approval matrix for devices

Registration Method	Auto Approval Setting	Device Inventory Status	License Count	Registration Result	Notes
Added via inventory file	Any	Permitted (or any user-defined status)	Licenses available	Success	A device with the status of *License Exceeded*, *Managed by ZoneDirector*, or *Lost ZoneDirector* is able to register successfully if licenses are available. Device status is set to Permitted
Added via inventory file	Any	Permitted (or any user-defined status)	Licenses exceeded	Fail	Device status appears as *License Exceeded*. The license held by the device is released.
Added via inventory file	Any	Permitted (or any user-defined status)	Any	Fail	If a standalone AP becomes managed by ZoneDirector, then its status changes to *Managed by ZoneDirector.* If a ZoneDirector device becomes managed by another FlexMaster server or the TR069 function is disabled, then its status changes to *Lost ZoneDirector.* If the ZoneDirector device is managed by another FlexMaster server, then the license held by the device is released on the original FlexMaster server. However, if the TR069 function is disabled, then the license status remains the same until the inventory status is changed to a status other than "Permitted".
Added via inventory file	Any	Admin Denied, RMA, or Unavailable	Any	Fail	The license held by the device is zero.
Auto registration (call home)	Enabled	Any	Licenses available	Success	Device status is set to *Permitted*. The auto registration state of the device is set to *Enabled.*
Auto registration (call home)	Enabled	Any	Licenses exceeded	Fail	Device status is set to *License Exceeded* and the license held by the device is released. The auto registration state of the device is set to *Enabled.*

Table 25. Approval matrix for devices (Continued)

Registration Method	Auto Approval Setting	Device Inventory Status	License Count	Registration Result	Notes
Auto registration (call home)	Disabled	Any	Any	Fail	Device status is set to *Admin Denied* and the license held by the device is released. The auto registration state of the device is set to *Disabled.*

For more information, refer to the following:

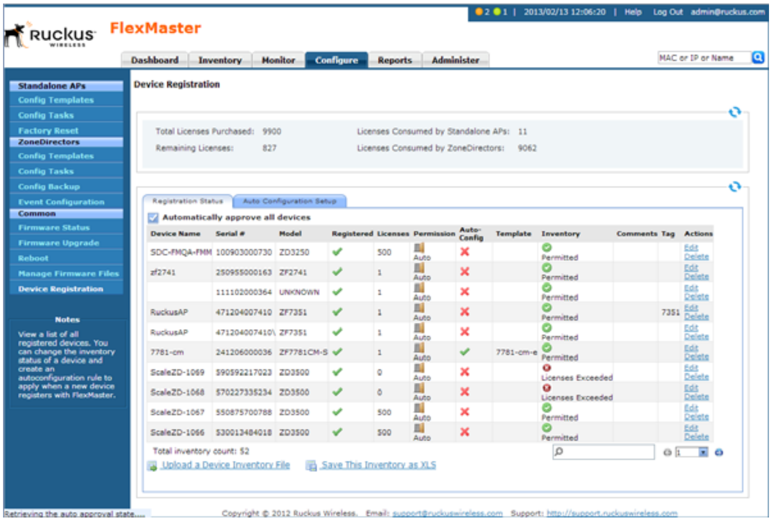
- Approving Automatic Device Registration
- Viewing Device Registration Status
- Manually Setting Device Registration Permissions
- Viewing Auto Configuration Rules
- Creating an Automatic Configuration Rule
- Viewing an Automatic Configuration Rule
- Stopping and Starting an Automatic Configuration Rule
- Deleting an Automatic Configuration Rule

Approving Automatic Device Registration

Approval of device registration can be automatic (default) or manual. When in automatic mode, all devices that attempt to register with FlexMaster are automatically accepted. To approve or deny automatic device registration, perform the following:

1. Navigate to *Configure* > *Common* > *Device Registration*. FlexMaster displays the *Device Registration/Registration Status* tab.

Figure 111. The Device Registration/Registration Status tab



Device Registration

Total Licenses Purchased: 9900
Remaining Licenses: 827
Licenses Consumed by Standalone APs: 11
Licenses Consumed by ZoneDirectors: 9062

☑ Automatically approve all devices

Device Name	Serial #	Model	Registered	Licenses	Permission	Auto-Config	Template	Inventory	Comments	Tag	Actions
SDC-FMQA-FMM	100903000730	ZD3250	✓	500	Auto	✗		Permitted			Edit Delete
zf2741	250955000163	ZF2741	✓	1	Auto	✗		Permitted			Edit Delete
	111102000364	UNKNOWN	✓	1	Auto	✗		Permitted			Edit Delete
RuckusAP	471204007410	ZF7351	✓	1	Auto	✗		Permitted		7351	Edit Delete
RuckusAP	471204007410\	ZF7351	✓	1	Auto	✗		Permitted			Edit Delete
7781-cm	241206000036	ZF7781CM-S	✓	1	Auto	✓	7781-cm-e	Permitted			Edit Delete
ScaleZD-1069	590592217023	ZD3500	✓	0	Auto	✗		Licenses Exceeded			Edit Delete
ScaleZD-1068	570227335234	ZD3500	✓	0	Auto	✗		Licenses Exceeded			Edit Delete
ScaleZD-1067	550875700788	ZD3500	✓	500	Auto	✗		Permitted			Edit Delete
ScaleZD-1066	530013484018	ZD3500	✓	500	Auto	✗		Permitted			Edit Delete

Total inventory count: 52

Notes

View a list of all registered devices. You can change the inventory status of a device and create an autoconfiguration rule to apply when a new device registers with FlexMaster.

Retrieving the auto approval state....

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

2. In the *Device Registration/Registration Status* tab, select the *Automatically approve all devices* checkbox to approve automatic device registration, or deselect the *Automatically approve all devices* checkbox to deny automatic device registration.

NOTE: When the *Automatically approve all devices* checkbox is not checked (deny automatic device registration), you must manually permit devices to register; refer to Manually Setting Device Registration Permissions.

3. Click **OK** in the verification prompt.

Viewing Device Registration Status

On the menu, click *Configure > Common > Device Registration*. FlexMaster displays the *Device Registration/Registration Status* tab. The table below describes the columns that appear in the *Device Registration/Registration Status* tab.

Table 26. Table columns in the Device Registration/Registration Status tab

Column	Description
Device Name	Name assigned to the device. Ruckus Wireless assigns APs "RuckusAP" as the default device name.
Serial #	Serial number of a registering device.
Model	Model of device.
Registered	✓ indicates that the device has registered with FlexMaster. ✗ indicates that the device has not yet registered with FlexMaster.
Licenses	How many licenses this device consumes.
Permission	Mode of acceptance as *Auto* (permission automatically assigned, no manual intervention) or *Manual* (permission changed using manual assignment).
Auto-Config	✓ indicates that the device was added to the inventory using via a comma-separated value (CSV) inventory file. ✗ indicates that the device has been added manually.
Template	Standalone AP template created using Creating an AP Configuration Template.
Inventory	Shows the permission status of the device. Default permission statuses include: • *Admin Denied*: The device not receive configuration and firmware upgrades from FlexMaster. • *Permitted*: The device is allowed to register with FlexMaster (default). • *RMA*: The device is currently being repair or replaced. RMA stands for Return Merchandise Authorization. • *Unavailable:* The device is not available. • *Inactive:* The device is offline.
Comments	Shows any notes that you have entered about the device. To add comments, click the **Edit** link that is in the same row as the device name, and then enter your comments in the *EDIT* form that appears below the table.
Tag	If you assigned a tag to the device in the auto configuration inventory file, then that tag appears here.

Table 26. Table columns in the Device Registration/Registration Status tab (Continued)

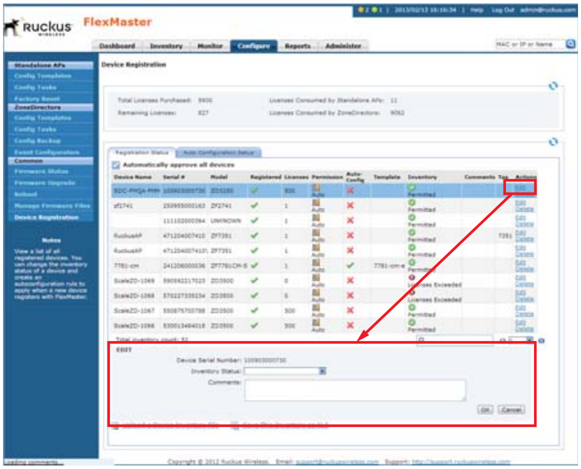
Column	Description
Actions	Clicking the **Edit** link enables you to change the device status to and from *Permitted, Admin Denied, RMA, Unavailable,* or any other status that you created. Clicking the **Delete** link allows you to delete a Ruckus Wireless device registration from the FlexMaster database. Deleting the device registration also releases the consumed license or licenses.

Manually Setting Device Registration Permissions

By default, Permission Mode is set to *Automatically approve all devices*, which allows all supported Ruckus Wireless devices to register with FlexMaster automatically. If there is a specific device that you want to prevent from registering with FlexMaster, then you need to manually change the permission for that device.

1. On the menu, click *Configure > Common > Device Registration.*
2. On the *Registration Status* tab, click **Edit** (under *Actions*) for the device whose permission you want to change. The *EDIT* form appear at the bottom of the page.

Figure 112. Manually setting device registration permissions



Notes

View a list of all registered devices. You can change the inventory status of a device and create an autoconfiguration rule to apply when a new device registers with FlexMaster.

Device Registration

Total Licenses Purchased: 9900
Remaining Licenses: 827
Licenses Consumed by Standalone APs: 11
Licenses Consumed by ZoneDirectors: 9062

☑ Automatically approve all devices

Device Name	Serial #	Model	Registered	Licenses	Permission	Auto-Config	Template	Inventory	Comments	Tag	Actions
SDC-FMQA-PHH	100903000730	ZD3250	✓	500	Auto	✗		Permitted			Edit
zf2741	250965000163	ZF2741	✓	1	Auto	✗		Permitted			Edit Delete
	111102000364	UNKNOWN	✓	1	Auto	✗		Permitted			Edit Delete
RuckusAP	471204007410	ZF7351	✓	1	Auto	✗		Permitted		7351	Edit Delete
RuckusAP	471204007410\	ZF7351	✓	1	Auto	✗		Permitted			Edit Delete
7781-cm	241206000036	ZF7781CM-S	✓	1	Auto	✓	7781-cm-e	Permitted			Edit Delete
ScaleZD-1069	590982217023	ZD3500	✓	0	Auto	✗		Licenses Exceeded			Edit Delete
ScaleZD-1068	570227335234	ZD3500	✓	0	Auto	✗		Licenses Exceeded			Edit Delete
ScaleZD-1067	550875700788	ZD3500	✓	500	Auto	✗		Permitted			Edit Delete
ScaleZD-1066	530013484018	ZD3500	✓	500	Auto	✗		Permitted			Edit Delete

Total inventory count: 52

EDIT

Device Serial Number: 100903000730
Inventory Status:
Comments:

Copyright © 2013 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

3. In *Inventory Status,* select the new permission that you want to assign to the device. Options include:
    - *Admin Denied*: Click this option to prevent the device from registering with FlexMaster. If the device is currently registered and you change the permission to Admin Denied, then the device no longer receives configuration and firmware upgrades from FlexMaster after you save the new permission.
    - *Permitted*: Click this option to allow the device to register with FlexMaster.

- *RMA*: Click this option is the device is currently being repair or replaced. RMA stands for Return Merchandise Authorization.
- *Unavailable*: Click this option if you want to designate this device as unavailable.

If you created any custom statuses on the *Administer > View Management > Inventory Status* tab, then they also appear as options when you are editing the inventory status of a device.

4. Enter optional comments in *Comments.*
5. Click **OK** to save your changes.

NOTE: If you deny a device that is already registered, then it remains in the inventory but FlexMaster no longer honors requests from that device.

NOTE: If you set the device status to *Admin Denied, RMA,* or *Unavailable,* then the device only appears on the *Device Registration* page.

NOTE: When you deny a device, its *Permission* changes to **Manual**. If later on you permit the same device, then its *Permission* remains as **Manual**. This behavior allows you to determine which devices in the inventory were permitted manually.

NOTE: If you permit a device, then it is able to register with FlexMaster at the next Perform Inform Interval.

NOTE: Only devices with a *Permitted* status consume licenses; devices in other statuses do not consume any licenses.

Viewing Auto Configuration Rules

FlexMaster allows you to create auto configuration rules to apply existing Standalone AP templates to devices as they automatically register with FlexMaster. Perform the following to view the current auto configuration rules.

1. Navigate to *Configure > Common > Device Registration*. FlexMaster displays the *Device Registration/Registration Status* tab.
2. Click the *Auto Configuration Setup* tab.

   The table below describes the columns that appear in the *Device Registration/Auto Configuration Setup* tab.

Table 27. Table columns on the Device Registration/Auto Configuration Status tab

Column	Description
Rule Name	Name of the auto configuration rule.
Create Time	When the rule was created.
Template Name	Standalone AP template created in Creating an AP Configuration Template.
Created by	Who created the auto configuration rule.
Tag	If you assigned a tag to the device in the auto configuration inventory file, then that tag appears here.
Action	• Clicking **View** allows you to look at the auto configuration rule. • Click **Delete** to delete the auto configuration rule. • Click **Stop** to halt use of the auto configuration rule.
Status	Shows the status of the auto configuration rule. Default statuses include: • *Running*: The auto configuration rule is in effect. • *Cancelled:* The auto configuration rule is not in effect.

Creating an Automatic Configuration Rule

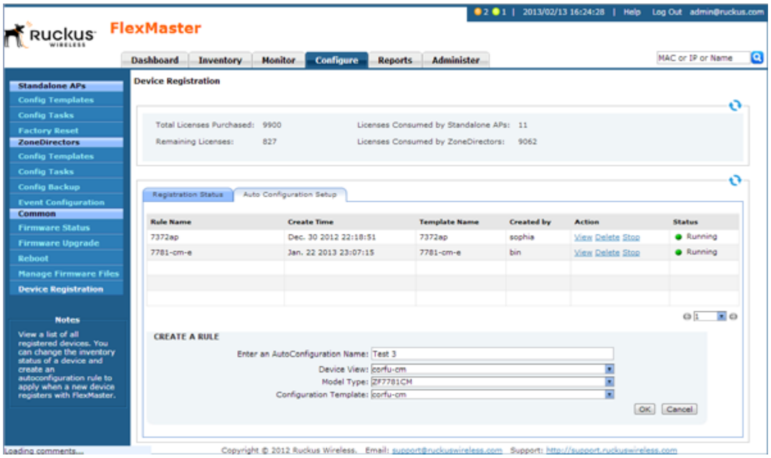
FlexMaster allows you to create auto configuration rules to apply existing Standalone AP templates to devices as they automatically register with FlexMaster.

- The Standalone AP devices must already be part of an AP view as described in Creating a Standalone AP View.
- The Standalone AP templates must already be created as described in Creating an AP Configuration Template.

Perform the following to create a new auto configuration rule:

1. Navigate to *Configure* > *Common* > *Device Registration*. FlexMaster displays the *Device Registration/Registration Status* tab.
2. Click the *Auto Configuration Setup* tab.
3. Click **Create a rule.** FlexMaster displays the *CREATE A RULE* section.

Figure 113. Creating an auto configuration rule



Device Registration

Total Licenses Purchased: 9900
Remaining Licenses: 827
Licenses Consumed by Standalone APs: 11
Licenses Consumed by ZoneDirectors: 9062

Rule Name	Create Time	Template Name	Created by	Action	Status
7372ap	Dec. 30 2012 22:18:51	7372ap	sophia	View Delete Stop	● Running
7781-cm-e	Jan. 22 2013 23:07:15	7781-cm-e	bin	View Delete Stop	● Running

CREATE A RULE

Enter an AutoConfiguration Name: Test 3
Device View: corfu-cm
Model Type: ZF7781CM
Configuration Template: corfu-cm

Notes

View a list of all registered devices. You can change the inventory status of a device and create an autoconfiguration rule to apply when a new device registers with FlexMaster.

Loading comments...

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

4. In the *CREATE A RULE* section, enter or select the following:
   - *Enter an AutoConfiguration Name:* Assign a name to this auto configuration rule.
   - *Device View:* Select a Standalone AP device view already created using Creating a Standalone AP View.
   - *Model Type:* Select a Standalone AP model type from the list.
   - *Configuration Template:* Select a Standalone AP template already created using Creating an AP Configuration Template.
5. Click **OK.** FlexMaster saves your auto configuration rule and adds it to the *Auto Configuration Setup* table.

Viewing an Automatic Configuration Rule

1. Navigate to *Configure > Common > Device Registration.*
2. Click the *Auto Configuration Setup* tab.
3. Click **View.** FlexMaster displays the *Device status of task: <Rule Name>* table.
   - If no APs have been autoconfigured using the selected rule, then the table is empty.
   - If APs have been autoconfigured using the selected rule, then the table lists the AP device information (if known):
     - Device Serial Number
     - Device Name
     - Tag
     - MAC Address
     - IPv6 Address
     - IP Address
     - External IP Address
     - Status of auto configuration rule: Success or Failure

- Click the device serial number link to have FlexMaster display the Device View.
- Click *Hide Detail* to close the *Device status of task: <Rule Name>* table.

Stopping and Starting an Automatic Configuration Rule

1. Navigate to *Configure > Common > Device Registration.*
2. Click the *Auto Configuration Setup* tab.
3. Click **Stop** or **Restart.** FlexMaster halts or restores application of the auto configuration rule.
   - When you click **Stop** the rule *Status* changes from *Running* to *Cancelled.*
   - When you click **Restart** the rule *Status* changes from *Cancelled* to *Running.*

Deleting an Automatic Configuration Rule

1. Navigate to *Configure > Common > Device Registration.*
2. Click the *Auto Configuration Setup* tab.
3. Click **Delete.**
4. Click **OK.** FlexMaster deletes the auto configuration rule.

Uploading a Device Inventory File

A device inventory file is a list of Ruckus Wireless devices that are preapproved for registration with FlexMaster. If you have a large number of Ruckus Wireless devices to register with FlexMaster for management, then you can work with your Ruckus Wireless representative to build and upload a device inventory file. This file enters each device into the FlexMaster inventory, thus saving time in your FlexMaster deployment and use. Once a list of devices is uploaded, the *Device Registration* table automatically refreshes to show the uploaded devices.

Preloading inventory files also enables you to preconfigure device settings so that when devices initially register with FlexMaster, they receive these preconfigured settings. For more on configuration, refer to Provisioning Tasks to Managed Devices.

Refer to the following sections for more information:

- When to Upload a Device Inventory File
- Preparing a Device Inventory File
- Uploading a Device Inventory File
- Exporting the Inventory List to a Microsoft Excel File

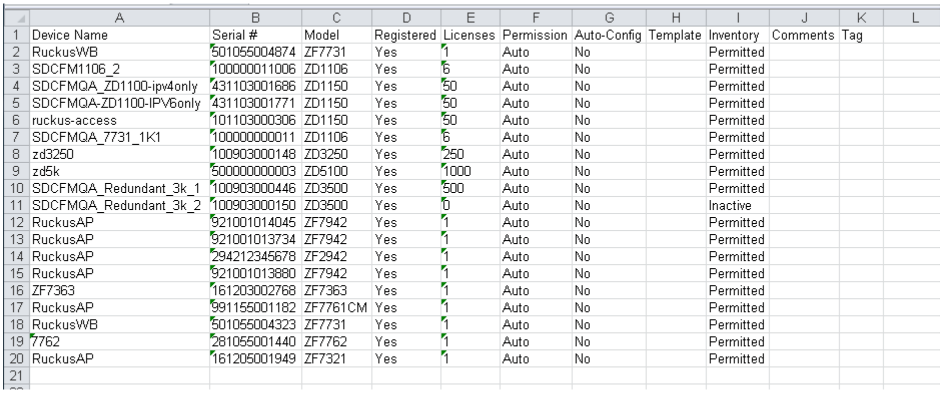
When to Upload a Device Inventory File

- If you disabled automatic device approval (by clearing the *Automatically approve all devices* check box) on the *Device Registration* page, then you need to manually approve each device registration request. When you have a large number of Ruckus Wireless devices that need to be managed by FlexMaster but do not want to enable automatic device approval, you can simply upload a device inventory file, which contains your list of pre-approved devices. Devices listed in the inventory file are able to register with FlexMaster even when automatic device approval is disabled.
- You can also upload an inventory file when you want to automatically configure a number of unregistered Ruckus Wireless devices when they register with FlexMaster.

Preparing a Device Inventory File

A device inventory file is a Microsoft Excel file with the same entries as the *Device Registration* table. After you upload the device inventory file with the pre-registration data, you need to create an auto-configuration task using the tag to select the target devices.

Figure 114. A sample device inventory file



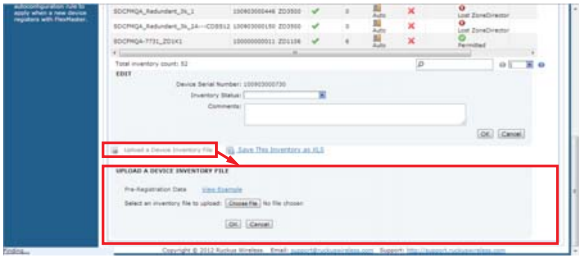
	A	B	C	D	E	F	G	H	I	J	K	L
1	Device Name	Serial #	Model	Registered	Licenses	Permission	Auto-Config	Template	Inventory	Comments	Tag	
2	RuckusWB	501055004874	ZF7731	Yes	1	Auto	No		Permitted			
3	SDCFM1106_2	100000011006	ZD1106	Yes	6	Auto	No		Permitted			
4	SDCFMQA_ZD1100-ipv4only	431103001686	ZD1150	Yes	50	Auto	No		Permitted			
5	SDCFMQA-ZD1100-IPV6only	431103001771	ZD1150	Yes	50	Auto	No		Permitted			
6	ruckus-access	101103000306	ZD1150	Yes	50	Auto	No		Permitted			
7	SDCFMQA_7731_1K1	100000000011	ZD1106	Yes	6	Auto	No		Permitted			
8	zd3250	100903000148	ZD3250	Yes	250	Auto	No		Permitted			
9	zd5k	500000000003	ZD5100	Yes	1000	Auto	No		Permitted			
10	SDCFMQA_Redundant_3k_1	100903000446	ZD3500	Yes	500	Auto	No		Permitted			
11	SDCFMQA_Redundant_3k_2	100903000150	ZD3500	Yes	0	Auto	No		Inactive			
12	RuckusAP	921001014045	ZF7942	Yes	1	Auto	No		Permitted			
13	RuckusAP	921001013734	ZF7942	Yes	1	Auto	No		Permitted			
14	RuckusAP	294212345678	ZF2942	Yes	1	Auto	No		Permitted			
15	RuckusAP	921001013880	ZF7942	Yes	1	Auto	No		Permitted			
16	ZF7363	161203002768	ZF7363	Yes	1	Auto	No		Permitted			
17	RuckusAP	991155001182	ZF7761CM	Yes	1	Auto	No		Permitted			
18	RuckusWB	501055004323	ZF7731	Yes	1	Auto	No		Permitted			
19	7762	281055001440	ZF7762	Yes	1	Auto	No		Permitted			
20	RuckusAP	161205001949	ZF7321	Yes	1	Auto	No		Permitted			
21												

Uploading a Device Inventory File

When you have the device inventory file ready, you need to upload it to FlexMaster.

1. Navigate to *Configure > Common > Device Registration*. FlexMaster displays the *Device Registration/Registration Status* tab.
2. Click the **Upload a Device Inventory File** link from below the *Registration Status* table. FlexMaster displays the *UPLOAD A DEVICE INVENTORY FILE* form.

Figure 115. The Upload a Device Inventory File form



Total inventory count: 52

EDIT

Device Serial Number: 100903000730

Inventory Status:

Comments:

OK Cancel

Upload a Device Inventory File

Save This Inventory as XLS

UPLOAD A DEVICE INVENTORY FILE

Pre-Registration Data View Example

Select an inventory file to upload: Choose File No file chosen

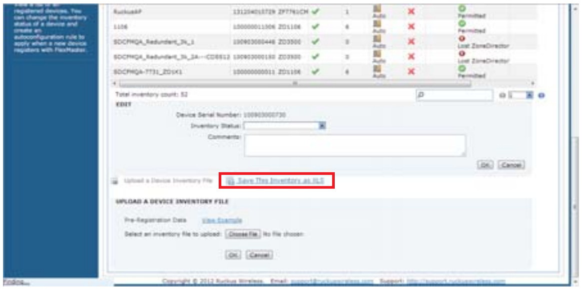
OK Cancel

3. In *Select an inventory file to upload,* click **Choose File** and find the file.
4. Once you have found the file, click **Open** in the *Browse* pop-up window.
5. Click **OK** to upload the inventory file.

Exporting the Inventory List to a Microsoft Excel File

FlexMaster supports exporting the device list from the Web interface to a Microsoft Excel file. If you need to prepare equipment inventory reports, then you could use the export to Excel feature so you do not have to manually type the details of each device.

Figure 116. Click the Save This Inventory as XLS link


Total inventory count: 52
EDIT
Device Serial Number:
Inventory Status:
Comments:
OK
Cancel
Upload a Device Inventory File
Save This Inventory as XLS
UPLOAD A DEVICE INVENTORY FILE
Pre-Registration Data
View Example
Select an inventory file to upload:
Choose File
No file chosen
OK
Cancel

1. Navigate to *Configure > Common > Device Registration*. FlexMaster displays the *Device Registration/Registration Status* tab.
2. Click the **Save This Inventory as XLS** link at the bottom of the page. FlexMaster saves the *inventory.xls* file to your workstation.
3. If necessary, click **Save**, and then select the location where you want to save the file.

You have completed exporting the device list to an Excel file. Go to the location where you exported the Excel file to verify that the file was saved successfully, and then use Microsoft Excel to open the file.

Releasing Device Licenses

Devices can be released on a per-serial number basis:

1. Go to *Configure > Common > Device Registration.*
2. Find the required *Device Name* in the table. Note the number of licenses consumed in the *Licenses* column.
3. Click **Delete** in the *Actions* column and respond to the confirmation prompt.

   FlexMaster deletes the device, releases the consumed license or licenses, and returns you to the *Registration Status* page.
4. In the *Registration Status* page, verify that the device entry is deleted.

Configuring VLAN and LAN Port Settings

When your wired network is segmented into VLANs and you want clients associated with a ZoneFlex AP to join these VLANs, then you can configure VLAN support on the AP using FlexMaster.

NOTE: Before configuring VLANs on your network, Ruckus Wireless recommends configuring a test network that mirrors your actual deployed network.

NOTE: When you have a ZoneFlex 2942 on the network and you want to enable the hotspot service, note that a wireless interface must be part of either the Management VLAN or Available Wireless Interfaces before you can set it as the hotspot interface. If the wireless interface belongs to any VLAN other than the Management VLAN, then you are unable to set it as the hotspot interface and the following message appears:

```
The specified wireless interface is not available for the hotspot
service.
```

For more information, refer to the following:

- Configuration Rules
- Before You Begin
- General Configuration Procedures
- How Dynamic VLANs Work
- Sample Dynamic VLAN Scenario

Configuration Rules

Take note of the following rules related to configuring VLANs:

- In its factory default configuration, all physical and wireless interfaces on the ZoneFlex AP belong to the Management VLAN (default VLAN) and are all assigned VLAN ID 1. This default configuration enables clients connected to any of the physical and wireless interfaces to communicate with each other.
- In addition to the Management VLAN (default), eight other VLAN profiles (named Vlan A to Vlan H) are available on the ZoneFlex AP. When you want specific physical or wireless interfaces on the AP to join a VLAN on your wired network, you need to edit one or more of these VLAN profiles.
- The Management VLAN cannot be renamed or deleted.
- When the AP is in its factory default state, all physical interfaces on the AP are untagged and all wireless interfaces are connected to the Management VLAN.
- By default, L2TP feature and L2TP tunnel state are both disabled on the AP.
- FlexMaster only uses the Tunnel Management VLAN when L2TP is enabled.
- VLANs with the same ID must have the same tunneled state.

- A physical interface can be configured as untagged on only one VLAN, and wireless interfaces cannot be configured as tagged on a ZoneFlex AP.
- A wireless interface can be connected to only one VLAN.
- Ethernet ports are defined as Trunk Ports, Access Ports, or General Ports. Trunk links pass VLAN information between switches. Access ports provide access to the network and can be configured as members of specific VLANs, thereby separating the traffic on these ports from traffic on other VLANs. General Ports are user-defined ports that can have any combination of up to 20 VLAN IDs assigned. At least one port on each AP must be designated as a Trunk Port.
- By default, all ports are enabled as Trunk Ports with Untagged VLAN set as 1 (except for ZoneFlex 7025, whose front ports are enabled as Access Ports by default). When configured as an Access Port, all untagged ingress traffic is the configured Untagged VLAN, and all egress traffic is untagged. If configured as a Trunk Port, then all untagged ingress traffic is the configured Untagged VLAN (by default, 1), and all VLAN-tagged traffic on VLANs 1-4094 is seen when present on the network.
  Trunking is a function that must be enabled on both sides of a link. When two switches are connected together, for example, both switch ports must be configured as trunk ports. The Trunk Port is a member of all the VLANs that exist on the AP/switch and carries traffic for all those VLANs between switches.
- All Access Ports are set to Untagged VLAN 1 by default. This means that all Access Ports belong to the native VLAN and are all part of a single broadcast domain. To remove ports from the native VLAN and assign them to specific VLANs, select Access Port and enter any valid VLAN ID in the VLAN ID field (valid VLAN IDs are 2-4094).
  The following table describes the behavior of incoming and outgoing traffic for Access Ports with VLANs configured.

VLAN Settings	Incoming Traffic (from the client)	Outgoing Traffic (to the client)
Access Port, Untag VLAN 1	All incoming traffic is native VLAN 1.	All outgoing traffic on the port is sent untagged.
Access Port, Untag VLAN [2-4094]	All incoming traffic is sent to the VLANs specified.	Only traffic belonging to the specified VLAN is forwarded. All other VLAN traffic is dropped.

- General ports are user-specified ports that can have any combination of up to 20 VLAN IDs assigned. Enter multiple valid VLAN IDs separated by commas or a range separated by a hyphen.
- Using Port-Based 802.1X: 802.1X authentication provides the ability to secure the network and optionally bind service policies for an authenticated user. 802.1X provides logical port control and leverages the EAP authentication and RADIUS protocols to allow the network policy to be effectively applied in real time, no matter where the user connects to the network.
  AP Ethernet ports can be individually configured to serve as either an 802.1X suppli-

cant (authenticating the AP to an upstream authenticator switch port), or as an 802.1X authenticator (receiving 802.1X authentication requests from downstream supplicants). A single port can not provide both supplicant and authenticator functionality at the same time.

- If mesh mode is enabled on ZoneDirector, then the 802.1X port settings are unavailable for any APs that support mesh. The ZoneFlex 7025 does not support mesh, so 802.1X settings are available for those access points even when mesh is enabled. However, the 802.1X settings are only available from the Editing [Access Point] dialogue, not from AP Groups. Therefore if you want to use 802.1X on ZoneFlex 7025 ports when mesh is enabled, you must configure each AP individually.
- Ethernet port as authenticator: The Access Point is fundamentally a wireless switch. On APs with two or more wired ports, the AP acts as a network edge switch and can be configured to authenticate downstream wired stations (which can even be another edge switch). When the AP Ethernet port is configured as an 802.1X authenticator, it can be further defined as either Port-based or MAC-based. MAC-based authenticator mode is only supported if the port is an Access Port.

	Trunk Port	**Access Port**	**General Port**
Port-based authenticator support	Yes	Yes	Yes
MAC-based authenticator support	No	Yes	No

- Ethernet port as supplicant: You can also configure a port to act as a supplicant and force it to authenticate itself to an upstream authenticator port. Until the AP has successfully done so, the state of the authenticator port is closed and packets from the AP or stations behind it are dropped at the authenticator port.
  In this configuration, it is expected that the connected authenticator port is configured as a Trunk Port to pass all VLAN packets, and in port-based authentication mode. Each AP is allowed to configure a maximum of one Ethernet port as an 802.1X supplicant, and the supplicant port must be a Trunk Port.
- In 802.1X port-based authenticator mode, only a single MAC host must be authenticated for all hosts to be granted access to the network.
- In 802.1X MAC-based authenticator mode, each MAC host is individually authenticated. Each newly-learned MAC address triggers an EAPOL request-identify frame.
  - Guest VLAN: (Default disabled). When a station fails to authenticate to this port, it is assigned to this “guest” VLAN, with access to Internet but not to internal resources.
  - Dynamic VLAN: (Default disabled). Dynamically assign VLANs based on the policies set on the RADIUS server.
  - Authenticator: Select the RADIUS server from the list. A RADIUS server must be selected to set this port as a MAC-based authenticator.

Before You Begin

Before you configure the VLAN settings of an AP, Ruckus Wireless recommends performing the following pre-configuration tasks to ensure that you have the information you need before you start:

- Verify that the VLAN on the wired LAN is configured and working correctly.
- Take note of the VLAN IDs assigned to each existing VLAN on the wired network.
- Decide which physical and wireless interfaces on the AP you want to connect to the wired VLAN.
- Determine if the VLAN on the wired network uses tagging or not.

General Configuration Procedures

The specific procedures for configuring the VLAN settings of an AP depend on several factors in your network environment. These factors include the number of physical and wireless interfaces that you want to segment and the number of VLANs to which you want these interfaces to be connected. Since VLAN configuration procedures typically differ from one network to another, this guide only provides high-level steps for configuring VLANs.

1. Launch the *VLAN configuration* page for the AP.

   VLAN settings need to be configured on a per-device basis. Log on to the FlexMaster Web interface, find the AP that you want to configure, and then launch the device view for that AP. You can find the VLAN-related settings by clicking VLAN on the Device Interface menu.

2. Remove the physical and wireless interfaces that you want to connect to the wired VLAN from the default Management VLAN.

   By default, all physical and wireless interfaces on the AP belong to the Management VLAN. This default configuration allows any client connected to any of the AP's interfaces to communicate with other clients that are connected to the same AP. Before you can connect a physical or wireless interface to another VLAN, you first need to disconnect it from the Management VLAN.

3. Edit a VLAN profile to connect the physical and wireless interfaces to the wired VLAN.

   Edit one of the available VLAN profiles on the AP to enable it to forward traffic to the target VLAN on the wired network, and then add the physical and wireless interfaces that you want to connect to that VLAN.

These are the three general steps for configuring the VLAN settings on an AP. For an example of specific configuration procedures, refer to the following sample scenario.

How Dynamic VLANs Work

By default, all wireless clients associated with Ruckus Wireless APs are segmented into a single VLAN (with VLAN ID 1, unless otherwise configured). When you want to individually assign wireless clients into specific VLANs (for example, for increased security), you can enable dynamic VLAN.

Dynamic VLAN allows ZoneDirector to separate wireless clients into different network segments based on the VLAN ID that is assigned to each wireless user on the RADIUS server. As such, dynamic VLAN is implemented on a per-user basis, typically by MAC address.

Priority of Dynamic VLAN, VLAN, and Tunnel Mode

If the VLAN, Dynamic VLAN and Tunnel Mode features are all enabled and they have conflicting rules, then ZoneDirector prioritizes and applies these three features in the following order:

1. Dynamic VLAN (top priority)
2. VLAN
3. Tunnel Mode

How it Works for Assigned Clients

When a client is dynamically assigned to a VLAN in the RADIUS server database, this is how it works:

1. Client associates with a WLAN on which Dynamic VLAN has been enabled.
2. The AP requires the client to authenticate with the RADIUS server.
3. When the RADIUS server completes the client authentication process, it sends the join approval and the VLAN ID that has been assigned to the AP.
4. Client joins the AP and is segmented to the assigned VLAN ID.

How it Works for Unassigned Clients

When a client is not assigned to a VLAN in the RADIUS server database, this is how it works:

1. Client associates with a WLAN on which Dynamic and Guest VLANs have been enabled. The client is currently blocked from access.
2. The RADIUS server notifies the AP that the client is not dynamically assigned to a VLAN.
3. Client joins the AP and is segmented to the Guest VLAN.

Sample Dynamic VLAN Scenario

Your wired LAN is segmented into several VLANs, including one called *Sales VLAN* (using VLAN 10) and one called Guest VLAN (using VLAN 11). You assign the Sales clients in a RADIUS (or other) server to VLAN 10, so the Sales clients stay on the same VLAN, no matter which AP they are using to access the wired network. The dynamic VLAN feature can also allow the Sales clients to roam across multiple APs without re-authenticating.

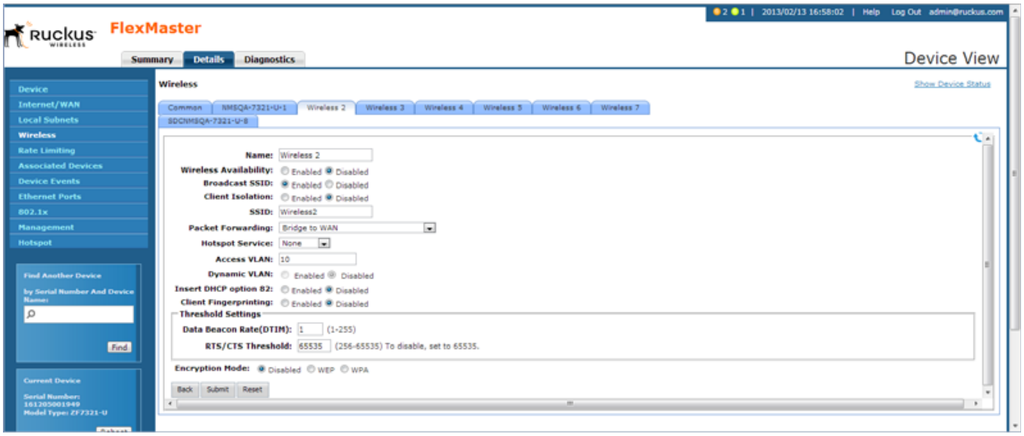
In this scenario, you have a ZoneFlex 7942 device deployed on the network and you want its Port 2 and a wireless interface to join the Sales VLAN on the wired LAN. Specifically, you want its physical ports Port 2 and Wireless 2 interface to be part of the Sales VLAN.

The Sales VLAN is assigned VLAN ID 10 and associated Guest VLAN is assigned VLAN ID 11.

Step 1: Configuring the Wireless LAN

1. Launch the Device View by clicking the serial number for the AP that you want to manage, click the **Details** tab, and then click **Wireless** (or **Wireless Radio 1** or **Wireless Radio 2**) on the menu. FlexMaster displays the selected *Wireless Radio* page.
2. In the *Wireless Radio* page, click the desired **Wireless #** tab, and then click **Edit Settings**. FlexMaster displays the *Edit Wireless LAN* page.

Figure 117. Edit Wireless LAN page



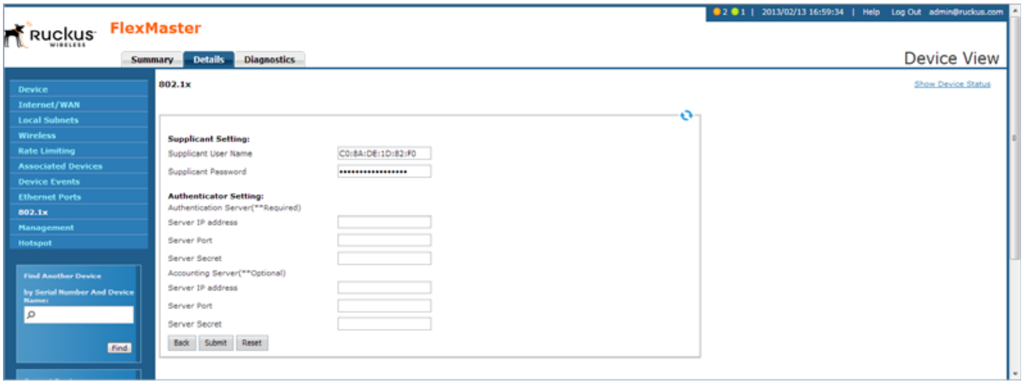
Name: Wireless 2
Wireless Availability: ○ Enabled ● Disabled
Broadcast SSID: ● Enabled ○ Disabled
Client Isolation: ○ Enabled ● Disabled
SSID: Wireless2
Packet Forwarding: Bridge to WAN
Hotspot Service: None
Access VLAN: 10
Dynamic VLAN: ○ Enabled ● Disabled
Insert DHCP option 82: ○ Enabled ● Disabled
Client Fingerprinting: ○ Enabled ● Disabled
Threshold Settings
Data Beacon Rate(DTIM): 1 (1-255)
RTS/CTS Threshold: 65535 (256-65535) To disable, set to 65535.
Encryption Mode: ● Disabled ○ WEP ○ WPA

3. In the *Edit Wireless LAN* page, edit the following:
   - (optional) *SSID* -- what the wireless clients see when they search for the Sales VLAN.
   - *Access VLAN* -- set to VLAN ID **10.**
4. In the *Edit Wireless LAN* page, click **Submit** to save your changes.

Step 2: Verifying 802.1X Configuration

1. In the Device View, click **802.1x** on the navigation menu.

Figure 118. Verifying 802.1X server settings



802.1x

Supplicant Setting:
Supplicant User Name: C0:8A:DE:1D:82:F0
Supplicant Password: ••••••••••••••••••

Authenticator Setting:
Authentication Server(**Required)
Server IP address
Server Port
Server Secret
Accounting Server(**Optional)
Server IP address
Server Port
Server Secret

2. Using the recommendations in Configuring VLAN and LAN Port Settings, make sure that the 802.1X server settings are correct.

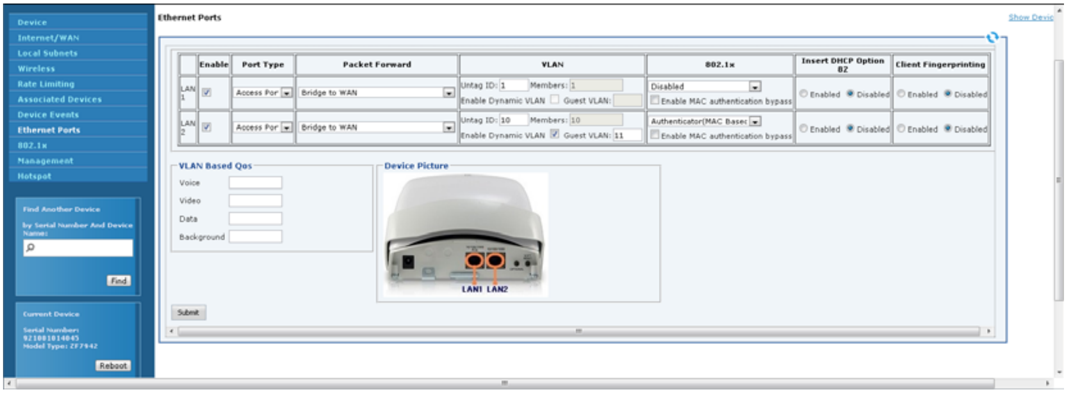
NOTE: You must configure an 802.1x authenticator on this page before configuring 802.1x parameters on the Ethernet Ports page.

Step 3: Configuring the Ethernet Port

For this example, we are configuring LAN Port 2 to support *Sales VLAN* 10 and *Guest VLAN* 11 as part of a dynamic VLAN.

1. In the Device View navigation bar, click **Ethernet Ports**. FlexMaster displays the *Ethernet Ports* page.

Figure 119. Ethernet Ports page



Ethernet Ports

	Enable	Port Type	Packet Forward	VLAN	802.1x	Insert DHCP Option 82	Client Fingerprinting
LAN 1	☑	Access Por	Bridge to WAN	Untag ID: 1 Members: 1 Enable Dynamic VLAN □ Guest VLAN:	Disabled □ Enable MAC authentication bypass	○ Enabled ● Disabled	○ Enabled ● Disabled
LAN 2	☑	Access Por	Bridge to WAN	Untag ID: 10 Members: 10 Enable Dynamic VLAN ☑ Guest VLAN: 11	Authenticator(MAC Basec □ Enable MAC authentication bypass	○ Enabled ● Disabled	○ Enabled ● Disabled

VLAN Based Qos

Voice
Video
Data
Background

Current Device
Serial Number: 921001014045
Model Type: ZF7942

2. In the LAN 2 *Port Type* entries, select **Access Port**.

3. In the Port 2 *802.1x* entries, select **Authenticator (MAC Based)**.

4. In the Port 2 *VLAN* entries:
   - Enter VLAN ID **10** in the *Untag ID* box.
   - Select the **Enable Dynamic VLAN** box.
   - Enter VLAN ID **11** in the *Guest VLAN* box.

5. If this ethernet port is to support MAC authentication bypass, then select the *802.1x* **Enable MAC authentication bypass** box.

   Enabling this option allows users with registered MAC addresses to be transparently authorized without having to log in. A user entry on the RADIUS server needs to be created using the client MAC address as both the username and password. (The MAC address format is a single string of characters without punctuation.) When MAC authentication is unsuccessful, the normal 802.1X authentication exchange is attempted.

6. In the *Ethernet Ports* page, click **Submit** to save your changes.

Step 4: Configuring the RADIUS Server

For dynamic VLAN to work, you must configure the following RADIUS attributes for each user:

- *Tunnel-Type:* Set this attribute to **VLAN**.
- *Tunnel-Medium-Type:* Set this attribute to **IEEE-802**.
- *Tunnel-Private-Group-ID:* Set this attribute to the VLAN ID to which you want to segment this user.

NOTE: Some RADIUS servers may also require the *User-Name* attribute to be configured.

Table 28. RADIUS user attributes required by dynamic VLAN

Attribute	Type ID	Expected Value (Numerical)
Tunnel-Type	64	VLAN (13)
Tunnel-Media-Type	65	802 (6)
Tunnel-Private-Group-ID	81	VLAN ID

Sample FreeRADIUS Entries

```
0018ded90ef3                          (MAC address)
User-Name = user1,
Tunnel-Type = VLAN,
Tunnel-Medium-Type = IEEE-802,
Tunnel-Private-Group-ID = 0010

00242b752ec4                          (MAC address)
User-Name = user2,
Tunnel-Type = VLAN,
Tunnel-Medium-Type = IEEE-802,
Tunnel-Private-Group-ID = 0012
```

In this scenario, when user1 client associates with the WLAN, the RADIUS server authenticates user1, and user1 joins the AP and is segmented to VLAN 10 which has been assigned by the RADIUS server.

However, when user2 client associates with the WLAN, the RADIUS server authenticates user2 and returns VLAN ID 12 to the AP, and because user2 is not assigned to VLAN 10, user2 is assigned to the Guest VLAN.

Creating a Hotspot

A hotspot is a venue or area that provides wireless Internet access to devices with wireless networking capability, such laptops, PDAs, and other portable devices. Hotspots are usually available in public venues such as hotels, airports, restaurants, and shopping malls.

NOTE: The hotspot feature is only available on ZoneFlex 2942 APs that are running on software version 5.1 and later.

Your ZoneFlex 2942 AP has a built-in hotspot feature that you can enable and configure to provide hotspot service to users in your environment. In addition to your ZoneFlex 2942 AP, you need the following to deploy a hotspot:

- Web Server: You need a Web server that can host the external portal/login page that clients use to gain access to the hotspot service. More information in the Web server requirements is available in the *ZoneFlex 2942 Hotspot Application Notes* (see note below).
- RADIUS Server: A Remote Authentication Dial-In User Service (RADIUS) through which users can authenticate.

For installation and configuration instructions for the captive portal and RADIUS server software, refer to the documentation that was provided with them.

NOTE: If you need additional information on how to deploy a hotspot with ZoneFlex 2942, then contact Ruckus Wireless Support at
`support@ruckuswireless.com`
and request the *ZoneFlex 2942 Hotspot Application Notes*.

For more information, refer to the following:

- Before You Begin
- Configuring Basic Hotspot Settings
- Configuring a Walled Garden
- Specifying Unrestricted Clients
- Configuring Advanced Settings

Before You Begin

Before enabling and configuring the hotspot service on ZoneFlex 2942, Ruckus Wireless recommends performing the following tasks:

- Set up, configure, and test the RADIUS server and captive portal that you are using for your hotspot deployment.
- Have the following information ready:
  - Redirect URL for the captive portal (the Web page where clients log on to gain access to the hotspot service)

- RADIUS server IP address
- RADIUS server shared secret

Decide on which wireless interface you want to use for the hotspot. ZoneFlex 2942 has four wireless interfaces; you can use any of these. You should also verify that Wireless Availability is enabled on that wireless interface.

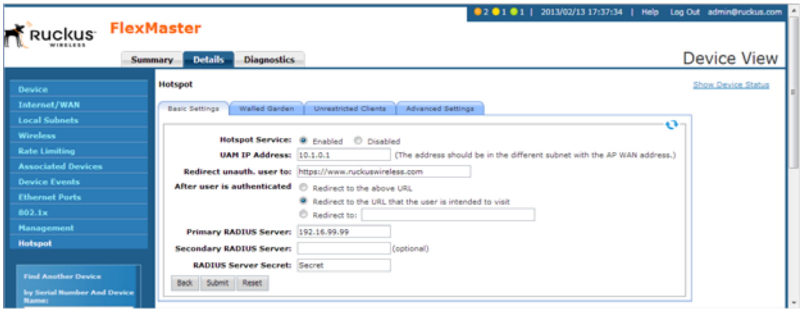
NOTE: A wireless interface must be part of either the Management VLAN or Available Wireless Interfaces before you can set it as the hotspot interface. When the wireless interface belongs to any VLAN other than the Management VLAN, you are unable to set it as the hotspot interface and the following message appears: `The specified wireless interface is not available for the hotspot service.`

Configuring Basic Hotspot Settings

Basic hotspot settings cover the essential configuration that you need to perform to make your hotspot operational. In this procedure, you need to configure the following settings.

1. On the navigation menu, click **Hotspot**. The *Basic Settings* tab appears.
2. Click **Edit Settings**.

Figure 120. Hotspot page Basic Settings tab



Hotspot Service: ● Enabled ○ Disabled
UAM IP Address: 10.1.0.1 (The address should be in the different subnet with the AP WAN address.)
Redirect unauth. user to: https://www.ruckuswireless.com
After user is authenticated ○ Redirect to the above URL
● Redirect to the URL that the user is intended to visit
○ Redirect to:
Primary RADIUS Server: 192.16.99.99
Secondary RADIUS Server: (optional)
RADIUS Server Secret: Secret

3. In *Hotspot Service*, click **Enabled**.
4. In *Hotspot Wireless Interface*, select the wireless interface that you want to use for the hotspot service. ZoneFlex 2942 has four wireless interfaces; you can select any of these.

NOTE: By default, client isolation is enabled on the hotspot interface. This means wireless clients that are connected to the same hotspot service are unable to communicate with each other.

5. In *Hotspot Wired Interface*, select the wired interfaces that you want to include in the hotspot service. Any device (for example, a network printer) connected to a wired interface that is part of the hotspot is accessible to hotspot users.

NOTE: When you are using one wired interface and one wireless interface for the hotspot service, and then you change one of them to another interface, the following error message can appear:

```
Interface {name or number} is already being used in a VLAN
```

To switch to another interface, do the following:

1. Disable the hotspot service.
2. Switch to another wired or wireless interface.
3. Enable the hotspot service.

6. In *Redirect unauth. users to,* type the URL to which users are redirected after they associate with the hotspot and launch their Web browser. This is the URL of the captive portal that you have set up, where users need to enter their user name and password to access the Internet service that your hotspot provides.
7. In *Primary RADIUS Server,* type the IP address of the RADIUS server on the network. Users logging on to the hotspot authenticate with this RADIUS server.
8. In *RADIUS Server Secret,* type the shared secret that you have configured on the RADIUS server. The shared secret is a password that is used to secure the communication between the AP and the RADIUS server.
9. Click **Submit.** The message "`Task #{N} is submitted. Please check the status area.`" appears.
10. Check the Status Area at the top of the page to see if the configuration change has been made successfully. When the device is online, it takes only a few minutes to apply configuration changes.

You have completed configuring your hotspot's basic settings. When your RADIUS server and captive portal are both configured correctly and running, your hotspot should now be operational.

Configuring a Walled Garden

The term *walled garden* refers to a list of URLs that users (who are associated with your hotspot) can access without providing a user name and password. When you are operating the hotspot in a hotel, for example, you can include the hotel's Web site in the walled garden. A walled garden for a corporate office, on the other hand, can include Web pages that show the office directory, emergency information or building maps.

You can add up to 64 entries to the Walled Garden hosts list. The following are the types of entries that are supported:

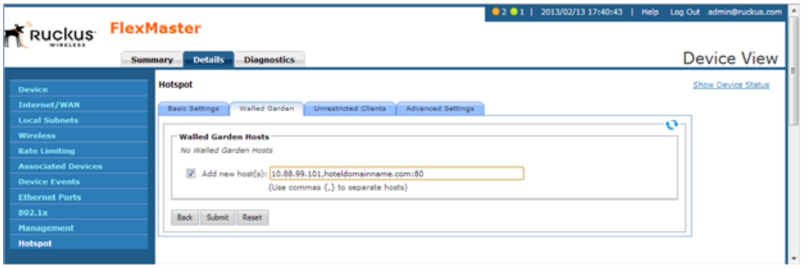
- IP address (for example, `10.1.1.1`)
- IP address/network mask (for example, `1.1.1.1/24`)
- Domain name (for example, `mydomainname.com`)

You can also append a port number to any of these entries (for example, `mydomainname.com:80`).

Follow these steps to add an entry to the walled garden list.

1. On the *Hotspot* page, click the **Walled Garden** tab. The *Walled Garden Hosts* page appears.
2. Click **Edit Settings**.

Figure 121. Hotspot page Walled Garden tab



Hotspot

Walled Garden Hosts

No Walled Garden Hosts

☑ Add new host(s): 10.88.99.101,hoteldomainname.com:80

(Use commas (,) to separate hosts)

3. Click the check box next to **Add new host(s)**. A text box appears.
4. In the text box, type the IP address, IP address/netmask, or domain name of the host that you want to add to the walled garden. When you are adding multiple hosts to the walled garden, use commas (,) to separate the hosts.
5. Click **Submit** to finish adding the entry to the list.

Repeat the same procedure for each entry that you want to add to the list.

To remove an entry, select the check box that is in the same row as the entry (under **Remove?**), and then click **Submit**.

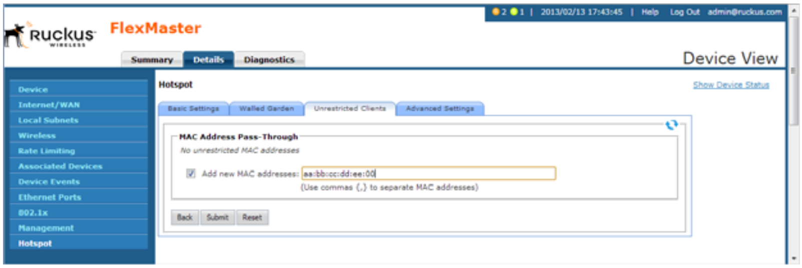
Specifying Unrestricted Clients

When there are certain wireless devices that you want to allow access to the hotspot service without having to go through the authentication process, you can add their MAC addresses to the passthrough list. You can add up to 64 MAC addresses to the passthrough list.

Follow these steps to add a MAC address to the pass-through list.

1. On the *Hotspot* page, click the **Unrestricted Clients** tab. The *MAC Address Pass-Through* page appears.
2. Click **Edit Settings**.

Figure 122. Hotspot page Unrestricted Clients tab



Hotspot

MAC Address Pass-Through

No unrestricted MAC addresses

☑ Add new MAC addresses: aa:bb:cc:dd:ee:00
(Use commas (,) to separate MAC addresses)

3. Click the check box next to **Add new MAC Address**. A text box appears.
4. In the text box, type the MAC address that you want to add to the pass-through list. When you are adding multiple MAC addresses to the pass-through list, use commas (,) to separate the MAC addresses.
5. Click **Submit** to finish adding the entry to the list.

Repeat the same procedure for each entry that you want to add to the pass-through list.

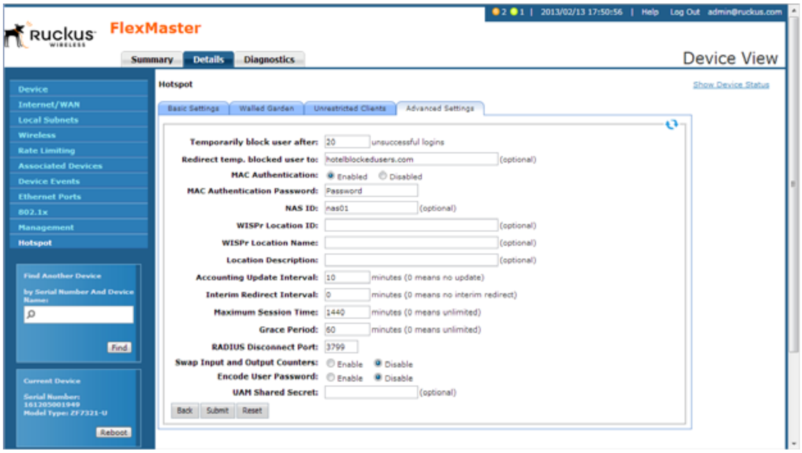
To remove an entry, select the check box that is in the same row as the entry (under **Remove?**), and then click **Submit**.

Configuring Advanced Settings

Advanced settings are optional settings that you may want to enable and configure to add functionality or to enhance your hotspot deployment. Advanced settings include DNS servers for hotspot users, a secondary RADIUS server, and SMTP relay, among others.

1. On the *Hotspot* page, click the **Advanced Settings** tab.
2. Click **Edit Settings**.

Figure 123. Hotspot page Advanced Settings tab



Temporarily block user after: 20 unsuccessful logins
Redirect temp. blocked user to: hotelblockedusers.com (optional)
MAC Authentication: ● Enabled ○ Disabled
MAC Authentication Password: Password
NAS ID: nas01 (optional)
WISPr Location ID: (optional)
WISPr Location Name: (optional)
Location Description: (optional)
Accounting Update Interval: 10 minutes (0 means no update)
Interim Redirect Interval: 0 minutes (0 means no interim redirect)
Maximum Session Time: 1440 minutes (0 means unlimited)
Grace Period: 60 minutes (0 means unlimited)
RADIUS Disconnect Port: 3799
Swap Input and Output Counters: ○ Enable ● Disable
Encode User Password: ○ Enable ● Disable
UAM Shared Secret: (optional)

3. Configure the following options:
   - *Temporarily block user after _x_ unsuccessful logins.*
   - *Redirect temp. blocked user to _x_* (optional).
   - *MAC Authentication:* Enabled or Disabled. (Add *MAC Authentication Password* if Enabled.
   - *NAS ID* (optional): Type the name which the RADIUS server uses to identify the AP.

NOTE: The *WISPr Location ID, WISPr Location Name* and *Location Description* parameters are location-related attributes that are sent to a RADIUS accounting server. If your organization operates multiple hotspots, then these attributes identify this specific hotspot location in the RADIUS data, which may be helpful for accounting.

- *WISPr Location ID:* Type the ISO and ITU country and area code that the AP includes in accounting and authentication requests. (Refer to **NOTE**.)
  The required code includes:
  – *isocc* (ISO-country-code) – The ISO country code that the AP includes in RADIUS authentication and accounting requests.
  – *cc* (country-code) – The ITU country code that the AP includes in RADIUS authentication and accounting requests.
  – *ac* (area-code) – The ITU area code that the AP includes in RADIUS authentication and accounting requests.

  – *network* - (to be determined)

  The following is an example of what the Location ID entry should look like:

  ```
  isocc=us,cc=1,ac=408,network=RuckusWireless
  ```

- *WISPr Location Name*. Type the name of the hotspot location. (Refer to **NOTE**.)
- *Location Description*. Type a description for the hotspot location. (Refer to **NOTE**.)
- *Accounting Update Interval _x_ minutes* (0 means no update).
- *Interim Redirect Interval _x_ minutes* (0 means no interim redirect).
- *Maximum Session Time _x_ minutes* (0 means unlimited).
- *Grace Period _x_ minutes* (0 means unlimited).
- *RADIUS Disconnect Port.* Default = 3799.
- *Swap Input and Output Counters:* Enable or Disable.
- *Encode User Password:* Enable or Disable.
- *UAM Shared Secret:* If you are using ChilliSpot as your access point controller application, then type the UAM password in UAM Secret. This is the password that the AP uses to access the ChilliSpot login CGI (`hotspotlogin.cgi`). The same password must be configured on the UAM server.

4. If you want portable devices that do not have input capability (for example, a keyboard to enter the user name and password) to still be able to access the hotspot, then click **Enabled** in *MAC Authentication*, and then type any value in *MAC Authentication Password.* The AP automatically authenticates these devices with the RADIUS server using their MAC addresses.

NOTE: Before these portable devices can access the hotspot service, you need to manually add their MAC addresses to the database of pre-approved devices on the RADIUS server. For information on how to do this, refer to the documentation provided with your RADIUS server software.

5. Click **Submit** to save your changes.

7

Monitoring Events and Network Activities

In This Chapter:

About the Monitor Page

The *Monitor* page allows you to view events that have occurred on FlexMaster and managed devices, and to configure alert notifications for connectivity issues that occur on various device views. It also provides SpeedFlex™, which you can use to measure the throughput from one device to another, and to view basic information about a specific client.

About User Customized Alarms

The operator can define customized threshold crossing alarms (alerts) for various events crossing operator-defined thresholds. These alarms can be sent as SNMP traps to SNMP servers, and/or via an email to a group or user, and/or to a syslog event. Refer to Configuring Alarm Settings for configuration instructions.

Setting user customized alerts requires defining two thresholds per event type, and then activating the corresponding alarms for the event type.

For instance, if the event type is *AP # of clients* and the thresholds are 100 and 200 clients, then FlexMaster can send alarms:

- When the client count goes up to 100 (send *low-threshold alarm set TCA*)
- When the client count goes up to 200 (send *high-threshold alarm set TCA*)
- When the client count goes down to 200 (send *high-threshold alarm clear TCA*)
- When the client count goes down to 100 (send *low-threshold alarm clear TCA*)

NOTE: For any alarms to be sent, the SNMP server information and/or email system information must be configured as described in "Configuring Alarm Settings" before FlexMaster can send the alarms.

Available Alarm Event Types

- *AP # of channel changes* (number of channel changes in the last hour)
- *AP # of clients* (number of concurrently connected clients)
- *AP # of reboot* (number of times in the last hour that the AP has rebooted)
- *AP lost connection* (number of hours the AP has been continuously disconnected)
- *AP traffic* (AP traffic, megabytes for the last hour)
- *FlexMaster server CPU usage* (FM CPU usage exceeds the threshold X percent 3 times continuously)
- *ZD CPU usage* (ZoneDirector CPU usage exceeds the threshold X percent 3 times continuously)

Monitoring Alarms

Alarms are a type of event that typically warrants your attention. Alarms are generated by managed access points and ZoneDirector devices and the FlexMaster server.

Alarms vary in severity. The following are the four alarm severity levels in FlexMaster (from highest severity to lowest severity):

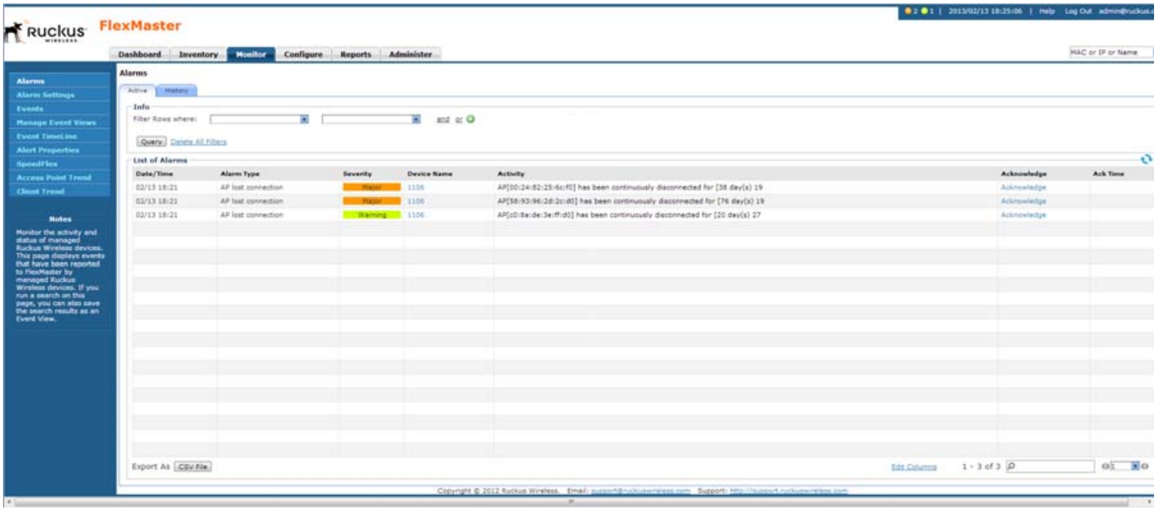
- Critical
- Major
- Minor
- Warning

Viewing and Acknowledging Alarms

Acknowledging an alarm lets other FlexMaster administrators know that someone is already looking into the issue.

1. Go to *Monitor > Alarms*. The **Active** tab, which lists the most recent alarms, appears by default. The **History** tab displays older alarms that have been acknowledged.

Figure 124. The Alarms page



Notes

Monitor the activity and status of managed Ruckus Wireless devices. This page displays events that have been reported to FlexMaster by managed Ruckus Wireless devices. If you run a search on this page, you can also save the search results as an Event View.

Date/Time	Alarm Type	Severity	Device Name	Activity	Acknowledge	Ack Time
02/13 18:21	AP lost connection	Major	1106	AP[00:24:82:25:6c:f0] has been continuously disconnected for [38 day(s) 19	Acknowledge	
02/13 18:21	AP lost connection	Major	1106	AP[58:93:96:2d:2c:d0] has been continuously disconnected for [76 day(s) 19	Acknowledge	
02/13 18:21	AP lost connection	Warning	1106	AP[c0:8a:de:3e:ff:d0] has been continuously disconnected for [20 day(s) 27	Acknowledge	

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

2. To acknowledge an alarm, click the alarm **Acknowledge** link.

   FlexMaster moves the alarm to the History tab, the *Acknowledge* column displays *Yes*, and the *Ack Time* column displays the date and time when the alarm was acknowledged.

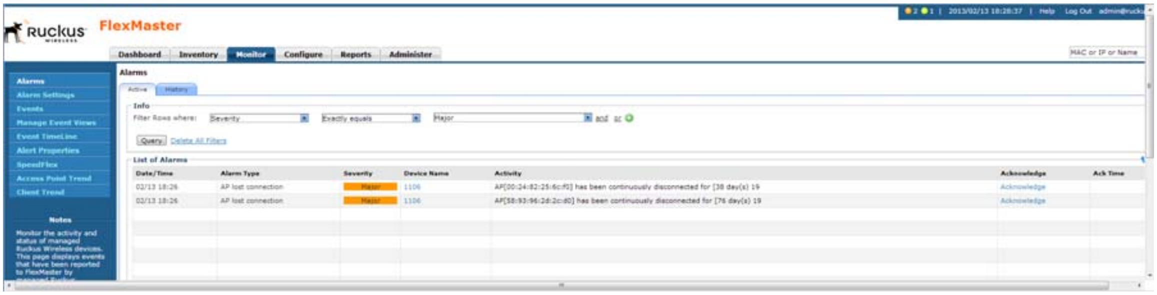
3. To view other alarms that have already been acknowledged, click the **History** tab.

Filtering Alarms

Use the *Info* section on the *Active* and *History* tabs to filter alarms based on a set of criteria.

1. On either the *Active* or *History* tab, look for the *Info* section. To search for alarms, you need to specify the criteria of the alarms that you want to display.

Figure 125. Creating a filter for major alarms



Filter Rows where: Severity | Exactly equals | Major

List of Alarms

Date/Time	Alarm Type	Severity	Device Name	Activity	Acknowledge	Ack Time
02/13 18:26	AP lost connection	Major	1106	AP[00:24:82:25:6c:f0] has been continuously disconnected for [38 day(s) 19	Acknowledge	
02/13 18:26	AP lost connection	Major	1106	AP[58:93:96:2d:2c:d0] has been continuously disconnected for [76 day(s) 19	Acknowledge	

2. In the first drop-down list box after **Filter Rows where**, select the filter attribute that you want to use. Options include *Date/Time, Alarm Type, Severity, Device Name*, and *Acknowledge* status.

3. In the second drop-down list box, select the filter operator that you want to use. Available filter operators include:

   - *Exactly equals*: Filter alarms with attributes that exactly match the filter parameter you entered. For example, if you selected *Severity* as the attribute and you entered `Critical` as the filter parameter, then only critical alarms appear in the filter results.
   - *Contains* (available only if *Device Name* is selected in the first drop-down list): Filter devices with attributes that include the filter parameter you entered. For example, if you entered `Ruckus` as the *Device Name* filter parameter, then all devices with "ruckus" in the device name (for example, **`ruckus`**`AP` and `AP`**`ruckus`**) appear in the filter results.
   - *Starts with* (available only if *Device Name* is selected in the first drop-down list): Filter devices with attributes that start with the filter parameter you entered. For example, if you entered `Ruckus` as the *Device Name* filter parameter, then only devices with device names that begin with "ruckus" (for example, **`ruckus`**`AP1,` **`ruckus`**`AP2)` appear in the filter results.
   - *Ends with* (available only if *Device Name* is selected in the first drop-down list): Filter devices with attributes that end with the filter parameter you entered. For example, if you entered `AP` as the *Device Name* filter parameter, then only devices with device names that end in "AP" (for example, `ruckus`**`AP`**`, lobby`**`AP`**) appear in the filter results.
   - *Later than* or *Earlier than* (available only if *Date/Time* is selected in the first drop-down list): Filter alarms based on the specified date and time.

   After you select a filter operator, a third (text) box appears.

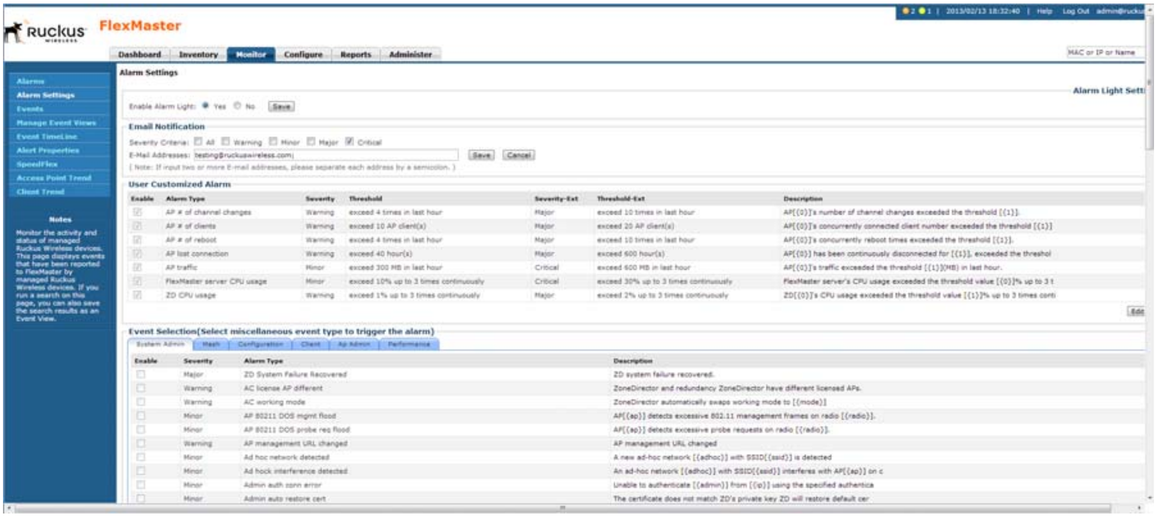
4. In the text box, type the filter parameter that you want to use with the attribute and operator that you selected. The required filter parameter depends on the attribute that you selected in the first drop-down list box.
   - If you selected *Date/Time*, then select a date and time in the text box.
   - If you selected *Alarm Type*, then select a specific alarm that you want to filter.
   - If you selected *Severity*, then select a severity level (Warning, Minor, Major, Critical) that you want to filter.
   - If you selected *Device Name*, then type the partial or full string of the device name that you want to filter.
   - If you selected *Acknowledge*, then select the acknowledgement status (No, Yes, Recovered, Duplicate) that you want to filter.
5. If you want to add another filter, then click ⊕. A second filter layer appears below the first. Complete the filter options as in the first filter. You can add up to three additional filters.
6. When you complete setting up the search filters, click **Query**. FlexMaster displays the alarms that match the filter criteria.

You have completed filtering alarms.

Configuring Alarm Settings

1. Go to *Monitor* > *Alarm Settings*. The *Alarm Settings* page appears.

Figure 126. The Alarm Settings page



Monitor the activity and status of managed Ruckus Wireless devices. This page displays events that have been reported to FlexMaster by managed Ruckus Wireless devices. If you run a search on this page, you can also save the search results as an Event View.

Enable Alarm Light: ● Yes ○ No

Severity Criteria: ☐ All ☐ Warning ☐ Minor ☐ Major ☑ Critical

E-Mail Addresses: testing@ruckuswireless.com;

(Note: If input two or more E-mail addresses, please separate each address by a semicolon.)

Enable	Alarm Type	Severity	Threshold	Severity-Ext	Threshold-Ext	Description
☑	AP # of channel changes	Warning	exceed 4 times in last hour	Major	exceed 10 times in last hour	AP[{0}]'s number of channel changes exceeded the threshold [{1}].
☑	AP # of clients	Warning	exceed 10 AP client(s)	Major	exceed 20 AP client(s)	AP[{0}]'s concurrently connected client number exceeded the threshold [{1}]
☑	AP # of reboot	Warning	exceed 4 times in last hour	Major	exceed 10 times in last hour	AP[{0}]'s concurrently reboot times exceeded the threshold [{1}].
☑	AP lost connection	Warning	exceed 40 hour(s)	Major	exceed 600 hour(s)	AP[{0}] has been continuously disconnected for [{1}], exceeded the threshol
☑	AP traffic	Minor	exceed 300 MB in last hour	Critical	exceed 600 MB in last hour	AP[{0}]'s traffic exceeded the threshold [{1}](MB) in last hour.
☑	FlexMaster server CPU usage	Minor	exceed 10% up to 3 times continuously	Critical	exceed 30% up to 3 times continuously	FlexMaster server's CPU usage exceeded the threshold value [{0}]% up to 3 t
☑	ZD CPU usage	Warning	exceed 1% up to 3 times continuously	Major	exceed 2% up to 3 times continuously	ZD[{0}]'s CPU usage exceeded the threshold value [{1}]% up to 3 times conti

Enable	Severity	Alarm Type	Description
☐	Major	ZD System Failure Recovered	ZD system failure recovered.
☐	Warning	AC license AP different	ZoneDirector and redundancy ZoneDirector have different licensed APs.
☐	Warning	AC working mode	ZoneDirector automatically swaps working mode to [{mode}]
☐	Minor	AP 80211 DOS mgmt flood	AP[{ap}] detects excessive 802.11 management frames on radio [{radio}].
☐	Minor	AP 80211 DOS probe req flood	AP[{ap}] detects excessive probe requests on radio [{radio}].
☐	Warning	AP management URL changed	AP management URL changed
☐	Minor	Ad hoc network detected	A new ad-hoc network [{adhoc}] with SSID[{ssid}] is detected
☐	Minor	Ad hock interference detected	An ad-hoc network [{adhoc}] with SSID[{ssid}] interferes with AP[{ap}] on c
☐	Minor	Admin auth conn error	Unable to authenticate [{admin}] from [{ip}] using the specified authentica
☐	Minor	Admin auto restore cert	The certificate does not match ZD's private key ZD will restore default cer

2. Configure the *Enable Alarm Light* section. When the alarm lights are enabled, they appear on the Help and Logout bar in the upper right corner of the Web interface.
   - To enable the alarm lights (default), click **Yes**.
   - To disable the alarm lights, click **No**.

   Click the **Save** button in the *Enable Alarm Light* section.
3. In the *Email Notification* section, configure the email address to which alarm notifications are sent. You also need to define the alarm severity for which to send notifications.
   - In *Email Addresses*, click **Edit** and then type the email address to which to send notifications. Use a semi-colon (;) to separate multiple email addresses.
   - In *Severity Criteria*, select the check boxes for the alarm severity for which you want to send notifications. Options include *All*, *Warning*, *Minor*, *Major* and *Critical*.

   Click the **Save** button in the *Email Notification* section.
4. Click **Edit** and then configure the alarm types in the *User Customized Alarm* section by assigning a severity level and setting a threshold value to each alarm type. Among others, these alarms include:
   - *AP # of channel changes*: Triggered when the number of channel changes per AP crosses either of the specified thresholds.
   - *AP # of clients*: Triggered when the number of clients per AP crosses either of the specified thresholds.
   - *AP lost connection*: Triggered when an AP is continuously disconnected for the either of the specified thresholds (numbers of hours).
   - *AP traffic*: Triggered when traffic on an AP crosses either of the specified thresholds (traffic in MB).
   - *FlexMaster server CPU usage*: Triggered when CPU usage on FlexMaster crosses either of the specified thresholds (CPU usage percentage).
   - *ZD CPU usage:* Triggered when CPU usage on a ZoneDirector crosses either of the specified thresholds (CPU usage percentage).

   Click the **Save** button in the *User Customized Alarm* section.
5. Configure the *Event Selection* section by selecting (enabling) events that trigger alarms. Events are categorized into the following tabs:
   - *System Admin*
   - *Mesh*
   - *Configuration*
   - *Client*
   - *AP Admin*
   - *Performance*

   Click the tab for an event group tab, click the **Edit** button at the bottom of the section, and then select the check boxes for events that trigger alarms. You can also change the severity level that is assigned to each event.

   Click the **Save** button in the *Event Selection* section.

You have completed configuring the alarm settings.

Monitoring Events

FlexMaster keeps a record of all events that occur on the server, managed ZoneDirector devices, standalone APs, and even on clients that associated with managed APs.

The Events section displays system events that have been reported by the managed Ruckus Wireless devices. The *List of Events* table columns include:

- *Date/Time*: When the event occurred.
- *Event Type*: Ruckus Wireless-designated event title.
- *Sev*: Severity of the event.
- *Device Name:* Name of the device.
- *Activity*: A description of the event.

Continue with the following:

- Searching for Events
- Creating an Event View

Searching for Events

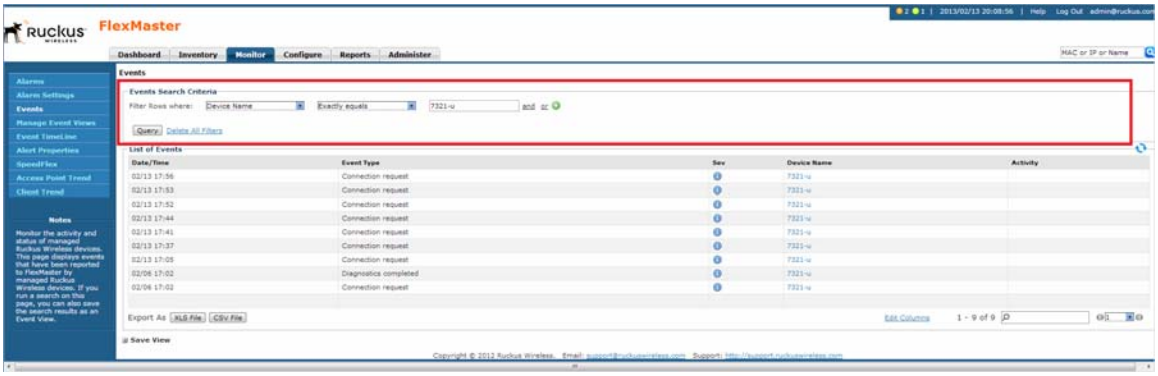
There are two ways to search for events:

- Search Using the Events Search Criteria
- Search Using the Search Box

Search Using the Events Search Criteria

1. Go to *Monitor* > *Events.*

Figure 127. Using Search Criteria to search for an event



Events

Events Search Criteria

Filter Rows where: Device Name | Exactly equals | 7321-u and or

List of Events

Date/Time	Event Type	Sev	Device Name	Activity
02/13 17:56	Connection request	●	7321-u	
02/13 17:53	Connection request	●	7321-u	
02/13 17:52	Connection request	●	7321-u	
02/13 17:44	Connection request	●	7321-u	
02/13 17:41	Connection request	●	7321-u	
02/13 17:37	Connection request	●	7321-u	
02/13 17:05	Connection request	●	7321-u	
02/06 17:02	Diagnostics completed	●	7321-u	
02/06 17:02	Connection request	●	7321-u	

1 - 9 of 9

Notes

Monitor the activity and status of managed Ruckus Wireless devices. This page displays events that have been reported to FlexMaster by managed Ruckus Wireless devices. If you run a search on this page, you can also save the search results as an Event View.

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

2. Look for the *Events Search Criteria* section. To search for events, you need to specify the criteria of the devices that you are looking for.

3. In the first drop-down list box after **Filter Rows where**, select the search attribute that you want to use. Options include *Date/Time*, *Event Type*, *Sev(erity)* and *Device Name*.

4. In the second drop-down list box, select the search operator that you want to use. Available search operators include:
   - *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected *Model* as the attribute and you entered `ZD3250` as the search parameter, then only devices of this model appear in the search results.
   - *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected *Serial Number* as the attribute and you entered `100` as the search parameter, then all devices with “100” in the serial number (for example, **`100`**`903000031` and `11090`**`100`**`0282`) appear in the search results.
   - *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected *Serial Number* as the attribute and you entered `3208` as the query parameter, then only devices with serial numbers that begin with “3208” (for example, `320833000219)` appear in the search results.

- *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected *Serial Number* as the attribute and you entered `011` as the query parameter, then only devices with model names that end in "001" (for example, 100903000**001**) appear in the search results.

After you select a search operator, a third (text) box appears.

5. In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.

6. If you want to add another search filter, then click ⊕. A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.

7. When you complete setting up the search filters, click **Query**. FlexMaster displays the devices that match the search criteria.

NOTE: When you save your query parameters as a view, any new events that occur after you create the view and meet the query criteria are automatically added to the saved view.

Additional Tasks That You Can Perform

After the search results appear, you can perform the following tasks:

- Save the search results as XLS (Microsoft® Excel® file format): In *Export As*, click **XLS File**. When the *Save As* dialog box appears, click **Save File**, and then click **OK**. Use Microsoft Excel to open the file.
- Save the search results as CSV (comma-separated value file): In *Export As*, click **CSV File**. When the *Save As* dialog box appears, click **Save File**, and then click **OK**. You can use any spreadsheet application (such as Microsoft Excel) to open the file.
- Save the results as an event view: Refer to Creating an Event View for more information.

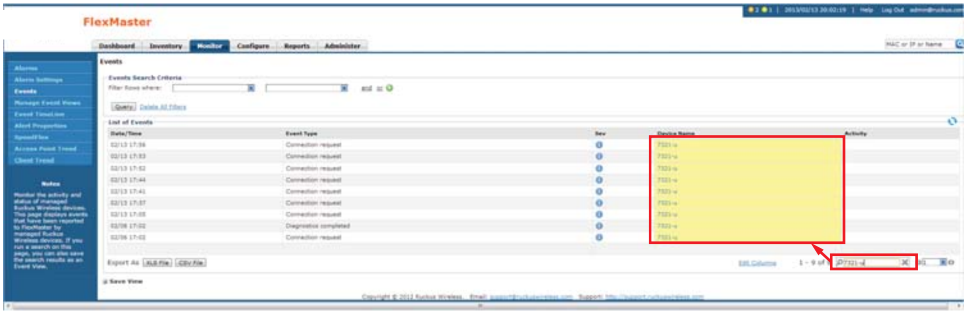
Search Using the Search Box

A search box exists at the bottom right area of the *List of Events* section. You can use this search box to search for events that have occurred on FlexMaster or any of the managed devices.

NOTE: When you save your query parameters as a view, any new events that occur after you create the view and meet the query criteria are automatically added to the saved view.

1. Type a search string into the box. The search string could be a partial or full string and can consist of numbers or letters or a combination of both.

Figure 128. The device property that matches the search string is highlighted in the search results



Date/Time	Event Type	Sev	Device Name	Activity
02/13 17:56	Connection request	●	7321-u	
02/13 17:53	Connection request	●	7321-u	
02/13 17:52	Connection request	●	7321-u	
02/13 17:44	Connection request	●	7321-u	
02/13 17:41	Connection request	●	7321-u	
02/13 17:37	Connection request	●	7321-u	
02/13 17:05	Connection request	●	7321-u	
02/06 17:02	Diagnostics completed	●	7321-u	
02/06 17:02	Connection request	●	7321-u	

2. Press **<Enter>**.

FlexMaster searches all its database columns for a match to the string that you entered, and then displays the results in the *List of Events* table.

Creating an Event View

An *event view* is a manually configured grouping of events with similar characteristics. For example, you can create an event view that contains ZoneDirector devices of the same model. Views are useful when want to view events that have occurred tasks on a group of devices.

1. Perform a search for events as described in Searching for Events.
2. When the search results appear, scroll down to the *Save as View* section.
3. In *View Name*, type a name that you want to assign to the view.
4. In *Description*, type an optional description for the view that you are saving. For example, when the view contains only ZoneDirector 3500 devices, you can type `ZD3500 only`.
5. Click **Save**.

The *Manage Event Views* page appears, displaying the event view that you have saved along with other saved event views (refer to Managing Event Views).

Managing Event Views

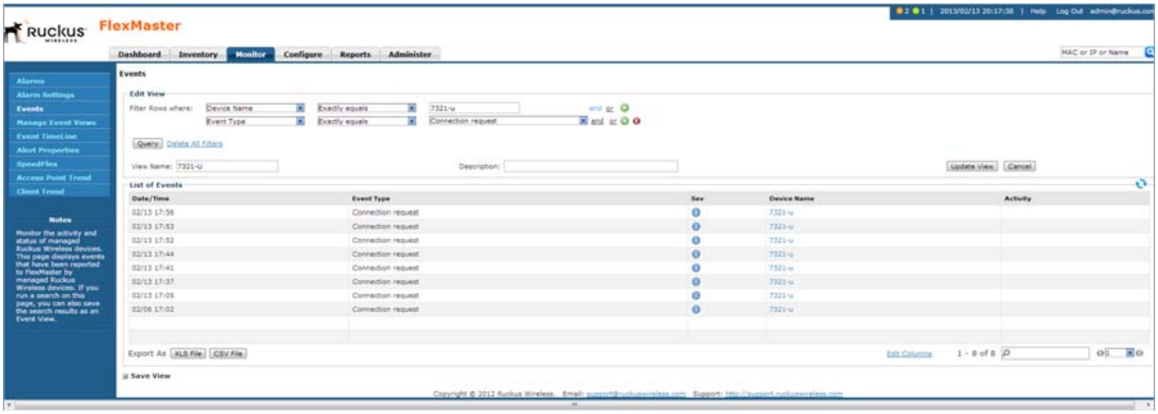
Use the *Manage Event Views* page to view list of existing event views, run a query, and edit or delete a view.

Editing an Event View

Editing an event view is very similar to the process of creating an event view.

1. Go to the *Monitor* > *Manage Event Views* page. All existing event views appear in the *Manage Event Views* section.

Figure 129. Editing an event view



Monitor the activity and status of managed Ruckus Wireless devices. This page displays events that have been reported to FlexMaster by managed Ruckus Wireless devices. If you run a search on this page, you can also save the search results as an Event View.

Events

Edit View

Filter Rows where: Device Name | Exactly equals | 7321-u | and or
Event Type | Exactly equals | Connection request | and or

View Name: 7321-U

Description:

List of Events

Date/Time	Event Type	Sev	Device Name	Activity
02/13 17:56	Connection request	ⓘ	7321-u	
02/13 17:53	Connection request	ⓘ	7321-u	
02/13 17:52	Connection request	ⓘ	7321-u	
02/13 17:44	Connection request	ⓘ	7321-u	
02/13 17:41	Connection request	ⓘ	7321-u	
02/13 17:37	Connection request	ⓘ	7321-u	
02/13 17:05	Connection request	ⓘ	7321-u	
02/06 17:02	Connection request	ⓘ	7321-u	

1 - 8 of 8

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

2. Look for the event view that you want to edit, and then click the **Edit** link that is in the same row as the event view name. The *Edit View* section appears.
3. Update any of the following to edit the view:
   - The search filter that you configured when you created the view
   - The view name
   - The description
4. To view devices that match the search filter that you updated, click **Query**.
5. To save the changes that you made, click **Update View**.

Deleting an Event View

1. Go to the *Inventory* > *ZoneDirector* > *Manage Views* page.
2. Click the event view **Delete** link. A confirmation message appears.
3. Click **OK** to confirm.

The *Manage Views* page refreshes, and then the view that you deleted disappears from the page.

Viewing the Event TimeLine

The Event TimeLine chart displays the events that have occurred on FlexMaster and its managed devices. Events are displayed per severity and include one- or two-word descriptions. The Event TimeLine chart is divided into the following areas:

1. Severity check boxes can be selected to show all or specific severities in the timeline.
2. Top gray area displays consolidated event types on a per-hour basis.
3. Bottom blue area displays consolidated event types on a per-day basis.
4. Within the bottom blue area, a gray “viewport” exists that corresponds to the span of time in the upper gray area. Thus, since the gray area displays a span of six hours, the gray viewport highlights those six hours in the blue area.

Figure 130. The Event TimeLine chart

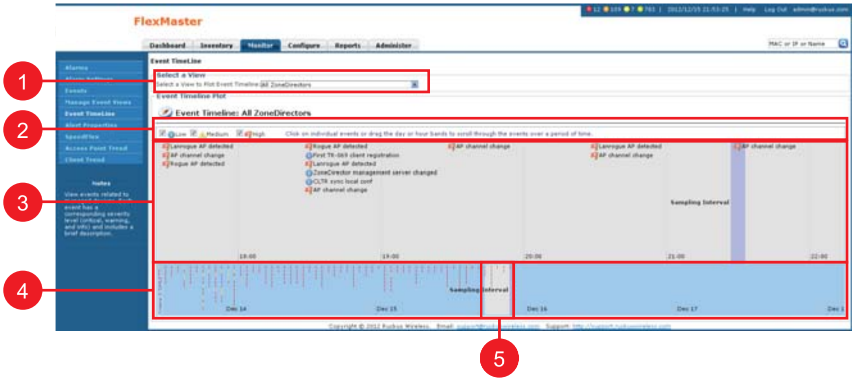


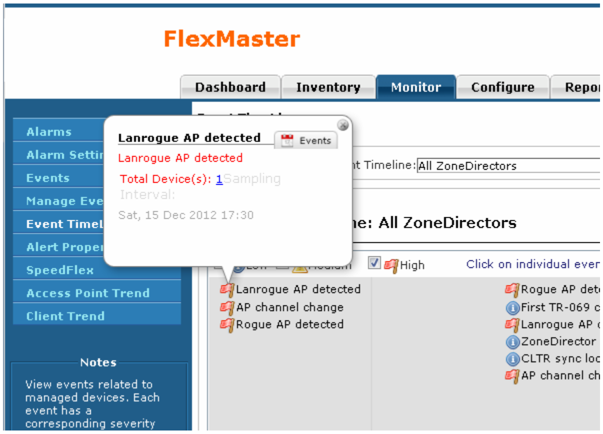
Table 29. Event TimeLine chart conventions

No.	Name	Description
1	Select a View	Select a view to filter the Event TimeLine graph based on the corresponding device view. By default, the graph defaults to *All Standalone APs*.
2	Severity selector	Info (blue), Warning (yellow) and Error (red) check boxes: • *Informational* events are lowest in severity, and are typically associated with configuration changes or device boot up. • *Warnings* events relate to device connectivity and communication. • *Errors* are critical events affecting the device's functionality.
3	Event details	Clicking an event from the gray area pops up an event window. You can click the *Total Device(s)* link displayed in this pop-up window to go to a *Monitor > Reports* view of the selected event. As the event may cover multiple devices, each device is displayed individually in the report.
4	Event summary	Shows higher-level visual information about the events.

Table 29. Event TimeLine chart conventions (Continued)

No.	Name	Description
5	Event summary sampling interval	Shows higher-level visual information about the events in the Event Details Sampling Interval.

Figure 131. The Event Detail pop-up window



Lanrogue AP detected
Lanrogue AP detected
Total Device(s): 1 Sampling Interval:
Sat, 15 Dec 2012 17:30

nt Timeline: All ZoneDirectors

ne: All ZoneDirectors

Click on individual ever

Lanrogue AP detected
AP channel change
Rogue AP detected

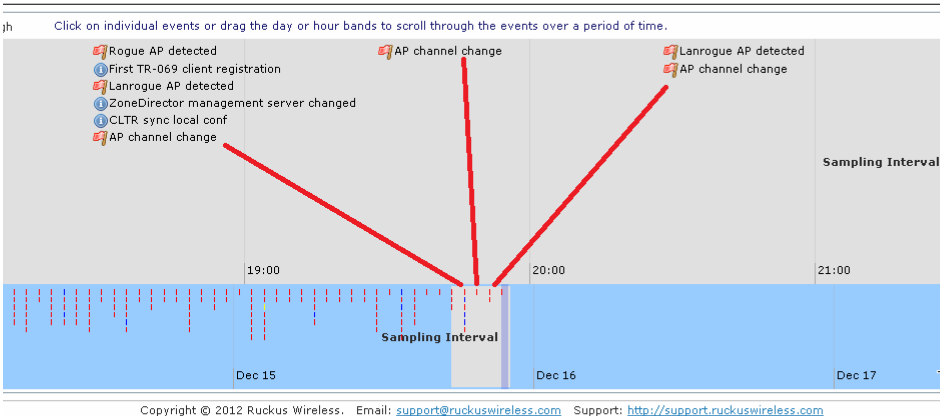
Rogue AP dete
First TR-069 c
Lanrogue AP c
ZoneDirector
CLTR sync loc
AP channel ch

Notes
View events related to managed devices. Each event has a corresponding severity

Colored Segments

In the blue area, each colored (vertical) segment represents a recorded event. The segment color identifies the severity of the event. Events are stacked by the hour in which they occurred. Thus, if there were seven events between 11:00 AM and 12:00 PM, then there are seven segments stacked in the blue area of the Event TimeLine according to the day and time.

Figure 132. Colored segments on the Events TimeLine widget



Click on individual events or drag the day or hour bands to scroll through the events over a period of time.

Rogue AP detected
First TR-069 client registration
Lanrogue AP detected
ZoneDirector management server changed
CLTR sync local conf
AP channel change

AP channel change

Lanrogue AP detected
AP channel change

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Hold and Drag

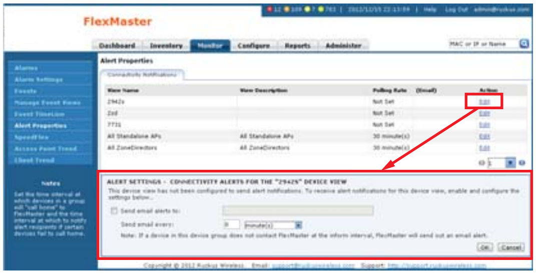
The Event TimeLine chart includes functionality that enables you to “drag” the timeline to view events in the past. By placing your pointer in either the gray or blue areas of the chart and holding down the left mouse button, you can drag the timeline (that is, moving your mouse to the right while holding down the left-mouse button) to view past segments of time and the events that occurred.

Configuring Alert Properties

The *Alert Properties* page enables you to set the "call home" interval for devices that belong to each device view. It also lets you set the amount of time to wait before FlexMaster sends out an alert message to the specified alert recipient for devices that fail to call home.

1. Go to *Monitor* > *Alert Properties*. All existing device views are listed.

Figure 133. Editing the alert property of a group


FlexMaster
Dashboard
Inventory
Monitor
Configure
Reports
Administer
MAC or IP or Name
Alarms
Alarm Settings
Events
Manage Event Views
Event TimeLine
Alert Properties
SpeedFlex
Access Point Trend
Client Trend
Notes
Set the time interval at which devices in a group will "call home" to FlexMaster and the time interval at which to notify alert recipients if certain devices fail to call home.
Connectivity Notifications

Alert Properties

View Name	View Description	Polling Rate	(Email)	Action
2942s		Not Set		Edit
2zd		Not Set		Edit
7731		Not Set		Edit
All Standalone APs	All Standalone APs	30 minute(s)		Edit
All ZoneDirectors	All ZoneDirectors	30 minute(s)		Edit

ALERT SETTINGS - CONNECTIVITY ALERTS FOR THE "2942S" DEVICE VIEW

This device view has not been configured to send alert notifications. To receive alert notifications for this device view, enable and configure the settings below...

□ Send email alerts to:

Send email every: 0 minute(s)

Note: If a device in this device group does not contact FlexMaster at the inform interval, FlexMaster will send out an email alert.

OK Cancel

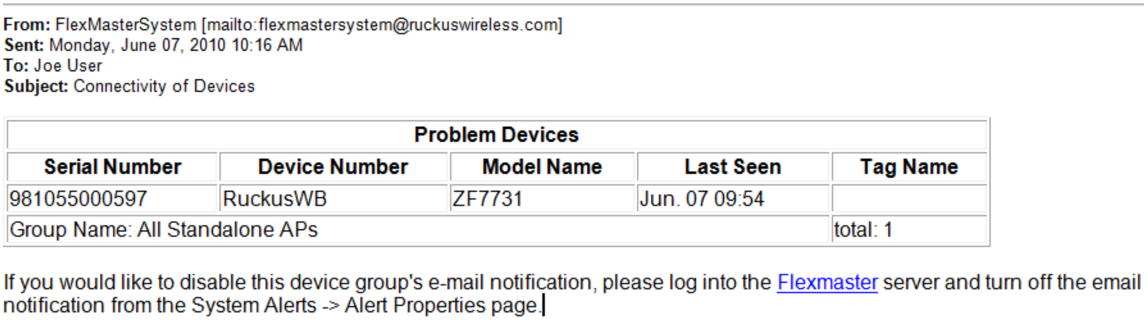
Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

> **NOTE:** The *Alert Properties* page can display up to five device views. If FlexMaster has more than five device views, then you need to click the ⊕ icon at the bottom-right side of the page to view the other device views on the next page.

2. In the *Action* column, click the **Edit** link that is in the same row as the name of the device view that you want to configure. The *ALERT SETTINGS* configuration form opens below the table.
3. Select the *Send email alerts to* check box to enable alert notification for this device view, and then enter the email address to which you want to send alert notifications. When you want to send alert notifications to multiple recipients, use commas (,) or semicolons (;) to separate their email addresses.
4. In *Send email every*, type a value and select the period of time (minutes, hours or days). The minimum interval is 1 minute.
5. Click **OK** to save your changes.

When a recipient does not want to receive subsequent alerts, he or she can click the FlexMaster link in the email message to open the FlexMaster Web interface, log on, and then turn off email notification in *Monitor* > *Alert Properties*.

Figure 134. Sample alert email message



From: FlexMasterSystem [mailto:flexmastersystem@ruckuswireless.com]
Sent: Monday, June 07, 2010 10:16 AM
To: Joe User
Subject: Connectivity of Devices

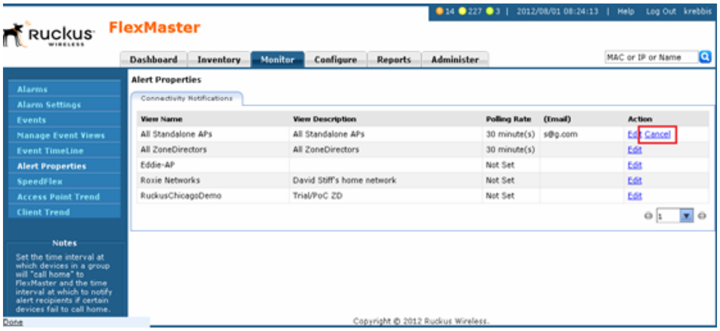
Problem Devices				
Serial Number	**Device Number**	**Model Name**	**Last Seen**	**Tag Name**
981055000597	RuckusWB	ZF7731	Jun. 07 09:54	
Group Name: All Standalone APs				total: 1

If you would like to disable this device group's e-mail notification, please log into the Flexmaster server and turn off the email notification from the System Alerts -> Alert Properties page.

Disabling an Alert

When you want to disable alert notifications for a certain device view, click the **Cancel** link that is in the same row as the device view name. You can also click the **Edit** link, then clear the *Send email alerts to* check box, and then click **OK**.

Figure 135. Click the Cancel link to disable alert notifications for the device group



View Name	View Description	Polling Rate	(Email)	Action
All Standalone APs	All Standalone APs	30 minute(s)	s@g.com	Edit Cancel
All ZoneDirectors	All ZoneDirectors	30 minute(s)		Edit
Eddie-AP		Not Set		Edit
Roxie Networks	David Stiff's home network	Not Set		Edit
RuckusChicagoDemo	Trial/PoC ZD	Not Set		Edit

Notes

Set the time interval at which devices in a group will "call home" to FlexMaster and the time interval at which to notify alert recipients if certain devices fail to call home.

Measuring Throughput Using SpeedFlex

FlexMaster includes a wireless performance tool called SpeedFlex that you can use to measure the downlink and uplink throughput between any of the following devices:

- ZoneDirector
- An AP that ZoneDirector is managing
- A wireless client that is associated with a FlexMaster- or ZoneDirector-managed AP

NOTE: When performing a site survey, you can use SpeedFlex to help find the optimum location for APs on the network with respect to user locations.

CAUTION! For SpeedFlex to work, the devices that you are testing must not be behind a NAT server. If one of the devices is behind a NAT server, then the test fails because SpeedFlex is unable to communicate with the device behind the NAT server.

To use SpeedFlex, you must first create a SpeedFlex task to assign the destination and source devices. When you create the task, you can also set it to run based on a recurring schedule.

Creating a SpeedFlex Task

Creating a SpeedFlex task requires that you specify the destination and source devices for running the test.

1. Go to *Monitor > SpeedFlex*.
2. Click the **Create Test** button. The *New SpeedFlex Test* form appears.
3. If you want to measure the throughput between hops (devices between the source and destination devices) in a mesh topology, then select the *Mesh Multi-hops Test* check box. If you want to measure the throughput between the source and destination devices only, then make sure that the *Mesh Multi-hops Test* check box is clear.
4. In *Source Device*, click the button with the ellipsis (...), and when the *Select Device* window appears, do the following:
    a. In *Select devices in the View*, select the device view to which the source device belongs. The *List of Devices* table refreshes, and displays the devices that belong to the selected view.
    b. Look for the device that you want to assign as the source device, and then click the **Select** link (in the *Actions* column) that is in the same row as the device name. The *Select Device* window disappears.

NOTE: You can only run SpeedFlex tests on devices that support the SpeedFlex feature and that are currently online. If the **Select** link does not appear in the same row as a particular device, then that device may be offline (check the *Connection* column) or may not support the SpeedFlex feature.

5. In *Dest Device*, repeat the steps your performed in Step 4, but this time, select the destination device.
6. Specify the traffic direction (uplink and downlink) for which you want to perform the throughput test. By default, both **Up Link** and **Dn Link** check boxes are selected, which means that FlexMaster tests the throughput for both directions.

NOTE: When you want to run the SpeedFlex test without saving it, skip the remaining steps and click the **Run** button now.

7. If you want this test to run automatically based on a recurring schedule, then do the following:
   a. Select the *Schedule Test* check box. The *Schedule* form appears below.
   b. In *Frequency*, select how often you want this test to run.
   c. In *Time of Day*, select the time when this test runs.
   d. In *Email report to*, type the email address to which the SpeedFlex test results are sent. When you want to send the report to multiple email addresses, use a comma (,) or semicolon (;) to separate the email addresses.
8. In *Test Name*, type a name that you want to use for this SpeedFlex test. After you save this test, it appears in the *List of SpeedFlex Tests* with the test name that you assigned.
9. Click **Save**. The *List of SpeedFlex Tests* table refreshes, and then the test that you created appears in the table.

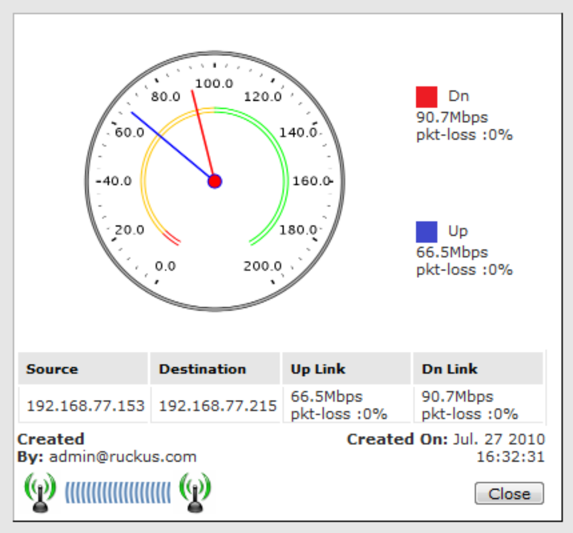
Running a SpeedFlex Task

In addition to scheduling when you want a SpeedFlex task to run, you can also run it manually.

1. Go to *Monitor > SpeedFlex.*
2. In *List of SpeedFlex Tests*, select the check box for the SpeedFlex test that you want to run. When you want to run multiple tests at the same time, select the check boxes for all the SpeedFlex tests that you want to run.
3. Click **Run Test(s)**. The SpeedFlex *Performance Test* window appears and displays a speedometer that indicates the downlink and uplink throughput detected by FlexMaster. When both downlink and uplink throughput values appear, the SpeedFlex test is complete.

If you selected multiple SpeedFlex tests to run, then FlexMaster runs the tests sequentially and shows all test results on the same page.

Figure 136. SpeedFlex test result sample



🟥 Dn
90.7Mbps
pkt-loss :0%

🟦 Up
66.5Mbps
pkt-loss :0%

Source	Destination	Up Link	Dn Link
192.168.77.153	192.168.77.215	66.5Mbps pkt-loss :0%	90.7Mbps pkt-loss :0%

Created By: admin@ruckus.com

Created On: Jul. 27 2010 16:32:31

Editing a SpeedFlex Test

When you want to change the traffic direction to test, change the test name, or change the test schedule, you can edit the SpeedFlex test.

1. In *List of SpeedFlex Tests*, look for the SpeedFlex test that you want to edit.
2. Click the **Edit** link that is in the same row as the test name. The *New SpeedFlex Test* form appears below.
3. Edit the test details as required.
4. Click **Save**.

You have completed editing the SpeedFlex test.

Deleting a SpeedFlex Test

When you no longer need a SpeedFlex test that you created previously, you can delete it.

1. In *List of SpeedFlex Tests*, look for the SpeedFlex test that you want to delete.
2. Select the check box (in the *Select* column) that is in the same row as the test name. You can select more than one test name to delete at the same time.
3. Click **Delete**. The *List of SpeedFlex Tests* refreshes, and then the SpeedFlex test that you deleted disappears from the list.

You have completed deleting a SpeedFlex test.

Monitoring Access Point Trends

The *Access Point Trend* page on the *Monitor* tab allows you to display basic information about a Ruckus Wireless AP. You need to know the AP's MAC address to be able to run a query on it.

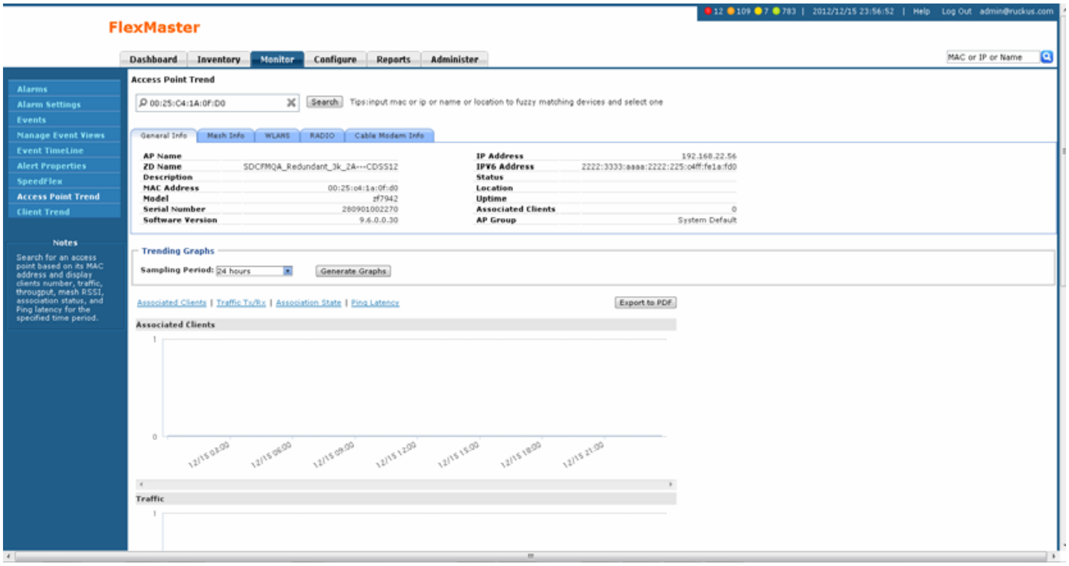
1. Go to the *Monitor > Access Point Trend* page.
2. In *MAC*, type the AP MAC address and click **Search**. FlexMaster displays the AP's basic information under four or five tabs:
   - *General Info*: The name and other information about the AP.
   - *Mesh Info*: The mesh type and other information about this AP, when the AP is part of a mesh network.
   - *WLANs*: The Name/ESSID of WLANs, and other information about this AP.
   - *Radio*: The Current Channel used by this AP's radio.
   - *Cable Modem Info*: When the AP is equipped with an integral cable modem (for instance, ZF7761-CM or ZF7781-CM), clicking this tab takes you to a cable modem *Trends* page.
3. To display trending graphs for the AP:
   - Select a *Sampling Period.*
   - Click **Generate Graphs**.

   FlexMaster displays the AP's trends information at the bottom of the page:
   - *Associated Clients*
   - *Traffic Tx and Rx*
   - *Association State*
   - *Ping Latency*

To save AP trending graphs:

- Click **Export to PDF.**
- FlexMaster prints the information on the screen to a PDF file on your workstation.

Figure 137. Access Point Trends page



Access Point Trend

00:25:C4:1A:0F:D0

Tips:input mac or ip or name or location to fuzzy matching devices and select one

AP Name		IP Address	192.168.22.56
ZD Name	SDCFMQA_Redundant_3k_2A---CDSS12	IPV6 Address	2222:3333:aaaa:2222:225:c4ff:fe1a:fd0
Description		Status	
MAC Address	00:25:c4:1a:0f:d0	Location	
Model	zf7942	Uptime	
Serial Number	280901002270	Associated Clients	0
Software Version	9.6.0.0.30	AP Group	System Default

Trending Graphs

Sampling Period: 24 hours

Associated Clients

Notes

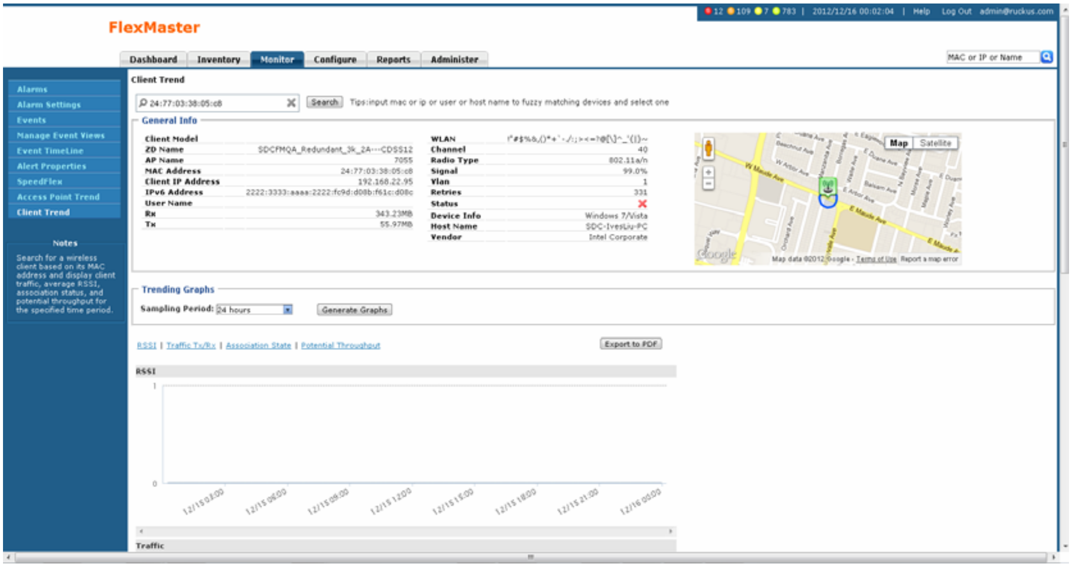
Search for an access point based on its MAC address and display clients number, traffic, througput, mesh RSSI, association status, and Ping latency for the specified time period.

Monitoring Client Trends

The *Monitor > Client Trend* page allows you to query basic information about a wireless client that is associated with a managed AP. You need to know the wireless client's MAC address to be able to run a query on it.

1. Go to the *Monitor > Client Trend* page.
2. In *MAC Address*, type the MAC address of the client which you want to query for basic information.

Figure 138. Client Trend page



Search for a wireless client based on its MAC address and display client traffic, average RSSI, association status, and potential throughput for the specified time period.

Client Trend

24:77:03:38:05:c8

Tips:input mac or ip or user or host name to fuzzy matching devices and select one

General Info

Client Model		WLAN	!"#$%&,()*+'-./:;><=?@[\]^_'{|}~
ZD Name	SDCFMQA_Redundant_3k_2A---CDSS12	Channel	40
AP Name	7055	Radio Type	802.11a/n
MAC Address	24:77:03:38:05:c8	Signal	99.0%
Client IP Address	192.168.22.95	Vlan	1
IPv6 Address	2222:3333:aaaa:2222:fc9d:d08b:f61c:d08c	Retries	331
User Name		Status	✗
Rx	343.23MB	Device Info	Windows 7/Vista
Tx	55.97MB	Host Name	SDC-IvesLiu-PC
		Vendor	Intel Corporate

Trending Graphs

Sampling Period: 24 hours

3. Click **Search**. The page refreshes, and then displays the client's basic information, including but not limited to:
   - *ZD Name*: The name of ZoneDirector device that is managing the client's parent AP.
   - *AP Name*: The name of the client's parent AP.
   - *User IP*: The IP address assigned to the client.
   - *WLAN*: The SSID or wireless network name with which the client is associated.
   - *Channel*: The wireless channel used by the WLAN.
   - *Radio Type*: The wireless radio used by the WLAN.
   - *Signal*: The RSSI strength of the WLAN.
   - *Status*: A green check mark indicates that the client is currently connected. A red cross mark indicates that is it disconnected.

   The right side of the page also displays a map with the client location indicated by a blue circle. The client location is determined by the AP.

4. When you want to view a graph version of the signal strength history for a specific time period, select a time period in *Sampling Period*, and then click **Generate Graphs.**

   FlexMaster displays graphs of the client's RSSI, traffic, association state, and potential throughput.

8

Working with Reports

In This Chapter:

Available Report Types

The following table lists the different report types that you can generate in FlexMaster. For instructions on how to generate each type of report, refer to the succeeding sections.

Table 30. Available reports in FlexMaster

Report Name	Description
Device View	Generate reports using different report types for selected device views. Generated reports can be saved so you can perform the same report query with a single click of a button. You can also edit and delete saved reports.
Active Firmware	View a list of devices that are currently using the selected firmware.
Historical Connectivity	View the connection statuses of managed devices in different device views.
Client Association	Identify clients that are currently associated with FlexMaster-managed, ZoneDirector-managed, and standalone APs.
SSID Report	View the number of ZoneDirector devices and APs on which a particular SSID is configured. You can also view graphs of associated clients, received traffic, and transmitted traffic per SSID.
Provision	List the statuses of all tasks that you have provisioned, listed by task types.
Events	List all events that match the selected event category, device category, and event type.
SpeedFlex	View completed throughput test results based on the test name, source and destination device names and IP addresses, date executed, tester, and other information.
Capacity	Display device capacity data based on throughput, associated clients, airtime utilization, and traffic, among others.
SLA	Display SLA related information, including uptime, downtime, and potential throughput.
Troubleshooting	Generate various graphs that are useful for troubleshooting, including # of Child APs, # of Hops, Change of Topology of Mesh, Client Phy Rate, Client RSSI, Mesh RSSI, # of Reboot, Physical Link Distance and Ping Test.
Resource Monitor	View CPU, memory, and disk usage on ZoneDirector devices.

Generating a Device View Report

A device view report includes device information such as, connected and disconnected devices and APs, connected wireless clients, wireless mesh report, connectivity report, diagnostic report, and bridge AP report.

NOTE: The *Report > Device View* is a real time report, while the *Dashboard > Standalone AP Device View* is updated every 15 minutes. Therefore, there are differences between the two views.

1. Go to *Reports > Report Categories > Device View.*
2. In *Device View*, select the device view for which you want to generate a report. Default device views include:
   - **All Standalone APs**
   - **All ZoneDirectors**

   When there are custom device views, they also appear in the list of options.

NOTE: If you selected 2-tier management mode, then ZoneDirector options are not visible on the page and ZoneDirector information is not included in the report that you are generating.

3. If you selected **All ZoneDirectors**, then continue with Step 4. If you selected **All Standalone APs**, then continue with Step 5.
4. If you selected **All ZoneDirectors**, then select one of the following options in *Report Type:*
   - *ZoneDirectors:* Shows all monitored ZoneDirectors.
   - *Connected ZoneDirectors:* Shows all currently-connected ZoneDirectors.
   - *Disconnected ZoneDirectors:* Shows all currently-disconnected ZoneDirectors.
   - *All Access Points:* Shows all ZoneDirector-managed APs.
   - *Connected Access Points:* Shows all currently-connected ZoneDirector-managed APs.
   - *Disconnected Access Points:* Shows all currently-disconnected ZoneDirector-managed APs.
   - *Connected Clients:* Shows all currently-connected ZoneDirector-managed clients.
   - *Mesh Report:* Shows the ZoneDirector devices on which mesh networking is enabled. To view the mesh tree for a particular ZoneDirector device, click the View Mesh link (in the *Details* column) that is in the same row as the ZoneDirector name. After you generate the mesh report, you can export the mesh tree information as a Microsoft Excel file by clicking the **Save This Report as XLS** link above the table.
   - *AP with no user connectivity:* Shows all currently-connected ZoneDirector-managed APs with no clients.
   - *Diagnostic:* Shows the connection status, uptime information, uplink and downlink RSSI, hop, # of downlinks, and distance (among others) for each ZoneDirector device in the selected view.

- *Rogue APs:* Shows information for all currently-detected rogue APs.

Continue with Step 6.

5. If you selected **All Standalone APs**, then select one of the following options in *Report Type:*
   - *APs:* Shows all directly-managed APs.
   - *Currently Connected:* Shows all directly-managed APs that communicated with FlexMaster at the last inform interval.
   - *Seen in Last 24 hours:* Shows all directly-managed APs that communicated with FlexMaster some time in the last 24 hours.
   - *Seen in Last 48 hours:* Shows all directly-managed APs that communicated with FlexMaster some time in the last 48 hours.
   - *Currently Disconnected:* Shows all directly-managed APs that did not communicate with FlexMaster at the last inform interval.
   - *Connected Clients:* Shows the clients associated with the all currently-connected directly-managed APs.
   - *Bridge APs:* Shows all directly-managed bridge APs. Details show include device name, serial number, MAC address, IP address, uptime, bridge mode, and RX and TX RSSI (among others)

   Continue with Step 6.
6. If you selected:
   - *Device View: All ZoneDirectors* and *Report Type: All Access Points*, or *Connected Access Points*, or *Disconnected Access Points*, also select:
     - *AP Type: APs, Root APs, Mesh APs*, or *eMesh APs*, and
     - *Period (for the report):* between *1 hour* and *24 hours*, or *Greater than 24 hours*.
   - *Device View: All ZoneDirectors* and *Report Type: AP with no user connectivity*, also select:
     - *Period (for the report):* between *1 hour* and *24 hours*, or *Greater than 24 hours*.
7. (Optional) If you want to add a search filter to your query, then configure the options in the *Filters* section.

   a. In the first drop-down list box after *Filter Rows where,* select the search attribute that you want to use. Options include *device name, serial number, location, MAC address, IP address, model, last seen,* and others.

   b. In the second drop-down list box, select the search operator that you want to use. Available search operators include:
     - *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered `172.17.16.176` as the search parameter, then only devices with this IP address appear in the search results.
     - *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered `100` as the search parameter, then all devices with "100" in the IP address (for example, `172.17.16.`**`100`** and **`100`**`.1.10.13`) appear in the search results.

- *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered `3908` as the query parameter, then only devices with serial numbers that begin with "3908" (for example, `390801005202`) appear in the search results.
- *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected **IP address** as the attribute and you entered `13` as the query parameter, then only devices with model names that end in "13" (for example, `100.1.10.`**`13`**) appear in the search results.

c. In the third text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.

d. If you want to add another search filter, then click ⊕. A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.

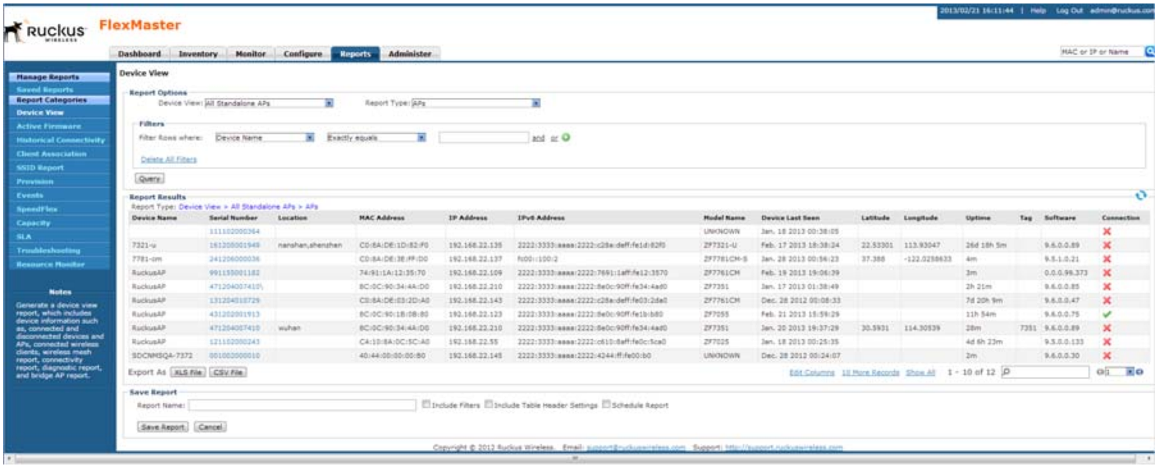
8. Click **Query**. The page refreshes, and then a list of devices that belong to the device view that you specified appears on the page.

For AP-related reports, device details that are shown on the *Reports* page include:

- Device Name
- Serial Number
- Location
- MAC Address
- IP Address
- IPv6 Address
- Model Name
- Device Last Seen
- Latitude
- Longitude
- Uptime
- Tag
- Software
- Connection (connected or disconnected)

NOTE: In any device view report, if you click an *AP MAC* Address hyperlink, then FlexMaster displays the *ZoneDirector > Monitor > Access Point Trend* window. Refer to Monitoring Access Point Trends.
If you click a *Client MAC* address hyperlink, then FlexMaster displays the *ZoneDirector > Monitor > Currently Active Clients* screen in another window. The *Currently Active Clients* screen includes the OS or Type (if known), the authorization method, the WLAN and VLAN used, the client IP address, and the AP MAC address, among others.

Figure 139. A sample device view report



Device View

Report Options

Device View: All Standalone APs   Report Type: APs

Filters

Filter Rows where: Device Name   Exactly equals   and or

Delete All Filters

Report Results

Report Type: Device View > All Standalone APs > APs

Device Name	Serial Number	Location	MAC Address	IP Address	IPv6 Address	Model Name	Device Last Seen	Latitude	Longitude	Uptime	Tag	Software	Connection
	111102000364					UNKNOWN	Jan. 18 2013 00:38:05						✗
7321-u	161200001949	nanshan,shenzhen	C0:8A:DE:1D:82:F0	192.168.22.135	2222:3333:aaaa:2222:c28a:deff:fe1d:82f0	ZF7321-U	Feb. 17 2013 18:38:24	22.53301	113.93047	26d 18h 5m		9.6.0.0.89	✗
7781-cm	241206000036		C0:8A:DE:38:FF:D0	192.168.22.137	fc00::100:2	ZF7781CM-S	Jan. 28 2013 00:56:23	37.388	-122.0258633	4m		9.5.1.0.21	✗
RuckusAP	991155001182		74:91:1A:12:35:70	192.168.22.109	2222:3333:aaaa:2222:7691:1aff:fe12:3570	ZF7761CM	Feb. 19 2013 19:06:39			3m		0.0.0.98.373	✗
RuckusAP	471204007410\		8C:0C:90:34:4A:D0	192.168.22.210	2222:3333:aaaa:2222:8e0c:90ff:fe34:4ad0	ZF7351	Jan. 17 2013 01:38:49			2h 21m		9.6.0.0.85	✗
RuckusAP	131204010729		C0:8A:DE:03:2D:A0	192.168.22.143	2222:3333:aaaa:2222:c28a:deff:fe03:2da0	ZF7761CM	Dec. 28 2012 00:08:33			7d 20h 9m		9.6.0.0.47	✗
RuckusAP	431202001913		8C:0C:90:1B:0B:80	192.168.22.123	2222:3333:aaaa:2222:8e0c:90ff:fe1b:b80	ZF7055	Feb. 21 2013 15:59:29			11h 54m		9.6.0.0.75	✓
RuckusAP	471204007410	wuhan	8C:0C:90:34:4A:D0	192.168.22.210	2222:3333:aaaa:2222:8e0c:90ff:fe34:4ad0	ZF7351	Jan. 20 2013 19:37:29	30.5931	114.30539	28m	7351	9.6.0.0.89	✗
RuckusAP	121102000243		C4:10:8A:0C:5C:A0	192.168.22.55	2222:3333:aaaa:2222:c610:8aff:fe0c:5ca0	ZF7025	Jan. 18 2013 00:25:35			4d 6h 23m		9.5.0.0.133	✗
SDCNMSQA-7372	001002000010		40:44:00:00:00:B0	192.168.22.145	2222:3333:aaaa:2222:4244:ff:fe00:b0	UNKNOWN	Dec. 28 2012 00:24:07			2m		9.6.0.0.30	✗

Export As

1 - 10 of 12

Save Report

Report Name: ☐ Include Filters ☐ Include Table Header Settings ☐ Schedule Report

Notes

Generate a device view report, which includes device information such as, connected and disconnected devices and APs, connected wireless clients, wireless mesh report, connectivity report, diagnostic report, and bridge AP report.

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Generating an Active Firmware Report

An active firmware report shows the firmware versions that are currently installed on APs or ZoneDirector devices that FlexMaster is managing.

1. Go to *Reports > Report Categories > Active Firmware.*
2. In *Firmware,* click the device model/firmware version combination that you want to search for. The options that appear on this menu correspond to the firmware files that you uploaded to FlexMaster on the *Configure > Common> Manage Firmware Files* page.
3. (Optional) If you want to add a search filter to your query, then configure the options in the *Filters* section.
   a. In the first drop-down list box after *Filter Rows where,* select the search attribute that you want to use. Options include device name, serial number, MAC address, IP address, model, last seen, and others.
   b. In the second drop-down list box, select the search operator that you want to use. Available search operators include:
      – *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered `172.17.16.176` as the search parameter, then only devices with this IP address appear in the search results.
      – *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered `100` as the search parameter, then all devices with "100" in the IP address (for example, `172.17.16.`**`100`** and **`100`**`.1.10.13`) appear in the search results.
      – *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered `3908` as the query parameter, then only devices with serial numbers that begin with "3908" (for example, `390801005202`) appear in the search results.
      – *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected **IP address** as the attribute and you entered `13` as the query parameter, then only devices with model names that end in "13" (for example, `100.1.10.`**`13`**) appear in the search results.
   c. In the third text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
   d. If you want to add another search filter, then click ⊕. A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.
4. Click **Query**.

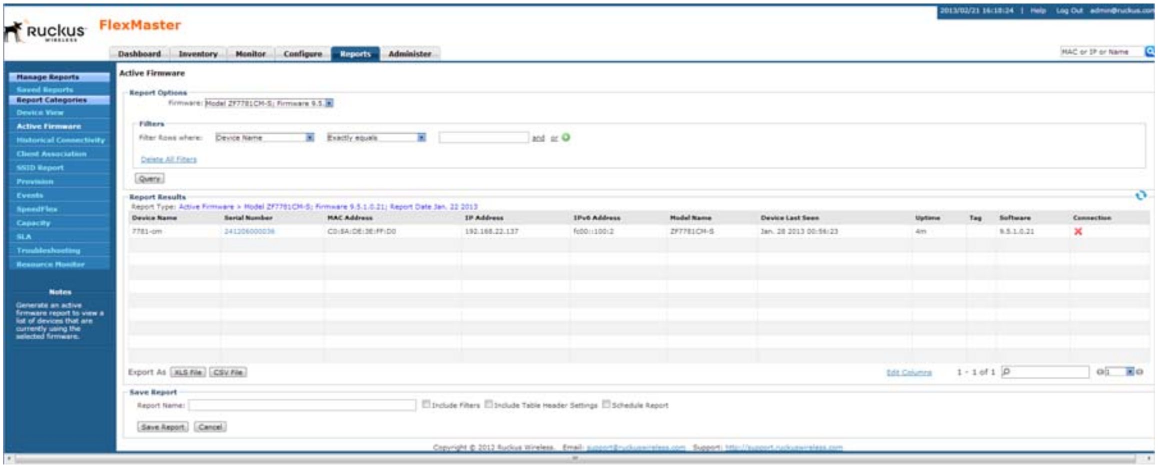
   The page refreshes, and then displays the devices that are currently using the firmware version you specified. Firmware details that are shown include:

   - Device Name

- Serial Number
- MAC Address
- IP Address
- IPv6 Address
- Model Name
- Device Last Seen
- Uptime
- Tag
- Software
- Connection (connected or disconnected)

NOTE: FlexMaster provides options for filtering devices that are included in the report. Options for saving the generated report, automating report generation, and saving the report as an Excel file are also available. For more information, refer to Using Advanced Report Options.

Figure 140. A sample active firmware report



Notes

Generate an active firmware report to view a list of devices that are currently using the selected firmware.

Active Firmware

Report Options

Firmware: Model ZF7781CM-S; Firmware 9.5.

Filters

Filter Rows where: Device Name | Exactly equals

Report Results

Report Type: Active Firmware > Model ZF7781CM-S; Firmware 9.5.1.0.21; Report Date Jan. 22 2013

Device Name	Serial Number	MAC Address	IP Address	IPv6 Address	Model Name	Device Last Seen	Uptime	Tag	Software	Connection
7781-cm	241206000036	C0:8A:DE:3E:FF:D0	192.168.22.137	fc00::100:2	ZF7781CM-S	Jan. 28 2013 00:56:23	4m		9.5.1.0.21	✗

1 - 1 of 1

Save Report

Report Name:

□ Include Filters □ Include Table Header Settings □ Schedule Report

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Generating a Historical Connectivity Report

A historical connectivity report displays the connection statuses of managed devices in different device views.

1. Go to *Reports* > *Report Categories* > *Historical Connectivity.*
2. In *Device View*, select the device view for which you want to generate a report. Default device views include:
   - **All Standalone APs**
   - **All ZoneDirectors**

   When there are custom device views, they also appear in the list of options.

NOTE: If you selected 2-tier management mode, then ZoneDirector options is not visible on the page and ZoneDirector information is not included in the report that you are generating.

3. In *Report Type*, configure the type of report that you want to view. The available report options depend on the device view that you selected in the previous step.
   - If you selected **All ZoneDirectors**, then select one of the following options in *Report Type:*
     - *Connected ZoneDirectors*: Shows all ZoneDirector devices that communicated with FlexMaster at the last inform interval
     - *Disconnected ZoneDirectors*: Shows all ZoneDirector devices that did not communicate with FlexMaster at the last inform interval
     - *Connected Access Points*: Shows all APs that are currently connected to their parent ZoneDirector
     - *Disconnected Access Points*: Shows all APs that have lost connection with their parent ZoneDirector.
     - *Continuously Disconnected APs*: Shows all APs that have continuously lost connection with their parent ZoneDirector.
   - If you selected **All Standalone APs**, then select one of the following options in *Report Type:*
     - *Connected*: Shows all directly-managed APs that communicated with FlexMaster at the last inform interval
     - *Disconnected*: Shows all directly-managed APs that did not communicate with FlexMaster at the last inform interval
4. (Optional) If you want to add a search filter to your query, then configure the options in the *Filters* section.

   a. In the first drop-down list box after *Filter Rows where,* select the search attribute that you want to use. Options include name, serial number, IP address, external IP address, model, last seen, and others.

   b. In the second drop-down list box, select the search operator that you want to use. Available search operators include:

- *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered `172.17.16.176` as the search parameter, then only devices with this IP address appear in the search results.
- *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered `100` as the search parameter, then all devices with "100" in the IP address (for example, `172.17.16.`**`100`** and **`100`**`.1.10.13`) appear in the search results.
- *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered `3908` as the query parameter, then only devices with serial numbers that begin with "3908" (for example, `390801005202`) appear in the search results.
- *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected **IP address** as the attribute and you entered `13` as the query parameter, then only devices with model names that end in "13" (for example, `100.1.10.`**`13`**) appear in the search results.

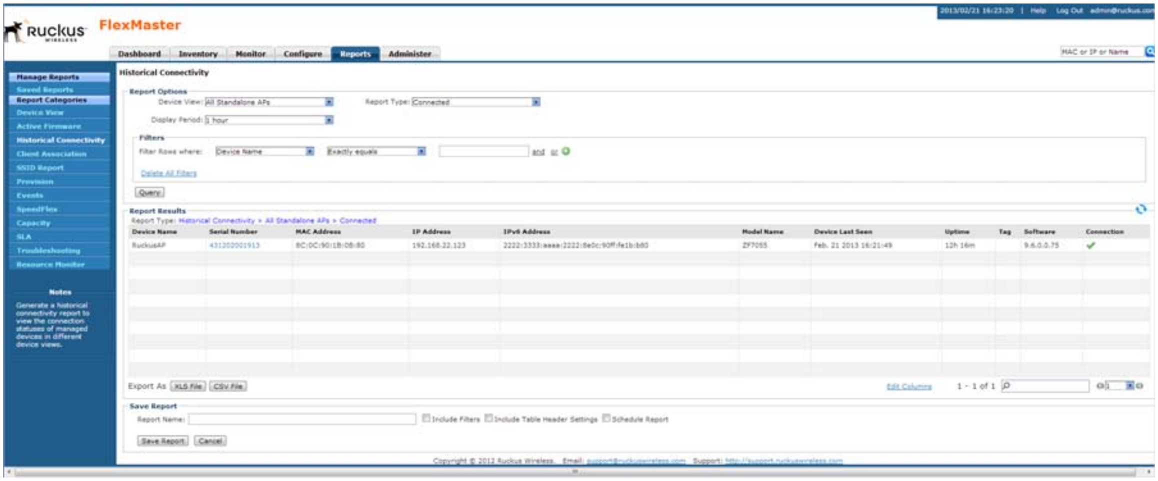
c. In the third text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.

d. If you want to add another search filter, then click ⊕. A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.

5. Click **Query**.

The page refreshes, and then displays devices that have not called home to FlexMaster within the defined inform interval.

Figure 141. A sample connectivity report



Generate a historical connectivity report to view the connection statuses of managed devices in different device views.

Historical Connectivity

Report Options

Device View: All Standalone APs

Report Type: Connected

Display Period: 1 hour

Filters

Filter Rows where: Device Name | Exactly equals

Report Results

Report Type: Historical Connectivity > All Standalone APs > Connected

Device Name	Serial Number	MAC Address	IP Address	IPv6 Address	Model Name	Device Last Seen	Uptime	Tag	Software	Connection
RuckusAP	431202001913	8C:0C:90:1B:08:80	192.168.22.123	2222:3333:aaaa:2222:8e0c:90ff:fe1b:b80	ZF7055	Feb. 21 2013 16:21:49	12h 16m		9.6.0.0.75	✓

Report Name:

☐ Include Filters ☐ Include Table Header Settings ☐ Schedule Report

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Generating a Client Association Report

A client association report identifies the clients that are currently associated with managed APs and the managed APs that are currently reporting to managed ZoneDirector devices.

1. Go to *Reports* > *Report Categories* > *Client Association.*
2. In *Device View*, select the device view for which you want to generate a report. Default device views include:
   - **All Standalone APs**
   - **All ZoneDirectors**

   When there are custom device views, they also appear in the list of options.

NOTE: If you selected 2-tier management mode, then ZoneDirector options are not visible on the page and ZoneDirector information are not included in the report that you are generating.

3. If you selected **All ZoneDirectors**, then continue with Step 4. If you selected **All Standalone APs**, then continue with Step 5.
4. If you selected **All ZoneDirectors**, then select one of the following options in *Report Type:*
   - *ZoneDirectors:* Shows all monitored ZoneDirectors.
   - *Connected ZoneDirectors:* Shows all currently-connected ZoneDirectors.
   - *Disconnected ZoneDirectors:* Shows all currently-disconnected ZoneDirectors.
   - *All Access Points:* Shows all ZoneDirector-managed APs.
   - *Connected Access Points:* Shows all currently-connected ZoneDirector-managed APs.
   - *Disconnected Access Points:* Shows all currently-disconnected ZoneDirector-managed APs.
   - *Connected Clients:* Shows all currently-connected ZoneDirector-managed clients.
   - *Mesh Report:* Shows all currently-connected ZoneDirector-managed meshes. To view the mesh tree for a particular ZoneDirector device, click the View Mesh link (in the *Details* column) that is in the same row as the ZoneDirector name. After you generate the mesh report, you can export the mesh tree information as a Microsoft Excel file by clicking the **Save This Report as XLS** link above the table.
   - *AP with no user connectivity:* Shows all currently-connected ZoneDirector-managed APs with no clients.
   - *Diagnostic:* Shows the connection status, uptime information, uplink and downlink RSSI, hop, # of downlinks, and distance (among others) for each ZoneDirector device in the selected view.
   - *Rogue APs:* Shows information for all currently-detected rogue APs.

   Continue with Step 6.
5. If you selected **All Standalone APs**, then select one of the following options in *Report Type:*
   - *APs:* Shows all directly-managed APs.

- *Currently Connected:* Shows all directly-managed APs that communicated with FlexMaster at the last inform interval.
- *Seen in Last 24 hours:* Shows all directly-managed APs that communicated with FlexMaster some time in the last 24 hours.
- *Seen in Last 48 hours:* Shows all directly-managed APs that communicated with FlexMaster some time in the last 48 hours.
- *Currently Disconnected:* Shows all directly-managed APs that did not communicate with FlexMaster at the last inform interval.
- *Connected Clients:* Shows the clients associated with the all currently-connected directly-managed APs.
- *Bridge APs:* Shows all directly-managed bridge APs.

Continue with Step 6.

6. If you selected:

- *Device View: All ZoneDirectors* and *Report Type: All Access Points*, or *Connected Access Points*, or *Disconnected Access Points*, also select:
  - *AP Type: APs, Root APs, Mesh APs*, or *eMesh APs*, and
  - *Period (for the report):* between *1 hour* and *24 hours*, or *Greater than 24 hours*.
- *Device View: All ZoneDirectors* and *Report Type: AP with no user connectivity*, also select:
  - *Period (for the report):* between *1 hour* and *24 hours*, or *Greater than 24 hours*.

7. (Optional) If you want to add a search filter to your query, then configure the options in the *Filters* section.

a. In the first drop-down list box after *Filter Rows where,* select the search attribute that you want to use. Options include name, serial number, IP address, external IP address, model, last seen, and others.

b. In the second drop-down list box, select the search operator that you want to use. Available search operators include:

- *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered `172.17.16.176` as the search parameter, then only devices with this IP address appear in the search results.
- *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered `100` as the search parameter, then all devices with "100" in the IP address (for example, `172.17.16.`**`100`** and **`100`**`.1.10.13`) appear in the search results.
- *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered `3908` as the query parameter, then only devices with serial numbers that begin with "3908" (for example, `390801005202`) appear in the search results.
- *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected **IP address** as the attribute and you entered `13` as the query parameter, then only devices with model names that end in "13" (for example, `100.1.10.`**`13`**) appear in the search results.

c. In the third text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.

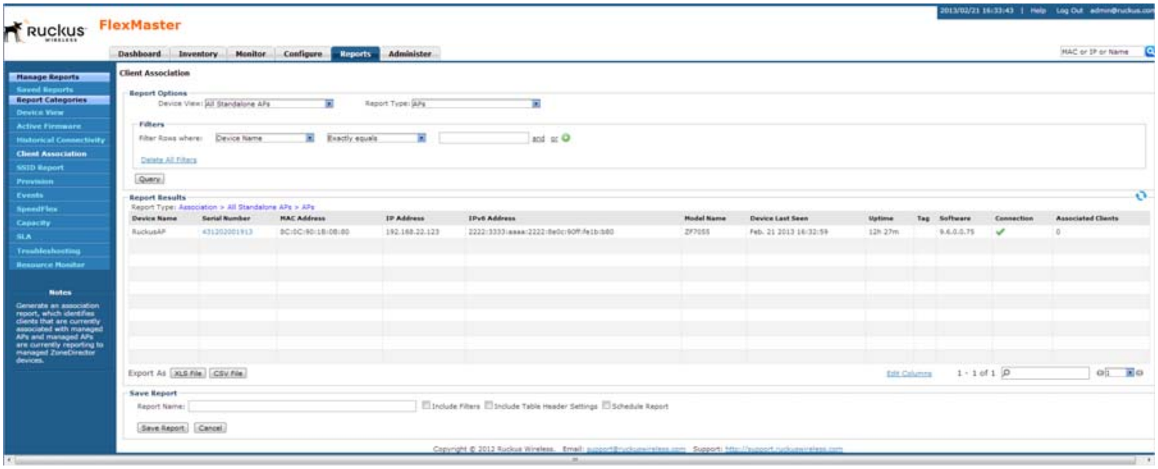
d. If you want to add another search filter, then click ⊕. A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.

8. Click **Query**. FlexMaster refreshes the page and displays the report that you selected.

NOTE: In any of the reports, clicking an Client *MAC Address* hyperlink causes FlexMaster to display

NOTE: FlexMaster provides options for filtering the devices that are included in the report. Options for saving the generated report, automating report generation, and saving the report as an Excel file are also available. For more information, refer to Using Advanced Report Options.

Figure 142. A sample client association report



Notes

Generate an association report, which identifies clients that are currently associated with managed APs and managed APs are currently reporting to managed ZoneDirector devices.

Client Association

Report Options

Device View: All Standalone APs   Report Type: APs

Filters

Filter Rows where: Device Name   Exactly equals   and or

Report Results

Report Type: Association > All Standalone APs > APs

Device Name	Serial Number	MAC Address	IP Address	IPv6 Address	Model Name	Device Last Seen	Uptime	Tag	Software	Connection	Associated Clients
RuckusAP	431202001913	8C:0C:90:18:08:80	192.168.22.123	2222:3333:aaaa:2222:8e0c:90ff:fe1b:b80	ZF7055	Feb. 21 2013 16:32:59	12h 27m		9.6.0.0.75	✓	0

1 - 1 of 1

Save Report

Report Name: □ Include Filters □ Include Table Header Settings □ Schedule Report

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Generating an SSID Report

An SSID report displays the number of ZoneDirector devices and APs on which a particular SSID is configured. You can also view graphs of associated clients, received traffic, and transmitted traffic per SSID.

1. Go to *Reports* > *Report Categories* > *SSID Report.*

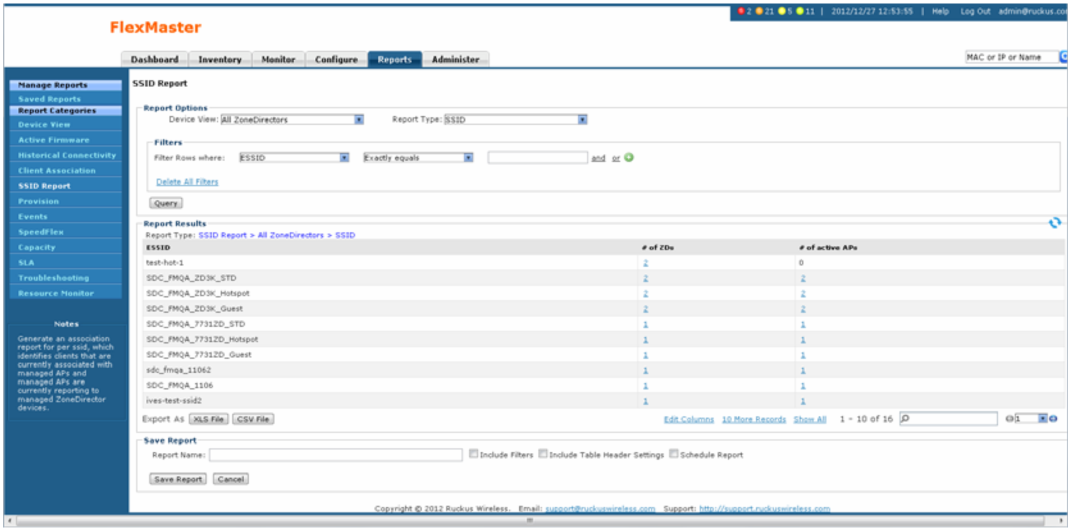
2. In *Device View*, select the device view for which you want to generate a report. The default device view is: All ZoneDirectors.

When there are custom device views, they also appear in the list of options.

NOTE: If you selected 2-tier management mode, then ZoneDirector options are not visible on the page and ZoneDirector information is not included in the report that you are generating.

3. In *Report Type*, configure the type of report that you want to view. The available report options depend on the device view that you selected in the previous step.
   - *SSID*: Shows the number of APs that are configured to use a particular SSID and the number of ZoneDirector devices that are managing these APs.
   - *Top Bar-Graph:* Can show the # of Associated Clients, Traffic-Tx or Traffic-Rx.
   - *Time Line Graph:* Can show the # of Associated Clients, Traffic-Tx+Rx or Traffic-Rx.
4. (Optional) If you selected **SSID** as the report type and you want to add a search filter to your query, then configure the options in the *Filters* section.
   - **a.** In the first drop-down list box after *Filter Rows where,* verify that **ESSID** is selected.
   - **b.** In the second drop-down list box, select the search operator that you want to use. Available search operators include:
     - *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered.
     - *Contains*: Search for devices with attributes that include the query parameter you entered.
     - *Starts with*: Search for devices with attributes that start with the query parameter you entered.
     - *Ends with*: Search for devices with attributes that end with the query parameter you entered.
   - **c.** In the third text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
   - **d.** If you want to add another search filter, then click ⊕. A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.
5. Click **Query**. If you selected report type that generates a graph, then click **Generate Graph**. The page refreshes, and then displays the SSID report that you queried or graph that you generated.

Figure 143. A sample SSID report



SSID Report

Report Options
Device View: All ZoneDirectors
Report Type: SSID

Filters
Filter Rows where: ESSID | Exactly equals

Report Results
Report Type: SSID Report > All ZoneDirectors > SSID

ESSID	# of ZDs	# of active APs
test-hot-1	2	0
SDC_FMQA_ZD3K_STD	2	2
SDC_FMQA_ZD3K_Hotspot	2	2
SDC_FMQA_ZD3K_Guest	2	2
SDC_FMQA_7731ZD_STD	1	1
SDC_FMQA_7731ZD_Hotspot	1	1
SDC_FMQA_7731ZD_Guest	1	1
sdc_fmqa_11062	1	1
SDC_FMQA_1106	1	1
ives-test-ssid2	1	1

Export As
1 - 10 of 16

Save Report
Report Name: ☐ Include Filters ☐ Include Table Header Settings ☐ Schedule Report

Notes
Generate an association report for per ssid, which identifies clients that are currently associated with managed APs and managed APs are currently reporting to managed ZoneDirector devices.

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Generating a Provision Report

A provision report lists the statuses of all the tasks that you have provisioned, categorized based on the task types.

1. Go to *Reports* > *Report Categories* > *Provision*.
2. In *Task Type*, click the type of provisioning task for which you want to generate a report. Available options include:
   - *Configuration Upgrade*
   - *Factory Reset*
   - *Firmware Upgrade*
   - *Reboot*
   - *ZD Restore*
   - *ZD Configuration*
3. (Optional) If you want to add a search filter to your query, then configure the options in the *Filters* section.
   a. In the first drop-down list box after *Filter Rows where,* select the search attribute that you want to use. Options include Task Name, Schedule, Created (on), and Created by.
   b. In the second drop-down list box, select the search operator that you want to use. Available search operators include:
      – *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered.
      – *Contains*: Search for devices with attributes that include the query parameter you entered.

- *Starts with*: Search for devices with attributes that start with the query parameter you entered.
- *Ends with*: Search for devices with attributes that end with the query parameter you entered.

c. In the third text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.

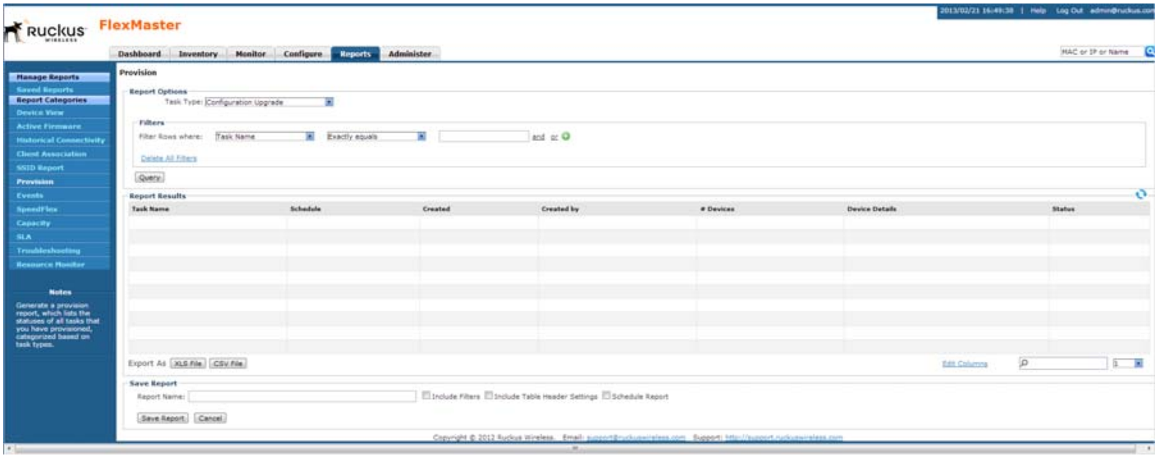
d. If you want to add another search filter, then click ⊕. A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.

4. Click **Query**.

The page refreshes, and then displays details of the provisioning task that you selected, including the number of devices on which the task succeeded and failed. To view details about the target devices, click the **Details** link in the *Device Details* column.

NOTE: FlexMaster provides options for filtering the devices that are included in the report. Options for saving the generated report, automating report generation, and saving the report as an Excel file are also available. For more information, refer to Using Advanced Report Options.

Figure 144. A sample provision report



Notes

Generate a provision report, which lists the statuses of all tasks that you have provisioned, categorized based on task types.

Provision

Report Options

Task Type: Configuration Upgrade

Filters

Filter Rows where: Task Name | Exactly equals | and or

Delete All Filters

Report Results

Task Name	Schedule	Created	Created by	# Devices	Device Details	Status

Export As

Save Report

Report Name: □ Include Filters □ Include Table Header Settings □ Schedule Report

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Generating Events-Related Reports

Events-related reports displays a list of events that match the selected event category, device category, and event type. There are four types of events-related report.

- An events report shows a summary of devices on which a particular event (for example, connectivity problem) has occurred.
- An event timeline report shows devices on which a specific event occurred (similar to an events report), but based on a configurable time period. For example, if you want to view a list of devices on which the "Connectivity problem" event occurred within the last seven days, then you can set the start time and end time ranges to cover the previous week.
- Similar to an events report, a detailed events report lists devices on which a particular event (for example, connectivity problem) has occurred, including all instances when the event occurred on each device. For example, if the "Connectivity problem" event occurred 10 times on a particular device, then the detailed events report shows details of all 10 occurrences, including the dates and times when the events occurred.
- An event plot report displays a graph version of five specific connectivity events that occurred on APs that are reporting to managed ZoneDirector devices.

NOTE: An events report does not indicate the number of times a particular event occurred on a device. If you need to know how frequently the event occurred on a device, then generate a detailed events report instead.

Follow these steps to generate an events-related report.

1. Go to *Reports* > *Report Categories* > *Events.*
2. In *Event Category*, select **Events**, **Event Timeline, Detailed Events** or **Event Plot**.
3. If you selected *Events* or *Detailed Events*, then in *Device Category* click the type of managed device for which you want to generate the report. Options include **ZoneDirectors** and **Standalone APs**.
4. If you selected *Event Timeline* or *Event Plot,* then in *Device View* click the device view for which you want to generate a report. Default device views include:
   - **All Standalone APs**
   - **All ZoneDirectors**

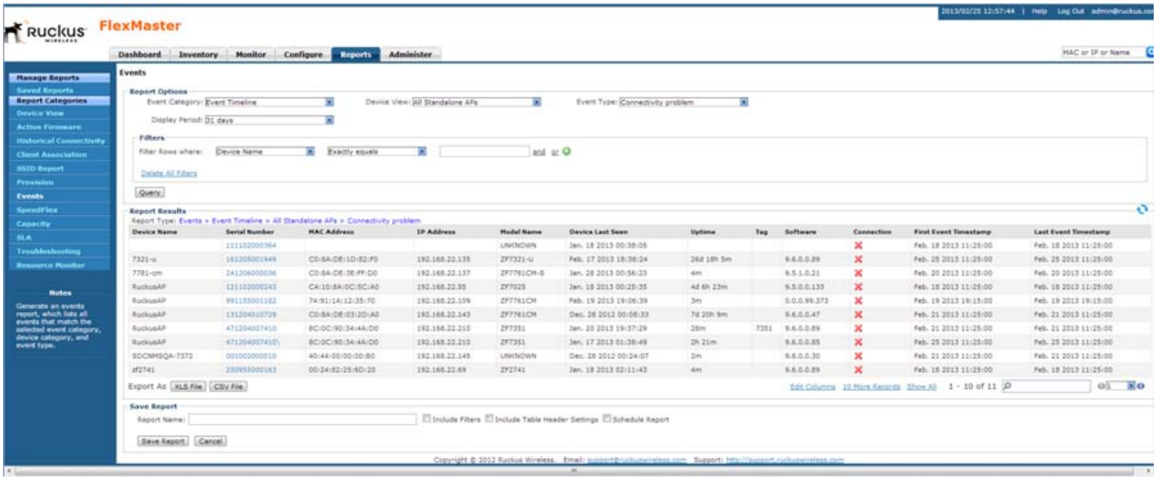
   When there are custom device views, they also appear in the list of options.
5. If you selected *Events, Event Timeline* or *Detailed Events,* then in *Event Type*, select the type of event for which you want a report.
6. If you selected *Event Timeline* or *Event Plot,* then in *Display Period*, select the period for this report.

Note that the time period covered by the report depends on the availability of events data on the FlexMaster database. If the events log has been purged recently, then the events report only displays events that occurred after the last purge. For more information, refer to Purge Policy.

NOTE: If you selected 2-tier management mode, then ZoneDirector options are not visible on the page and ZoneDirector information is not included in the report that you are generating.

7. (Optional) If you want to add a search filter to your query, then configure the options in the *Filters* section.
   - **a.** In the first drop-down list box after *Filter Rows where,* select the search attribute that you want to use. Options include name, serial number, IP address, external IP address, model, and last seen (among others).
   - **b.** In the second drop-down list box, select the search operator that you want to use. Available search operators include:
     - *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered `172.17.16.176` as the search parameter, then only devices with this IP address appear in the search results.
     - *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered `100` as the search parameter, then all devices with "100" in the IP address (for example, `172.17.16.`**`100`** and **`100`**`.1.10.13`) appear in the search results.
     - *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered `3908` as the query parameter, then only devices with serial numbers that begin with "3908" (for example, `390801005202`) appear in the search results.
     - *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected **IP address** as the attribute and you entered `13` as the query parameter, then only devices with model names that end in "13" (for example, `100.1.10.`**`13`**) appear in the search results.
   - **c.** In the third text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
   - **d.** If you want to add another search filter, then click ⊕. A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.
8. If you selected *Events, Event Timeline* or *Detailed Events,* then click **Query**.

Figure 145. A sample events report



Notes

Generate an events report, which lists all events that match the selected event category, device category, and event type.

Events

Report Options

Event Category: Event Timeline
Device View: All Standalone APs
Event Type: Connectivity problem
Display Period: 31 days

Filters

Filter Rows where: Device Name | Exactly equals | and or

Report Results

Report Type: Events > Event Timeline > All Standalone APs > Connectivity problem

Device Name	Serial Number	MAC Address	IP Address	Model Name	Device Last Seen	Uptime	Tag	Software	Connection	First Event Timestamp	Last Event Timestamp
	111102000364			UNKNOWN	Jan. 18 2013 00:38:05				✗	Feb. 18 2013 11:25:00	Feb. 18 2013 11:25:00
7321-u	161205001949	C0:8A:DE:1D:82:F0	192.168.22.135	ZF7321-U	Feb. 17 2013 18:38:24	26d 18h 5m		9.6.0.0.89	✗	Feb. 25 2013 11:25:00	Feb. 25 2013 11:25:00
7781-cm	241206000036	C0:8A:DE:3E:FF:D0	192.168.22.137	ZF7781CM-S	Jan. 28 2013 00:56:23	4m		9.5.1.0.21	✗	Feb. 20 2013 11:25:00	Feb. 20 2013 11:25:00
RuckusAP	121102000243	C4:10:8A:0C:5C:A0	192.168.22.55	ZF7025	Jan. 18 2013 00:25:35	4d 6h 23m		9.5.0.0.133	✗	Feb. 18 2013 11:25:00	Feb. 18 2013 11:25:00
RuckusAP	991155001182	74:91:1A:12:35:70	192.168.22.109	ZF7761CM	Feb. 19 2013 19:06:39	3m		0.0.0.99.373	✗	Feb. 19 2013 19:15:00	Feb. 19 2013 19:15:00
RuckusAP	131204010729	C0:8A:DE:03:2D:A0	192.168.22.143	ZF7761CM	Dec. 28 2012 00:08:33	7d 20h 9m		9.6.0.0.47	✗	Feb. 21 2013 11:25:00	Feb. 21 2013 11:25:00
RuckusAP	471204007410	8C:0C:90:34:4A:D0	192.168.22.210	ZF7351	Jan. 20 2013 19:37:29	28m	7351	9.6.0.0.89	✗	Feb. 21 2013 11:25:00	Feb. 21 2013 11:25:00
RuckusAP	471204007410\	8C:0C:90:34:4A:D0	192.168.22.210	ZF7351	Jan. 17 2013 01:38:49	2h 21m		9.6.0.0.85	✗	Feb. 25 2013 11:25:00	Feb. 25 2013 11:25:00
SDCNMSQA-7372	001002000010	40:44:00:00:00:80	192.168.22.145	UNKNOWN	Dec. 28 2012 00:24:07	2m		9.6.0.0.30	✗	Feb. 21 2013 11:25:00	Feb. 21 2013 11:25:00
zf2741	250955000163	00:24:82:25:6D:20	192.168.22.69	ZF2741	Jan. 18 2013 02:11:43	4m		9.6.0.0.89	✗	Feb. 18 2013 11:25:00	Feb. 18 2013 11:25:00

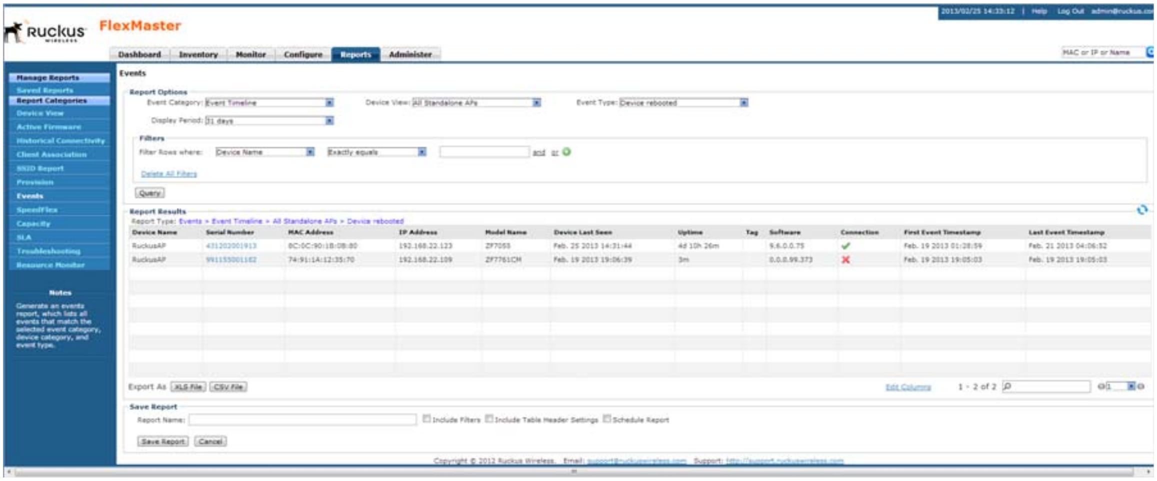
1 - 10 of 11

Save Report

Report Name: ☐ Include Filters ☐ Include Table Header Settings ☐ Schedule Report

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Figure 146. A sample event timeline report



Notes

Generate an events report, which lists all events that match the selected event category, device category, and event type.

Events

Report Options

Event Category: Event Timeline
Device View: All Standalone APs
Event Type: Device rebooted
Display Period: 31 days

Filters

Filter Rows where: Device Name | Exactly equals | and or

Report Results

Report Type: Events > Event Timeline > All Standalone APs > Device rebooted

Device Name	Serial Number	MAC Address	IP Address	Model Name	Device Last Seen	Uptime	Tag	Software	Connection	First Event Timestamp	Last Event Timestamp
RuckusAP	431202001913	8C:0C:90:1B:08:80	192.168.22.123	ZF7055	Feb. 25 2013 14:31:44	4d 10h 26m		9.6.0.0.75	✓	Feb. 19 2013 01:28:59	Feb. 21 2013 04:06:32
RuckusAP	991155001182	74:91:1A:12:35:70	192.168.22.109	ZF7761CM	Feb. 19 2013 19:06:39	3m		0.0.0.99.373	✗	Feb. 19 2013 19:05:03	Feb. 19 2013 19:05:03

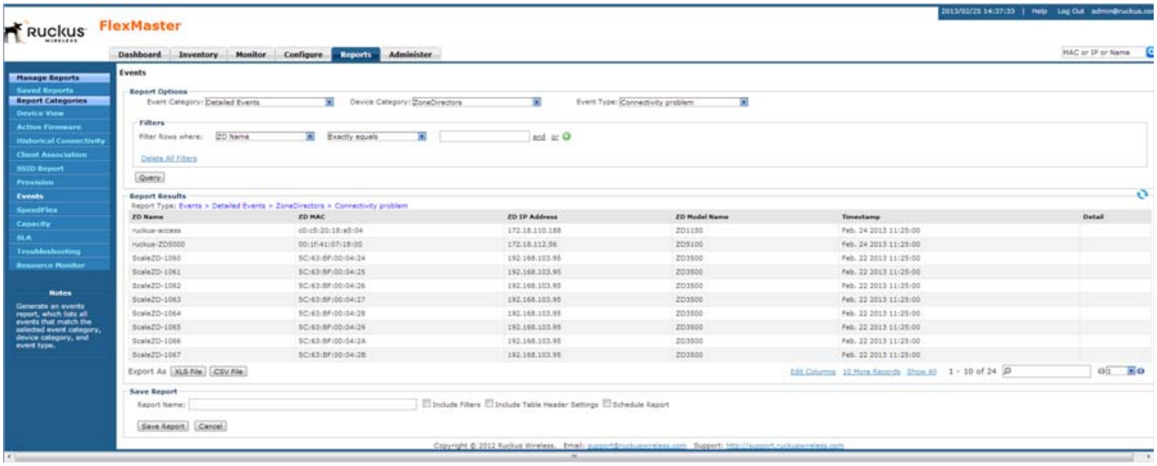
1 - 2 of 2

Save Report

Report Name: ☐ Include Filters ☐ Include Table Header Settings ☐ Schedule Report

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Figure 147. A sample detailed events report



Notes

Generate an events report, which lists all events that match the selected event category, device category, and event type.

Events

Report Options

Event Category: Detailed Events   Device Category: ZoneDirectors   Event Type: Connectivity problem

Filters

Filter Rows where: ZD Name   Exactly equals   and or

Delete All Filters

Report Results

Report Type: Events > Detailed Events > ZoneDirectors > Connectivity problem

ZD Name	ZD MAC	ZD IP Address	ZD Model Name	Timestamp	Detail
ruckus-access	c0:c5:20:18:a5:04	172.18.110.188	ZD1150	Feb. 24 2013 11:25:00	
ruckus-ZD5000	00:1f:41:07:18:00	172.18.112.56	ZD5100	Feb. 24 2013 11:25:00	
ScaleZD-1060	5C:63:BF:00:04:24	192.168.103.95	ZD3500	Feb. 22 2013 11:25:00	
ScaleZD-1061	5C:63:BF:00:04:25	192.168.103.95	ZD3500	Feb. 22 2013 11:25:00	
ScaleZD-1062	5C:63:BF:00:04:26	192.168.103.95	ZD3500	Feb. 22 2013 11:25:00	
ScaleZD-1063	5C:63:BF:00:04:27	192.168.103.95	ZD3500	Feb. 22 2013 11:25:00	
ScaleZD-1064	5C:63:BF:00:04:28	192.168.103.95	ZD3500	Feb. 22 2013 11:25:00	
ScaleZD-1065	5C:63:BF:00:04:29	192.168.103.95	ZD3500	Feb. 22 2013 11:25:00	
ScaleZD-1066	5C:63:BF:00:04:2A	192.168.103.95	ZD3500	Feb. 22 2013 11:25:00	
ScaleZD-1067	5C:63:BF:00:04:2B	192.168.103.95	ZD3500	Feb. 22 2013 11:25:00	

Export As   1 - 10 of 24

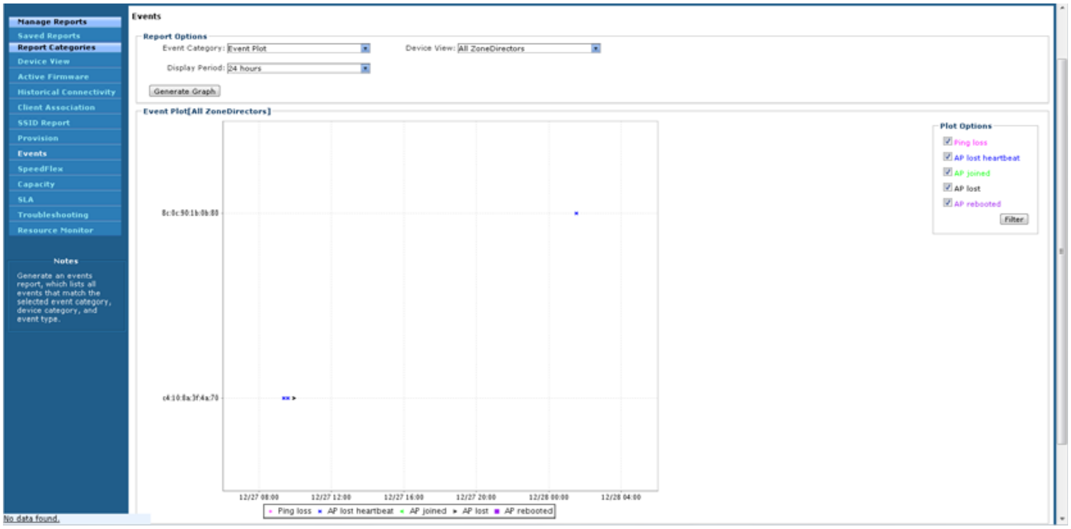
Save Report

Report Name: □ Include Filters □ Include Table Header Settings □ Schedule Report

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

9. If you selected *Event Plot*, then click **Generate Graph**.

Figure 148. A sample event plot report



Notes

Generate an events report, which lists all events that match the selected event category, device category, and event type.

Events

Report Options

Event Category: Event Plot   Device View: All ZoneDirectors

Display Period: 24 hours

Event Plot[All ZoneDirectors]

Plot Options

☑ Ping loss
☑ AP lost heartbeat
☑ AP joined
☑ AP lost
☑ AP rebooted

The page refreshes, and then displays your report.

If you generated an event plot report, then the five types of events that are plotted on the graph include:

- *Ping loss*
- *AP lost heartbeat*

- *AP joined*
- *AP lost*
- *AP rebooted*

To hide an event from the graph, go to the *Plot Options* section, clear the check box before the event name, and then click *Filter*.

NOTE: FlexMaster provides options for filtering the devices that are included in the report. Options for saving the generated report, automating report generation, and saving the report as an Excel or .CSV file are also available. For more information, refer to Using Advanced Report Options.

Generating a SpeedFlex Report

Generate a SpeedFlex report to view completed throughput test results based on the test name, source or destination IP address, date executed, user, and so on.

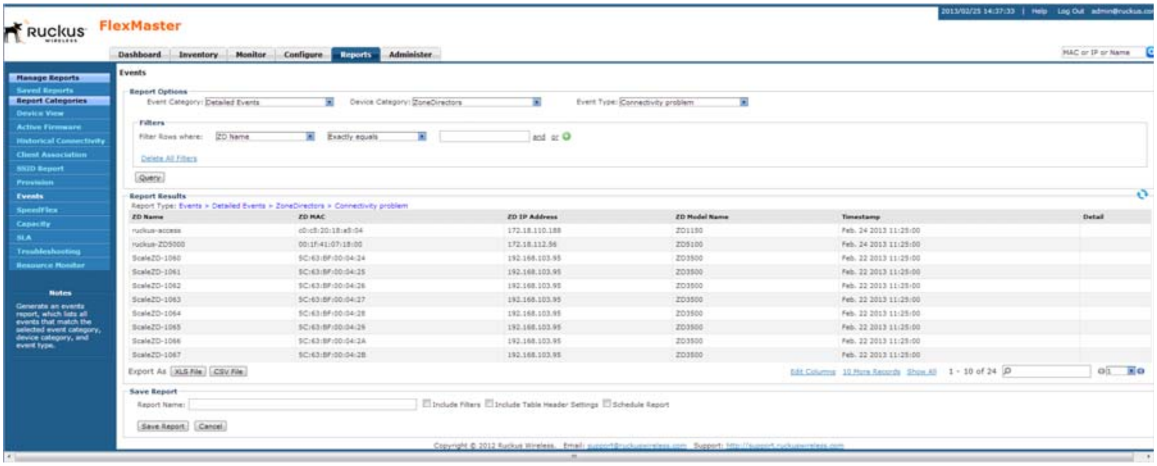
1. Go to *Reports* > *Report Categories* > *SpeedFlex*.
2. Go to the *Filters* section in *Report Options*.
3. To search for previously run SpeedFlex tests to include in the SpeedFlex report, specify the criteria of the SpeedFlex tests that you are looking for.

NOTE: If you want to display *all* SpeedFlex tests that have been run, then skip the *Filters* section (steps 4 to 8), and simply click the **Query** button.

4. In the first drop-down list box after *Filter Rows where*, select the search attribute that you want to use. Options include test name, source or destination IP address, mesh test, execute time, and finish time (among others).
5. In the second drop-down list box, select the search operator that you want to use. Available search operators include:
   - *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **Src.IP** as the attribute and you entered `172.17.16.176` as the search parameter, then only devices with this IP address appear in the search results.
   - *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **Src.IP** as the attribute and you entered `100` as the search parameter, then all devices with "100" in the IP address (for example, `172.17.16.`**`100`** and **`100`**`.1.10.13`) appear in the search results.
   - *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Test Name** as the attribute and you entered `3908` as the query parameter, then only tests that begin with "3908" (for example, `390801005202`) appear in the search results.
   - *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected **Dest.IP** as the attribute and you entered `13` as the query parameter, then only devices with model names that end in "13" (for example, `100.1.10.`**`13`**) appear in the search results.
6. In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
7. If you want to add another search filter, then click ⊕. A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.
8. Click **Query**.

The page refreshes, and then displays all the SpeedFlex tests that match the filter criteria that you specified. If you did not specify any filter criteria, then FlexMaster displays all SpeedFlex tests that have been run and stored on the FlexMaster database.

Figure 149. A sample SpeedFlex report



Notes
Generate an events report, which lists all events that match the selected event category, device category, and event type.

Events

Report Options
Event Category: Detailed Events
Device Category: ZoneDirectors
Event Type: Connectivity problem

Filters
Filter Rows where: ZD Name Exactly equals and or
Delete All Filters

Report Results
Report Type: Events > Detailed Events > ZoneDirectors > Connectivity problem

ZD Name	ZD MAC	ZD IP Address	ZD Model Name	Timestamp	Detail
ruckus-access	c0:c5:20:18:a5:04	172.18.110.188	ZD1150	Feb. 24 2013 11:25:00	
ruckus-ZD5000	00:1f:41:07:18:00	172.18.112.56	ZD5100	Feb. 24 2013 11:25:00	
ScaleZD-1060	5C:63:BF:00:04:24	192.168.103.95	ZD3500	Feb. 22 2013 11:25:00	
ScaleZD-1061	5C:63:BF:00:04:25	192.168.103.95	ZD3500	Feb. 22 2013 11:25:00	
ScaleZD-1062	5C:63:BF:00:04:26	192.168.103.95	ZD3500	Feb. 22 2013 11:25:00	
ScaleZD-1063	5C:63:BF:00:04:27	192.168.103.95	ZD3500	Feb. 22 2013 11:25:00	
ScaleZD-1064	5C:63:BF:00:04:28	192.168.103.95	ZD3500	Feb. 22 2013 11:25:00	
ScaleZD-1065	5C:63:BF:00:04:29	192.168.103.95	ZD3500	Feb. 22 2013 11:25:00	
ScaleZD-1066	5C:63:BF:00:04:2A	192.168.103.95	ZD3500	Feb. 22 2013 11:25:00	
ScaleZD-1067	5C:63:BF:00:04:2B	192.168.103.95	ZD3500	Feb. 22 2013 11:25:00	

Export As
1 - 10 of 24

Save Report
Report Name: □ Include Filters □ Include Table Header Settings □ Schedule Report

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Generating a Capacity Report

Generate various graphs that display device capacity data based on throughput, associated clients, airtime utilization, and traffic, among others.

1. Go to *Reports* > *Report Categories* > *Capacity.*
2. In *Device View*, select the device view for which you want to generate a report. Default device views include:
   - **All Standalone APs**
   - **All ZoneDirectors**

   When there are custom device views, they also appear in the list of options.

NOTE: If you selected 2-tier management mode, then ZoneDirector options are not visible on the page and ZoneDirector information is not included in the report that you are generating.

3. In *Report Type*, select the type of report that you want to generate. The options that appear depend on the device view that you selected in the previous step.

   If you selected a device view consisting of ZoneDirector devices, then the following report type options appear:
   - *# of Associated Clients*
   - *Air-Time Utilization*

- *AP Actual Throughput*
- *AP Traffic*
- *Client Actual Throughput*
- *Client Traffic*

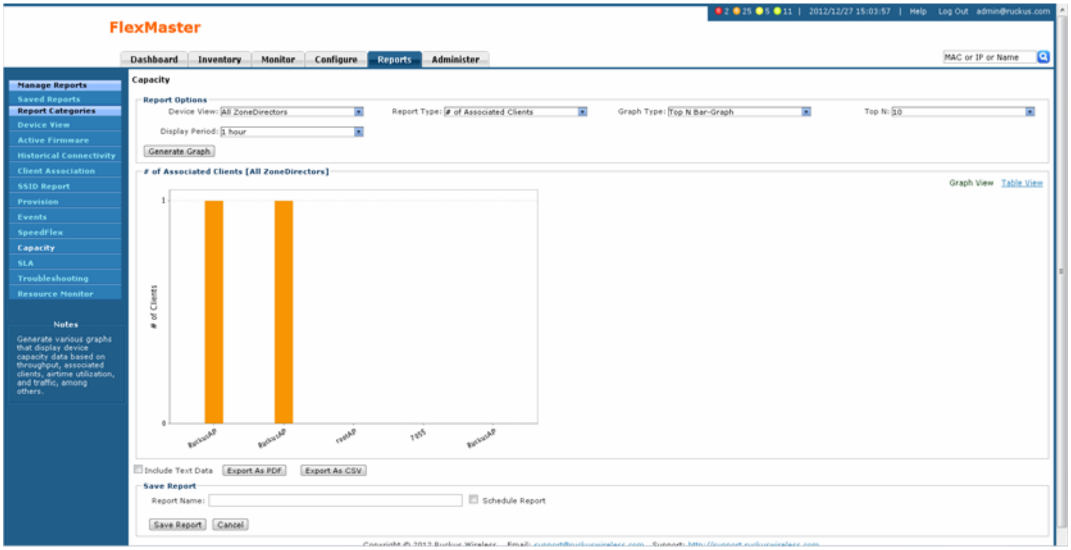
If you selected a device view consisting of Standalone APs, then *Backhaul Throughput* is the only report type option that appears.

4. In *Graph Type*, select the type of graph to use in the report. Options include:
    - *Top N Bar-Graph*: Displays the top *N* devices for the selected report type. *N* is the number of devices to show in the report. The default value is 10. To change this value, select a new value from the *Top N* drop-down list.
    - *Bottom N Bar-Graph*: Displays the bottom *N* devices for the selected report type. *N* is the number of devices to show in the report. The default value is 10. To change this value, select a new value from the *Bottom N* drop-down list.
    - *Histogram*: Displays the density of managed devices against a specific variable (report type).
5. In *Display Period*, select the time period for which you want to generate the report. Options range from 1 hour to 31 days.
6. Click **Generate Graph**.

The page refreshes, and then the graph appears below the *Report Options* section. The *Sampling Info* section in the upper-right corner of the graph displays the report settings that you configured and the number of samples that were included in the report.

To view the report in a tabular format, click the **Table View** link above the *Sampling Info* section. To save a PDF version of the report, click **Export As PDF**, and then save the PDF file to your local computer when the browser prompt appears. To save a comma-separated variables version of the report, click **Export As CSV**, and then save the csv file to your local computer when the browser prompt appears.

Figure 150. A sample capacity report



Generate various graphs that display device capacity data based on throughput, associated clients, airtime utilization, and traffic, among others.

Capacity

Report Options

Device View: All ZoneDirectors

Report Type: # of Associated Clients

Graph Type: Top N Bar-Graph

Top N: 10

Display Period: 1 hour

Generating an SLA Report

Generate various graphs that display service-level agreement (SLA) related information, including uptime, downtime, and potential throughput.

1. Go to *Reports > Report Categories > SLA*.
2. In *Device View*, select the device view for which you want to generate a report. Default device views include:
   - **All Standalone APs**
   - **All ZoneDirectors**

   When there are custom device views, they also appear in the list of options.

NOTE: If you selected 2-tier management mode, then ZoneDirector options are not visible on the page and ZoneDirector information is not included in the report that you are generating.

3. In *Report Type*, select the type of report that you want to generate. The options that appear depend on the device view that you selected in the previous step.

   If you selected a device view consisting of ZoneDirector devices, then the following report type options appear:
   - *AP Downtime*
   - *AP Uptime*
   - *Client Potential Throughput*

- *Client Associated Time*

If you selected a device view consisting of Standalone APs, then the following report type options appear:

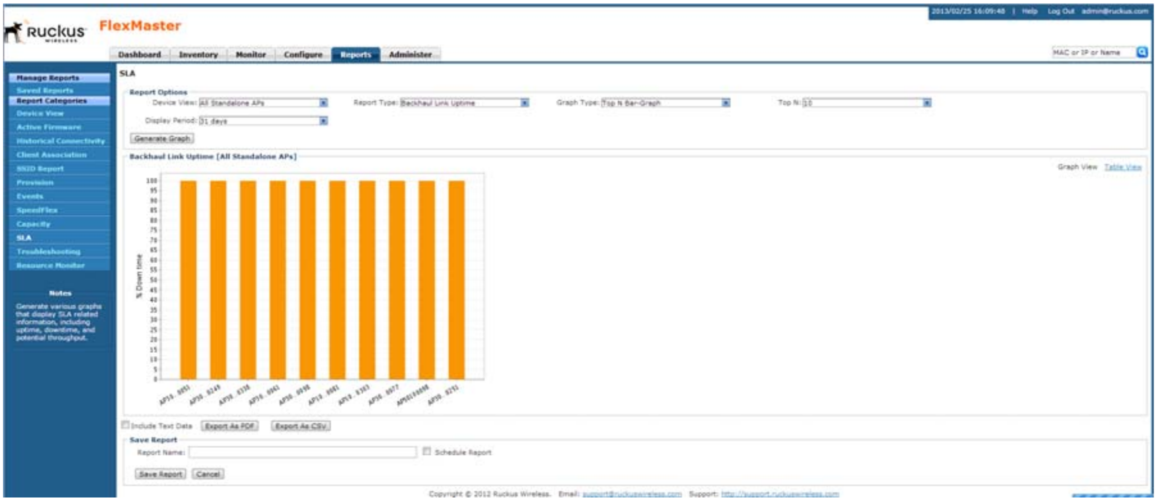
- *AP Downtime*
- *AP Uptime*
- *Backhaul Link Uptime*

4. In *Graph Type*, select the type of graph to use in the report. Options include:
   - *Top N Bar-Graph*: Displays the top *N* devices for the selected report type. *N* is the number of devices to show in the report. The default value is 10. To change this value, select a new value from the *Top N* drop-down list.
   - *Bottom N Bar-Graph*: Displays the bottom *N* devices for the selected report type. *N* is the number of devices to show in the report. The default value is 10. To change this value, select a new value from the *Bottom N* drop-down list.
   - *Histogram*: Displays the density of managed devices against a specific variable (report type).
5. In *Display Period*, select the time period for which you want to generate the report. Options range from 1 hour to 31 days.
6. Click **Generate Graph**.

The page refreshes, and then the graph appears below the *Report Options* section. The *Sampling Info* section in the upper-right corner of the graph displays the report settings that you configured and the number of samples that were included in the report.

To view the report in a tabular format, click the **Table View** link above the *Sampling Info* section.

Figure 151. A sample SLA report



SLA

Report Options

Device View: All Standalone APs

Report Type: Backhaul Link Uptime

Graph Type: Top N Bar-Graph

Top N: 10

Display Period: 31 days

Backhaul Link Uptime [All Standalone APs]

Save Report

Report Name:

Notes

Generate various graphs that display SLA related information, including uptime, downtime, and potential throughput.

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Generating a Troubleshooting Report

Generate various graphs that are useful for troubleshooting.

1. Go to *Reports* > *Report Categories* > *Troubleshooting.*
2. In *Device View*, select the device view for which you want to generate a report. Default device views include:
   - **All Standalone APs**
   - **All ZoneDirectors**

   When there are custom device views, they also appear in the list of options.

NOTE: If you selected 2-tier management mode, then ZoneDirector options are not visible on the page and ZoneDirector information is not included in the report that you are generating.

3. In *Report Type*, select the type of report that you want to generate. The options that appear depend on the device view that you selected in the previous step.

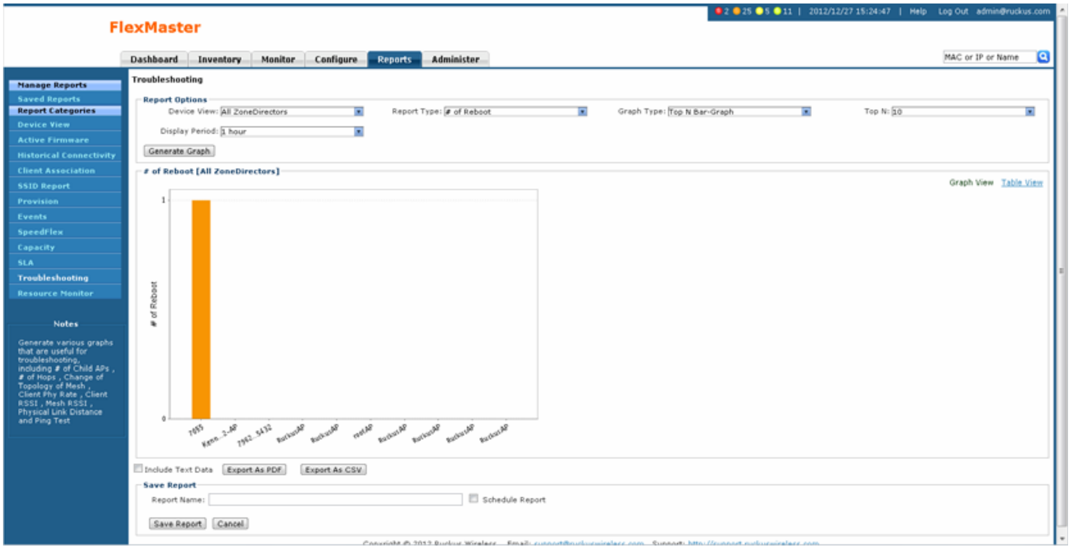
   If you selected a device view consisting of ZoneDirector devices, then the following report type options appear:
   - *# of Child APs*
   - *# of Hops*
   - *Change of Topology of Mesh*
   - *Client Phy Rate*
   - *Client RSSI*
   - *Mesh RSSI*
   - *# of Reboot*
   - *Physical Link Distance*
   - *Ping Test*

   If you selected a device view consisting of Standalone APs, then *Backhaul Change of State* is the only report type option that appears.
4. In *Graph Type*, select the type of graph to use in the report. Options include:
   - *Top N Bar-Graph*: Displays the top *N* devices for the selected report type. *N* is the number of devices to show in the report. The default value is 10. To change this value, select a new value from the *Top N* drop-down list.
   - *Bottom N Bar-Graph*: Displays the bottom *N* devices for the selected report type. *N* is the number of devices to show in the report. The default value is 10. To change this value, select a new value from the *Bottom N* drop-down list.
   - *Histogram*: Displays the density of managed devices against a specific variable (report type).
5. In *Display Period*, select the time period for which you want to generate the report. Options range from 1 hour to 31 days.
6. Click **Generate Graph**.

The page refreshes, and then the graph appears below the *Report Options* section. The *Sampling Info* section in the upper-right corner of the graph displays the report settings that you configured and the number of samples that were included in the report.

To view the report in a tabular format, click the **Table View** link above the *Sampling Info* section.

Figure 152. A sample troubleshooting report



Troubleshooting

Report Options

Device View: All ZoneDirectors
Report Type: # of Reboot
Graph Type: Top N Bar-Graph
Top N: 10
Display Period: 1 hour

# of Reboot [All ZoneDirectors]

☐ Include Text Data

Save Report

Report Name:
☐ Schedule Report

Notes

Generate various graphs that are useful for troubleshooting, including # of Child APs , # of Hops , Change of Topology of Mesh , Client Phy Rate , Client RSSI , Mesh RSSI , Physical Link Distance and Ping Test

Generating a Resource Monitor Report

Generate a resource monitor report to view CPU, memory, and disk usage on managed ZoneDirector devices.

1. Go to *Reports > Report Categories > Resource Monitor.*
2. Go to the *Report Options* section.

   The *Report Type* parameter has only one selection (**CPU/Mem/Disk Usage**), which cannot be changed.
3. In *Device View*, select the device view for which you want to generate a report. The default device view is:
   - **All ZoneDirectors**

   When there are custom ZoneDirector device views, they also appear in the list of options.
4. (Optional) If you want to add a search filter to your query, then configure the options in the *Filters* section.

a. In the first drop-down list box after *Filter Rows where,* select the search attribute that you want to use. Options include ZoneDirector name, model, serial number, IP address, %CPU, %Mem, and %Disk (among others).

b. In the second drop-down list box, select the search operator that you want to use. Available search operators include:

- *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered `172.17.16.176` as the search parameter, then only devices with this IP address appear in the search results.
- *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered `100` as the search parameter, then all devices with "100" in the IP address (for example, `172.17.16.`**`100`** and **`100`**`.1.10.13`) appear in the search results.
- *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered `3908` as the query parameter, then only devices with serial numbers that begin with "3908" (for example, `390801005202`) appear in the search results.
- *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected **IP address** as the attribute and you entered `13` as the query parameter, then only devices with model names that end in "13" (for example, `100.1.10.`**`13`**) appear in the search results.

After you select a search operator, a third (text) box appears.

c. In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.

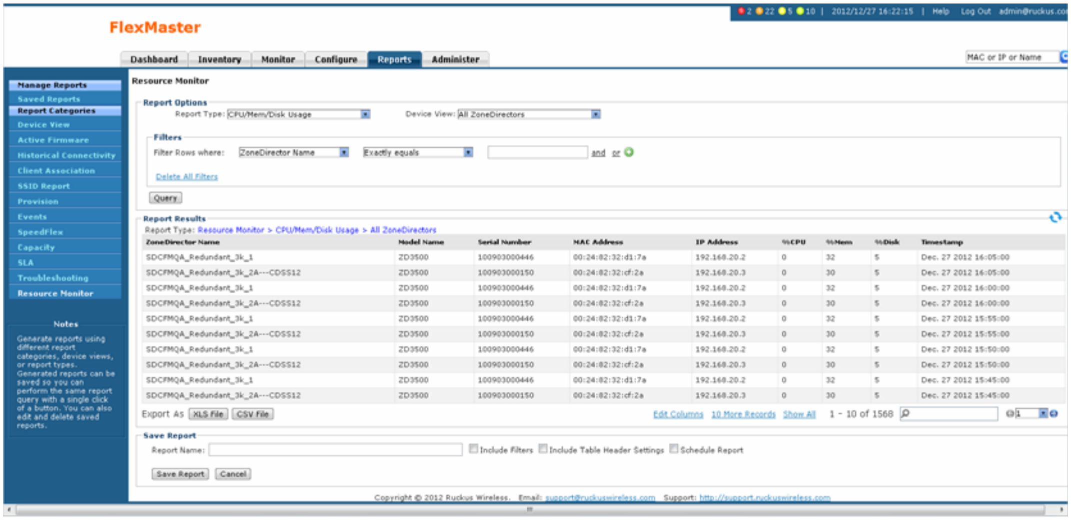
5. If you want to add another search filter, then click ⊕. A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.

6. Click **Query**.

The page refreshes, and then displays the current resource usage (CPU, memory, and disk) of all ZoneDirector devices in the selected device view.

NOTE: FlexMaster provides options for filtering the devices that are included in the report. Options for saving the generated report, automating report generation, and saving the report as an Excel file are also available. For more information, refer to Using Advanced Report Options.

Figure 153. A sample resource monitor report



Generate reports using different report categories, device views, or report types. Generated reports can be saved so you can perform the same report query with a single click of a button. You can also edit and delete saved reports.

Resource Monitor

Report Options

Report Type: CPU/Mem/Disk Usage   Device View: All ZoneDirectors

Filters

Filter Rows where: ZoneDirector Name   Exactly equals   and or

Delete All Filters

Query

Report Results

Report Type: Resource Monitor > CPU/Mem/Disk Usage > All ZoneDirectors

ZoneDirector Name	Model Name	Serial Number	MAC Address	IP Address	%CPU	%Mem	%Disk	Timestamp
SDCFMQA_Redundant_3k_1	ZD3500	100903000446	00:24:82:32:d1:7a	192.168.20.2	0	32	5	Dec. 27 2012 16:05:00
SDCFMQA_Redundant_3k_2A---CDSS12	ZD3500	100903000150	00:24:82:32:cf:2a	192.168.20.3	0	30	5	Dec. 27 2012 16:05:00
SDCFMQA_Redundant_3k_1	ZD3500	100903000446	00:24:82:32:d1:7a	192.168.20.2	0	32	5	Dec. 27 2012 16:00:00
SDCFMQA_Redundant_3k_2A---CDSS12	ZD3500	100903000150	00:24:82:32:cf:2a	192.168.20.3	0	30	5	Dec. 27 2012 16:00:00
SDCFMQA_Redundant_3k_1	ZD3500	100903000446	00:24:82:32:d1:7a	192.168.20.2	0	32	5	Dec. 27 2012 15:55:00
SDCFMQA_Redundant_3k_2A---CDSS12	ZD3500	100903000150	00:24:82:32:cf:2a	192.168.20.3	0	30	5	Dec. 27 2012 15:55:00
SDCFMQA_Redundant_3k_1	ZD3500	100903000446	00:24:82:32:d1:7a	192.168.20.2	0	32	5	Dec. 27 2012 15:50:00
SDCFMQA_Redundant_3k_2A---CDSS12	ZD3500	100903000150	00:24:82:32:cf:2a	192.168.20.3	0	30	5	Dec. 27 2012 15:50:00
SDCFMQA_Redundant_3k_1	ZD3500	100903000446	00:24:82:32:d1:7a	192.168.20.2	0	32	5	Dec. 27 2012 15:45:00
SDCFMQA_Redundant_3k_2A---CDSS12	ZD3500	100903000150	00:24:82:32:cf:2a	192.168.20.3	0	30	5	Dec. 27 2012 15:45:00

Export As XLS File CSV File   Edit Columns 10 More Records Show All 1 - 10 of 1568

Save Report

Report Name: □ Include Filters □ Include Table Header Settings □ Schedule Report

Save Report Cancel

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

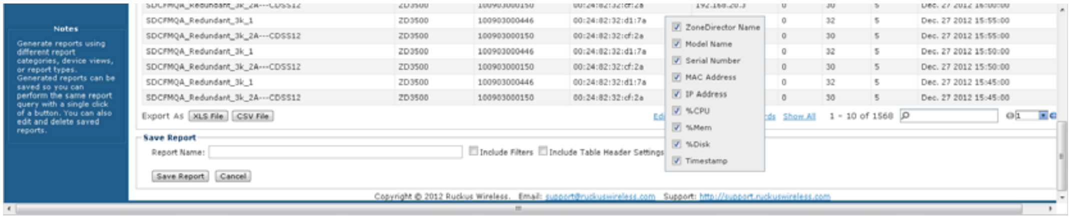
Hiding and Showing Columns in Reports

By default, all columns that are available for a particular report are displayed. When you want the report to show only specific columns, you can hide the columns that you do not want to display.

1. Right-click any of the column headings in the report that you have generated. A pop-up menu appears, displaying all the column headings that are available for that particular report.
2. Clear the check boxes for the column headings that you want to hide. As soon as you clear a check box, the corresponding column disappears from the report.
3. When you finish clearing the check boxes for the columns that you want to hide, click on any area outside the pop-up menu to close the pop-up menu.

To display columns that are currently hidden, repeat the same procedure as above. This time, however, select the check boxes for the columns that you want to display.

Figure 154. Clear the check boxes for the columns that you want to hide



Generate reports using different report categories, device views, or report types. Generated reports can be saved so you can perform the same report query with a single click of a button. You can also edit and delete saved reports.

SDCFMQA_Redundant_3k_2A---CDSS12	ZD3500	100903000150	00:24:82:32:cf:2a	192.168.20.3	0	30	5	Dec. 27 2012 16:00:00
SDCFMQA_Redundant_3k_1	ZD3500	100903000446	00:24:82:32:d1:7a		0	32	5	Dec. 27 2012 15:55:00
SDCFMQA_Redundant_3k_2A---CDSS12	ZD3500	100903000150	00:24:82:32:cf:2a		0	30	5	Dec. 27 2012 15:55:00
SDCFMQA_Redundant_3k_1	ZD3500	100903000446	00:24:82:32:d1:7a		0	32	5	Dec. 27 2012 15:50:00
SDCFMQA_Redundant_3k_2A---CDSS12	ZD3500	100903000150	00:24:82:32:cf:2a		0	30	5	Dec. 27 2012 15:50:00
SDCFMQA_Redundant_3k_1	ZD3500	100903000446	00:24:82:32:d1:7a		0	32	5	Dec. 27 2012 15:45:00
SDCFMQA_Redundant_3k_2A---CDSS12	ZD3500	100903000150	00:24:82:32:cf:2a		0	30	5	Dec. 27 2012 15:45:00

☑ ZoneDirector Name
☑ Model Name
☑ Serial Number
☑ MAC Address
☑ IP Address
☑ %CPU
☑ %Mem
☑ %Disk
☑ Timestamp

Export As XLS File CSV File   Ed… …ds Show All 1 - 10 of 1568

Save Report

Report Name: □ Include Filters □ Include Table Header Settings

Save Report Cancel

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

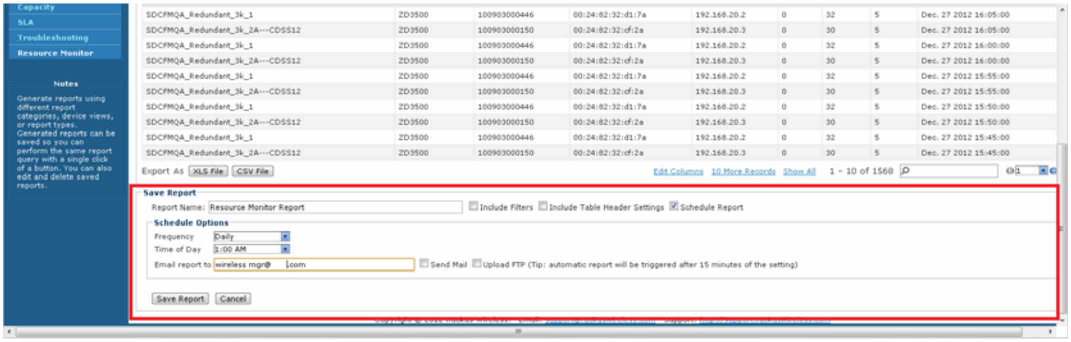
Using Advanced Report Options

You can configure the options of a report, and then the report so you can easily generate the report anytime without having to reconfigure the report options. You can even configure FlexMaster to automatically generate the report based on a schedule and send it to email recipients that you specify.

1. Click the **Reports** tab.
2. On the *Report Categories* menu, click the name of the report that you want to configure.
3. Go to the *Save Report* section.
4. In *Report Name*, type a descriptive name for the report that you are saving.
5. Configure the following settings:
   - *Include Filters:* Select this check box when you want the saved report to include the report filter that you configured, if any. This check box only appears if the report that you are saving provides report filters.
   - *Include Table Header Settings:* Select this check box when you want the saved report to include only the table columns that are currently displayed. If you hid columns in the report and you want the saved report to show exactly the same columns, then select this check box. For more information on how to hide report columns, refer to Hiding and Showing Columns in Reports.
   - *Schedule Report:* Select this check box when you want FlexMaster to generate this report automatically based on a schedule that you specify, with a display period as short as once per hour. After you select this check box, the *Schedule Options* section appears below. Configure the following settings:
     - *Frequency*: Specify how often you want FlexMaster to generate this report. Options include *Daily, Weekly* and *Monthly.* If you selected **Weekly**, then select the **Day of the Week** when FlexMaster generates the report. If you selected **Monthly**, then select the **Day of the Month** when FlexMaster generates the report.
     - *Time of Day*: Set the time when FlexMaster generates the report.
     - *Email report to*: Type the email address to which the report is sent. When you are sending the report to multiple email addresses, use a comma to separate the email addresses.
     - Select *Send Mail* and/or *Upload FTP,* as required.
6. Click **Save Report**.

You have completed configuring FlexMaster to generate and email this report automatically. The report should now appear on the *Saved Reports* page. For more information on working with saved reports, refer to Managing Saved Reports.

Figure 155. Saving a report and automating report generation



Capacity
SLA
Troubleshooting
Resource Monitor

Notes

Generate reports using different report categories, device views, or report types. Generated reports can be saved so you can perform the same report query with a single click of a button. You can also edit and delete saved reports.

SDCFMQA_Redundant_3k_1	ZD3500	100903000446	00:24:82:32:d1:7a	192.168.20.2	0	32	5	Dec. 27 2012 16:05:00
SDCFMQA_Redundant_3k_2A---CDSS12	ZD3500	100903000150	00:24:82:32:cf:2a	192.168.20.3	0	30	5	Dec. 27 2012 16:05:00
SDCFMQA_Redundant_3k_1	ZD3500	100903000446	00:24:82:32:d1:7a	192.168.20.2	0	32	5	Dec. 27 2012 16:00:00
SDCFMQA_Redundant_3k_2A---CDSS12	ZD3500	100903000150	00:24:82:32:cf:2a	192.168.20.3	0	30	5	Dec. 27 2012 16:00:00
SDCFMQA_Redundant_3k_1	ZD3500	100903000446	00:24:82:32:d1:7a	192.168.20.2	0	32	5	Dec. 27 2012 15:55:00
SDCFMQA_Redundant_3k_2A---CDSS12	ZD3500	100903000150	00:24:82:32:cf:2a	192.168.20.3	0	30	5	Dec. 27 2012 15:55:00
SDCFMQA_Redundant_3k_1	ZD3500	100903000446	00:24:82:32:d1:7a	192.168.20.2	0	32	5	Dec. 27 2012 15:50:00
SDCFMQA_Redundant_3k_2A---CDSS12	ZD3500	100903000150	00:24:82:32:cf:2a	192.168.20.3	0	30	5	Dec. 27 2012 15:50:00
SDCFMQA_Redundant_3k_1	ZD3500	100903000446	00:24:82:32:d1:7a	192.168.20.2	0	32	5	Dec. 27 2012 15:45:00
SDCFMQA_Redundant_3k_2A---CDSS12	ZD3500	100903000150	00:24:82:32:cf:2a	192.168.20.3	0	30	5	Dec. 27 2012 15:45:00

Export As XLS File CSV File   Edit Columns 10 More Records Show All 1 - 10 of 1568

Save Report

Report Name: Resource Monitor Report ☐ Include Filters ☐ Include Table Header Settings ☑ Schedule Report

Schedule Options

Frequency: Daily
Time of Day: 1:00 AM
Email report to: wireless mgr@ .com ☐ Send Mail ☐ Upload FTP (Tip: automatic report will be triggered after 15 minutes of the setting)

Save Report   Cancel

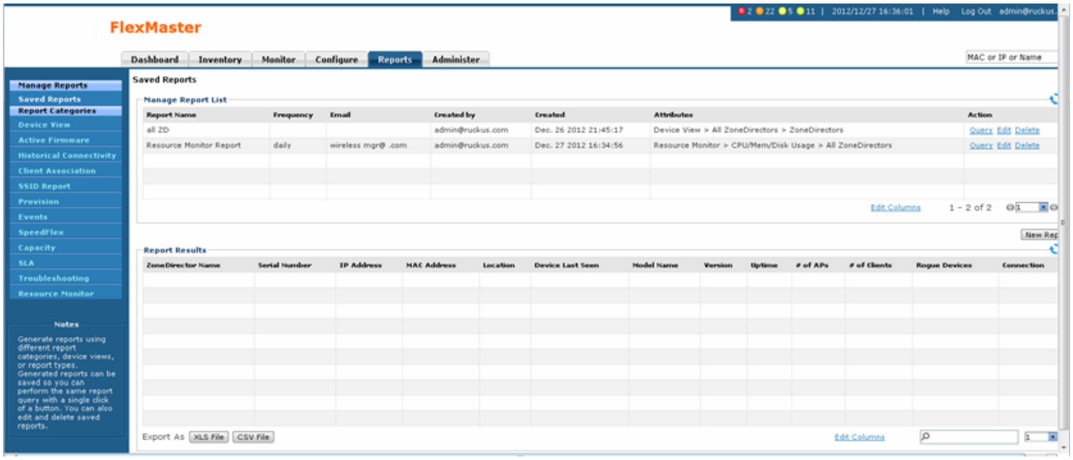
Managing Saved Reports

The *Saved Reports* page displays reports that you have previously configured and saved. There are three tasks that you can perform on the *Saved Report* page:

- Querying a Report
- Editing a Report
- Deleting a Report

NOTE: A button named **New Report** appears below the *Manage Report List* section. You can click the button to save a new report. Other than the *Select a Report Category* option (which you use to select the type of report to save), the procedure for configuring and saving a report from the *Saved Reports* page is essentially the same as when doing it from the main page for the specific report.

Figure 156. The Saved Reports page



Notes

Generate reports using different report categories, device views, or report types. Generated reports can be saved so you can perform the same report query with a single click of a button. You can also edit and delete saved reports.

Saved Reports

Manage Report List

Report Name	Frequency	Email	Created by	Created	Attributes	Action
all ZD			admin@ruckus.com	Dec. 26 2012 21:45:17	Device View > All ZoneDirectors > ZoneDirectors	Query Edit Delete
Resource Monitor Report	daily	wireless mgr@ .com	admin@ruckus.com	Dec. 27 2012 16:34:56	Resource Monitor > CPU/Mem/Disk Usage > All ZoneDirectors	Query Edit Delete

Edit Columns 1 - 2 of 2

New Rep

Report Results

ZoneDirector Name	Serial Number	IP Address	MAC Address	Location	Device Last Seen	Model Name	Version	Uptime	# of APs	# of Clients	Rogue Devices	Connection

Export As XLS File CSV File   Edit Columns

Querying a Report

Querying a report refers to manually generating the report using the options that you configured when you saved the report.

1. Go to *Reports > Manage Reports > Saved Reports*.
2. In the *Manage Report List* section, look for the report that you want to query.
3. Click the **Query** link that is in the same row as the name of the saved report.

The page refreshes, and then the report that you queried appears below, in the *Report Results* section.

Editing a Report

When you need to change the report options, you can edit the report settings from the *Saved Reports* page.

1. Go to *Reports > Manage Reports > Saved Reports*.
2. In the *Manage Report List* section, look for the report that you want to edit.
3. Click the **Edit** link that is in the same row as the name of the saved report. The *Edit Report* section appears below.
4. Update the report options as needed.
5. Click **Save Report**.

You have completed editing a report.

Deleting a Report

When you no longer want a report to appear on the *Saved Reports* page, you can delete it.

1. Go to *Reports > Manage Reports > Saved Reports*.
2. In the *Manage Report List* section, look for the report that you want to delete.
3. Click the **Delete** link that is in the same row as the name of the saved report. A confirmation message appears.
4. Click **OK** to confirm that you want to delete the report.

The page refreshes, and then the report that you deleted disappears from the *Manage Report List* section.

9

Performing Administrative Tasks

In This Chapter:

About the Administer Tab

The *Administer* tab provides options for viewing audit logs, updating the FlexMaster license file, configuring system settings, and managing users.

Viewing Audit Logs

Audit logs describe configuration actions that were performed on the FlexMaster and identify the users who initiated each action. Auditing is an important function that can help you determine when a configuration change was made and by whom in order to troubleshoot possible issues.

The following table lists the entries that can appear in the audit logs.

Table 31. Audit log entries

Audit Type	Description
Task creation error occurred	User created a provisioning task but it failed.
Configuration upgraded	User created a configuration upgrade task.
Firmware upgraded	User created a firmware upgrade task.
Device rebooted	User created a reboot task.
Device reset to factory default	User created a factory reset task.
Configuration settings updated	User updated a device's configuration from the Device View.
User logged in	User logged into the FlexMaster Web interface.
User logged out	User log out of the FlexMaster Web interface.
User account created	Administrator created a new user account.
User account updated	Administrator updated a user account.
User account deleted	Administrator deleted a user account.
Device log file retrieved	User retrieved an AP's log file from the Device View.
Device log file emailed	User sent out an AP's log file via email.
Device ping test performed	User performed a PING test from the Device View.
VLAN settings updated	User updated the AP's VLAN settings from the Device View.
Audit log emailed	User sent out FlexMaster's audit log via email.
License file verification	The maximum number of devices supported by your FlexMaster license has been reached. To manage additional devices, please contact Ruckus Wireless Support and obtain a license for additional devices.

Table 31. Audit log entries (Continued)

Audit Type	**Description**
License file uploaded	User uploaded a new license file into FlexMaster.
Device registered	A device registered with FlexMaster.
Inventory file imported	User imported an inventory file (XLS) into FlexMaster.
Firmware file imported	User uploaded new firmware image files.
Configuration template created or updated	User edited the configuration template.
Device group created or updated	User created or updated the device group.
Device tag created or updated	User created or updated a tag name.
Task cancelled	A user-created task has been cancelled.
Approval mode updated	User updated the AP approval mode on the *Inventory* page.
Auto configuration rule created	User created a new auto-configuration rule.
ZoneDirector configuration obtained	User performed “obtain ZD configuration” from a ZoneDirector device.
SSL certificate uploaded	User uploaded an SSL certificate to FlexMaster.
Inventory status created	User created an inventory status.
Inventory status modified	User updated an inventory status.
Inventory status assigned	User changed an AP's inventory status.
Inventory comment assigned	User edited an AP's comment on the *Inventory* page.
Inventory status deleted	User deleted an inventory status.
ZoneDirector configuration cloned	User created a “Clone ZoneDirector” task.
Managed group created	User created a group for delegated management.
Managed group updated	User updated a group for delegated management.
Managed group deleted	User deleted a group for delegated management.
Managed group device(s) added	User assigned devices to a managed group.
Managed group device(s) removed	User removed devices from a managed group.

Table 31. Audit log entries (Continued)

Audit Type	Description
User group mapping updated	User changed the "user account" and "managed group" mapping.
User logged in via the Northbound interface	A 3rd party system logged into FlexMaster via the Northbound interface.
User logged out via the Northbound interface	A 3rd party system logged out of FlexMaster via the Northbound interface.
Northbound interface operation invoked	A 3rd party system invoked the Northbound interface.
Upgrade script started	User installed a patch on the FlexMaster server.
Upgrade successful	User patched FlexMaster successfully.
Upgrade failed	User patch for FlexMaster failed.
ZoneDirector could not be reached	FlexMaster could not reach a managed ZoneDirector.
Task deleted	User deleted a task.
Task restarted	User restarted a failed task.
Automatic report created or updated	User created an automatic report.
User failed to log in.	User used an incorrect password to log in to FlexMaster three times.
Automatic report emailed	Automatic report has been sent out.

Managing FlexMaster Licenses

After you install FlexMaster, the number of Ruckus Wireless APs that FlexMaster can manage is limited to 100. Once this limit is reached, no additional devices are able register with FlexMaster (and none appear on the *Inventory* page). To enable FlexMaster to manage additional APs, you need to upload at least one license file. Use the *License* page in *Management > License* to upload a license file.

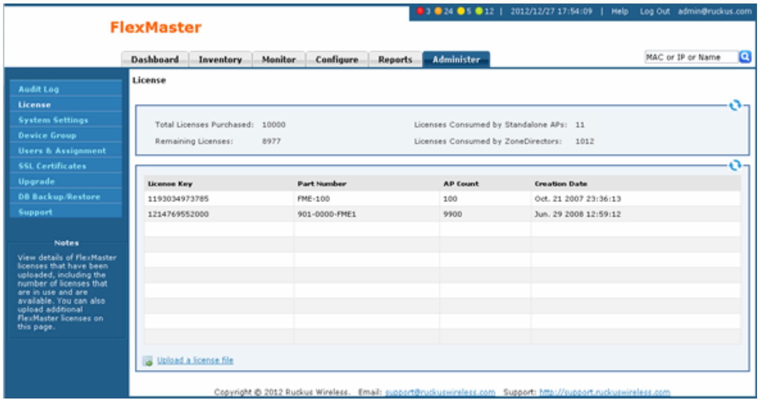
NOTE: When managed devices consume all the available license seats that the current license file supports, an alert message appears on the Dashboard.

Total AP count represents the total number of Ruckus Wireless APs that can be managed by your FlexMaster according to the installed licenses. Each FlexMaster license enables management of a maximum number of Ruckus Wireless APs. When your total inventory nears the total in your initial license, you buy a new license to add on to the maximum number; that is, a new license adds on to the previous license, it does not overwrite the previous license. Thus, *Total AP count* is the sum of AP counts within each license file.

NOTE: If your inventory count reaches your license total, then any new devices attempting to register are denied (and do not appear in your Inventory) until your license situation is resolved.

NOTE: Licenses Consumed by ZoneDirectors indicates the total number of APs that your ZoneDirector licenses can support, not the number of APs that your ZoneDirector devices are currently managing.

Figure 157. The License page



License

Total Licenses Purchased: 10000
Remaining Licenses: 8977
Licenses Consumed by Standalone APs: 11
Licenses Consumed by ZoneDirectors: 1012

License Key	Part Number	AP Count	Creation Date
1193034973785	FME-100	100	Oct. 21 2007 23:36:13
1214769552000	901-0000-FME1	9900	Jun. 29 2008 12:59:12

Upload a license file

Notes

View details of FlexMaster licenses that have been uploaded, including the number of licenses that are in use and are available. You can also upload additional FlexMaster licenses on this page.

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Uploading a License File

You can update your current FlexMaster license by uploading additional license files using the FlexMaster Web interface.

1. Once you obtain the license file from Ruckus Wireless, log in to the FlexMaster Web interface.
2. Go to *Administer > License.*
3. Click the **Upload a license file link** located below the *License* table. The *Upload a License File* form opens below the link.
4. Click the **Browse** button next to *Select file to be uploaded.*
5. Select the license file, and then click **OK** within the dialog box to close the *Browse* window.
6. Click **Upload** to upload the license file to FlexMaster.

Configuring System Settings

The System Settings option allows you to specify an SMTP server and a support-level user for sending FlexMaster system email messages. Audit and system logs are sent to the specified email address when initiated from those respective areas.

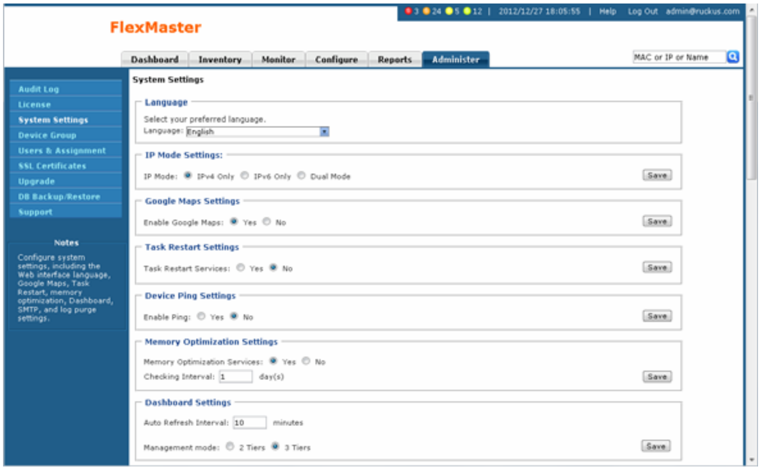
It also enables configuration of a purge policy. A purge policy establishes a length of time FlexMaster-generated files (such as logs, events, and graph data) should be maintained on FlexMaster. Once the configured length of time has been reached, files/items older than the date are purged from FlexMaster to save disk space. This prevents those files from growing interminably.

You can also change the display language settings on the *System Settings* page and enable or disable Google Maps.

This section describes how to configure the following settings:

- Language Settings
- IP Mode Settings
- Google Maps Settings
- Task Restart Settings
- Device Ping Settings
- Memory Optimization Settings
- Dashboard Settings
- SMTP Settings
- Purge Policy
- TACACS+ Settings
- FTP Server Settings
- Logo Settings

Figure 158. System Settings page (part 1 of 3)



Configure system settings, including the Web interface language, Google Maps, Task Restart, memory optimization, Dashboard, SMTP, and log purge settings.

System Settings

Language

Select your preferred language.
Language: English

IP Mode Settings:

IP Mode: ● IPv4 Only ○ IPv6 Only ○ Dual Mode Save

Google Maps Settings

Enable Google Maps: ● Yes ○ No Save

Task Restart Settings

Task Restart Services: ○ Yes ● No Save

Device Ping Settings

Enable Ping: ○ Yes ● No Save

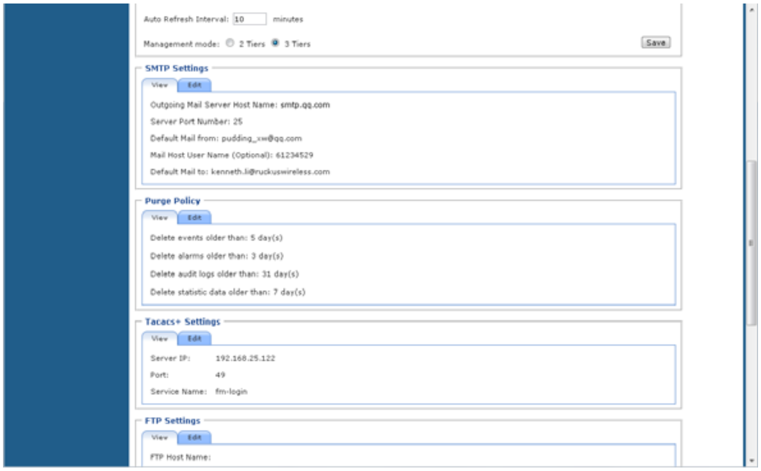
Memory Optimization Settings

Memory Optimization Services: ● Yes ○ No
Checking Interval: 1 day(s) Save

Dashboard Settings

Auto Refresh Interval: 10 minutes
Management mode: ○ 2 Tiers ● 3 Tiers Save

Figure 159. System Settings page (part 2 of 3)



Auto Refresh Interval: 10 minutes

Management mode: ○ 2 Tiers ● 3 Tiers

SMTP Settings

Outgoing Mail Server Host Name: smtp.qq.com

Server Port Number: 25

Default Mail from: pudding_xw@qq.com

Mail Host User Name (Optional): 61234529

Default Mail to: kenneth.li@ruckuswireless.com

Purge Policy

Delete events older than: 5 day(s)

Delete alarms older than: 3 day(s)

Delete audit logs older than: 31 day(s)

Delete statistic data older than: 7 day(s)

Tacacs+ Settings

Server IP: 192.168.25.122

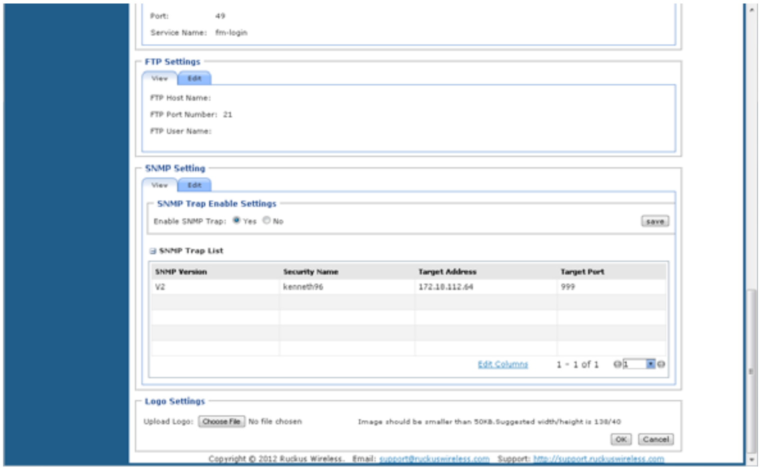
Port: 49

Service Name: fm-login

FTP Settings

FTP Host Name:

Figure 160. System Settings page (part 3 of 3)



Port: 49

Service Name: fm-login

FTP Settings

FTP Host Name:

FTP Port Number: 21

FTP User Name:

SNMP Setting

SNMP Trap Enable Settings

Enable SNMP Trap: ● Yes ○ No

SNMP Trap List

SNMP Version	Security Name	Target Address	Target Port
V2	kenneth96	172.18.112.64	999

1 - 1 of 1

Logo Settings

Upload Logo: Choose File No file chosen

Image should be smaller than 50KB.Suggested width/height is 138/40

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Language Settings

The FlexMaster Web interface supports five display languages:

- English (default)
- Chinese Simplified
- Japanese
- Spanish
- Arabic

You can switch to any of these languages as follows.

NOTE: Although the FlexMaster Web interface supports these five languages, the installation script is only available in English.

1. Go to *Administer > System Settings.*
2. In **Language**, select the language to which you want to change the Web interface display. The Web interface refreshes, and then changes the display to the language you selected.

IP Mode Settings

FlexMaster supports IPv4, IPv6, and dual IPv4/IPv6 operation modes. If dual mode is used, then FlexMaster keeps both IPv4 and IPv6 IP addresses. By default, FlexMaster operates in IPv4 mode. When you want to change the IP mode, follow the procedure below.

1. Go to *Administer > System Settings.*
2. Under *IP Mode Settings*, select the mode that you want FlexMaster to use. Options include **IPv4 Only**, **IPv6 Only** and **Dual Mode**.
3. Click the **Save** button that is in the same section.

Google Maps Settings

FlexMaster uses Google Maps to show the geographical locations of managed devices. This requires FlexMaster to have active connection to Google Maps via the Internet and for Google Maps to be enabled on FlexMaster. By default, Google Maps is enabled on FlexMaster.

When FlexMaster is unable to access Google Maps, gray boxes appear on the FlexMaster Web interface, instead of the map that Google Maps provides. If your location or network is preventing FlexMaster from accessing Google Maps, then you can disable Google Maps on FlexMaster to hide these gray boxes.

1. Go to *Administer > System Settings.*
2. Under *Google Maps Settings*, click **No** to disable or **Yes** to enable Google Maps.
3. Click the **Save** button that is in the same section.

Task Restart Settings

If you want FlexMaster to automatically restart failed configuration upgrade or firmware upgrade tasks, then click the **Yes** option, and then click the **Save** button in the *Task Restart Settings* section. By default, automatic task restart is disabled.

Device Ping Settings

FlexMaster managed devices have a built-in ping feature that can be used to test the connection status between two devices. You can enable and disable ping on these managed devices from the FlexMaster Web interface.

1. Go to *Administer > System Settings.*
2. Under *Enable Ping*, click either **Yes** or **No**. Ping is enabled by default.
3. Click the **Save** button that is in the same section.

Memory Optimization Settings

To help ensure that FlexMaster has enough memory resources to process tasks, you can configure the system settings to clear its memory cache periodically.

Do this by clicking **Yes**, and then setting the interval (in days) at which FlexMaster clears its memory cache. When you are done, click the **Save** button in the Memory Optimization Settings section.

NOTE: Memory optimization requires that your FlexMaster server is running on Linux kernel 2.6.16 or later version. If your Linux kernel version is older, then the memory optimization settings that you configure are not applied.

Dashboard Settings

Dashboard settings include options for configuring the refresh rate of information that is displayed on the Dashboard and device management mode that you want to display on the Dashboard.

Follow these steps to configure the refresh rate of the Dashboard data.

1. Go to *Administer > System Settings.*
2. Scroll down to the *Dashboard Settings* section.
3. In *Auto Refresh Interval*, type refresh interval (in minutes) that you want to set for the Dashboard data. The default refresh interval is 10 minutes.
4. Click the **Save** button that is in the same section.

Setting 2 Tier or 3 Tier Device Management

To select the device management mode that you want to display on the Web interface:

1. Go to *Administer > System Settings.*
2. Scroll down to the *Dashboard Settings* section.
3. In *Management mode*, select one of the following options:
   - *2 Tiers*: Shows data related to FlexMaster and APs only. Click this option if APs on the network are being managed directly by FlexMaster.
   - *3 Tiers* (default): Shows data related to FlexMaster, ZoneDirector devices, and APs. Click this option if APs on the network are being managed by ZoneDirector devices (which, in turn, are being managed by FlexMaster).
4. Click the **Save** button that is in the same section.

SMTP Settings

You must configure FlexMaster's host server to enable it to send email notifications. For example, the Audit Log and System Log menu items offer email options. When sending logs via email, the entire contents of these log files are sent to the pre-configured recipient (*Default Mail To*) specified on the *SMTP Settings* page.

NOTE: You may have already configured the SMTP settings during FlexMaster installation.

For the email functionality to work, you need either [1] a DNS server that can supply the IP address of the SMTP server, or [2] the correct mapping to the SMTP server in your hosts file (located in the `/etc` directory). If you choose the second option, then you need to add lines similar to the following in your `/etc/hosts` file:

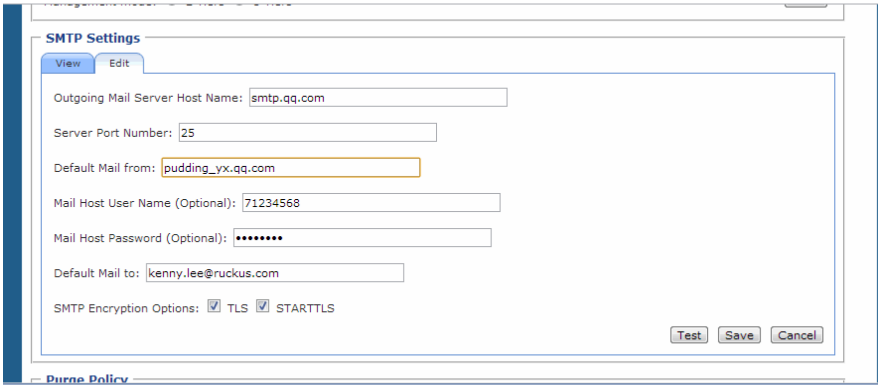
```
127.0.0.1 fully.qualified.domain.name localhost
123.123.123.123 fully.qualified.smtpdomain.name smtp-
server_hostname
```

NOTE: If you edited the hosts file before you installed FlexMaster (as described in Editing the Server Hosts File, then the first line should already exist in the hosts file; you do not need to add the same line again.

Follow these steps to edit the SMTP settings.

1. Go to *Administer > System Settings.*
2. Scroll down to the *SMTP Settings* section.
3. Click the **Edit** tab.

Figure 161. Editing SMTP Settings



SMTP Settings

Outgoing Mail Server Host Name: smtp.qq.com

Server Port Number: 25

Default Mail from: pudding_yx.qq.com

Mail Host User Name (Optional): 71234568

Mail Host Password (Optional): ••••••••

Default Mail to: kenny.lee@ruckus.com

SMTP Encryption Options: ☑ TLS ☑ STARTTLS

4. In *Outgoing Mail Server Host Name*, type the host name of the outgoing SMTP server.
5. In *Server Port Number,* type the SMTP server's listening port number. The default SMTP port number is 25.

NOTE: If you select *TLS* or *STARTTLS SMTP Encryption Option*s, then define a different port number, because different SMTP server protocols do not support port 25. For example, the Gmail server uses 587 as its STARTTLS port and 465 as the TLS port, and the QQ server uses 25 as its non-SSL port and 465 as its TLS port.

If your port number setting and protocol setting do not match, emails cannot be sent successfully. For example, if you select port 25 and select STARTTLS for a QQ server, testing will fail. Emails do not automatically revert to the non-TLS protocol.

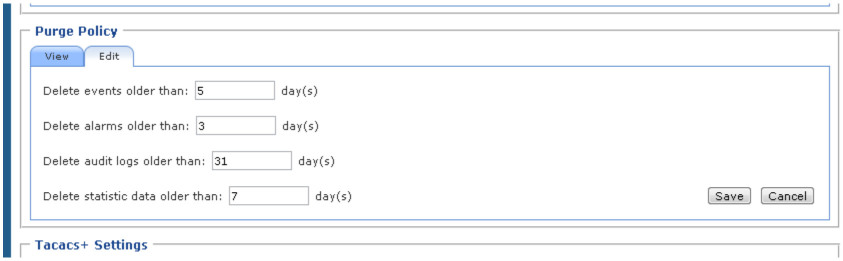
6. In *Default Mail from*, type the email address that appears as the sender of the email.
7. In *Mail Host User Name (Optional)*, type the SMTP user name for the email account that you are using to send email notifications.
8. In *Mail Host Password (Optional)*, type the SMTP password for the email account.
9. In *Default Mail to*, type the email address of the user to whom you want to send email notifications.
10. In *SMTP Encryption Options:*
    - Check the *TLS* box if you want FlexMaster to use Transport Layer Security cryptographic protocol.
    - Also check the *STARTTLS* box if you want FlexMaster to use the STARTTLS extension to upgrade plain email connections to encrypted TLS connections instead of using a separate port for encrypted communication.
11. Click **Test** to verify that FlexMaster is able to use the SMTP settings that you configured to send email notifications. If an error appears, then check your settings and update them with the correct settings.
12. Click the **Save** button that is in the same section.

Purge Policy

Use Purge Policy to automatically delete FlexMaster event logs, audit logs, and graph data after they age past a certain number of days. This helps ensure that FlexMaster has sufficient disk space to perform tasks.

1. Go to *Administer > System Settings.*
2. Scroll down to the *Purge Policy* section.
3. Click the **Edit** tab.

Figure 162. Editing Purge Policy settings



Purge Policy

Delete events older than: 5 day(s)

Delete alarms older than: 3 day(s)

Delete audit logs older than: 31 day(s)

Delete statistic data older than: 7 day(s)

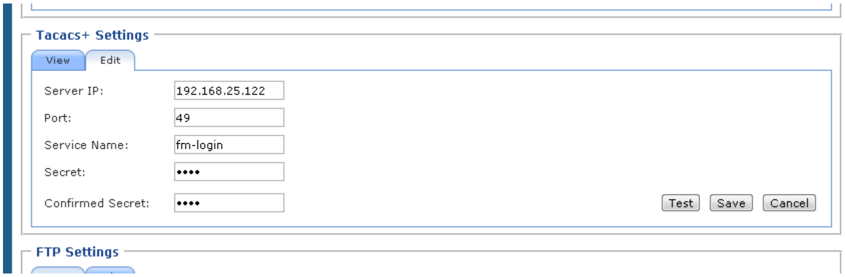
4. Type a numerical value (all values are number of days) for one or more of the following:
   - *Delete events older than:* default is 30 days
   - *Delete alarms older than:* default is 30 days
   - *Delete audit logs older than:* default is 30 days
   - *Delete statistic data older than:* default is 7 days
5. Click **Save**.

TACACS+ Settings

TACACS+ is an access control network protocol that provides separate authentication, authorization and accounting services. For your Ruckus Wireless devices, you must configure the devices to communicate with the TACACS+ server.

1. Go to *Administer > System Settings.*
2. Scroll down to the *Tacacs+ Settings* section.
3. Click the **Edit** tab.

Figure 163. Editing TACACS+ settings



Tacacs+ Settings

Server IP: 192.168.25.122
Port: 49
Service Name: fm-login
Secret: ••••
Confirmed Secret: ••••

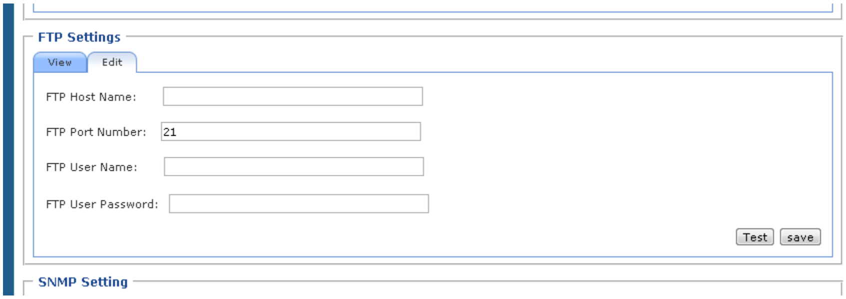
4. Enter the TACACS+ parameters:
   - *Server* - IPv4 or IPv6 server address.
   - *Port* - 49 is the default, but it can be set to any available TCP port.
   - *Service Name*.
   - *Secret*.
   - *Confirmed Secret*.
5. Click **Test** to verify that FlexMaster is able to use the TACACS+ settings that you configured. If an error appears, then check your settings and update them with the correct settings.
6. Click **Save**.

FTP Server Settings

You must configure FTP server settings for your Ruckus Wireless devices to communicate with an FTP server.

1. Go to *Administer > System Settings.*
2. Scroll down to the *FTP Settings* section.
3. Click the **Edit** tab.

Figure 164. Editing FTP server settings



FTP Settings

FTP Host Name:
FTP Port Number: 21
FTP User Name:
FTP User Password:

4. Enter the FTP parameters:
   - *FTP Host Name* - IPv4 or IPv6 server address.

- *FTP Port Number* - 49 is the default, but it can be set to any available TCP port.
- *FTP User Name* - Login.
- *FTP User Password* - Server password.

5. Click **Test** to verify that FlexMaster is able to use the FTP server settings that you configured. If an error appears, then check your settings and update them with the correct settings.
6. Click **Save**.

SNMP Server Settings

If you have an SNMP trap receiver on the network, then you can configure FlexMaster to send SNMP trap notifications to the server. Enable this feature if you want to automatically receive notifications for ZoneDirector, AP, and client events that indicate possible network issues.

Enabling SNMP Traps

Before you can send SNMP trap notifications, you must enable SNMP trap notifications.

1. Go to *Administer > System Settings.*
2. Scroll down to the *SNMP Settings* section.
3. Click the **View** tab.
4. In *Enable SNMP Trap*, click **Yes** or **No**.
5. Click **save**.
6. Continue with Configuring SNMP Settings.

Configuring SNMP Settings

After you enable SNMP trap, you need to configure the SNMP V2/V3 settings, depending on the SNMP version that the SNMP trap receiver is using.

If Your Network Uses SNMP v2

1. Click the *Administer > System Settings > SNMP Settings >* **Edit** tab.
2. Under *SNMP v2 Settings*, configure the following settings:
   - *Community:* Enter the SNMP v2 community string.
   - *Read:* Select this check box to enable SNMP read access.
   - *Trap:* Select this check box to send SNMP traps to the trap server on the network.

NOTE: To add another SNMP v2 community string, click the ⊕ icon, and then configure the community string and read and trap privileges.

3. Click **save** to save your changes.
4. Under *SNMP Trap*, configure the following settings:
   - *SNMP Version:* Select **V2**.
   - *Security Name:* Enter the security name.
   - *Target Address:* Enter the IP address of the SNMP trap receiver.
   - *Target Port:* Enter the SNMP port number on the SNMP trap receiver.
5. Click **save** to save your changes.

If Your Network Uses SNMPv3

1. Click the *Administer* > *System Settings* > *SNMP Settings* > **Edit** tab.
2. Under *SNMP v3 Settings*, configure the following settings:
   - *User Name*: Enter a user name between 1 and 31 characters long.
   - *Auth Protocol*: Select **MD5**, **SHA** or **NONE** authentication method (default is MD5).
     - *MD5* (Message-Digest algorithm 5) is a message hash function with 128-bit output.
     - *SHA* (Secure Hash Algorithm) is a message hash function with 160-bit output.
   - *Auth Password*: Enter a passphrase between 8 and 32 characters long.
   - *Priv Protocol*: Select **DES**, **AES** or **NONE**.
     - *DES* (Data Encryption Standard), data block cipher.
     - *AES* (Advanced Encryption Standard), data block cipher.
     - *NONE:* No Privacy passphrase is required.
   - *Priv Password*: If either *DES* or *AES* is selected, then enter a Privileged Password between 8 and 32 characters long.
   - *Read*: Select this check box to enable SNMP read access.
   - *Trap*: Select this check box to send SNMP traps to the trap server on the network.

NOTE: To add another SNMP v3 community string, click the ⊕ icon, and then configure the community string and read and trap privileges.

3. Click **save** to save your changes.
4. Under *SNMP Trap*, configure the following settings:
   - *SNMP Version*: Select **V3**.
   - *Security Name*: Enter the security name.
   - *Target Address*: Enter the IP address of the SNMP trap receiver.
   - *Target Port*: Enter the SNMP port number on the SNMP trap receiver.
5. Click **save** to save your changes.

Default Events for Which FlexMaster Sends Trap Notifications

There are several event types for which FlexMaster sends trap notifications to the SNMP server that you specified.

The default event types include:

- System administration events
- Mesh events
- Configuration events
- Client events
- AP admin events
- Performance events
- Standalone AP events
- Alarm events

Default *System Admin* trap notifications:

- ZD System Failure Recovered
- Admin restart
- Admin shutdown
- Admin upgrade
- System cold restarted
- System warm restarted

Default *AP Admin* trap notifications:

- AP delete
- AP joined
- AP joined with reason
- AP lost
- AP lost heartbeat

Default *Standalone AP* trap notifications:

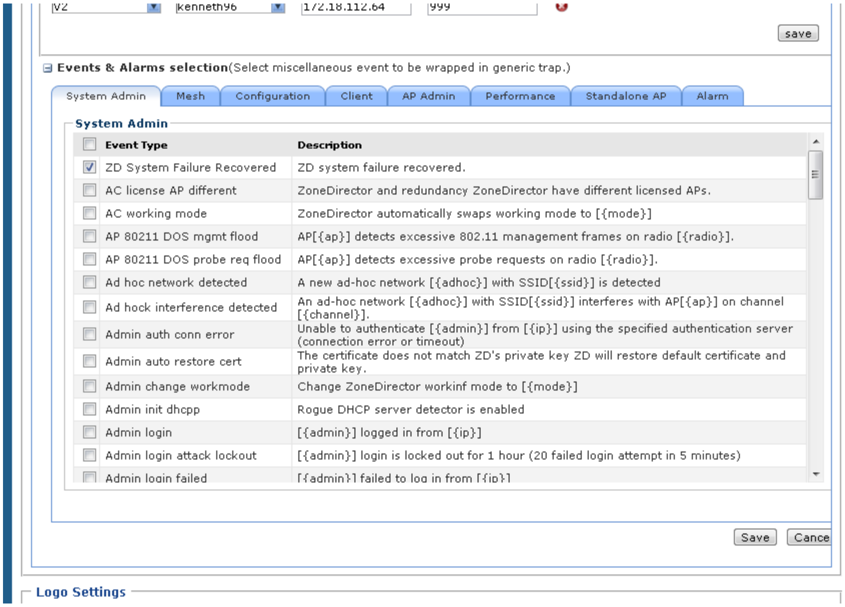
- Connectivity problem
- Device rebooted
- Device recovers from disconnect state
- Firmware successfully written to flash

Setting Events and Alarms for Which FlexMaster Sends Trap Notifications

If you want FlexMaster to send trap notifications for non-default events, then you need to enable trap notifications for these events.

1. In the *SNMP Settings* section, scroll down to the *Events & Alarms selection* section (under *SNMP Trap*).
2. If the *Events & Alarms selection* section is collapsed, then click the ⊞ icon to expand it. The configuration tabs for the various event types appear.

Figure 165. Events & Alarms selection



V2 | kenneth96 | 172.18.112.64 | 999

save

⊟ **Events & Alarms selection**(Select miscellaneous event to be wrapped in generic trap.)

System Admin

□	**Event Type**	**Description**
☑	ZD System Failure Recovered	ZD system failure recovered.
□	AC license AP different	ZoneDirector and redundancy ZoneDirector have different licensed APs.
□	AC working mode	ZoneDirector automatically swaps working mode to [{mode}]
□	AP 80211 DOS mgmt flood	AP[{ap}] detects excessive 802.11 management frames on radio [{radio}].
□	AP 80211 DOS probe req flood	AP[{ap}] detects excessive probe requests on radio [{radio}].
□	Ad hoc network detected	A new ad-hoc network [{adhoc}] with SSID[{ssid}] is detected
□	Ad hock interference detected	An ad-hoc network [{adhoc}] with SSID[{ssid}] interferes with AP[{ap}] on channel [{channel}].
□	Admin auth conn error	Unable to authenticate [{admin}] from [{ip}] using the specified authentication server (connection error or timeout)
□	Admin auto restore cert	The certificate does not match ZD's private key ZD will restore default certificate and private key.
□	Admin change workmode	Change ZoneDirector workinf mode to [{mode}]
□	Admin init dhcpp	Rogue DHCP server detector is enabled
□	Admin login	[{admin}] logged in from [{ip}]
□	Admin login attack lockout	[{admin}] login is locked out for 1 hour (20 failed login attempt in 5 minutes)
□	Admin login failed	[{admin}] failed to log in from [{ip}]

3. Click the tab names to view the list of events from event types, and then select the check box for each event type that you want FlexMaster to send trap notifications. Repeat as required.
4. Click **Save** to save your changes.

Setting User Customized Alarms

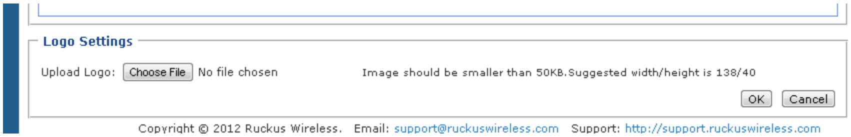
Refer to "About User Customized Alarms" on page 214 and "Configuring Alarm Settings" on page 217 for information about user-customized threshold-crossing alarms.

Logo Settings

You can change the Ruckus Wireless logo that appears up on the upper-left corner of the FlexMaster Web interface to a different image (for example, your company logo). To do this, you need to upload an image file to replace the Ruckus Wireless logo. The image file must be smaller than 50kb, with a recommended size of 138px by 40px.

1. Prepare a 138px by 40px version of your logo.
2. Go to *Administer > System Settings.*
3. Scroll down to the *Logo Settings* section.

Figure 166. Logo settings



Logo Settings

Upload Logo: Choose File No file chosen

Image should be smaller than 50KB.Suggested width/height is 138/40

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

4. Click the **Choose File** button.
5. When the *Open/Browse* dialog box appears, browse to the location where you saved the custom logo that you want to upload, and then select it.
6. Click **Open** to save your selection.
7. Click **OK** to finish uploading the custom logo file.

The FlexMaster Web interface refreshes, and the custom logo that you uploaded appears in place of the default Ruckus Wireless logo.

Managing Device Groups

FlexMaster allows you to create and edit device groups, and to assign devices to existing device groups. Each device can be assigned to a single device group at a time, and can be moved to a different device group at any time.

- Creating a Device Group
- Assigning Devices to a Device Group
- Editing a Device Group Name
- Deleting a Device Group

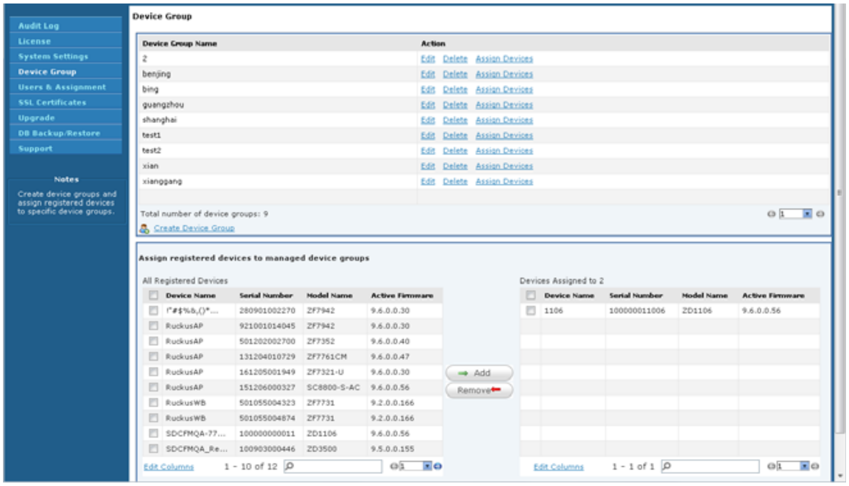
Creating a Device Group

1. Go to *Administer > Device Group.*
2. Click **Create Device Group**.
3. In the *CREATE DEVICE GROUP* section, enter the new device group name in *Device Group Name.*
4. Click **OK**.

Assigning Devices to a Device Group

1. Go to *Administer > Device Group.*
2. Click **Assign Devices** on the same line as the target device group name.

Figure 167. Assigning devices to a device group



Create device groups and assign registered devices to specific device groups.

Device Group

Device Group Name	Action
2	Edit Delete Assign Devices
benjing	Edit Delete Assign Devices
bing	Edit Delete Assign Devices
guangzhou	Edit Delete Assign Devices
shanghai	Edit Delete Assign Devices
test1	Edit Delete Assign Devices
test2	Edit Delete Assign Devices
xian	Edit Delete Assign Devices
xianggang	Edit Delete Assign Devices

Total number of device groups: 9

Create Device Group

Assign registered devices to managed device groups

All Registered Devices

□	Device Name	Serial Number	Model Name	Active Firmware
□	!"#$%&,()*...	280901002270	ZF7942	9.6.0.0.30
□	RuckusAP	921001014045	ZF7942	9.6.0.0.30
□	RuckusAP	501202002700	ZF7352	9.6.0.0.40
□	RuckusAP	131204010729	ZF7761CM	9.6.0.0.47
□	RuckusAP	161205001949	ZF7321-U	9.6.0.0.30
□	RuckusAP	151206000327	SC8800-S-AC	9.6.0.0.56
□	RuckusWB	501055004323	ZF7731	9.2.0.0.166
□	RuckusWB	501055004874	ZF7731	9.2.0.0.166
□	SDCFMQA-77...	100000000011	ZD1106	9.6.0.0.56
□	SDCFMQA_Re...	100903000446	ZD3500	9.5.0.0.155

Edit Columns 1 - 10 of 12

Devices Assigned to 2

□	Device Name	Serial Number	Model Name	Active Firmware
□	1106	100000011006	ZD1106	9.6.0.0.56

Edit Columns 1 - 1 of 1

3. In the *Assign registered devices to managed device groups* section, the left pane lists all the registered devices that are not already assigned to a device group. The right pane lists all of the devices assigned to the target device group.
4. Select the individual device check boxes and use the **Add** and **Remove** buttons to move devices to and from the right and left panes.
5. As you add devices to the right pane, FlexMaster assigns them to the target device group.

Editing a Device Group Name

1. Go to *Administer > Device Group.*
2. Click **Edit** on the same line as the target device group name.
3. In the *EDIT DEVICE GROUP* section, change the device group name in *Device Group Name.*
4. Click **OK**.

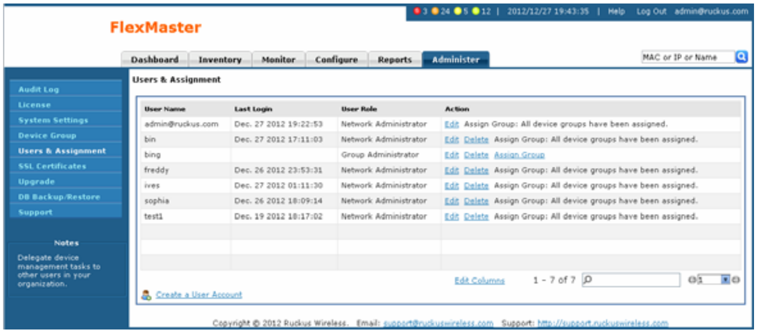
Deleting a Device Group

1. Go to *Administer > Device Group.*
2. Click **Delete** on the same line as the target device group name.
3. In the verification dialog, click **OK**. FlexMaster deletes the device group.

Managing User Accounts

When you want to share or delegate device management and monitoring tasks with other users in your organization, FlexMaster allows you to create additional user accounts. You should create a new user account and assign an appropriate role for each person who uses FlexMaster. Ruckus Wireless recommends against using one login account for multiple users as doing this may not produce useful audit log results.

Figure 168. Users & Assignment page


● 3 ● 24 ● 5 ● 12 | 2012/12/27 19:43:35 | Help Log Out admin@ruckus.com
FlexMaster
Dashboard
Inventory
Monitor
Configure
Reports
Administer
MAC or IP or Name
Audit Log
License
System Settings
Device Group
Users & Assignment
SSL Certificates
Upgrade
DB Backup/Restore
Support
Notes
Delegate device management tasks to other users in your organization.
Edit Columns
1 - 7 of 7
Create a User Account
Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Users & Assignment

User Name	Last Login	User Role	Action
admin@ruckus.com	Dec. 27 2012 19:22:53	Network Administrator	Edit Assign Group: All device groups have been assigned.
bin	Dec. 27 2012 17:11:03	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
bing		Group Administrator	Edit Delete Assign Group
freddy	Dec. 26 2012 23:53:31	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
ives	Dec. 27 2012 01:11:30	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
sophia	Dec. 26 2012 18:09:14	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
test1	Dec. 19 2012 18:17:02	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.

Understanding User Roles and Privileges

By default, the built-in admin account is listed; this account cannot be deleted or the User Name or User Role changed, but the password can be changed. User roles determine privileges and views available to a user within the FlexMaster system.

NOTE: There is no limit to the number of accounts that you can create for each user role.

User roles determine privileges and views available to a user within the FlexMaster system. The following are the roles that you can assign in FlexMaster:

Network Administrator

The Network Administrator role grants full read and write privileges to the entire FlexMaster system. The installation process creates one default Network Administrator (admin) account; this default admin account cannot deleted or renamed.

NOTE: The default Network Administrator (also called *Super User*) has the highest account privilege and can view, edit, and delete templates, auto-provisioning rules, and other user accounts (including other Network Administrator accounts).

A Network Administrator can perform the following tasks:

- Manage all devices in the Inventory

- Create other user accounts, including Group Administrators, Group Operators, Operators, or other Network Administrators
- Assign devices to device management groups. These device groups can be assigned to specific Group Administrators for managements.

Group Administrator

The Group Administrator role grants full read and write privileges to the assigned devices. A Group Administrator can perform the following tasks:

- Manage devices that belong to assigned groups
- Create Group Operator and Operator accounts
- Assign devices to device management groups
- View Dashboard and Inventory information related to the assigned devices
- Create configuration templates for assigned devices
- Provision configuration upgrade tasks for assigned devices

Group Operator

The Group Operator role grants read privileges only to the assigned devices. A Group Operator can perform the following tasks:

- View Dashboard information related to the assigned devices
- View Inventory information related to the assigned devices
- Only assigned devices appear on the *Inventory* page
- Only assigned devices appear in the search results
- Reports are only generated for assigned devices
- Receive system alerts for assigned devices. (**Note:** The Group Administrator defines the system alerts that a Group Operator can receive.)

NOTE: A Group Operator does not have Configure and Administer privileges. Although the Configure and Administer tabs still appear on the Web interface, changes to these by the Group Operator cannot be saved.

Device Operator

A Device Operator has read/write access at the device level only. Upon login, a Device Operator sees the *Device View* page without content. The Device Operator must enter the serial number or MAC address of a managed device to view details for that device. A Device Operator role is typically assigned to customer support personnel; the Operator can only see details once the customer provides the device information.

3rd Party Partner

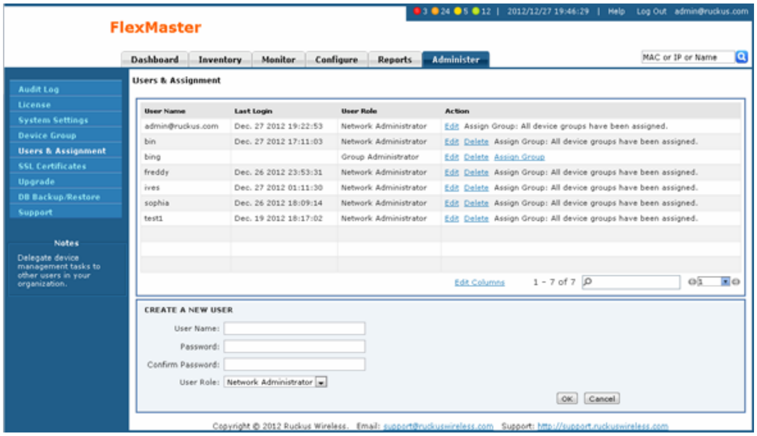
You can assign a 3rd-party partner as a device operator. The 3rd party system logs into FlexMaster via the Northbound interface.

Creating a New User Account

When you want to delegate the responsibility of managing FlexMaster and its managed devices to other authorized users in your organization, you can create a user account for each of them. There is no limit to the number of user accounts that you can create.

1. Go to *Administer > Users & Assignment.*
2. Click **Create a User Account**. FlexMaster displays the *CREATE A NEW USER* pane.

Figure 169. Creating a user account



Users & Assignment

User Name	Last Login	User Role	Action
admin@ruckus.com	Dec. 27 2012 19:22:53	Network Administrator	Edit Assign Group: All device groups have been assigned.
bin	Dec. 27 2012 17:11:03	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
bing		Group Administrator	Edit Delete Assign Group
freddy	Dec. 26 2012 23:53:31	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
ives	Dec. 27 2012 01:11:30	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
sophia	Dec. 26 2012 18:09:14	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
test1	Dec. 19 2012 18:17:02	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.

Edit Columns 1 - 7 of 7

CREATE A NEW USER

User Name:
Password:
Confirm Password:
User Role: Network Administrator

OK Cancel

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

3. In *User Name*, type a name that you want to assign to this user account. For example, you can type john or john doe. The user name is not case-sensitive and can contain up to 45 alphanumeric characters and spaces.
4. In *Password*, type a password for the account. The password is case-sensitive and can contain up to 45 alphanumeric characters.
5. Repeat the password in *Confirm Password.*
6. In *User Role*, select the role that you want to assign to this user. The options that appear on the User Role menu depends on your own user role. If you are a Network Administrator, then the following user roles appear on the menu: **Network Administrator**, **Group Administrator**, **Group Operator**, **Device Operator** and **3rd Party Partner**.

   For more information on user roles, refer to Understanding User Roles and Privileges.

6. Click **OK** to create the account.

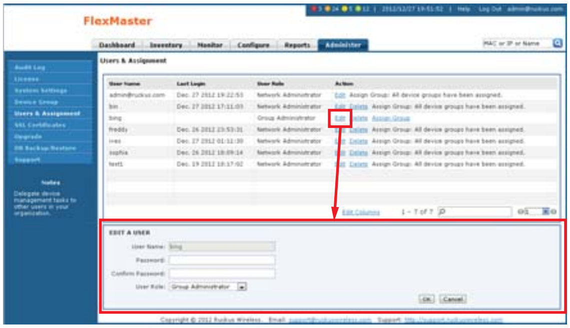
The page refreshes, and then the user account you have created appears in the *Users* list.

Editing a User Account

Edit a user account if you need to make account changes, such as the user password or the user role.

1. Go to *Administer > Users & Assignment.*
2. Find the row in the Users table for the desired user account to edit, and then click **Edit** in the *Action* column.

Figure 170. Editing a user account



Users & Assignment

User Name	Last Login	User Role	Action
admin@ruckus.com	Dec. 27 2012 19:22:53	Network Administrator	Edit Assign Group: All device groups have been assigned.
bin	Dec. 27 2012 17:11:03	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
bing		Group Administrator	Edit Delete Assign Group
freddy	Dec. 26 2012 23:53:31	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
ives	Dec. 27 2012 01:11:30	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
sophia	Dec. 26 2012 18:09:14	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
test1	Dec. 19 2012 18:17:02	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.

Edit Columns 1 - 7 of 7

EDIT A USER

User Name: bing
Password:
Confirm Password:
User Role: Group Administrator

OK Cancel

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

3. Edit the following options as required:
   - *User Name*
   - *Password*
   - *Confirm Password*
   - *User Role* (except for default "admin" account)
4. Click **OK** to save your changes.

Deleting a User Account

Delete user accounts that you no longer need to save space on the FlexMaster database and prevent unauthorized users from gaining access to the FlexMaster Web interface.

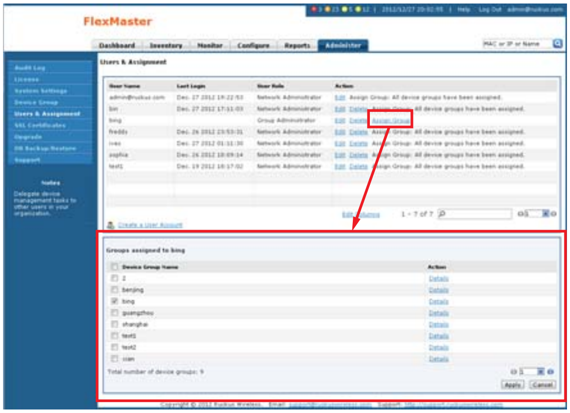
1. Go to *Administer > Users & Assignment.*
2. Find the row in the *Users* table for the desired user account to delete, and then click **Delete** in the *Action* column.

The page refreshes, and then the user account you deleted is removed from the *Users* list.

Assigning Users to Manage Device Groups

1. Create a User account as described in Creating a New User Account.
2. Create a Device Group as described in Creating a Device Group.
3. Assign devices to a Device Group as described in Assigning Devices to a Device Group.
4. Go to *Administer > Users & Assignment.*
5. Find the entry for the user account that you want to assign as group owner.
6. Click the **Assign Group** link that is in the same row as the user name. The *Groups Assigned to {User Name}* pane appears, displaying the names of existing device groups.

Figure 171. Assigning a user to manage the group



Users & Assignment

User Name	Last Login	User Role	Action
admin@ruckus.com	Dec. 27 2012 19:22:53	Network Administrator	Edit Assign Group: All device groups have been assigned.
bin	Dec. 27 2012 17:31:03	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
bing		Group Administrator	Edit Delete Assign Group
freddy	Dec. 26 2012 23:53:31	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
ivan	Dec. 27 2012 01:11:30	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
sophia	Dec. 26 2012 18:09:14	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.
test1	Dec. 19 2012 18:17:02	Network Administrator	Edit Delete Assign Group: All device groups have been assigned.

Groups assigned to bing

□ Device Group Name	Action
□ 2	Details
□ beijing	Details
☑ bing	Details
□ guangzhou	Details
□ shanghai	Details
□ test1	Details
□ test2	Details
□ xian	Details

Total number of device groups: 9

7. Select the check box for each managed group that you want to assign to the user account.
8. Click **Apply** to save your changes.

When the group owner logs into the FlexMaster Web interface, he or she is able to view and manage the devices that belong to the assigned group.

Managing SSL Certificates

When you use HTTPS to connect to the FlexMaster Web interface, a security warning appears every time you connect to the Web interface. This is because the default SSL certificate (or security certificate) that FlexMaster is using for HTTPS communication is signed by Ruckus Wireless and is not recognized by most Web browsers.

If you want to prevent these security warnings from appearing, then you need to import an SSL certificate that was issued by a recognized certificate authority such as VeriSign.

NOTE: FlexMaster currently supports only VeriSign security certificates.

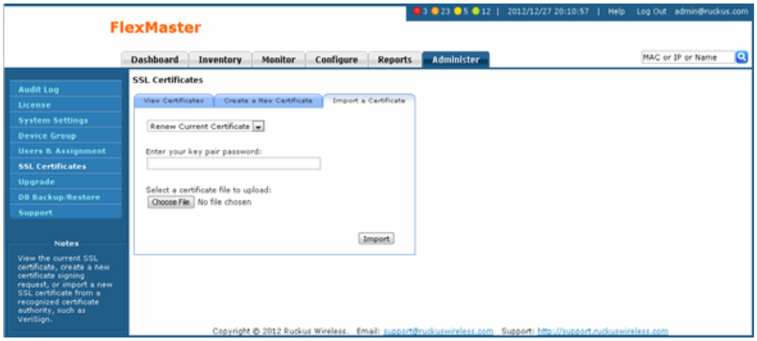
This section describes how to generate a certificate request file to obtain an SSL certificate from VeriSign and how to import a VeriSign SSL certificate into FlexMaster.

Importing an SSL Certificate

When you already have an SSL certificate issued by VeriSign, you can import it into FlexMaster and use it for HTTPS communication. To complete this procedure, you need the SSL certificate file and the key pair password that you set when you created the certificate signing request (CSR) file.

1. Copy the certificate file to location (either on the local drive or a network share) that you can access from the FlexMaster Web interface.
2. Go to *Administer > SSL Certificates.*
3. On the *SSL Certificates* page, click the **Import a Certificate** tab.

Figure 172. Importing an SSL certificate



SSL Certificates

Renew Current Certificate

Enter your key pair password:

Select a certificate file to upload:
No file chosen

Notes

View the current SSL certificate, create a new certificate signing request, or import a new SSL certificate from a recognized certificate authority, such as VeriSign.

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

4. In *Enter your key pair password,* type the key pair password that was set when you created the CSR file.
5. In *Select a certificate file to upload,* click **Choose File**, and then go to the location where you saved the certificate file. Select the certificate file, and then click **Open**.

6. Click **Import**. A message appears, informing you that the certificate has been imported successfully.
7. Click the **View Certificates** tab, and check the value for *Issuer* in the current certificate file. Verify that it shows the following:

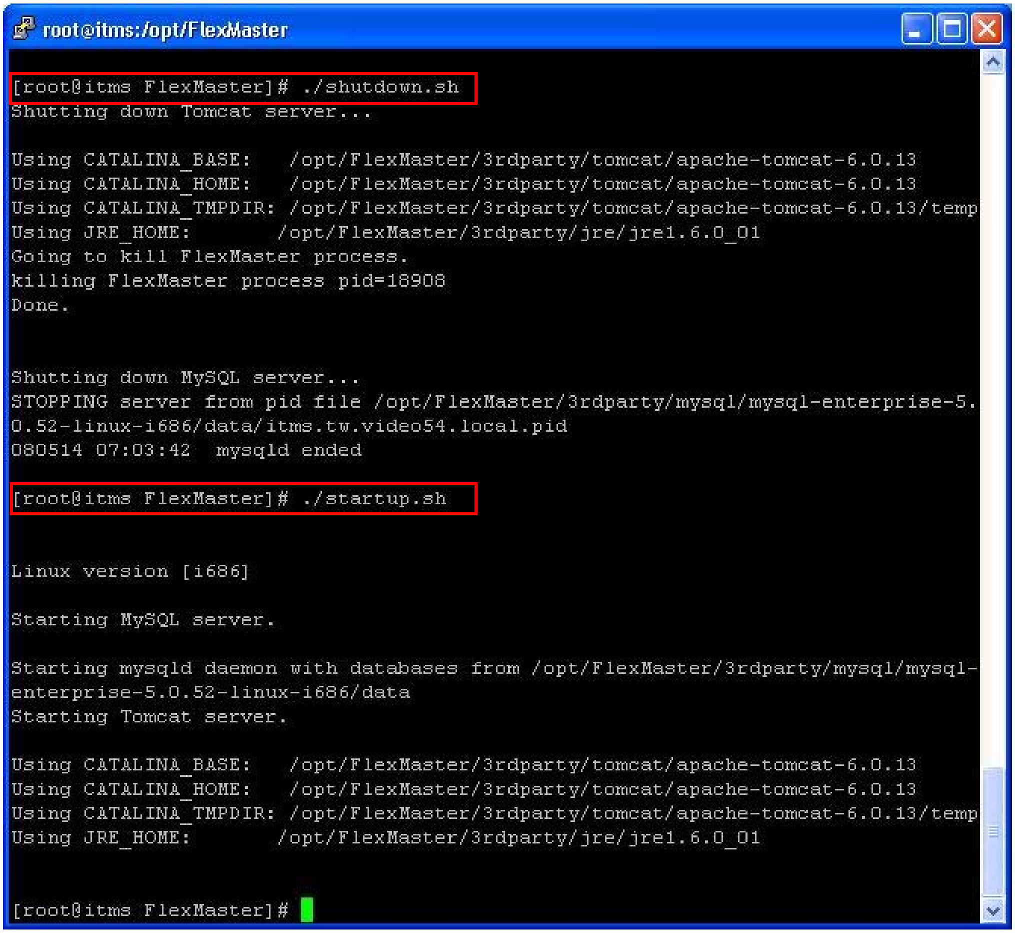
   ```
   Issuer: CN:VeriSign Class 3 Secure Server CA
   ```

   For more information, refer to Viewing the Current Certificates.
8. After you verify that the new certificate has been imported successfully, shut down the FlexMaster service by executing the following script:

   ```
   # /opt/FlexMaster/shutdown.sh
   ```
9. Restart the FlexMaster service by executing the following script:

   ```
   # /opt/FlexMaster/startup.sh
   ```

Figure 173. Shutting down and restarting the FlexMaster service



```
[root@itms FlexMaster]# ./shutdown.sh
Shutting down Tomcat server...

Using CATALINA_BASE:   /opt/FlexMaster/3rdparty/tomcat/apache-tomcat-6.0.13
Using CATALINA_HOME:   /opt/FlexMaster/3rdparty/tomcat/apache-tomcat-6.0.13
Using CATALINA_TMPDIR: /opt/FlexMaster/3rdparty/tomcat/apache-tomcat-6.0.13/temp
Using JRE_HOME:       /opt/FlexMaster/3rdparty/jre/jre1.6.0_01
Going to kill FlexMaster process.
killing FlexMaster process pid=18908
Done.


Shutting down MySQL server...
STOPPING server from pid file /opt/FlexMaster/3rdparty/mysql/mysql-enterprise-5.
0.52-linux-i686/data/itms.tw.video54.local.pid
080514 07:03:42  mysqld ended

[root@itms FlexMaster]# ./startup.sh


Linux version [i686]

Starting MySQL server.

Starting mysqld daemon with databases from /opt/FlexMaster/3rdparty/mysql/mysql-
enterprise-5.0.52-linux-i686/data
Starting Tomcat server.

Using CATALINA_BASE:   /opt/FlexMaster/3rdparty/tomcat/apache-tomcat-6.0.13
Using CATALINA_HOME:   /opt/FlexMaster/3rdparty/tomcat/apache-tomcat-6.0.13
Using CATALINA_TMPDIR: /opt/FlexMaster/3rdparty/tomcat/apache-tomcat-6.0.13/temp
Using JRE_HOME:       /opt/FlexMaster/3rdparty/jre/jre1.6.0_01


[root@itms FlexMaster]#
```

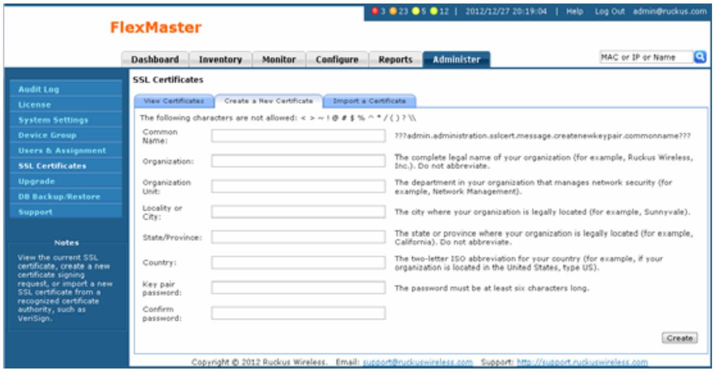
You have completed importing a VeriSign-issued SSL certificate. Try connecting to the FlexMaster Web interface using HTTPS. The security alert should no longer appear.

Creating a Certificate Signing Request File for VeriSign

When you do not have a VeriSign certificate, you need to create a certificate signing request (CSR) file and send it to VeriSign to purchase an SSL certificate. The FlexMaster Web interface provides a form that you can use to create the CSR file.

1. On the *SSL Certificates* page, click the **Create a New Certificate** tab.
2. In the boxes provided, fill in the following information:
   - *Common Name*: Type the fully qualified domain name of your Web server. This must be an exact match (for example, `www.ruckuswireless.com`).
   - *Organization*: Type the complete legal name of your organization (for example, `Ruckus Wireless, Inc.`). Do not abbreviate your organization name.
   - *Organization Unit*: Type the name of the division, department, or section in your organization that manages network security (for example, `Network Management`).
   - *Locality or City*: Type the city where your organization is legally located (for example, `Sunnyvale`).
   - *State/Province*: Type the state or province where your organization is legally located (for example, `California`). Do not abbreviate the state or province name.
   - *Country*: Type the two-letter ISO abbreviation for your country (for example, if your organization is located in the United States, type `US`).
   - *Key pair password*: Type the password that you want to use for the SSL certificate. The key pair password must consist of at least six characters.
   - *Confirm password*: Retype the key pair password to confirm.

Figure 174. Fill in the boxes to create the Certificate Signing Request



SSL Certificates

Notes

View the current SSL certificate, create a new certificate signing request, or import a new SSL certificate from a recognized certificate authority, such as VeriSign.

The following characters are not allowed: < > ~ ! @ # $ % ^ * / ( ) ? \\

Common Name:		???admin.administration.sslcert.message.createnewkeypair.commonname???
Organization:		The complete legal name of your organization (for example, Ruckus Wireless, Inc.). Do not abbreviate.
Organization Unit:		The department in your organization that manages network security (for example, Network Management).
Locality or City:		The city where your organization is legally located (for example, Sunnyvale).
State/Province:		The state or province where your organization is legally located (for example, California). Do not abbreviate.
Country:		The two-letter ISO abbreviation for your country (for example, if your organization is located in the United States, type US).
Key pair password:		The password must be at least six characters long.
Confirm password:		

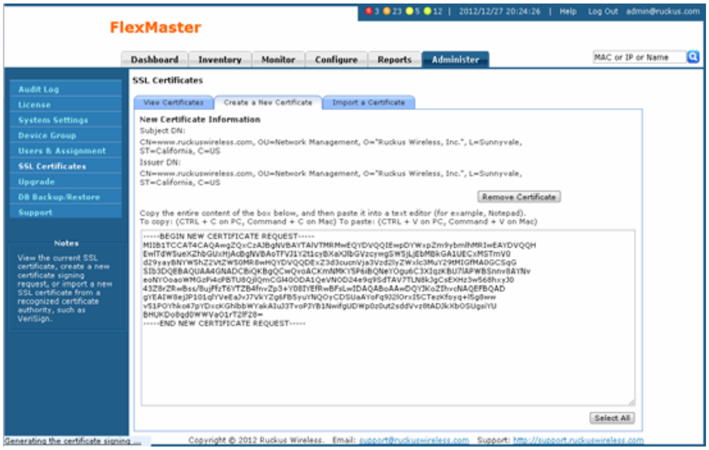
Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

WARNING! Remember the key pair password that you set in this procedure. You need to enter this password when you import the SSL certificate that VeriSign sends you into FlexMaster.

3. Click **Create**. The *New Certificate* page appears, displaying a summary of the certificate information that you entered. If you find any incorrect information or if you want to edit the certificate information, then click *Remove Certificate*, and then go back to Step 1. If the certificate information is correct, then continue to Step 4.

4. Click **Generate CSR**. The page refreshes, and then displays the content of the CSR.

Figure 175. Copy the content of the CSR and save it to a text file



SSL Certificates

New Certificate Information

Subject DN:

CN=www.ruckuswireless.com, OU=Network Management, O="Ruckus Wireless, Inc.", L=Sunnyvale, ST=California, C=US

Issuer DN:

CN=www.ruckuswireless.com, OU=Network Management, O="Ruckus Wireless, Inc.", L=Sunnyvale, ST=California, C=US

Copy the entire content of the box below, and then paste it into a text editor (for example, Notepad).
To copy: (CTRL + C on PC, Command + C on Mac) To paste: (CTRL + V on PC, Command + V on Mac)

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB1TCCAT4CAQAwgZQxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRIwEAYDVQQH
EwlTdW5ueXZhbGUxHjAcBgNVBAoTFVJ1Y2t1cyBXaXJlbGVzcywgSW5jLjEbMBkGA1UECxMSTmV0
d29yayBNYW5hZ2VtZW50MR8wHQYDVQQDExZ3d3cucnVja3Vzd2lyZWxlc3MuY29tMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCwQvoACKmNMKY5P6iBQNeYOgu6C3XIqzKBU7lAPWBSnnv8AYNv
eoNYOoaoWMGzPi4dPBTU8QjlQmCGl40ODA1QeVN0D24e9q9SdTAV7TLN8kJgCsEXHz3w568hxyJ0
43Z8rZRwBss/8ujFfzT6YTZB4fnvZp3+Y08IYEfRwBFsLwIDAQABoAAwDQYJKoZIhvcNAQEFBQAD
gYEAIW8ejJP101qlYVeEaJvJ7VkYZg6FB5yuYNQOyCDSUaAYoFq9J2lOrxI5CTezKfoyq+l5g8ww
v51POYhko47pYDxcKGhlbbWYakAIuJ3TvoPJYB1NwifgUDWp0z0ut2sddVvz8tADJkXbOSUgsiYU
BHUKDo8qd0WWVa01rT2lF28=
-----END NEW CERTIFICATE REQUEST-----
```

Notes

View the current SSL certificate, create a new certificate signing request, or import a new SSL certificate from a recognized certificate authority, such as VeriSign.

Generating the certificate signing ...

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

5. Copy the complete content of the CSR request, and then paste it into a text editor (for example, Notepad). Save the file.

6. Go to the VeriSign Web site and follow the instructions for purchasing an SSL certificate. For more information, visit:

   `www.verisign.com/ssl/buy-ssl-certificates/index.html`

7. When the VeriSign Web site prompts for the certificate signing request, copy and paste the content of the text file that you saved in Step 5, and then complete the certificate purchase.

   After VeriSign approves your CSR, you receive the VeriSign-signed certificate via email. The following is a sample signed certificate that you receive from VeriSign:

```
-----BEGIN CERTIFICATE-----
MIIFVjCCBD6gAwIBAgIQLfaGuqKukMumWhbVf5v4vDANBgkqhkiG9w0BAQUFADCB
sDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
BgEFBQcBAQRtMGswJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlzaWduLmNv
bTBDBggrBgEFBQcwAoY3aHR0cDovL1NWUlNlY3VyZS1haWEudmVyaXNpZ24uY29t
L1NWUlNlY3VyZTIwMDUtYWlhLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFowWDBW
FglpbWFnZS9naWYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEFGDAm
FiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZIhvcN
AQEFBQADggEBAI/S2dmm/kgPeVAlsIHmx751o4oq8+fwehRDBmQDaKiBvVXGZ5ZM
noc3DMyDjx0SrI9lkPsn223CV3UVBZo385g1T4iKwXgcQ7/WF6QcUYOE6HK+4ZGc
HermFf3fv3C1FoCjq+zEu8ZboUf3fWbGprGRA+MR/dDI1dTPtSUG7/zWjXO5jC//
0pykSldW/q8hgO8kq30S8JzCwkqrXJfQ050N4TJtgb/YC4gwH3BuB9wqpRjUahTi
```

```
K1V1ju9bHB+bFkMWIIMIXc1Js62JC1WzwFgaGUS2DLE8xICQ3wU1ez8RUPGnwSxA
YtZ2N7zDxYDP2tEiO5j2cXY7O8mR3ni0C30=
-----END CERTIFICATE-----
```

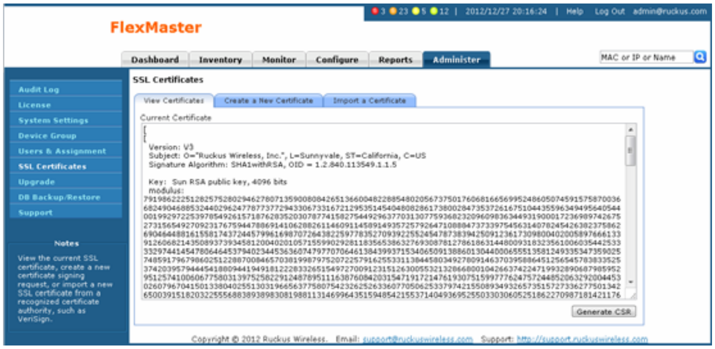
8. Copy the content of the signed certificate, and then paste it into a text file. Save the file.

You can now import the signed certificate from VeriSign into your FlexMaster server. For instructions, refer to Importing an SSL Certificate.

Viewing the Current Certificates

To view the details of the certificate file that FlexMaster is currently using, click the **View Certificates** tab on the *SSL Certificates* page. If you imported a VeriSign-signed SSL certificate, then the current certificate should show VeriSign as the certificate issuer.

Figure 176. The default SSL certificate on FlexMaster



Notes

View the current SSL certificate, create a new certificate signing request, or import a new SSL certificate from a recognized certificate authority, such as VeriSign.

Current Certificate

```
[
[
  Version: V3
  Subject: O="Ruckus Wireless, Inc.", L=Sunnyvale, ST=California, C=US
  Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

  Key:  Sun RSA public key, 4096 bits
  modulus:
791986222512825752802946278071359008084265136600482288548020567375017606816656995248605074591575870036
682490468853244029624778773772943306733167212953514540480828617380028473537261675104435596349495640544
001992972253978549261571876283520307877415827544929637703130775936823209609836344931900017236989742675
273156549270923176759447886914106288261146091145891493572579264710888473733975456314078245426382375862
690464488161558174372445799616987072643822597783527093922552454787383942509123617309800402005897666133
912606821435089373934581200402010571559902928118356538632769308781278618631448009318323561006035442533
332974414547806464537940234453636074797707064613843993715340650913886013044000655513581249335347359025
748591796798602512288700846570381998797520722579162553311384458034927809146370395886451256545783833525
374203957944454188094419491812228332651549727009123151263005532132866800104266374224719932890687985952
951257410060677580313975258229124878951116387608420315471917214761930751599777624757244852063292004453
026079670415013380402551303196656377580754232625263360770506253379742155089349326573515727336277501342
650039151820322555688389389830819881131469964351594854215537140493695255033030605251862270987181421176
```

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Upgrading the FlexMaster Software

Ruckus Wireless may periodically release FlexMaster software updates that contain feature enhancements or fixes for known issues. These software updates are made available on the Ruckus Wireless Support Web site or released through authorized channels.

Update files typically use `{version number}.patch` for their file naming convention (for example, *9.6.0.0.11.patch*).

WARNING! Although the software update process has been designed to preserve all FlexMaster configuration settings, Ruckus Wireless strongly recommends that you back up the FlexMaster database, in case the update process fails for any reason.
For information on how to back up and restore FlexMaster database, refer to the man pages located in `<FlexMaster_installation_directory>/3rdparty/mysql/mysql-enterprise-5.0.52-linux-i686` or the MySQL AB Web documentation located at `http://dev.mysql.com/doc version 5.0`.

NOTE: After you upgrade your FlexMaster server, some of the configuration templates that you created using the previous version may no longer provision successfully. To help ensure successful provisioning, recreate the templates using the new FlexMaster version and delete the old templates.

1. Log in to the host server as root.
2. Insert the FlexMaster upgrade CD into the CD-ROM drive.
3. If the FlexMaster server does not automatically mount the FlexMaster CD-ROM, then continue with Step 4. If the server automatically mounts the CD-ROM, then continue with Step 6.
4. Type the following command to create a mount point (or directory where you want to mount the CD-ROM):

   ```
   # mkdir -p /mnt/cdrom
   ```

5. Type the following command to mount the CD-ROM manually to the created mount point:

   ```
   # mount /dev/cdrom /mnt/cdrom
   ```

6. Upload the patch file (for example, *9.6.0.0.11.patch.tar*) to the FlexMaster server.
7. Copy the patch file to the FlexMaster folder */opt/FlexMaster/*:

   ```
   # cp 9.6.0.0.11.patch.tar /opt/FlexMaster/
   ```

8. Untar the patch file with following command:

   ```
   # tar -vxf 9.6.0.0.11.patch.tar
   ```

9. Make sure that the *{version number}.patch* file, such as *9.6.0.0.11.patch,* has been extracted from the tar file.
10. Upgrade FlexMaster with following command:

    ```
    # ./upgrade.sh 9.6.0.0.11
    ```

WARNING! After installing a software update, Ruckus Wireless recommends backing up the FlexMaster database so you have a backup of the updated database schema. Refer to Backing Up and Restoring the Database from the Web Interface or Backing Up the Database from the Command Line Interface for more information.

11. If the FlexMaster upgrade fails for any reason, then send the upgrade log file, **`/opt/FlexMaster/9.6.0.0.11.patch`**, and the screen dump to Ruckus Wireless Support.

Recovering FlexMaster from an Unsuccessful Software Update

If the software update fails for any reason, then the FlexMaster software update script is designed to automatically recover and restore your previous FlexMaster installation. If the auto restore process also fails, then you can still restore your previous FlexMaster installation manually from the database that you backed up.

To recover your FlexMaster installation manually, do the following:

Step 1: Remove the Unsuccessful FlexMaster Installation

Step 2: Reinstall the Previous FlexMaster Software Version

Step 3: Shut Down the FlexMaster Service

Step 4: Restore the Backup FlexMaster Database

Step 5: Restart the FlexMaster Service

NOTE: To recover FlexMaster from an unsuccessful installation, you must have a backup copy of the FlexMaster database.

Step 1: Remove the Unsuccessful FlexMaster Installation

1. Log in to the FlexMaster server.
2. Execute the FlexMaster uninstall script.

```
# ./uninstall.sh
```

3. After you execute the uninstall script, it performs the following steps:
   a. It shuts down the Tomcat server.
   b. It shuts down the MySQL server.
   c. It deletes the configuration files, and uninstalls the FlexMaster services.
   d. It restores the original `/etc/my.cnf` file.
   e. It finds /etc/my.cnf.ruckus, and then renames it to `/etc/my.cnf`.
   f. Finally, it deletes the `/opt/FlexMaster` directory.

When the uninstall script completes deleting the `/opt/FlexMaster` directory, the uninstallation process is complete.

Step 2: Reinstall the Previous FlexMaster Software Version

Follow the FlexMaster installation instructions described in Installing the FlexMaster Software.

Step 3: Shut Down the FlexMaster Service

After you install the FlexMaster software update, you need to shut down the FlexMaster service in preparation for restoring the backup FlexMaster database. Shut down the FlexMaster service by running the following script in the FlexMaster root directory:

```
# shutdown.sh
```

Step 4: Restore the Backup FlexMaster Database

Before starting this procedure, take note of the file path to the FlexMaster database backup file. You need to enter this file path when you execute the restore script.

Follow these steps to restore a backup copy of the FlexMaster database.

1. On the Linux server, go to the FlexMaster root directory (`/opt/FlexMaster`), where the database restore script is located.
2. Execute the database restore script by entering the following command:

   ```
   # ./restore.sh {file path and file name of the backup file that
   you want to restore}
   ```

   where `{file path and file name of the backup file that you want to restore}` is the file path and name of the FlexMaster database backup file that you want to restore.

   For example, when you want to restore a backup file named `Mybackup.tgz` that is located in the FlexMaster root directory, enter the following command:

   ```
   # ./restore.sh Mybackup.tgz
   ```

When the restore process is completed, a message appears in the command line interface, informing you that the FlexMaster database that you specified has been restored successfully.

Step 5: Restart the FlexMaster Service

Restart the FlexMaster service by running the following script in the FlexMaster root directory:

```
# startup.sh
```

You have completed recovering your previous FlexMaster installation. To verify that the installation was successful, try connecting to the FlexMaster Web interface.

Backing Up and Restoring the Database from the Web Interface

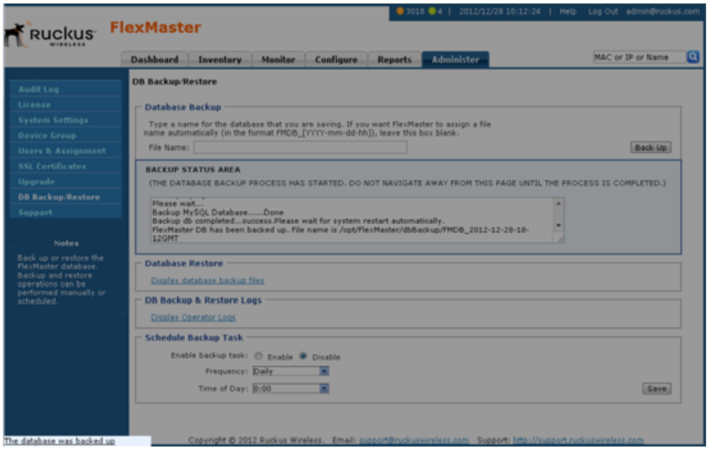
You can also perform database backup from the Web interface. This section describes how to use the Web interface to perform manual and scheduled database backup. It also describes how to restore the FlexMaster database from a backup file.

Backing Up the Database from the Web Interface

CAUTION! This procedure halts the FlexMaster operation. Do not perform this procedure when you need FlexMaster to be operating properly.

1. Go to *Administer > DB Backup/Restore.*
2. Look for the *Database Backup* section.
3. In *File Name*, type a name that you want to assign to the backup file. When you want FlexMaster to automatically assign a file name (in the format `FMDB_[YYYY-mm-dd-hh].tgz`), skip this step.
4. Click **Back Up**. The Backup Status Area window appears and displays the progress of the backup process.

Figure 177. The Backup Status Area shows the progress of the backup process



Back up or restore the FlexMaster database. Backup and restore operations can be performed manually or scheduled.

DB Backup/Restore

Database Backup

Type a name for the database that you are saving. If you want FlexMaster to assign a file name automatically (in the format FMDB_[YYYY-mm-dd-hh]), leave this box blank.

File Name:

Back Up

BACKUP STATUS AREA

(THE DATABASE BACKUP PROCESS HAS STARTED. DO NOT NAVIGATE AWAY FROM THIS PAGE UNTIL THE PROCESS IS COMPLETED.)

```
Please wait...
Backup MySQL Database......Done
Backup db completed...success.Please wait for system restart automatically.
FlexMaster DB has been backed up. File name is /opt/FlexMaster/dbBackup/FMDB_2012-12-28-18-
12GMT
```

Database Restore

Display database backup files

DB Backup & Restore Logs

Display Operator Logs

Schedule Backup Task

Enable backup task: ○ Enable ● Disable

Frequency: Daily

Time of Day: 0:00

Save

The database was backed up

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

5. Check the Backup Status Area window for the following message:

```
FlexMaster DB has been backed up. File name is /opt/FlexMaster/
dbBackup/{FM-database-file-name}.tgz
```

6. Click the **HIDE STATUS** link.

You have completed backing up the FlexMaster database.

CAUTION! Do not navigate away from the *DB Backup/Restore* page while the backup process is in progress. Doing so cancels the backup process. Wait for the Backup Status window to display the message that the process is complete.

Scheduling Database Backup

You can also configure FlexMaster to back up its database automatically based on a schedule that you set.

1. Go to *Administer > DB Backup/Restore.*
2. Look for the *Schedule Backup Task* section.
3. In *Enable backup task*, click **Enable**.
4. In *Frequency*, specify how often you want FlexMaster to automatically back up the database. Options include **Daily**, **Weekly**, and **Monthly**.
5. Configure additional options for the *Frequency* option that you clicked.
   - If you clicked **Daily**, then set the *Time of Day* when you want FlexMaster to back up the database.
   - If you clicked **Weekly**, then set the *Day of the Week* and *Time of Day* when you want FlexMaster to back up the database.
   - If you clicked **Monthly**, then set the *Day of the Month* and *Time of Day* when you want FlexMaster to back up the database.
6. Click **Save**.

You have completed configuring FlexMaster to back up its database automatically.

Viewing and Deleting Database Backup Files

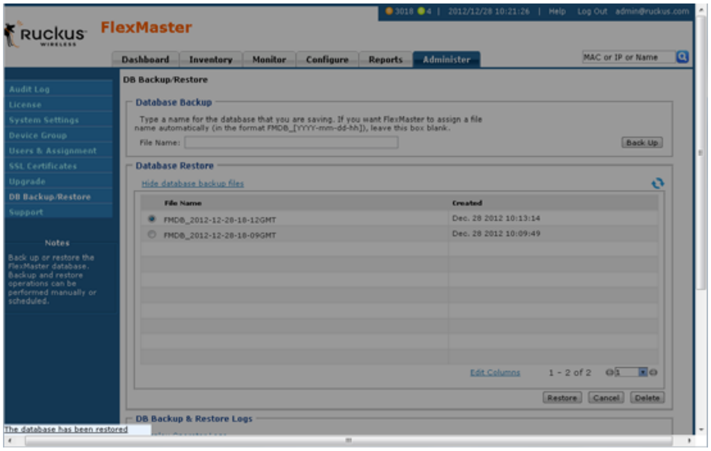
1. Go to *Administer > DB Backup/Restore.*
2. Look for the *Database Restore* section.
3. Click the **Display database backup files** link. A table appears, displaying the file names of the database backup files and the dates when they were created.
4. To delete a database backup file, click the option button next to the database file name, and then click **Delete**.

Restoring a Backup Copy of the Database

1. Go to *Administer > DB Backup/Restore.*
2. Look for the *Database Restore section.*
3. Click the **Display database backup files** link. A table appears and displays the file names of the database backup files and the dates when they were created.
4. Click the option button next to the database file name that you want to restore.

5. Click **Restore**. The *Restore Status Area* window appears and displays the progress of the restore process.

Figure 178. The Restore Status Area shows the progress of the restore process



DB Backup/Restore

Database Backup

Type a name for the database that you are saving. If you want FlexMaster to assign a file name automatically (in the format FMDB_[YYYY-mm-dd-hh]), leave this box blank.

File Name:

Database Restore

	File Name	Created
●	FMDB_2012-12-28-18-12GMT	Dec. 28 2012 10:13:14
○	FMDB_2012-12-28-18-09GMT	Dec. 28 2012 10:09:49

DB Backup & Restore Logs

Notes

Back up or restore the FlexMaster database. Backup and restore operations can be performed manually or scheduled.

The database has been restored

6. Check the *Restore Status Area* window for the following message:

```
restore db completed...success. Please wait for system restart
automatically.
```

```
FlexMaster DB has been restored with {FM-database-file-name}.tgz
```

7. Wait for the FlexMaster login page to appear.

When the login page appears, you have completed restoring the backup database.

Generating Support Information

When you request technical support from Ruckus Wireless, you may be asked to collect information about FlexMaster that may help Ruckus Wireless troubleshoot the issue. You need to generate system logs.

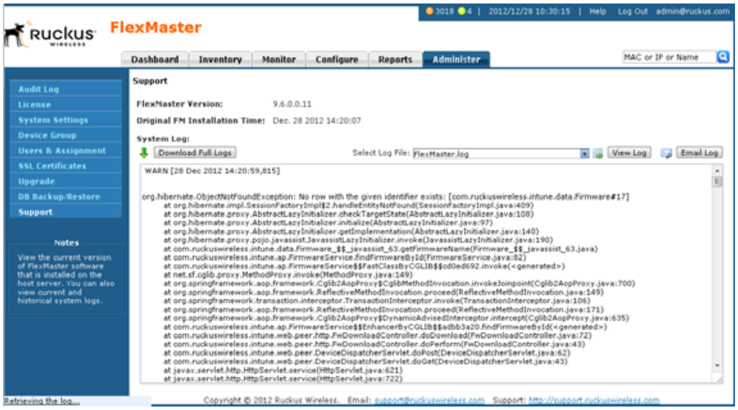
The System Log is a low level system server log which is useful to support personnel.

Viewing System Logs

The system log captures information in 12-hour sets. After 12 hours, the "expired" log is backed up and a new log is started. This log rotation prevents the system log from becoming too long. New logs start at midnight (12:00 AM or 0:00) and midday (12:00 PM).

1. Go to *Administer* > *Support.*
2. In *Select Log File*, select the required log file.
3. Click **View Log**. The log displays information from either midnight to the current time or midday to current time.

Figure 179. Viewing a system log file



View the current version of FlexMaster software that is installed on the host server. You can also view current and historical system logs.

Support

FlexMaster Version: 9.6.0.0.11

Original FM Installation Time: Dec. 28 2012 14:20:07

System Log:

Select Log File: FlexMaster.log

```
WARN [28 Dec 2012 14:20:59,815]


org.hibernate.ObjectNotFoundException: No row with the given identifier exists: [com.ruckuswireless.intune.data.Firmware#17]
	at org.hibernate.impl.SessionFactoryImpl$2.handleEntityNotFound(SessionFactoryImpl.java:409)
	at org.hibernate.proxy.AbstractLazyInitializer.checkTargetState(AbstractLazyInitializer.java:108)
	at org.hibernate.proxy.AbstractLazyInitializer.initialize(AbstractLazyInitializer.java:97)
	at org.hibernate.proxy.AbstractLazyInitializer.getImplementation(AbstractLazyInitializer.java:140)
	at org.hibernate.proxy.pojo.javassist.JavassistLazyInitializer.invoke(JavassistLazyInitializer.java:190)
	at com.ruckuswireless.intune.data.Firmware_$$_javassist_63.getFirmwareName(Firmware_$$_javassist_63.java)
	at com.ruckuswireless.intune.ap.FirmwareService.findFirmwareById(FirmwareService.java:82)
	at com.ruckuswireless.intune.ap.FirmwareService$$FastClassByCGLIB$$cd0ed692.invoke(<generated>)
	at net.sf.cglib.proxy.MethodProxy.invoke(MethodProxy.java:149)
	at org.springframework.aop.framework.Cglib2AopProxy$CglibMethodInvocation.invokeJoinpoint(Cglib2AopProxy.java:700)
	at org.springframework.aop.framework.ReflectiveMethodInvocation.proceed(ReflectiveMethodInvocation.java:149)
	at org.springframework.transaction.interceptor.TransactionInterceptor.invoke(TransactionInterceptor.java:106)
	at org.springframework.aop.framework.ReflectiveMethodInvocation.proceed(ReflectiveMethodInvocation.java:171)
	at org.springframework.aop.framework.Cglib2AopProxy$DynamicAdvisedInterceptor.intercept(Cglib2AopProxy.java:635)
	at com.ruckuswireless.intune.ap.FirmwareService$$EnhancerByCGLIB$$adbb3a20.findFirmwareById(<generated>)
	at com.ruckuswireless.intune.web.peer.http.FwDownloadController.doDownload(FwDownloadController.java:72)
	at com.ruckuswireless.intune.web.peer.http.FwDownloadController.doPerform(FwDownloadController.java:43)
	at com.ruckuswireless.intune.web.peer.DeviceDispatcherServlet.doPost(DeviceDispatcherServlet.java:62)
	at com.ruckuswireless.intune.web.peer.DeviceDispatcherServlet.doGet(DeviceDispatcherServlet.java:43)
	at javax.servlet.http.HttpServlet.service(HttpServlet.java:621)
	at javax.servlet.http.HttpServlet.service(HttpServlet.java:722)
```

Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

Downloading System Logs

1. Go to *Administer* > *Support.*
2. Click **Download Full Logs**.

   FlexMaster zips all the existing log files and downloads the `fm_logs.zip` file to your client workstation.

NOTE: If the FlexMaster web page is not available, please retrieve the log file from `/opt/FlexMaster/3rdparty/tomcat/apache-tomcat-6.0.18/webapps/intune/WEB-INF/logs/`. Backed-up logs appear as (midnight) *FlexMaster.log.yyyy-mm-dd-AM* or (midday) *FlexMaster.log.yyyy-mm-dd-PM*.

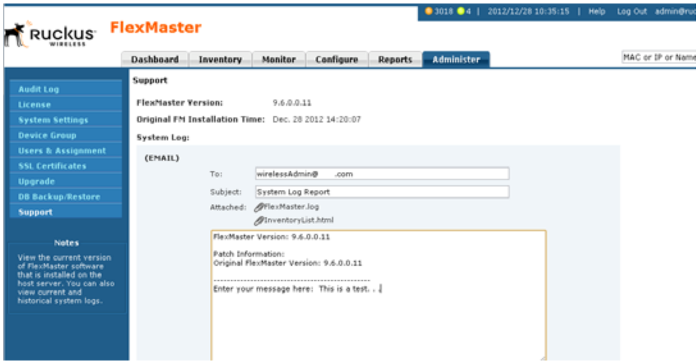
Emailing a Copy of the System Log File

1. Go to *Administer* > *Support.*
2. Click the **Email Log** button. The *System Log* form appears.

   The *To* and *Subject* fields are filled out, and the system log has been added as attachment.

   The *To* address must be previously configured in the System Settings. [Configuring System Settings]()
3. Type any information you want to highlight in the message box.
4. Click **Send** to send the email message.

Figure 180. Sending the system log via email



Support

FlexMaster Version: 9.6.0.0.11

Original FM Installation Time: Dec. 28 2012 14:20:07

System Log:

(EMAIL)

To: wirelessAdmin@ .com

Subject: System Log Report

Attached: FlexMaster.log
InventoryList.html

```
FlexMaster Version: 9.6.0.0.11

Patch Information:
Original FlexMaster Version: 9.6.0.0.11

-----------------------------------------------
Enter your message here:  This is a test. .
```

Notes

View the current version of FlexMaster software that is installed on the host server. You can also view current and historical system logs.

NOTE: If the FlexMaster web page is not available, please send the log file from `/opt/FlexMaster/3rdparty/tomcat/apache-tomcat-6.0.18/webapps/intune/WEB-INF/logs/`. Backed-up logs appear as (midnight) *FlexMaster.log.yyyy-mm-dd-AM* or (midday) *FlexMaster.log.yyyy-mm-dd-PM.*

Manually Transferring Files

There may be times when you would like to manually transfer log and other files between a Windows workstation and a FlexMaster server. Ruckus Wireless recommends that you use a free Windows file transfer tool, *WinSCP*, or equivalent to simplify the file transfers. WinSCP can be downloaded from http://winscp.net/eng/download.php and installed on your Windows workstation.

To transfer files to the Windows workstation:

1. Launch WinSCP and log in with the following selections:
   - *File Protocol:* **SFTP**, **SCP** or **FTP**
   - *Encryption:* **None, SSL/TLS Implicit, SSL Explicit** or **TLS Explicit**
   - *Host Name*
   - *Port number*
   - *User name*
   - *Password*
   - *Account*
   - *Anonymous login*
2. In the WinSCP window, find the required files and transfer them to the Windows workstation.

   The most common FlexMaster log files are:
   - `/opt/FlexMaster/<version number>.patch.log`
   - `/opt/FlexMaster/install.log`
   - `/opt/FlexMaster/3rdparty/tomcat/apache-tomcat-<version>/webapps/intune/WEB-INF/logs/FlexMaster.log`
   - `/opt/FlexMaster/3rdparty/tomcat/apache-tomcat-<version>/webapps/intune/WEB-INF/logs/Intune.log`
   - `/tmp/<ZD log file name>.xml`
   - `/opt/FlexMaster/3rdparty/tomcat/httpshellproxy/logs/<logname>.log`
   - `/opt/FlexMaster/3rdparty/tomcat/apache-tomcat-<version>/webapps/intune/WEB-INF/ZDWebUtils/instances/$<instance_port_number>/webs.log`

After you have transferred the file(s), you can use them as directed by Ruckus Wireless. Support.

Index

Simply Better Wireless.

350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com