



# **Ruckus Wireless™ FlexMaster™ 9.1**

## User Guide

Part Number 800-70303-001  
Published December 2010

[www.ruckuswireless.com](http://www.ruckuswireless.com)



# Contents

## About This Guide

### 1 Introducing Ruckus Wireless FlexMaster

Overview of Ruckus Wireless FlexMaster .....	2
FlexMaster Management Software and Server .....	2
FlexMaster Time .....	2
Management Protocol .....	3
Internet Accessibility .....	3
Potential Conflict with Ruckus Wireless ZoneDirector .....	3
How FlexMaster Communicates with Managed Devices .....	4
Directly Accessible Method .....	4
L2TP Tunneling Method .....	4
Where Should You Place FlexMaster? .....	5
Deployment Scenarios .....	5
Service Provider Scenario .....	5
Hotspot Scenario .....	7
Key Terms in FlexMaster .....	8

### 2 Installing FlexMaster

Preparing Your Server for FlexMaster Installation .....	12
What You Will Be Doing .....	12
Server System Requirements .....	12
Web Browser Requirements .....	13
Ensuring That APs Can Connect to FlexMaster .....	14
Option 1: Register FlexMaster with a DNS Server .....	14
Option 2: Customize Your DHCP Server .....	14
Option 3: Set the FlexMaster Server URL Manually from the Device View .....	19
Editing the Server Hosts File .....	20
Installing the FlexMaster Software .....	21
Mounting the FlexMaster CD-ROM Manually .....	27
Notable Files in the FlexMaster Root Directory .....	29

Upgrading the FlexMaster Software .....	29
Uninstalling FlexMaster .....	30
Backing Up the Database from the Command Line Interface .....	30
Restoring the Database from the Command Line Interface .....	31
What's Next? .....	32

### 3 Getting Started with FlexMaster

Logging into FlexMaster .....	34
Features of the FlexMaster Web Interface .....	36
Getting to Know the Dashboard and Its Widgets .....	38
Widgets That You Can Display .....	39
Available Widget Slots .....	50
Default Widgets .....	50
Adding a Widget .....	51
Hiding a Widget .....	52
Deleting a Widget .....	52
Getting Started Tasks .....	53
Changing the Default Password .....	53
Pointing Your Ruckus Wireless AP to FlexMaster .....	54
Checking Your FlexMaster License .....	57
Configuring Your Devices to Communicate with FlexMaster over L2TP .....	58

### 4 Working with Device Inventory

About the Inventory Page .....	64
ZoneDirector Inventory Pages .....	64
Standalone APs Inventory Pages .....	66
Client Inventory Pages .....	68
Text View and Map View .....	70
Working with ZoneDirector Inventory .....	72
Viewing a Summary of ZoneDirector Devices .....	72
Searching for ZoneDirector Devices .....	73
Editing ZoneDirector Details .....	75
Viewing APs That Report to a ZoneDirector Device .....	76
Viewing Mesh Connections .....	77
Creating a ZD View .....	78
Managing ZD Views .....	79

Working with Standalone AP Inventory .....	83
Viewing a Summary of Standalone APs .....	83
Searching for APs .....	83
Editing AP Details .....	86
Creating an AP View .....	87
Managing AP Views .....	88
Working with Client Inventory .....	91
Viewing a Summary of Clients .....	91
Searching for Clients .....	92
Creating a Client View .....	95
Managing Client Views .....	96

## 5 Managing a Single Standalone Access Point

About the Device View .....	100
Device View for ZoneDirector .....	101
Device View Tabs .....	101
Viewing Device Summary .....	103
Viewing and Editing Device Details .....	105
Configuring Replacement Options for ZoneFlex 7731 Wireless Bridge .....	107
Performing Device Diagnostics .....	108
Running a Ping Test .....	108
Viewing the Device Log .....	108

## 6 Monitoring Events and Network Activities

About the Monitor Page .....	114
Monitoring Events .....	114
Searching for Events .....	114
Creating an Event View .....	117
Managing Event Views .....	119
Editing an Event View .....	119
Deleting an Event View .....	120
Viewing the Event Timeline .....	120
Configuring Alert Properties .....	124
Disabling an Alert .....	125
Measuring Throughput Using SpeedFlex .....	126
Creating a SpeedFlex Task .....	126

Running a SpeedFlex Task .....	127
Editing a SpeedFlex Test .....	128
Deleting a SpeedFlex Test .....	128
Monitoring Clients .....	129

## 7 Provisioning Tasks to Managed Devices

About Provisioning Tasks .....	132
Provisioning Conventions and Recommended Practices .....	132
Understanding the Status of a Task .....	133
Provisioning Tasks to Standalone APs .....	135
Working with AP Configuration Templates .....	135
Performing an AP Configuration Upgrade .....	145
Performing an AP Factory Reset .....	151
Creating an Auto Configuration Task .....	154
Provisioning Tasks to ZoneDirector Devices .....	162
Working with ZoneDirector Configuration Templates .....	162
Working with ZoneDirector Event Configuration .....	164
Performing a ZoneDirector Configuration Upgrade .....	169
Backing Up and Restoring ZoneDirector Configuration .....	170
Provisioning Common Tasks .....	174
Working with Device Firmware .....	174
Working with Reboot Tasks .....	178
Managing Firmware Files .....	180
Managing Device Registration .....	182
Uploading a Device Inventory File .....	187
Configuring VLAN Settings .....	191
Before You Begin .....	191
Configuration Rules .....	192
General Configuration Procedures .....	192
Sample Scenario .....	193
Configuring the Hotspot Feature on ZoneFlex 2942 .....	196
Before You Begin .....	196
Configuring Basic Hotspot Settings .....	197
Configuring the Walled Garden .....	199
Specifying Unrestricted Clients .....	200
Configuring Advanced Settings .....	202
Setting Device Information for the RADIUS Accounting Server .....	204

## 8 Working with Reports

Available Report Types	208
Generating a Device View Report	209
Generating an Active Firmware Report	212
Generating a Historical Connectivity Report	214
Generating an Association Report	217
Generating a Provision Report	219
Generating Events-related Reports	221
Generating an Events Report	221
Generating an Event Timeline Report	223
Generating a Detailed Events Report	226
Generating an Event Plot Report	228
Generating a SpeedFlex Report	230
Generating a Capacity Report	232
Generating an SLA Report	234
Generating a Troubleshooting Report	236
Generating a PCI Report	238
Hiding and Showing Columns in Reports	240
Using Advanced Report Options	241
Managing Saved Reports	243
Query a Report	243
Edit a Report	244
Delete a Report	244

## 9 Performing Administrative Tasks

About the Administer Tab	245
Viewing Audit Logs	245
Managing FlexMaster Licenses	248
Uploading a License File	249
Configuring System Settings	250
Language Settings	251
Google Maps Settings	252
Task Restart Settings	252
Memory Optimization Settings	252
Dashboard Settings	253
SMTP Settings	253

Purge Policy .....	254
Managing Users .....	255
Understanding User Roles and Privileges .....	255
Creating a New User Account .....	257
Editing a User Account .....	258
Deleting a User Account .....	259
Assigning Users to Manage Device Groups .....	260
Step 1: Create a User Account .....	260
Step 2: Create a Managed Group .....	261
Step 3: Assign Devices to the Managed Group .....	262
Step 4: Assign a User to Manage the Group .....	263
Managing SSL Certificates .....	264
Importing an SSL Certificate .....	265
Creating a Certificate Signing Request File for VeriSign .....	267
Viewing the Current Certificate .....	269
Upgrading FlexMaster Software .....	270
Recovering FlexMaster from an Unsuccessful Software Update .....	271
Backing Up and Restoring the Database from the Web Interface .....	273
Backing Up the Database from the Web Interface .....	273
Scheduling Database Backup .....	274
Viewing and Deleting Database Backup Files .....	275
Restoring a Backup Copy of the Database .....	275
Generating Support Information .....	276
Generating System Logs .....	276

## Index



# About This Guide

This guide describes how to install, configure, and manage the Ruckus Wireless™ FlexMaster™ version 9.1. 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:** If 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

[Table 1](#) and [Table 2](#) 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]>
<b>monospace bold</b>	Represents information that you enter	[Device name]> <b>set ipaddr 10.0.0.12</b>
<b>default font bold</b>	Keyboard keys, software buttons, and field names	On the <b>Start</b> menu, click <b>All Programs</b> .
<i>italics</i>	Screen or page names	Click <b>Advanced Settings</b> . The <i>Advanced Settings</i> page appears.

Table 2. Notice Conventions

Icon	Notice Type	Description
	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:

[docs@ruckuswireless.com](mailto:docs@ruckuswireless.com)

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 User Guide
- Part number: 800-70260-001 rev 001
- Page 88

## Introducing Ruckus Wireless FlexMaster

### In This Chapter

<a href="#">Overview of Ruckus Wireless FlexMaster</a> .....	2
<a href="#">FlexMaster Management Software and Server</a> .....	2
<a href="#">How FlexMaster Communicates with Managed Devices</a> .....	4
<a href="#">Where Should You Place FlexMaster?</a> .....	5
<a href="#">Deployment Scenarios</a> .....	5
<a href="#">Key Terms in FlexMaster</a> .....	8

## Overview of Ruckus Wireless FlexMaster

The Ruckus Wireless FlexMaster software is an intelligent, scalable network management system designed to facilitate the 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://flex-master/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 Red Hat Linux-based server. FlexMaster installation includes Web server and MySQL database components for communication with and tracking of your dispersed Ruckus Wireless devices.

For more on FlexMaster installation, see [“Installing the FlexMaster Software”](#).

## 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 FlexMaster server time is not synchronized with the local time, scheduled tasks may not run when expected. To ensure that scheduled tasks run exactly 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](http://www.dslforum.org)).

## Internet Accessibility

FlexMaster requires an Internet-accessible interface to:

- *Be managed from a remote computer.* 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. If 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, see [“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](http://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 Ruckus Wireless ZoneDirector is detected on the network, a FlexMaster-managed AP will stop communicating with FlexMaster and register instead with ZoneDirector. If this same AP gets provisioned with a firmware or configuration upgrade from FlexMaster, the task status will appear as “Started” (pending) on the task status page as FlexMaster cannot contact the AP. If the AP registers with ZoneDirector, FlexMaster will display the status of the AP being managed by “ZD” on the **Configure > Device Registration** page.

## How FlexMaster Communicates with Managed Devices

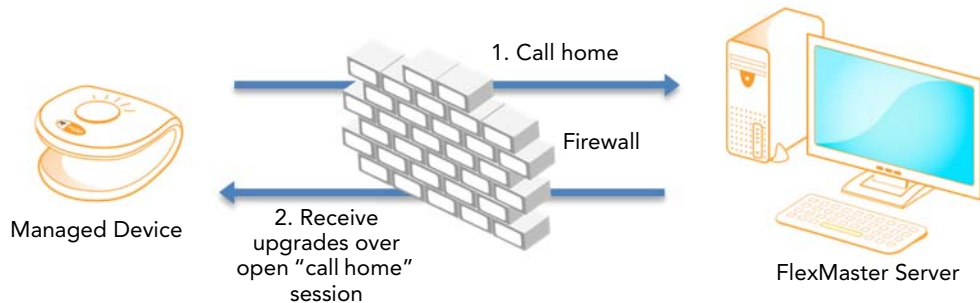
There are two methods by which FlexMaster can communicate with the devices that it manages. These are:

- Directly Accessible Method, and;
- 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 be 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.

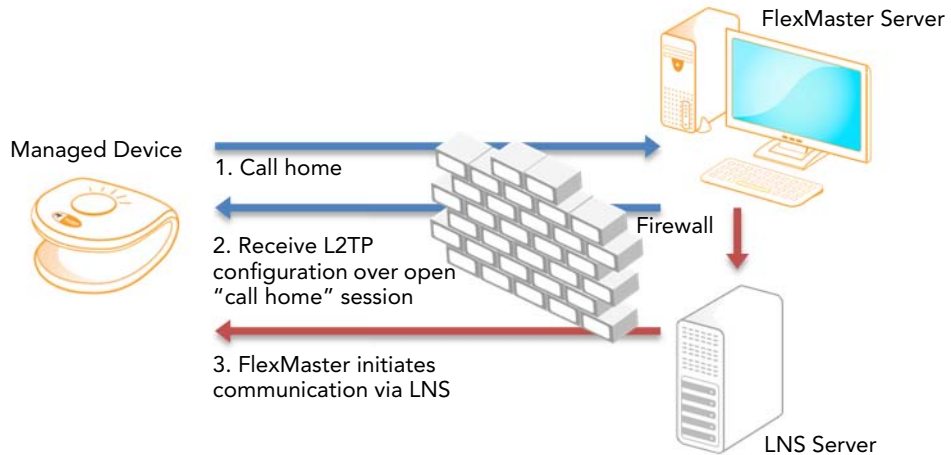
Figure 1. How a managed device calls home directly to FlexMaster



### L2TP Tunneling Method

The FlexMaster connection initiation mechanism relies on the managed Ruckus Wireless AP having a routable IP address. If 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), 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, see [“Configuring Your Devices to Communicate with FlexMaster over L2TP”](#).

Figure 2. How a managed device calls home to FlexMaster via an 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. See ["Option 1: Register FlexMaster with a DNS Server"](#).

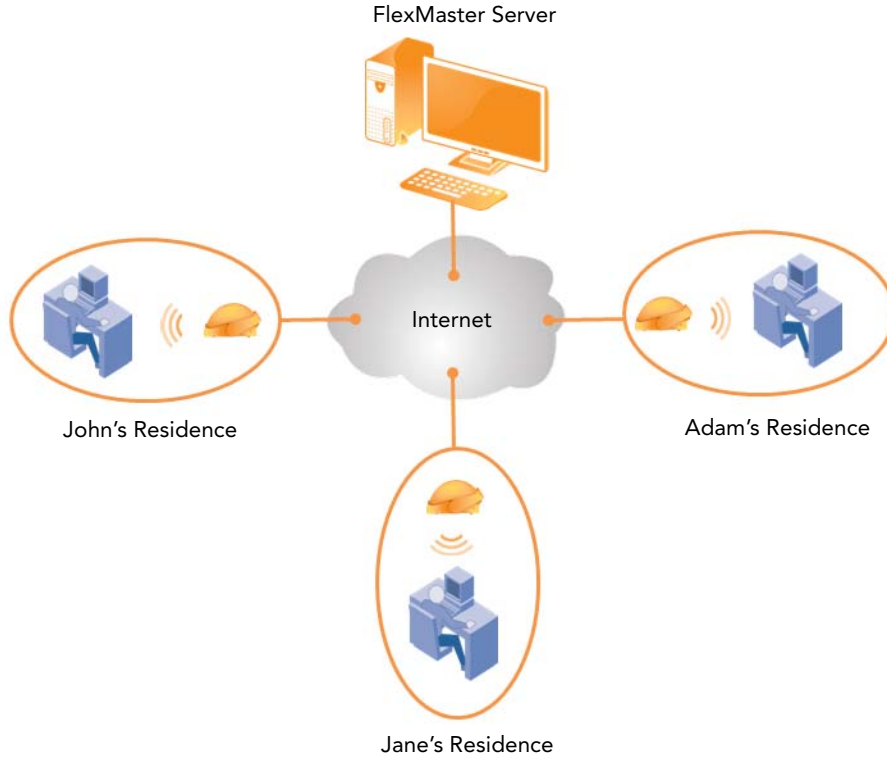
## Deployment Scenarios

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 FlexMaster 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 configuration to be pushed to the device when it registers after boot up.

Figure 3. Service provider scenario

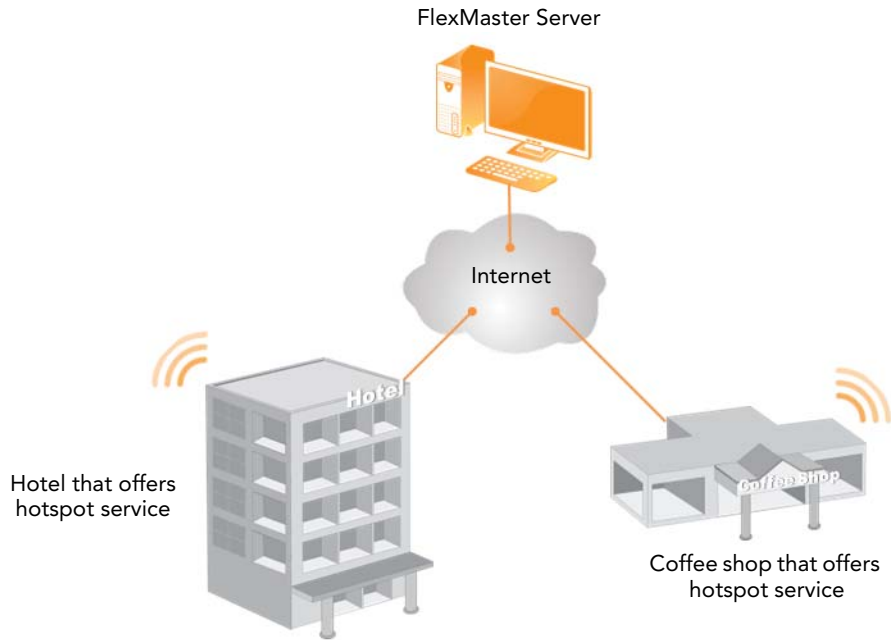




## Hotspot Scenario

Hotspots such as hotels and coffee shops offering wireless service can utilize 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.

Figure 4. Hotspot scenario



## 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. [Table 1](#) lists terms that are key to full understanding and proper use of FlexMaster.

Table 1. Key terms in FlexMaster

Term	Description
Call Home	Upon 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	<p><i>Device View:</i> Since FlexMaster manages many devices, you can consolidate devices with similar attributes into views. <i>Device views</i> are a powerful component within FlexMaster. Devices that are grouped into views can be:</p> <ul style="list-style-type: none"><li>• Provisioned as one</li><li>• Consolidated in reports</li><li>• Quickly recalled to filter a list</li></ul> <p>The grouping attributes are user customizable, and may include device type, geographic location, or any other quality that you want to use as grouping criterion.</p> <p>By default, FlexMaster includes two pre-configured device views: <i>All Standalone APs</i> and <i>All ZoneDirectors</i>. <i>All Standalone APs</i> is a snapshot of all APs currently managed by FlexMaster. <i>All ZoneDirectors</i> is a snapshot of all ZoneDirector devices that are currently managed by FlexMaster.</p> <p>Much like device views, Event Views can be created to quickly reference a list of events as filtered using the <b>Monitor &gt; Events &gt; New Search</b> tab options.</p> <p>You can also create an Audit View, which groups audit log results based on the options in <b>Administer &gt; Audit Log &gt; New Search</b>.</p>

Table 1. Key terms in FlexMaster

Term	Description
Device Registration	<p>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, go to the <b>Configure &gt; Device Registration</b> page.</p> <p>The Device Registration option also enables you to pre-load a device inventory file prior to 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, MAC address), as well as automatically permit or deny registration with FlexMaster.</p> <p>For more on device registration, see <a href="#">"Managing Device Registration"</a>.</p>
Periodic Inform Interval	<p>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, 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.</p> <p>To set this interval, see <a href="#">"Performing an AP Configuration Upgrade"</a>.</p>
Provisioning	<p>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.</p> <p>For more on provisioning, see <a href="#">"Provisioning Tasks to Managed Devices"</a>.</p>
Device View	<p>A dynamic group of devices filtered based on a specific criterion (for example, model number, partial serial number, etc.). Device Views should not to be confused with <i>Device Groups</i>, which refers to a physical grouping of devices typically used for assigning devices for management by users.</p>

Table 1. Key terms in FlexMaster

Term	Description
Tag	<p>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.</p> <p>You can set a tag by editing the device details on the <b>Inventory</b> page.</p>
Default Mail to:	<p>This phrase refers to the email address which will be sent messages from the system based on various events. You enter this email address either during the FlexMaster installation procedure or in the <b>To</b> field on the <b>Administer &gt; System Settings &gt; SMTP Settings</b> page.</p> <p>You must specify an SMTP server to send email notifications to this user. See <a href="#">"SMTP Settings"</a>.</p>

# Installing FlexMaster

## In This Chapter

<a href="#">Preparing Your Server for FlexMaster Installation</a> .....	12
<a href="#">Ensuring That APs Can Connect to FlexMaster</a> .....	14
<a href="#">Editing the Server Hosts File</a> .....	20
<a href="#">Installing the FlexMaster Software</a> .....	21
<a href="#">Notable Files in the FlexMaster Root Directory</a> .....	29
<a href="#">Upgrading the FlexMaster Software</a> .....	29
<a href="#">Uninstalling FlexMaster</a> .....	30
<a href="#">Backing Up the Database from the Command Line Interface</a> .....	30
<a href="#">Restoring the Database from the Command Line Interface</a> .....	31
<a href="#">What's Next?</a> .....	32




---

**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.

---

# 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 Red Hat 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 server on which to install FlexMaster, you need to consider the number of devices that your FlexMaster installation will be managing. 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: Red Hat Linux Enterprise Edition 5.0 or later
- HDD: 160GB of disk space dedicated to FlexMaster
- CD-ROM device if you choose to use this method of installation
- Mouse
- Network adapter



**WARNING!** To ensure that FlexMaster operations run smoothly, make sure that the target Linux server has at least 160 GB of free disk space dedicated to FlexMaster. If FlexMaster does not have sufficient disk space, the MySQL server for FlexMaster may encounter errors.

---



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

---

## Minimum Recommended RAM and CPU

The amount of memory and CPU power required on the server on which you will be installing FlexMaster depends on the number of ZoneDirector devices and standalone APs that FlexMaster will be managing. Refer to [Table 2](#) for the minimum recommended RAM and CPU for managing ZoneDirector devices.

Table 2. Minimum recommended RAM and CPU for managing ZoneDirector devices

Managed Population	Minimum RAM	Minimum CPU
Less than 25 ZoneDirector devices with up to 1,000 managed APs	4GB	2.5GHz Core 2 Intel® Xeon® E5420 or equivalent
25 to 50 ZoneDirector devices with 1,000 to 10,000 managed APs	8GB	2.5GHz Core 2 Intel® Xeon® E5420 or equivalent
More than 50 ZoneDirector devices with more than 10,000 managed APs	16GB	2.5GHz Quad Core Intel® Xeon® E5420 or equivalent

If FlexMaster will only be managing standalone APs, the minimum recommended RAM and CPU are listed in [Table 3](#).

Table 3. Minimum recommended RAM and CPU for managing standalone APs

Managed Population	Minimum RAM	Minimum CPU
Less than 1,000 standalone APs	4GB	2.5GHz Core 2 Intel® Xeon® E5420 or equivalent
More than 1,000 standalone APs	8GB	2.5GHz Quad Core Intel® Xeon® E5420 or equivalent

## Web Browser Requirements

To access the FlexMaster Web interface, you will need to use one of the following Web browsers:

- Microsoft Internet Explorer® 7.0 and later
- Mozilla® Firefox® 3.0 and later
- Google Chrome

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, FlexMaster’s IP address must be reachable via HTTP or HTTPS from outside of 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, 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 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, the procedure may be different. Refer to your DHCP server’s documentation for the relevant information.

---

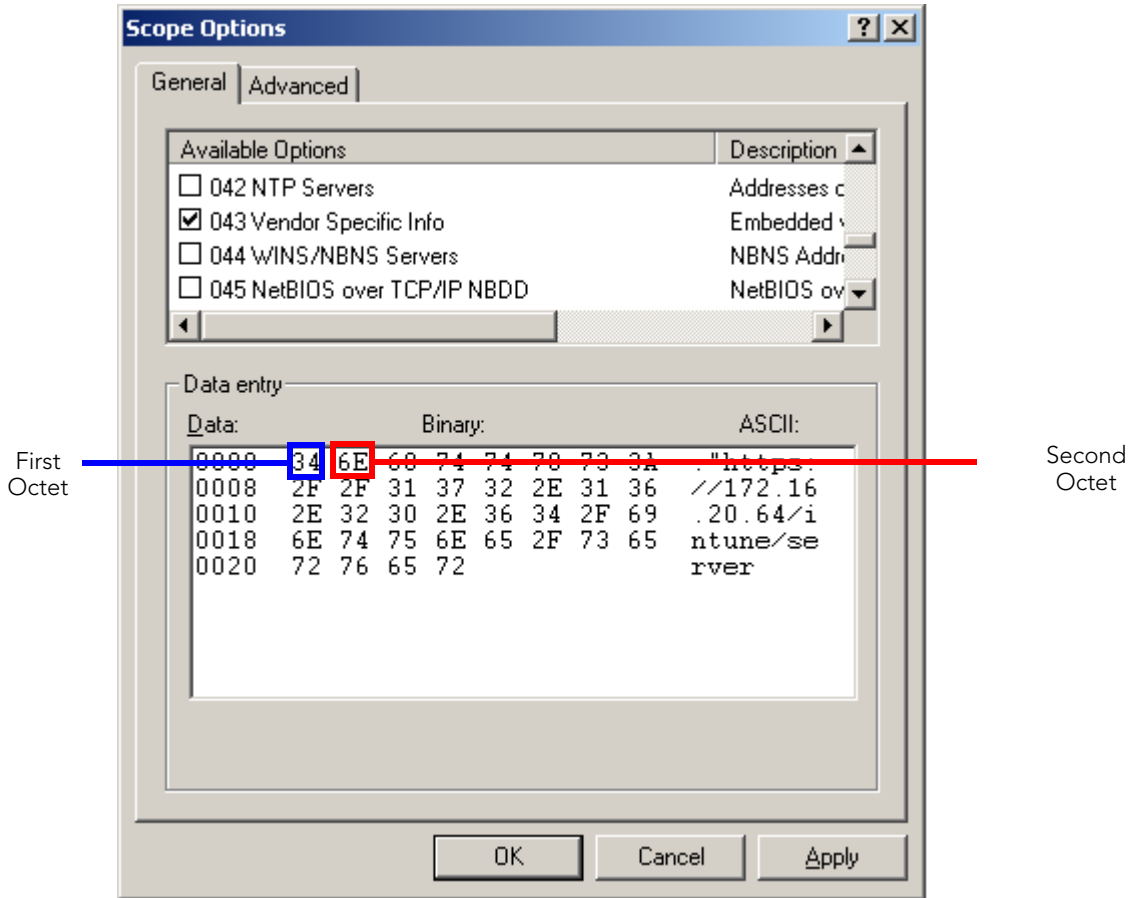
#### To customize your DHCP server

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, 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 (see [Figure 5](#)), and then type 01.

Figure 5. Selecting the first and second octets



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`, 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 value is equivalent to 18 in hexadecimal value.
10. In the *Binary area*, select the second octet (see [Figure 5](#)), 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 ([Figure 6](#)), HTTPS with a host name ([Figure 7](#)), HTTP with an IP address ([Figure 8](#)), and HTTPS with an IP address ([Figure 9](#)).



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

Figure 6. HTTP with a host name

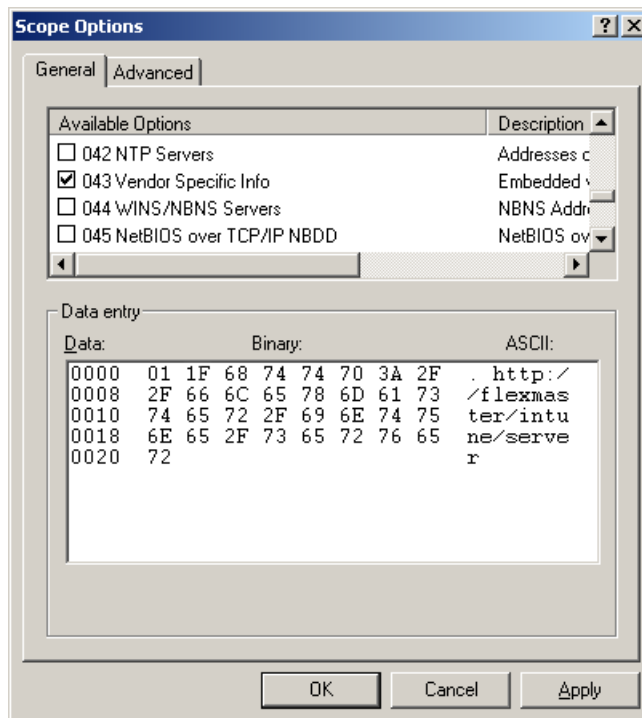
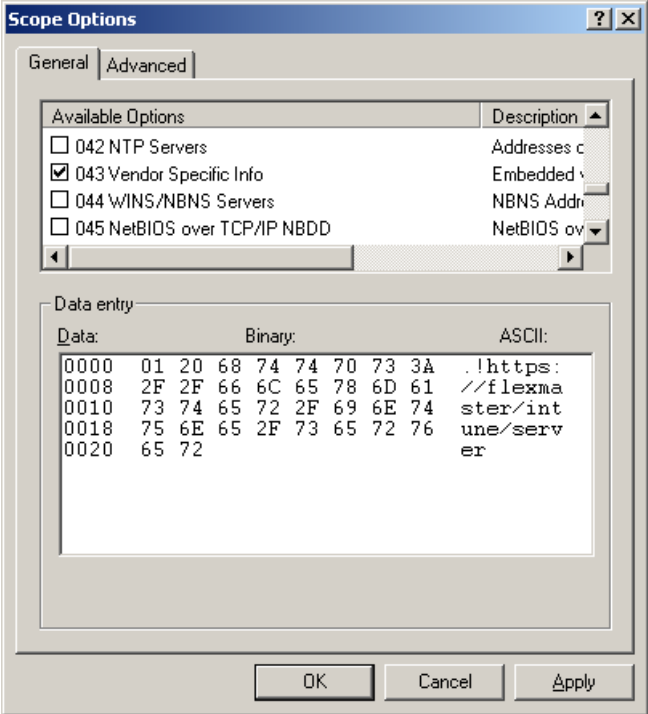


Figure 7. HTTPS with a host name



## Installing FlexMaster

Ensuring That APs Can Connect to FlexMaster

Figure 8. HTTP with an IP address

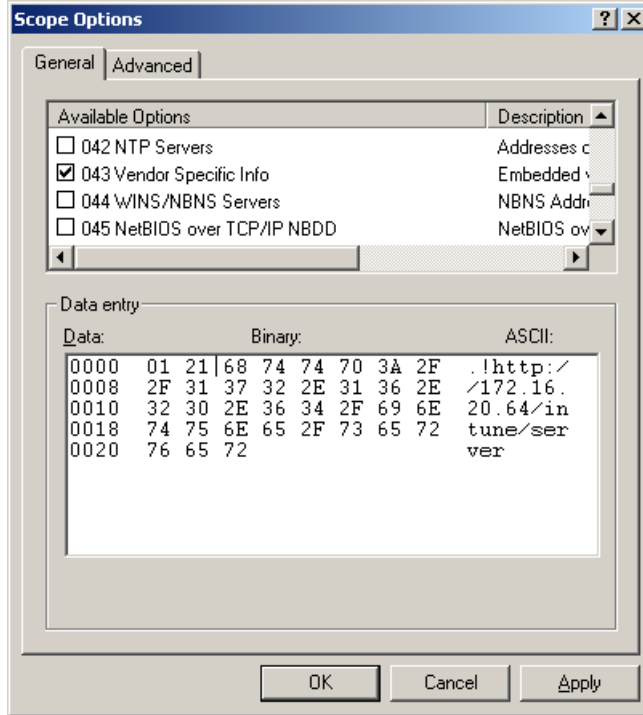
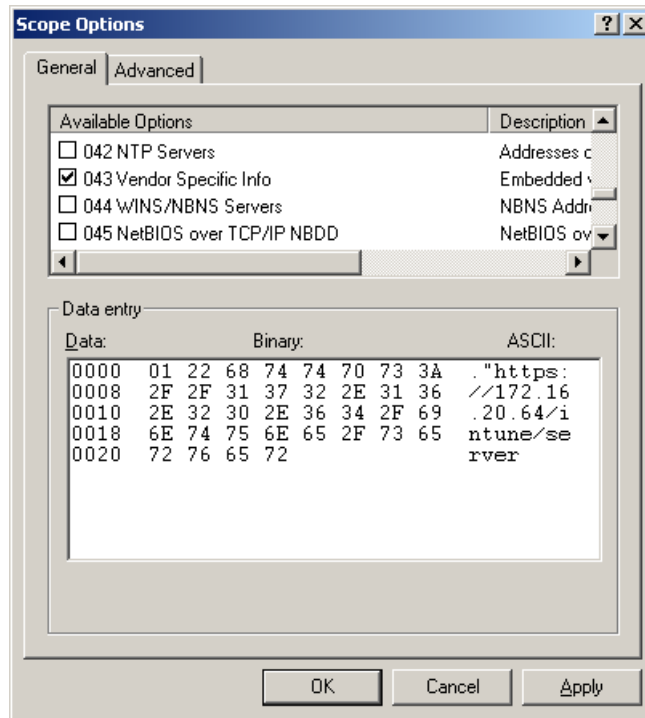


Figure 9. HTTPS with an IP address



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

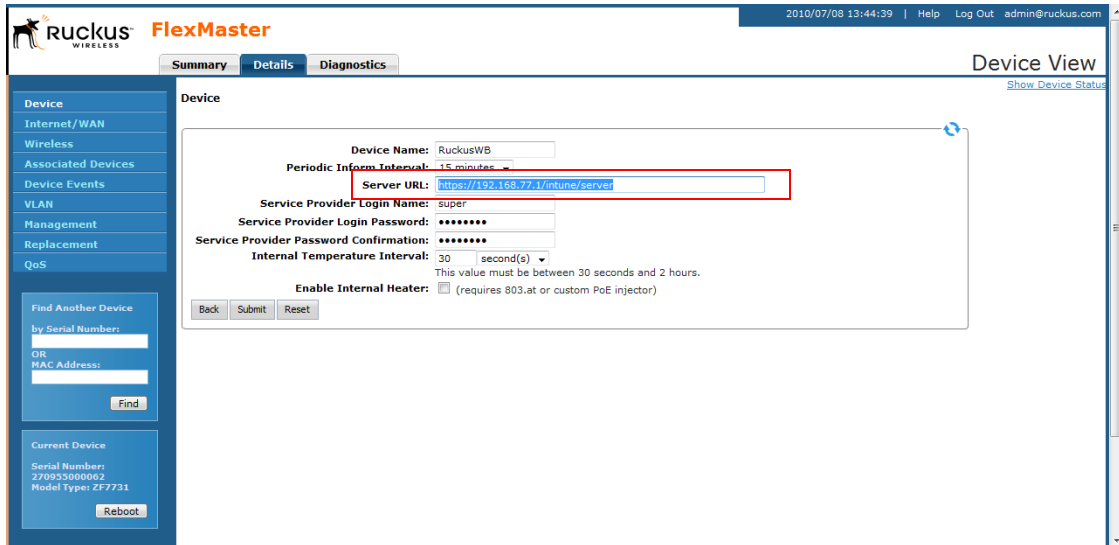
You can also manually point the device to the FlexMaster server by setting the FlexMaster server URL from the Device View.

### To set the FlexMaster server URL manually

1. Go to the **Inventory > Standalone APs > Search** page.
2. Click the serial number of the AP that you want to configure. The Device View appears.
3. Click the **Details** tab.
4. Click the **Edit Settings** button.
5. In *Server URL*, type the URL of the FlexMaster server.
6. 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



## 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.

### To edit the hosts file

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, 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 meeting the system requirements noted 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 prior to FlexMaster installation, that MySQL instance and all dependent packages must be uninstalled prior to initializing FlexMaster installation.

---



---

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

---

## To install the FlexMaster software

1. Log in to the host server as the root user.
2. Insert the FlexMaster CD into the CD-ROM drive.



---

**NOTE:** If the CD-ROM drive does not get automatically mounted, mount it manually using the `mount` command. For information on how to mount a drive, refer to ["Mounting the FlexMaster CD-ROM Manually"](#).

---

3. Change directory (`cd`) to the mount point for the CD-ROM.
  4. Execute the install script (`install.sh`).
5. 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] :
```

6. 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, see ["Understanding User Roles and Privileges"](#).
- ```
domain name (e.g., <your_domain>.com): domain.com
```
7. Enter a password for the FlexMaster `admin@domain.com` user account.
- ```
Password: password
Please confirm your password: password
```
8. Enter a password for the MySQL root account.

## Installing FlexMaster

Installing the FlexMaster Software

Password: password

Please confirm your password: password

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

Https port[443]:



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

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

## Installing FlexMaster

### Installing the FlexMaster Software

The SMTP server is the email server that FlexMaster will use to send alert notifications or system logs. You will have the option to 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
u after installation.
SMTP host: smtpserver
SMTP port[25]:
Mail to: admin@domain.com

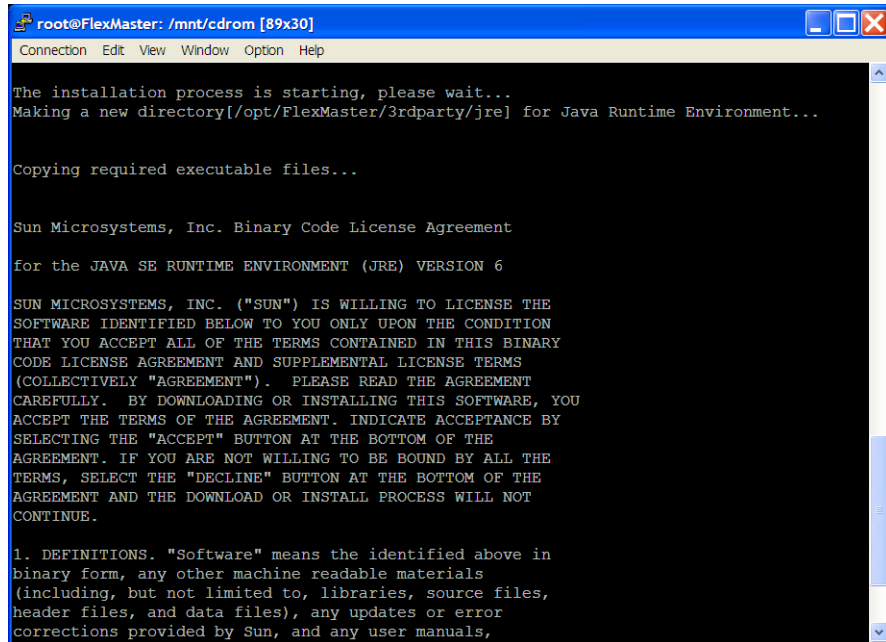
Please note that all devices that wish to register with Flexmaster will be automatic
approved.
You will have the option to change this setting from the Inventory-->Device Registrat
menu after installation.

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

10. Press <Enter> to start the installation process.

Once installation begins, you are presented with a license agreement from Sun Microsystems. See [Figure 13](#).

Figure 13. Sun Microsystems license agreement within the installation script



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

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,
```

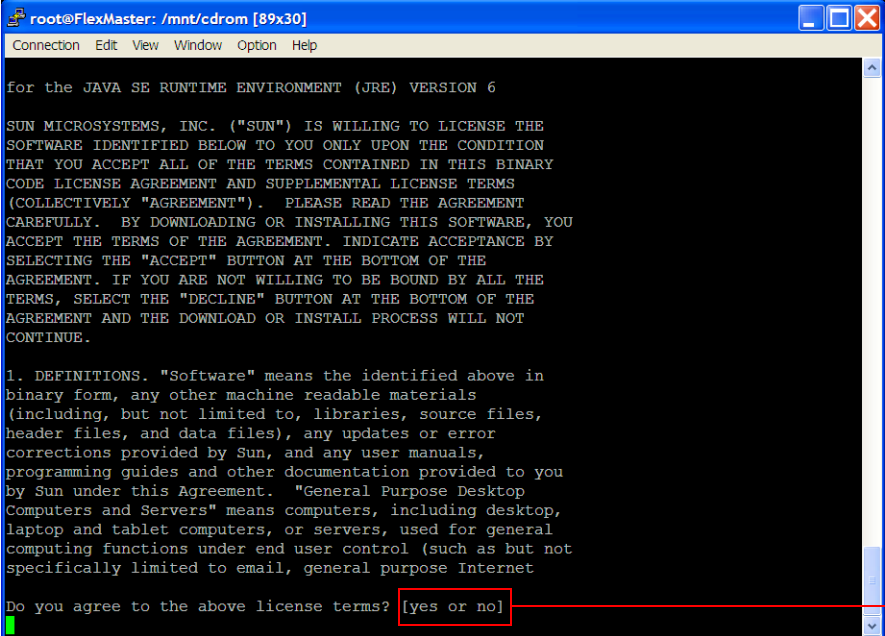
11. Read the license agreement, and accept by typing "yes" at the prompt, and then press <Enter>. See [Figure 14](#).

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

## Installing FlexMaster

Installing the FlexMaster Software

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 (see [Figure 15](#)):

```
*** 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/httpservletproxy
Using CATALINA_HOME: /opt/FlexMaster/3rdparty/tomcat/httpservletproxy
Using CATALINA_TMPDIR: /opt/FlexMaster/3rdparty/tomcat/httpservletproxy/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, 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.

## Mounting the FlexMaster CD-ROM Manually

If the Linux server does not mount the FlexMaster CD-ROM automatically, you must mount it manually to be able to access the installation script on the CD-ROM.

### To mount the CD-ROM manually

1. Type the following command to create a mount point (or directory where you want to mount the CD-ROM):  

```
mkdir -p /mnt/cdrom
```
2. Press <Enter>.
3. Type the following command to mount the CD-ROM manually to the mount point that you created in Step 1:

## Installing FlexMaster

Installing the FlexMaster Software

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

4. Press <Enter>.

You have completed mounting the CD-ROM to /mnt/cdrom. To access the installation script, change directory to /mnt/cdrom.

*Figure 16. Commands for creating a mount point and mounting the CD-ROM*

```
root@FlexMaster:/opt/FlexMaster# mkdir -p /mnt/cdrom  
root@FlexMaster:/opt/FlexMaster# mount /dev/cdrom /mnt/cdrom
```

## 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 may periodically release FlexMaster software updates that contain feature enhancements or fixes for known issues. These software updates may be made available on the Ruckus Wireless support Web site or released through authorized channels. Update files typically use `{version number}.patch` for its file naming convention (for example, `9.2.0.0.15.patch`).



---

**CAUTION!** 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, see [“Backing Up the Database from the Command Line Interface”](#).

---

### To upgrade the FlexMaster server software

1. Copy the patch (software upgrade) file that you received from Ruckus Wireless to the computer where you are accessing the FlexMaster Web interface or any location on the network that is accessible from the Web interface.
2. On the Network View of the FlexMaster Web interface, go to **Administer > Support**. Take note of the current software version as shown in FlexMaster version.
3. Go to **Administer > Upgrade**. The Upgrade page appears.
4. In *Select file to upload*, click **Browse**. The File Upload dialog box appears.
5. Go to the location where you saved the patch file.
6. Select the patch file, and then click **Open**.

7. On the *Upgrade* page, click **Upload**. A status box appears and displays the progress of the software upgrade process. When the upgrade process is complete, the message “Upgrade successful” appears in the status box, along with the software version number to which FlexMaster has been upgraded.
8. Go to **Administer > Support**. You should see the following changes:
  - *FlexMaster Version* shows the software version that you have installed.
  - *Patch Information* shows Original FlexMaster version (previous version) and Patch Version Upgrade Date (new version and date installed).

If FlexMaster Version shows the software version that you have installed, you have successfully upgraded the FlexMaster software.



---

**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, see [“Backing Up the Database from the Command Line Interface”](#).

---

## Uninstalling FlexMaster

### To uninstall the FlexMaster software from the host server

1. Execute the FlexMaster uninstall script.  

```
[root@flexmaster FlexMaster]# ./uninstall.sh
```
2. After you execute the uninstall script, it performs the following steps (in the same order):
  - 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.

### 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 to automatically set the p

- 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}
```

where {file path and file name where you want to save the backup file} is the file path and name where you want to save the backup file.

If you want to save the backup file to the FlexMaster root directory with the file name `Mybackup.tgz`, 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
```

The backup file will be created in the default backup folder, `/opt/FlexMaster/backup` folder, and the file name will be assigned automatically based on the date and time when the backup script was executed (for example, `2009-12-30_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 and is located in the FlexMaster root directory.



---

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

---

#### 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}
```

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, if 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.

## What's Next?

With your Ruckus Wireless FlexMaster now installed, you can login and configure FlexMaster to manage your Ruckus Wireless devices. The chapters that follow will guide you through all of these options.

# Getting Started with FlexMaster

**In This Chapter**

<a href="#">Logging into FlexMaster</a> .....	34
<a href="#">Features of the FlexMaster Web Interface</a> .....	36
<a href="#">Getting to Know the Dashboard and Its Widgets</a> .....	38
<a href="#">Getting Started Tasks</a> .....	53

## Logging into FlexMaster

Use one of the following Web browsers to access the FlexMaster Web interface:

- Internet Explorer version 7.0 and later
- Firefox version 3.0 and later



---

**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, 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.

---

### To log into FlexMaster

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, a security alert dialog box appears. Click **OK/Yes** to proceed.

The *Ruckus Wireless Admin* login page appears.



---

**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, you can install a certificate issued by a recognized certificate authority such as VeriSign. For information, refer to ["Managing SSL Certificates"](#).

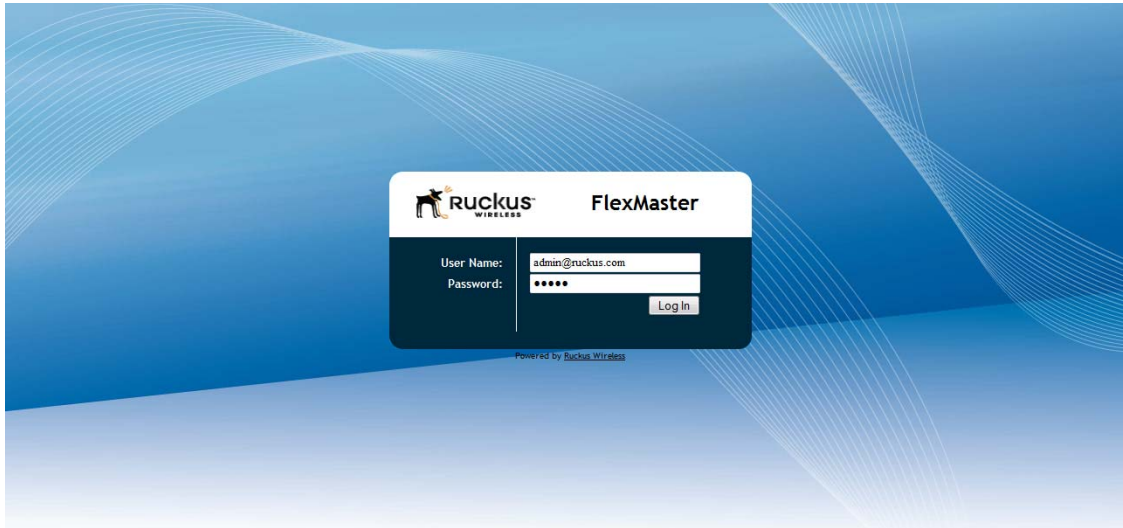
---

4. 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 (see ["Installing the FlexMaster Software"](#)). For example:

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

Password: **admin**

Figure 17. The FlexMaster login page



5. 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, see [“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, Ruckus Wireless strongly recommends that you clear your Web browser’s cache before logging into the FlexMaster Web interface. This will help ensure that the FlexMaster Web interface shows all the changes and enhancements that were implemented in the new software version.

---

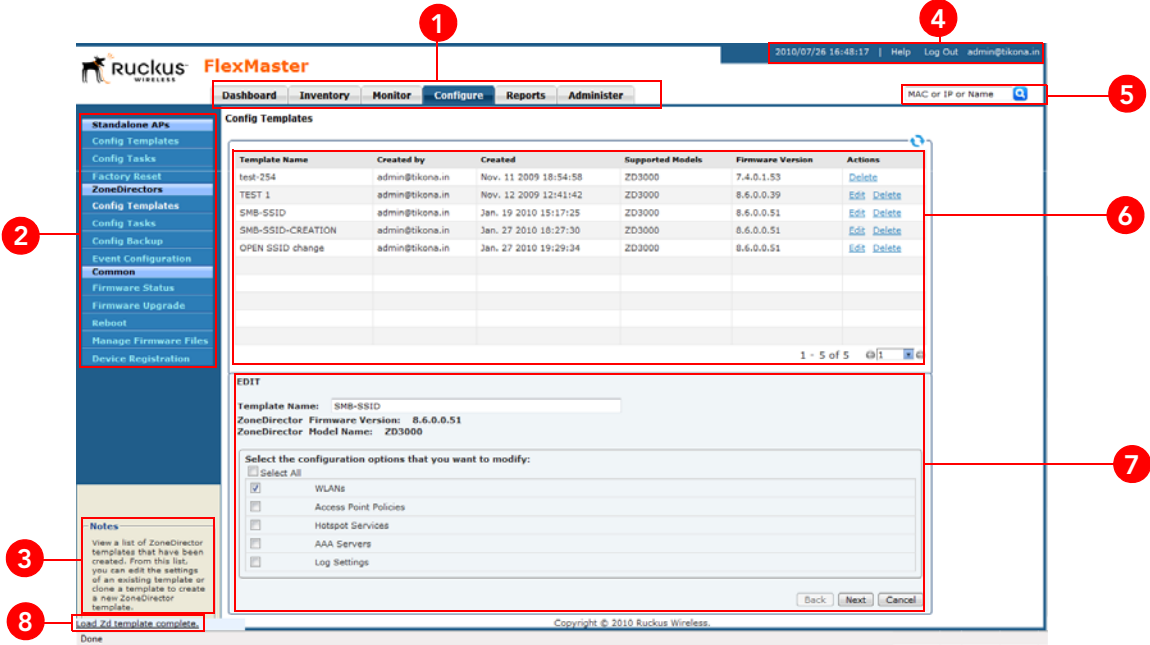
## Features of the FlexMaster Web Interface

[Table 4](#) identifies and describes the elements that are available on the FlexMaster Web interface.

Table 4. FlexMaster Web interface features

No.	Interface Element	Description
1	Main Menu	Six tabs that group related tasks that you can perform in FlexMaster. These tabs include: <ul style="list-style-type: none"><li>• Dashboard</li><li>• Inventory</li><li>• Monitor</li><li>• Configure</li><li>• Reports</li><li>• Administer</li></ul>
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.
4	Help and Logout	<ul style="list-style-type: none"><li>• Shows the current FlexMaster date and time.</li><li>• Click the <b>Help</b> link to open the online help.</li><li>• Click the <b>Log Out</b> link to log out of the FlexMaster. The user name in parenthesis identifies the user who is logged in.</li></ul>
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.
8	Task Status Box	Whenever you perform an action on the Web interface, a single-line task status message appears in this box. To learn more about the status, click the message. The status box also displays error messages.  Informational messages appear in black, whereas error messages appear in red.

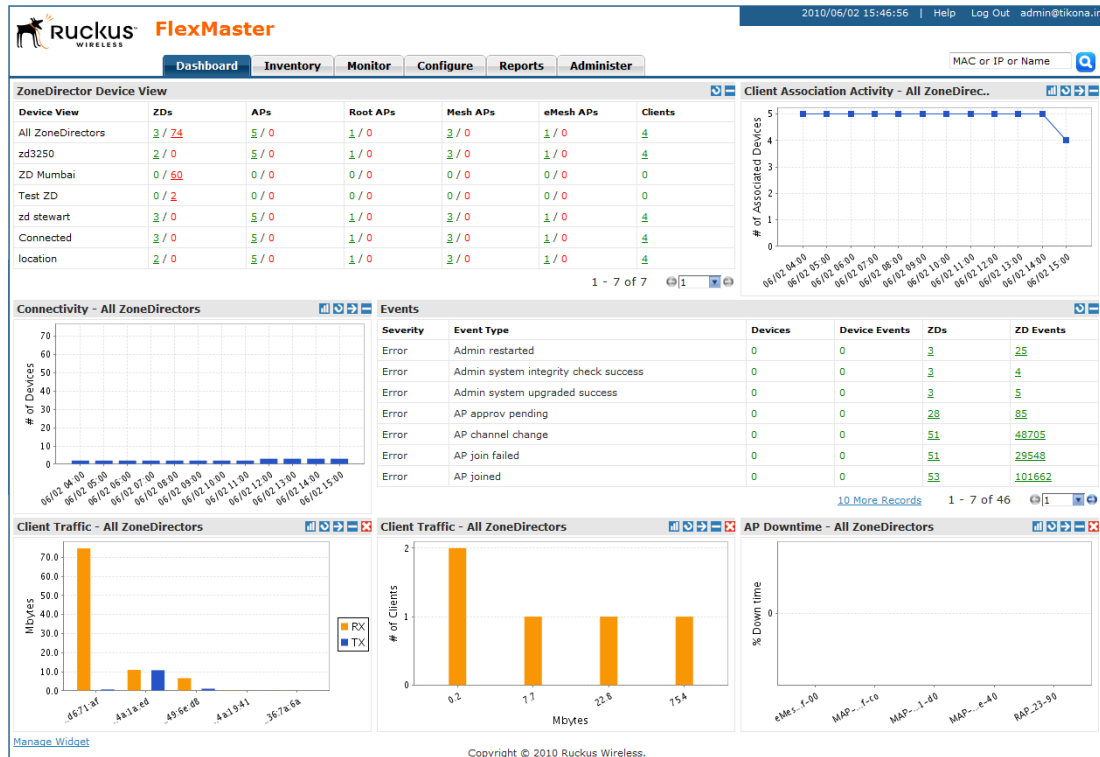
Figure 18. The FlexMaster Web interface has eight primary elements



# Getting to Know the Dashboard and Its Widgets

After you log into 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 19. The Dashboard




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:** Information on most of the Dashboard widgets refreshes automatically based on preconfigured time intervals. To refresh the information on a widget manually, click the  button in the upper-right corner of the 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 ZoneDirector on the network, you could switch to 2-tier management mode to hide data for 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 five standard widgets, which cannot be deleted (only minimized) from the Dashboard:

- [ZoneDirector Device View Widget](#)
- [AP Device View Widget](#)
- [Events Widget](#)
- [Connectivity Widget](#)
- [Client Association Activity 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.

[Table 5](#) describes the columns that appear on the ZoneDirector Device View widget.



**NOTE:** If 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 will appear as "0" (zero) on the ZoneDirector Device View widget.

Table 5. 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 <i>All ZoneDirectors</i> exists, which contains all ZoneDirector devices detected on the network.
ZDs	<p>Shows the number of ZoneDirector units that are registered with FlexMaster. There are two numbers under the ZDs column and they are separated by a slash symbol (for example, X/X).</p> <ul style="list-style-type: none"> <li>The number in green (before the slash symbol) indicates the number of ZoneDirector devices that are currently online.</li> <li>The number in red (after the slash symbol) indicates the number of ZoneDirector devices that are currently offline or disconnected from FlexMaster.</li> </ul> <p>The sum of these two numbers is equal to the total number of ZoneDirector devices that are registered with FlexMaster. Clicking either number (hyperlink) will take you to the <b>Inventory &gt; Reports</b> page, which shows details of all these connected or disconnected ZoneDirector units.</p>
APs	<p>Shows the number of APs that are registered with ZoneDirector devices (which, in turn, are being managed by FlexMaster). There are two numbers under the APs column and they are separated by a slash symbol (for example, X/X).</p> <ul style="list-style-type: none"> <li>The number in green (before the slash symbol) indicates the number of APs that are currently online.</li> <li>The number in red (after the slash symbol) indicates the number of APs devices that are currently offline or disconnected from ZoneDirector.</li> </ul> <p>The sum of these two numbers is equal to the total number of APs that are registered with ZoneDirector. Clicking either number (hyperlink) will take you to the <b>Inventory &gt; Reports</b> page, which shows details of all these connected or disconnected APs.</p> <p><b>NOTE:</b> If mesh networking is enabled on ZoneDirector, three additional columns (namely, <i>Root APs</i>, <i>Mesh APs</i>, and <i>eMesh APs</i>) 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. See "<a href="#">Additional AP Columns When Mesh Networking Is Enabled</a>" for more information.</p>

Table 5. Columns on the ZoneDirector Device View Widget

Column Name	Description
Clients	Shows the number of clients that are associated with the currently connected APs. Clicking this number (hyperlink) will take you to the <b>Inventory &gt; Reports</b> 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.

If 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.



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

Figure 20. Root APs, Mesh APs, and eMesh APs columns on the ZoneDirector Device View widget

Device View	ZDs	APs	Root APs	Mesh APs	eMesh APs	Clients
All ZoneDirectors	3 / 74	5 / 0	1 / 0	3 / 0	1 / 0	4
zd3250	2 / 0	5 / 0	1 / 0	3 / 0	1 / 0	4
ZD Mumbai	0 / 60	0 / 0	0 / 0	0 / 0	0 / 0	0
Test ZD	0 / 2	0 / 0	0 / 0	0 / 0	0 / 0	0
zd stewart	3 / 0	5 / 0	1 / 0	3 / 0	1 / 0	4
Connected	3 / 0	5 / 0	1 / 0	3 / 0	1 / 0	4
location	2 / 0	5 / 0	1 / 0	3 / 0	1 / 0	4

1 - 7 of 7

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 Ethernet (that is, wired) interface. There are two numbers under the Root APs column and they are separated by a slash symbol (for example, X/X).
  - 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 under the Mesh APs column and they are separated by a slash symbol (for example, X/X).
  - 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 Ethernet (wired) interface. If the MAP to which the LAP is connected goes offline, the eMesh AP may 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.

## AP Device View Widget

The 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, see [“Creating an AP View”](#).

---

[Table 6](#) describes the table columns in the Device View widget.

Table 6. Columns on the AP Device View widget

Column Name	Description
Device View	Shows the name of the AP device view. A default device view named <i>All Standalone APs</i> exists.
Connected	Shows the number of APs that are currently connected to FlexMaster. Clicking this number (hyperlink) will take you to the <b>Inventory &gt; Reports</b> 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 <b>Inventory &gt; Reports</b> 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 ago. Click the link to go to <b>Inventory &gt; Reports</b> 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) will take you to the <b>Inventory &gt; Reports</b> page, which shows details of all these disconnected APs.

---

Table 6. Columns on the AP Device View widget

Column Name	Description
Clients	Shows the number of clients that are associated with the currently connected APs. Clicking this number (hyperlink) will take you to the <b>Inventory &gt; Reports</b> 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 under the **Connected** and **Disconnected** columns.

Figure 21. The AP Device View widget

AP Device View <span style="float: right;">⌵</span>					
Device View	Connected	Seen in 1 day	Seen in 2 days	Disconnected	Clients
All Standalone APs	<a href="#">32</a>	<a href="#">35</a>	<a href="#">35</a>	<a href="#">10</a>	<a href="#">7</a>
7363 APs	0	<a href="#">1</a>	<a href="#">1</a>	<a href="#">1</a>	0

1 - 2 of 2 ⏪ 1 ⏩

## Events Widget

The Events widget displays events that have occurred on FlexMaster, on managed ZoneDirector devices and standalone APs, and on clients that report to managed APs.

[Table 7](#) describes the information that you can find on the Events widgets.

Table 7. Columns on the Events widget

Column Name	Description
Severity	<p>Indicates the importance of an events. There are three event severity levels in FlexMaster:</p> <ul style="list-style-type: none"> <li>• <i>Error</i> (high importance): These are events that you should check. For example, if you see <code>Rouge AP detected</code> in the Event Type column, you might want to check whether it is an AP that should authorized or if someone is attempting to spoof authorized APs.</li> <li>• <i>Warning</i> (medium importance): These are events that may require your attention. For example, if you see <code>Connectivity problem</code>, you might want to check what is causing the connectivity issue. If a significant number of devices is experiencing this issue, it might indicate a network issue that needs to be resolved.</li> <li>• <i>Info</i> (low importance): These are informational events that typically do not require your attention (for example, <code>Device rebooted</code>).</li> </ul>
Event Type	Displays the name of the event (as assigned by Ruckus Wireless)
Devices	Displays the number of APs reporting the event. Click this link to go to an <b>Inventory &gt; Reports</b> view of the devices reporting the specific event.
Device Events	Displays the number of events generated by all Standalone APs.
ZDs	Displays the total number of ZoneDirector devices that have reported the event. Click this link to go to an <b>Inventory &gt; Reports</b> view of the devices reporting the specific event.
ZD Events	Displays the total number of events generated by all ZoneDirector units.


Figure 22. Columns on the Events widget

Severity	Event Type	Devices	Device Events	ZDs	ZD Events
Error	Admin restarted	0	0	3	25
Error	Admin system integrity check success	0	0	3	4
Error	Admin system upgraded success	0	0	3	5
Error	AP approv pending	0	0	28	85
Error	AP channel change	0	0	51	48705
Error	AP join failed	0	0	51	29548
Error	AP joined	0	0	53	101662

[10 More Records](#)    1 - 7 of 46   

## Connectivity Widget

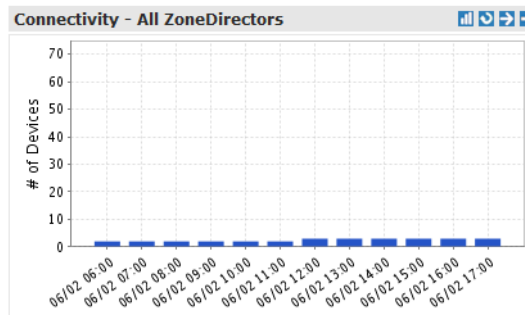
The Connectivity widget displays (in a bar graph format) the number of connectivity or loss-of-connectivity events on devices. The default Connectivity widget displays connectivity information for the All ZoneDirectors device view.

If 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 will take 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.

### To customize the Connectivity widget


1. Click the  (Edit) icon in the upper-right corner of the widget. The Customize Trending Graph window appears.

2. Configure the options under *Select Query 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 Association Activity Widget

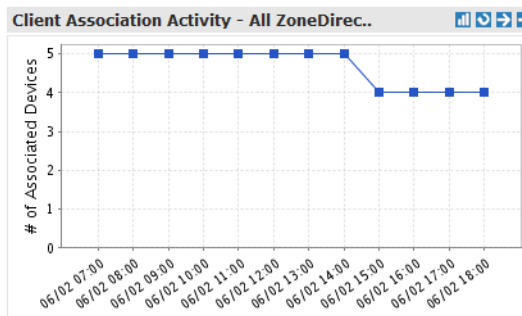
The Client Association Activity widget shows the number of clients that have associated with managed APs. The default Client Association Activity widget displays connectivity information for the All ZoneDirectors device view and on all radios on the managed APs.

If 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 will take you to the 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 24. 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.

### To customize the Client Association Activity widget

1. Click the  (Edit) icon in the upper-right corner of the widget. The Customize Trending Graph window appears.



2. Configure the options under Select Query 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*: Select the radio for which you want to display association information. Options include **All Radios**, **11b/g**, **11n/a**, and **11n/g**.
  - *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*: If 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.

## Customized Widgets

In addition to the five 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. Refer to [Table 8](#) for the types of information that you can show on the Capacity widget.

Table 8. Information that you can show on the Capacity widget

Information	Device	Description
# 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	

## Getting Started with FlexMaster

Getting to Know the Dashboard and Its Widgets

Table 8. Information that you can show on the Capacity widget

Information	Device	Description
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. Refer to [Table 9](#) for the types of information that you can show on the SLA widget.

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

Information	Device	Description
AP Downtime	ZoneDirector/ Standalone AP	
AP Uptime	ZoneDirector/ Standalone AP	
Client Potential Throughput	ZoneDirector	
Client Uptime	ZoneDirector	
Backhaul Link Uptime	Standalone AP	

### Troubleshooting Widget

The Troubleshooting widget can show information that maybe helpful in resolving connectivity issues on the network. Refer to [Table 10](#) for the types of information that you can show on the Troubleshooting widget.

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

Information	Device	Description
# of Child APs	ZoneDirector	
# of Hops	ZoneDirector	
Change of Topology Mesh	ZoneDirector	
Client Phy Rate	ZoneDirector	
Client RSSI	ZoneDirector	
Mesh RSSI	ZoneDirector	

*Table 10. Information that you can show on the Troubleshooting widget*

<b>Information</b>	<b>Device</b>	<b>Description</b>
Physical Link Distance	ZoneDirector	
Backhaul Change of State	Standalone AP	

## Available Widget Slots

FlexMaster provides nine slots on the Dashboard for placing widgets. [Figure 25](#) marks these nine widget slots.

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



Manage Widget Link

## Default Widgets

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

- ZoneDirector Device View
- AP Device View
- Events View
- Client Association Activity View
- 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.

### To add a widget

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 (see [Figure 25](#)).
3. Release the mouse button to place the widget.

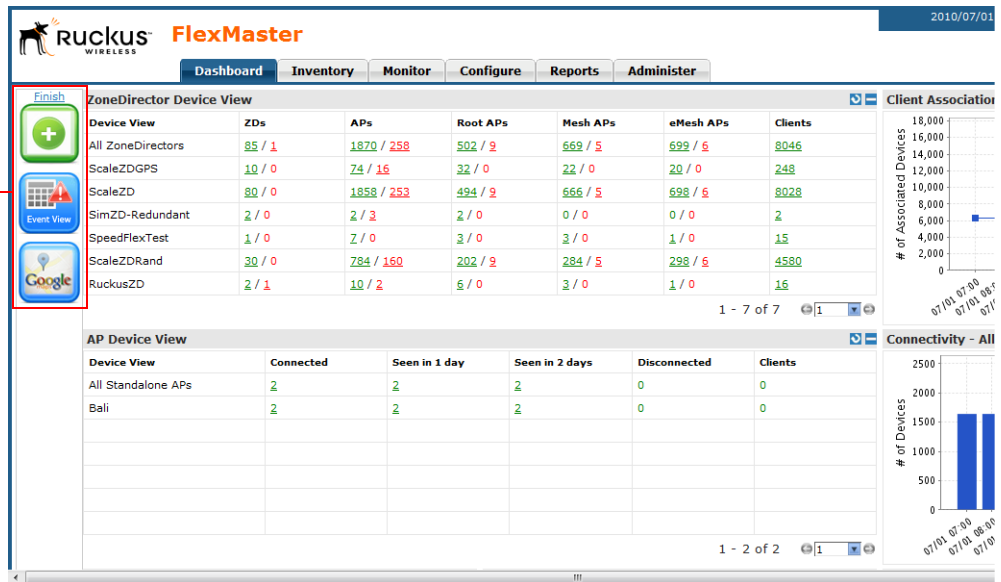
The page refreshes, and the widget that you added appears in the slot where you placed it.



**NOTE:** If 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 that displays widgets that you can add



## 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”](#).

### To hide a default widget

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

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

### To delete a widget

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 APs and ZoneDirector devices, Ruckus Wireless recommends performing the following tasks:

- [Changing the Default Password](#)
- [Pointing Your Ruckus Wireless AP to FlexMaster](#)
- [Checking Your FlexMaster License](#)
- [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.

### To change the default password

1. After logging in to the FlexMaster Web interface, go to **Administer** > **Users**.
2. In the *Users* table, look for the admin user account that you used to log into the FlexMaster Web interface.
3. Click the **Edit** link (under the *Action* column) that is in the same row as the user account name. The *Edit a User* form appears below the table.
4. Type a new password in the **Password** field.
  - Passwords must be between 6 and 32 characters in length, and be comprised of letters and numbers only.
  - Passwords are case-sensitive.
  - Do not use spaces.



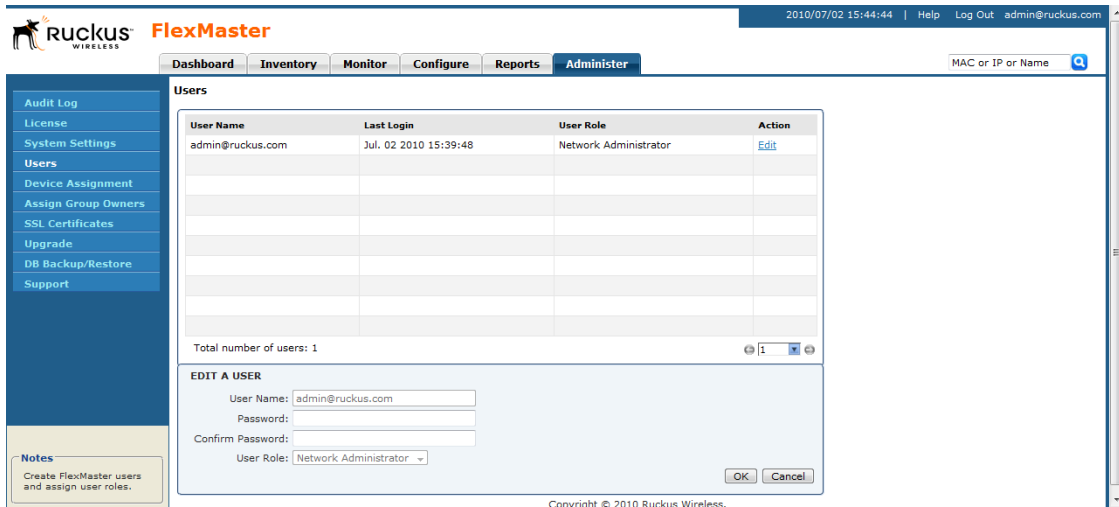
---

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

---

5. Click **OK**.

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



## 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 to be available over the Internet.

Take note of the following:

- ZoneFlex APs shipped with this version are preconfigured with the URL of your FlexMaster server (see [Figure 29](#)), 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, 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.



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

The screenshot shows the 'Administrator :: Management' page. At the top, it displays 'Network Profile: 4bss'. Below this, there are several sections for configuring access protocols:

- Telnet access?** with radio buttons for 'Enabled' and 'Disabled' (selected).
- Telnet Port:** a text input field containing '23'.
- SSH access?** with radio buttons for 'Enabled' (selected) and 'Disabled'.
- SSH Port:** a text input field containing '22'.
- HTTP access?** with radio buttons for 'Enabled' and 'Disabled' (selected).
- HTTP Port:** a text input field containing '80'.
- HTTPS access?** with radio buttons for 'Enabled' (selected) and 'Disabled'.
- HTTPS Port:** a text input field containing '443'.

At the bottom of the settings, there is an 'Auto-provisioning?' section with radio buttons for 'Enabled' and 'Disabled' (selected). Below that, the status 'Certificate verification PASSED' is shown in green. At the very bottom, there are two buttons: 'Update Settings' and 'Restore previous settings'.

## Getting Started with FlexMaster

### Getting Started Tasks

Figure 29. The ZF2942 Administrator > Management page after upgrading to 6.0

The screenshot shows the 'Management' page in the ZF2942 Administrator interface. The left sidebar contains navigation menus for Status, Configuration, Maintenance, and Administrator. The main content area is divided into several sections:

- SSH access?**  Enabled  Disabled
- SSH Port:**
- HTTP access?**  Enabled  Disabled
- HTTP Port:**
- HTTPS access?**  Enabled  Disabled
- HTTPS Port:**
- Certificate verification** PASSED
- Auto-provisioning?**  Enabled  Disabled

**TR069/SNMP Management Choice**

- Auto
- SNMP only
- FlexMaster Only

**DHCP Discovery:**

- FlexMaster Server URL:**  (highlighted with a red box)
- Digest-authentication Username:**
- Digest-authentication password:**
- Contact FlexMaster every**

**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)

Buttons:  [Restore previous settings](#)

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

1. Log into your Ruckus Wireless AP's Web interface.
2. Go to **Administrator > Management**. See "Figure 29." on page 56.
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. See [“Creating an AP Configuration Task”](#).

## 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. If you will also be managing ZoneDirector using FlexMaster, note that the number of license seats that ZoneDirector will consume depends on the maximum number of APs that it can support. ZoneDirector 3250 (which supports up to 250 clients), for example, will consume 250 license seats.

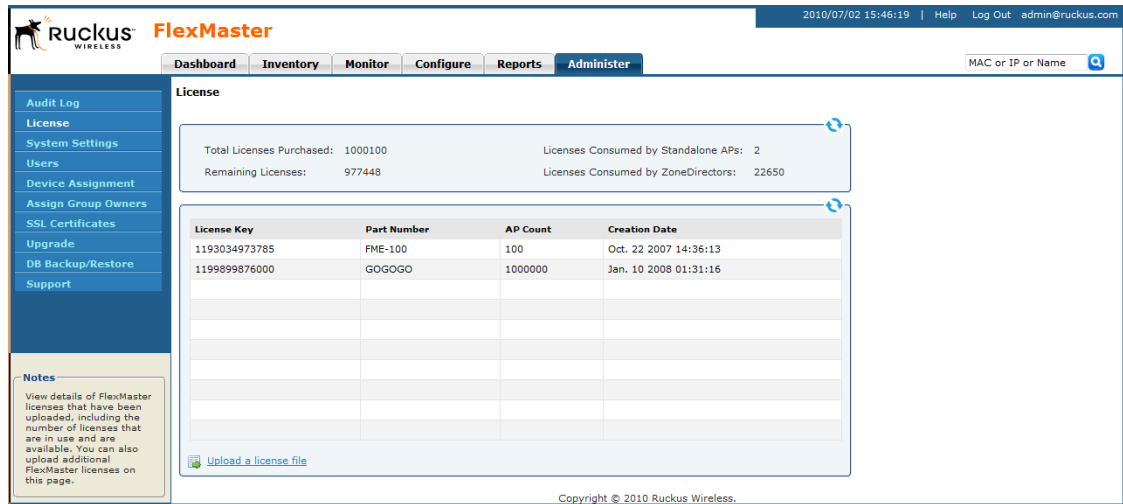
When this seat limit is reached, no additional devices will be able to register with FlexMaster until a license file (that provides additional license seats) is uploaded. FlexMaster will show the following message on the Dashboard to inform you that the seat limit has been reached:

```
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, you will need to contact Ruckus Wireless Support, obtain a license file for additional devices, and upload it to FlexMaster.

Figure 30. The Administer &gt; License page



The screenshot shows the FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The 'Administer' tab is selected. The left sidebar contains various menu items: Audit Log, License, System Settings, Users, Device Assignment, Assign Group Owners, SSL Certificates, Upgrade, DB Backup/Restore, and Support. The main content area is titled 'License' and displays the following statistics:

- Total Licenses Purchased: 1000100
- Remaining Licenses: 977448
- Licenses Consumed by Standalone APs: 2
- Licenses Consumed by ZoneDirectors: 22650

Below the statistics is a table with the following data:

License Key	Part Number	AP Count	Creation Date
1193034973785	FME-100	100	Oct. 22 2007 14:36:13
1198899876000	GOGOGO	1000000	Jan. 10 2008 01:31:16

At the bottom of the table, there is a link to 'Upload a license file'. A 'Notes' section on the left provides instructions on how to view and upload license details.

## Configuring Your Devices to Communicate with FlexMaster over L2TP

If your network prevents FlexMaster from initiating communication across the Internet to managed devices, you can utilize 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, 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 upgrade 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 will allow FlexMaster to initiate future connections subsequently.

### Create the L2TP Configuration Template

To create the configuration template

1. Go to **Configure > Standalone APs > Config Templates**.
2. Click **Create a template**. The “Create New” configuration form opens at the bottom of the page.
3. In **Template Name**, type a name for this L2TP-specific template.
4. In **Select Product Type**, select the product model for which you want to create an L2TP configuration template.
5. Under **Select the configuration options you would like to modify**, select the **Internet** and **VLAN Setting** check boxes.



---

**CAUTION!** You must select both the Internet and VLAN Setting check boxes to create an L2TP configuration template successfully. If you only select the Internet check box, you will be able to create the configuration template, but it will not be applied.

---

6. Click **Next**. The Internet settings page appears.
7. Select the **L2TP Tunnel** check box, and then click the **Enabled** option. After you click the **Enabled** option, additional L2TP configuration parameters appear.

The following LNS values are required:

- L2TP Server IP Address
- Server Secret
- L2TP User Name
- L2TP Password (appropriate to the User Name account)

8. Click **Next**.
9. On the Tunnel Management VLAN configuration page, select and configure the parameters according to your VLAN settings. If you do not use VLANs, you do not need to configure these settings.
10. Click **Next**.
11. When you reach the Configuration Parameter/Value List 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 selected, then when the template is provisioned to a group of devices via Configuration Upgrade task, the devices will retain these template settings even after a factory reset. If this box is left unchecked, then the parameters provisioned in this template will revert to factory defaults after a factory reset.

12. On the Configuration Parameter/Value List page, click **Save** to save the template.

Figure 31. Required L2TP settings

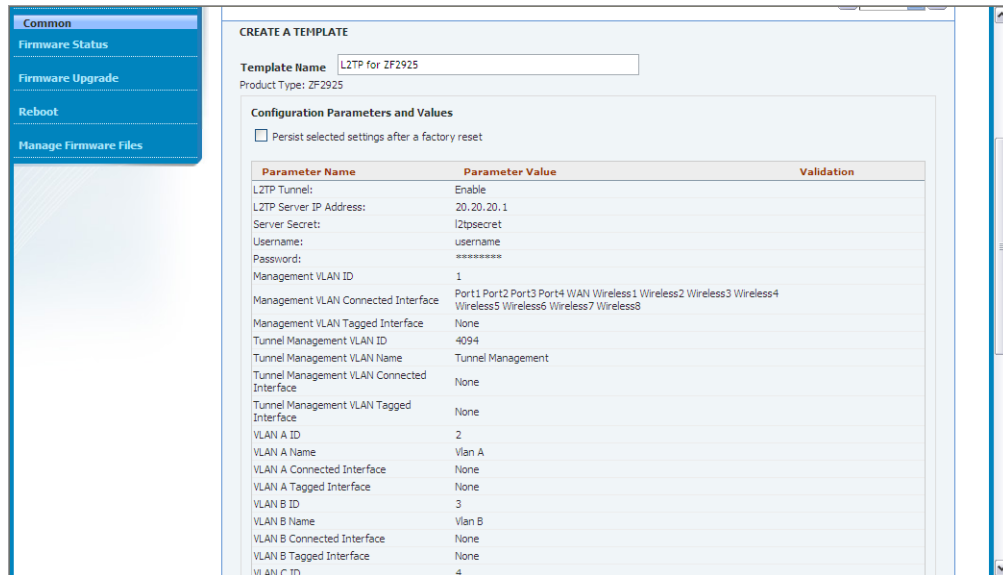
The screenshot shows a web-based configuration interface for creating a template. On the left is a navigation menu with options: Common, Firmware Status, Firmware Upgrade, Reboot, and Manage Firmware Files. The main area is titled 'CREATE A TEMPLATE' and shows the following configuration details:

- Template Name: L2TP for ZF2925
- Product Type: ZF2925
- Section: Internet
- Parameter Value table:
  - Gateway: [ ][ ][ ][ ]
  - DNS Server List: [ ] (Maximum 2 DNS servers, separated by a comma. DNS Server must be a valid IP address.)
  - NTP Server: [ ]
  - Internet Connection Type:  DHCP  Static IP
  - IP Address: [ ][ ][ ][ ] (Warning: This parameter must be set separately for each device.)
  - Mask: [ ][ ][ ][ ]
  - 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: [ ][ ][ ][ ]
  - Server Secret: [ ]
  - Username: [ ] (Username for PPP authentication over L2TP (optional))
  - Password: [ ] (Confirmation) (Password for PPP authentication over L2TP (optional))

13. Click **Next**.
14. On the *Tunnel Management VLAN* configuration page, select and configure the parameters according to your VLAN settings. If you do not use VLANs, you do not need to configure these settings.
15. Click **Next**.
16. When you reach the *Configuration Parameter/Value List* page, a summary of the L2TP settings are displayed. Verify that the settings you have configured are correct.

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

Figure 32. Verify that the L2TP settings are correct



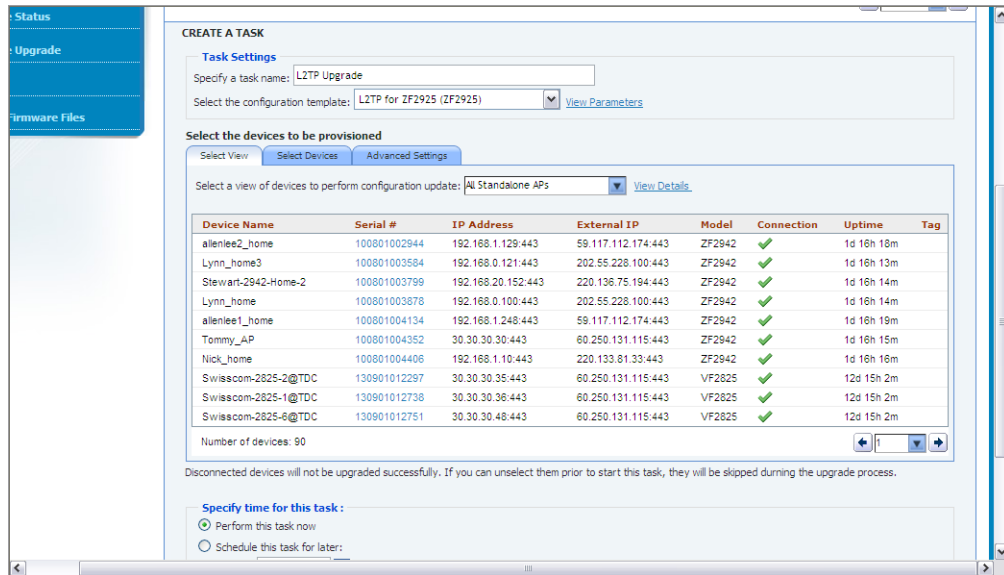
17. Click **Save** to save the template.

## Create the L2TP Configuration Upgrade Task

### To create the Configuration Upgrade task

1. Go to **Configure > Configuration Upgrades**.
2. Click **Create a task**. The "Create a Task" form appears at the bottom of the page.
3. Type a name for this L2TP-specific upgrade at *Specify Task Name*.
4. Toggle the *Select the Configuration Template* drop-down list to select the previously configured L2TP configuration template.
5. (Optional) Under the *Saved Views* 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.
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 33. Creating the L2TP configuration upgrade task





## Working with Device Inventory

### In This Chapter

<a href="#">About the Inventory Page</a> .....	64
<a href="#">Working with ZoneDirector Inventory</a> .....	72
<a href="#">Working with Standalone AP Inventory</a> .....	83
<a href="#">Working with Client Inventory</a> .....	91

## 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:

- ZoneDirector devices (reporting to FlexMaster)
- Standalone APs (reporting to ZoneDirector devices)
- 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

[Table 11](#) and [Table 12](#) list the fields and table columns that appear in the *ZoneDirectors* section of the *Inventory* tab.

Table 11. 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. See <a href="#">"Searching for ZoneDirector Devices"</a> .
Text View/Map View	By default, the page displays a <b>Text View</b> of devices (in a tabular form). If you want to display the geographical location of devices in the current view (whose GPS coordinates have been configured), click <b>Map View</b> . See <a href="#">"Text View and Map View"</a> .
List of ZDs	By default, this table lists all managed ZoneDirector devices. If you search for devices using the ZD Search Criteria section, the devices that match the search criteria will appear in this table.  For information on the columns that appear in this table, refer to <a href="#">Table 12</a> .
Export as XLS File or CSV File	If you want to save the devices that currently appear in the table to an XLS file, click the <b>XLS File</b> button. To save them to a CSV file, click the <b>CSV File</b> button.
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. If 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. See <a href="#">"Search Using the ZD Search Criteria"</a> .

Table 12. 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.
External IP	<p>IP address assigned to the device</p> <p><b>NOTE:</b> The port number after the IP address indicates the protocol that you can use to gain access to the device's Web interface.</p> <ul style="list-style-type: none"> <li>If :443 appears after the port number, you can access the device's Web interface using <code>https://{device-IP-address}</code>.</li> <li>If :80 appears after the IP address, you can access the device's Web interface using <code>http://{device-IP-address}</code>.</li> </ul> <p>If both HTTPS and HTTP management options are enabled, only :443 will appear after the IP address.</p>
Model	Model of the managed Ruckus Wireless device
Last Seen	Date and time when FlexMaster last communicated with the device
Connection	Indicates whether the device is currently online (✔) or offline (✘).
Redundancy State	<p>ZoneDirector's Smart Redundancy feature allows two ZoneDirector devices to be configured as a redundant pair, with one unit actively managing APs while the other serves as a backup in standby mode, ready to take over if the first unit fails or loses power. This column indicates whether this device is part of a Smart Redundancy deployment and its current redundancy state. Three states are possible:</p> <ul style="list-style-type: none"> <li><b>Active:</b> This device is part of a Smart Redundancy deployment and is currently the active ZoneDirector device.</li> <li><b>Standby:</b> This device is part of a Smart Redundancy deployment and is currently the backup ZoneDirector device.</li> <li><b>Standalone:</b> This device is not part of a Smart Redundancy deployment.</li> </ul>

Table 12. Columns that appear in the List of ZDs table

Column	Description
Tag	If configured, this column shows a generic attribute that can be used to identify the device. For example, if this ZoneDirector device is located in main office, you can assign the tag "Main" to it. To assign a tag, edit the device details on the Inventory page.
Software	Shows the software version that is installed on the device
Actions	Actions you can take on the device, including: <ul style="list-style-type: none"><li>• <b>Edit:</b> Allows you change the tag name assigned to the device, as well as its location, GPS coordinates, and Web port mapping.</li><li>• <b>AP List:</b> Displays a table that lists the APs that are reporting to this ZoneDirector device.</li><li>• <b>Mesh View:</b> Display a table that lists the mesh details of this ZoneDirector device.</li></ul>

## Standalone APs Inventory Pages

[Table 13](#) and [Table 14](#) list the fields and table columns that appear in the *Standalone APs* section of the *Inventory* tab.

Table 13. Information that appears in the Standalone APs section of the Inventory page

Field/Column	Description
AP Search Criteria section	Use these filters to search for specific standalone APs. You can save the search results as a new AP view. See " <a href="#">Searching for APs</a> ".
Text View/Map View	By default, the page displays a <b>Text View</b> of devices (in a tabular form). If you want to display the geographical location of devices in the current view (whose GPS coordinates have been configured), click <b>Map View</b> . See " <a href="#">Text View and Map View</a> ".
List of APs	By default, this table lists all standalone APs. If you search for devices using the AP Search Criteria section, the devices that match the search criteria will appear in this table.  For information on the columns that appear in this table, refer to <a href="#">Table 12</a> .
Export as XLS File or CSV File	If you want to save the devices that currently appear in the table to an XLS file, click the <b>XLS File</b> button. To save them to a CSV file, click the <b>CSV File</b> button.

Table 13. Information that appears in the Standalone APs section of the Inventory page

Field/Column	Description
Search box	<p>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.</p> <p>FlexMaster displays up to ten search results on each page. If 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.</p>
Save As View	<p>Use this section to save the search results as a device view. See <a href="#">"Search Using the AP Search Criteria"</a>.</p>

Table 14. 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.
IP Address	<p>IP address assigned to the device</p> <p><b>NOTE:</b> <i>The port number after the IP address indicates the protocol that you can use to gain access to the device's Web interface.</i></p> <ul style="list-style-type: none"><li>• If :443 appears after the port number, you can access the device's Web interface using <code>https://{device-IP-address}</code>.</li><li>• If :80 appears after the IP address, you can access the device's Web interface using <code>http://{device-IP-address}</code>.</li></ul> <p>If both HTTPS and HTTP management options are enabled, only :443 will appear after the IP address.</p>

Table 14. Columns that appear in the List of APs table

Column	Description
External IP	If the device is behind a NAT server, this is the IP address and port number that FlexMaster will use to communicate with the device.  NOTES <ul style="list-style-type: none"><li>If the device is not behind a NAT server, the values for IP Address (above) and External IP Address are the same.</li><li>If the device is behind a NAT server, make sure that you configure port forwarding for the device on the NAT server. Then, click the <b>Edit</b> 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.</li></ul>
Model	Model of the managed Ruckus Wireless device
Last Seen	Date and time when FlexMaster last communicated with the device
Location	If configured, this column shows the location of the device.
Uptime	Shows how long since the device was last rebooted
Connection	Indicates whether the device is currently online (✔) or offline (✘).
Tag	If configured, this column shows a generic attribute that can be used to identify the device. For example, if this AP device is located in main office, you can assign the tag "Main" to it. To assign a tag, edit the device details on the Inventory page.
Software	Shows the software version that is installed on the device
Actions	Clicking <b>Edit</b> allows you change the tag name assigned to the device, as well as its location, GPS coordinates, and Web port mapping.

## Client Inventory Pages

[Table 15](#) and [Table 16](#) list the fields and table columns that appear in the *Clients* section of the *Inventory* tab.

Table 15. 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. See " <a href="#">Searching for Clients</a> ".

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

Field/Column	Description
Text View/Map View	By default, the page displays a <b>Text View</b> of devices (in a tabular form). If you want to display the geographical location of devices in the current view (whose GPS coordinates have been configured), click <b>Map View</b> . See <a href="#">“Text View and Map View”</a> .
List of Clients	By default, this table lists all clients. If you search for devices using the Clients Search Criteria section, the devices that match the search criteria will appear in this table.  For information on the columns that appear in this table, refer to <a href="#">Table 12</a> .
Export as XLS File or CSV File	If you want to save the devices that currently appear in the table to an XLS file, click the <b>XLS File</b> button. To save them to a CSV file, click the <b>CSV File</b> button.
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. If 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. See <a href="#">“Search Using the Client Search Criteria”</a> .

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

Column	Description
Client MAC	MAC address of the wireless client
ZoneDirector Name	Name of the ZoneDirector device that is managing the AP with which this client is associated
User IP Address	IP address assigned to the client
AP Name	Name of the AP with which this client is associated
Description	Description of the AP with which this client is associated
WLAN	WLAN name with which this client is associated
Channel	Radio channel that the client is using
Signal	Strength of wireless signal

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

Column	Description
Connection	Indicates whether the client is currently online (🟢) or offline (🔴).

## Text View and Map View

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

The Map View also shows the connection status of each managed device – green markers on the map represent online devices, whereas red markers represent offline devices. If multiple devices (with some offline and some online) are in the same location, FlexMaster shows a single yellow marker.


By default, the Text View is displayed and the Map View is hidden. To display the Map View, click the **Map View** link on the following pages:

- Inventory > ZoneDirectors > Search
- Inventory > Standalone APs > Search
- Inventory > Clients > Search

When the Map View appears, you can switch to any of the following view types:

- *Map*: Standard flat globe view
- *Satellite*: Satellite view of the globe
- *None*: View of the devices without the map



**NOTE:** If a device changes status (online or offline), its status will not be updated on the Map View. You will need to click the  (Refresh) button in the upper-right corner of the page to show the updated device status on the Map View.

Moving your mouse pointer over a map marker displays basic information about the devices located at that marker, including the serial number. Click the serial number value to open the Device View for that device.

If there are multiple devices with the same GPS coordinates, the serial numbers of all the devices will be displayed in the information window, but only one marker will appear on the map. Click any **Serial Number** value in the information window to open the Device View for that device. See [Figure 34](#).



**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



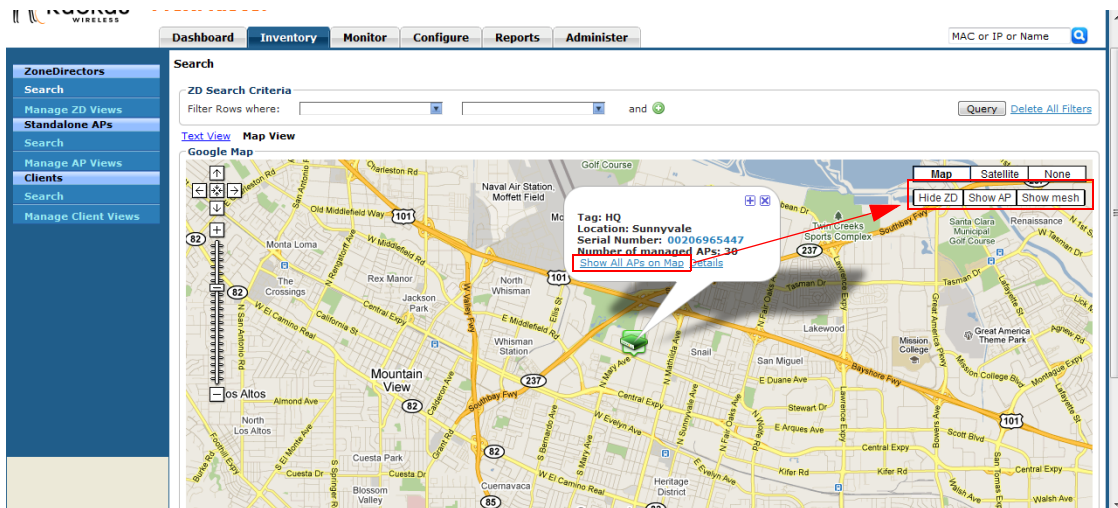
or ZoneDirector from the FlexMaster Web interface, search for the device on the Inventory page, and then click the **Edit** link under the *Action* column. When the *Edit Tag* form appears at the bottom of the page, enter the GPS coordinates of the device, and then click **OK**.

## 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:

- Tag name and location (if configured)
- The ZoneDirector serial number (hyperlink): Clicking this link opens the ZoneDirector Web interface in a new window.
- The number of managed APs
- **Show All APs on the Map** (hyperlink): Clicking this link will display the APs on the Map View. After clicking this link, three buttons additional appear in the upper-right corner of the Map View:
  - **Hide ZD**: Click to hide the ZoneDirector device on the Map View.
  - **Hide AP**: Click to hide APs on the Map View.
  - **Show Mesh**: Click to show APs that are part of the mesh network on the Map View.

Figure 34. Clicking Show All APs on the Map displays AP icons on the map and three additional buttons in the top-right corner



- **Details** (hyperlink): Clicking this link shows (in a table) details of the APs reporting to this ZoneDirector device. Similar to the Text View for APs, the AP details that are shown include serial number, model name, IP address, # of clients, and connection status. If mesh networking is enabled on ZoneDirector, you can click **Show Mesh Data** to view the mesh tree.

## 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 as shown in [Figure 35](#). The total number of managed ZoneDirector devices is indicated below the table, right next to the device search box.

Figure 35. A list of ZoneDirector devices that have registered with FlexMaster appears under the List of ZDs section

The screenshot shows the FlexMaster web interface. The 'Inventory' tab is selected. The 'List of ZDs' section contains a table with the following data:

ZD Name	Serial Number	IP Address	External IP	Model	Last Seen	Location	Uptime	Connection	Redundancy State	Tag	Software	Act
zd3250-stewart-01	123456789098	192.168.20.5:443	60.250.131.117:8445	ZD3250	May. 13 2010 10:21:55	Palo Alto ca USA	19h 1m	✓	Active	zd3250 stewart	9.0.0.99.523	Edt
zd3500-stewart-04	320833000219	192.168.20.46:443	60.250.131.117:8448	ZD3500	May. 13 2010 10:22:17	Sanjose ca USA	19h 2m	✓	Standalone	zd3500 stewart	9.0.0.99.523	Edt

Below the table, the text 'Total number of managed' is displayed with a red box around the number '21' in the pagination '1 - 2 of 21'.

The List of ZDs section can show up to 10 ZoneDirector devices at a time. If FlexMaster is managing more than 10 ZoneDirector devices, you can view the succeeding pages that list the remaining ZoneDirector devices by click 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

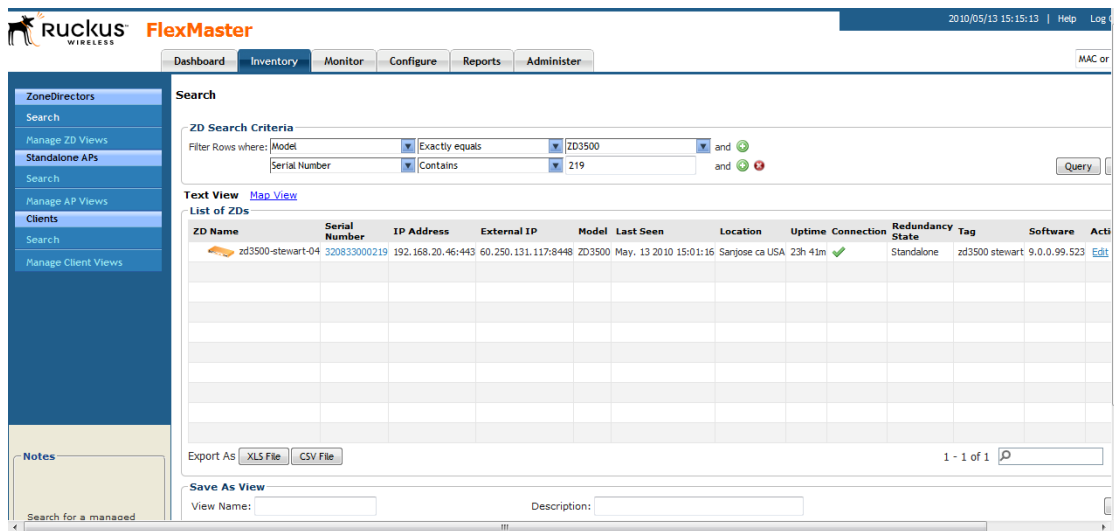
1. Go to **Inventory > ZoneDirector > Search**.
2. Look for the **ZD Search Criteria** section. To search for ZoneDirector devices, you will need to specify the criteria of the devices that you are looking for.
3. In the first drop-down list box after **Filter Rows where**, select the search attribute that you want to use. Options include name, serial number, 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, only devices with this IP address will 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, all devices with "100" in the IP address (for example, 172 . 17 . 16 . **100** and **100** . 1 . 10 . 13) will 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, only devices with serial numbers that begin with "3208" (for example, 320833000219) will 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, only devices with model names that end in "13" (for example, 100 . 1 . 10 . **13**) will 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 may consist of numbers or letters (depending on be the attribute that you selected in the first drop-down list box) and may be a partial or full string. Refer to the previous step for search examples.
6. If you want to add another search filter, 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.

- When you complete setting up the search filters, click **Query**. FlexMaster displays the devices that match the search criteria.

Figure 36. Using Search Criteria to search for a ZoneDirector device



**NOTE:** If you save your query parameters as a view, any new devices that later register with FlexMaster and meet the query criteria will be added automatically 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: See ["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.



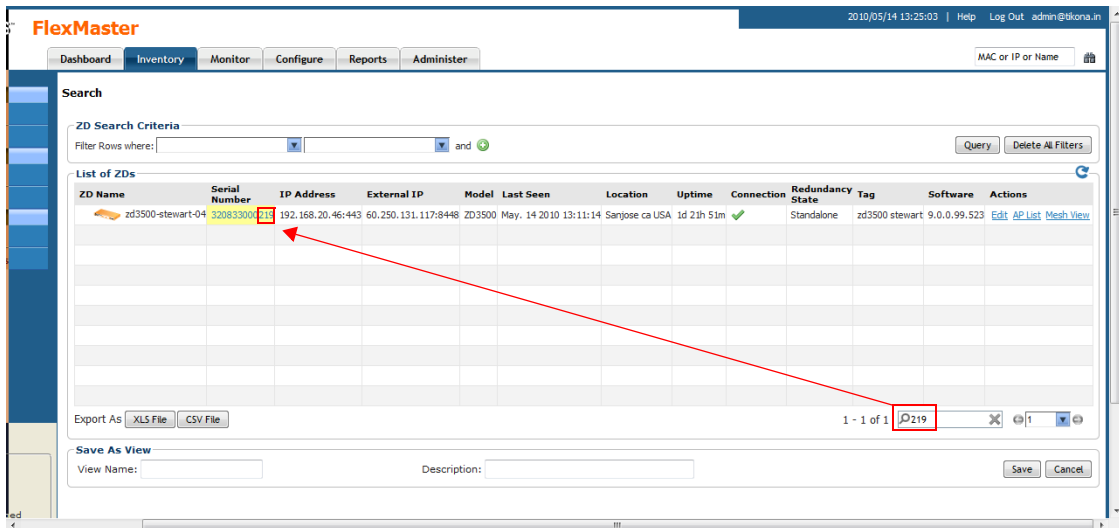
**NOTE:** If you save your query parameters as a view, any new devices that later register with FlexMaster and meet the query criteria will be added automatically to the saved view.

### To use the search box

1. Type a search string into the box. The search string could be a partial or full string and may 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 the table. In Figure 37, the search string '291' matched part of a ZoneDirector device's serial number and, therefore, is highlighted in yellow.

Figure 37. The device property that matches the search string is highlighted in the search results



## Editing ZoneDirector Details

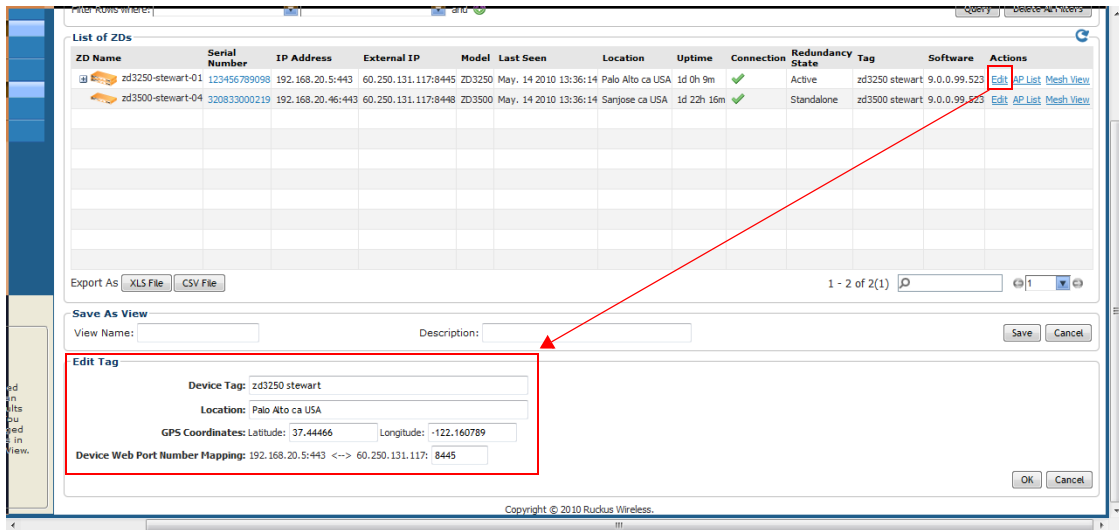
You can edit a ZoneDirector device's tag name, location, GPS coordinates, and Web port number mapping (for devices behind a NAT server).

### To edit a ZoneDirector device's details

1. On the *List of ZDs* table, look for the device that you want to edit. If 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 device properties that you want to update. Properties that you can edit include:
  - Device Tag
  - Location

- GPS Coordinates (Latitude and Longitude)
  - Device Web Port Number Mapping
4. After you make changes, click **Save**.

Figure 38. Editing ZoneDirector details



## Viewing APs That Report to a ZoneDirector Device

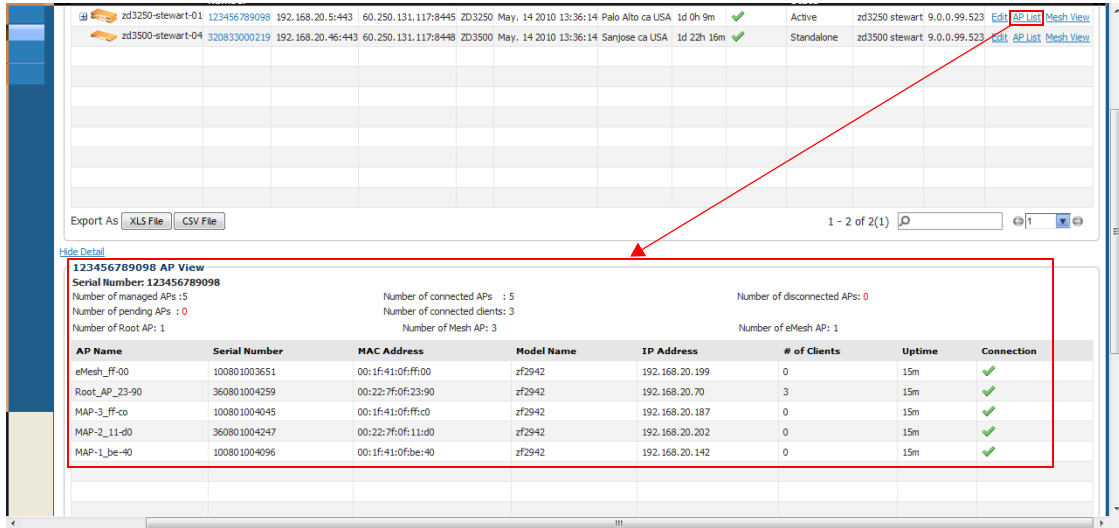
To view a list of APs that are reporting to a ZoneDirector device

1. On the *List of ZDs* table, look for the device that you want to edit. If 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 **AP List** link that is in the same row as the device name. The *AP View* section appears at the bottom of the page.

The *AP View* section shows a list of APs reporting to the ZoneDirector device and displays the following details for each AP:

- AP Name
- Serial Number
- MAC Address
- Model Name
- IP Address
- # of Clients
- Uptime
- Connection

Figure 39. The AP View section shows a list of APs reporting to the ZoneDirector device

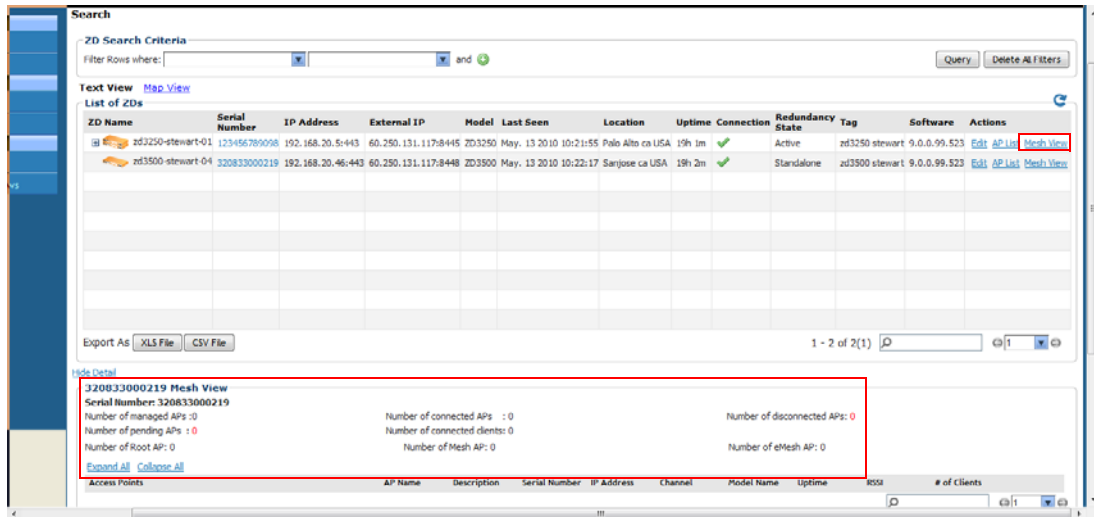


## Viewing Mesh Connections

If a ZoneDirector device is part of a mesh network, you can view the mesh networks details for that ZoneDirector device by clicking the **Mesh View** link that is in the same row as the ZD name. Clicking the Mesh View link displays a box that shows the following mesh details:

- Serial Number
- Number of managed APs
- Number of pending APs
- Number of connected APs
- Number of disconnected APs
- Number of connected clients
- Number of Root APs
- Number of Mesh APs
- Number of eMesh APs

Figure 40. Clicking Mesh View displays mesh details in a table below



## 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.

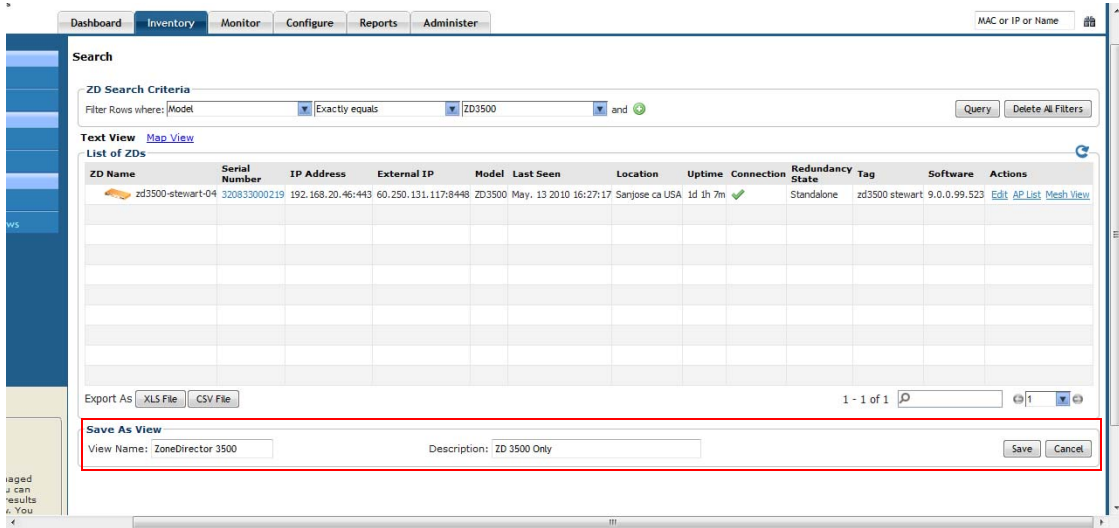
### To create a ZD view

1. Perform a search for clients through 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 a description for the view that you are saving. For example, if the view contains only ZoneDirector 3500 devices, you can type **ZD3500 only**.
5. Click **Save**.

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



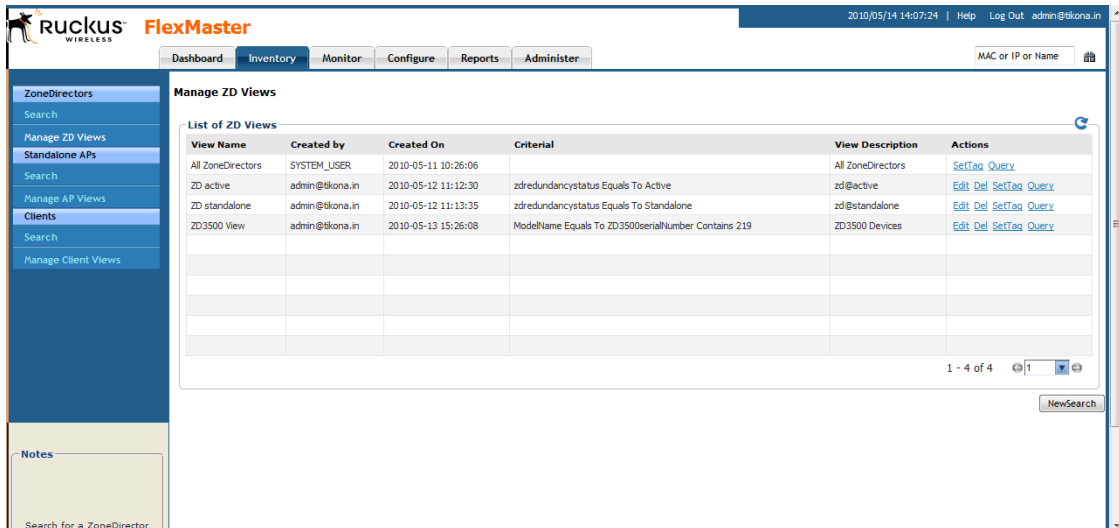
Figure 41. Creating a ZD view that contains only ZoneDirector 3500 devices



## 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 42. The Manage ZD View page lists all existing ZoneDirector views



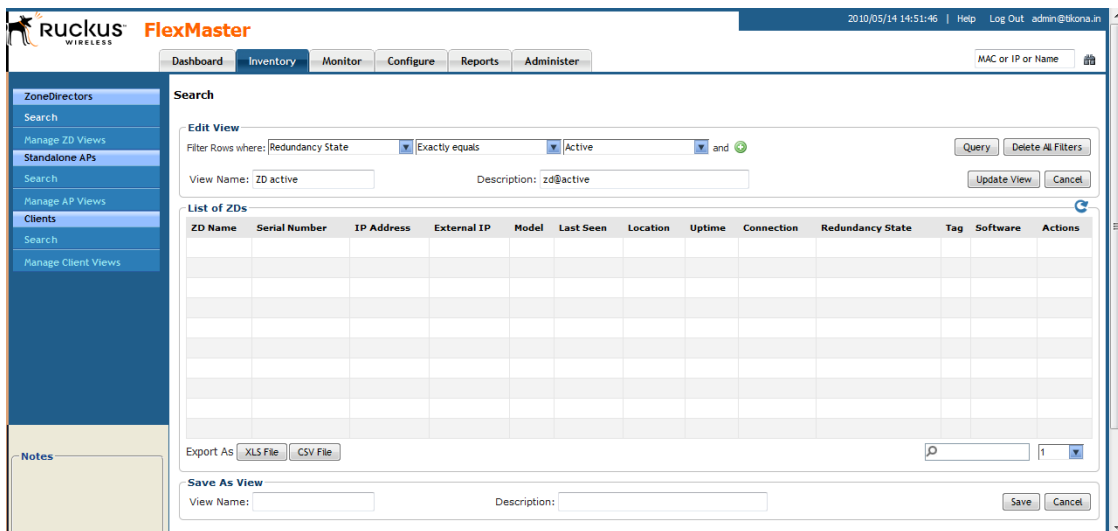
## Editing a ZD View

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

### To edit 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 the **Edit** link that is in the same row as the ZD 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**.

Figure 43. Editing a ZD view



## Deleting a ZD View

### To delete a ZD view

1. Go to the **Inventory > ZoneDirector > Manage Views** page.
2. Look for the ZD 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.

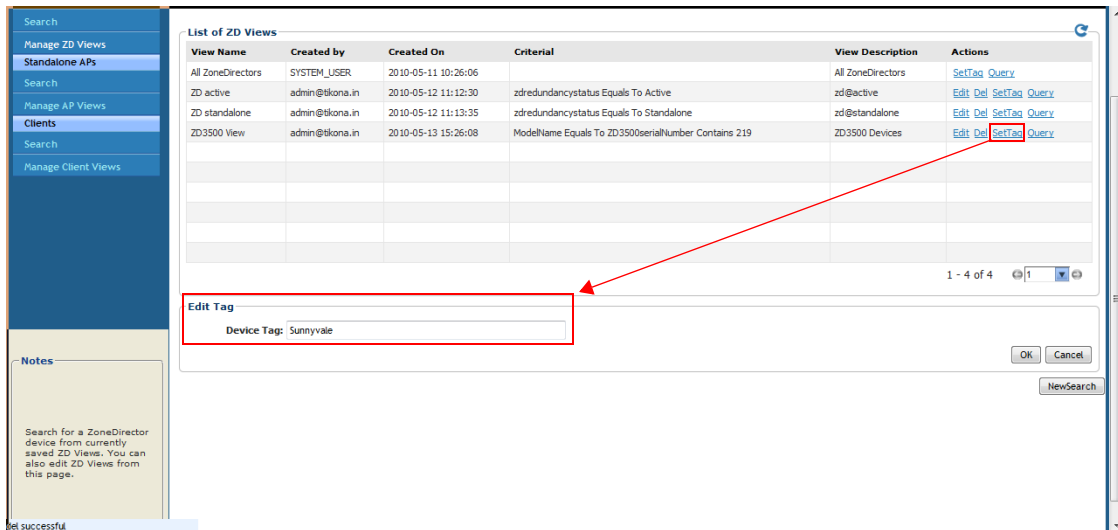
## Setting Tags

If you have a view with all the devices in the same location, you can use the geographical location of those devices as the tag to enable FlexMaster to display the devices on the *Map View*.

### To assign a tag to a view

1. Go to the **Inventory > ZoneDirector > Manage Views** page.
2. Look for the ZD view to which you want to assign a tag.
3. Click the **Set Tag** link that is in the same row as the view name. The Edit Tag section appears at the bottom of the page.
4. In **Device Tag**, type the tag that you want to assign to the view.
5. Click **OK** to save your changes.

Figure 44. Assigning a tag to a view



## Viewing Devices That Belong to a View

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

### To run a query

1. Go to the **Inventory > ZoneDirector > Manage Views** page.
2. Look for the ZD view on which you want to run a query.

## Working with Device Inventory

### Working with ZoneDirector Inventory

3. Click the **Query** link that is in the same row as the view name. The ZoneDirector Search page appears, and then devices that belong to the view appears in the *List of ZDs* section.

Figure 45. After you click the Query link, devices that belong to the view appear in the List of ZDs section

The screenshot shows the FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The 'Inventory' tab is selected. Below the navigation bar, there is a search section with 'ZD Search Criteria' and a 'Query' button. The 'List of ZDs' section is highlighted with a red box and contains the following table:

ZD Name	Serial Number	IP Address	External IP	Model	Last Seen	Location	Uptime	Connection	Redundancy State	Tag	Software	Actions
ruckus	100903000421	192.168.20.196:443	60.250.131.117:8447	ZD3500	May. 14 2010 16:02:32	Mounthill ca USA	2h 0m	✓	Standalone	zd3500 stewart	9.0.0.99.523	<a href="#">Edit</a> <a href="#">AP List</a> <a href="#">Mesh View</a>
zd3500-stewart-04	320833000219	192.168.20.46:443	60.250.131.117:8448	ZD3500	May. 14 2010 16:02:14	Sanjose ca USA	2d 0h 42m	✓	Standalone	this,that	9.0.0.99.523	<a href="#">Edit</a> <a href="#">AP List</a> <a href="#">Mesh View</a>

Below the table, there are 'Export As' buttons for 'XLS File' and 'CSV File', and a 'Save As View' section with 'View Name' and 'Description' input fields, and 'Save' and 'Cancel' buttons.

## Working with Standalone AP Inventory

The AP inventory page displays a list of APs that are *directly reporting* to FlexMaster. It also provides options for searching for specific 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 APs That Report to a ZoneDirector Device”](#).

## Viewing a Summary of Standalone APs

To view APs that have registered with FlexMaster, click the **Inventory** tab. A list of APs appears in the **List of APs** section as shown in [Figure 46](#). The total number of managed APs is indicated below the table, right next to the device search box.

Figure 46. A list of APs that have registered with FlexMaster appears in the List of APs section

The screenshot shows the FlexMaster web interface. The 'Inventory' tab is selected. The 'List of APs' section is visible, containing a table with the following data:

AP Name	Serial Number	IP Address	External IP	Model	Last Seen	Location	Uptime	Connection	Tag	Software	Actions
stewart-7811	180801000625	1.1.1.136:443	60.250.131.115:443	VF7811	May, 14 2010 16:26:28		18d 2h 47m	✓		5.3.1.0.124M	Edit
stewart-7811	390801005202	1.1.1.91:443	60.250.131.115:443	VF7811	May, 14 2010 16:26:28		18d 2h 47m	✓		5.3.1.0.124M	Edit
stewart-7811	390801005312	1.1.1.118:443	60.250.131.115:443	VF7811	May, 14 2010 16:26:29		18d 2h 47m	✓		5.3.2.0.146M	Edit

Below the table, the text 'Total number of managed APs' is displayed, with a red box around the number '3' in the pagination '1 - 3 of 3'.

The *List of APs* section can show up to 10 APs at a time. If 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 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 the **Inventory > Standalone APs > Search**.
2. Look for the **AP Search Criteria** section. To search for APs, you will 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, 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, only devices with this IP address will 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, all devices with "100" in the IP address (for example, 172 . 17 . 16 . **100** and **100** . 1 . 10 . 13) will 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, only devices with serial numbers that begin with "3908" (for example, 390801005202) will 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, only devices with model names that end in "13" (for example, 100 . 1 . 10 . **13**) will 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 may consist of numbers or letters (depending on be the attribute that you selected in the first drop-down list box) and may be a partial or full string. Refer to the previous step for search examples.
6. If you want to add another search filter, 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 47. Using Search Criteria to search for an AP

The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The left sidebar has 'ZoneDirectors', 'Search', 'Manage ZD Views', 'Stand-alone APs', 'Search', 'Manage AP Views', 'Clients', 'Search', and 'Manage Client Views'. The main content area is titled 'Search' and shows 'AP Search Criteria' with a filter for 'Serial Number' starting with '3908'. Below this is a table of APs with columns: AP Name, Serial Number, IP Address, External IP, Model, Last Seen, Location, Uptime, Connection, Tag, Software, and Actions. Two APs are listed: 'stewart-7811' with serial numbers '390801005202' and '390801005312', both with IP addresses '1.1.1.91:443' and '1.1.1.118:443', and model 'VF7811'. The 'Last Seen' column shows 'May, 14 2010 16:41:28' and 'May, 14 2010 16:41:29'. The 'Uptime' column shows '18d 3h 2m' for both. The 'Connection' column shows a green checkmark for both. The 'Software' column shows '5.3.1.0.124M' and '5.3.2.0.146M'. The 'Actions' column has 'Edit' links for each row. Below the table are 'Export As' buttons for 'XLS File' and 'CSV File', and a 'Save As View' section with 'View Name' and 'Description' fields.



**NOTE:** If you save your query parameters as a view, any new devices that later register with FlexMaster and meet the query criteria will be added automatically 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: See ["Creating an 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, any new devices that later register with FlexMaster and meet the query criteria will be added automatically to the saved view.

#### To use the search box

1. Type a search string into the box. The search string could be a partial or full string and may 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. In Figure 48, the search string 3908 matched part of two APs's serial numbers and, therefore, are highlighted in yellow.

Figure 48. The device property that matches the search string is highlighted in the search results

The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The left sidebar has a 'Search' section with options for 'ZoneDirectors', 'Manage ZD Views', 'Standalone APs', 'Manage AP Views', 'Clients', and 'Manage Client Views'. The main content area is titled 'Search' and contains an 'AP Search Criteria' section with a filter set to 'Y and'. Below this is a table titled 'List of APs' with columns: AP Name, Serial Number, IP Address, External IP, Model, Last Seen, Location, Uptime, Connection, Tag, Software, and Actions. Two rows are visible, both for 'stewart-7811'. The 'Serial Number' column for both rows is highlighted in yellow. A red arrow points from the search input field at the bottom right to the highlighted serial numbers. The search input field contains '3908' and is also highlighted in red. The page number '1 - 2 of 2' is visible at the bottom right.

AP Name	Serial Number	IP Address	External IP	Model	Last Seen	Location	Uptime	Connection	Tag	Software	Actions
stewart-7811	39081005202	1.1.1.91:443	60.250.131.115:443	VF7811	May, 14 2010 16:56:28	18d 3h 17m	✓			5.3.1.0.124M	Edit
stewart-7811	39081005312	1.1.1.118:443	60.250.131.115:443	VF7811	May, 14 2010 16:56:29	18d 3h 17m	✓			5.3.2.0.146M	Edit

## Editing AP Details

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

### To edit an A P's details

1. On the *List of APs* table, look for the device that you want to edit. If 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 device properties that you want to update. Properties that you can edit include:
  - Device Tag
  - Location
  - GPS Coordinates (Latitude and Longitude)
  - Device Web Port Number Mapping
  - Device Wakeup Port Number Mapping





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

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

Figure 49. Editing AP details

AP Name	Serial Number	IP Address	External IP	Model	Last Seen	Location	Uptime	Connection	Tag	Software	Actions
stewart-7811	180801000625	1.1.1.136:443	60.250.131.115:443	VF7811	May, 14 2010 17:01:28		18d 3h 22m	✓		5.3.1.0.124M	Edit
stewart-7811	390801005202	1.1.1.91:443	60.250.131.115:443	VF7811	May, 14 2010 17:01:28		18d 3h 22m	✓		5.3.1.0.124M	Edit
stewart-7811	390801005312	1.1.1.118:443	60.250.131.115:443	VF7811	May, 14 2010 17:01:29		18d 3h 22m	✓		5.3.2.0.146M	Edit

Export As:   1 - 3 of 3

Save As View  
View Name:  Description:

Edit Tag  
Device Tag:   
Location:   
GPS Coordinates: Latitude:  Longitude:   
Device Web Port Number Mapping: 1.1.1.136:443 <-> 60.250.131.115: 443  
Device Wakeup Port Number Mapping: 1.1.1.136:8082 <-> 60.250.131.115: 8082

## Creating an 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 you 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.

### To create an AP view

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, if the view contains only 7811 APs devices, you can type **7811 APs only**.
5. Click **Save**.

## Working with Device Inventory

### Working with Standalone AP Inventory

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

Figure 50. Creating a AP view that contains only 7811 APs

The screenshot shows the Ruckus FlexMaster interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The left sidebar has 'ZoneDirectors', 'Manage ZD Views', 'Standalone APs', 'Manage AP Views', 'Clients', and 'Manage Client Views'. The main content area is titled 'Search' and contains 'AP Search Criteria' and 'List of APs'. The search criteria are set to 'Model VF7811'. The list of APs shows three entries for 'stewart-7811' with serial numbers 180801000625, 390801005202, and 390801005312. The 'Save As View' section is highlighted with a red box, showing 'View Name: 7811 APs' and 'Description: 7811 APs only'.

## Managing 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 a view.

Figure 51. The *Manage AP View* page lists all existing AP views

The screenshot shows the Ruckus FlexMaster interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The left sidebar has 'ZoneDirectors', 'Manage ZD Views', 'Standalone APs', 'Manage AP Views', 'Clients', and 'Manage Client Views'. The main content area is titled 'Manage AP Views' and contains 'List of AP Views'. The list of AP Views shows two entries: 'All Standalone APs' and '7811 APs'. The '7811 APs' view is highlighted, showing its view name, description, and actions.

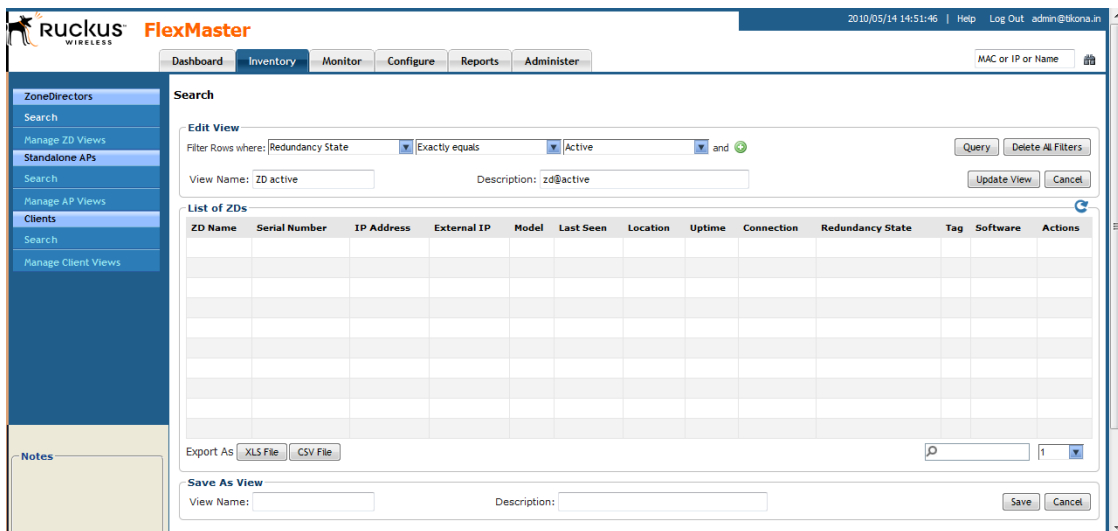
## Editing an AP View

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

### To edit an AP View

1. Go to the **Inventory > Standalone APs > Manage AP Views** page. 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 **Edit** link that is in the same row as the AP 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**.

Figure 52. Editing an AP view



## Deleting an AP View

### To delete a ZD 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 Tags

If you have a view with all the devices in the same location, you can use the geographical location of those devices as the tag to enable FlexMaster to display the devices on the *Map View*.

### To assign a tag to a view

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

Figure 53. Assigning a tag to a view

The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The left sidebar has a menu with 'ZoneDirectors', 'Manage ZD Views', 'Standalone APs', 'Manage AP Views', 'Clients', and 'Manage Client Views'. The main content area is titled 'Manage AP Views' and contains a table of AP views. The table has the following data:

View Name	Created by	Created On	Criteria	View Description	Actions
All Standalone APs	SYSTEM_USER	2010-05-11 10:26:06		All Standalone APs	<a href="#">SetTag</a> <a href="#">Query</a>
7811 APs	admin@tikona.in	2010-05-14 17:08:59	ModelName Equals To VF7811	7811 APs only	<a href="#">Edit</a> <a href="#">Del</a> <a href="#">SetTag</a> <a href="#">Query</a>

Below the table, there is an 'Edit Tag' section with a text input field containing 'Mumbai' and 'Device Tag: Mumbai' label. There are 'OK' and 'Cancel' buttons at the bottom right of the 'Edit Tag' section. A red arrow points from the 'SetTag' link in the table to the 'Edit Tag' section.

## Viewing Devices That Belong to a View

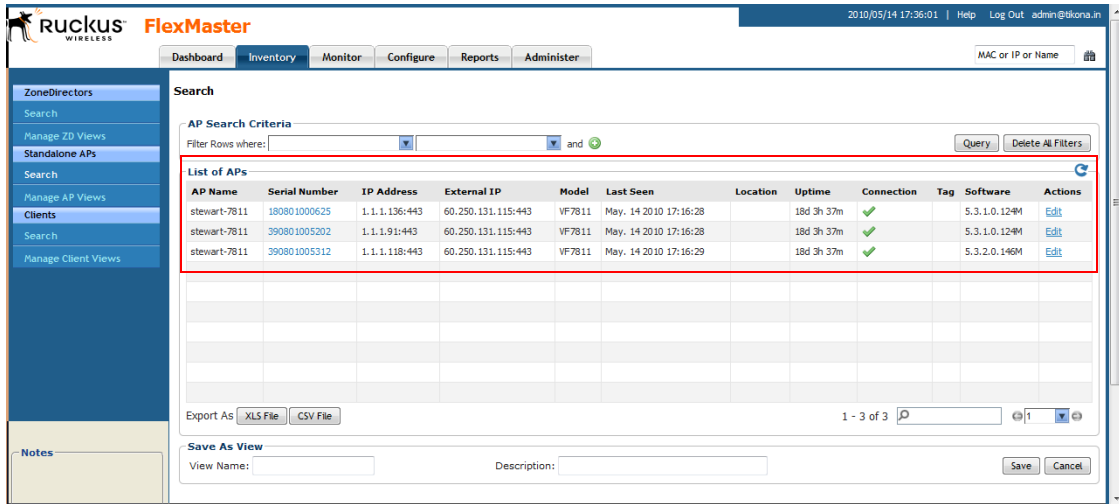
Use the **Query** link on the Manage Views page to display the devices that belong to a view.

### To run a query

1. Go to the **Inventory > Standalone APs > Manage 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.

Figure 54. After you click the Query link, devices that belong to the view appear in the List of APs section



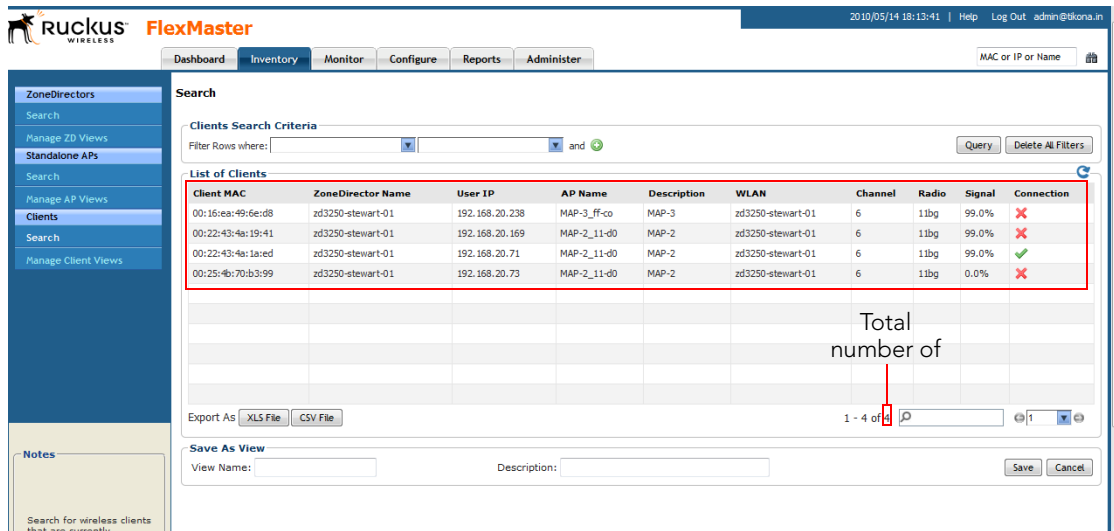
## Working with Client Inventory

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 as shown in [Figure 55](#). The total number of clients (associated with APs reporting to managed Zone-Director devices) is indicated below the table, right next to the device search box.

Figure 55. A list of clients appears in the List of Clients section



The *List of Clients* section can show up to 10 clients at a time. If managed clients on the network exceed 10, 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. Look for the **Client Search Criteria** section. To search for clients, you will 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 MAC address, (parent) ZoneDirector name, user IP address, AP name, 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 **User IP** as the attribute and you entered 172 . 17 . 16 . 176 as the search parameter, only devices with this IP address will appear in the search results.
- *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **User IP** as the attribute and you entered 100 as the search parameter, all devices with "100" in the IP address (for example, 172 . 17 . 16 . **100** and **100** . 1 . 10 . 13) will 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, only devices with serial numbers that begin with "00:16" (for example, 00 : 16 : ea : 49 : 6e : d8) will 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 **User IP** as the attribute and you entered 13 as the query parameter, only devices with model names that end in "13" (for example, 100 . 1 . 10 . **13**) will appear in the search results.

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


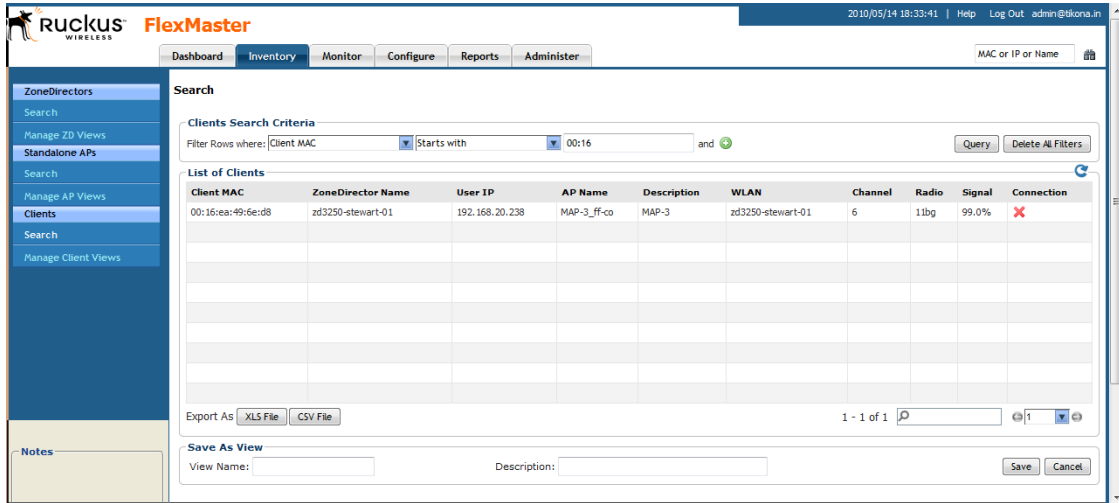
5. In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter may consist of numbers or letters (depending on be the attribute that you selected in the first drop-down list box) and may be a partial or full string. Refer to the previous step for search examples.
6. If you want to add another search filter, 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 56. Using Search Criteria to search for a client



**NOTE:** If you save your query parameters as a view, any new devices that later register with FlexMaster and meet the query criteria will be added automatically 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: See ["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, any new devices that later register with FlexMaster and meet the query criteria will be added automatically to the saved view.

#### To use the search box

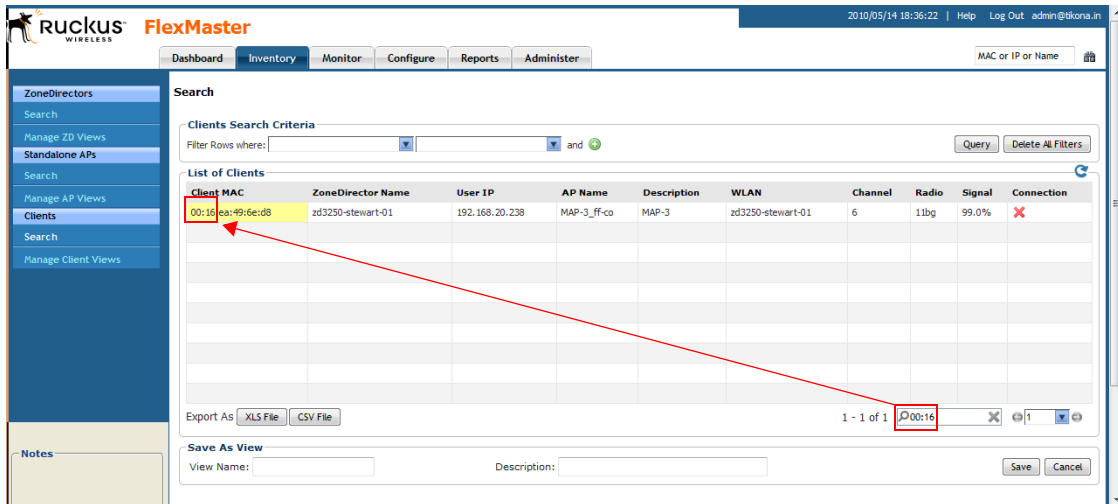
1. Type a search string into the box. The search string could be a partial or full string and may consist of numbers or letters or a combination of both.



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 57, the search string 00:16 matched part of a client's MAC address and, therefore, is highlighted in yellow.

Figure 57. 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 you want to deploy tasks to a group of devices.

### To create a client view

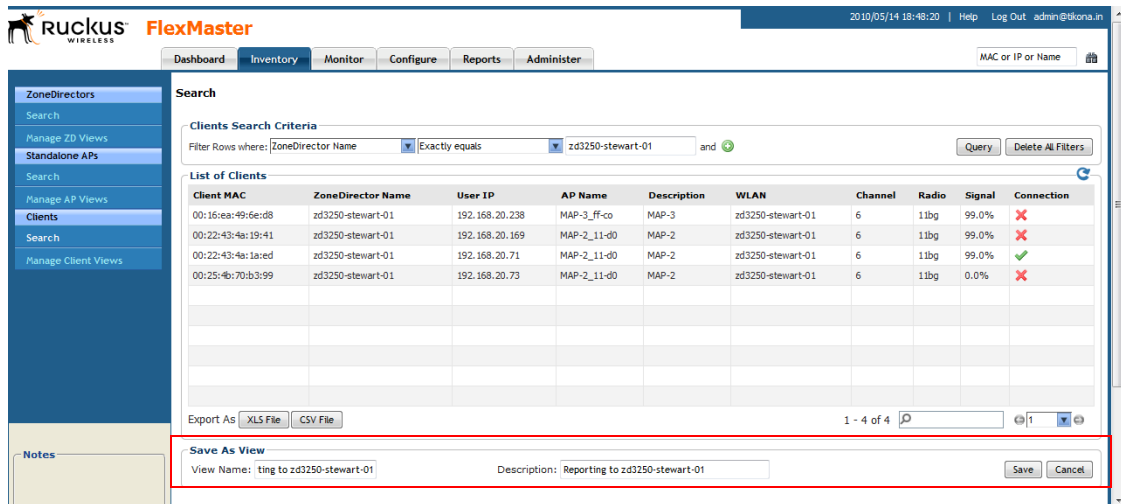
1. Perform a search for clients through one of these search methods:
  - [Search Using the Client Search Criteria](#), or
  - [Search Using the Search Box](#)
2. When the search results appear, scroll down to the *Save as View* section.
3. In **View Name**, type a name that you want to assign to the view.
4. In **Description**, type a description for the view that you are saving. For example, if the view contains only is reporting to a ZoneDirector device named `zd3250-stewart-01`, you can type **Reporting to zd3250-stewart-01**.
5. Click **Save**.

## Working with Device Inventory

### Working with Client Inventory

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

Figure 58. Creating a client view that consists of clients reporting to zd3250-stewart-01



**Search**

**Clients Search Criteria**

Filter Rows where: ZoneDirector Name Exactly equals zd3250-stewart-01 and

**List of Clients**

Client MAC	ZoneDirector Name	User IP	AP Name	Description	WLAN	Channel	Radio	Signal	Connection
00:16:ea:49:6e:d8	zd3250-stewart-01	192.168.20.238	MAP-3_ff-co	MAP-3	zd3250-stewart-01	6	11bg	99.0%	✗
00:22:43:4a:19:41	zd3250-stewart-01	192.168.20.169	MAP-2_11-d0	MAP-2	zd3250-stewart-01	6	11bg	99.0%	✓
00:22:43:4a:1a:ed	zd3250-stewart-01	192.168.20.71	MAP-2_11-d0	MAP-2	zd3250-stewart-01	6	11bg	99.0%	✓
00:25:4b:70:b3:99	zd3250-stewart-01	192.168.20.73	MAP-2_11-d0	MAP-2	zd3250-stewart-01	6	11bg	0.0%	✗

Export As: XLS File CSV File 1 - 4 of 4

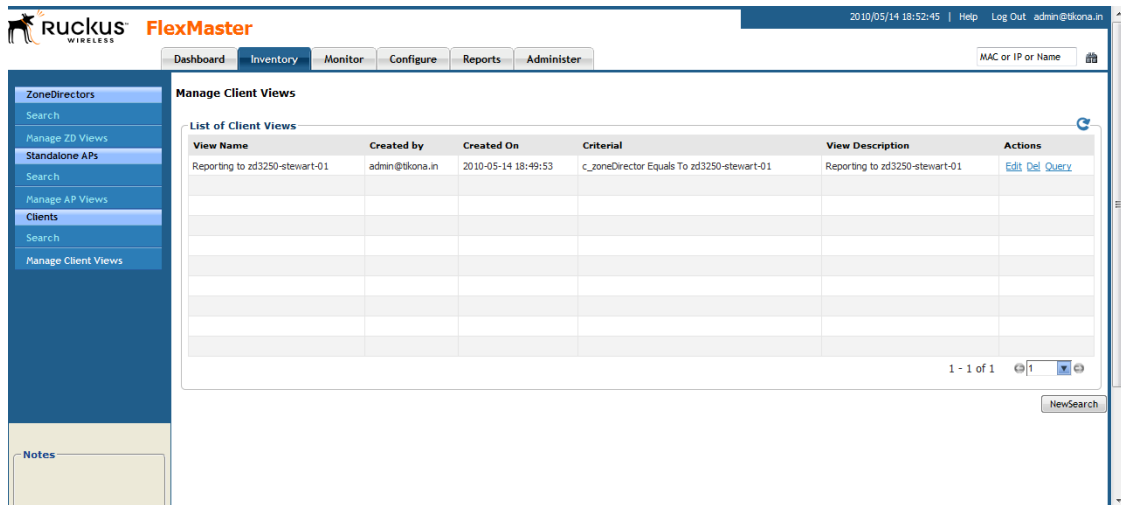
**Save As View**

View Name: tting to zd3250-stewart-01 Description: Reporting to zd3250-stewart-01 Save Cancel

## 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 59. The *Manage Client View* page lists all existing client views



**Manage Client Views**

**List of Client Views**

View Name	Created by	Created On	Critical	View Description	Actions
Reporting to zd3250-stewart-01	admin@tkona.in	2010-05-14 18:49:53	c_zoneDirector Equals To zd3250-stewart-01	Reporting to zd3250-stewart-01	Edit Del Query

1 - 1 of 1 NewSearch

## Editing a Client View

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

### To edit 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.
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 60. Editing a client view

The screenshot shows the 'Edit View' interface. At the top, there is a 'Search' section with an 'Edit View' title. Below this, there are two filter rows: 'Filter Rows where: ZoneDirector Name' with a dropdown set to 'Exactly equals' and a text input containing 'zd3250-stewart-01', and 'and' followed by a green checkmark icon. To the right of these filters are 'Query' and 'Delete All Filters' buttons. Below the filters, there are two text input fields: 'View Name: Reporting to zd3250-stew;' and 'Description: Reporting to zd3250-stewart-01'. To the right of these fields are 'Update View' and 'Cancel' buttons. Below the filter section is a 'List of Clients' section with a table. The table has the following columns: Client MAC, ZoneDirector Name, User IP, AP Name, Description, WLAN, Channel, Radio, Signal, and Connection. The table is currently empty. Below the table, there is an 'Export As' section with 'XLS File' and 'CSV File' buttons, a search icon, and a dropdown menu set to '1'. At the bottom, there is a 'Save As View' section with 'View Name:' and 'Description:' text input fields, and 'Save' and 'Cancel' buttons. On the left side of the interface, there is a navigation menu with items: ZoneDirectors, Search, Manage ZD Views, Standalone APs, Search, Manage AP Views, Clients, Search, and Manage Client Views. At the bottom left, there is a 'Notes' section with a small text box containing instructions: 'Search for wireless clients that are currently associated with managed APs. You can also save the search results as a...'

## Deleting a Client View

### To delete 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 **Del** 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.

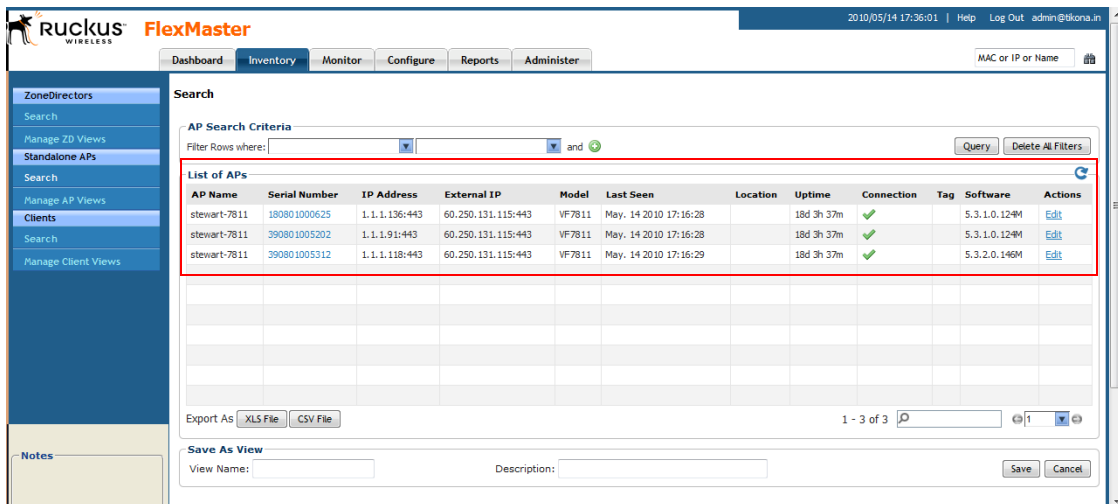
## Viewing Clients That Belong to a View

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

### To run a query

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.

Figure 61. After you click the *Query* link, clients that belong to the view appear in the *List of Clients* section



The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The left sidebar contains a menu with 'ZoneDirectors', 'Manage ZD Views', 'Standalone APs', 'Manage AP Views', 'Clients', and 'Manage Client Views'. The main content area is titled 'Search' and contains an 'AP Search Criteria' section with a 'Filter Rows where:' dropdown and a 'Query' button. Below this is a table titled 'List of APs' with the following data:

AP Name	Serial Number	IP Address	External IP	Model	Last Seen	Location	Uptime	Connection	Tag	Software	Actions
stewart-7811	180801000625	1.1.1.136:443	60.250.131.115:443	VF7811	May, 14 2010 17:16:28		18d 3h 37m	✓		5.3.1.0.124M	<a href="#">Edit</a>
stewart-7811	390801005202	1.1.1.91:443	60.250.131.115:443	VF7811	May, 14 2010 17:16:28		18d 3h 37m	✓		5.3.1.0.124M	<a href="#">Edit</a>
stewart-7811	390801005312	1.1.1.118:443	60.250.131.115:443	VF7811	May, 14 2010 17:16:29		18d 3h 37m	✓		5.3.2.0.146M	<a href="#">Edit</a>

Below the table, there are 'Export As' buttons for 'XLS File' and 'CSV File', and a 'Save As View' section with 'View Name:' and 'Description:' input fields, and 'Save' and 'Cancel' buttons.

# Managing a Single Standalone Access Point

## In This Chapter

<a href="#">About the Device View</a> .....	100
<a href="#">Viewing Device Summary</a> .....	103
<a href="#">Viewing and Editing Device Details</a> .....	105
<a href="#">Performing Device Diagnostics</a> .....	108

## About the 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 that specific standalone AP without having to provision tasks. You can use the Device View when you only want to manage a single standalone AP.

Figure 62. Clicking a standalone AP's serial number opens the Device View

The screenshot shows the FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. A search bar is present with the text 'MAC or IP or Name'. The left sidebar contains various menu items like 'ZoneDirectors', 'Clients', and 'Standalone APs'. The main content area is titled 'List of APs' and contains a table with columns: AP Name, Serial Number, IP Address, External IP, Model, Last Seen, Location, Uptime, Connection, Tag, Software, and Actions. The first row is highlighted, and a tooltip points to the serial number '180801000625'.

AP Name	Serial Number	IP Address	External IP	Model	Last Seen	Location	Uptime	Connection	Tag	Software	Actions
stewart-7811	180801000625	1.1.1.136:443	60.250.131.115:443	VF7811	May. 28 2010 11:03:58	31d 21h 12m	31d 21h 12m	✓		5.3.1.0.124M	Edit
stewart-7811	3908010005312	1.1.1.118:443	60.250.131.115:443	VF7811	May. 28 2010 11:05:33	31d 21h 14m	31d 21h 14m	✓		5.3.1.0.124M	Edit
stewart-7811	3908010005312	1.1.1.118:443	60.250.131.115:443	VF7811	May. 28 2010 11:05:48	31d 21h 14m	31d 21h 14m	✓		5.3.2.0.146M	Edit
RuckusAP	430701003921	192.168.0.31:443	192.168.0.31:443	ZF2942	Apr. 14 2010 19:14:14	7h 31m		✗		7.4.0.0.24	Edit
RuckusWB	450955000498	10.0.66.199:443	10.0.66.199:443	ZF7731	Feb. 22 2010 14:27:16	2d 3h 53m		✗		8.2.0.0.33	Edit
RuckusWB	450955000541	10.0.66.198:443	10.0.66.198:443	ZF7731	Feb. 22 2010 14:25:25	40d 22h 8m		✗		8.2.0.0.33	Edit
RuckusAP	510855000002	192.168.1.100:443	113.193.16.5:443	ZF2741	Apr. 29 2010 20:11:18	2h 4m		✗		7.4.0.0.30	Edit

Figure 63. The Device View opens in a new browser window

The screenshot shows the 'Device View' for a specific AP. The top navigation bar includes 'Summary', 'Details', and 'Diagnostics'. The left sidebar contains a search form and a 'Reboot' button. The main content area is titled 'Device View' and contains a 'Summary' section with a device image and a 'Details' section with various parameters.

**Summary**

Find Another Device by Serial Number:  OR MAC Address:

Current Device: Serial Number: 180801000625 Model Type: VF7811

**SSIDs**

- stewart-7811-02(00:00:00:00:00:00)

**Details**

Model Type: VF7811  
 Customer ID: ruckus  
 Device Name: stewart-7811  
 MAC Address: 00:1F:41:24:89:F0  
 Serial Number: 180801000625  
 Firmware Version: 5.3.1.0.124M  
 Service Provider Login Name: super  
 Device Last Seen: May. 28 2010 11:08:58  
 IP Address: 1.1.1.136  
 External IP: 60.250.131.115  
 Server URL: http://60.250.131.116/intune/server  
 Periodic Inform Status:  Enabled  
 Periodic Inform Interval: 5 minutes  
 Uptime: 31d 21h 17m  
 Associated-Clients Monitoring Mode:  Disabled



---

**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"](#).

---

## Device View for ZoneDirector

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.

If the ZoneDirector device that you want to manage is behind a firewall or NAT server, FlexMaster will be unable to redirect you to the ZoneDirector Web interface until port mapping is configured. For instructions on how to edit a ZoneDirector device's port mapping, refer to ["Editing ZoneDirector Details"](#).

## Device View Tabs

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. [Table 17](#) lists the tabs that are available on the Device View.

Table 17. 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 <a href="#">"Viewing Device Summary"</a> .
Details	Displays network configuration information and provides options for editing these settings. For more information, refer to <a href="#">"Viewing and Editing Device Details"</a> .
Diagnostics	Provides options for running a PING test from the device and for viewing logs. For more information, refer to <a href="#">"Performing Device Diagnostics"</a> .

Also noteworthy are the status boxes located in the lower-left and upper-right corners of the page.

- The lower-left box displays statuses related to user actions. For example, if you use the Find Another Device View window to search for another AP, the lower-left box will show if a matching device has been found.
- The upper-right box displays statuses related to device operations. For example, if 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**

## Managing a Single Standalone Access Point

### About the Device View

**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, this status box displays the requested change and the user who initiated the change. You can force a status refresh by clicking the **Refresh Now!** link.

Figure 64. The ZoneFlex 2942 AP Device View

The screenshot shows the FlexMaster web interface for a ZoneFlex 2942 AP. At the top, there are navigation tabs: Summary, Details, and Diagnostics. The 'SUMMARY' section displays the following information:

- Model Type: ZF2942
- Customer ID: hboss
- Device Name: Ruckus\_Meet
- MAC Address: 00:1F:41:0F:C1:D0
- Serial Number: 100801003584
- Firmware Version: 8.2.0.0.53
- Service Provider Login Name: admin
- Device Last Seen: Jan. 08 2010 16:23:09
- IP Address: 192.168.0.233
- External IP: 202.55.228.100
- Server URL: http://97.74.124.173/intune/server
- Periodic Inform Status: Enabled
- Periodic Inform Interval: 1 minute
- Uptime: 9d 23h 56m

The 'SSIDs' section lists several wireless networks, each with a status icon (green for success, red for error):

- NEC(00:1f:41:0f:c1:d8) [Success]
- Wireless 2(00:00:00:00:00:00) [Error]
- Wireless 3(00:00:00:00:00:00) [Error]
- Wireless 4(00:00:00:00:00:00) [Error]
- Wireless 5(00:00:00:00:00:00) [Error]
- Wireless 6(00:00:00:00:00:00) [Error]
- Wireless 7(00:00:00:00:00:00) [Error]
- Wireless 8(00:00:00:00:00:00) [Error]

The 'Associated Stations' table shows the following columns: MAC Address, IP Address, Authentication State, Transmit RSSI, Receive RSSI, Throughput Estimated, Received Packets, Sent Packets, Packets in Queue, Packets Dropped by Queue Overflow, and Packets Dropped by Excessive Rate/Time.

The 'Status Area' in the top right corner displays the following task logs:

- Task: #214 Serial Number: 100801002944 Status: Success
- Task: #213 Serial Number: 100801002944 Status: Success
- Task: #214 Serial Number: 100801002944 Status: Started
- Task: #213 Serial Number: 100801002944 Status: Started



## Viewing Device Summary

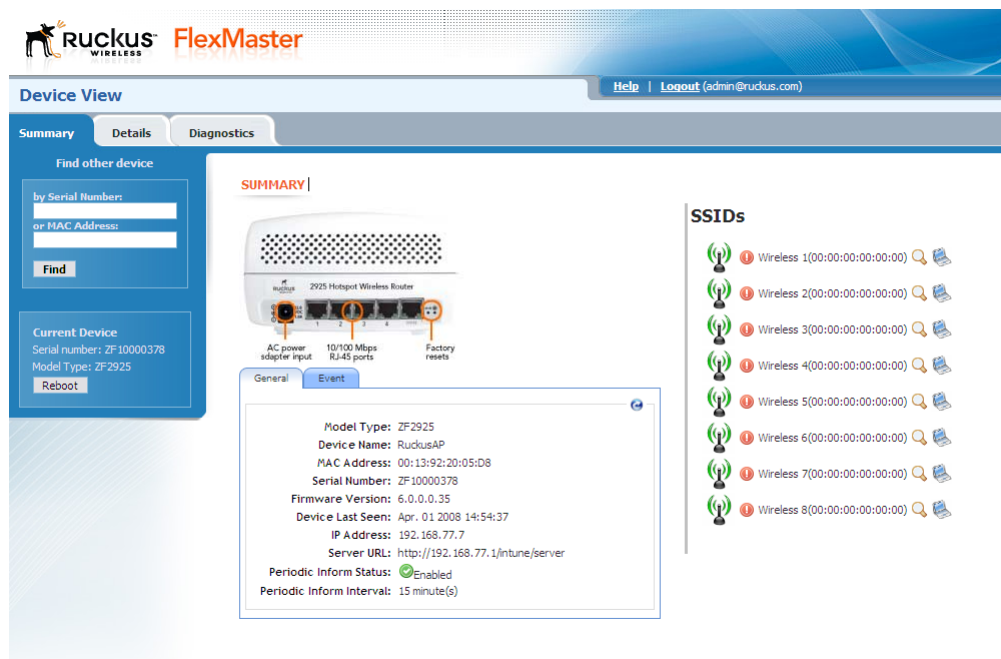
The *Summary* tab offers a quick look at general details of the device, including a picture of the device model, the device name, IP address, and available SSIDs.

[Table 18](#) lists the tasks that you can perform on the Summary tab.

Table 18. Tasks you can perform on the Summary tab

Task	How To Do It
Find another device	In the <i>Find other device</i> box on the upper left corner of the page, type the serial number or MAC address of another device, and then click <b>Find</b> to find matching devices.
Reboot the device	Under <i>Current Device</i> , click <b>Reboot</b> 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 <b>Events</b> tab under the picture of the device opens a summary of device events.
View SSID details	Click the icons to display SSID status and settings, including associated clients.

Figure 65. The Summary tab of Device View



## Managing a Single Standalone Access Point

### Viewing Device Summary

Take note of the magnifying glass and laptop icons in the *SSIDs* section of the page. Clicking these icons opens details below the *SSIDs* table corresponding to the device type. Devices show details on associated clients, including their MAC addresses, IP addresses, and authentication statuses.



**NOTE:** If a wireless client obtained its IP address from the Ruckus Wireless device with which it is associated, the IP address appears under the IP address column. However, if it obtained its IP address from another DHCP server on the network or directly from the ISP, the IP address column shows Not available.

Figure 66. Clicking the laptop icon shows details about stations currently associated with the AP

**SUMMARY**

Model Type: ZF2942  
 Customer ID: #bss  
 Device Name: Ruckus\_Meet  
 MAC Address: 00:1F:41:0F:C1:D0  
 Serial Number: 100801003584  
 Firmware Version: 8.2.0.0.53  
 Service Provider Login Name: admin  
 Device Last Seen: Jan. 08 2010 16:23:09  
 IP Address: 192.168.0.233  
 External IP: 202.55.228.100  
 Server URL: http://97.74.124.173/intune/server  
 Periodic Inform Status: ✔Enabled  
 Periodic Inform Interval: 1 minute  
 Uptime: 9d 23h 56m

\*This device is not directly reachable; it might be offline or behind a firewall.

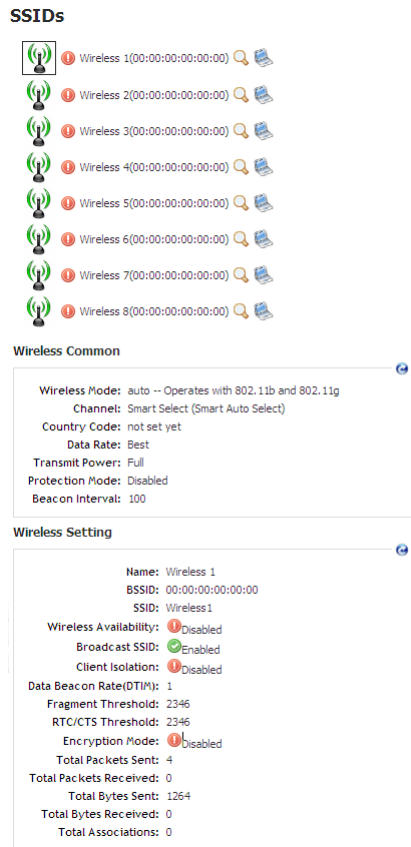
**SSIDs**

- ✔ NEC(00:1f:41:0f:c1:d8)
- ! Wireless 2(00:00:00:00:00:00)
- ! Wireless 3(00:00:00:00:00:00)
- ! Wireless 4(00:00:00:00:00:00)
- ! Wireless 5(00:00:00:00:00:00)
- ! Wireless 6(00:00:00:00:00:00)
- ! Wireless 7(00:00:00:00:00:00)
- ! Wireless 8(00:00:00:00:00:00)

**Associated Stations**  
 The following devices are associated with this AP.

MAC Address	IP Address	Authentication State	Transmit RSSI	Receive RSSI	Throughput Estimated	Received Packets	Sent Packets	Packets in Queue	Packets Dropped by Queue Overflow	Packets Dropped by Excessive Retries	Packets Dropped by Excessive Time
00:0e:35:26:10:b7		✔	0	27	31015	3033	131585	0	0	82	132
00:0e:35:36:00:96		✔	0	18	23072	2357	38560	0	0	71	128
00:1d:e0:0c:75:b7		✔	0	23	28179	11302	119951	0	1687	131	713

Figure 67. Clicking the magnifying glass icon shows a summary of the AP's wireless settings



## 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 under the **Details** tab, the page that displays is a static view (view-only) of the details for that option. You click the **Edit Settings** button to edit option details.

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

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



**NOTE:** Managed devices will attempt to contact FlexMaster at the specified inform interval. If an AP is unable to contact FlexMaster after one hour, it will automatically extend 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, it may extend the inform interval to 15 minutes. The AP will continue to extend the interval exponentially 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:** For all **Device View > Details** configuration options, refer to the user guide appropriate to the Ruckus Wireless device type.

---



**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.

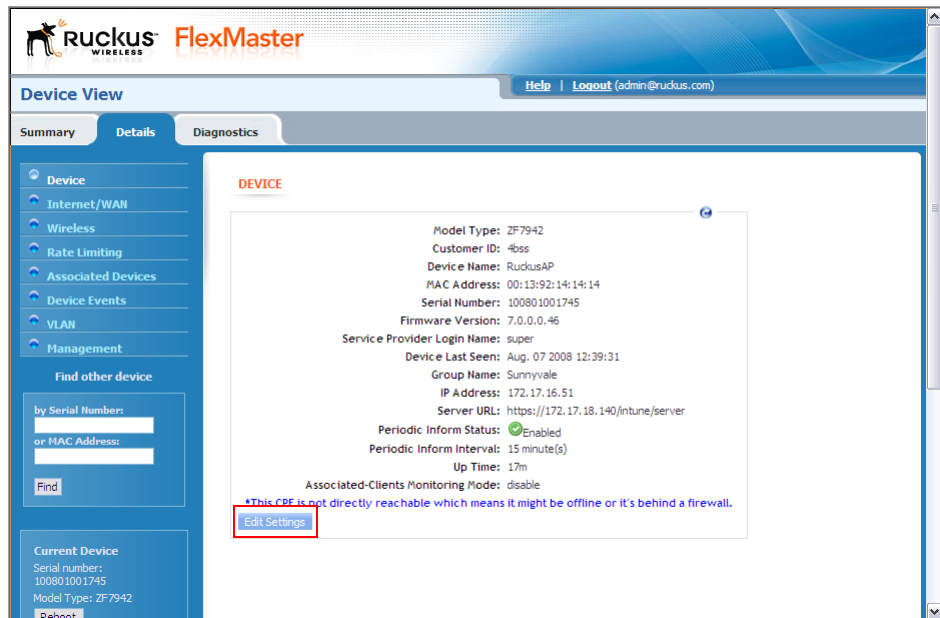
---



**NOTE:** ZoneFlex 7962 AP has two built-in radios. Its Summary page, therefore, shows details about two radios.

---

Figure 68. To change the device settings, click Edit Settings



## Configuring Replacement Options for ZoneFlex 7731 Wireless Bridge

If you have a pair of ZoneFlex 7731 Wireless Bridge devices that are 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.



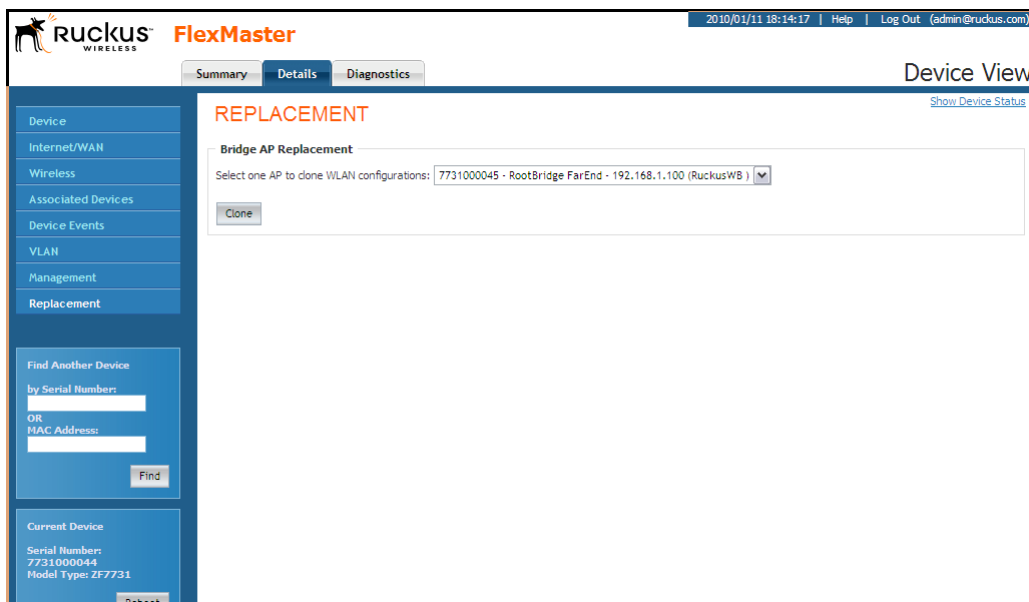
**NOTE:** This option is only available on the Device View of ZoneFlex 7731 Wireless Bridge.

### 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 **Replacement** on the 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 then copies them to the replacement unit.

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

Figure 69. The Replacement page for ZoneFlex 7731 Wireless Bridge



## 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 **Input IP** option and enter an IP address in the accompanying text field to ping the destination address by clicking **Start**.

### Viewing the Device Log

Click **Retrieve Log from Device** to retrieve the device's log and save it to your client (**Save Log to Local File**) and/or email it to Ruckus Wireless Technical Support (**Send Email to Support**). 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 will time out. Ruckus Wireless recommends upgrading all FlexMaster managed APs to the latest version to retrieve logs successfully.



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



**NOTE:** If a managed AP is behind a NAT server and you click the Retrieve Log from Device button, FlexMaster will be 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, 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.*

Figure 70. Example of a successful PING test

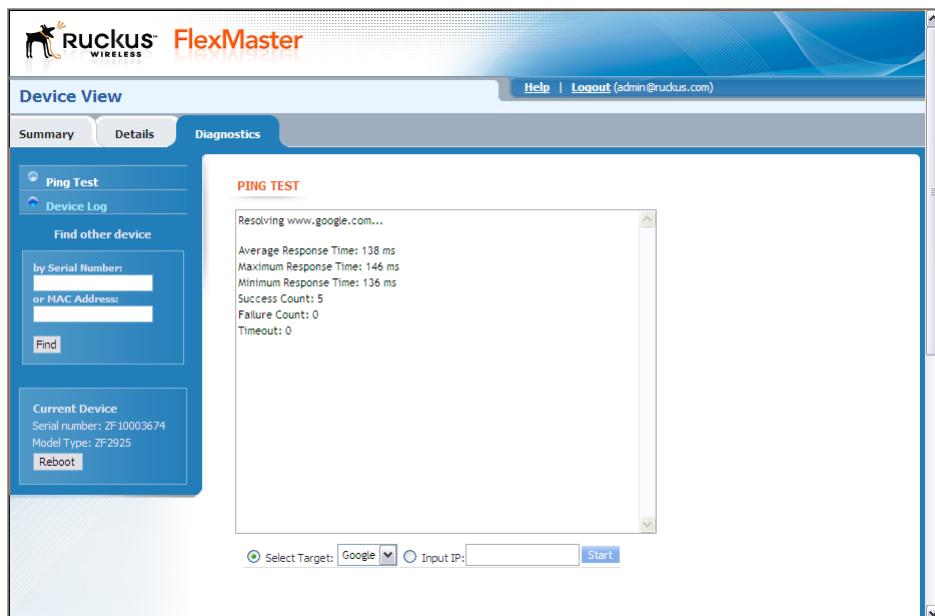


Figure 71. Example of a failed PING test

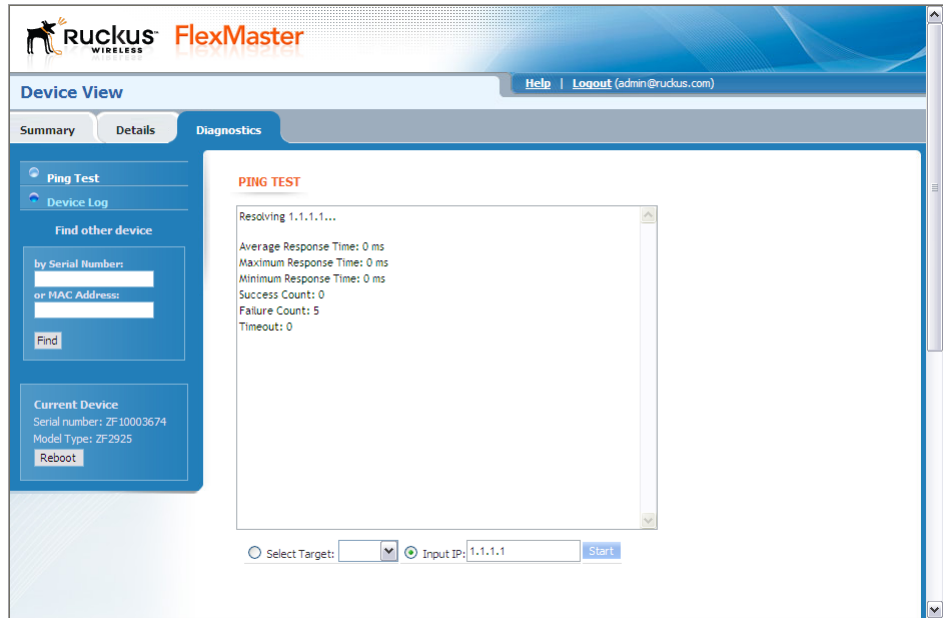




Figure 72. The Device Log page

**RUCKUS WIRELESS FlexMaster**

Help | Logout (admin@ruckus.com)

Device View

Summary | Details | **Diagnostics**

Ping Test  
Device Log  
Find other device  
by Serial Numbers  
or MAC Address  
Find  
Current Device  
Serial number: ZF10003674  
Model Type: ZF-2925  
Reboot

**DEVICE LOG**

Device Management Status Log File

```
----733755057
Content-Disposition: form-data; name="logfile.txt";
filename="/tmp/logfile.txt"
Content-Type: text/plain

122.182564 (619) Save Event: 6 CONNECTION REQUEST
CommandKey:
122.184254 (619)Save Event: 6 CONNECTION REQUEST | | : 0
122.184633 (619)InformLock is now unlocked
122.185886 (585)Inform activation by signal at Mon Aug 18 03:37:50
2008
122.222499 (585) rks_pre_session_setup_l2tp: ip=0.0.0.0'
netmask=0.0.0.0' gw='172.17.16.1'
user=" passwd="
122.223961 (585)locking InformLock
122.224251 (585)InformLock now locked
122.224505 (585)locking paramLock
122.224761 (585)iparamLock now locked
InformLock and paramLock now both locked122.225030 (585) just
before calling dimarkMain
122.226210 (585) VmSize:          7924 kB
122.226633 (585) VmData:         4036 kB
122.226961 (585) VmStk:          208 kB
122.227289 (585) VmExe:          1244 kB
122.227622 (585) VmLib:          2268 kB
122.229903 (585) tr069d: main: acs_is_known_flag=1
122.242027 (619)wait on soap_accept
122.265746 (585)ProductClass: ZoneFlex
122.267101 (585)SerialNumber: ZF10003674
```

AP Configuration Log File

```
----733747703
Content-Disposition: form-data; name="supportLogfile.txt";
filename="/tmp/supportLogfile.txt"
Content-Type: text/plain

### Boot Version ###
Boot Version: RB.0.3.2.1 - built 17:06:18, Jun 26 2006

### Active SW ###
SW Version: 7.0.0.0.45

### Firmware Upgrade ###
Check Result: not running

### SW images on flash ###
#Main image Control+Header Info#<Control Info>
ipaddr: 0.0.0.0
file: //intune//fw?fw=3
size: 4833280 MD5:
B08369334C404C4196B7800CB0868A37
type: 0
local_file
<Image1 FW header>
Magic: RCKS
next_image: d0000
invalid: 0
hdr_len: 160
compression: 17
load_address: 0x80041000
```

Retrieve Log from Device | Save Log to Local File | Send E-Mail to Support

Status Area - Click here to open

Copyright © 2008 Ruckus Wireless.

## Managing a Single Standalone Access Point

Performing Device Diagnostics

# Monitoring Events and Network Activities

**In This Chapter**

<a href="#">About the Monitor Page</a> .....	114
<a href="#">Monitoring Events</a> .....	114
<a href="#">Managing Event Views</a> .....	119
<a href="#">Viewing the Event Timeline</a> .....	120
<a href="#">Configuring Alert Properties</a> .....	124
<a href="#">Measuring Throughput Using SpeedFlex</a> .....	126
<a href="#">Monitoring Clients</a> .....	129

## 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.

## 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 *Events* table columns include:

- *Event Type*: Ruckus Wireless-designated event title
- *Serial Number*: Serial number of the device
- *Model Name*: Model of the device
- *Timestamp*: Time the event occurred
- *Detail*: Clicking the **View Parameters** link under this column displays the parameter that was sent for the event and the parameter value.

### To monitor events for one or more managed devices

1. Go to **Monitor > Events**. The *Events* table displays the most current events for all managed devices.
2. If you want view events based on a specific set of criteria, you can configure the Events Search Criteria. For more information, refer to ["Searching for Events"](#).

## 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 the **Monitor > Events**.
2. Look for the **Events Search Criteria** section. To search for events, you will 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 event type, serial number, model name, MAC address, description, and event timestamp.

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 Name** as the attribute and you entered ZD3250 as the search parameter, only devices of this model will 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, all devices with "100" in the IP address (for example, 100903000031 and 110901000282) will 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, only devices with serial numbers that begin with "3208" (for example, 320833000219) will 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, only devices with model names that end in "001" (for example, 100903000001) will 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 may consist of numbers or letters (depending on be the attribute that you selected in the first drop-down list box) and may be a partial or full string. Refer to the previous step for search examples.
6. If you want to add another search filter, 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 73. Using Search Criteria to search for an event

The screenshot shows the FlexMaster web interface. At the top, there is a navigation bar with tabs for Dashboard, Inventory, Monitor, Configure, Reports, and Administer. The 'Monitor' tab is selected. Below the navigation bar, there is a search box for 'MAC or IP or Name'. The main content area is titled 'Events' and contains an 'Events Search Criteria' section with a filter for 'Serial Number' starting with '100'. Below this is a 'List of Events' table with columns for Event Type, Serial Number, Model Name, MAC Address, Description, Event Timestamp, and Detail. The table lists several events, including connectivity problems and AP channel changes. At the bottom of the table, there are options to 'Export As' (XLS File, CSV File) and 'Save As View' (View Name, Description, Save, Cancel).

Event Type	Serial Number	Model Name	MAC Address	Description	Event Timestamp	Detail
Connectivity problem	100903000031	ZD3250	00:24:82:32:ce:3c	ZD	Jun. 03 2010 04:48:45	
Connectivity problem	100903000282	ZD3250	00:24:82:32:d0:32	ZD	Jun. 03 2010 04:48:45	
Connectivity problem	100903000307	ZD3250	00:24:82:32:d0:64	ZD	Jun. 03 2010 04:48:45	
Connectivity problem	100903000321	ZD3250	00:24:82:32:d0:80	ZD	Jun. 03 2010 13:13:53	
AP channel change	100903000322	ZD3250	00:22:7f:28:e2:00	ZDAP	Jun. 03 2010 04:48:45	[Poonam Tower-4 (R@00:24:82:26:55:b0) detects interference on rad
MAP disconnect	100903000322	ZD3250	00:22:7f:28:e2:00	ZDAP	Jun. 03 2010 04:48:45	Mesh [Poonam NagarB3 B4@00:22:7f:28:ad:00] disconnects from [RN
AP channel change	100903000322	ZD3250	00:22:7f:28:e2:00	ZDAP	Jun. 03 2010 04:48:45	[Jahangir Tower-3 @04:4f:aa:34:0b:90] detects interference on radio
AP lost heartbeat	100903000322	ZD3250	00:22:7f:28:e2:00	ZDAP	Jun. 03 2010 04:48:45	[Poonam NagarB3 B4@00:22:7f:28:ad:00] heartbeats lost
MAP root downlink connected	100903000322	ZD3250	00:22:7f:28:e2:00	ZDAP	Jun. 03 2010 04:48:45	Root [RNA Courtyard F w@00:22:7f:28:4a:a0] accepts Mesh [Poonam
MAP root downlink connected	100903000322	ZD3250	00:22:7f:28:e2:00	ZDAP	Jun. 03 2010 04:48:45	Root [RNA Courtyard F w@00:22:7f:28:4a:a0] accepts Mesh [Poonam



**NOTE:** If you save your query parameters as a view, any new events that occur after you create the view and meet the query criteria will be added automatically 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: See [“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.



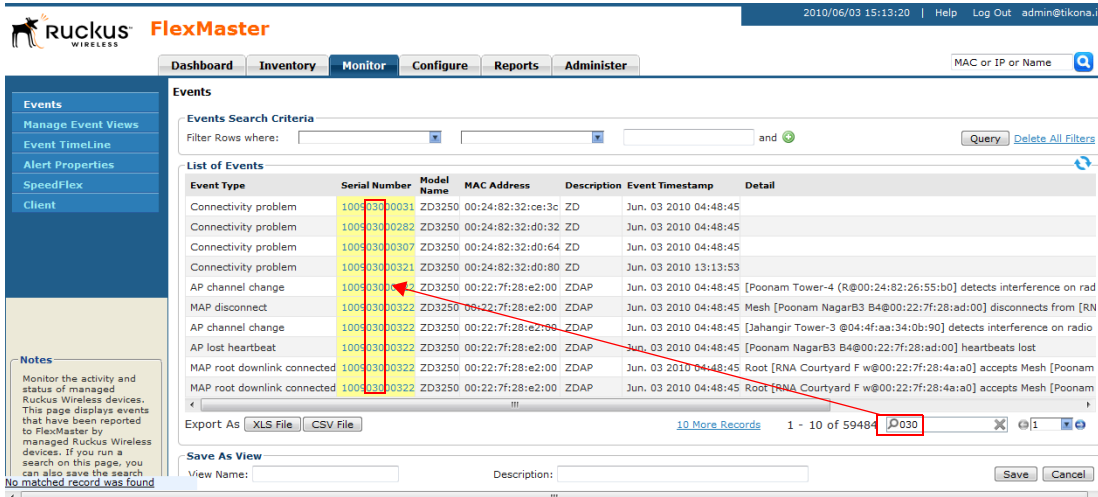
**NOTE:** If you save your query parameters as a view, any new events that occur after you create the view and meet the query criteria will be added automatically to the saved view.

**To use the search box**

1. Type a search string into the box. The search string could be a partial or full string and may 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 Events* table. The event property that matches the search string is highlighted in the table. In [Figure 74](#), the search string '030' matched part of devices' serial numbers on which events occurred and, therefore, are highlighted in yellow.

Figure 74. The device property that matches the search string is highlighted in the search results



**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.

**To create an event view**

1. Perform a search for event through one of these search methods:
  - [Search Using the Events 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.

## Monitoring Events and Network Activities

### Creating an Event View

4. In **Description**, type a description for the view that you are saving. For example, if 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.

Figure 75. Saving search results as an event view

The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The 'Monitor' tab is active. On the left, there is a sidebar with 'Events' selected. The main content area displays a table of events with columns for Event Type, Serial Number, Model Name, MAC Address, Description, Event Timestamp, and Detail. Below the table, there are options to export as XLS or CSV file, and a 'Save As View' dialog box is open. The dialog box has a red border and contains the following text:

**Save As View**  
View Name: Events with serial 030  
Description: Devices with serial 030  
[Save] [Cancel]

At the bottom of the interface, it says 'Copyright © 2010 Ruckus Wireless.' and 'No matched record was found'.



## 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.

Figure 76. The *Manage Event View* page lists all existing event views

The screenshot displays the 'Manage Event Views' interface in the Ruckus FlexMaster web application. The page title is 'Manage Event Views' and it shows a 'List of Event Views' table. The table contains one entry with the following details:

View Name	Created by	Created On	Criteria	View Description	Actions
ZD3250 Only	admin@tikona.in	2010-06-03 15:42:19	modelName Equals To ZD3250	ZD3250 Only	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Query</a>

Below the table, there is a 'New Search' button and a pagination indicator showing '1 - 1 of 1'. The page also features a 'Notes' section on the left side with the text: 'Search for a device event from saved Event Views. You can also edit Event Views from this page.'

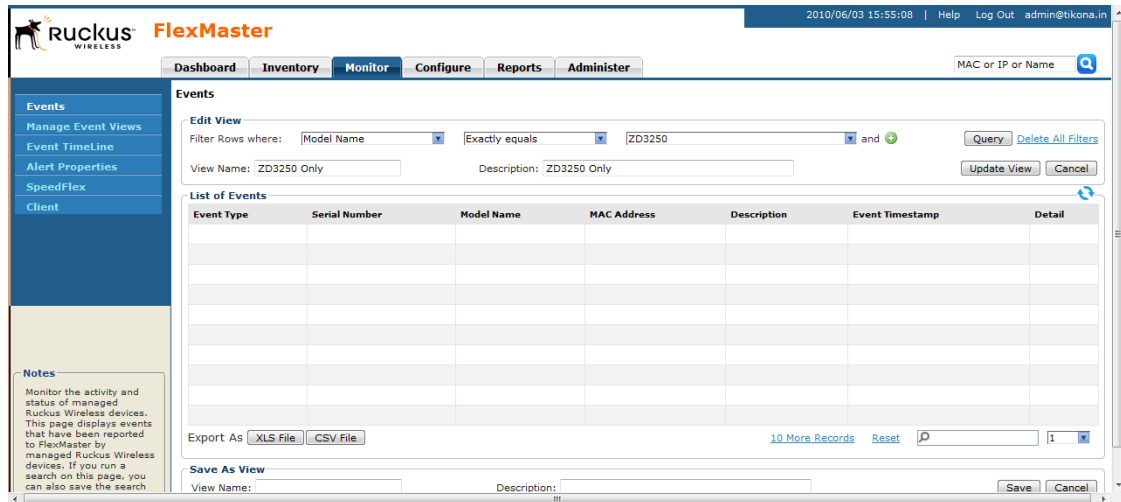
## Editing an Event View

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

### To edit an event view

1. Go to the **Monitor > Manage Event Views** page. All existing event views appear in the *Manage Event Views* section.
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**.

Figure 77. Editing an event view



## Deleting an Event View

### To delete an event view

1. Go to the **Inventory > ZoneDirector > Manage Views** page.
2. Look for the ZD 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.

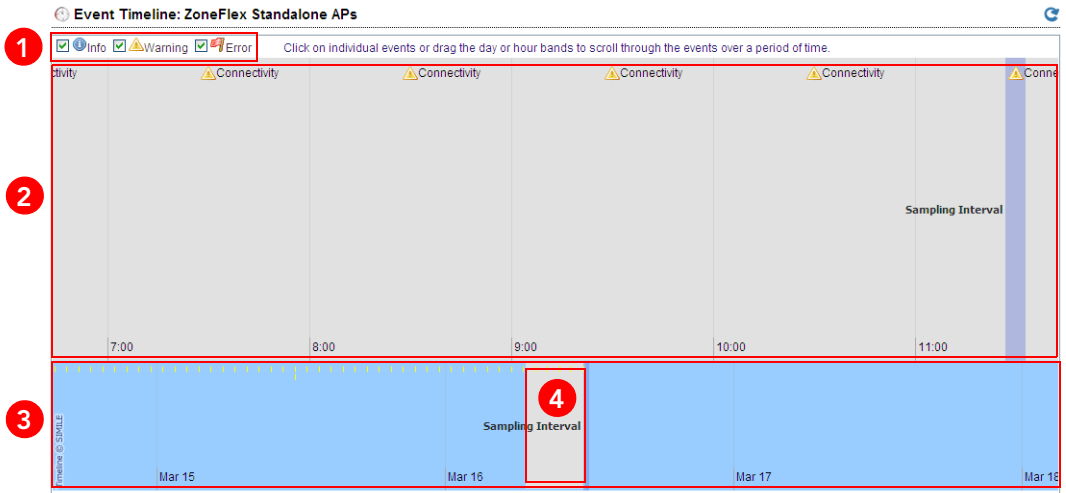
The Manage Views page refreshes, and then the view that you deleted disappears from the page.

## 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 split 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, and
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 78. The Event Timeline widget

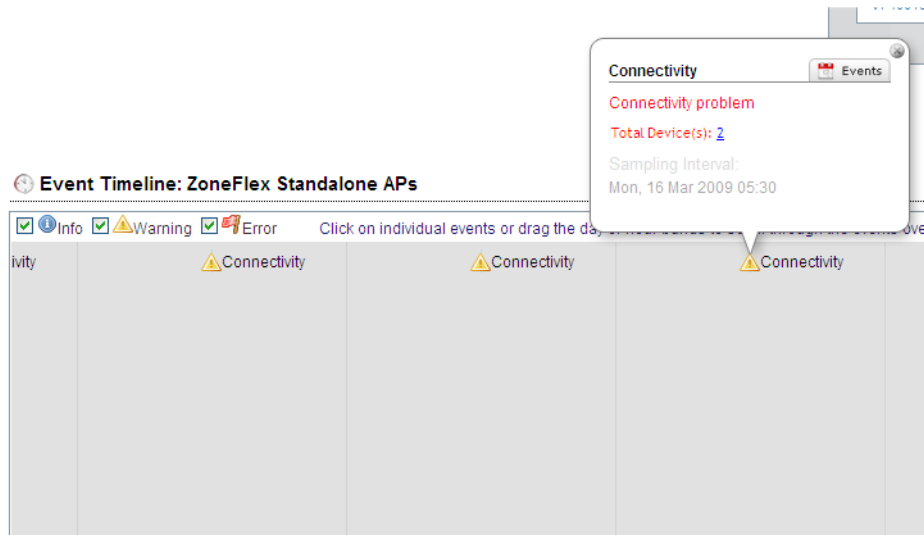


The Event Timeline widget uses the following conventions:

**Table 1:**

Device View widget	Click the <b>Event Timeline</b> link under the <i>Event Details</i> column to filter the Event Timeline graph based on the corresponding device view. By default, the graph defaults to <i>All Standalone APs</i> .
Event Severity	Info (blue), Warning (yellow) and Error (red) check boxes: <ul style="list-style-type: none"> <li>• <i>Informational</i> events are lowest in severity, and are typically associated with configuration changes or device boot up.</li> <li>• <i>Warnings</i> events relate to device connectivity and communication.</li> <li>• <i>Errors</i> are critical events affecting the device's functionality.</li> </ul>
Event Detail	Clicking an event from the gray area pops up an event window. You can click the <i>Total Device(s)</i> link displayed in this pop-up window to go to a <b>Monitor &gt; Reports</b> view of the selected event. As the event may cover multiple devices, each device is displayed individually in the report.

Figure 79. The Event Detail pop-up window



## 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” according to the hour in which they occurred. Thus, if there were seven events between 11:00 AM and 12:00 PM, there would be seven segments stacked in the blue area of the Event Timeline according to the day and time.

Figure 80. Colored segments on the Events Timeline widget



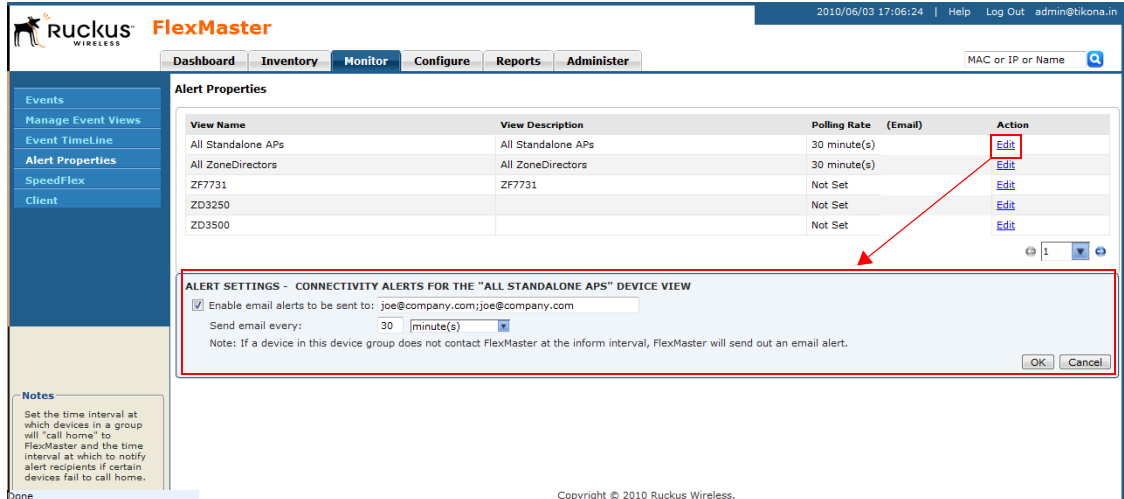
### Hold and Drag

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.


Figure 81. Editing the alert property of a group



## To configure Alert Properties settings for a device view

1. Go to **Monitor > Alert Properties**. All existing device views are listed.



**NOTE:** The Alert Properties page can display up to five device views. If FlexMaster has more than five device views, you will need to click the  icon at the bottom-right side of the page to view the other device views on the next page.

2. Under 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 **Enable email alerts to be sent 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. If 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.

[Figure 82](#) shows an example of the alert email message. If 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 82. 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

If 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, and then clear the **Enable email alerts to be sent to** check box.

Figure 83. Click the Cancel link to disable alert notifications for the device group

The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The 'Alert Properties' page is displayed, showing a table with columns for View Name, View Description, Polling Rate, (Email), and Action. The 'Cancel' link in the Action column for the 'All Standalone APs' row is highlighted with a red box. A sidebar on the left contains navigation links for Events, Manage Event Views, Event TimeLine, Alert Properties, SpeedFlex, and Client. A 'Notes' section at the bottom left provides instructions on setting time intervals for device calls home.

View Name	View Description	Polling Rate	(Email)	Action
All Standalone APs	All Standalone APs	30 minute(s)	joe@company.com;joe@company.com	Edit <b>Cancel</b>
ZF7731	ZF7731	1 day(s)		Edit
ZD3500		1 day(s)		Edit
Test ZD	Test ZD	1 day(s)		Edit
ZD3250		1 hour(s)		Edit

## 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, the test will fail because SpeedFlex will be 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.

### To create a SpeedFlex task

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, select the **Mesh Multi-hops Test** check box. If you want to measure the throughput between the source and destination devices only, 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 then 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 (under the *Action* 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, that device may be offline (check the Connection column) or may not support the SpeedFlex feature.

---

5. In *Dest Device*, repeat the steps you 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 will test the throughput for both directions.



---

**NOTE:** If you want to run the SpeedFlex test without saving it, skip the remaining steps and click the **Run** button now.

---

7. In *Test Name*, type a name that you want to this SpeedFlex test. After you save this test, it will appear in the *List of SpeedFlex Table* with the test name that you assigned.
8. If you want this test to run automatically based on a recurring schedule, 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 will run.
  - d. In *Email report to*, type the email address to which the SpeedFlex test results will be sent. If you want to send the report to multiple email addresses, use a comma (,) or semicolon (;) to separate the email addresses.
9. Click **Save**. The *List of SpeedFlex Test* table refreshes, and then the test that you created appears in the table.

## Running a SpeedFlex Task

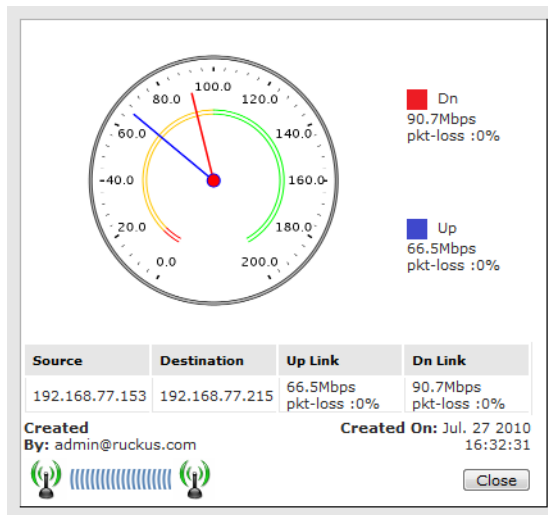
In addition to scheduling when you want a SpeedFlex task to run, you can also run it manually.

### To run a SpeedFlex task 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. If 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, FlexMaster runs the tests sequentially and shows all test results on the same page.

Figure 84. SpeedFlex test result sample



## Editing a SpeedFlex Test

If you want to change the traffic direction to test, change the test name, or change the test schedule, you can edit the SpeedFlex test.

### To edit a 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

If you no longer need a SpeedFlex test that you created previously, you can delete it.

### To delete a SpeedFlex test

1. In *List of SpeedFlex Tests*, look for the SpeedFlex test that you want to delete.
2. Select the check box (under the *Select* column) that is in the same row as the test name.
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 Clients

The *Client* page on the **Monitor** tab allows you to query basic information about a wireless client that is associated with a managed AP. You will need to know the wireless client's MAC address to be able to run a query on it.

### To query basic client information

1. Go to the **Monitor > Client** page.
2. In *MAC Address*, type the MAC address of the client on which you want to query basic information.
3. Click **Search**.

The page refreshes, and then displays the client's basic information, including:

- *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*: The wireless radio used by the WLAN.
- *Signal*: The RSSI strength of the WLAN. If 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** to display graphs of the client's RSSI, traffic, association state, and potential throughput for the selected sampling period.



---

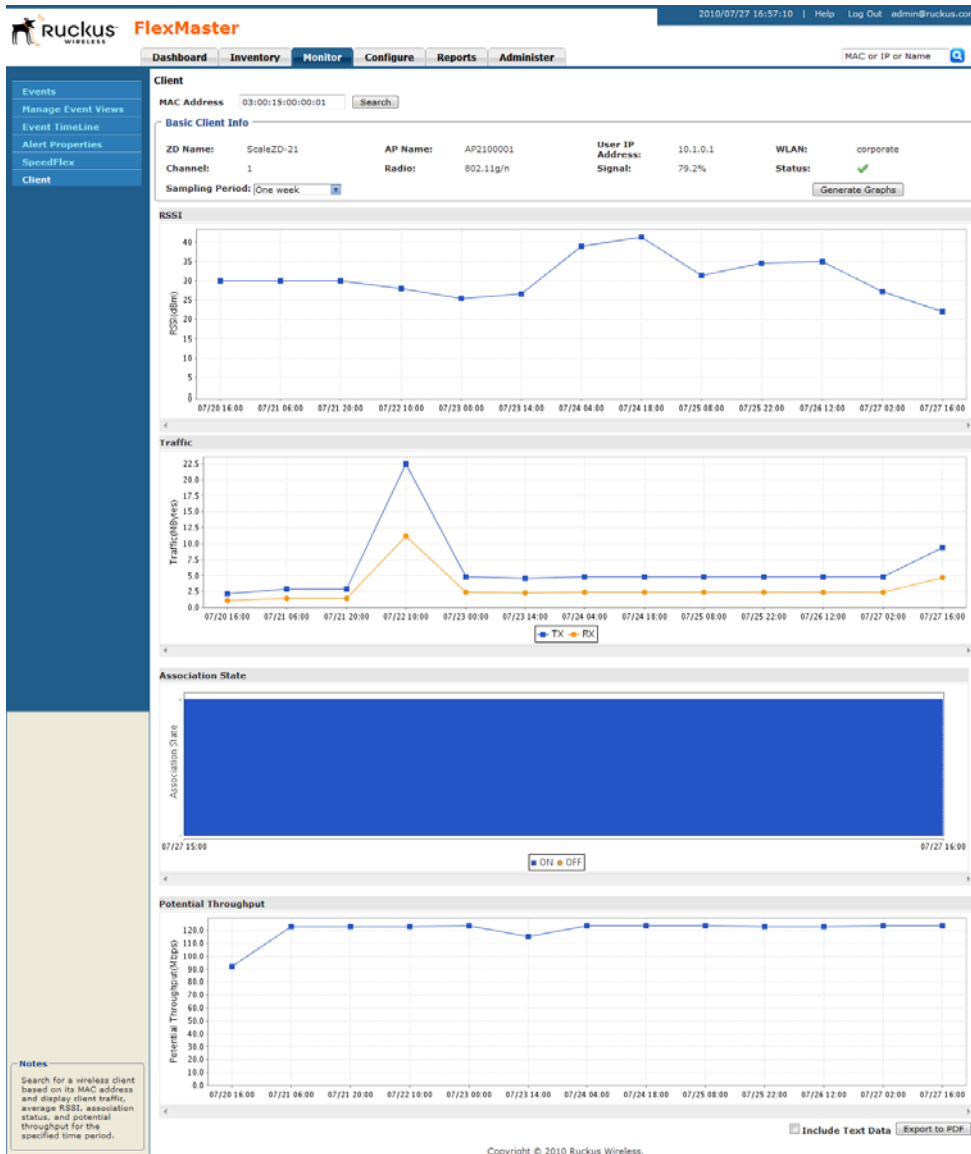
**NOTE:** Because of the sizes of the client graphs, only the RSSI graph is visible after you click the **Generate** button. To view the other graphs, scroll down the page.

---

- *Status*: A green check mark indicates that the client is currently connected. A red cross mark indicates that it is disconnected.

Monitoring Events and Network Activities  
Monitoring Clients

Figure 85. The Client page displays basic client information and graphs that illustrate their RSSI, traffic, association state, and potential throughput



# Provisioning Tasks to Managed Devices

**In This Chapter**

<a href="#">About Provisioning Tasks</a> .....	132
<a href="#">Provisioning Tasks to Standalone APs</a> .....	135
<a href="#">Provisioning Tasks to ZoneDirector Devices</a> .....	162
<a href="#">Provisioning Common Tasks</a> .....	174

## About Provisioning Tasks

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

As FlexMaster may 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 may select from any 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 may be momentarily disrupted for maintenance purposes, you may want to schedule Configure tasks during such a time.



**WARNING!** When scheduling tasks, make sure that there is adequate time interval between tasks that target the same devices. For example, if 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 will fail or expire.

---

## 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, under the **Status** column. Check this column to determine if the task that you deployed has been completed successfully.

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 if the task is being provisioned to multiple devices, multiple task statuses may appear under the Status column. If you provision a reboot task to 10 APs, for example, and this task succeeded on 8 APs but failed on 2 APs, you will 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).

[Table 19](#) lists all possible task statuses that may appear under the Status column.

*Table 19. Task status descriptions*

Task Status	Description
Started	The task has started successfully on these devices. If 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). If 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.
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 <b>Restart</b> link under the <b>Actions</b> column.
Canceled	The scheduled task has been canceled.
Success	The task has completed successfully.

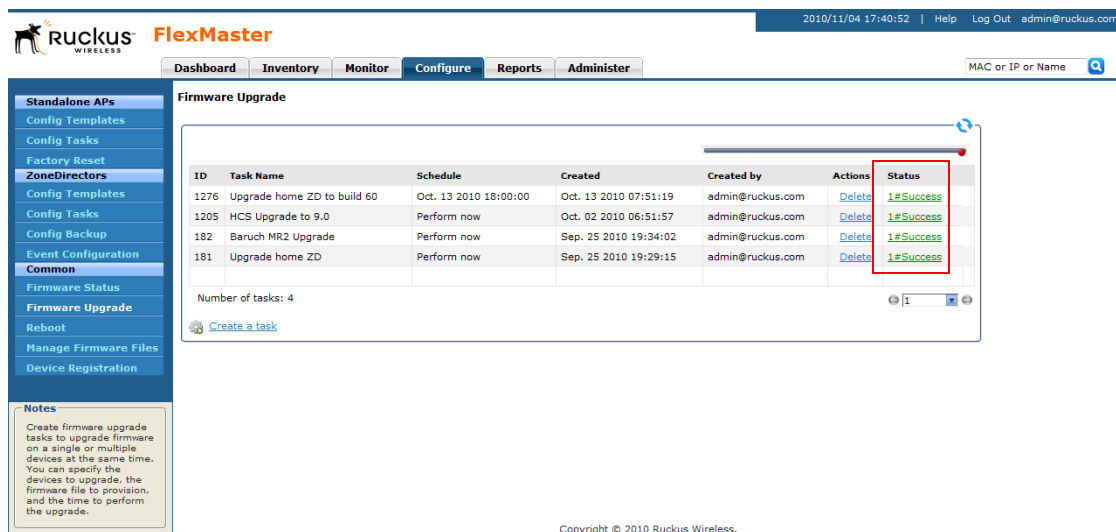
## Provisioning Tasks to Managed Devices

### About Provisioning Tasks

Table 19. Task status descriptions

Task Status	Description
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 <b>Restart</b> link under the <b>Actions</b> column.

Figure 86. The task status column (in red box) on the Firmware Upgrade page



The screenshot displays the Ruckus FlexMaster interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The left sidebar lists various configuration options, with 'Firmware Upgrade' selected. The main content area is titled 'Firmware Upgrade' and contains a table of tasks. The table has the following data:

ID	Task Name	Schedule	Created	Created by	Actions	Status
1276	Upgrade home ZD to build 60	Oct. 13 2010 18:00:00	Oct. 13 2010 07:51:19	admin@ruckus.com	Delete	1#Success
1205	HCS Upgrade to 9.0	Perform now	Oct. 02 2010 06:51:57	admin@ruckus.com	Delete	1#Success
182	Baruch MR2 Upgrade	Perform now	Sep. 25 2010 19:34:02	admin@ruckus.com	Delete	1#Success
181	Upgrade home ZD	Perform now	Sep. 25 2010 19:29:15	admin@ruckus.com	Delete	1#Success

Below the table, it indicates 'Number of tasks: 4' and provides a 'Create a task' button. A red box highlights the 'Status' column for the last three tasks, which all show '1#Success'. The bottom of the page includes a 'Notes' section and a copyright notice: 'Copyright © 2010 Ruckus Wireless.'



## 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. (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 **Standalone APs > Config Templates**, 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 Upgrade action; see [“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, 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 will be unsuccessful if you configure BSSIDs 5 to 8.

---



---

**NOTE:** If 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.

---

#### To create a configuration template for a group of Ruckus Wireless devices

1. Go to **Configure > Standalone APs > Config Templates**.

## Provisioning Tasks to Managed Devices

### Provisioning Tasks to Standalone APs

2. Click **Create New**. The “Create New” configuration wizard opens at the bottom of the page.

Figure 87. Select the check boxes for the options that you want to configure

**CREATE A TEMPLATE**

Template Name: ZF2925 Device General

Product Type: ZF2925

Select product type: Ruckus ZF2925 Device

Select the configuration options you want to modify:

Select All

<input checked="" type="checkbox"/>	Device General
<input type="checkbox"/>	Internet
<input type="checkbox"/>	Wireless Common
<input type="checkbox"/>	Wireless 1
<input type="checkbox"/>	Wireless 2
<input type="checkbox"/>	Wireless 3
<input type="checkbox"/>	Wireless 4
<input type="checkbox"/>	Wireless 5
<input type="checkbox"/>	Wireless 6
<input type="checkbox"/>	Wireless 7
<input type="checkbox"/>	Wireless 8
<input type="checkbox"/>	Management
<input type="checkbox"/>	Device Registration Settings
<input type="checkbox"/>	VLAN Setting

Back Next Cancel

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, see [“Creating an AP Configuration Task”](#).
  - For L2TP Settings, see [“Configuring Your Devices to Communicate with FlexMaster over L2TP”](#).

- Under **Select the configuration options you would like to modify**, select the check boxes for the configuration categories that you want the template to cover. Each category covers multiple parameters.

Table 20. Configuration categories and example parameters

Category	Example Parameters
Device General	Device Name, Super User Name, Super User Password
Internet	IP address, DNS Server Addresses, Connection Type
Wireless Common	Wireless Mode, Country Code, Data Rate
Wireless tabs per device type	Wireless tabs differ per Ruckus Wireless product type
Management	SSH Access, HTTP/HTTPS Access
Device Registration Settings	Server URL, Periodic Inform Interval (for more on these settings, see <a href="#">"Creating an AP Configuration Task"</a> )
VLAN Settings	<ul style="list-style-type: none"> <li>• Management VLAN settings, VLAN ID, and VLAN connected interface</li> <li>• VLAN A to VLAN H settings</li> <li>• Untagged port settings</li> </ul>



**NOTE:** To configure VLANs, you must do so on a per-device basis from the Device View. You cannot configure VLAN settings through the template options. For more on the Device View, see ["Managing a Single Standalone Access Point"](#).

Figure 88. Enter the values for the parameters that you want to modify

**CREATE A TEMPLATE**

Template Name:

Product Type: ZF2925

**Device General**

<input type="checkbox"/> Parameter	Value
<input type="checkbox"/> Device Name:	<input type="text"/>
<input checked="" type="checkbox"/> Super User Name:	<input type="text" value="admin"/>
<input checked="" type="checkbox"/> Super User Password:	<input type="password" value="••••"/> <input type="password" value="••••"/> (Confirmation)



---

**NOTE:** If you modify any of the values in the template or click any option or text box, FlexMaster will assume that you want to change this parameter and will automatically select the check box under the Checked column.

---

6. Click **Next**.
7. Depending on the check boxes you selected in "5." on page 137, 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. If the check box under the Checked column is not selected, that parameter will not be provisioned as part of the template.
8. Click **Next** after each category selection and configuration.
9. When you reach the *Configuration Parameter/Value List* page, a summary of the configurations you have specified are displayed. If FlexMaster detected any errors, the corresponding fields will be flagged in red.

Also on this summary page is the **Persist selected settings after a factory reset** check box. If this check box is selected, all attributes that are provisioned to one or more devices will have precedence over the factory default settings, even if the device is reset to factory defaults. If this check box is cleared, the parameters provisioned in this template will revert to factory defaults after a factory reset.

10. Click **Save** to save your configuration template.



---

**NOTE:** After you click **Save**, if any of the values that you entered in the configuration template is invalid, an error message will appear under the Validation column. You will 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, the value set in the last template takes precedence.

Figure 89. Click Save to save the configuration template that you are creating

**CREATE A TEMPLATE**

Template Name: ZF2925 Device General  
Product Type: ZF2925

**Configuration Parameters and Values**

Persist selected settings after a factory reset

Parameter Name	Parameter Value	Validation
Super User Name:	admin	
Super User Password:	*****	

Back Save Cancel

## Viewing the Settings of an AP Configuration Template

To view the settings of an existing 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 for which settings 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

To edit 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, related options will 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, select the **Persist selected settings after a factory reset** check box.
8. Click **Save** to save your changes.

## Deleting an AP Configuration Template

### To delete an AP configuration template that you have created

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.

### To copy 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 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 **Save** 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

### To export an AP configuration template that you created

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. Click **Save**, and then select the location where you want to save the file.
5. Click **OK**.
6. 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, this could indicate a device issue. To learn how to receive notifications for devices that do not call home at the inform interval, see [“Configuring Alert Properties”](#).

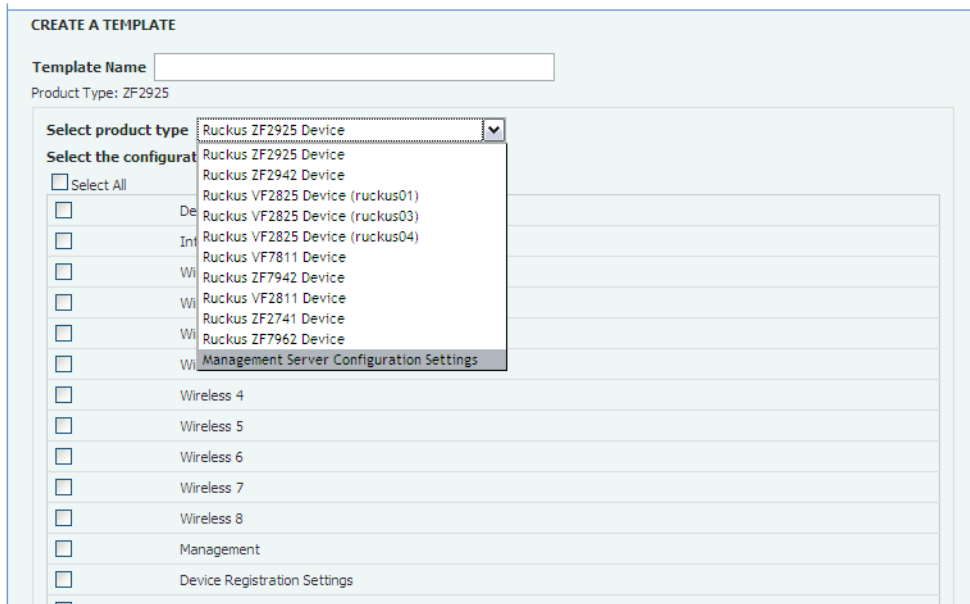
### To create a management server configuration template

1. Go to **Configure > Standalone APs > Config Templates**.
2. Click **Create New**. The “Create New” 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.

## Provisioning Tasks to Managed Devices

### Provisioning Tasks to Standalone APs

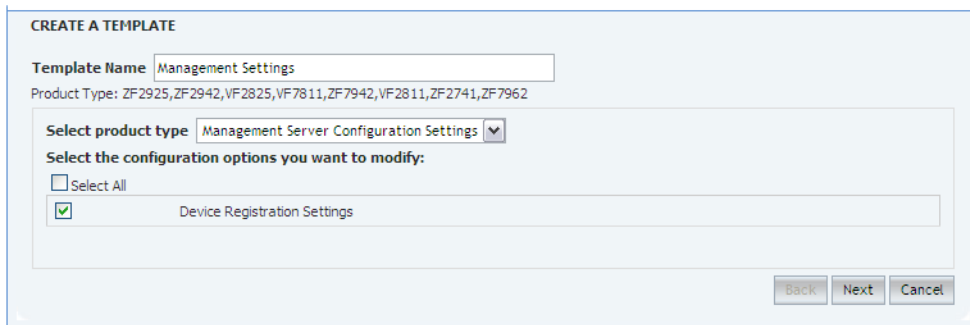
Figure 90. Select the target product type



The screenshot shows the 'CREATE A TEMPLATE' form. The 'Template Name' field is empty. The 'Product Type' is set to 'ZF2925'. The 'Select product type' dropdown menu is open, showing a list of Ruckus devices and configuration settings. The 'Management Server Configuration Settings' option is highlighted. The 'Select the configuration options you want to modify' section has several checkboxes, with 'Device Registration Settings' being the one to be selected according to the instructions.

5. Under *Select the configuration options you would like to modify*, select the **Device Registration Settings** check box.

Figure 91. Select Device Registration Settings



The screenshot shows the 'CREATE A TEMPLATE' form with the 'Template Name' field containing 'Management Settings'. The 'Product Type' is now a list of device types: 'ZF2925,ZF2942,VF2825,VF7811,ZF7942,VF2811,ZF2741,ZF7962'. The 'Select product type' dropdown is set to 'Management Server Configuration Settings'. In the 'Select the configuration options you want to modify' section, the 'Device Registration Settings' checkbox is checked. At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

6. Click **Next**.



7. Under *Registration Settings*, select the parameters to configure.

Table 21. 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, it will be provisioned successfully to APs running on pre-7.0 software, but the interval that they will use is 5 minutes (the shortest interval that they can support).
Remote Management Mode	Select the remote management option that you want to apply to the device: <ul style="list-style-type: none"> <li>• <b>AUTO</b> to allow the device to be managed via SNMP or TR-69 (FlexMaster)</li> <li>• <b>SNMP</b> to allow only SNMP management</li> <li>• <b>TR-69</b> to allow only FlexMaster management</li> </ul> NOTE: If you enable SNMP management, FlexMaster will no longer be able to manage the device.

## Provisioning Tasks to Managed Devices

### Provisioning Tasks to Standalone APs

Figure 92. Configure the parameters that you want to modify

The screenshot shows a web interface titled "CREATE A TEMPLATE". The "Template Name" is "Management Settings" and the "Product Type" is "ZF2925,ZF2942,VF2825,VF7811,ZF7942,VF2811,ZF2741,ZF7962". The "Device Registration Settings" section includes:

- Parameter Value
- Server URL:   
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:  (dropdown)
- Remote Management Mode:  (dropdown)  
Warning: Once SNMP is enabled, the CPE will no longer be managed by FlexMaster.

Buttons: Back, Next, Cancel

8. Click **Next**.

Figure 93. Review your configuration settings, and then click Save.

The screenshot shows the "CREATE A TEMPLATE" page with "Management Settings" as the template name. The "Configuration Parameters and Values" section includes:

- Persist selected settings after a factory reset
- Table of Configuration Parameters and Values:

Parameter Name	Parameter Value	Validation
Periodic Inform Interval:	1 Hour	

Buttons: Back, Save, Cancel

9. After saving the template, create an AP configuration upgrade task that will provision this configuration template to all managed devices. See ["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 may 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 that will be updated. Since configuration templates are specific to a product model, it is possible that not all devices in a device view will be 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 ZF2942 and two MM2225s, you will 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 will cause 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 you to deploy a configuration template that you have created. Before you create a configuration task, you must therefore have an existing configuration template.



**NOTE:** Configuration, firmware, reboot, and factory reset tasks cannot be deleted. Tasks that have not yet started, however, can be cancelled, although 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.

---

### To create an AP configuration task

1. Go to **Configure > Standalone APs > Config Tasks**.
2. Click **Create a task**. The Create Task for 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 the 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 all settings in the configuration template to a device group or to specific devices, click the **Apply the configuration to the selected devices below** option.
      - If you want to apply the template to a device group, click the **Select View** tab, and then select the target device group from the drop-down list. All default and custom device groups appear in the drop-down list. Note that if the template is model-specific, the settings in the template will only be applied to devices that match the model.
      - If you want to apply the template to specific devices, click the **Select Devices** tab, and then select the check boxes for the devices to which you want to apply the configuration template. Note that if the template is model-specific, the settings in the template will only be applied to devices that match the model. If you select a device of a different model, an error message will appear when you save the configuration upgrade task.



---

**NOTE:** In addition to the default device view (All Standalone APs), device views that you manually created from search results will also appear on the **Select View** tab. If you deploy an upgrade task to a manually-created device view, only the current members of that view will be marked for provisioning. New devices that match the view criteria but that registered with FlexMaster after the upgrade task is saved will not be provisioned. You will need to create a new upgrade task to include these new devices.

---

- To apply different parameter settings to target devices, click the **Specify Advanced Settings** option, and then do the following:
    - a. In **Serial Number**, enter the serial number of the device that you want to configure.
    - b. 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 boxes provided.
    - c. 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, click the Save button at the bottom of the page.
    - d. Repeat Steps a to d 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 select 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, an error message appears.

To cancel a configuration upgrade task, see [“Canceling a Scheduled Configuration Upgrade Task”](#).

Figure 94. Selecting the configuration template and the target devices

**CREATE A TASK**

**Task Settings**

Specify a task name:

Select the configuration template:  [View Parameters](#)

**Select the devices to be provisioned**

Select View:

Select a view of devices to perform configuration update:  [View Details](#)

Device Name	Serial #	IP Address	External IP	Model	Connection	Uptime	Tag
alienlee2_home	100801002944	192.168.1.129:443	59.117.125.87:443	ZF2942	✓	9d 4h 5m	
Lynn_home3	100801003584	192.168.0.121:443	202.55.228.100:443	ZF2942	✓	3d 0h 43m	Sunnyvale
Stewart-2942-Home-2	100801003799	192.168.20.152:443	118.168.195.27:443	ZF2942	✗	2m	Sunnyvale
Lynn_home	100801003878	192.168.0.100:443	202.55.228.100:443	ZF2942	✓	7d 4h 40m	Sunnyvale
alienlee1_home	100801004134	192.168.1.248:443	59.117.125.87:443	ZF2942	✓	9d 4h 9m	
Tommy_AP	100801004352	30.30.30.30:443	60.250.131.115:443	ZF2942	✓	6d 23h 16m	Los Angeles
Nick_home	100801004406	192.168.1.10:443	220.133.81.33:443	ZF2942	✓	9d 4h 6m	
BillKish_Home	190801001138	192.168.0.100:443	166.129.53.26:443	ZF2942	✓	8d 17h 27m	
AlbertAP	190801001312	192.168.1.111:443	71.202.65.107:443	ZF2942	✓	9d 4h 12m	
FrankRuffo_Home	190801001313	192.168.201.125:443	12.51.41.26:443	ZF2942	✓	9d 4h 4m	

Number of devices: 63

Disconnected devices will not be upgraded successfully. If you can unselect them prior to start 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:

Time:

## Viewing the Status of an AP Configuration Upgrade Task

### To view the status of an AP configuration task

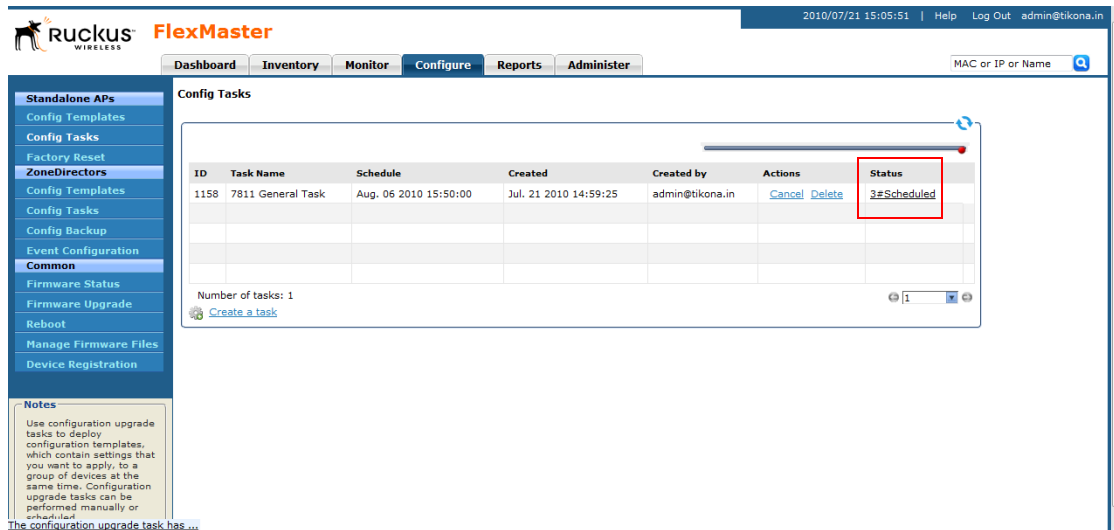
1. Go to **Configure > Standalone APs > Config Tasks**. A list of upgrade tasks that you have created appears on the page.
2. Look for the upgrade task for which status you want to view.
3. Under the **Status** column, check the value that appears on the same row as the task name:
  - **n#Success**: 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.

## Provisioning Tasks to Managed Devices

### Provisioning Tasks to Standalone APs

- **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, click the Detail link under the Failure column to see what may have caused the task failure.
- Other statuses may appear under the **Status** column. For a complete list of all statuses, see ["Understanding the Status of a Task"](#).

Figure 95. Viewing the status of a configuration upgrade task



The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The left sidebar lists various configuration options under 'Standalone APs', 'Config Tasks', 'Factory Reset', 'ZoneDirectors', 'Event Configuration', and 'Common'. The main content area is titled 'Config Tasks' and displays a table with the following data:

ID	Task Name	Schedule	Created	Created by	Actions	Status
1158	7811 General Task	Aug. 05 2010 15:50:00	Jul. 21 2010 14:59:25	admin@tikona.in	<a href="#">Cancel</a> <a href="#">Delete</a>	3#Scheduled

Below the table, it indicates 'Number of tasks: 1' and provides a 'Create a task' link. A red box highlights the 'Status' column for the task shown.

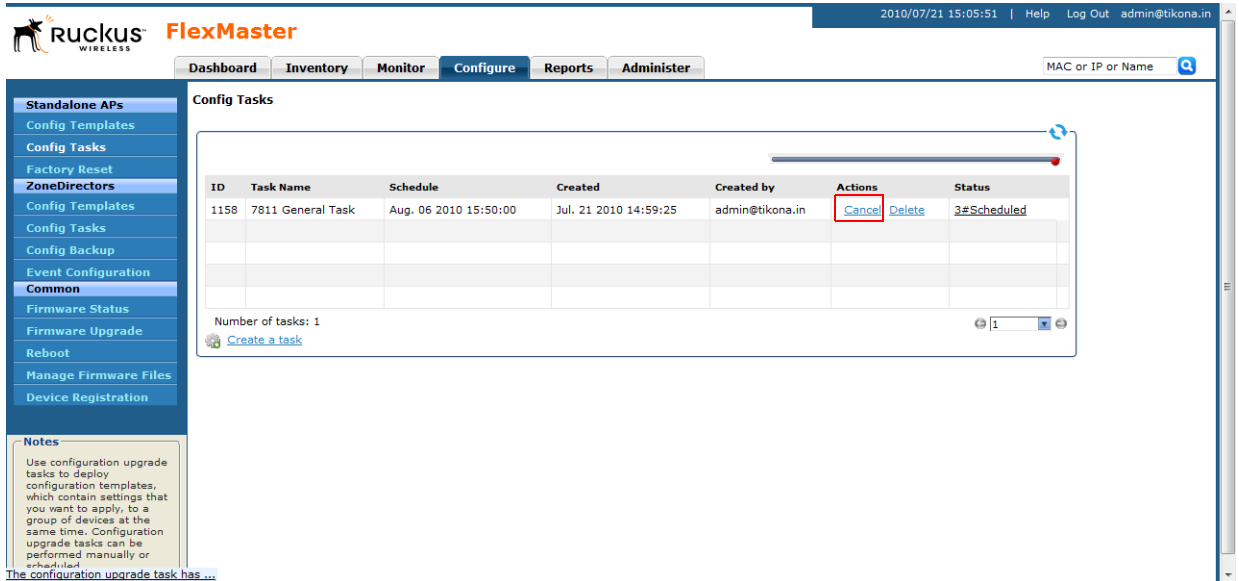
## Canceling a Scheduled Configuration Upgrade Task

Provisioning tasks that have not yet started can be cancelled. For all cancelled tasks, the record of their creation and scheduling remain on the FlexMaster database.

### To cancel a configuration upgrade task

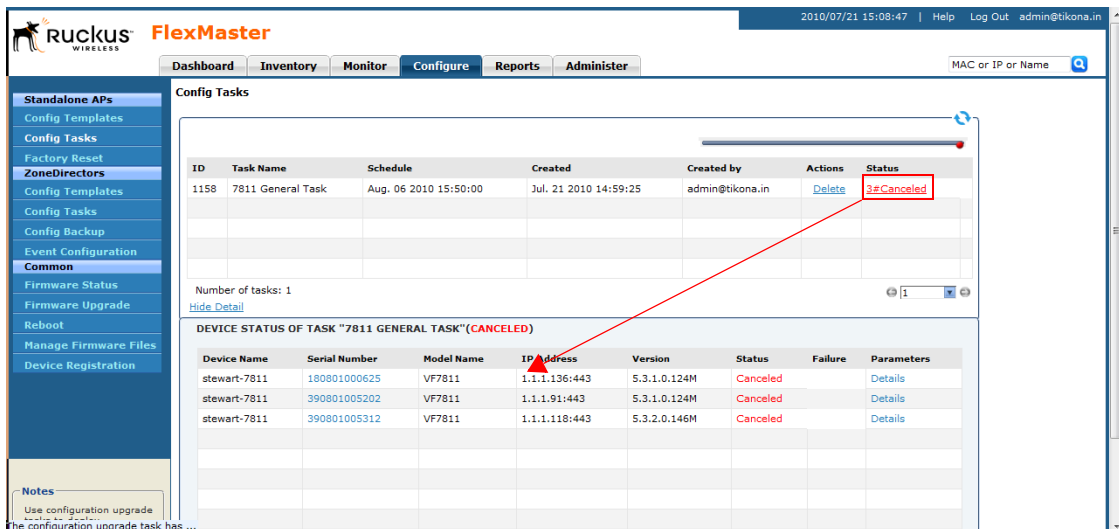
1. Go to **Configure > Standalone APs > Config Tasks**.
2. Locate the upgrade task you want to cancel in the *Configuration Upgrade* table.
3. Click **Cancel** under the *Action* column.

Figure 96. Click Cancel to cancel a scheduled task



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 **View** link for the cancelled upgrade to view all task details.

Figure 97. Viewing details of the canceled task



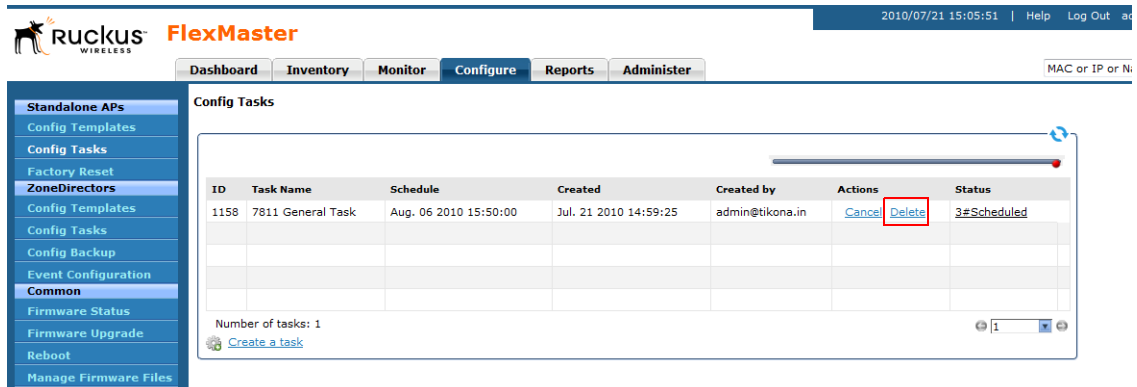
## Deleting a Configuration Upgrade Task

To delete a configuration upgrade task that you have created

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 98. Click Delete to delete the configuration upgrade task



The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes the Ruckus logo, the title 'FlexMaster', and the date/time '2010/07/21 15:05:51'. Below the navigation bar are tabs for 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The 'Configure' tab is active. On the left is a sidebar menu with options like 'Standalone APs', 'Config Templates', 'Config Tasks', 'Factory Reset', 'ZoneDirectors', 'Event Configuration', 'Common', 'Firmware Status', 'Firmware Upgrade', 'Reboot', and 'Manage Firmware Files'. The main content area is titled 'Config Tasks' and contains a table with the following data:

ID	Task Name	Schedule	Created	Created by	Actions	Status
1158	7811 General Task	Aug. 06 2010 15:50:00	Jul. 21 2010 14:59:25	admin@tikona.in	<a href="#">Cancel</a> <a href="#">Delete</a>	3 Scheduled

Below the table, it says 'Number of tasks: 1' and there is a 'Create a task' button. The 'Delete' link in the Actions column of the first row is highlighted with a red box.

## Restarting a Configuration Upgrade Task

If a configuration task that you deployed fails for any reason, 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. Under 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, 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 will not be affected by the restart task option.

To restart a configuration upgrade task

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 will affect 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 (see [“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 will erase 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

### To create an AP factory reset task

1. Go to **Configure > Standalone AP > Factory Reset**.
2. Click **Create a task**. The Create A Task form appears at the bottom of the page.
3. In *Specify 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, select the Clear post factory persistent configuration changes check box.

## Provisioning Tasks to Managed Devices

### Provisioning Tasks to Standalone APs

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 time for the 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**.

Figure 99. Creating a factory reset task

The screenshot displays the 'CREATE A TASK' configuration page in the Ruckus Wireless management interface. The page is divided into several sections:

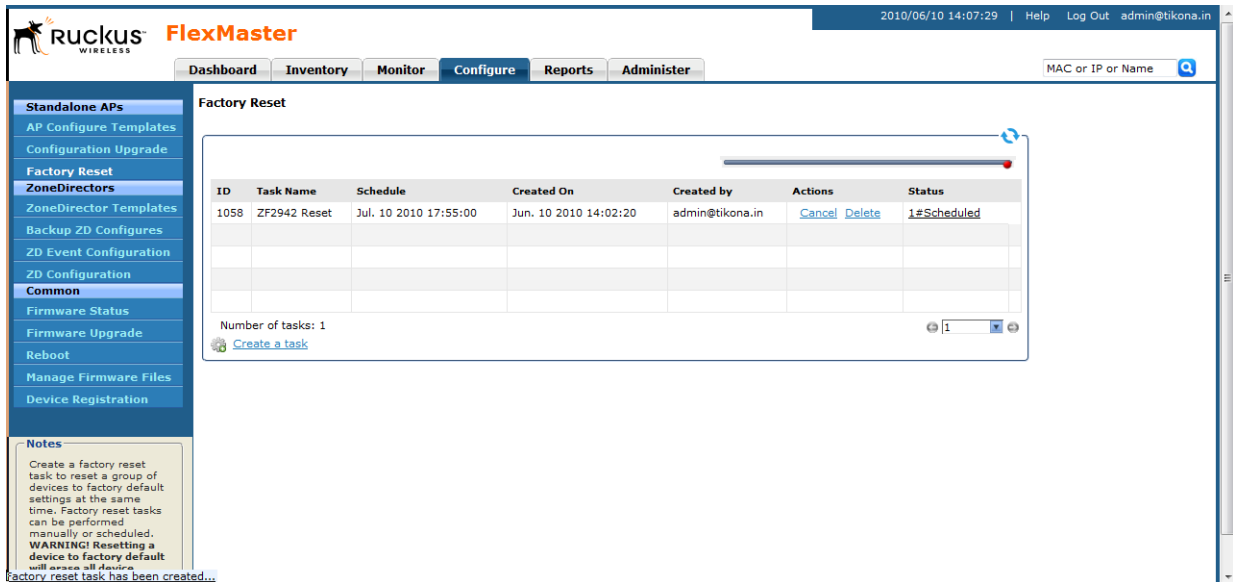
- Task Settings:** A text field for 'Specify a task name' contains 'Reset.ZF2924'. Below it are two checkboxes: 'Clear post factory persistent configuration changes' (unchecked) and 'Reboot device after factory reset' (checked).
- Select a view to reset to factory default:** This section has two tabs: 'Select View' and 'Select Devices'. The 'Select Devices' tab is active. A dropdown menu shows 'ZF2942-All' with a 'View Details' link.
- Device List Table:** A table with columns: Device Name, Serial #, IP Address, External IP, Model, Connection, Uptime, and Tag. It lists 10 devices, including 'allenlee2\_home', 'Lynn\_home3', 'Stewart-2942-Home-2', 'Lynn\_home', 'allenlee1\_home', 'Tommy\_AP', 'Nick\_home', 'BillKish\_Home', 'AlbertAP', and 'FrankRuffo\_Home'. The 'Connection' column shows green checkmarks for most devices and a red 'X' for 'Stewart-2942-Home-2'.
- Specify time for this task:** Two radio buttons are present: 'Perform this task now' (unselected) and 'Schedule this task for later:' (selected). The 'Schedule this task for later:' section includes a date field set to '2009-10-08' and a time field set to '05:15:00 PM'.

## Viewing AP Factory Reset Tasks

### To view a list of AP factory reset tasks that have been created

Go to **Configure > Standalone AP > Factory Reset**. The Factory Reset page appears and lists that factory reset tasks that have been created.

Figure 100. The Factory Reset page lists that factory reset tasks that have been created



## Canceling an AP Factory Reset Task

### To cancel an AP factory reset task

1. Go to **Configure > Standalone AP > 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 message appears.
3. Click **OK** to continue.

The page refreshes, and then the *Status* column for the task now display #Canceled. You have completed canceling the AP factory reset task.

## Deleting an AP Factory Reset Task

### To delete an AP factory reset task

1. Go to **Configure > Standalone AP > 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 message 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 provisioned automatically with a set of settings that were 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. If a device is already registered with FlexMaster, its settings will not be updated by the auto configuration task, even if it is part of the target device view for auto configuration.

### Before You Begin

Before creating an auto configuration task, verify that device registration is set of Auto (this is the default setting). To check if device registration is set to *Auto*:

1. Go to **Configure > Common > Device Registration**.
2. On the **Registration Status** tab, check if the **Automatically approve all devices** check box is selected. If the check box is clear, select it. A popup message appears, prompting you to confirm that you want to enable automatic approval of devices.
3. Click **Yes** to finish enabling automatic approval of devices.

Figure 101. Verify that device registration is set to Auto

## DEVICE REGISTRATION

The screenshot shows the 'Device Registration' interface. At the top, there are license statistics:

- Total Licenses Purchased: 10400
- Licenses Consumed by Standalone APs: 7
- Licenses Remaining: 10051
- Licenses Consumed by ZoneDirectors: 342

Below the statistics is a 'Refresh data' button. The main interface has two tabs: 'Registration Status' (selected) and 'Auto Configuration Setup'. Under 'Registration Status', there is a checkbox labeled 'Automatically approve all devices' which is checked. Below this is a table of registered devices:

Device Name	Serial Number	Model Name	Registered	Permission Mode	Auto Configured	Status	Comments	Auto Configured Tag	Actions
ZD_FM_0964	340701000964	ZD1006	✓	Auto	✗	Permitted			<a href="#">Edit</a>
RuckusAP	VF40043146	VF2825	✓	Auto	✗	Permitted			<a href="#">Edit</a>

If you intentionally disabled automatic device registration, you can still run auto configuration tasks, but you will 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 1: Create a Configuration Template

Create a configuration template that defines the settings that you want to provision to new devices. For example, if you want to auto configure the VLAN settings of all ZoneFlex 2942 access points that will be registering with FlexMaster, select Ruckus 2942 Device in *Select Product Type*, and then select the **VLAN Setting** check box (see [Figure 102](#)) when you create it.

Figure 102. Creating a basic VLAN auto configuration template for ZoneFlex 2942 access points

**CREATE A TEMPLATE**

Template Name

Product Type: ZF2925

Select product type

Select the configuration options you want to modify:

Select All

<input type="checkbox"/>	Device General
<input type="checkbox"/>	Internet
<input type="checkbox"/>	Wireless Common
<input type="checkbox"/>	Wireless 1
<input type="checkbox"/>	Wireless 2
<input type="checkbox"/>	Wireless 3
<input type="checkbox"/>	Wireless 4
<input type="checkbox"/>	Wireless 5
<input type="checkbox"/>	Wireless 6
<input type="checkbox"/>	Wireless 7
<input type="checkbox"/>	Wireless 8
<input type="checkbox"/>	Management
<input type="checkbox"/>	Device Registration Settings
<input checked="" type="checkbox"/>	VLAN Setting

Ruckus Wireless recommends assigning a descriptive name to the template that you will be creating for ease of identification, especially if you have multiple configuration templates on FlexMaster. For instructions on how to create a configuration template, refer to [“Creating an AP Configuration Template”](#).



**NOTE:** If 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.

Figure 103. Radio channel related settings when creating a new configuration template

The screenshot shows a web-based configuration interface titled "CREATE A TEMPLATE". At the top, there is a "Template Name" input field and "Product Type: ZF2925". Below this is a "Wireless Common" section with a table of parameters. A red rectangular box highlights the "Channel" and "Country Code" rows. The "Channel" row shows a dropdown menu set to "SmartSelect" with a note below it: "The device will reboot automatically if the Channel is changed." The "Country Code" row shows a dropdown menu set to "United States" with a note below it: "The device will reboot automatically if the Country Code is changed." Other parameters include "Wireless Mode" (Auto-select), "Transmit Power" (Full), and "Protection Mode" (radio buttons for Disabled, CTS-only, and RTS-CTS). At the bottom right of the form are "Back", "Next", and "Cancel" buttons.

Parameter	Value
Wireless Mode:	Auto-select <small>The device will reboot automatically if the Wireless Mode is changed.</small>
Channel:	SmartSelect <small>The device will reboot automatically if the Channel is changed.</small>
Country Code:	United States <small>The device will reboot automatically if the Country Code is changed.</small>
Transmit Power:	Full
Protection Mode:	<input checked="" type="radio"/> Disabled <input type="radio"/> CTS-only <input type="radio"/> RTS-CTS

## Step 2: Define the Target Devices for Auto Configuration

The next step is to specify the devices that will be 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, if 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 Name > Exactly Equals > ZF2942, and then save the results as a device view.

Use a descriptive name for the view; you will be selecting this name as the target view later when you create an auto configuration task.

Figure 104. Running a search for ZoneFlex 2942 devices

## MANAGE DEVICES

Text View [Map View](#) Refresh data

Select a Device Category:

Show devices where:    and or

[Save Search as a View](#)

Device Name	Serial Number	IP Address	External IP Address	Model Name	Last Seen	Uptime	Connection Status	Tag	Actions
MPaparella	VF40013337	10.0.0.11:443	118.173.77.80:443	ZF2925	Mar. 11 2009 13:44:26	4d 21h 1m	✗	mumbai, india	<a href="#">Edit</a>
RuckusAP	ZF10002551	172.16.40.101:443	64.81.255.250:443	ZF2925	Mar. 16 2009 14:19:51	1h 11m	✓	Sunnyvale, Cali...	<a href="#">Edit</a>
RuckusAP	ZF10003245	172.16.40.100:443	64.81.255.250:443	ZF2925	Mar. 16 2009 14:19:47	1h 11m	✓	bangalore, indi...	<a href="#">Edit</a>
RuckusAP	ZF10004280	172.16.40.102:443	64.81.255.250:443	ZF2925	Mar. 16 2009 14:16:13	1h 7m	✓	Sunnyvale, Cali...	<a href="#">Edit</a>

Number of devices for this search: 4

For instructions on how to run a search and save the results as a view, refer to [“Creating a ZD View”](#) and [“Creating an AP View”](#).

### Option 2: Upload an Inventory File of Devices to Auto Configure

If 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, you will need to upload an inventory file for FlexMaster to be able to auto configure devices.

#### 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.

## Provisioning Tasks to Managed Devices

### Provisioning Tasks to Standalone APs

3. In Column B, assign a tag to each device in the list. These tags will function as the group names for the devices in the list.

Figure 105. A sample inventory file

	A	B	C	D
1	VF6000022	MediaFlex - Custom Group		
2	VF6000053	MediaFlex - Custom Group		
3	VF6000409	MediaFlex - Custom Group		
4	VF6000443	MediaFlex - Custom Group		
5	VF6000444	MediaFlex - Custom Group		
6	ZF10003694	ZoneFlex - Custom Group		
7	ZF10007351	ZoneFlex - Custom Group		
8	ZF10009986	ZoneFlex - Custom Group		
9	ZF10003333	ZoneFlex - Custom Group		
10	ZF10006754	ZoneFlex - Custom Group		
11	ZF10007655	ZoneFlex - Custom Group		
12				
13				
14				

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. Click **Pre-Registration Data**, and then click **Browse**.
8. Go to the location of the inventory file (in XLS format) that you saved earlier, and then click **Open**.
9. Click **Upload**.

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 under the Auto Configured Tag column on the **Registration Status** tab.

## Step 3: 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 as any device views you may have created. If you uploaded an inventory file, the tag names that you assigned to the devices in the group function as group names.



6. In **Model Type**, select the model number of the target device. Available options include:
  - ZF2925 (ZoneFlex 2925 802.11g AP)
  - ZF2942 (ZoneFlex 2942 802.11g AP)
  - VF2825 (MediaFlex 2825 AP)
  - VF7811 (MediaFlex 7811 Adapter)
  - ZF7942 (ZoneFlex 7942)
  - VF2811 (MediaFlex 2811 Adapter)
  - ZF2741 (ZoneFlex 2741 Outdoor AP)
  - ZF7962 (ZoneFlex 7962)
  - ZF7762 (ZoneFlex 7762 802.11n Outdoor AP)
  - ZF7731 (ZoneFlex 7731 802.11n Bridge AP)
  - ZF7343 (ZoneFlex 7363 802.11n Indoor Single-Band AP)
  - ZF7363 (ZoneFlex 7363 802.11n Indoor Dual-Band AP)
  - ZF7762-S (ZoneFlex 7762-S 802.11n Outdoor Sector AP)
  - ZF7025 (ZoneFlex 7025 Multiservice 802.11n Wired/Wireless Wall Switch)
  - ZF7341 (ZoneFlex 7341 2.4GHz 802.11n Smart Wi-Fi 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, you will be unable to save the auto configuration task.

---


## Provisioning Tasks to Managed Devices

### Provisioning Tasks to Standalone APs

Figure 106. Creating an auto configuration task for the VLAN settings of ZoneFlex 2942 access points

## DEVICE REGISTRATION

Total Licenses Purchased: 10400      Licenses Consumed by Standalone APs: 7  
Licenses Remaining: 10051      Licenses Consumed by ZoneDirectors: 342


Refresh data 


Registration Status    Auto Configuration Setup


Rule Name	Create Time	Template Name	Created by	Action	Status

**CREATE A RULE**

Enter an AutoConfiguration Name:

Device View:  

Model Type:  

Configuration Template:  

**8. Click Save.**

The Web interface refreshes and the auto configuration task that you create appears in Auto Configuration Setup table.

Figure 107. The auto configuration task you created appears in the table

## DEVICE REGISTRATION

Total Licenses Purchased: 10400      Licenses Consumed by Standalone APs: 7  
Licenses Remaining: 10051      Licenses Consumed by ZoneDirectors: 342

Refresh data

Registration Status    Auto Configuration Setup

Rule Name	Create Time	Template Name	Created by	Action	Status
ZF2925 VLAN	Mar. 16 2009 14:27:53	ZF2925 VLAN	admin@company1.com	<a href="#">View</a> <a href="#">Stop</a>	Running

Create a rule

Note that an auto configuration task cannot be edited or deleted once you create it. You can only view the task status or stop 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 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

If 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 Configured column shows two types of icons that indicate the auto registration status of a device:

-  means auto configured
-  means not auto configured

## 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 are 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:** If 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 which to provision a template, standby ZoneDirector devices are automatically filtered from the list. Once the active ZoneDirector device is provisioned, it synchronizes its settings automatically with the standby ZoneDirector device.

---

### Creating a ZoneDirector Configuration Template



---

**NOTE:** Before creating a ZoneDirector configuration template, you must have backup configuration of at least one ZoneDirector device. For information on how to back up ZoneDirector configuration, see ["Backing Up ZoneDirector Configuration"](#).

---

#### To create a configuration template for a group of ZoneDirector devices

1. Go to **Configure > ZoneDirectors > Config Templates**.
2. Click **Create New**. The "Create New" 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 Backup Configuration*, select a backup configuration that you will use as base configuration for the template that you are creating. You will need to make modifications to the backup configuration to create your ZoneDirector configuration template.
5. Under *Select the configuration options you want to modify*, select the check boxes for the configurations that you want to modify. If you want to modify all configurations, select the **Select All** check box. Configurations that you can modify include:
  - WLANs
  - Access Point Policies
  - Hotspot Services
  - AAA Servers

- Log Settings



---

**NOTE:** To continue, you must modify at least the WLAN settings.

---

6. Click **Next**. The configuration form for the first set of configurations that you selected appears.



---

**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. Complete the configuration, and then click **Next** to continue to the next set of settings. If you only selected one check box to modify, click **Save** to finish creating the ZoneDirector configuration template.



---

**NOTE:** Note that to save the configuration changes that you made, you must click the **Apply**, **OK**, or **Save** button that is in the same frame as the configuration form. After that, you can click the **Next** or **Save** button at the bottom of the page to proceed to the next configuration form or to save all the changes that you have made.

---

The page refreshes, and the ZoneDirector configuration template that you created appears in the list of available templates.

## Editing a ZoneDirector Configuration Template

### To edit a ZoneDirector configuration template

1. Go to **Configure > ZoneDirectors > Config Templates**. A list of templates that you have created appears on the page.
2. Look for the ZoneDirector 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, related options will 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. Click **Save**.

## Deleting an ZoneDirector Configuration Template

To delete a ZoneDirector configuration template that you created

1. Go to **Configure > ZoneDirectors > 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 then 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 get 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

By default, a ZoneDirector event configuration named Default Event Configuration exists. This default event configuration includes all important ZoneDirector events as defined by Ruckus Wireless.

If 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.

To create a ZoneDirector event configuration

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.



**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).

3. In *New Event Configuration Name*, type a name that you want to assign to this event configuration. For example, if you are including only critical ZoneDirector events in this event configuration, you can type **Critical ZD Events Only**.
4. Click each of the six event type tabs, and then select the check boxes for the ZoneDirector events that you want to include in the event configuration that you are creating.
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"](#).

Figure 108. The New Event Configuration form appears at the bottom of the page

**ZD Event Configuration**

Event Configuration | Configured ZDs | Config Task Log

ID	Configuration Name	Created On	Created By	Action
1	Default Event Configuration	Jun. 04 2010 10:11:58	admin@tikona.in	<a href="#">Assign ZDs</a>

1 - 1 of 1

[Create a New Event Configuration](#)

**New Event Configuration**

New Event Configuration Name:

System Admin | Mesh | Configuration | Client | AP Admin | Performance

**System Admin**

Event Type	Description
<input type="checkbox"/> AC license ap different	ZoneDirector and redundancy ZoneDirector have different licensed APs.
<input type="checkbox"/> AC working mode	ZoneDirector automatically swaps working mode to {{mode}}
<input type="checkbox"/> AP 80211 DOS mgmt flood	{{ap}} detects excessive 802.11 management frames on radio {{radio}}.

## 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 will deploy that particular event configuration to the target ZoneDirector devices.



---

**NOTE:** You can only assign one event configuration to each ZoneDirector device.

---

### To assign an event configuration to ZoneDirector devices

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.
4. In *Select a View*, select the ZoneDirector view from which you want to select ZoneDirector devices for assignment to this event configuration. The default *All ZoneDirectors* view as well as any custom ZoneDirector views you have created 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 though that this will only select the devices that are on the current page. If there are devices listed on other pages, you will 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. If 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.

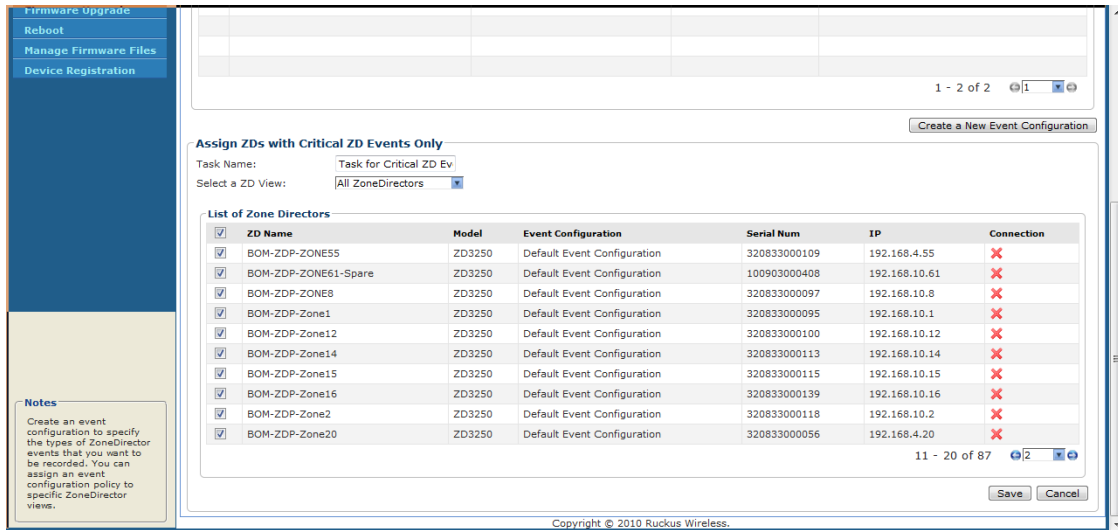
---

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”](#).



Figure 109. Assigning an event configuration to ZoneDirector devices



## Viewing the Status of an Event Configuration Task

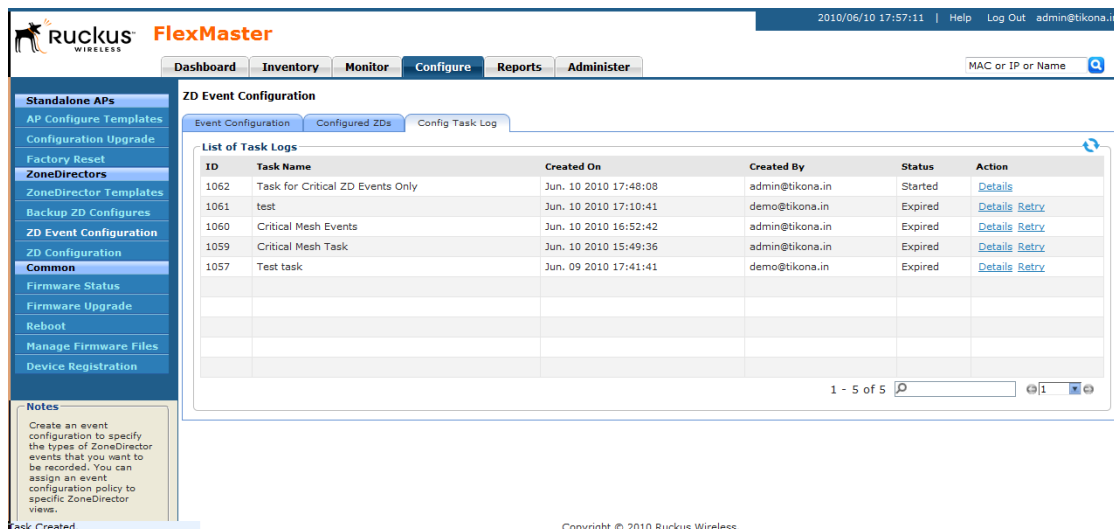
After you assign ZoneDirector devices to an event configuration task, you can check the provisioning status of the task by going to the **Config Task Log** tab.

### To view the status of an event configuration task

1. Go to **Configure > ZoneDirectors > Event Configuration**.
2. Click the **Config Task Log** tab.
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.

Figure 110. Check the Status column for the status of the event configuration task




## Viewing the Event Configuration Assigned to a ZoneDirector Device

To view which event configuration is 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, only devices with this IP address will 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, all devices with “100” in the IP address (for example, 172 . 17 . 16 . **100** and **100** . 1 . 10 . 13) will 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, only devices with serial numbers that begin with “3208” (for example, 320833000219) will 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, only devices with model names that end in “13” (for example, 100 . 1 . 10 . **13**) will 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 may consist of numbers or letters (depending on be the attribute that you selected in the first drop-down list box) and may be a partial or full string. Refer to the previous step for search examples.
- iv. If you want to add another search filter, 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, see [“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 of the user actions on the database, FlexMaster can produce accurate audit logs of system configuration activities.

---

## Creating a ZoneDirector Configuration Upgrade Task

To perform a ZoneDirector configuration upgrade

1. Go to **Configure > ZoneDirectors > Config Tasks**.

2. Click **Create a task**. The Create 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, see ["Restoring ZoneDirector Configuration"](#).

---

- In *Select configuration template*, select the ZoneDirector configuration template that you want to deploy.
4. In *Select ZoneDirector to restore*, choose the target ZoneDirector devices.
    - If 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 if the template is model-specific, the settings in the template will only be applied to ZoneDirector devices that match the model.
    - If 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 if the template is model-specific, the settings in the template will only be applied to ZoneDirector devices that match the model. If you select a device of a different model, an error message will appear 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 will also appear on the *Select View* tab. If you deploy a configuration template to a manually-created device view, only the current members of that view will be marked for provisioning. New ZoneDirector devices that match the view criteria but that registered with FlexMaster after the configuration task is created will not be provisioned. You will 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.

Click **Save** to save the ZoneDirector configuration task. If FlexMaster detects a problem in the configuration upgrade task that you are saving, an error message appears.

## Backing Up and Restoring ZoneDirector Configuration

This section describes how to create a backup file that contains the configuration settings of a ZoneDirector device and how to restore configuration back to the same ZoneDirector device or to another ZoneDirector device of the same model.

## Backing Up ZoneDirector Configuration

Ruckus Wireless strongly recommends that you back up the settings of your ZoneDirector devices periodically to ensure that you can easily recover their settings if they ever become corrupted. You can also back up (or “clone”) the settings of a particular ZoneDirector device and apply them to other ZoneDirector devices.



---

**NOTE:** If your ZoneDirector device is behind a NAT server, you need to set up port forwarding on the **Inventory > ZoneDirectors > Search** page. Click the **Edit** link that is in the same row as the ZoneDirector device name, and then type the port forwarding settings in the **Device Web Port Number Mapping** box.

---

### To back up the configuration of a ZoneDirector device

1. Go to **Configure > ZoneDirectors > Config Backup**.
2. On the *Config Backup* page, click **Obtain New ZoneDirector Configuration**. The Obtain New ZoneDirector Configuration form appears near the bottom of the page.
3. In *Select a view of ZoneDirector*, select the view from which you want to select a ZoneDirector to back up. If you have not created any ZoneDirector views, only **All ZoneDirectors** appear in *Select a view of ZoneDirector*.
4. Check the list of ZoneDirectors that appear on the page, and then decide which ZoneDirector you want to back up.
5. To select a ZoneDirector to back up, click the **Select** link that is in the same row as the ZoneDirector name. The name of the ZoneDirector device that you selected appears in *Selected ZoneDirector*.
6. In *Enter a description for the Configuration*, type a name for the ZoneDirector configuration that you are backing up. Use a descriptive name that will help you identify this backup configuration (especially if have multiple ZoneDirector backup configurations).
7. Click **OK**. FlexMaster backs up the ZoneDirector configuration that you specified.

Check the list of available backups and verify that the ZoneDirector configuration you backed up appears in the list. An entry with the same description that you assigned to the backup should appear in the list.

## Restoring 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, 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 if 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, all APs that are managed by the primary ZoneDirector device will be able to report to the secondary ZoneDirector device automatically. If you choose this restore type, you will 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 if you want to apply the same set of common settings to multiple ZoneDirector devices. You will 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 will not be exported to the target devices. The target devices will 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, refer to [“Backing Up and Restoring ZoneDirector Configuration”](#) for more information.

Restoring ZoneDirector settings from a backup file will overwrite 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, if you only want to restore the wireless, access control, and user settings, make sure you select *Policy Restore*. Selecting *Full Restore* will overwrite all existing ZoneDirector settings, including the IP address, system name, user name, and password.

### **To restore ZoneDirector settings from a backup file**

1. Go to **Configure > ZoneDirectors > Config Tasks**.
2. Click **Create a task**. The Create 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 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 will be 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, see "[Supported ZoneDirector Restore Types](#)".
4. In *Select ZoneDirector to restore*, choose the target ZoneDirector devices.
- If 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 if the template is model-specific, the settings in the template will only be applied to ZoneDirector devices that match the model.
  - If 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 if the template is model-specific, the settings in the template will only be applied to ZoneDirector devices that match the model. If you select a device of a different model, an error message will appear 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 will also appear on the *Select View* tab. If you deploy a configuration template to a manually-created device view, only the current members of that group will be marked for provisioning. New ZoneDirector devices that match the view criteria but that registered with FlexMaster after the configuration task is created will not be provisioned. You will 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. If FlexMaster detects a problem in the restore task that you are saving, an error message appears.

To view the status of the task, check the Status column. For information on the possible tasks statuses, see "[Understanding the Status of a Task](#)". If you are deploying the restore task to multiple devices (either to a device view or select ZoneDirector devices), click the **View** link under 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](#)

## 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:** If 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. Refer to [Table 22](#) for descriptions of the columns that appear on the page.



Figure 111. The Firmware Status page displays the firmware versions that are installed on managed devices

The screenshot shows the Ruckus FlexMaster interface. The main content area is titled 'Firmware Status' and contains a table with the following data:

Model Type	Software Version	Date	Number of Devices	Actions
VF7811	5.3.1.0.124M	Nov. 14 2008	2	<a href="#">Save as a view</a>
VF7811	5.3.2.0.146M	Apr. 13 2009	1	<a href="#">Save as a view</a>
ZD3250	8.6.0.0.51	Dec. 09 2009	2	<a href="#">Save as a view</a>
ZD3250	8.6.0.0.68	Feb. 09 2010	71	<a href="#">Save as a view</a>
ZD3250	8.6.0.0.74	Apr. 07 2010	1	<a href="#">Save as a view</a>
ZD3250	9.0.0.0.16	Jun. 06 2010	2	<a href="#">Save as a view</a>
ZD3250	9.0	Sep. 05 2009	6	<a href="#">Save as a view</a>
ZD3500	9.0.0.0.16	Jun. 06 2010	1	<a href="#">Save as a view</a>
ZD3500	9.0	Sep. 05 2009	4	<a href="#">Save as a view</a>
ZF2741	7.4.0.0.30	Jun. 17 2009	1	<a href="#">Save as a view</a>

At the bottom right of the table, there is a pagination control showing '1 - 10 of 12' and a button with a globe icon.




**NOTE:** The table can show up to ten rows. If it has more than ten rows, click the  button at the bottom-right corner of the table to show the next ten rows.

Table 22. 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 model
Date	Date when the firmware was uploaded to FlexMaster
Number of Devices	Number of devices that are using this firmware
Actions	Shows the <b>Save as a View</b> link. Clicking this link will show options for saving devices in this group as a view, based on their firmware version.

## 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 will 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, see [“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 of the user actions in the database, FlexMaster can produce accurate audit logs of system configuration activities.

---

#### To create a firmware upgrade task

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 112. The Create a Task form

**CREATE A TASK**

**Task Settings**

Specify a task name:

Select the firmware file for each model

	ZF2925	<input type="text" value="2925_8.0.0.0.57.B17 ( 2925_8.0.0.0.57.B17 )"/>
	ZF2942	<input type="text" value="2942_8.0.0.0.57.B17 ( 2942_8.0.0.0.57.B17 )"/>
	VF2825	<input type="text" value="2825_5.3.0.0.51M.B17 ( 2825_5.3.0.0.51M.B17 )"/>

Reboot the device(s) after upgrading the firmware

**Select the view to upgrade:**

Select View **Select Devices**

Select a view of devices to perform firmware upgrade:  [View Details](#)

Device Name	Serial Number	IP Address	External IP Address	Model Name	Last Seen	Uptime	Tag
Eddie-2825	130801001640	192.168.0.2:443	80.189.250.233:443	VF2825	Mar. 16 2009 14:30:26	1m	49 Nightingales, GU6 SDE
Sari-2942AP	430701000924	192.168.1.2:443	86.97.89.4:443	ZF2942	Mar. 13 2009 00:32:53	4d 20h 37m	Sample Tag
MPaparella	VF40013337	10.0.0.11:443	118.173.77.80:443	ZF2925	Mar. 11 2009 13:44:26	4d 21h 1m	mumbai, india
RuckusAP	VF40043146	172.16.20.52:443	67.111.52.66:443	VF2825	Mar. 16 2009 14:29:51	1m	Sunnyvale, California
RuckusAP	ZF10002551	172.16.40.101:443	64.81.255.250:443	ZF2925	Mar. 16 2009 14:30:14	1h 21m	Sunnyvale, California
RuckusAP	ZF10003245	172.16.40.100:443	64.81.255.250:443	ZF2925	Mar. 16 2009 14:30:10	1h 21m	bangalore, india
RuckusAP	ZF10004280	172.16.40.102:443	64.81.255.250:443	ZF2925	Mar. 16 2009 14:26:16	1h 17m	Sunnyvale, California

- 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, under the *Select* column, select the check box for each device you want to update.
- In *Specify Task Name*, type a name for the firmware upgrade task that you are creating.
- 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, that device will not be updated.
- (Optional) Mark the check box at **Reboot device after firmware upgrade** 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 reboot.

---

7. Under *Specify time for the 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]) when the task should run.
8. Click **Save**. A pop-up window appears.  
Click **OK** in the pop-up window to confirm the task.

## Deleting a Firmware Upgrade Task

To delete a firmware upgrade task

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 then 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 purposes, such as configuration changes, firmware upgrades, and rebooting. Since the device cannot forward end-user traffic during reboot, it goes out of service during 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 113. The Create a Task form appears at the bottom of the page

**CREATE A TASK**

**Task Settings**  
Specify a task name:

**Select the view to reboot:**

Select View: **Select Devices**

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

Device Name	Serial #	IP Address	External IP Address	Model	Connection	Uptime	Tag
allenlee2_home	100801002944	192.168.1.129:443	59.117.113.29:443	ZF2942	✓	68d 8h 34m	
4F_NEC	100801003584	192.168.0.233:443	202.55.228.100:443	ZF2942	✓	3d 8h 50m	
Stewart-2942-Home-2	100801003799	192.168.100.65:443	118.168.202.83:443	ZF2942	✓	77d 5h 32m	
NEC_7F	100801003820	192.168.0.235:443	202.55.228.100:443	ZF2942	✓	27d 2h 43m	
kobayashi B00	100801003878	192.168.0.234:443	202.55.228.100:443	ZF2942	✓	8d 3h 5m	
Swisscom-2825-2@TDC	130901012297	20.20.20.16:443	60.250.131.115:443	VF2825	✓	37d 7h 11m	
Swisscom-2825-6@TDC	130901012751	20.20.20.18:443	60.250.131.115:443	VF2825	✓	37d 7h 11m	
Swisscom-2825-4@TDC	140901000749	20.20.20.19:443	60.250.131.115:443	VF2825	✓	37d 7h 11m	
Swisscom-2825-5@TDC	140901000764	20.20.20.15:443	60.250.131.115:443	VF2825	✓	37d 7h 10m	
ATT16	160801001884	192.168.1.126:443	24.6.120.64:443	VF7811	✓	22d 5h 37m	

Number of devices: 42

**Specify a time to perform this task:**

Perform this task now

Schedule this task for later:

Date:

Time:

- Under *Select the view of devices to be rebooted*, 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.
- Type a name for your reboot task at *Specify Task Name*.
- Under *Specify time for the 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]) when the task should run.
- 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.

### To view the status of a reboot task that you created

- Go to **Configure > Common > Reboot**. A list of reboot tasks that you have created appears on the page.
- Look for the reboot task for which status you want to view.
- Under 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 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, click the **Detail** link under the **Failure** column to see what may have caused the task failure.

A few other statuses may appear under the **Status** column. For a complete list of possible statuses, see [“Understanding the Status of a Task”](#).

## Deleting a Reboot Task

To delete a reboot task that you created

1. Go to the **Configure > Common > Reboot** page.
2. Look for the reboot 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 then the task that you deleted disappears from the list.

## Managing Firmware Files

The Manage Firmware Files option provides storage and management of Ruckus Wireless firmware files. Firmware files must be uploaded to FlexMaster for firmware upgrade tasks.

Once a firmware file has been uploaded to FlexMaster, the file 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 if it is being used by an existing scheduled firmware upgrade task.

---

Each device model requires its own firmware; thus, firmware files and device models must be matched.

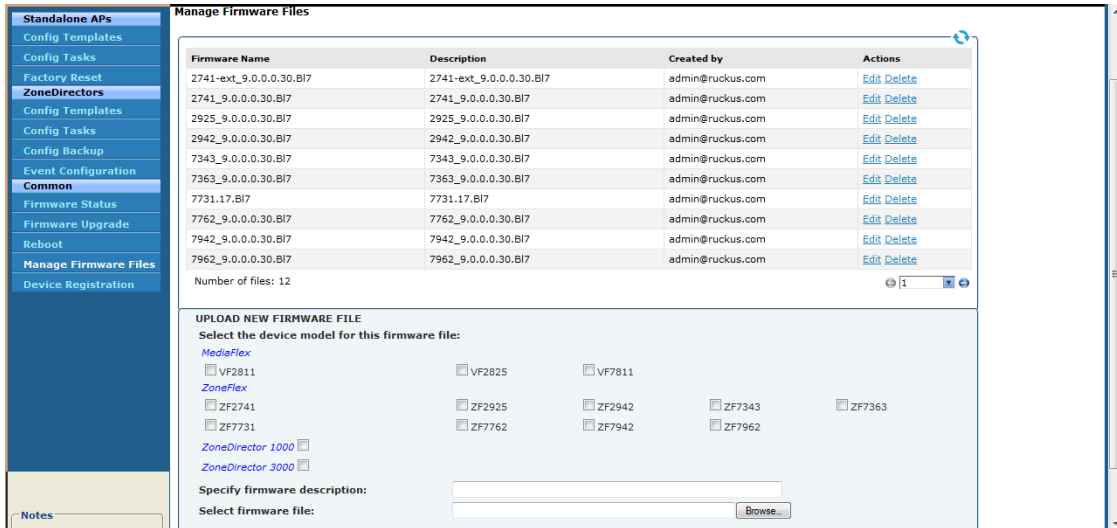
## Uploading a Firmware File

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 114. The Upload New Firmware File form appears at the bottom of the page



3. Under *Specify device model for this firmware file*, select the check box by the Ruckus Wireless device(s) to specify the devices 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 **Browse** to search your client workstation or other reachable location for the firmware file.
- Click **Upload** 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 will be installed.



**NOTE:** If you assign a firmware to an unsupported product model (on which the firmware cannot be installed), you will still be able to edit and save the firmware file, but the firmware will not be installed on that product model.

### To edit a firmware file

1. Go to **Configure > Common > Manage Firmware Files**.

2. Look for the firmware file that you want to edit.
3. Click the **Edit** link that is in the same row as the firmware name. The Edit form appears below the table.
4. Edit the firmware details as required. You can select the product models on which FlexMaster will attempt to provision the firmware. You can also edit the firmware description.
5. Click **OK** to save your changes.

The page refreshes. You have completed editing the firmware file.

## Deleting a Firmware File

### To delete a firmware file that you uploaded

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 prior to 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 table below describes the columns that appear in the Device Registration table.

*Table 23. Table columns on the Device Registration page*

Column	Description
Device Name	Name assigned to the device. Ruckus Wireless assigns APs "RuckusAP" as the default device name.
Serial Number	Serial number of a registering device
Model Name	Model type of device



Table 23. Table columns on the Device Registration page

Column	Description
Registered	<p>✓ indicates that the device has registered with FlexMaster</p> <p>✗ indicates that the device has not yet registered with FlexMaster</p>
Permission Mode	Mode of acceptance as <i>Auto</i> (permission automatically assigned, no manual intervention) or <i>Manual</i> (permission requires manual assignment).
Auto Configured	<p>✓ indicates that the device was added to the inventory using via a comma-separated value (CSV) inventory file</p> <p>✗ indicates that the device has been added manually</p>
Status	<p>Shows the permission status of the device. Default permission statuses include:</p> <ul style="list-style-type: none"> <li>• <i>Admin Denied</i>: The device not receive configuration and firmware upgrades from FlexMaster.</li> <li>• <i>Permitted</i>: The device is allowed to register with FlexMaster.</li> <li>• <i>RMA</i>: The device is currently being repair or replaced. RMA stands for Return Merchandise Authorization.</li> <li>• <i>Unavailable</i></li> </ul>
Comments	Shows any notes that you have entered about the device. To add comments, click the <b>Edit</b> 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.
Auto Configured Tag	If you assigned a tag to the device in the auto configuration inventory file, that tag will appear here.
Actions	Clicking the <b>Edit</b> link enables you to change the device status to and from <i>Permitted</i> , <i>Admin Denied</i> , <i>RMA</i> , <i>Unavailable</i> , or any other status that you created.

Figure 115. The Device Registration page

The screenshot shows the Ruckus FlexMaster interface. At the top, there's a navigation bar with 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. Below this is a search bar for 'MAC or IP or Name'. The left sidebar contains a menu with categories like 'Standalone APs', 'Common', and 'Device Registration'. The main content area is titled 'Device Registration' and includes a summary box with license statistics: 'Total Licenses Purchased: 10100', 'Licenses Consumed by Standalone APs: 42', 'Remaining Licenses: 9701', and 'Licenses Consumed by ZoneDirectors: 357'. Below this is a table of registered devices. The table has columns for Device Name, Serial #, Model, Registered, Licenses, Permission, Auto-Config, Template, Inventory, Comments, Tag, and Actions. The 'Registered' column shows green checkmarks, and the 'Permission' column shows 'Auto' with a red 'X' icon. The 'Actions' column contains 'Edit' and 'Delete' links for each device.

Device Name	Serial #	Model	Registered	Licenses	Permission	Auto-Config	Template	Inventory	Comments	Tag	Actions
RuckusJerryAP	490801010085	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
AlexKang_Home	190801002210	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
AndyGram_Home	190801001922	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
Frank_home	490801010258	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
EricZD9	120730000003	ZD1025	✓	1	Auto	✗		Permitted		ZD1K 9.0	Edit Delete
VF7811@TDC_Lab	180801000249	VF7811	✓	1	Auto	✗		Permitted			Edit Delete
Lakshimi_Home	190801003136	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
TELOTV_HOME_2	350801004829	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete

## Setting Device Registration Permissions

By default, Permission Mode is set to *Auto*, 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, you need to manually change the permission for that device to Admin Denied.

### To change permissions

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.
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, the device will no longer receive 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, they will also appear as options when you are editing the inventory status of a device.

4. Click **OK** to save your changes.

Figure 116. Editing a device's registration settings

The screenshot shows the FlexMaster interface with the 'Device Registration' table. The table has columns: Device Name, Serial #, Model, Registered, Licenses, Permission, Auto-Config, Template, Inventory, Comments, Tag, and Actions. Below the table is an 'EDIT' form for a device with Serial Number 100801003878. The form includes fields for 'Inventory Status' (with a dropdown menu highlighted by a red arrow), 'Comments', and buttons for 'OK' and 'Cancel'. There are also links for 'Upload a Device Inventory File' and 'Save This Inventory as XLS'.

Device Name	Serial #	Model	Registered	Licenses	Permission	Auto-Config	Template	Inventory	Comments	Tag	Actions
RuckusJerryAP	490801010085	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
AlexKang_Home	190801002210	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
AndyGram_Home	190801001922	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
Frank_home	490801010258	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
EricZD9	120730000003	ZD1025	✓	1	Auto	✗		Permitted		ZD1K 9.0	Edit Delete
VF7811@TDC_Lab	180801000249	VF7811	✓	1	Auto	✗		Permitted			Edit Delete
Lakshmi_Home	190801003136	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
TELOIV_HOME_2	350801004829	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
Sonny-AP	190801002980	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete
kobayashi B00	100801003878	ZF2942	✓	1	Auto	✗		Permitted			Edit Delete

Total inventory count: 48

EDIT

Device Serial Number: 100801003878

Inventory Status: [Dropdown Menu]

Comments: [Text Area]

Upload a Device Inventory File Save This Inventory as XLS

OK Cancel



**NOTE:** If you deny a device that is already registered, it will remain in the inventory but FlexMaster will no longer honor requests from that device.



**NOTE:** If you set the device status to Admin Denied, RMA, or Unavailable, the device will appear only on the Device Registration page.



**NOTE:** When you deny a device, its **Permission Mode** changes to **Manual**. If later on you permit the same device, its **Permission Mode** will remain as **Manual**. This behavior allows you to determine which devices in the inventory were permitted manually.



**NOTE:** If you permit a device, it will be able to register with FlexMaster at the next Perform Inform Interval.



**NOTE:** Only devices in **Permitted** status consume license; devices in other statuses do not consume any licenses.

## Approving Devices

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. The Automatically approve all devices check box at the top of the Device Registration table

## Provisioning Tasks to Managed Devices

### Provisioning Common Tasks

can be (1) checked to globally *allow* devices “calling home” to register with FlexMaster, or (2) unchecked to globally *deny* device registration. When this box is not checked, you must manually permit devices to register; see [“Setting Device Registration Permissions”](#).

Figure 117. Enabling auto approval

The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The left sidebar lists various configuration options, with 'Device Registration' selected. The main content area shows 'Device Registration' settings. A summary box displays license statistics: Total Licenses Purchased: 10100, Licenses Consumed by Standalone APs: 42, Remaining Licenses: 9701, and Licenses Consumed by ZoneDirectors: 357. Below this, there are tabs for 'Registration Status' and 'Auto Configuration Setup'. The 'Automatically approve all devices' checkbox is checked and highlighted with a red box. A table below shows a list of devices with columns for Device Name, Serial #, Model, Registered, Licenses, Permission, Auto-Config, Template, Inventory, Comments, Tag, and Actions. The table contains several rows of device information, including RuckusJerryAP, AlexKang\_Home, AndyGram\_Home, Frank\_home, EricZD9, VF7811@TDC\_Lab, Lakshimi\_Home, and TELOIV\_HOME\_2.

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 24. 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 <i>License Exceeded</i> , <i>Managed by ZoneDirector</i> , or <i>Lost ZoneDirector</i> will be able to register successfully if licenses are available. Device status will be set to Permitted
Added via inventory file	Any	Permitted (or any user-defined status)	Licenses exceeded	Fail	Device status will appear as <i>License Exceeded</i> . The license held by the device will be released.

Table 24. 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)	Any	Fail	<p>If a standalone AP becomes managed by ZoneDirector, its status will change to <i>Managed</i> by ZoneDirector.</p> <p>If a ZoneDirector device becomes managed by another FlexMaster server or the TR069 function is disabled, its status will change to <i>Lost</i> ZoneDirector.</p> <p>If the ZoneDirector device is managed by another FlexMaster server, the license held by the device will be released on the original FlexMaster server. However, if the TR069 function is disabled, the license status will remain the same until the inventory status is changed to a status other than "Permitted".</p>
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 will be set to <i>Permitted</i> . The auto registration state of the device will be set to <i>Enabled</i> .
Auto registration (call home)	Enabled	Any	Licenses exceeded	Fail	Device status will be set to <i>License Exceeded</i> and the license held by the device will be released. The auto registration state of the device will be set to <i>Enabled</i> .
Auto registration (call home)	Disabled	Any	Any	Fail	Device status will be set to <i>Admin Denied</i> and the license held by the device will be released. The auto registration state of the device will be set to <i>Disabled</i> .

## 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, 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, see "[Provisioning Tasks to Managed Devices](#)".

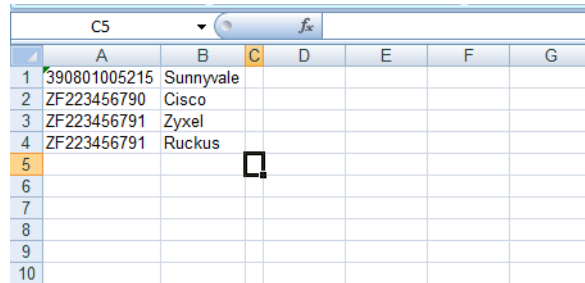
## When to Upload a Device Inventory File

- If you disabled automatic device approval (by clearing the Automatically approve all devices check box) on the Device Registration page, you will need to manually approve each device registration request. If 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 will be 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 the Device Inventory File

A device inventory file is a Microsoft Excel file with two columns that contain the serial number and an auto-configuration tag for each device. After you upload the device inventory file with the pre-registration data, you will need to create an auto-configuration task using the tag to select the target devices.

Figure 118. An example of a device inventory file



	A	B	C	D	E	F	G
1	390801005215	Sunnyvale					
2	ZF223456790	Cisco					
3	ZF223456791	Zyxel					
4	ZF223456791	Ruckus					
5			□				
6							
7							
8							
9							
10							

## Procedure for Uploading the Device Inventory File

When you have the device inventory file ready, you will need to upload it to FlexMaster.

### To upload the device inventory file

1. Click the **Upload a device inventory file** link from below the *Device Registration* table. The *Upload a Device Inventory File* form appears.
2. In **Select an inventory file to upload**, click the **Browse** button to find the file.
3. Once you have found the file, click **Open** in the *Browse* pop-up window.
4. Click **Upload** to upload the inventory file.

Figure 119. The Upload a Device Inventory File form

Registration Status Auto Configuration Setup

Automatically approve all devices

Device Name	Serial #	Model	Registered	Permission	Auto-Config	Template	Inventory	Comments	Tag	Actions
ruckus	320833000274	ZD3250	✓	Auto	✗		Permitted			Edit Delete
SimZD_Standby	800-782588	ZD3250	✓	Auto	✗		Permitted			Edit Delete
ruckus-zd3000	800-782587	ZD3250	✓	Auto	✗		Permitted			Edit Delete
SimZD_Active	800-782586	ZD3250	✓	Auto	✗		Permitted			Edit Delete
RuckusWB	981055000596	ZF7731	✓	Auto	✗		Permitted			Edit Delete
RuckusWB	270955000062	ZF7731	✓	Auto	✗		Permitted			Edit Delete
ScaleZD-201	060017673219	ZD3250	✓	Auto	✗		Permitted		ScaleZD-GPS	Edit Delete
ScaleZD-202	080870124144	ZD3250	✓	Auto	✗		Permitted		ScaleZD-GPS	Edit Delete
ScaleZD-203	100729688737	ZD3250	✓	Auto	✗		Permitted		ScaleZD-GPS	Edit Delete
ScaleZD-204	120589614738	ZD3250	✓	Auto	✗		Permitted		ScaleZD-GPS	Edit Delete

Total inventory count: 86

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:

Retrieving the auto approval state... Copyright © 2010 Ruckus Wireless.

## 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, you could use the export to Excel feature so you do not have to manually type the details of each device.

Figure 120. Click the Save this inventory as XLS link

Registration Status Auto Configuration Setup

Automatically approve all devices

Device Name	Serial Number	Model Name	Registered	Permission Mode	Auto Configured	Status	Comments	Auto Configured Tag	Actions
ZD_FM_0964	340701000964	ZD1006	✓	Auto	✗	Permitted			Edit
RuckusAP	VF40043146	VF2825	✓	Auto	✗	Permitted			Edit
430701005496	430701005496	ZD1025	✓	Auto	✗	Permitted			Edit
MPaparella	VF40013337	ZF2925	✓	Auto	✗	Permitted			Edit
RuckusAP	ZF10002551	ZF2925	✓	Auto	✗	Permitted			Edit
RuckusAP	ZF10004280	ZF2925	✓	Auto	✗	Permitted			Edit
RuckusAP	ZF10003245	ZF2925	✓	Auto	✗	Permitted			Edit
Sari-2942AP	430701000924	ZF2942	✓	Auto	✗	Permitted			Edit
Ruckus	200801004687	ZD1012	✓	Auto	✗	Permitted			Edit
Eddie-2825	130801001640	VF2825	✓	Auto	✗	Permitted			Edit

Total inventory count: 12

Upload a Device Inventory File [Save This Inventory as XLS](#)

Refreshing data

Loading comments...  
Loading comments...  
Loading comments...  
Getting the auto approval state...

#### To export the device list to an Excel file

1. On the *Device Registration* page, click the **Save this inventory as XLS** link at the bottom of the page. A dialog box appears and prompts you if you want to open or save the file to your computer.
2. Click **Save**, and then select the location where you want to save the file.
3. Click **Save**.

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.



## Configuring VLAN Settings

If your wired network is segmented into VLANs and you want clients associated with a ZoneFlex AP to join these VLANs, you can configure VLAN support on the AP via FlexMaster.



---

**NOTE:** Before configuring VLANs on your network, Ruckus Wireless recommends configuring a test network that mirrors your actual deployed network.

---



---

**NOTE:** If you have 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, you will be unable to set it as the hotspot interface and the following message will appear:

```
The specified wireless interface is not available for the hotspot service.
```

---

### 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.

## 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. If you want specific physical or wireless interfaces on the AP to join a VLAN on your wired network, you will 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 ZoneFlex AP.
- A wireless interface can be connected to only one VLAN.

## 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.

The following are the general procedures for configuring the VLAN settings of an AP:

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.

## Sample Scenario

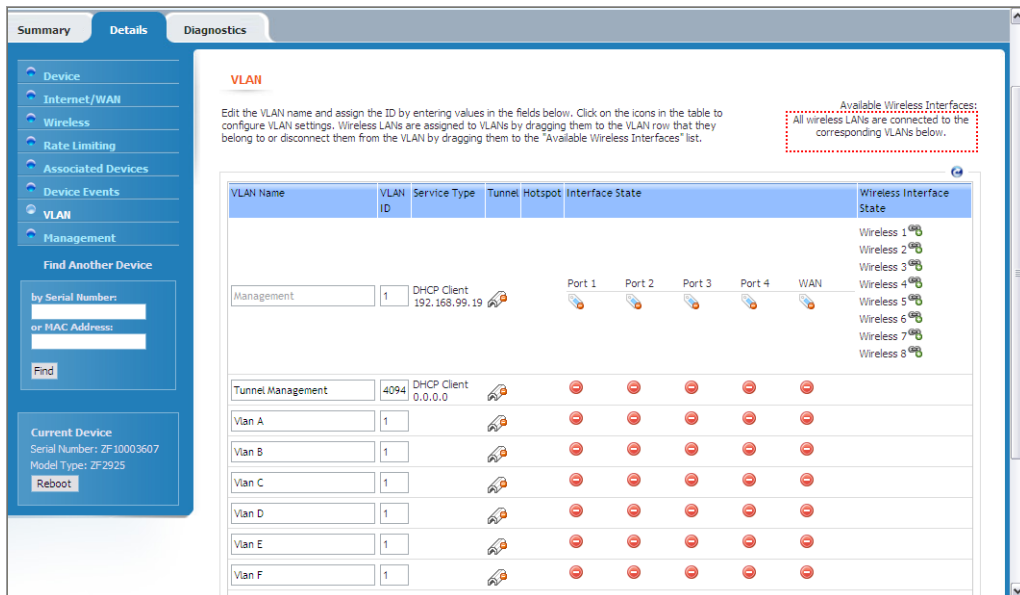
Your wired LAN is segmented into several VLANs, including one called *Sales VLAN*. You have a ZoneFlex 2942 appliance deployed on the network and you want some of its ports and wireless interfaces to join the Sales VLAN on the wired LAN. Specifically, you want two physical ports (Port 1 and Port 2) and two wireless interfaces (Wireless 1 and Wireless 2) to be part of the Sales VLAN.

The Sales VLAN is assigned VLAN ID 1000 and VLAN tagging is disabled.

### Step 1: Launch the VLAN Configuration Page for the AP

Launch the Device View for the AP that you want to manage, click the **Details** tab, and then click VLAN on the menu. The VLAN configuration page appears, as shown in [Figure 121](#).

Figure 121. VLAN Configuration Page







## Step 2: Move Ports 1-2 and Wireless 1-2 to VLAN A

By default, all ports on the AP are part of the Management VLAN (VLAN ID 1). This default configuration enables clients connected to the AP (whether via the wireless or physical interfaces) to communicate with each other.

Since each physical interface and wireless interface can only be connected to one VLAN at any given time, you need to remove Port 1, Port 2, Wireless 1, and Wireless 2 from the Management VLAN first and connect them to the Vlan A (which we will later connect to Sales VLAN).

### To move these interfaces from the Management VLAN to Vlan A

1. Under the Wireless Interface State column, click the icon for Wireless 1, and then drag it to the same row as Vlan A. Wireless 1 now appears on the same row as Vlan A.
2. Move Wireless 2 to Vlan A by repeating the procedure described in Step 1.
3. Under the Port 1 column, look for the  icon that is in the same row as Management. Click it repeatedly until it changes to the  icon, which indicates that the port is disconnected from the Management VLAN.
4. Disconnect Port 2 from the Management VLAN by repeating the procedure described in Step 3.
5. Under the Port 1 column, look for the  icon that is in the same row as Vlan A. Click it repeatedly until it changes to the  icon, which indicates that the port is untagged and connected to Vlan A.
6. Connect Port 2 to Vlan A by repeating the procedure described in Step 5.
7. Change the VLAN ID of Vlan A from 1 (default) to 1000. VLAN ID 1000 is the same as the Sales VLAN ID to which you want this VLAN to connect.
8. Change the VLAN IDs of Vlan B-Vlan H to unique or unused VLAN IDs. For example, you can assign VLAN ID 2 to Vlan B, VLAN ID 3 to Vlan C, and so forth.



---

**NOTE:** If you do not change the VLAN IDs of Vlan B-Vlan H to unique IDs, you will be unable to save your VLAN configuration.

---

9. (Optional) Change the VLAN Name of Vlan A to Sales VLAN. This will help you identify later on which VLAN on the AP is connected to the Sales VLAN.

Figure 122. Connecting Ports 1-2 and Wireless 1-2 to Vlan A

**VLAN**

[Show Device Status](#)

Available Wireless Interfaces:  
All wireless LANs are connected to the corresponding VLANs below.

Edit the VLAN name and assign the ID by entering values in the fields below. Click on the icons in the table to configure VLAN settings. Wireless LANs are assigned to VLANs by dragging them to the VLAN row that they belong to or disconnect them from the VLAN by dragging them to the "Available Wireless Interfaces" list.

VLAN Name	VLAN ID	Service Type	Tunnel	Interface State	Wireless Interface State	
Management	1	DHCP Client 192.168.1.100		Port 0 	Port 0 	Wireless 1 Wireless 2 Wireless 3 Wireless 4 Wireless 5 Wireless 6 Wireless 7 Wireless 8
Tunnel Management	4094	DHCP Client 0.0.0.0				
Vlan A	65					
Vlan B	66					
Vlan C	67					
Vlan D	68					
Vlan E	69					
Vlan F	70					
Vlan G	71					
Vlan H	72					

[Show Legend](#)

10. Click **Submit** to save your changes. A message at the top of the page appears, informing you that the changes have been submitted.

11. Click the (Refresh) button in the upper-right corner of the page.

The VLAN page refreshes, and then shows the updated VLAN configuration. Note the following changes:

- Vlan A now appears as Sales VLAN and is assigned VLAN ID 1000.
- All VLANs are assigned unique VLAN IDs.
- The Interface State column for Port 1 and Port 2 shows (connected, untagged) in the Sales VLAN row. This indicates that they are connected to the Sales VLAN.
- Wireless 1 and Wireless 2 appear on the same row as Sales VLAN. This indicates that they are connected to the Sales VLAN.



**NOTE:** If the status message at the bottom of the page indicated that the settings were saved but the VLAN page does not reflect the configuration you just completed, the AP may be offline or is unable to receive commands from FlexMaster. Check the Status Area at the bottom of the page and see if FlexMaster encountered a problem completing the task.

At this point, you have completed configuring the VLAN settings on the AP. Port 1, Port 2, Wireless 1, and Wireless 2 should now be part of the Sales VLAN.

## Configuring the Hotspot Feature on ZoneFlex 2942

A hotspot is a venue or area that provides wireless Internet access to devices with wireless networking capability, such as 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 will need the following to deploy a hotspot:

- **Web Server:** You need a Web server that can host the external portal/login page that users will 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, contact Ruckus Wireless Support at [support@ruckuswireless.com](mailto:support@ruckuswireless.com) and request for the *ZoneFlex 2942 Hotspot Application Notes*.

---

### 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 will be using for your hotspot deployment.
- Have the following information ready:
  - Redirect URL for the captive portal (the Web page where users will 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. If the wireless interface belongs to any VLAN other than the Management VLAN, you will be unable to set it as the hotspot interface and the following message will appear: 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 will need to configure the settings shown in [Figure 123](#).

Figure 123. Basic Settings tab of the Hotspot page

The screenshot displays the Ruckus FlexMaster web interface. The top navigation bar includes the Ruckus logo and 'FlexMaster' branding, along with 'Help' and 'Logout (admin@ruckus.com)' links. The main content area is titled 'HOTSPOT' and features several tabs: 'Basic Settings', 'Walled Garden', 'Unrestricted Clients', 'Advanced Settings', and 'Information'. The 'Basic Settings' tab is active, showing a note: 'Note: The following must be set before starting the Hotspot service: Redirect URL, Primary RADIUS Server, Shared Secret, Wireless and/or Wired interface'. Below this, the 'General' section contains 'Hotspot Service' (radio buttons for 'Enabled' and 'Disabled', with 'Disabled' selected), 'Hotspot Wireless Interface' (a dropdown menu), and 'Hotspot Wired Interface' (a dropdown menu). The 'Web Redirection and Authentication' section includes 'Redirect URL' (text input with 'http://172.17.16.97/cgi-bin/hc'), 'Primary RADIUS Server' (text input with '172.17.16.97'), and 'RADIUS Shared Secret' (text input with '12345'). At the bottom of the form are 'Back', 'Submit', and 'Reset' buttons. A left sidebar contains a navigation menu with options like 'Device', 'Internet/WAN', 'Wireless', and 'Hotspot'. A search box is also present in the sidebar.

To enable the hotspot feature and configure the basic hotspot settings

1. On the menu, click **Hotspot**. The Basic Settings tab appears.
2. Click **Edit Settings**.

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 may 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 will be 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 will be accessible to hotspot users.



---

**NOTE:** If 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 may 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 URL**, type the URL to which users will be 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 will 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 bottom of the page to see if the configuration change has been made successfully. If the device is online, it takes only a few minutes to apply configuration changes.

You have completed configuring your hotspot's basic settings. If your RADIUS server and captive portal are both configured correctly and running, your hotspot should now be operational.



## Configuring the Walled Garden

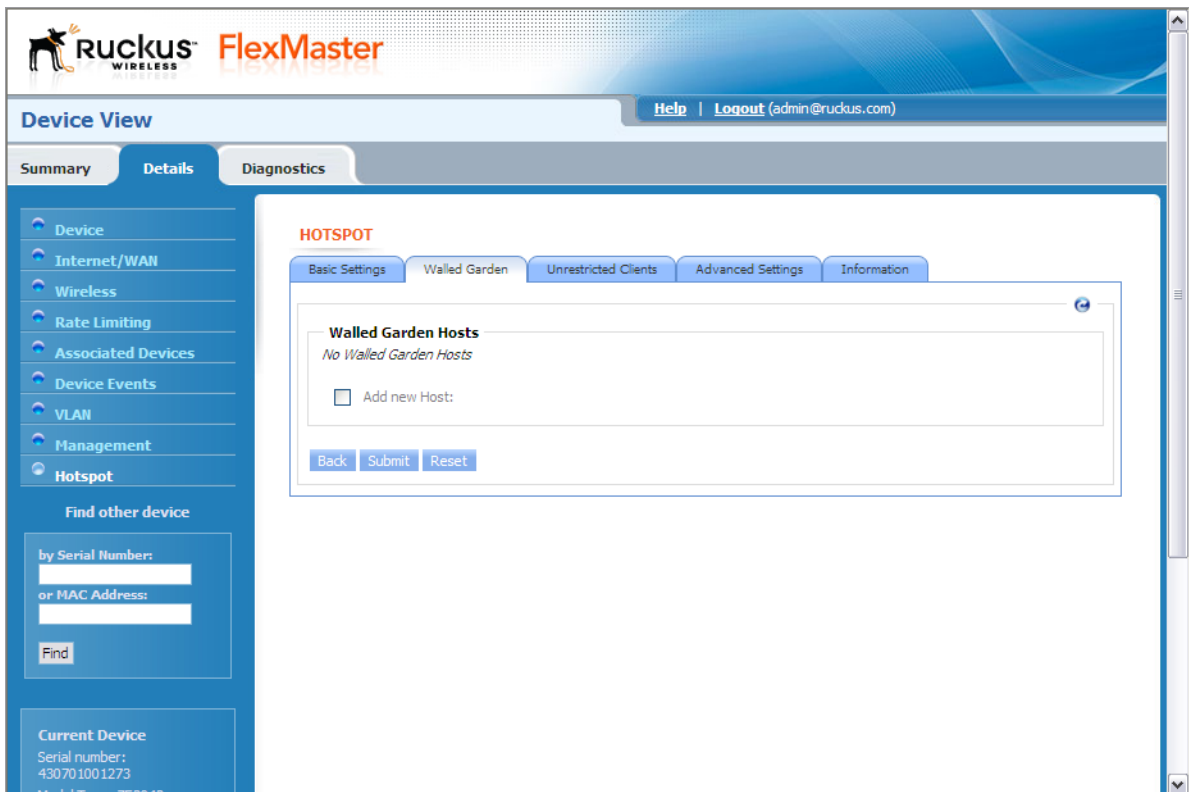
The term *walled garden* refers to a list of URLs that users (who are associated with your hotspot) can access without providing a user name and password. If you are operating the hotspot in a hotel, for example, you can include the hotel's Web site in the walled garden. A walled garden for a corporate office, on the other hand, may 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).

Figure 124. Walled Garden tab of the Hotspot page



### 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 the check box next to **Add new host**. A text box appears.
3. 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. If you are adding multiple hosts to the walled garden, use commas (,) to separate the hosts.
4. Click **Submit** to finish adding the entry to the list.

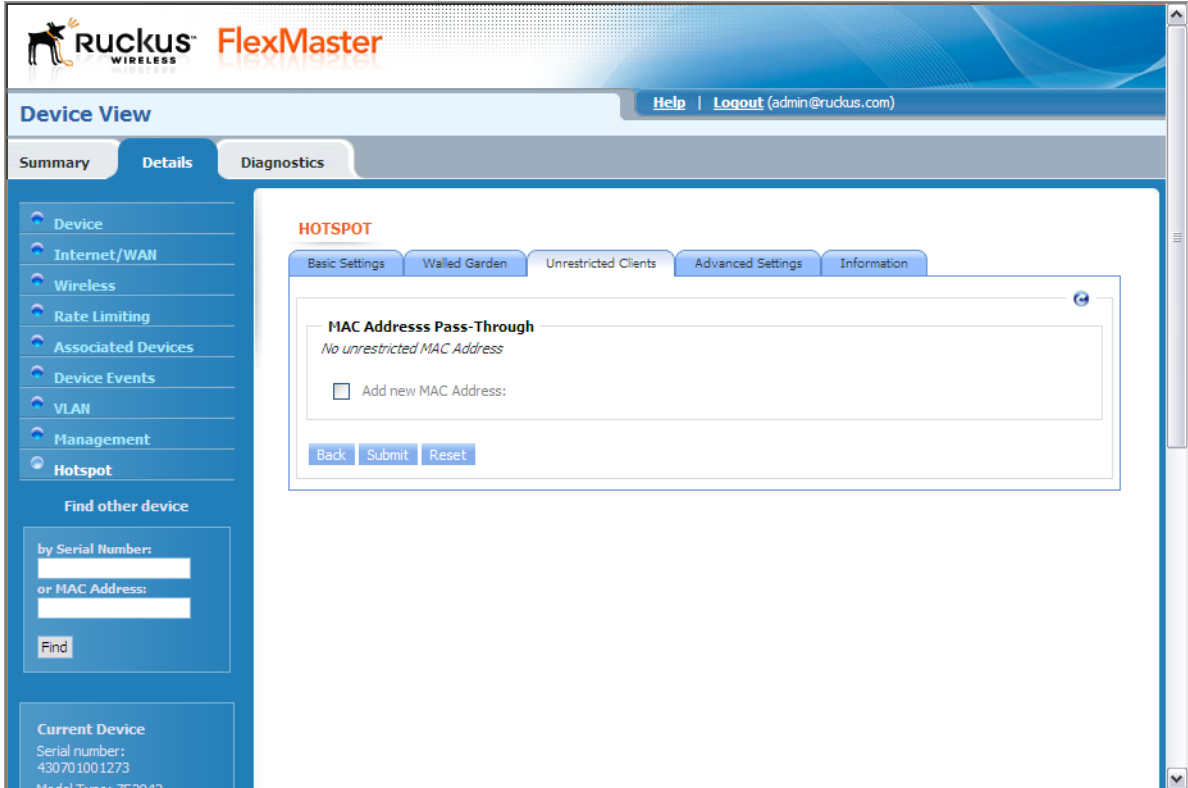
Repeat the same procedure for each entry that you want to add to the list.

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

If 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.

Figure 125. Unrestricted Clients tab of the Hotspot page



### 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 Table page appears.
2. Click the check box next to **Add new MAC Address**. A text box appears.
3. In the text box, type the MAC address that you want to add to the pass-through list. If you are adding multiple MAC addresses to the pass-through list, use commas (,) to separate the MAC addresses.
4. Click **Submit** to finish adding the entry to the list.

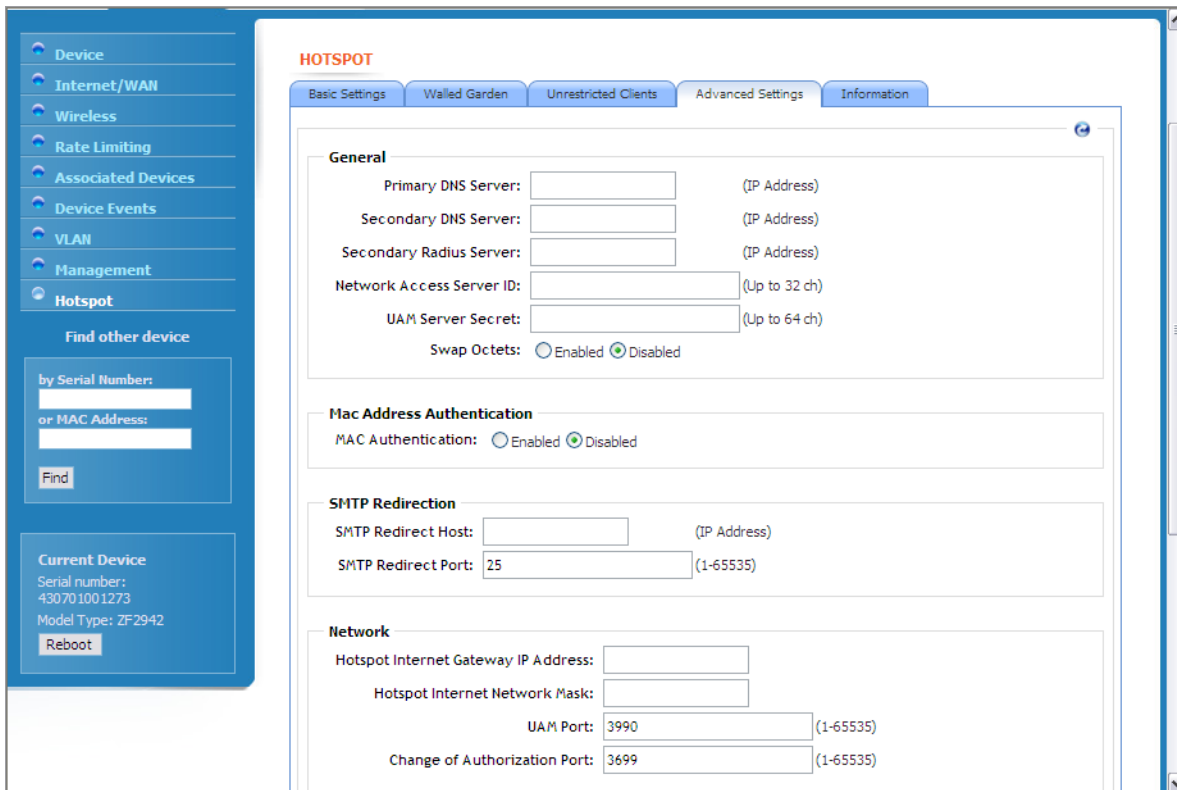
Repeat the same procedure for each entry that you want to add to the pass-through list.

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.

Figure 126. Advanced Settings tab of the Hotspot page



### To configure advanced hotspot settings

1. On the Hotspot page, click the **Advanced Settings** tab.
2. Under the **General** section, configure the following options:
  - *Primary DNS*: If you want hotspot users to use a different DNS server from the one that the AP is currently using, type the IP address of a new DNS server in Primary DNS Server.
  - *Secondary DNS*: If you have another DNS server, type the IP address of the other DNS server in Secondary DNS Server.
  - *Secondary RADIUS Server*: If you have another RADIUS server on the network and you want to use it to process some of the authentication requests from hotspot users, type the IP address of that server in Secondary RADIUS Server. In addition

to being an auxiliary server for processing authentication requests, this second RADIUS server will also function as a backup server in case the primary server becomes unavailable.

- *NAS ID*: Type the name by which the RADIUS server will identify the AP.
  - *UAM Secret*: If you are using ChilliSpot as your access point controller application, type the UAM password in UAM Secret. This is the password that the AP will use to access the ChilliSpot login CGI (`hotspotlogin.cgi`). The same password must be configured on the UAM server.
  - *Swap Octets*: Click **Enabled** if you want to use ChilliSpot-defined standards for counting the number of bytes that a client has sent (output) and received (input) on the RADIUS server. Leave it Disabled if you want to use WISPr-defined standards.
3. 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, click **Enabled in MAC Address Authentication**, and then type any value in Password. The AP will automatically authenticate these devices with the RADIUS server using their MAC addresses.



---

**NOTE:** Before these portable devices can access the hotspot service, you will 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.

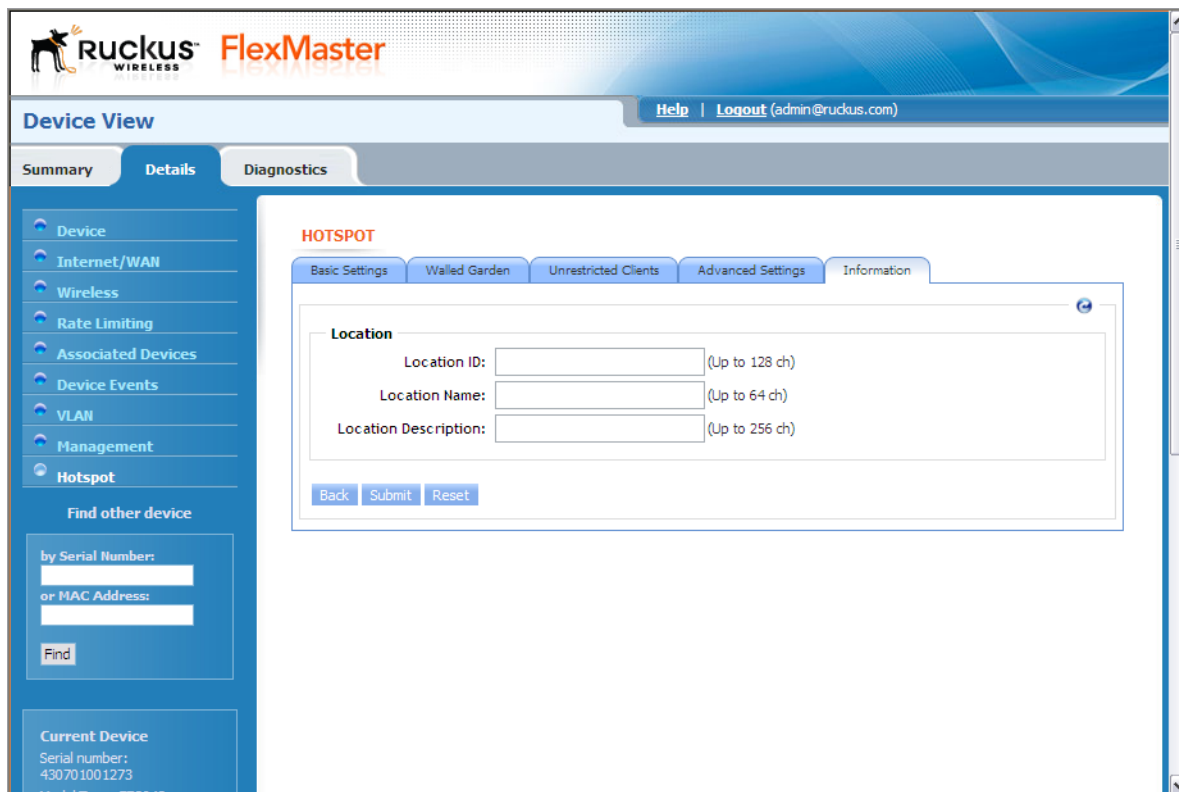
---

4. If your ISP is blocking outgoing SMTP messages to control spam, you can redirect your SMTP traffic to an external mail server (not within your ISP's domain) to ensure that hotspot users will be able to send email messages. Under SMTP Redirection, configure the following options:
  - *SMTP Redirect Host*: Type the IP address of the SMTP server to which SMTP traffic from your hotspot will be relayed.
  - *SMTP Redirect Port*: Type the port number used for SMTP on the redirect host (typically, this value is set to 25).
5. If you want to define the subnet for your hotspot, configure the following options under Network Settings:
  - *Hotspot Internal Gateway IP Address*: The gateway IP address assigned to the AP (default is 10 . 1 . 0 . 1). The built-in DHCP server on the AP will assign IP addresses to hotspot clients based on the gateway IP address. For example, if the gateway IP address is 10 . 1 . 0 . 1, the DHCP server will assign IP addresses to clients from 10 . 1 . 0 . 2 onwards.
  - *Hotspot Internal Network Mask*: The subnet mask for the gateway IP address (default is 255 . 255 . 255 . 0).
  - *UAM Port*: The TCP port used to receive authentication requests (default is 3990).
  - *Change of Authorization Port*: The TCP port used to receive Change-of-Authorization (CoA) messages (default is 3699).
6. Click **Submit** to save your changes.

## Setting Device Information for the RADIUS Accounting Server

Information settings include location-related attributes that are sent to the RADIUS accounting server. If your organization operates multiple hotspots, setting these attributes will identify this specific hotspot location in the RADIUS data, which may be helpful for accounting purposes.

Figure 127. Advanced Settings tab of the Hotspot page



### To set the location attributes

1. On the Hotspot page, click the **Information Settings** tab.
2. In **Location ID**, type the ISO and ITU country and area code that the AP includes in accounting and authentication requests. The required code includes:
  - **isoc** (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

The following is an example of what the Location ID entry should look like:

```
isoc=us,cc=1,ac=408,network=RuckusWireless
```

3. In **Location Name**, type the name of the hotspot location.
4. In **Location Description**, type a description for the hotspot location.
5. Click **Submit** to save your changes.

## Provisioning Tasks to Managed Devices

Configuring the Hotspot Feature on ZoneFlex 2942



# Working with Reports

**In This Chapter**

<a href="#">Available Report Types</a> .....	208
<a href="#">Generating a Device View Report</a> .....	209
<a href="#">Generating an Active Firmware Report</a> .....	212
<a href="#">Generating an Association Report</a> .....	217
<a href="#">Generating a Provision Report</a> .....	219
<a href="#">Generating Events-related Reports</a> .....	221
<a href="#">Generating a SpeedFlex Report</a> .....	230
<a href="#">Generating a Capacity Report</a> .....	232
<a href="#">Generating an SLA Report</a> .....	234
<a href="#">Generating a Troubleshooting Report</a> .....	236
<a href="#">Generating a PCI Report</a> .....	238
<a href="#">Using Advanced Report Options</a> .....	241

## Available Report Types

[Table 25](#) 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 25. Available reports in FlexMaster

Report Name	Description
Device View	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.
Active Firmware	Generate an active firmware report to view a list of devices that are currently using the selected firmware.
Historical Connectivity	Generate a historical connectivity report to view the connection statuses of managed devices in different device views.
Association	Generate an association report, which identifies clients that are currently associated with managed APs and managed APs are currently reporting to managed ZoneDirector devices.
Provision	Generate a provision report, which lists the statuses of all tasks that you have provisioned, categorized based on task types.
Events	Generate an events report, which lists all events that match the selected event category, device category, and event type.
SpeedFlex	Generate a SpeedFlex report to view completed throughput test results based on the test name, source or destination IP address, date executed, user, etc.
Capacity	Generate various graphs that display device capacity data based on throughput, associated clients, airtime utilization, and traffic, among others.
SLA	Generate various graphs that 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, Physical Link Distance and Ping Test.
PCI	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.

## 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.

### To generate a device view report

1. Go to **Inventory > Reports**.
2. On the *Report Categories* menu, click **Device View**.
3. Go to the *Report Options* section.
4. In *Device View*, select the device view for which you want to generate a report. Default device views include:
  - All Standalone APs
  - All ZoneDirectors

If you created custom device views, they will also appear in the list of options.




---

**NOTE:** If you selected 2-tier management mode, ZoneDirector options will not be visible on the page and ZoneDirector information will not be included in the report that you are generating.

---

5. 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**, select one of the following options in *Report Type*:
    - *ZoneDirectors*: Shows all ZoneDirector devices that FlexMaster is managing
    - *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
    - *Access Points*: Shows all APs that are reporting to all ZoneDirector devices that FlexMaster is managing
    - *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.
    - *Connected Clients*: Shows all wireless clients that are currently connected to APs being managed by ZoneDirector devices
    - *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 (under 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 managed APs that currently have zero wireless clients for the selected time period.

- *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.
  - If you selected **All Standalone APs**, select one of the following options in *Report Type*:
    - *APs*: Shows all APs that are FlexMaster is managing directly
    - *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 within the last 24 hours
    - *Seen in Last 48 Hours*: Shows all directly-managed APs that communicated with FlexMaster within 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 all wireless clients that are currently connected to APs that are directly managed by FlexMaster
    - *Bridge APs*: Shows information about standalone bridge APs that FlexMaster is managing directly. Details show include device name, serial number, MAC address, IP address, uptime, bridge mode, and RX and TX RSSI (among others).
  - 6. (Optional) If you want to add a search filter to your query, 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, only devices with this IP address will 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, all devices with "100" in the IP address (for example, 172.17.16.100 and 100.1.10.13) will 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, only devices with serial numbers that begin with "3908" (for example, 390801005202) will 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, only devices with model names that end in "13" (for example, 100.1.10.13) will 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 may consist of numbers or letters (depending on be the attribute that you selected in the first drop-down list box) and may be a partial or full string. Refer to the previous step for search examples.
- d. If you want to add another search filter, 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.

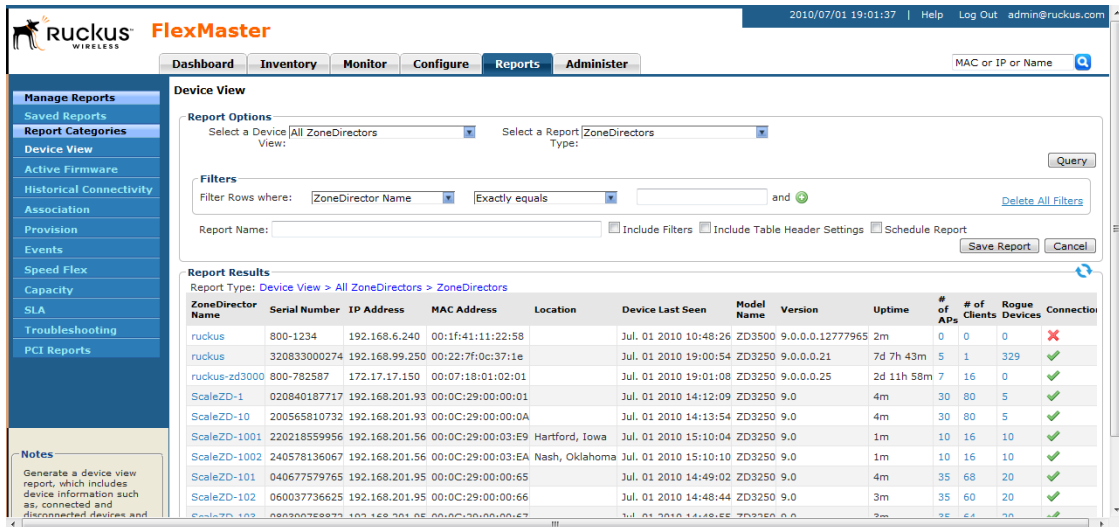
7. Click **Query**.

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
- MAC Address
- IP Address
- Model Name
- Device Last Seen
- Uptime
- Tag
- Software
- Connection status (connected or disconnected)

Figure 128. An example of a Device View report



The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The left sidebar contains 'Manage Reports', 'Report Categories', 'Device View', 'Active Firmware', 'Historical Connectivity', 'Association', 'Provision', 'Events', 'Speed Flex', 'Capacity', 'SLA', 'Troubleshooting', and 'PCI Reports'. The main content area is titled 'Device View' and contains a 'Report Options' section with dropdowns for 'View' (All ZoneDirectors) and 'Type' (ZoneDirectors). Below this is a 'Filters' section with a 'Filter Rows where:' dropdown set to 'ZoneDirector Name', an operator dropdown set to 'Exactly equals', and a text input field. A 'Query' button is to the right. Below the filters are checkboxes for 'Report Name', 'Include Filters', 'Include Table Header Settings', and 'Schedule Report', along with 'Save Report' and 'Cancel' buttons. The 'Report Results' section shows a table with the following columns: ZoneDirector Name, Serial Number, IP Address, MAC Address, Location, Device Last Seen, Model Name, Version, Uptime, # of APs, # of Clients, Rogue Devices, and Connection. The table contains several rows of device data.


ZoneDirector Name	Serial Number	IP Address	MAC Address	Location	Device Last Seen	Model Name	Version	Uptime	# of APs	# of Clients	Rogue Devices	Connection
ruckus	800-1234	192.168.6.240	00:1f:41:11:22:58		Jul. 01 2010 10:48:26	ZD3500	9.0.0.0.12777965	2m	0	0	0	✗
ruckus	320833000274	192.168.99.250	00:22:7f:0c:37:1e		Jul. 01 2010 19:00:54	ZD3250	9.0.0.0.0.21	7d 7h 43m	5	1	329	✓
ruckus-zd3000	800-782587	172.17.17.150	00:07:18:01:02:01		Jul. 01 2010 19:01:08	ZD3250	9.0.0.0.0.25	2d 11h 58m	7	16	0	✓
ScaleZD-1	020840187717	192.168.201.93	00:0C:29:00:00:01		Jul. 01 2010 14:12:09	ZD3250	9.0	4m	30	80	5	✓
ScaleZD-10	200565810732	192.168.201.93	00:0C:29:00:00:0A		Jul. 01 2010 14:13:54	ZD3250	9.0	4m	30	80	5	✓
ScaleZD-1001	220218559956	192.168.201.56	00:0C:29:00:03:E9	Hartford, Iowa	Jul. 01 2010 15:10:04	ZD3250	9.0	1m	10	16	10	✓
ScaleZD-1002	240578136067	192.168.201.56	00:0C:29:00:03:EA	Nash, Oklahoma	Jul. 01 2010 15:10:10	ZD3250	9.0	1m	10	16	10	✓
ScaleZD-101	040677579765	192.168.201.95	00:0C:29:00:00:65		Jul. 01 2010 14:49:02	ZD3250	9.0	4m	35	68	20	✓
ScaleZD-102	060037736625	192.168.201.95	00:0C:29:00:00:66		Jul. 01 2010 14:48:44	ZD3250	9.0	3m	35	60	20	✓

## 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.

### To generate an Active Firmware report

1. Go to **Inventory > Reports**.
2. On the *Report Categories* menu, click **Active Firmware**.
3. Go to the *Report Options* section.
4. In **Select a 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 > Manage Firmware Files** page.
5. (Optional) If you want to add a search filter to your query, 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, only devices with this IP address will 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, all devices with “100” in the IP address (for example, 172 . 17 . 16 . **100** and **100** . 1 . 10 . 13) will 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, only devices with serial numbers that begin with “3908” (for example, 390801005202) will 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, only devices with model names that end in “13” (for example, 100 . 1 . 10 . **13**) will 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 may consist of numbers or letters (depending on be the attribute that you selected in the first drop-down list box) and may be a partial or full string. Refer to the previous step for search examples.

- d. If you want to add another search filter, 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**.

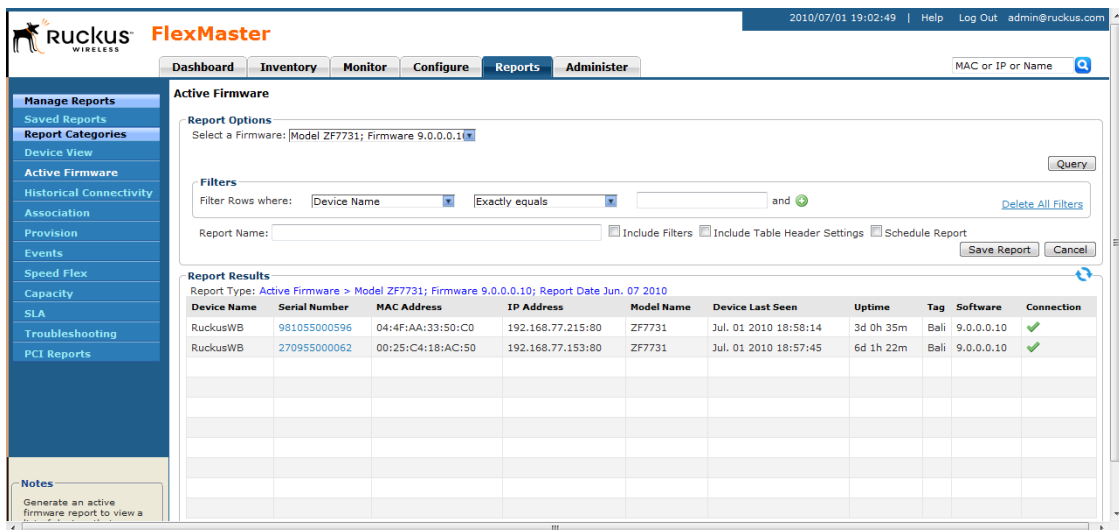
The page refreshes, and then displays the devices that are currently using the firmware version you specified. Firmware details that are shown include:

- Device Name
- Serial Number
- MAC Address
- IP Address
- Model Name
- Device Last Seen
- Uptime
- Tag
- Software
- Connection status (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, see ["Using Advanced Report Options"](#).

Figure 129. An example of an Active Firmware report



The screenshot shows the Ruckus FlexMaster interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The 'Reports' section is active, showing 'Active Firmware' options. The 'Report Options' section allows selecting a firmware version (Model ZF7731; Firmware 9.0.0.0.10). The 'Filters' section shows a filter for 'Device Name' set to 'Exactly equals'. The 'Report Results' section displays a table with the following data:

Device Name	Serial Number	MAC Address	IP Address	Model Name	Device Last Seen	Uptime	Tag	Software	Connection
RuckusWB	981055000596	04:4F:AA:33:50:C0	192.168.77.215:80	ZF7731	Jul. 01 2010 18:58:14	3d 0h 35m	Bali	9.0.0.0.10	✓
RuckusWB	270955000062	00:25:C4:18:AC:50	192.168.77.153:80	ZF7731	Jul. 01 2010 18:57:45	6d 1h 22m	Bali	9.0.0.0.10	✓

## Generating a Historical Connectivity Report

A Historical Connectivity report displays the connection statuses of managed devices in different device views.

### To generate a connectivity report

1. Go to **Inventory > Reports**.
2. On the *Report Categories* menu, click **Historical Connectivity**.
3. Go to the *Report Options* section.
4. In **Device View**, select the device view for which you want to generate a report. Default device views include:
  - All Standalone APs
  - All ZoneDirectors

If you created custom device views, they will also appear in the list of options.



---

**NOTE:** If you selected 2-tier management mode, ZoneDirector options will not be visible on the page and ZoneDirector information will not be included in the report that you are generating.


---

5. 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**, 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.
  - If you selected **All Standalone APs**, 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
6. (Optional) If you want to add a search filter to your query, 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, only devices with this IP address will 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, all devices with "100" in the IP address (for example, 172 . 17 . 16 . **100** and **100** . 1 . 10 . 13) will 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, only devices with serial numbers that begin with "3908" (for example, 390801005202) will 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, only devices with model names that end in "13" (for example, 100 . 1 . 10 . **13**) will appear in the search results.

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

- In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter may consist of numbers or letters (depending on be the attribute that you selected in the first drop-down list box) and may be a partial or full string. Refer to the previous step for search examples.
- If you want to add another search filter, 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. Click **Query**.

The page refreshes, and then displays devices that have not called home to FlexMaster within the defined inform interval.

*Figure 130. An example of a Connectivity report*

Working with Reports  
 Generating a Historical Connectivity Report

The screenshot displays the Ruckus FlexMaster web interface. At the top, the navigation menu includes Dashboard, Inventory, Monitor, Configure, Reports, and Administrator. The 'Reports' tab is active, showing the 'Historical Connectivity' report configuration page. The interface includes a sidebar with various report categories and a main content area for report options and results.

**Report Options:**

- Select a Device View: All ZoneDirectors
- Select a Report Type: Connected ZoneDirectors

**Filters:**

- Filter Rows where: ZoneDirector Name Exactly equals

**Report Results:**

Report Type: Historical Connectivity > All ZoneDirectors > Connected ZoneDirectors

ZoneDirector Name	Serial Number	IP Address	MAC Address	Device Last Seen	Model Name	Version	Uptime	# of APs	# of Clients	Rogue Devices	Connection
ruckus	800-1234	192.168.6.240	00:1f:41:111:22:58	Jul. 01 2010 10:48:26	ZD3500	9.0.0.0.12777965	2m	0	0	0	✗
ruckus	320833000274	192.168.99.250	00:22:7f:0c:37:1e	Jul. 01 2010 19:07:54	ZD3250	9.0.0.0.21	7d 7h 50m	5	1	335	✓
ruckus-zd3000	800-782587	172.17.17.150	00:07:18:01:02:01	Jul. 01 2010 19:08:08	ZD3250	9.0.0.0.25	2d 12h 5m	7	16	0	✓
ScaleZD-1	020840187717	192.168.201.93	00:0C:29:00:00:01	Jul. 01 2010 14:12:09	ZD3250	9.0	4m	30	80	5	✓
ScaleZD-10	200565810732	192.168.201.93	00:0C:29:00:00:0A	Jul. 01 2010 14:13:54	ZD3250	9.0	4m	30	80	5	✓
ScaleZD-1001	220218559956	192.168.201.56	00:0C:29:00:03:E9	Jul. 01 2010 15:10:04	ZD3250	9.0	1m	10	16	10	✓
ScaleZD-1002	240578136067	192.168.201.56	00:0C:29:00:03:EA	Jul. 01 2010 15:10:10	ZD3250	9.0	1m	10	16	10	✓
ScaleZD-101	040677579765	192.168.201.95	00:0C:29:00:00:65	Jul. 01 2010 14:49:02	ZD3250	9.0	4m	35	68	20	✓
ScaleZD-102	060037736625	192.168.201.95	00:0C:29:00:00:66	Jul. 01 2010 14:48:44	ZD3250	9.0	3m	35	60	20	✓
ScaleZD-103	080390758872	192.168.201.95	00:0C:29:00:00:67	Jul. 01 2010 14:48:55	ZD3250	9.0	3m	35	64	20	✓

## Generating an Association Report

An Association report identifies the clients that are currently associated with managed APs and the managed APs that are currently reporting to managed ZoneDirector devices.

### To generate an association report

1. Go to **Inventory > Reports**.
2. On the *Report Categories* menu, click **Association**.
3. Go to the *Report Options* section.
4. In **Device View**, select the device view for which you want to generate a report. Default device views include:
  - All Standalone APs
  - All ZoneDirectors

If you created custom device views, they will also appear in the list of options.



---


**NOTE:** If you selected 2-tier management mode, ZoneDirector options will not be visible on the page and ZoneDirector information will not be included in the report that you are generating.

---

5. 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**, 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.
  - If you selected **All Standalone APs**, 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
6. (Optional) If you want to add a search filter to your query, 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, only devices with this IP address will 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, all devices with "100" in the IP address (for example, 172 . 17 . 16 . **100** and **100** . 1 . 10 . 13) will 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, only devices with serial numbers that begin with "3908" (for example, 390801005202) will 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, only devices with model names that end in "13" (for example, 100 . 1 . 10 . **13**) will appear in the search results.

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

- In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter may consist of numbers or letters (depending on be the attribute that you selected in the first drop-down list box) and may be a partial or full string. Refer to the previous step for search examples.
- If you want to add another search filter, 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. Click **Query**.

The page refreshes, and then displays association events for the device view that you selected.



---

**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, see ["Using Advanced Report Options"](#).

---

Figure 131. An example of an Association report

The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The 'Reports' section is active, showing 'Association' report options. The 'Report Options' section has 'Select a Device' set to 'All ZoneDirectors' and 'Select a Report' set to 'ZoneDirectors'. The 'Filters' section shows 'Filter Rows where: ZoneDirector Name Exactly equals' with a search field and a 'Query' button. Below the filters is a 'Report Results' section with a table of data.

ZoneDirector Name	IP Address	MAC Address	Device Last Seen	Model Name	Serial Number	Version	Uptime	# of Clients	Connection
ruckus	192.168.99.250	00:22:7f:0c:37:1e	Jul. 01 2010 19:08:54	ZD3250	320833000274	9.0.0.0.21	7d 7h 51m	1	✓
ScaleZD-1	192.168.201.93	00:0C:29:00:00:01	Jul. 01 2010 14:12:09	ZD3250	020840187717	9.0	4m	80	✓
ScaleZD-10	192.168.201.93	00:0C:29:00:00:0A	Jul. 01 2010 14:13:54	ZD3250	200565810732	9.0	4m	80	✓
ScaleZD-1001	192.168.201.56	00:0C:29:00:03:E9	Jul. 01 2010 15:10:04	ZD3250	220218559956	9.0	1m	16	✓
ScaleZD-1002	192.168.201.56	00:0C:29:00:03:EA	Jul. 01 2010 15:10:10	ZD3250	240578136067	9.0	1m	15	✓
ScaleZD-101	192.168.201.95	00:0C:29:00:00:65	Jul. 01 2010 14:49:02	ZD3250	040677579765	9.0	4m	68	✓
ScaleZD-102	192.168.201.95	00:0C:29:00:00:66	Jul. 01 2010 14:48:44	ZD3250	060037736625	9.0	3m	60	✓
ScaleZD-103	192.168.201.95	00:0C:29:00:00:67	Jul. 01 2010 14:48:55	ZD3250	080390758872	9.0	3m	64	✓
ScaleZD-104	192.168.201.95	00:0C:29:00:00:68	Jul. 01 2010 14:49:07	ZD3250	100250251672	9.0	3m	68	✓
ScaleZD-105	192.168.201.95	00:0C:29:00:00:69	Jul. 01 2010 14:49:49	ZD3250	120609578016	9.0	4m	72	✓

## Generating a Provision Report


A Provision report lists the statuses of all the tasks that you have provisioned, categorized based on the task types.

### To generate a provisioning report

1. Go to **Inventory > Reports**.
2. On the *Report Categories* menu, click **Provision**.
3. Go to the Report Options section.
4. 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
5. (Optional) If you want to add a search filter to your query, 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.

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

- In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter may consist of numbers or letters (depending on be the attribute that you selected in the first drop-down list box) and may be a partial or full string. Refer to the previous step for search examples.
- If you want to add another search filter, 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 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 under 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, see ["Using Advanced Report Options"](#).

Figure 132. An example of a Provision report

Task Name	Schedule	Created	Created by	# Devices	Device Details	Status
Reboot ZD	Jul. 28 2011 19:15:00	Jul. 01 2010 19:12:08	admin@ruckus.com	3	<a href="#">View Details</a>	3#Scheduled

## 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. This section describes how to generate them:

- [Generating an Events Report](#)
- [Generating an Event Timeline Report](#)
- [Generating a Detailed Events Report](#)
- [Generating an Event Plot Report](#)

### Generating an Events Report

An Events report shows a summary of devices on which a particular event (for example, connectivity problem) has occurred.



---

**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, generate a detailed events report instead (see "[Generating a Detailed Events Report](#)").

---

#### To generate an Events report

1. Go to **Inventory > Reports**.
2. On the *Report Categories* menu, click **Events**.
3. Go to the *Report Options* section.
4. In *Event Category*, click **Events**.
5. In *Select a Device Category*, click the type of managed device for which you want to generate the report. Options include **ZoneDirectors** and **Standalone APs**.




---

**NOTE:** If you selected 2-tier management mode, ZoneDirector options will not be visible on the page and ZoneDirector information will not be included in the report that you are generating.

---

6. In *Event Type*, click the type of event for which you want to generate a report. The options that appear depend on the device category that you selected in the previous step. Managed devices generate dozens of events. The following are examples of ZoneDirector events that appear in the list:
  - Connectivity problem
  - First TR-069 client registration
  - Device rebooted
  - Configuration request initiated
  - Value changed due to configuration request
  - Firmware successfully written to flash
  - Diagnostics completed

- Unknown event occurred
  - Device rebooted - system fault
  - Associated with ZoneDirector
  - VLAN configuration rolled back
  - AP management URL changed
  - Device recovers from disconnected state
7. (Optional) If you want to add a search filter to your query, 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, only devices with this IP address will 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, all devices with "100" in the IP address (for example, 172 . 17 . 16 . **100** and **100** . 1 . 10 . 13) will 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, only devices with serial numbers that begin with "3908" (for example, 390801005202) will 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, only devices with model names that end in "13" (for example, 100 . 1 . 10 . **13**) will 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 may consist of numbers or letters (depending on be the attribute that you selected in the first drop-down list box) and may be a partial or full string. Refer to the previous step for search examples.
  - d. If you want to add another search filter, 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 devices on which the event you selected occurred.



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 will only display events that occurred after the last purge. For more information, see [“Purge Policy”](#).



**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, see [“Using Advanced Report Options”](#).

Figure 133. An example of an Events report

The screenshot shows the Ruckus FlexMaster interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The 'Reports' section is active, showing 'Event Options' with dropdowns for 'Event Category' (Events), 'Select a Device' (ZoneDirectors), and 'Select an Event' (Admin login). Below this is a 'Filters' section with a dropdown for 'Filter Rows where:' (ZoneDirector Name) and a radio button for 'Exactly equals'. The 'Report Results' section shows a table with columns: ZoneDirector Name, Serial Number, IP Address, MAC Address, Device Last Seen, Model Name, Version, Uptime, # of APs, # of Clients, Rogue Devices, Connection, and First Eve. The table contains four rows of data.

ZoneDirector Name	Serial Number	IP Address	MAC Address	Device Last Seen	Model Name	Version	Uptime	# of APs	# of Clients	Rogue Devices	Connection	First Eve
ruckus	320833000274	192.168.99.250	00:22:7f:0c:37:1e	Jul. 01 2010 19:14:54	ZD3250	9.0.0.0.21	7d 7h 57m	5	1	341	✓	Jun. 30 2010
ruckus	800-1234	192.168.6.240	00:1f:41:11:22:58	Jul. 01 2010 10:48:26	ZD3500	9.0.0.0.12777965	2m	0	0	0	✗	Jul. 01 2010
ruckus-zd3000	800-782587	172.17.17.150	00:07:18:01:02:01	Jul. 01 2010 19:15:08	ZD3250	9.0.0.0.25	2d 12h 12m	7	16	0	✓	Jun. 29 2010
SecZD_253_Lawrence	SN5678	10.1.131.253	00:22:7f:0c:36:3e	Jul. 01 2010 19:13:26	ZD3050	9.0.0.0.25	1d 4h 16m	0	0	0	✓	Jun. 30 2010

## Generating an Event Timeline Report

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, you can set the start time and end time ranges to cover the previous week.

### To generate an event timeline report

1. Go to **Inventory > Reports**.
2. On the *Report Categories* menu, click **Events**.
3. Go to the *Report Options* section.
4. In *Event Category*, click **Events**.
5. In *Select a Device View*, click the device view for which you want to generate an events report. Default device views include:

- All Standalone APs
- All ZoneDirectors


If you created custom device views, these will also appear in the list of options.



---


**NOTE:** If you selected 2-tier management mode, ZoneDirector options will not be visible on the page and ZoneDirector information will not be included in the report that you are generating.

---

6. In *Event Type*, click the type of event for which you want to generate a report. The options that appear depend on the device category that you selected in the previous step. Managed devices generate dozens of events. The following are examples of ZoneDirector events that appear in the list:
  - Connectivity problem
  - First TR-069 client registration
  - Device rebooted
  - Configuration request initiated
  - Value changed due to configuration request
  - Firmware successfully written to flash
  - Diagnostics completed
  - Unknown event occurred
  - Device rebooted - system fault
  - Associated with ZoneDirector
  - VLAN configuration rolled back
  - AP management URL changed
  - Device recovers from disconnected state
7. Click the *Start Date* box, and then type the start date (format is YYYY-MM-DD) of the date range for which to generate the report. Alternatively, click the  icon, and then select the start date from the calendar that appears.
8. Repeat the previous step for the *End Date* box, but this time type or select the end date of the date range.
9. (Optional) If you want to add a search filter to your query, 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, only devices with this IP address will 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, all devices with “100” in the IP address (for example, 172 . 17 . 16 . **100** and **100** . 1 . 10 . 13) will 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, only devices with serial numbers that begin with “3908” (for example, 390801005202) will 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, only devices with model names that end in “13” (for example, 100 . 1 . 10 . **13**) will appear in the search results.

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

- In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter may consist of numbers or letters (depending on be the attribute that you selected in the first drop-down list box) and may be a partial or full string. Refer to the previous step for search examples.
- If you want to add another search filter, 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.

#### 11. Click **Query**.

The page refreshes, and then displays devices on which the event you selected occurred within the date range you specified.



---

**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, see [“Using Advanced Report Options”](#).

---

Figure 134. An example of an Event Timeline report

The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The 'Reports' section is active. On the left, a sidebar menu lists various report categories, with 'Events' selected. The main content area is titled 'Events' and contains a 'Report Options' section with dropdowns for 'Event Category' (set to 'Event Timeline'), 'Select a Device' (set to 'All ZoneDirectors'), and 'Select an Event' (set to 'Admin login'). It also has date pickers for 'Start Date' (2010-06-27) and 'End Date' (2010-06-30). Below this is a 'Filters' section with a 'Filter Rows where:' dropdown set to 'ZoneDirector Name', a comparison operator set to 'Exactly equals', and a search input field. There are checkboxes for 'Include Filters', 'Include Table Header Settings', and 'Schedule Report'. A 'Query' button is present. The 'Report Results' section shows a table with the following data:

ZoneDirector Name	Serial Number	IP Address	MAC Address	Device Last Seen	Model Name	Version	Uptime	# of APs	# of Clients	Rogue Devices	Connection	First Event Time
ruckus	320833000274	192.168.99.250	00:22:7f:0c:37:1e	Jul. 01 2010 19:16:54	ZD3250	9.0.0.0.21	7d 7h 59m	5	1	341	✓	Jun. 30 2010 15
ruckus-zd3000	800-782587	172.17.17.150	00:07:18:01:02:01	Jul. 01 2010 19:17:08	ZD3250	9.0.0.0.25	2d 12h 14m	7	16	0	✓	Jun. 29 2010 16
SecZD_253_Lawrence	SN5678	10.1.131.253	00:22:7f:0c:36:3e	Jul. 01 2010 19:13:26	ZD3050	9.0.0.0.25	1d 4h 16m	0	0	0	✓	Jun. 30 2010 09

## Generating a Detailed Events Report

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, the detailed events report will show details of all 10 occurrences, including the dates and times when the events occurred.

### To generate a detailed events report

1. Go to **Inventory > Reports**.
2. On the *Report Categories* menu, click **Events**.
3. Go to the *Report Options* section.
4. In *Event Category*, click **Detailed Events**.
5. In *Select a Device Category*, click the type of managed device for which you want to generate the report. Options include **ZoneDirectors** and **Standalone APs**.



**NOTE:** If you selected 2-tier management mode, ZoneDirector options will not be visible on the page and ZoneDirector information will not be included in the report that you are generating.

6. In *Select an Event Type*, click the type of event for which you want to generate a report. The options that appear depend on the device category that you selected in the previous step. Managed devices generate dozens of events. The following are examples of ZoneDirector events that appear in the list:
  - Connectivity problem
  - First TR-069 client registration
  - Device rebooted
  - Configuration request initiated
  - Value changed due to configuration request
  - Firmware successfully written to flash
  - Diagnostics completed
  - Unknown event occurred
  - Device rebooted - system fault
  - Associated with ZoneDirector
  - VLAN configuration rolled back
  - AP management URL changed
  - Device recovers from disconnected state
7. (Optional) If you want to add a search filter to your query, 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, only devices with this IP address will 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, all devices with "100" in the IP address (for example, 172 . 17 . 16 . **100** and **100** . 1 . 10 . 13) will 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, only devices with serial numbers that begin with "3908" (for example, 390801005202) will 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, only devices with model names that end in "13" (for example, 100 . 1 . 10 . **13**) will 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 may consist of numbers or letters (depending on be the attribute that you selected in the first drop-down list box) and may be a partial or full string. Refer to the previous step for search examples.
- 8. If you want to add another search filter, 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.
- 9. Click **Query**.

The page refreshes, and then displays all occurrences of the selected event on all devices that belong to the selected device category.

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 will only display events that occurred after the last purge. For more information, see "[Purge Policy](#)".



**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, see "[Using Advanced Report Options](#)".

Figure 135. An example of a Detailed Events report

The screenshot shows the FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The 'Reports' section is active. On the left, a sidebar menu lists various report categories like 'Manage Reports', 'Saved Reports', 'Report Categories', etc. The main content area is titled 'Events' and contains a 'Report Options' section with dropdowns for 'Event Category' (Detailed Events), 'Select a Device' (ZoneDirectors), and 'Select an Event' (Admin login). Below this is a 'Filters' section with a 'Filter Rows where:' field set to 'ZD Name' and 'Exactly equals'. The 'Report Results' section shows a table with columns for ZD Name, ZD MAC, ZD IP Address, ZD Model Name, Timestamp, and Detail. The table lists several events for devices like 'ruckus' and 'ruckus-zd3000'.

ZD Name	ZD MAC	ZD IP Address	ZD Model Name	Timestamp	Detail
ruckus	00:22:7f:0c:37:1e	192.168.99.250	ZD3250	Jun. 30 2010 15:33:34	time:Jun. 30 2010 15:33:34
ruckus	00:1f:41:11:22:58	192.168.6.240	ZD3500	Jul. 01 2010 10:48:23	time:Jul. 01 2010 10:48:23
ruckus	00:22:7f:0c:37:1e	192.168.99.250	ZD3250	Jul. 01 2010 15:24:57	time:Jul. 01 2010 15:24:57
ruckus-zd3000	00:07:18:01:02:01	172.17.17.150	ZD3250	Jun. 29 2010 16:25:10	time:Jun. 29 2010 16:25:10
ruckus-zd3000	00:07:18:01:02:01	172.17.17.150	ZD3250	Jun. 29 2010 16:24:40	time:Jun. 29 2010 16:24:40
ruckus-zd3000	00:07:18:01:02:01	172.17.17.150	ZD3250	Jun. 29 2010 16:28:58	time:Jun. 29 2010 16:28:58
ruckus-zd3000	00:07:18:01:02:01	172.17.17.150	ZD3250	Jun. 29 2010 16:31:21	time:Jun. 29 2010 16:31:21
ruckus-zd3000	00:07:18:01:02:01	172.17.17.150	ZD3250	Jun. 29 2010 18:03:41	time:Jun. 29 2010 18:03:41
ruckus-zd3000	00:07:18:01:02:01	172.17.17.150	ZD3250	Jun. 29 2010 17:53:50	time:Jun. 29 2010 17:53:50
ruckus-zd3000	00:07:18:01:02:01	172.17.17.150	ZD3250	Jun. 30 2010 09:02:05	time:Jun. 30 2010 09:02:05

## Generating an Event Plot Report

An Event Plot report displays a graph version of five specific connectivity events that occurred on APs that are reporting to managed ZoneDirector devices.

### To generate an event plot report

1. Go to **Inventory > Reports**.
2. On the *Report Categories* menu, click **Events**.
3. Go to the *Report Options* section.
4. In *Event Category*, click **Event Plot**.
5. In *Select a Device View*, click the ZoneDirector device view for which you want to generate a report. The default ZoneDirector device view, *All ZoneDirectors*, is selected by default.

If you created custom device views, these will also appear in the list of options.

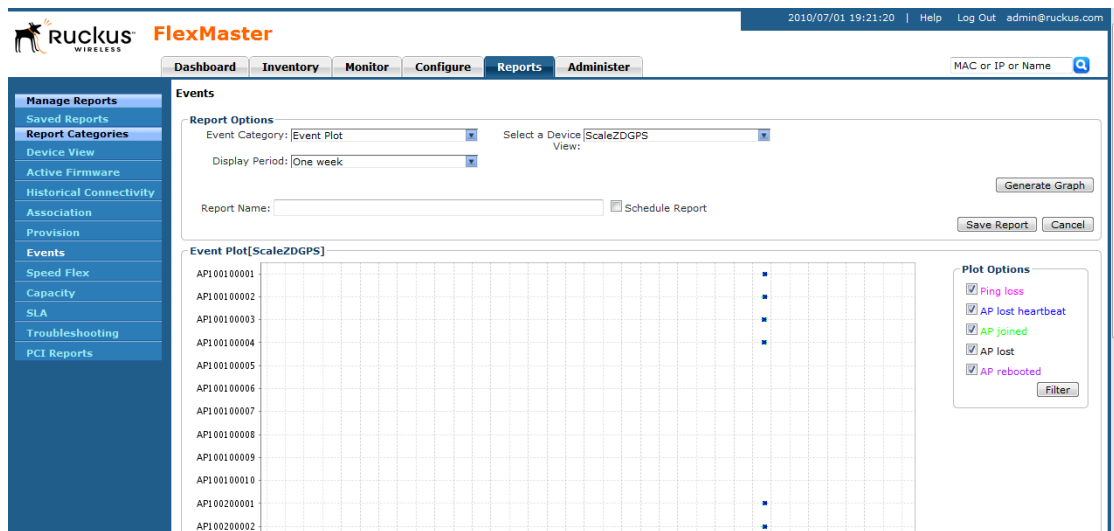
6. In *Display Period*, select the time period for which you want to generate the report. Options range from 1 hour to one week. If you want to specify a date range, select **Date Range**, and then select a one-week date range in **Start Date** and **End Date**.
7. Click **Generate Graph**.

The page refreshes, and then the events plot graph appears below the Report Options section. 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**.

Figure 136. An example of an Event Plot report



## 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, etc.

### To generate a SpeedFlex report

1. Go to **Inventory > Reports**.
2. On the *Report Categories* menu, click **SpeedFlex**.
3. Go to the *Report Options* section.
4. Look for the *Filters* section. 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, skip the *Filters* section (steps 4 to 8), and simply click the **Query** button.

5. 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).
6. In the second drop-down list box, select the search operator that you want to use. Available search operators include:



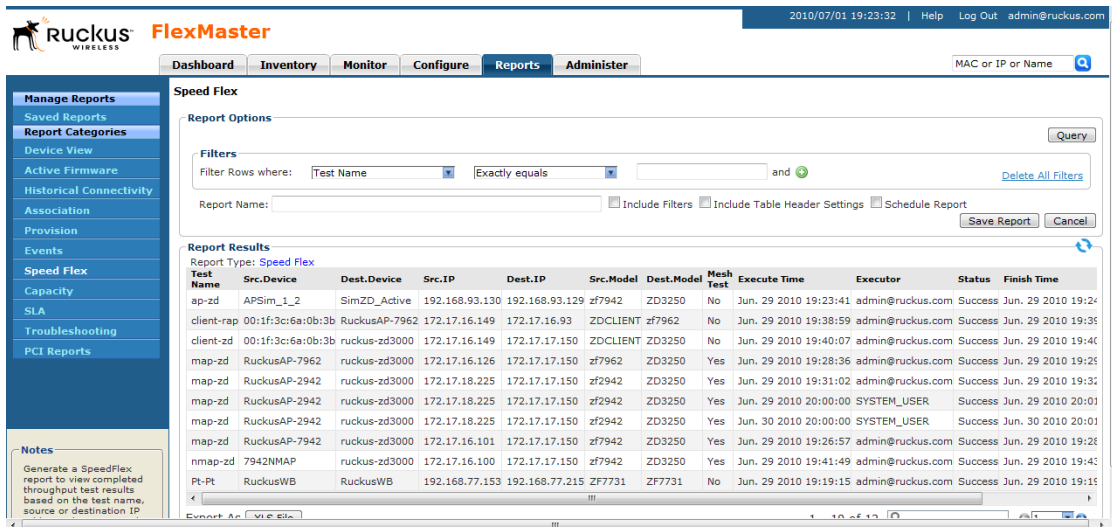
- *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered 172 . 17 . 16 . 176 as the search parameter, only devices with this IP address will appear in the search results.
- *Contains*: 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, all devices with "100" in the IP address (for example, 172 . 17 . 16 . **100** and **100** . 1 . 10 . 13) will 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, only devices with serial numbers that begin with "3908" (for example, 390801005202) will 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, only devices with model names that end in "13" (for example, 100 . 1 . 10 . **13**) will appear in the search results.

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

7. In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter may consist of numbers or letters (depending on be the attribute that you selected in the first drop-down list box) and may be a partial or full string. Refer to the previous step for search examples.
8. If you want to add another search filter, 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.
9. 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, FlexMaster displays all SpeedFlex tests that have been run and stored on the FlexMaster database.

Figure 137. An example of a SpeedFlex report



## Generating a Capacity Report

Generate various graphs that display device capacity data based on throughput, associated clients, airtime utilization, and traffic, among others.

### To generate a capacity report

1. Go to **Inventory > Reports**.
2. On the *Report Categories* menu, click **Capacity**.
3. Go to the *Report Options* section.
4. In *Device View*, select the device view for which you want to generate a report. Default device views include:
  - All Standalone APs
  - All ZoneDirectors

If you created custom device views, they will also appear in the list of options.



**NOTE:** If you selected 2-tier management mode, ZoneDirector options will not be visible on the page and ZoneDirector information will not be included in the report that you are generating.

5. 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, the following report type options appear:

- # Associated Clients
- Air-Time Utilization
- AP Actual Throughput
- AP Traffic - TX (transmitted)
- AP Traffic - RX (received)
- Client Actual Throughput
- Client Traffic - TX (transmitted)
- Client Traffic - RX (received)

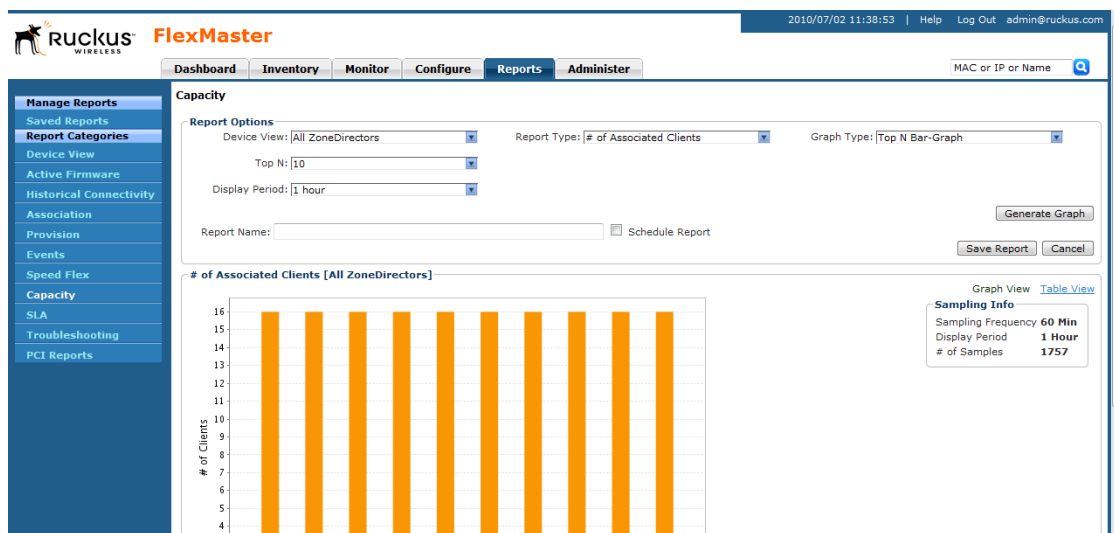
If you selected a device view consisting of Standalone APs, *Backhaul Throughput* is the only report type option that appears.

6. 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).
7. In *Display Period*, select the time period for which you want to generate the report. Options range from 1 hour to one week. If you want to specify a date range, select **Date Range**, and then select a one-week date range in **Start Date** and **End Date**.
8. 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.

Figure 138. An example of a Capacity report



## Generating an SLA Report

Generate various graphs that display service-level agreement (SLA) related information, including uptime, downtime, and potential throughput.

### To generate an SLA report

1. Go to **Inventory > Reports**.
2. On the *Report Categories* menu, click **SLA**.
3. Go to the *Report Options* section.
4. In *Device View*, select the device view for which you want to generate a report. Default device views include:
  - All Standalone APs
  - All ZoneDirectors

If you created custom device views, they will also appear in the list of options.



**NOTE:** If you selected 2-tier management mode, ZoneDirector options will not be visible on the page and ZoneDirector information will not be included in the report that you are generating.

5. 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, the following report type options appear:

- AP Downtime
- Client Potential Throughput
- Client Uptime

If you selected a device view consisting of Standalone APs, the following report type options appear:

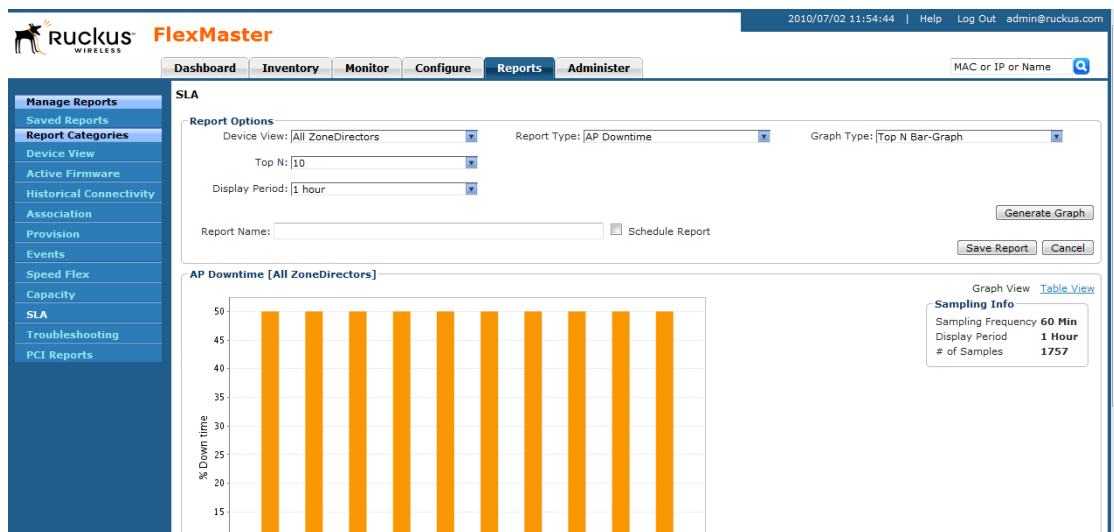
- AP Downtime
- Backhaul Link Uptime

6. 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).
7. In *Display Period*, select the time period for which you want to generate the report. Options range from 1 hour to one week. If you want to specify a date range, select **Date Range**, and then select a one-week date range in **Start Date** and **End Date**.
8. 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 139. Example of an SLA report



## Generating a Troubleshooting Report

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.

### To generate a troubleshooting report

1. Go to **Inventory > Reports**.
2. On the *Report Categories* menu, click **Troubleshooting**.
3. Go to the *Report Options* section.
4. In *Device View*, select the device view for which you want to generate a report. Default device views include:
  - All Standalone APs
  - All ZoneDirectors

If you created custom device views, they will also appear in the list of options.



**NOTE:** If you selected 2-tier management mode, ZoneDirector options will not be visible on the page and ZoneDirector information will not be included in the report that you are generating.

5. 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, the following report type options appear:

- # of Child APs
- # of Hops
- Change of Topology of Mesh
- Client Phy Rate
- Client RSSI
- Mesh RSSI
- Physical Link Distance
- Ping Test

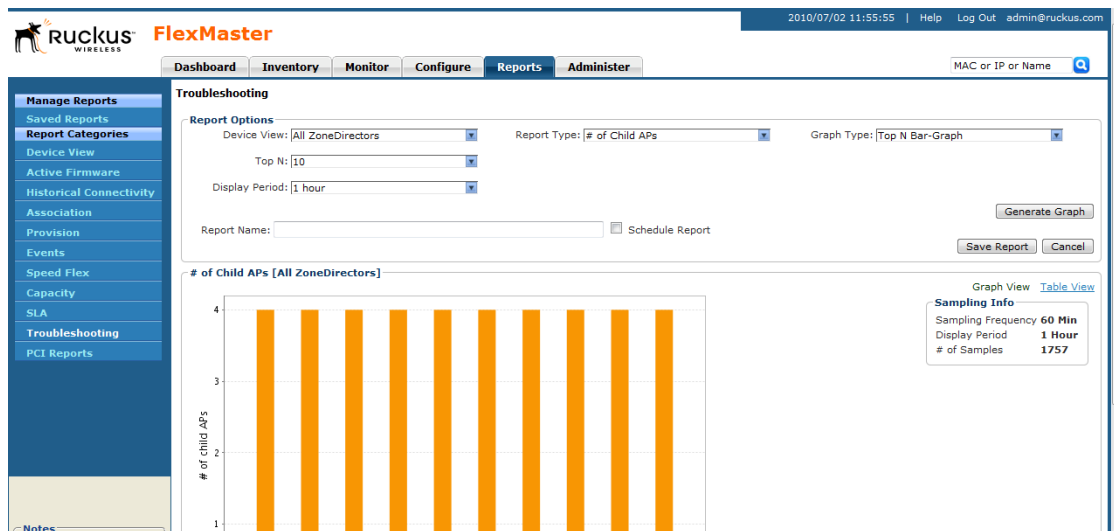
If you selected a device view consisting of Standalone APs, *Backhaul Change of State* is the only report type option that appears.

6. 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).
7. In *Display Period*, select the time period for which you want to generate the report. Options range from 1 hour to one week. If you want to specify a date range, select **Date Range**, and then select a one-week date range in **Start Date** and **End Date**.
8. 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 140. Example of a troubleshooting report



## Generating a PCI 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.

### To generate a PCI report

1. Go to **Inventory > Reports**.
2. On the *Report Categories* menu, click **PCI Reports**.
3. Go to the *Report Options* section.
4. In *Select a Device View*, click the device view for which you want to generate a report. Default device views include:
  - All Standalone APs
  - All ZoneDirectors

If you created custom device views, these will also appear in the list of options.



**NOTE:** If you selected 2-tier management mode, ZoneDirector options will not be visible on the page and ZoneDirector information will not be included in the report that you are generating.

5. In *Select a 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, the following report type options appear:

- All Access Points
- Connected Access Points
- Disconnected Access Points
- Connected Clients

---

**NOTE:** If you selected any of the three Access Point options above, you must select in *Select AP Type* the type of APs to include in the report. Options include *APs* (all AP types), *Root APs*, *Mesh APs*, and *eMesh APs*.


---

If you selected a device view consisting of Standalone APs, the following report type options appear:

- APs
  - Connected Clients
6. In *Select Period*, select the time period for which you want to generate the report. Options range from 1 hour to one week. If you want to specify a date range, select *Date Range*, and then select a one-week date range in **Start Date** and **End Date**.
  7. (Optional) If you want to add a search filter to your query, 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, only devices with this IP address will 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, all devices with “100” in the IP address (for example, 172 . 17 . 16 . **100** and **100** . 1 . 10 . 13) will 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, only devices with serial numbers that begin with “3908” (for example, 390801005202) will 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, only devices with model names that end in “13” (for example, 100 . 1 . 10 . **13**) will appear in the search results.
- After you select a search operator, a third (text) box appears.

## Working with Reports

### Hiding and Showing Columns in Reports

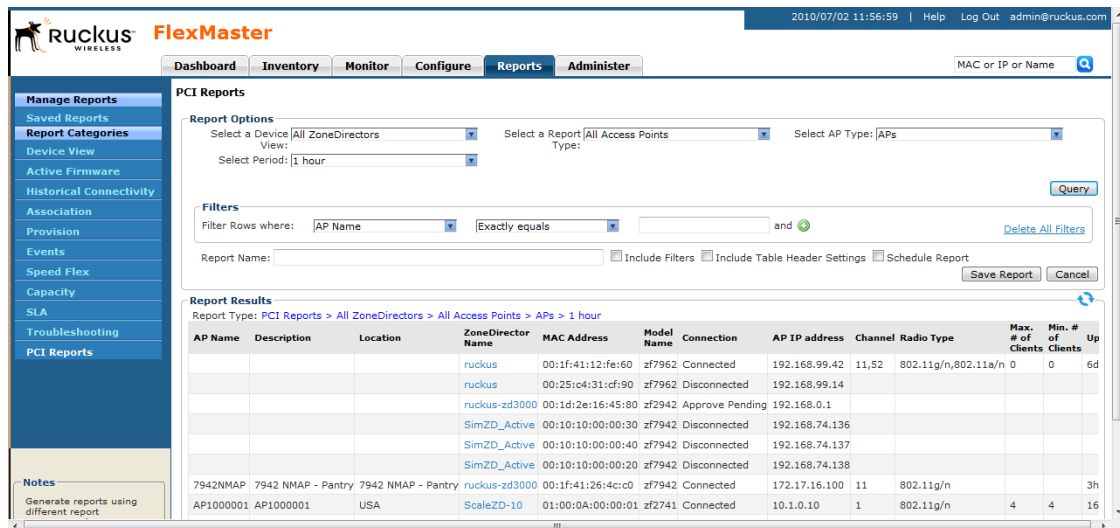
- c. In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter may consist of numbers or letters (depending on be the attribute that you selected in the first drop-down list box) and may be a partial or full string. Refer to the previous step for search examples.
8. If you want to add another search filter, 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.
9. Click **Query**.

The page refreshes, and then displays devices that match the report options that you specified.



**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, see ["Using Advanced Report Options"](#).

Figure 141. Example of a PCI report



The screenshot shows the Ruckus FlexMaster interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The 'Reports' section is active, showing 'PCI Reports' options. The 'Report Options' section includes dropdowns for 'Select a Device' (All ZoneDirectors), 'Select a Report' (All Access Points), and 'Select AP Type' (APs). The 'Filters' section has a dropdown for 'Filter Rows where:' (AP Name) and a dropdown for 'Exactly equals'. The 'Report Results' section shows a table with columns: AP Name, Description, Location, ZoneDirector Name, MAC Address, Model Name, Connection, AP IP address, Channel, Radio Type, Max. # of Clients, Min. # of Clients, and Up. The table contains several rows of data, including entries for 'ruckus', 'ruckus-zd3000', 'SimZD\_Active', and 'ScaleZD-10'.

AP Name	Description	Location	ZoneDirector Name	MAC Address	Model Name	Connection	AP IP address	Channel	Radio Type	Max. # of Clients	Min. # of Clients	Up
			ruckus	00:1f:41:12:fe:60	zf7962	Connected	192.168.99.42	11,52	802.11g/n,802.11a/n	0	0	6d
			ruckus	00:25:c4:31:cf:90	zf7962	Disconnected	192.168.99.14					
			ruckus-zd3000	00:1d:2e:16:45:80	zf2942	Approve Pending	192.168.0.1					
			SimZD_Active	00:10:10:00:00:30	zf7942	Disconnected	192.168.74.136					
			SimZD_Active	00:10:10:00:00:40	zf7942	Disconnected	192.168.74.137					
			SimZD_Active	00:10:10:00:00:20	zf7942	Disconnected	192.168.74.138					
7942NMAP	7942 NMAP - Pantry	7942 NMAP - Pantry	ruckus-zd3000	00:1f:41:26:4c:c0	zf7942	Connected	172.17.16.100	11	802.11g/n			3h
AP1000001	AP1000001	USA	ScaleZD-10	01:00:0A:00:00:01	zf2741	Connected	10.1.0.10	1	802.11g/n	4	4	16

## Hiding and Showing Columns in Reports

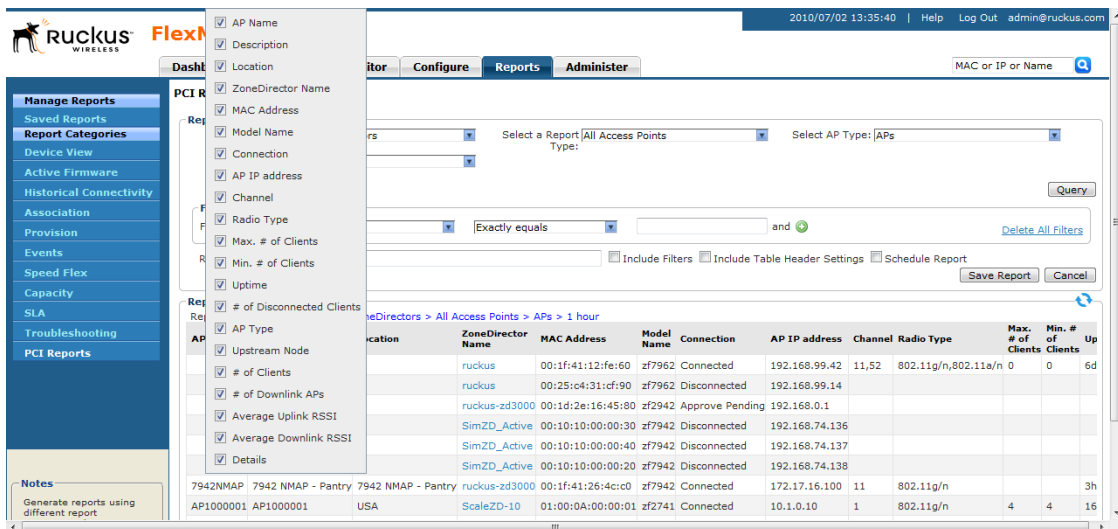
By default, all columns that are available for a particular report are displayed. If you want the report to show only specific columns, you can hide the columns that you do not want to display.

### To hide columns in reports

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 142. Clear the check boxes for the columns that you want to hide



## 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.

### To configure the advanced report options

1. Go to the **Reports** page.
2. On the *Report Categories* menu, click the name of the report that you want to configure.
3. Go to the *Report Options* section.
4. In *Report Name*, type a descriptive name for the report that you are saving.

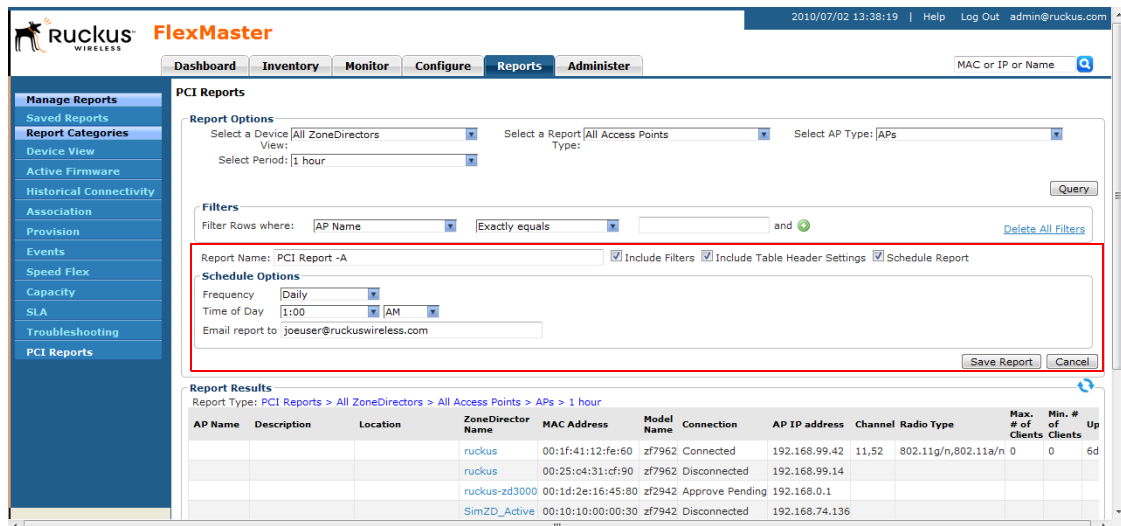
5. Configure the following settings:

- **Include Filters:** Select this check box if 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 provide report filters.
- **Include Table Header Settings:** Select this check box if 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, 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 if you want FlexMaster to generate this report automatically based on a schedule that you specify. 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**, select the **Day of the Week** when FlexMaster will generate the report. If you selected **Monthly**, select the **Day of the Month** when FlexMaster will generate the report.
  - *Time of Day:* Set the time when FlexMaster will generate the report.
  - *Email report to:* Type the email address to which the report will be sent. If you are sending the report to multiple email addresses, use a comma to separate the email addresses.

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 143. Saving a report and automating report generation



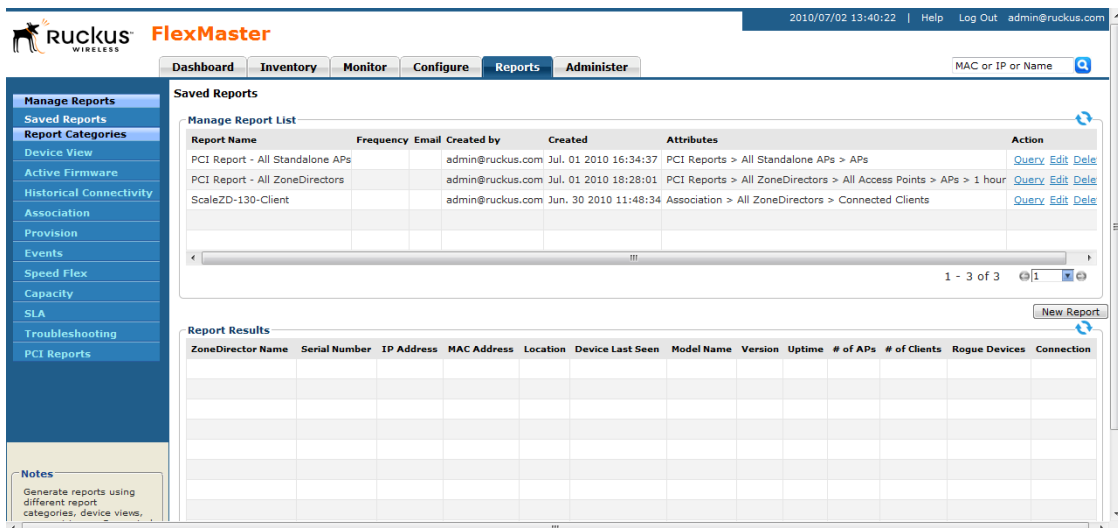
## Managing Saved Reports

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:

- [Query a Report](#)
- [Edit a Report](#)
- [Delete 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 144. The Saved Reports page



## Query a Report

Querying a report refers to manually generating the report using the options that you configured when you saved the report.

### To query a report

1. Go to **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.

## Edit a Report

If you need to change the report options, you can edit the report settings from the Saved Reports page.

### To edit a report

1. Go to **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.

## Delete a Report

If you no longer want a report to appear on the Saved Reports page, you can delete it.

### To query a report

1. Go to **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.

# Performing Administrative Tasks

## In This Chapter

<a href="#">About the Administer Tab</a> .....	245
<a href="#">Viewing Audit Logs</a> .....	245
<a href="#">Managing FlexMaster Licenses</a> .....	248
<a href="#">Configuring System Settings</a> .....	250
<a href="#">Managing Users</a> .....	255
<a href="#">Assigning Users to Manage Device Groups</a> .....	260
<a href="#">Upgrading FlexMaster Software</a> .....	270
<a href="#">Backing Up and Restoring the Database from the Web Interface</a> .....	273
<a href="#">Generating Support Information</a> .....	276

## 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 may appear in the audit logs.

Table 26. *Audit log entries*

Audit Log Entry	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

Table 26. Audit log entries

Audit Log Entry	Description
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
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 canceled	A user-created task has been canceled
Approval mode updated	User updated the AP approval mode on the Inventory page



Table 26. Audit log entries

<b>Audit Log Entry</b>	<b>Description</b>
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
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

Table 26. Audit log entries

Audit Log Entry	Description
Task restarted	User restarted a failed task
Automatic report created or updated	User created an automatic report
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 will be able to register with FlexMaster (and none will 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, any new devices attempting to register will be denied (and will 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 145. The License page

## LICENSE

The screenshot shows the License page interface. At the top, there are two statistics: Total Licenses Purchased: 10400 and Licenses Remaining: 10051. To the right, there are two more statistics: Licenses Consumed by Standalone APs: 7 and Licenses Consumed by ZoneDirectors: 342. Below this is a table with four columns: License Key, Part Number, AP Count, and Creation Date. The table contains three rows of data. At the bottom, there is a section titled 'UPLOAD A LICENSE FILE' with a text input field labeled 'Select file to upload' and a 'Browse...' button. There are also 'OK' and 'Cancel' buttons at the bottom right.

License Key	Part Number	AP Count	Creation Date
1193034973785	FME-100	100	Oct. 22 2007 14:36:13
1214769442000	901-0500-FME0	400	Jun. 30 2008 03:57:22
1214769552000	901-0000-FME1	9900	Jun. 30 2008 03:59:12

**UPLOAD A LICENSE FILE**

Select file to upload

## Uploading a License File

### To upload a license file

1. Once you obtain the license file from Ruckus Wireless, log into 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 by *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 will be sent to the specified email address when initiated from those respective areas.

It also enable 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](#)
- [Google Maps Settings](#)
- [Task Restart Settings](#)
- [Memory Optimization Settings](#)
- [Dashboard Settings](#)
- [SMTP Settings](#)
- [Purge Policy](#)

Figure 146. Top half of the System Settings page

## SYSTEM SETTINGS

**Language**  
Select your preferred language.  
Language:  

**Google Maps Settings**  
Disable Google Maps:  Yes  No

**Task Restart Settings**  
Task Restart Services:  Yes  No

**Memory Optimization Settings**  
Memory Optimization Services:  Yes  No   
Checking Interval:  day(s)

**Dashboard Settings**  
Auto Refresh Interval:  minutes

**SMTP Settings**  
   
Outgoing Mail Server Host Name: plus.smtp.mail.yahoo.com  
Server Port Number: 465  
Default Mail to: san\_kalyan@yahoo.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 by configuring the language settings on the System Settings page.



**NOTE:** Although the FlexMaster Web interface supports these five languages, the installation script is only available in English.

### To change the Web interface display language

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.

## 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.

If 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 FlexMaster to hide these gray boxes.

### To disable Google Maps

1. Go to **Administer > System Settings**.
2. Under *Google Maps Settings*, click **Yes**.
3. Click the **Save** button in the Google Maps Settings section to apply and save your settings.

## Task Restart Settings

If you want FlexMaster to automatically restart failed configuration upgrade or firmware upgrade tasks, click the Yes option, and then click the Save button in the Task Restart Settings section. By default, automatic task restart is disabled.

## 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 the Yes option, 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, the memory optimization settings that you configure will not be 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.

### 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.

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 will be 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, 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
smtpserver_hostname
```



---

**NOTE:** If you edited the hosts file before you installed FlexMaster (as described in [“Editing the Server Hosts File”](#)), the first line should already exist in the hosts file; you do not need to add the same line again.

---

### To edit SMTP settings

1. Go to **Administer > System Settings**.
2. Click the **Edit** tab.
3. Type the host name of the outgoing SMTP server at *Outgoing Mail Server Hostname*.
4. (Default port is 25) If not 25, type the SMTP server’s listening port number in *Server Port Number*.
5. Type the email address of the user to notify at *Default Mail To*.
6. Click **Save**.

Figure 147. Editing SMTP Settings

The screenshot shows a window titled "SMTP Settings". At the top, there are two tabs: "View" and "Edit". The "Edit" tab is selected. Below the tabs, there are five input fields with labels: "Outgoing Mail Server Host Name:", "Server Port Number:" (with the value "25" entered), "Default Mail to:", "Mail Host User Name (Optional):", and "Mail Host Password (Optional):". At the bottom right of the window, there are two buttons: "Save" and "Cancel".

## 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 will help ensure that FlexMaster will have sufficient disk space to perform tasks.

### To configure Purge Policy parameters

1. Go to **Administer > System Settings**.
2. Click the **Edit** tab.
3. 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 audit logs older than: default is 30 days
  - Delete historical graph data older than: default is 7 days
  - Delete system logs older than: default is 7 days
4. Click **Save**.



Figure 148. Editing Purge Policy settings

**Purge Policy**

View Edit

Delete events older than:  day(s)

Delete audit logs older than:  day(s)

Delete historical graph data older than:  day(s)

Delete system logs older than:  day(s)

Save Cancel

## Managing Users

If 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 will use FlexMaster. Ruckus Wireless recommends against the usage of one login account for multiple users as this methodology may not produce useful audit log results.

Figure 149. Users list on the Administer > Users page

### USERS

User Name	Last Login	User Role	Action
admin@company1.com	Mar. 16 2009 10:17:10	Network Administrator	<a href="#">Edit</a>
bruce@company1.com	Mar. 06 2009 12:28:18	Network Administrator	<a href="#">Edit</a> <a href="#">Delete</a>
david		Device Operator	<a href="#">Edit</a> <a href="#">Delete</a>
eddie@company1.com	Mar. 04 2009 16:52:39	Network Administrator	<a href="#">Edit</a> <a href="#">Delete</a>
emea@company1.com	Mar. 04 2009 23:27:02	Network Administrator	<a href="#">Edit</a> <a href="#">Delete</a>
eric@company1.com	Mar. 04 2009 21:58:29	Network Administrator	<a href="#">Edit</a> <a href="#">Delete</a>
guest@company1.com	Mar. 14 2009 07:39:20	Network Administrator	<a href="#">Edit</a> <a href="#">Delete</a>
luiz@company1.com		Network Administrator	<a href="#">Edit</a> <a href="#">Delete</a>

Total number of users: 21

[Create a User Account](#)

## 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 Flex-Master system. The installation process creates one default Network Administrator (admin) account; this default admin account cannot be 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 management.

## 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.

## Creating a New User Account

If 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.

### To create a new user

1. Go to **Administer** > **Users**.
2. Click the **Create a User Account** link below the *Users* table. The *Create a New User* pane appears below the link.
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. 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, the following user roles appear on the menu: **Network Administrator**, **Group Administrator**, **Group Operator**, and **Device Operator**.

For more information on user roles, see ["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.

Figure 150. Creating a user account

## USERS

User Name	Last Login	User Role	Action
admin@company1.com	Mar. 16 2009 10:17:10	Network Administrator	<a href="#">Edit</a>
bruce@company1.com	Mar. 06 2009 12:28:18	Network Administrator	<a href="#">Edit</a> <a href="#">Delete</a>
david		Device Operator	<a href="#">Edit</a> <a href="#">Delete</a>
eddie@company1.com	Mar. 04 2009 16:52:39	Network Administrator	<a href="#">Edit</a> <a href="#">Delete</a>
emea@company1.com	Mar. 04 2009 23:27:02	Network Administrator	<a href="#">Edit</a> <a href="#">Delete</a>
eric@company1.com	Mar. 04 2009 21:58:29	Network Administrator	<a href="#">Edit</a> <a href="#">Delete</a>
guest@company1.com	Mar. 14 2009 07:39:20	Network Administrator	<a href="#">Edit</a> <a href="#">Delete</a>
luiz@company1.com		Network Administrator	<a href="#">Edit</a> <a href="#">Delete</a>

Total number of users: 21 ◀ 1 ▶

---

**CREATE A NEW USER**

User Name:

Password:

Confirm Password:

User Role:  ▼

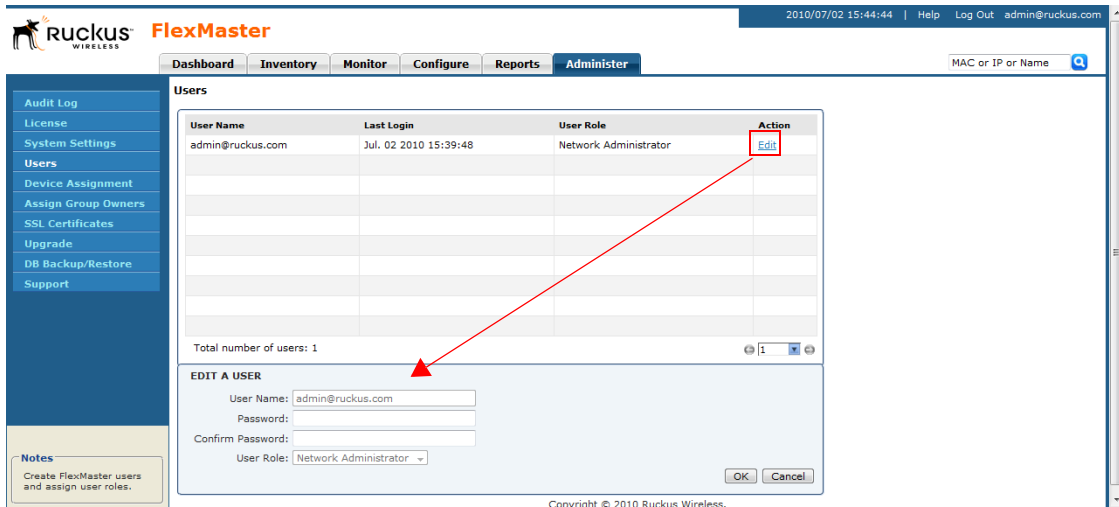
## Editing a User Account

Edit a user account if you need to make account changes, such as the user password or the user role.

### To edit a user account

1. Go to **Administer > Users**.
2. Find the row in the Users table for the desired user account to edit, and then click **Edit** under the *Action* column.
3. Edit the following options as required:
  - Password
  - Confirm Password (must exactly match the value for Password)
  - User Role (except for default "admin" account)
4. Click **OK** to save your changes.

Figure 151. Editing a user account



## 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.

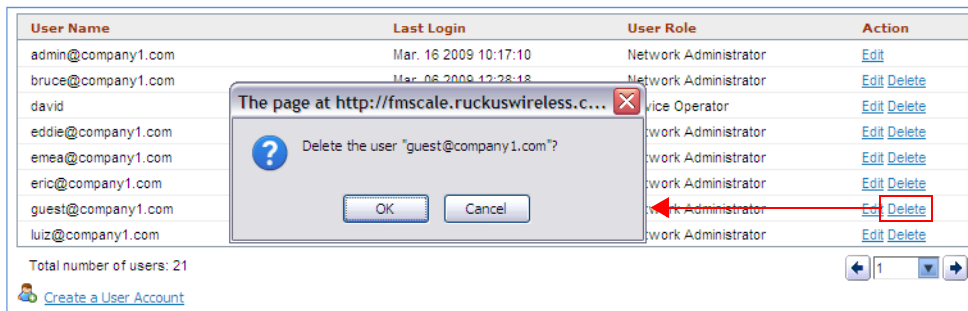
### To delete a user account

1. Go to **Administer > Users**.
2. Find the row in the *Users* table for the desired user account to delete, and then click **Delete** under the *Action* column.

The page refreshes, and then the user account you deleted disappears from the Users list.

Figure 152. Deleting a user account

## USERS



## Assigning Users to Manage Device Groups

Use the Assign Group Owners option on the **Administer** tab to delegate device management tasks to other users in your organization. Complete the following steps:

- [Step 1: Create a User Account](#)
- [Step 2: Create a Managed Group](#)
- [Step 3: Assign Devices to the Managed Group](#)
- [Step 4: Assign a User to Manage the Group](#)

### Step 1: Create a User Account

To create a new user account

1. Go to **Administer** > **Users**.
2. Click the **Create a User Account** link below the Users table. The Create a New User pane appears below the link.
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. 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, the following user roles appear on the menu:
  - Network Administrator
  - Group Administrator
  - Group Operator
  - Device Operator.

For more information on user roles, see ["Understanding User Roles and Privileges"](#).

6. Click **OK** to create the account. The page refreshes, and then the user account you created appears in the Users list.
7. Continue to ["Step 2: Create a Managed Group"](#).

Figure 153. Creating a user account

## USERS

User Name	Last Login	User Role	Action
admin@company1.com	Mar. 16 2009 10:17:10	Network Administrator	<a href="#">Edit</a>
bruce@company1.com	Mar. 06 2009 12:28:18	Network Administrator	<a href="#">Edit</a> <a href="#">Delete</a>
david		Device Operator	<a href="#">Edit</a> <a href="#">Delete</a>
eddie@company1.com	Mar. 04 2009 16:52:39	Network Administrator	<a href="#">Edit</a> <a href="#">Delete</a>
emea@company1.com	Mar. 04 2009 23:27:02	Network Administrator	<a href="#">Edit</a> <a href="#">Delete</a>
eric@company1.com	Mar. 04 2009 21:58:29	Network Administrator	<a href="#">Edit</a> <a href="#">Delete</a>
guest@company1.com	Mar. 14 2009 07:39:20	Network Administrator	<a href="#">Edit</a> <a href="#">Delete</a>
luiz@company1.com		Network Administrator	<a href="#">Edit</a> <a href="#">Delete</a>

Total number of users: 21 ◀ 1 ▶

**CREATE A NEW USER**

User Name:

Password:

Confirm Password:

User Role:  ▼

## Step 2: Create a Managed Group

### To create a managed group

1. Go to **Administer > Device Assignment**.
2. Click **Create Group**.
3. In **Group Name**, type a name that you want to assign to the managed group. For example, if this managed group contains APs based in *Sunnyvale*, you can assign the name *Sunnyvale APs* to this group.
4. Click **OK** to create the managed group. The page refreshes, and then the group that you created appears in the Device Assignment list.
5. Continue to [“Step 3: Assign Devices to the Managed Group”](#).

Figure 154. Creating a managed group

## MANAGED DEVICE ASSIGNMENT

The screenshot displays a web interface for managing device groups. At the top, there is a table with two columns: 'Group Name' and 'Action'. The first row contains 'readonly\_group' and links for 'Edit', 'Delete', and 'Assign Devices'. Below the table, it indicates 'Total number of groups: 1' with a pagination control showing '1'. A 'CREATE GROUP' section is visible at the bottom, featuring a text input field with 'ZoneFlex 2825 APs' and a note: 'The maximum length of group name is 32 characters.' There are 'OK' and 'Cancel' buttons at the bottom right of this section.

### Step 3: Assign Devices to the Managed Group

#### To assign device to a managed group

1. On the *Device Assignment* page, look for the managed group that you created in the previous step (Step 2: Create a Managed Group).
2. Click the **Assign Devices** link that is in the same row as the managed group name. The Devices Assigned to {Group Name} form appears at the bottom of the page. This form shows two panes:
  - *All Registered Devices* (left): Shows all devices that can be assigned to the group.
  - *Managed Devices* (right): Shows all devices that are currently assigned to the group.
3. To assign a device to the group, select the check box for the device in the All Registered Devices pane, and then click the Add button. Repeat this procedure for each device that you want to add to the group.

To add all devices, select the check box before Serial Number in the All Registered Devices pane to select all devices, and then click the Add button.
4. When you have finished adding devices to the group, click **Assign** to save your changes.



Figure 155. Assigning devices to a managed group

**Assign registered devices to managed device groups**

All Registered Devices

<input type="checkbox"/>	Serial Number	Model Name
<input type="checkbox"/>	VF40013337	ZF2925
<input type="checkbox"/>	ZF10002551	ZF2925
<input type="checkbox"/>	ZF10004280	ZF2925
<input type="checkbox"/>	ZF10003245	ZF2925
<input type="checkbox"/>	430701000924	ZF2942
<input type="checkbox"/>	120801001585	ZD1006

Total number of devices: 6

Devices Assigned to ZoneFlex 2825 APs

<input type="checkbox"/>	Serial Number	Model Name
<input type="checkbox"/>	VF40043146	VF2825
<input type="checkbox"/>	130801001640	VF2825

Total number of devices: 2

Buttons: Add, Remove, Assign

## Step 4: Assign a User to Manage the Group

### To assign a user to manage the group

1. Go to **Administer > Assign Group Owners**.
2. Look for the Group Administrator or Group Operator user account that you want to assign as group owner.
3. 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 device groups that you have created.
4. Select the check box for each managed group that you want to assign to the user account.
5. Click **OK** to save your changes.

When the group owner logs into the FlexMaster Web interface, he or she will be able to view and manage the devices that belong to the assigned group.

Figure 156. Assigning a user to manage the group

User Name	User Role	Action
admin@company1.com	Network Administrator	All device groups are assigned
bruce@company1.com	Network Administrator	All device groups are assigned
david	Device Operator	<a href="#">Assign Group</a>
eddie@company1.com	Network Administrator	All device groups are assigned
emea@company1.com	Network Administrator	All device groups are assigned
eric@company1.com	Network Administrator	All device groups are assigned
joe	Group Administrator	<a href="#">Assign Group</a>
luiz@company1.com	Network Administrator	All device groups are assigned

Total number of users: 21

Groups assigned to joe

<input type="checkbox"/>	Group Name	Action
<input type="checkbox"/>	readonly_group	<a href="#">Details</a>
<input checked="" type="checkbox"/>	ZoneFlex 2825 APs	<a href="#">Details</a>

Total number of groups: 2

OK

## Managing SSL Certificates

If 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, you will 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.

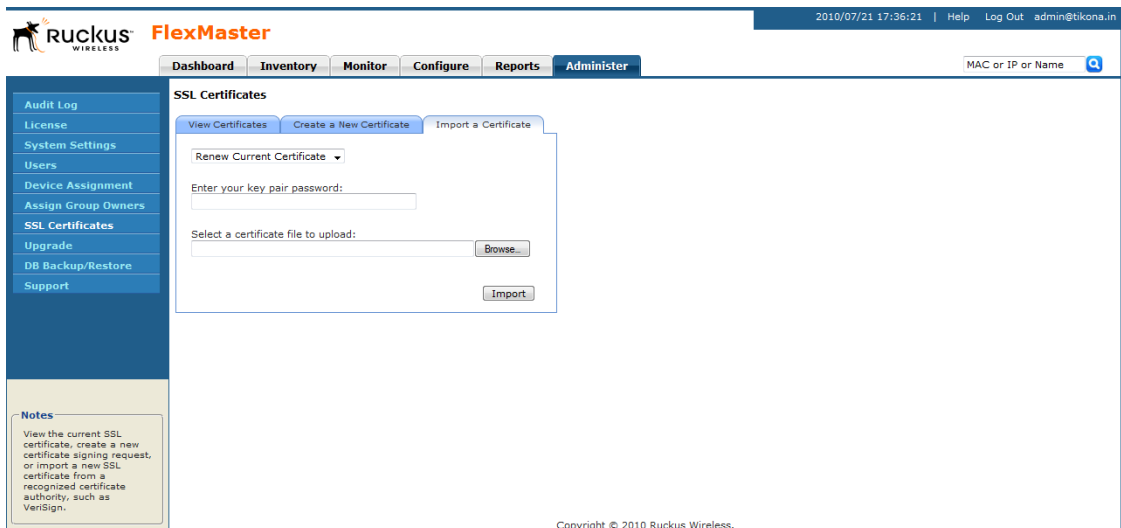
## Importing an SSL Certificate

If 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 will need the SSL certificate file and the key pair password that you set when you created the certificate signing request (CSR) file.

### To import a VeriSign-issued SSL certificate

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. Log on to the FlexMaster Web interface, and then click the Administer tab.
3. On the menu, click **SSL Certificates**.
4. On the SSL Certificates page, click the **Import a Certificate** tab.
5. In **Please enter your key pair password**, type the key pair password that was set when you created the CSR file.
6. In **Select a certificate file to upload**, click **Browse**, and then go to the location where you saved the certificate file. Select the certificate file, and then click **Open**.
7. Click **Import**. A message appears, informing you that the certificate has been imported successfully.

Figure 157. Importing an SSL certificate



8. Click the **View Certificate** 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 Certificate”](#).

9. 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
```

10. Restart the FlexMaster service by executing the following script:

```
/opt/FlexMaster/startup.sh
```

Figure 158. Shutting down and restarting the FlexMaster service

```

root@itms:/opt/FlexMaster
[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-1686/data/itms.tw.video54.local.pid
080514 07:03:42 mysqld ended

[root@itms FlexMaster]# ./startup.sh

Linux version [1686]

Starting MySQL server.

Starting mysqld daemon with databases from /opt/FlexMaster/3rdparty/mysql/mysql-enterprise-5.0.52-linux-1686/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

If you do not have a VeriSign certificate, you will 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.

### To create a certificate request file

1. On the SSL Certificates page, click the **Generate a Request** tab.
2. Click the **Create new key pair and replace the current one** option.
3. 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 159. Fill in the boxes to create the Certificate Signing Request

The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The 'Administer' tab is selected. The main content area is titled 'SSL Certificates' and has three sub-tabs: 'View Certificates', 'Create a New Certificate', and 'Import a Certificate'. The 'Create a New Certificate' tab is active. Below the tabs, there is a warning: 'The following characters are not allowed: < > ~ ! @ # \$ % ^ \* / ( ) ? \\''. The form contains the following fields and values:

Common Name:	www.ruckuswireless.com	Help text: ???admin.administration.sslcert.message.createkeypair.commonname???
Organization:	Ruckus Wireless, Inc.	The complete legal name of your organization (for example, Ruckus Wireless, Inc.). Do not abbreviate.
Organization Unit:	Network Management	The department in your organization that manages network security (for example, Network Management).
Locality or City:	Sunnyvale	The city where your organization is legally located (for example, Sunnyvale).
State/Province:	California	The state or province where your organization is legally located (for example, California). Do not abbreviate.
Country:	US	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:	*****	

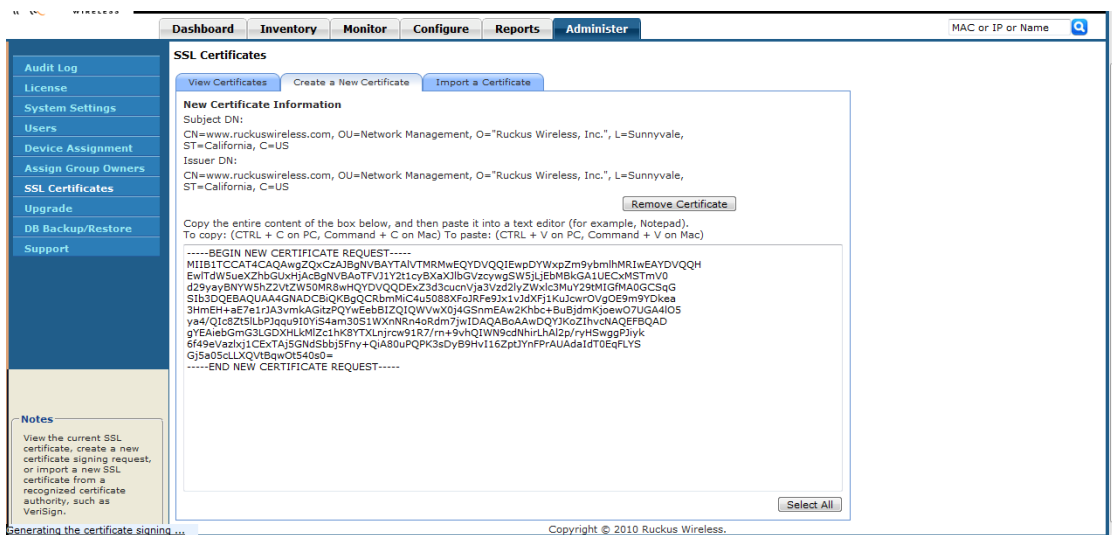
A 'Create' button is located at the bottom right of the form. On the left side of the interface, there is a sidebar menu with options like 'Audit Log', 'License', 'System Settings', 'Users', 'Device Assignment', 'Assign Group Owners', 'SSL Certificates', 'Upgrade', 'DB Backup/Restore', and 'Support'. A 'Notes' section at the bottom left provides instructions: '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.'



**WARNING!** Remember the key pair password that you set in this procedure. You will need to enter this password when you import the SSL certificate (that VeriSign will be sending you) into FlexMaster.

4. 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, click Remove Certificate, and then go back to Step 4. If the certificate information is correct, continue to Step 5.
5. Click **Generate CSR**. The page refreshes, and then display the content of the CSR.

Figure 160. Copy the content of the CSR and save it to a text file



6. Copy the complete content of the CSR request, and then paste it into a text editor (for example, Notepad). Save the file.
7. 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](http://www.verisign.com/ssl/buy-ssl-certificates/index.html)
8. 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 6., and then complete the certificate purchase.

After VeriSign approves your CSR, you will receive the VeriSign-signed certificate via email. The following is an example of a signed certificate that you will receive from VeriSign:

```
-----BEGIN CERTIFICATE-----  
MIIFVjCCBD6gAwIBAgIQLfaGuqKukMumWhbVf5v4vDANBgkqhkiG9w0BAQUFADCB  
sDELMAkGA1UEBhMCVVMxZjZAVBgNVBAoTD1Zlcm1TaWduLCBjb2MwMR8wHQYDVQQL  
BgEFBQcBAQRlMGswJAYIKwYBBQUHMAGGGH0dHA6Ly9vY3NwLnZlcm1zaWduLmNv  
bTBDBggrBgEFBQcwoY3aHR0cDovL1NWU1N1Y3VyZS1haWEudmVyaXNpZ24uY29t  
L1NWU1N1Y3VyZTIwMDU0Y29tY29tY29tY29tY29tY29tY29tY29tY29tY29tY29t  
F1RodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMMS5naWYwDQYJKoZIhvcN  
AQEFBQADggEBAl/S2dmm/kgPeValSIHmx751o4oq8+fwehRDBmQDaKiBvVXGZ5ZM  
noc3DMYDjx0SrI9lkPsn223CV3UVBZo385g1T4iKwXgcQ7/WF6QcUYOE6HK+4ZGc  
HermFf3fv3C1FoCjq+zEu8ZboUf3fWbGprGRA+MR/dDI1dTPtSUG7/zWjXO5jC//  
0pykSlDw/q8hgO8kq30S8JzCwkqrXJfQ050N4TJtgb/YC4gwh3BuB9wqRjUahTi  
KlV1ju9bHB+bFkMWIIMIXc1Js62JC1WzwFgaGUS2DL8xICQ3wU1ez8RUPGnwSxA  
YtZ2N7zDxYDP2tEiO5j2cXY708mR3ni0C30=  
-----END CERTIFICATE-----
```

- Copy the content of the signed certificate, and then paste it into a text file. Save the file. You may now import the signed certificate from VeriSign into your FlexMaster server. For instructions, refer to ["Importing an SSL Certificate"](#).

## Viewing the Current Certificate

To view the details of the certificate file that FlexMaster is currently using, click the **View Certificate** tab on the SSL certificate page. If you imported a VeriSign-signed SSL certificate, the current certificate should show VeriSign as the certificate issuer (see [Figure 162](#)).

Figure 161. The default SSL certificate on FlexMaster (signed by Ruckus Wireless)

### SSL CERTIFICATES

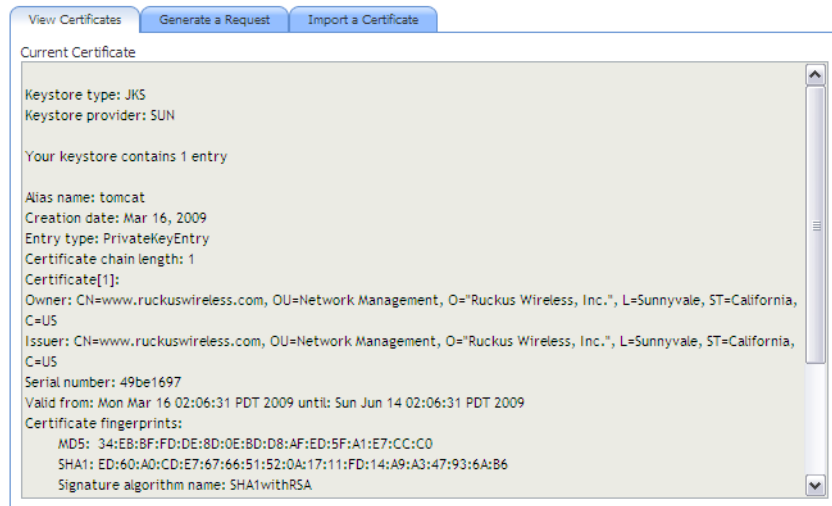
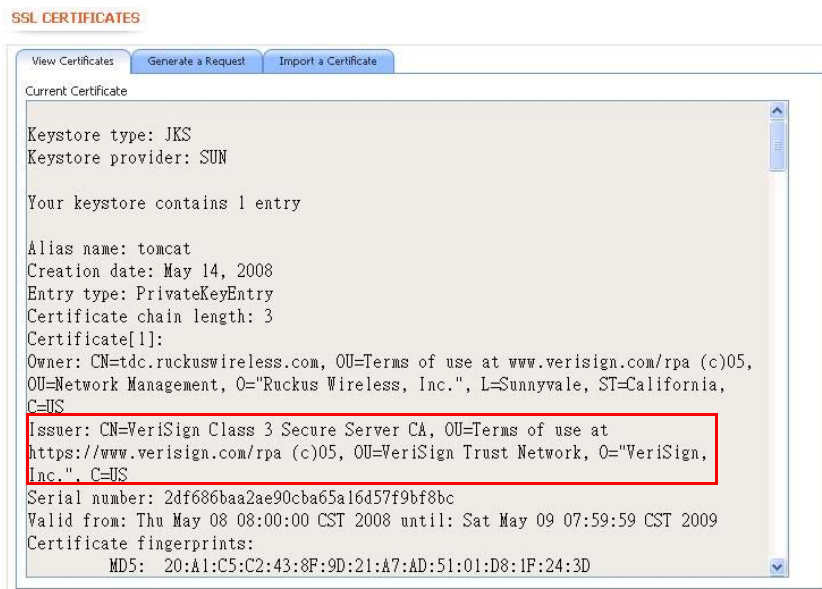


Figure 162. VeriSign-signed SSL certificate



## Upgrading FlexMaster Software

Ruckus Wireless may periodically release FlexMaster software updates that contain feature enhancements or fixes for known issues. These software updates may be made available on the Ruckus Wireless support Web site or released through authorized channels.

Update files typically use {version number}.patch for its file naming convention (for example, 8.2.0.0.15.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.



### To install a FlexMaster software update

1. On the Network View of the FlexMaster Web interface, go to **Administer > Support**. Take note of the current software version as shown in FlexMaster version.
2. On the Linux server where FlexMaster is installed, log in as root.
3. Copy the patch file to the FlexMaster installation directory. If you did not change the default installation path, the installation directory is `/opt/FlexMaster`.
4. Go to the FlexMaster installation directory.
5. Execute the following command to launch the upgrade process:

```
./upgrade {version number}
```

where {version number} is the version number of the patch that you are installing.

When the upgrade process is complete, the following message appears:

```
FLEXMASTER PATCH UPGRADE SUCCESSFUL
```

6. On the Network View of the FlexMaster Web interface, go to **Administer > Support**. You should see the following changes:
  - **FlexMaster Version** shows the software version that you have installed.
  - **Patch Information** shows **Original FlexMaster** version (previous version) and **Patch Version Upgrade Date** (new version and date installed).

If FlexMaster Version shows the software version that you have installed, you have successfully upgraded the FlexMaster software.



**WARNING!** After installing a software update, Ruckus Wireless recommends backing up the FlexMaster database so that 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.

---

## Recovering FlexMaster from an Unsuccessful Software Update

If the software update fails for any reason, the FlexMaster software update script is designed to automatically recover and restore your previous FlexMaster installation. If the autorestore process also fails, 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 into the FlexMaster server.
2. Execute the FlexMaster uninstall script.  

```
[root@flexmaster FlexMaster]# ./uninstall.sh
```
3. After you execute the uninstall script, it performs the following steps (in the same order):
  - 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 will 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 will need to enter this file path when you execute the restore script.

### 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, if 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

### To back up the FlexMaster database from the Web interface

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. If you want FlexMaster to assign a file name (in the format `FMDB_[YYYY-mm-dd-hh].tgz`) automatically, skip this step.
4. Click **Back Up**. The Backup Status Area window appears and displays the progress of the backup process.
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.

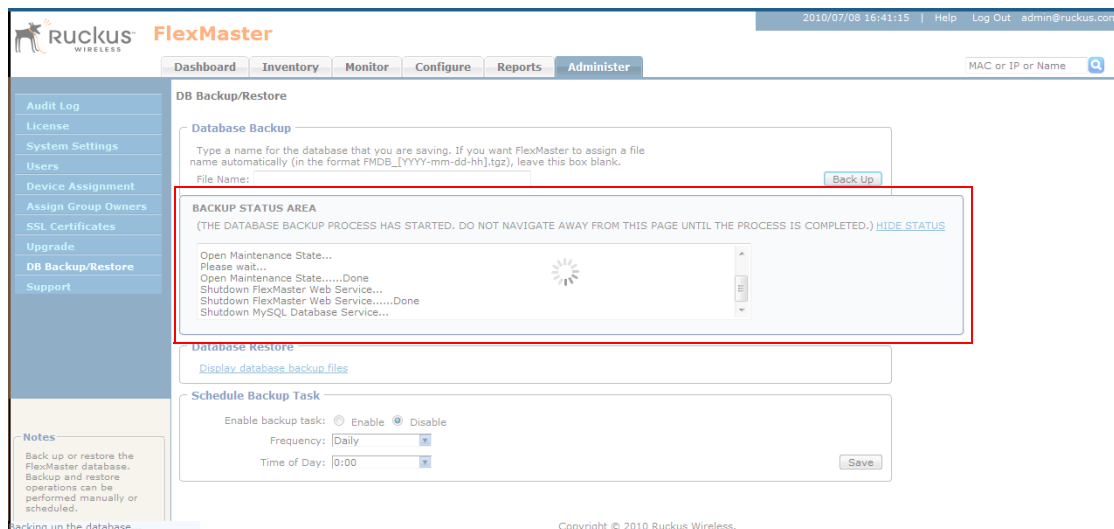
## Performing Administrative Tasks

### Backing Up and Restoring the Database from the Web Interface



**CAUTION!** Do not navigate away from the *DB Backup/Restore* page while the backup process is in progress. Doing so will cancel the backup process. Wait for the Backup Status window to display the message that the process is complete.

Figure 163. The Backup Status Area shows the progress of the backup process



## Scheduling Database Backup

You can also configure FlexMaster to back up its database automatically based on a schedule that you set.

### To schedule a database backup

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**, set the *Time of Day* when you want FlexMaster to back up the database.
  - If you clicked **Weekly**, set the *Day of the Week* and *Time of Day* when you want FlexMaster to back up the database.
  - If you clicked **Monthly**, 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

To view a list of the database files that you have backed up

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 below and displays 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 the Delete button.

## Restoring a Backup Copy of the Database

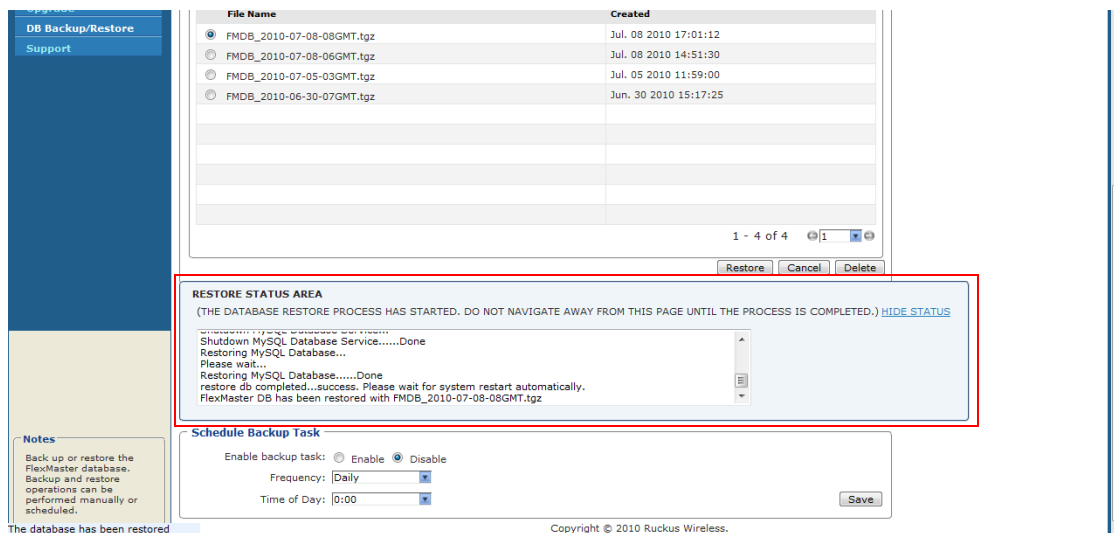
To restore a backup copy of the database

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 below 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.
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.

Figure 164. The Restore Status Area shows the progress of the restore process



## Generating Support Information

If 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 will need to generate system logs.

## Generating System Logs

The System Log is a low level system server log which is useful to support personnel. 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 are started at midnight (12:00 AM or 0:00) and midday (12:00 PM). Backed up logs appear as (midnight) FlexMaster.log.yyyy-mm-dd-AM or (midday) FlexMaster.log.yyyy-mm-dd-PM.

The system log is located in the FlexMaster installation directory under `3rdparty/tomcat/apache-tomcat-6.0.13/webapps/intune/WEB-INF/logs/`.

### To generate the system log

1. On the menu, click **Administer > Support**.
2. Click **Retrieve Log**. The log displays information from either midnight to the current time or midday to current time.

## Sending a Copy of the System Log File via Email

1. Perform the procedure in the previous section to retrieve the system log.

2. After retrieving the log, click the **Send Email** 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 165. Sending the system log via email

## SUPPORT

FlexMaster Version: 8.0.0.0.11

### System Log:

Latest System Log  Log History

#### (EMAIL)

To:

Subject: System Log Report

Attached:  FlexMaster.log.  
 InventoryList.html

Enter your message here:

**Performing Administrative Tasks**

Generating Support Information



# Index

## A

Admin Denied, 183  
auto configuration task, 154

## C

call-home, 2  
changing password, 53  
configuration upgrade tasks  
  canceling, 148  
  deleting, 150  
  restarting, 150

## D

Dashboard, 38  
deployment scenarios, 5  
device inventory, 63  
device inventory file, 187  
device operator, 257  
device registration  
  approval, 185  
  permissions, 184  
Device View widget, 42  
DHCP server, 14  
DNS server, 14

## E

Events widget, 44

## F

firmware upgrade, 178

## FlexMaster

  communication with managed devices,  
  4  
  deployment location, 5  
  getting started tasks, 53  
  installation, 11  
  installation procedure, 21  
  key terms, 8  
  L2TP communication, 58  
  license, 57  
  uninstalling, 29  
FlexMaster time, 2

## G

getting started, 53  
Google Maps, 3  
group administrator, 256  
group operator, 256

## H

hosts file, 20

## I

installation, 11  
  overview, 12  
  system requirements, 12

## K

key terms, 8

## L

L2TP communication, 58  
L2TP tunneling, 4  
license, 57  
logging in, 34

## **M**

management server configuration template, 141

## **N**

network administrator, 256

## **P**

Permitted, 183

provisioning

conventions, 132

hotspot, 196

VLAN settings, 191

## **R**

RMA, 183

## **S**

SpeedFlex, 126

system requirements, 12

## **T**

task status, 133

task status box, 36

TR-069, 3

## **U**

Unavailable, 183

user roles, 255

device operator, 257

group administrator, 256

group operator, 256

network administrator, 256

## **V**

VLAN settings, 191

## **W**

walled garden, 199

Web browser, 13

Web Interface

features, 36

Web interface

Dashboard, 38

## **Z**

ZoneDirector Device View, 101

ZoneDirector Device View widget, 44