



Ruckus Wireless™ FlexMaster™ 9.5

User Guide

Part Number 800-70386-001
Published November 2012

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	6
Service Provider Scenario	6
Hotspot Scenarios	7
Firewall Ports that Must be Open for Communications	8
Key Terms in FlexMaster	10

2 Installing FlexMaster

Preparing Your Server for FlexMaster Installation	14
What You Will Be Doing	14
Server System Requirements	14
Web Browser Requirements	15
Ensuring That APs Can Connect to FlexMaster	16
Option 1: Register FlexMaster with a DNS Server	16
Option 2: Customize Your DHCP Server	16
Option 3: Set the FlexMaster Server URL Manually from the Device View	23
Editing the Server Hosts File	24
Installing the FlexMaster Software	25
Notable Files in the FlexMaster Root Directory	31

Upgrading the FlexMaster Software	32
Uninstalling FlexMaster	34
Backing Up the Database from the Command Line Interface	35
Restoring the Database from the Command Line Interface	36
What's Next?	36

3 Getting Started with FlexMaster

Logging into FlexMaster	38
Features of the FlexMaster Web Interface	40
Getting to Know the Dashboard and Its Widgets	42
Widgets That You Can Display	43
Available Widget Slots	53
Default Widgets	55
Adding a Widget	55
Hiding a Widget	56
Deleting a Widget	56
Getting Started Tasks	57
Changing the Default Password	57
Pointing Your Ruckus Wireless AP to FlexMaster	58
Checking Your FlexMaster License	60
Configuring Your Devices to Work with TACACS+	62
Configuring Your Devices to Communicate with FlexMaster over L2TP	65

4 Working with Device Inventory

About the Inventory Page	70
ZoneDirector Inventory Pages	70
Standalone APs Inventory Pages	75
Client Inventory Pages	78
Text View and Map View	81
Working with ZoneDirector Inventory	87
Viewing a Summary of ZoneDirector Devices	87
Searching for ZoneDirector Devices	88
Editing a ZoneDirector Tag	91
Viewing ZoneDirector APs	92
Viewing ZoneDirector Mesh Connections	93
Viewing ZoneDirector WLANs and WLAN Groups	94

Viewing ZoneDirector AP Groups	95
Creating a ZD View	96
Managing ZD Views	97
Working with Standalone APs Inventory	101
Viewing a Summary of Standalone APs	101
Searching for Standalone APs	102
Editing a Standalone AP Tag	105
Creating a Standalone AP View	106
Managing Standalone AP Views	107
Viewing 7731 Bridge Relationships	110
Working with Client Inventory	113
Viewing a Summary of Clients	113
Searching for Clients	114
Creating a Client View	117
Managing Client Views	118

5 Managing a Single Standalone Access Point

Device View	122
Device View Tabs and Status Boxes	123
Viewing Device Summary	125
Viewing and Editing Device Details	127
Configuring Replacement Options for ZoneFlex 7731 Wireless Bridge	129
Performing Device Diagnostics	130
Running a Ping Test	130
Viewing the Device Log	130

6 Provisioning Tasks to Managed Devices

About Provisioning Tasks	134
Provisioning Conventions and Recommended Practices	134
Understanding the Status of a Task	135
Provisioning Tasks to Standalone APs	137
Working with AP Configuration Templates	137
Performing an AP Configuration Upgrade	148
Performing an AP Factory Reset	153
Creating an Auto Configuration Task	157
Provisioning Tasks to ZoneDirector Devices	164

Working with ZoneDirector Configuration Templates	164
Working with ZoneDirector Event Configuration	166
Performing a ZoneDirector Configuration Upgrade	171
Backing Up and Restoring ZoneDirector Configuration	173
Provisioning Common Tasks	178
Working with Device Firmware	178
Working with Reboot Tasks	183
Managing Firmware Files	185
Managing Device Registration	187
Uploading a Device Inventory File	192
Releasing Device Licenses	195
Configuring VLAN and LAN Port Settings	196
Before You Begin	196
Configuration Rules	196
General Configuration Procedures	199
How Dynamic VLAN Works	200
Sample Dynamic VLAN Scenario	201
Creating a Hotspot	204
Before You Begin	205
Configuring Basic Hotspot Settings	206
Configuring a Walled Garden	207
Specifying Unrestricted Clients	209
Configuring Advanced Settings	210
Setting Device Information for the RADIUS Accounting Server	212

7 Monitoring Events and Network Activities

About the Monitor Page	214
Monitoring Alarms	214
Viewing and Acknowledging Alarms	214
Configuring Alarm Settings	217
Monitoring Events	219
Searching for Events	219
Creating an Event View	222
Managing Event Views	223
Editing an Event View	223
Deleting an Event View	224

Viewing the Event TimeLine	225
Configuring Alert Properties	228
Disabling an Alert	229
Measuring Throughput Using SpeedFlex	230
Creating a SpeedFlex Task	230
Running a SpeedFlex Task	231
Editing a SpeedFlex Test	232
Deleting a SpeedFlex Test	232
Monitoring Access Point Trends	233
Saving the AP Trends to PDF	233
Monitoring Client Trends	234

8 Working with Reports

Available Report Types	238
Generating a Device View Report	239
Generating an Active Firmware Report	242
Generating a Historical Connectivity Report	244
Generating a Client Association Report	246
Generating an SSID Report	248
Generating a Provision Report	250
Generating Events-Related Reports	252
Generating a SpeedFlex Report	257
Generating a Capacity Report	258
Generating an SLA Report	260
Generating a Troubleshooting Report	261
Generating a Resource Monitor Report	263
Hiding and Showing Columns in Reports	265
Using Advanced Report Options	265
Managing Saved Reports	267
Querying a Report	267
Editing a Report	268
Deleting a Report	268

9 Performing Administrative Tasks

About the Administer Tab	270
--------------------------------	-----

Viewing Audit Logs	270
Managing FlexMaster Licenses	272
Uploading a License File	273
Configuring System Settings	274
Language Settings	275
IP Mode Settings	276
Google Maps Settings	276
Task Restart Settings	276
Device Ping Settings	277
Memory Optimization Settings	277
Dashboard Settings	277
SMTP Settings	278
Purge Policy	279
TACACS+ Settings	280
FTP Server Settings	281
SNMP Server Settings	282
Logo Settings	284
Managing Device Groups	286
Creating a Device Group	286
Assigning Devices to a Device Group	286
Editing a Device Group Name	287
Deleting a Device Group	287
Managing User Accounts	288
Understanding User Roles and Privileges	288
Creating a New User Account	290
Editing a User Account	291
Deleting a User Account	291
Assigning Users to Manage Device Groups	292
Managing SSL Certificates	293
Importing an SSL Certificate	293
Creating a Certificate Signing Request File for VeriSign	296
Viewing the Current Certificates	298
Upgrading the FlexMaster Software	298
Recovering FlexMaster from an Unsuccessful Software Update	300
Backing Up and Restoring the Database from the Web Interface	302
Backing Up the Database from the Web Interface	302
Scheduling Database Backup	303

Viewing and Deleting Database Backup Files	303
Restoring a Backup Copy of the Database	303
Generating Support Information	305
Viewing System Logs	305
Downloading System Logs	306
Emailing a Copy of the System Log File	306

Index

About This Guide

This guide describes how to install, configure and manage the Ruckus Wireless™ FlexMaster™ version 9.5. 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

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

Table 1. Text Conventions

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

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 9.5 User Guide*
- Part number: 800-70386-001
- Page 87

Introducing Ruckus Wireless FlexMaster

In This Chapter

Overview of Ruckus Wireless FlexMaster	2
FlexMaster Management Software and Server	2
How FlexMaster Communicates with Managed Devices	4
Where Should You Place FlexMaster?	5
Deployment Scenarios	6
Firewall Ports that Must be Open for Communications	8
Key Terms in FlexMaster	10

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



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 when scheduled, synchronize the time on the FlexMaster server with the local time. You can do this by installing an NTP client on the FlexMaster server.

Management Protocol

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

Internet Accessibility

FlexMaster requires an Internet-accessible interface to:

- *Enable remote management:* If the computer that you are using to access the FlexMaster Web interface is not on the same local network as FlexMaster, then logging into the FlexMaster Web interface remotely requires the host Linux server to be remotely accessible via HTTP or HTTPS.
- *Enable the Map View feature.* Map View data is provided by Google Maps, thus FlexMaster must be able to connect to Google Maps via the Internet to display the maps. 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 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 stops communicating with FlexMaster and registers instead with ZoneDirector. If this same AP gets provisioned with a firmware or configuration upgrade from FlexMaster, the task status appears as “Started” (pending) on the task status page as FlexMaster cannot contact the AP. If the AP registers with ZoneDirector, FlexMaster displays the status of the AP being managed by “ZD” on the **Configure > Device Registration** page.

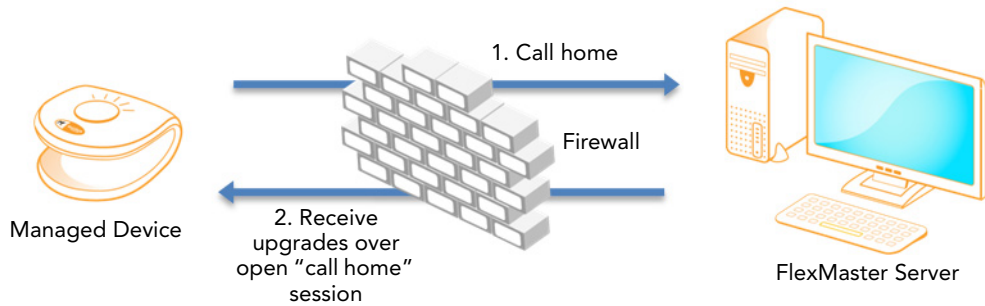
How FlexMaster Communicates with Managed Devices

FlexMaster can communicate with the devices that it manages using the [Directly Accessible Method](#) and the [L2TP Tunneling Method](#).

Directly Accessible Method

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

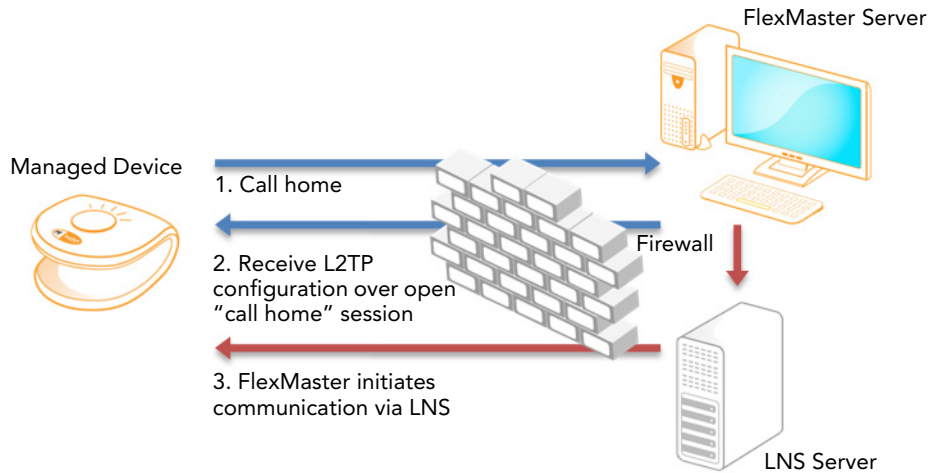
Figure 1. How a managed device calls home directly to FlexMaster



L2TP Tunneling Method

The FlexMaster connection initiation mechanism relies on the managed Ruckus Wireless AP having a routable IP address. 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](#).

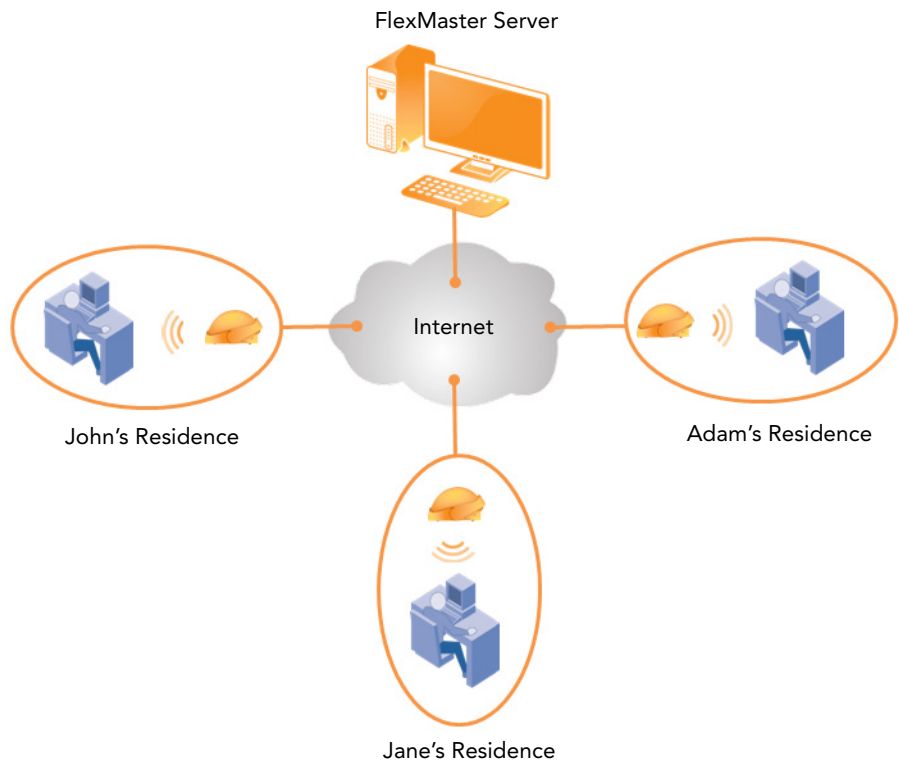
Deployment Scenarios

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

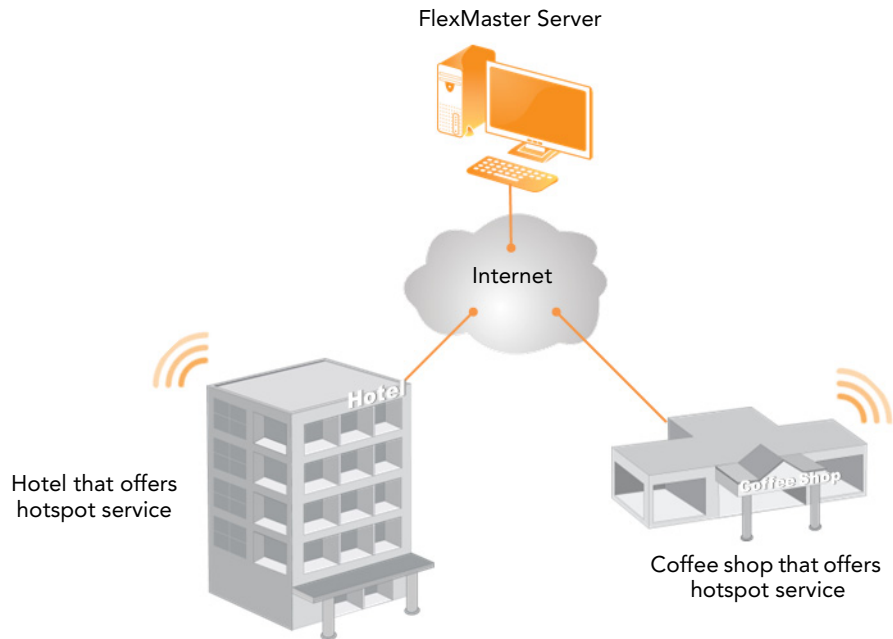


Hotspot Scenarios

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.

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

Figure 4. Hotspot scenario



Firewall Ports that Must be Open for Communications

Depending on how your network is designed, you may need to open firewall ports on any firewalls located between FlexMaster and managed ZoneDirector devices and access points. The following table lists the ports that need to be open for different types of communications.

Table 1. Firewall ports that must be open for FlexMaster communications

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

Table 1. Firewall ports that must be open for FlexMaster communications

Communication	Ports
Standalone AP > FlexMaster firmware upgrade	TCP destination port 80 (HTTP)

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

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

Key Terms in FlexMaster

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

Table 2. 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">• Provisioned as one• Consolidated in reports• Quickly recalled to filter a list <p>The grouping attributes are user customizable, and can include device type, geographic location, or any other quality that you want to use as grouping criterion.</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 Monitor > Events > New Search tab options.</p> <p>You can also create an Audit View, which groups audit log results based on the options in Administer > Audit Log > New Search.</p>
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 Configure > Device Registration page.</p> <p>The Device Registration option also enables you to pre-load a device inventory file before actual device registration. This enables you to stay ahead of your dispersal of Ruckus Wireless devices and keep track of each device's details (for example, serial number and MAC address), as well as automatically permit or deny registration with FlexMaster.</p> <p>For more on device registration, see Managing Device Registration.</p>

Table 2. Key terms in FlexMaster

Term	Description
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 Performing an AP Configuration Upgrade.</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 Provisioning Tasks to Managed Devices.</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 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>
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 Inventory page.</p>
Default Mail to:	<p>This phrase refers to the email address which is sent messages from the system based on various events. You enter this email address either during the FlexMaster installation procedure or in the To field on the Administer > System Settings > SMTP Settings page.</p> <p>You must specify an SMTP server to send email notifications to this user. See SMTP Settings.</p>

Introducing Ruckus Wireless FlexMaster

Key Terms in FlexMaster

Installing FlexMaster

In This Chapter

Preparing Your Server for FlexMaster Installation	14
Ensuring That APs Can Connect to FlexMaster	16
Editing the Server Hosts File	24
Installing the FlexMaster Software	25
Notable Files in the FlexMaster Root Directory	31
Upgrading the FlexMaster Software	32
Uninstalling FlexMaster	34
Backing Up the Database from the Command Line Interface	35
Restoring the Database from the Command Line Interface	36
What's Next?	36



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 manage. The target server must meet the following minimum requirements:

- CPU and RAM: Depends on the number of managed ZoneDirector devices and standalone APs. Refer to [Minimum Recommended RAM and CPU](#) below for more information.
- OS: Red Hat Linux Enterprise Edition 5.0 (64-bit)
- 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 helps ensure a successful database backup.

Minimum Recommended RAM and CPU

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

Table 3. Minimum recommended RAM and CPU for managing ZoneDirector devices

Managed Population	Minimum RAM	Minimum CPU
Up to 1,000 ZoneDirector-managed APs	8GB	2.0GHz Quad Core Intel® Xeon® E5506 or equivalent
Up to 5,000 ZoneDirector-managed APs	16GB	2.5GHz Six Core Intel® Xeon® E5670 or equivalent
Up to 10,000 ZoneDirector-managed APs	32GB	2* 2.5GHz Six Core Intel® Xeon® E5670 or equivalent

If FlexMaster will only be managing standalone APs, the minimum recommended RAM and CPU are listed in the following table.

Table 4. Minimum recommended RAM and CPU for managing standalone APs

Managed Population	Minimum RAM	Minimum CPU
Less than 1,000 standalone APs	8GB	2.5GHz Six Core Intel® Xeon® E5670 or equivalent
More than 1,000 standalone APs	16GB	2* 2.5GHz Six Core Intel® Xeon® E5670 or equivalent

Web Browser Requirements

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

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

Ensuring That APs Can Connect to FlexMaster

To enable FlexMaster to manage an AP, the AP must be able to communicate with FlexMaster when the AP performs its periodic “call home” procedure. To ensure successful communication between FlexMaster and the AP, 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 discover and associate with FlexMaster.



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

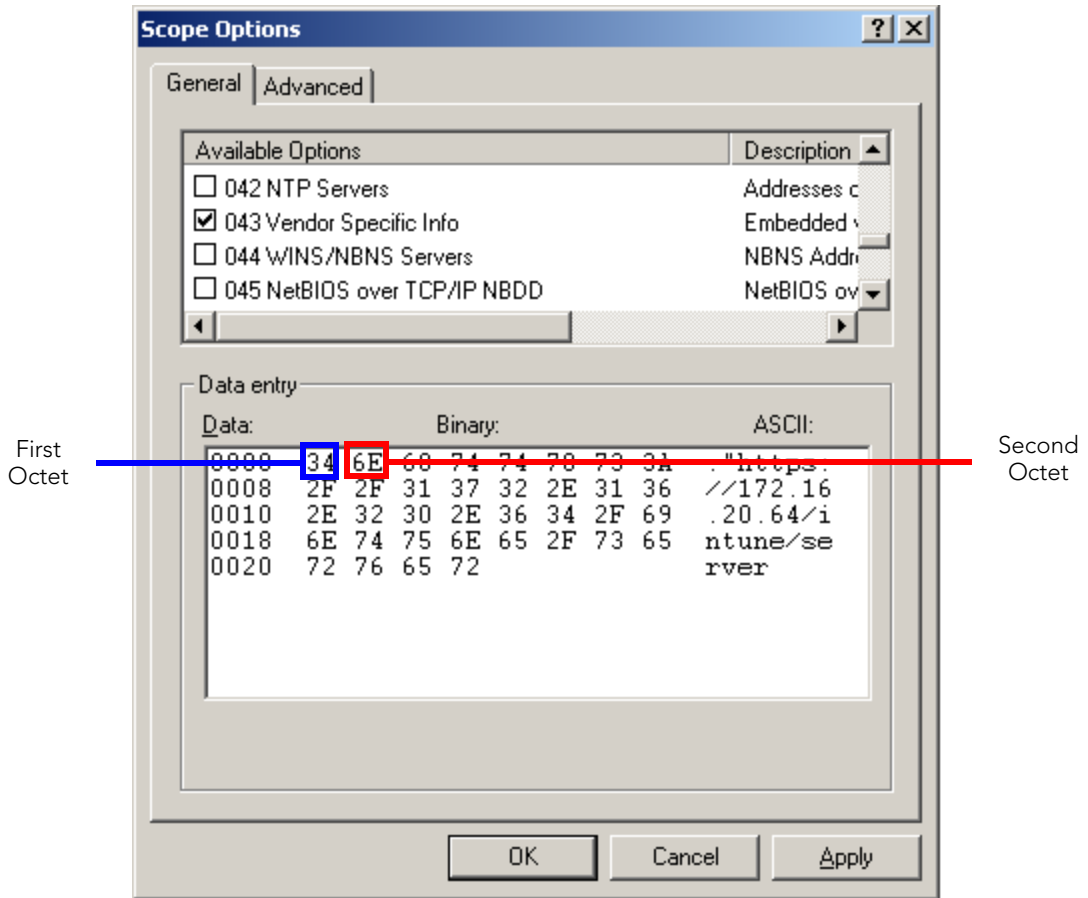


NOTE: The following procedure describes how to customize a DHCP server running on Microsoft Windows. If your DHCP server is running on a different operating system, the procedure may be different. Refer to your DHCP server’s documentation for the relevant information.

1. From the Windows Administrative Tools, open *DHCP*, and then select the DHCP server you want to configure.
2. If the *Scope* folder is collapsed, 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.

Installing FlexMaster

Ensuring That APs Can Connect to FlexMaster

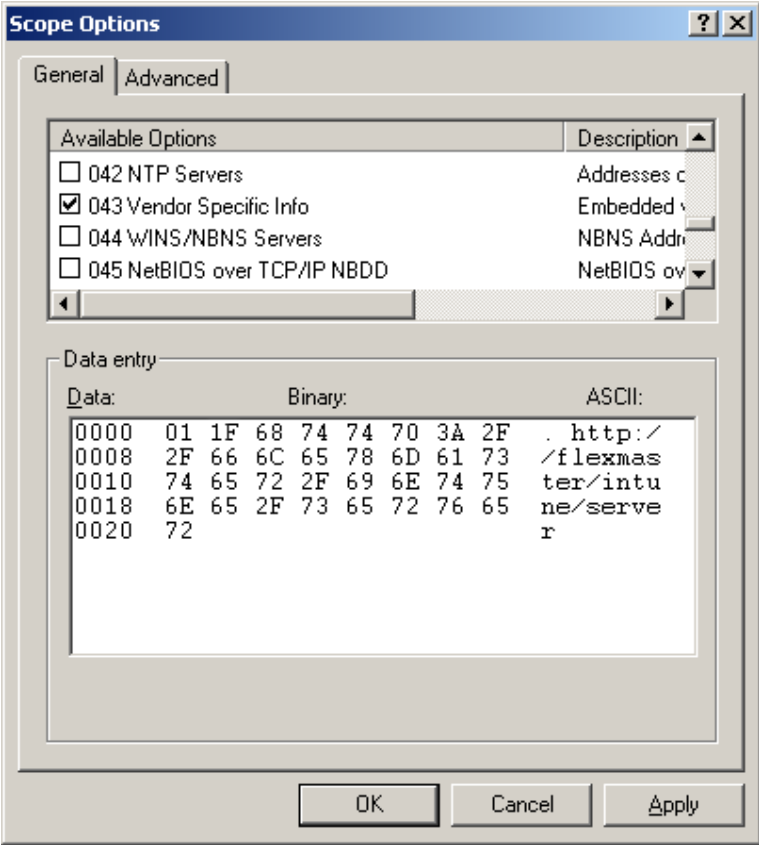
9. Take note of the hexadecimal equivalent of the number of characters in the FlexMaster server URL. Following the example above, 24 in decimal value is equivalent to 18 in hexadecimal value.
10. In the *Binary area*, select the second octet (see [Figure 5](#)), and then type the hexadecimal equivalent 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 can be different from what is shown in the following examples if you are using a different URL.

Figure 6. HTTP with a host name



Installing FlexMaster

Ensuring That APs Can Connect to FlexMaster

Figure 7. HTTPS with a host name

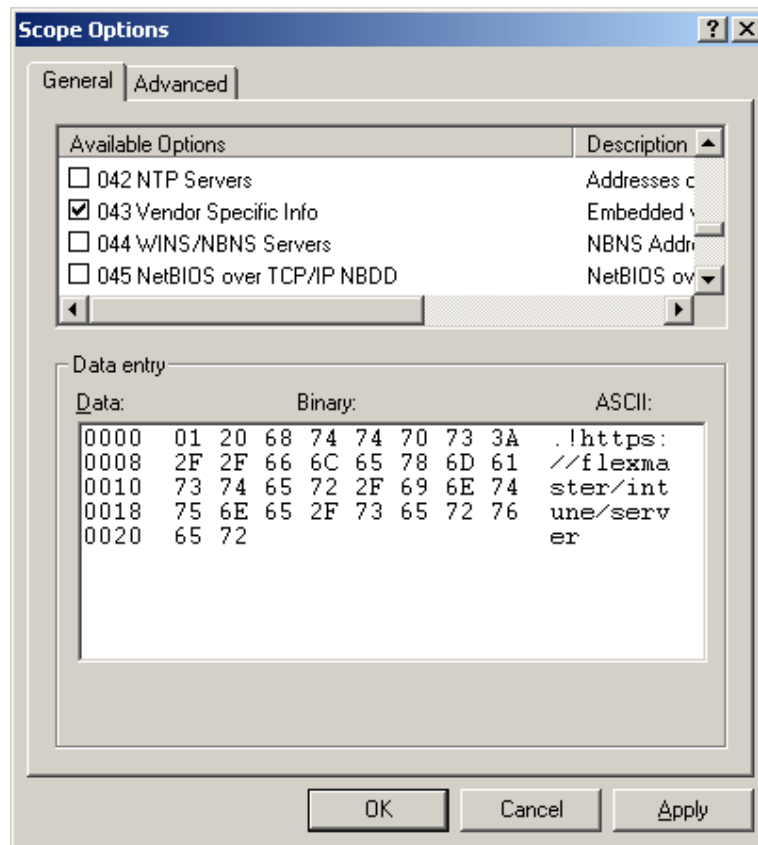
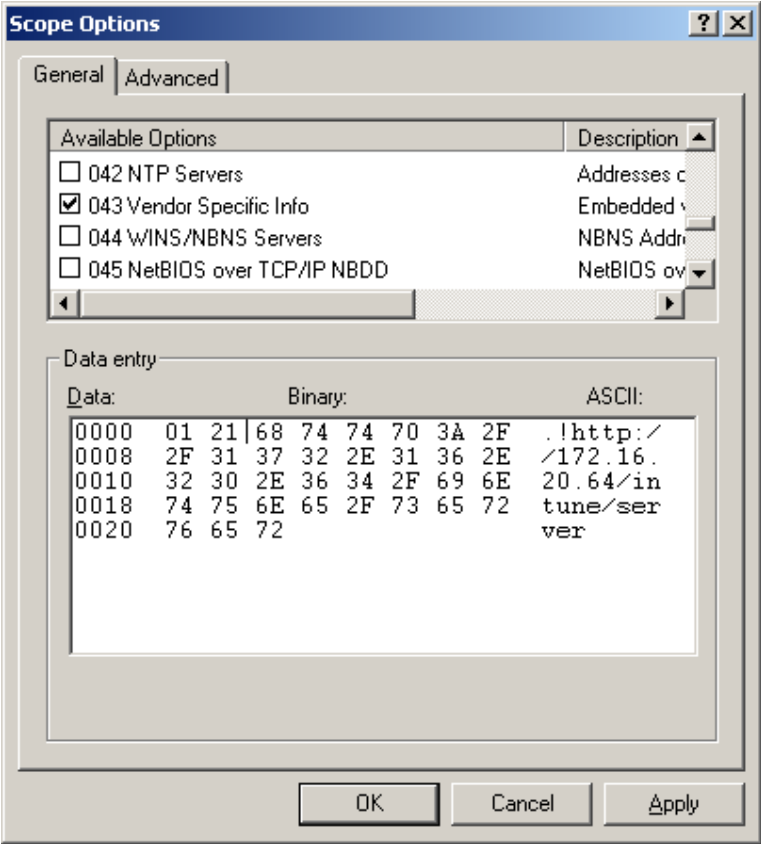


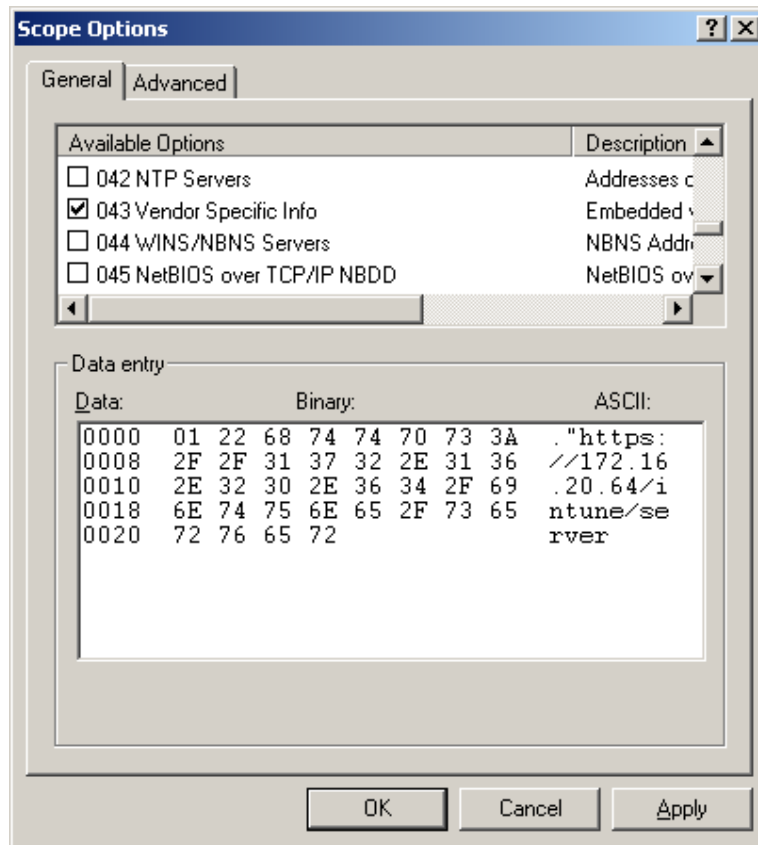
Figure 8. HTTP with an IP address



Installing FlexMaster

Ensuring That APs Can Connect to FlexMaster

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.

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

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

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

The screenshot displays the Ruckus FlexMaster web interface. The top navigation bar includes the Ruckus logo, the title 'FlexMaster', and a user menu with 'Log Out' and 'admin@ruckus.com'. Below the navigation bar are tabs for 'Summary', 'Details', and 'Diagnostics'. The main content area is titled 'Device View' and shows configuration details for a device named 'RuckusAP'. The 'Server URL' field is highlighted with a red box and contains the value 'https://192.168.24.33/intune/server'. Other visible fields include Device Name, Model Type, Customer ID, Serial Number, Firmware Version, Service Provider Login Name, Uptime, MAC Address, External IP Address, IPv6 Address, Periodic Inform Status, and Periodic Inform Interval.

Field	Value
Device Name	RuckusAP
Model Type	ZF7942
Customer ID	4855
Serial Number	921001013880
Firmware Version	0.0.0.99.260
Service Provider Login Name	super
Uptime	13m
MAC Address	04:4F:AA:2E:CD:D0
External IP Address	192.168.22.144
IPv6 Address	2222:3333:aaaa:2222:64f:aaff:fe2e:cdd0
Periodic Inform Status	Enabled
Periodic Inform Interval	1 minute
Device Last Seen	Jul 09 2012 15:31:07
Server URL	https://192.168.24.33/intune/server

Editing the Server Hosts File

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

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

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

3. Save the hosts file.



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

Installing the FlexMaster Software

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



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



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



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

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

```
# mkdir -p /mnt/cdrom
```
5. Type the following command to mount the CD-ROM manually to the created mount point:

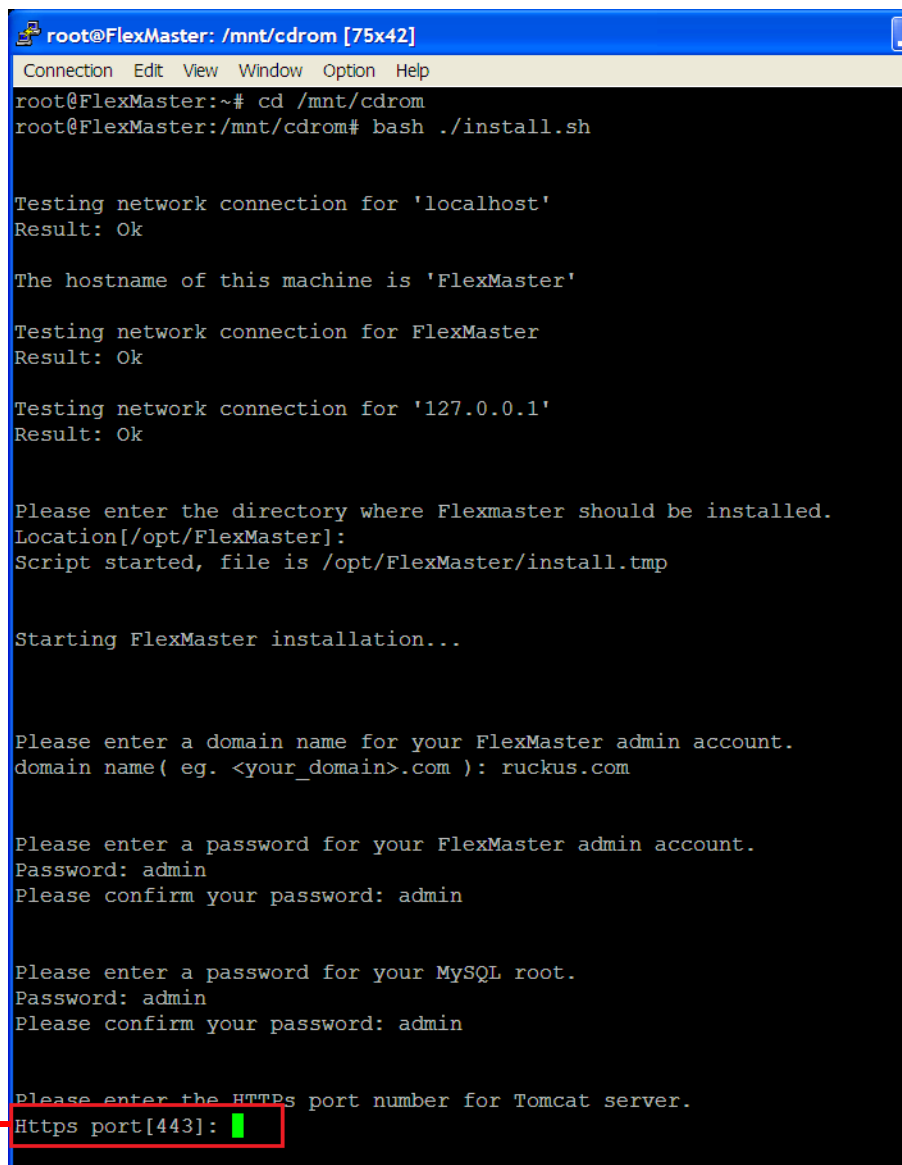
```
# mount /dev/cdrom /mnt/cdrom
```
6. Change directory (`cd`) to the mount point for the CD-ROM.
7. Execute the install script `install.sh`.

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

Installing FlexMaster

Installing the FlexMaster Software

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



```
root@FlexMaster: /mnt/cdrom [75x42]
Connection Edit View Window Option Help
root@FlexMaster:~# cd /mnt/cdrom
root@FlexMaster:/mnt/cdrom# bash ./install.sh

Testing network connection for 'localhost'
Result: Ok

The hostname of this machine is 'FlexMaster'

Testing network connection for FlexMaster
Result: Ok

Testing network connection for '127.0.0.1'
Result: Ok

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

Starting FlexMaster installation...

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

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

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

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

Tomcat Web
server HTTPS
port

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

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

9. The installation script performs some connection tests:

```
Testing network connection for 'localhost'  
Result: Ok
```

```
The hostname of this machine is 'localhost.localdomain'
```

```
Testing network connection for localhost.localdomain  
Result: Ok
```

```
Testing network connection for '127.0.0.1'  
Result: Ok
```

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

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

11. Enter your organization's domain name. By default, the domain name is appended to the word "admin", creating the default FlexMaster user account: *admin@domain.com*. The *admin@domain.com* user account is a Super User in the FlexMaster system and cannot be deleted. For more on roles, see [Understanding User Roles and Privileges](#).

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

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

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

13. Enter a password for the MySQL root account.

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

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

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

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

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

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

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

Installing FlexMaster

Installing the FlexMaster Software

Figure 12. Configuring the SMTP settings

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

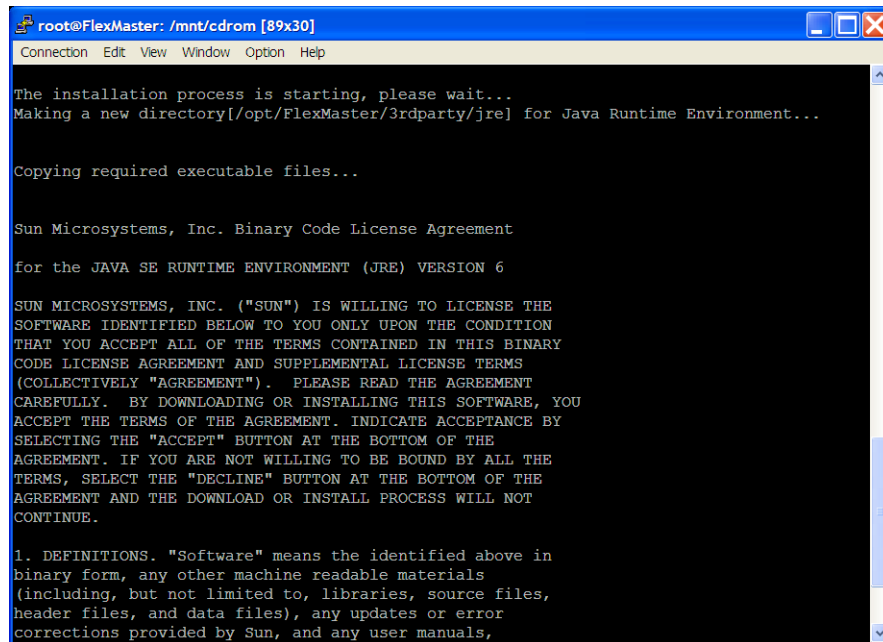
Please note that all devices that wish to register with Flexmaster will be automatically
approved.
You will have the option to change this setting from the Inventory-->Device Registration
menu after installation.

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

SMTP server
settings

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

Figure 13. Sun Microsystems license agreement within the installation script



```
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

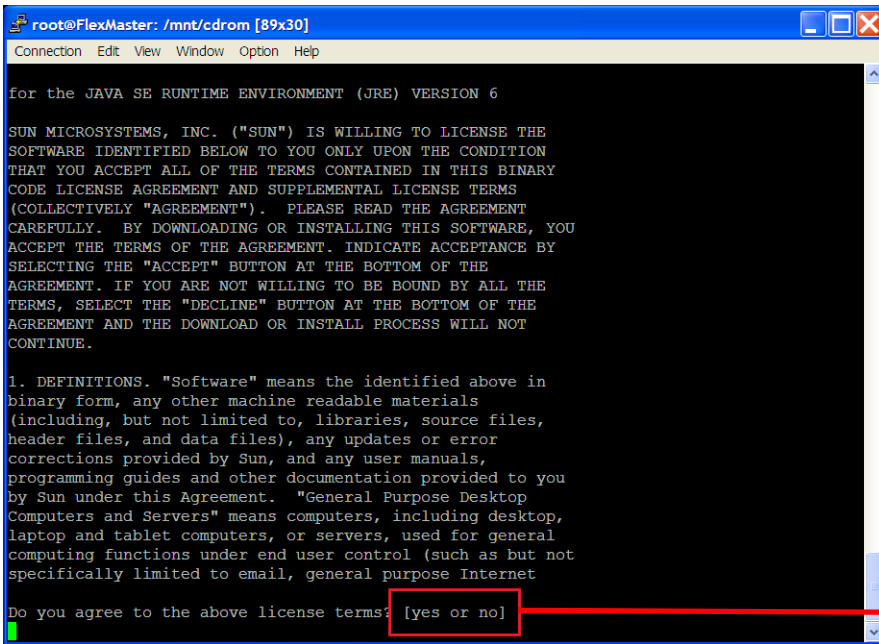
SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE
SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON THE CONDITION
THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY
CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS
(COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT
CAREFULLY. BY DOWNLOADING 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,
```

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

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


Figure 14. Accepting the Sun license agreement



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

for the JAVA SE RUNTIME ENVIRONMENT (JRE) VERSION 6

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

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

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

Type 'yes' to accept the
license agreement

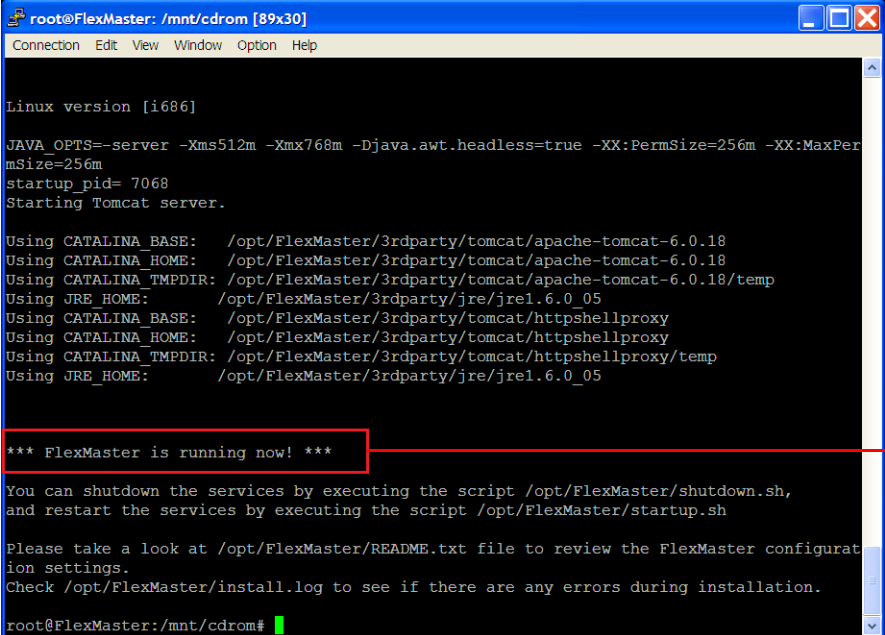
After you accept the license agreement, the installation script installs all required packages. When the installation completes, the following message appears:

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

Installing FlexMaster

Installing the FlexMaster Software

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:MaxPermSize=256m
startup_pid= 7068
Starting Tomcat server.

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

*** FlexMaster is running now! ***

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

Please take a look at /opt/FlexMaster/README.txt file to review the FlexMaster configuration 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.

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 are made available on the Ruckus Wireless support Web site or released through authorized channels. Update files typically use `{version number}.patch.tar` for their file naming convention (for example, `9.5.0.0.11.patch.tar`).



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

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

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

```
# mkdir -p /mnt/cdrom
```
5. Type the following command to mount the CD-ROM manually to the created mount point:

```
# mount /dev/cdrom /mnt/cdrom
```
6. Upload the patch file (for example, `9.5.0.0.11.patch.tar`) to the FlexMaster server.
7. Copy the patch file to the FlexMaster folder `/opt/FlexMaster/`:

```
# cp 9.5.0.0.11.patch.tar /opt/FlexMaster/
```
8. Untar the patch file with following command:

```
# tar -vxf 9.5.0.0.11.patch.tar
```
9. Make sure that the `{version number}.patch` file, such as `9.5.0.0.11.patch`, has been extracted from the tar file.
10. Upgrade FlexMaster with following command:

```
# ./upgrade.sh 9.5.0.0.11
```



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

Uninstalling FlexMaster

1. Execute the FlexMaster uninstall script.

```
# [root@flexmaster FlexMaster]# ./uninstall.sh
```
2. After you execute the uninstall script, it performs the following steps:
 - a. It shuts down the Tomcat server.
 - b. It shuts down the MySQL server.
 - c. It deletes the configuration files, and uninstalls the FlexMaster services.
 - d. It restores the original `/etc/my.cnf` file.
 - e. It finds `/etc/my.cnf.ruckus`, and then renames it to `/etc/my.cnf`.
 - f. Finally, it deletes the `/opt/FlexMaster` directory.

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

Backing Up the Database from the Command Line Interface

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

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

Follow these steps to back up the FlexMaster database.

1. On the Linux server, go to the FlexMaster root directory (`/opt/FlexMaster`).
2. Execute the database backup script. You can either specify the file path and file name of the backup file, or you can let FlexMaster automatically set the path.

- To back up the FlexMaster database to a specific file path and file name, enter the following command:

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

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

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

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

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

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

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

Restoring the Database from the Command Line Interface

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



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

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

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

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

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

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

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

What's Next?

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

Getting Started with FlexMaster

In This Chapter

Logging into FlexMaster	38
Features of the FlexMaster Web Interface	40
Getting Started Tasks	57

Logging into FlexMaster

Use one of the Web browsers described in [Web Browser Requirements](#) to access the FlexMaster Web interface:



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

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

http://<ipaddress> or https://<ipaddress>

--OR--

http://flexmaster or https://flexmaster

3. Press <ENTER> to initiate the connection.

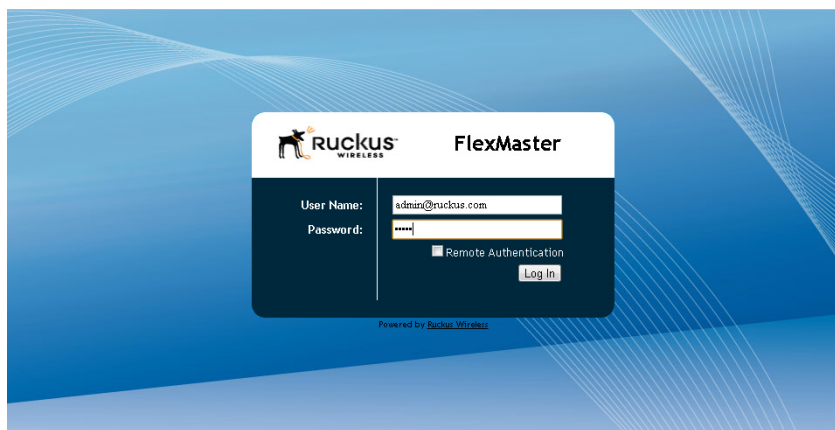
If you are using HTTPS, a security alert dialog box appears. Click **OK/Yes** to proceed.



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](#).

The *Ruckus Wireless Admin* login page appears.

Figure 16. The FlexMaster login page



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

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

Password: **admin**

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



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

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

For more on the Dashboard, 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 helps ensure that the FlexMaster Web interface shows all the changes and enhancements that were implemented in the new software version.

Features of the FlexMaster Web Interface

Figure 17 shows the FlexMaster web interface features, and the following table describes the elements available on the FlexMaster Web interface.

Figure 17. The FlexMaster Web interface has eight primary elements

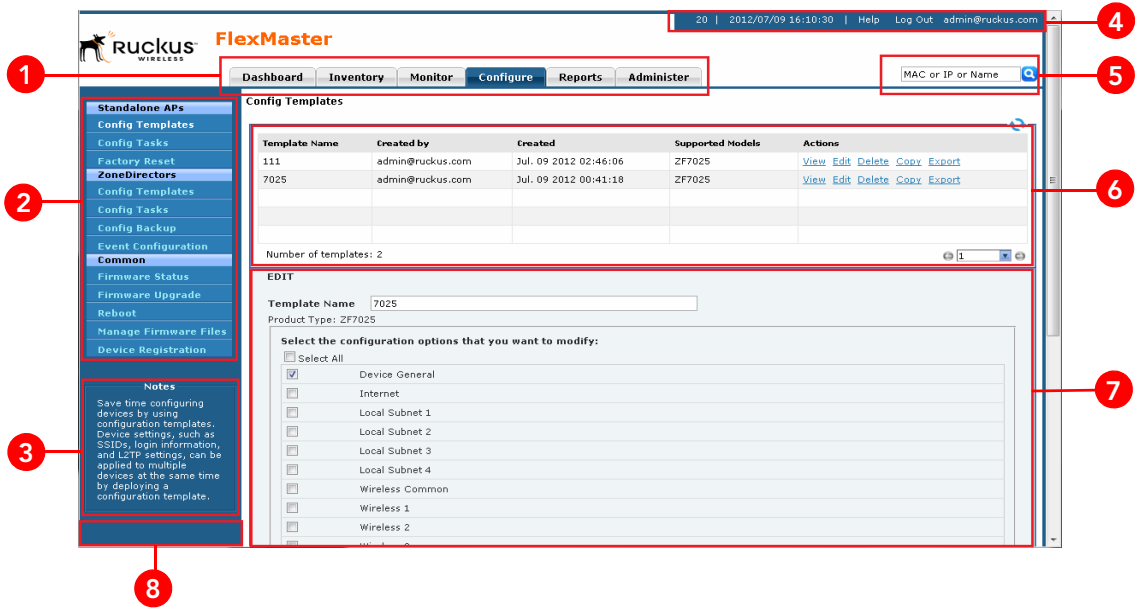


Table 5. FlexMaster Web interface features

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"> • Dashboard • Inventory • Monitor • Configure • Reports • Administer
2	Submenu	On each tab are second level menu items that, when clicked, display related options in the content area to the right.

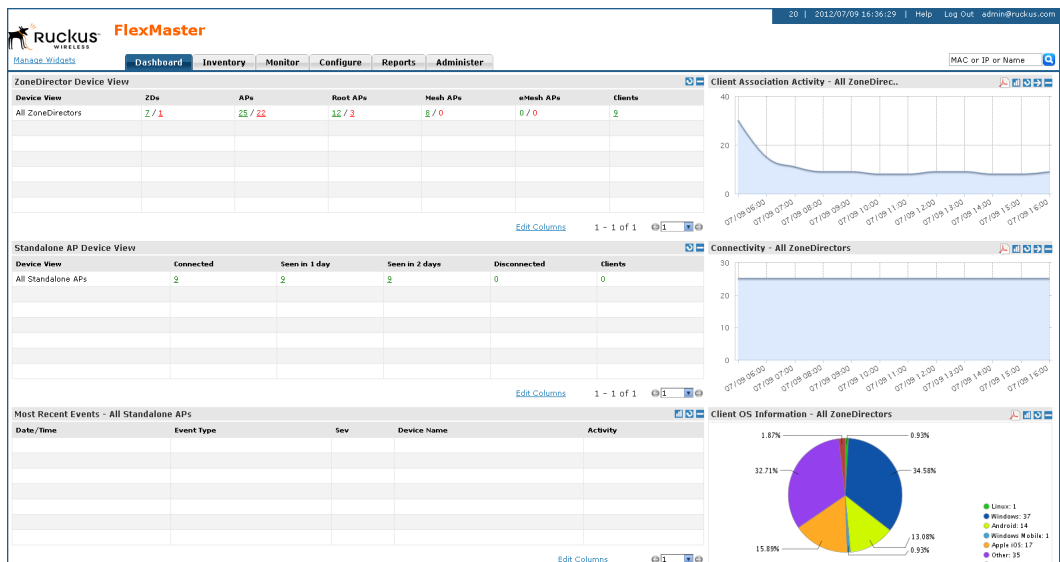
Table 5. FlexMaster Web interface features

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

Getting to Know the Dashboard and Its Widgets

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

Figure 18. The Dashboard




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

- [Widgets That You Can Display](#)
- [Available Widget Slots](#)
- [Default Widgets](#)
- [Adding a Widget](#)
- [Hiding a Widget](#)
- [Deleting a Widget](#)



NOTE: By default, FlexMaster uses the 3-tier management mode. This means that the Web interface displays data for FlexMaster, ZoneDirector, and APs. If you do not have 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 six standard widgets, which cannot be deleted (only minimized) from the Dashboard:

- [ZoneDirector Device View Widget](#)
- [Standalone AP Device View Widget](#)
- [Most Recent Events Widget](#)
- [Connectivity Widget](#)
- [Client Association Activity Widget](#)
- [Client OS Information Widget](#)

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

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

ZoneDirector Device View Widget

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

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



NOTE: 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 appears as "0" (zero) on the ZoneDirector Device View widget.

Table 6. Columns on the ZoneDirector Device View Widget

Column Name	Description
Device View	Shows the name of the ZoneDirector device view. By default, a group called <i>All ZoneDirectors</i> exists, which contains all ZoneDirector devices detected on the network.

Table 6. Columns on the ZoneDirector Device View Widget

Column Name	Description
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"> The number in green (before the slash symbol) indicates the number of ZoneDirector devices that are currently online. The number in red (after the slash symbol) indicates the number of ZoneDirector devices that are currently offline or disconnected from FlexMaster. <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) takes you to the Inventory > Reports 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"> The number in green (before the slash symbol) indicates the number of APs that are currently online. The number in red (after the slash symbol) indicates the number of APs devices that are currently offline or disconnected from ZoneDirector. <p>The sum of these two numbers is equal to the total number of APs that are registered with ZoneDirector. Clicking either number (hyperlink) takes you to the Inventory > Reports page, which shows details of all these connected or disconnected APs.</p> <p>NOTE: 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 Additional AP Columns When Mesh Networking Is Enabled for more information.</p>
Clients	<p>Shows the number of clients that are associated with the currently connected APs. Clicking this number (hyperlink) takes you to the Inventory > Reports page, which shows details of all these associated clients and the APs with which they are associated.</p>

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

ZoneDirector Device View						
Device View	ZDs	APs	Root APs	Mesh APs	eMesh APs	Clients
All ZoneDirectors	2 / 1	28 / 24	18 / 4	2 / 0	0 / 0	8
ruckus-access	1 / 0	8 / 2	2 / 1	1 / 0	0 / 0	2

[Edit Columns](#) 1 - 2 of 2

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

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

Standalone AP Device View Widget

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



NOTE: For more on creating device views, see [Creating a Standalone AP View](#).



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

Table 7. Columns on the Standalone AP Device View widget

Column Name	Description
Device View	Shows the name of the AP device view. A default device view named <i>All Standalone APs</i> exists.
Connected	Shows the number of APs that are currently connected to FlexMaster. Clicking this number (hyperlink) takes you to the Inventory > Reports 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 Inventory > Reports 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 Inventory > Reports for a view of the devices that reported in within during the last 48 hours.
Disconnected	Shows the number of APs that are reporting to FlexMaster, but are currently disconnected. Clicking this number (hyperlink) takes you to the Inventory > Reports page, which shows details of all these disconnected APs.
Clients	Shows the number of clients that are associated with the currently connected APs. Clicking this number (hyperlink) takes you to the Inventory > Reports 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 20. The Standalone AP Device View widget

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

[Edit Columns](#) 1 - 1 of 1

Most Recent Events Widget

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

Table 8. Columns on the Most Recent Events widget

Column Name	Description
Severity	<p>Indicates the importance of an events. There are three event severity levels in FlexMaster:</p> <ul style="list-style-type: none"> <i>Error</i> (high importance): These are events that you should check. For example, if you see <code>Rogue 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. <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. <i>Info</i> (low importance): These are informational events that typically do not require your attention (for example, <code>Device rebooted</code>).
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 Inventory > Reports view of the devices reporting the specific event.
Device Events	Displays the number of events generated by all Standalone APs.

Table 8. Columns on the Most Recent Events widget


Column Name	Description
ZDs	Displays the total number of ZoneDirector devices that have reported the event. Click this link to go to an Inventory > Reports view of the devices reporting the specific event.
ZD Events	Displays the total number of events generated by all ZoneDirector units.

Figure 21. Columns on the Most Recent Events widget

Date/Time	Event Type	Sev	Device Name	Activity

Connectivity Widget

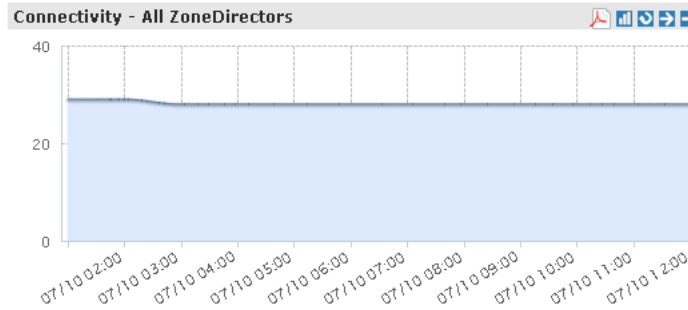
The Connectivity widget displays (in a bar graph format) the number of connectivity or loss-of-connectivity events on devices. The default Connectivity widget displays connectivity information for the All ZoneDirectors device view.

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 takes you to the Historical Connectivity page on the *Reports* tab, where you can view detailed connectivity information for the selected device view.




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

Figure 22. The Connectivity widget for the All ZoneDirectors device view



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


Follow these steps to customize the Connectivity widget.

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

You have completed customizing the widget.

Client Association Activity Widget

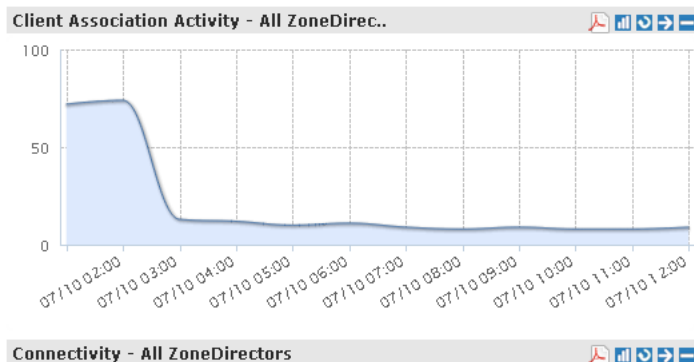
The Client Association Activity widget shows the number of clients that have associated with managed APs. The default Client Association Activity widget displays connectivity information for the All ZoneDirectors device view and on all radios on the managed APs.

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 takes you to the Client Association page on the *Reports* tab, where you can view detailed client association information for the selected device view.



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

Figure 23. The Client Association Activity widget for the All ZoneDirectors device view



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

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

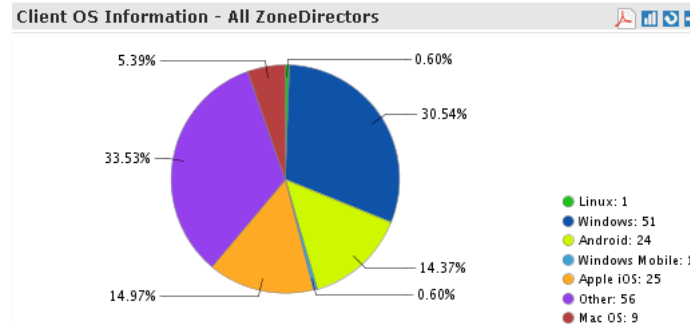
You have completed customizing the widget.


Client OS Information Widget

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

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

Figure 24. The Client OS Information widget for All ZoneDirectors



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

You have completed customizing the widget.

Customized Widgets

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

- [Capacity Widget](#)
- [SLA Widget](#)
- [Troubleshooting Widget](#)



NOTE: For instructions on how to add these widgets, refer to [Adding a Widget](#).

Capacity Widget

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

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

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

SLA Widget

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

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

Information	Device
AP Downtime	ZoneDirector/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 may be helpful in resolving connectivity issues on the network. Refer to the following table for the types of information that you can show on the Troubleshooting widget.

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

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

Available Widget Slots

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

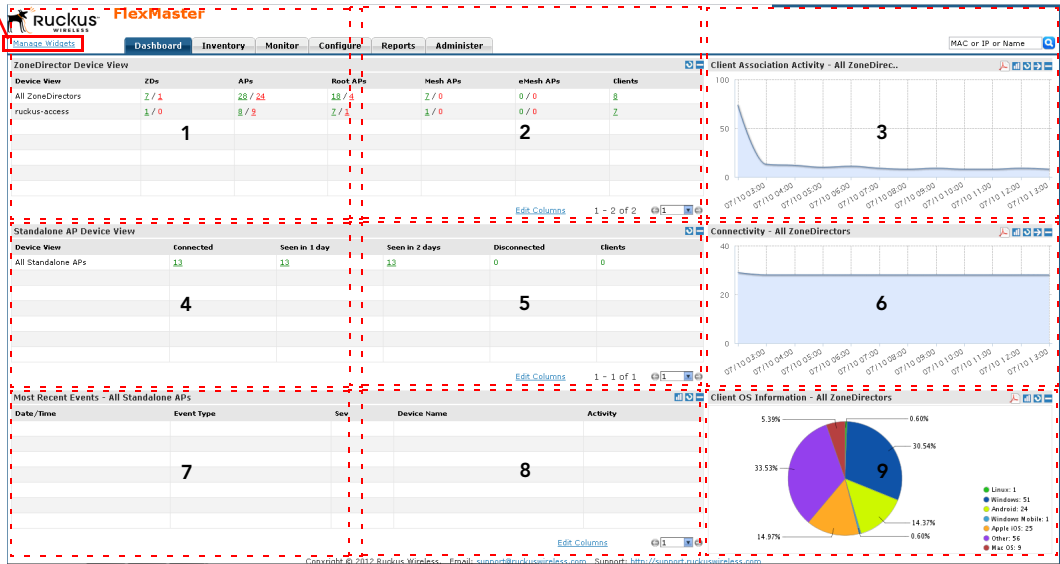
Note that some widgets are wider (for example, the ZoneDirector Device View widget) and require two widget slots. Make sure there are enough empty slots on the Dashboard before you add a widget.

Getting Started with FlexMaster

Getting to Know the Dashboard and Its Widgets

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
- Standalone AP Device View
- Most Recent 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.

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.



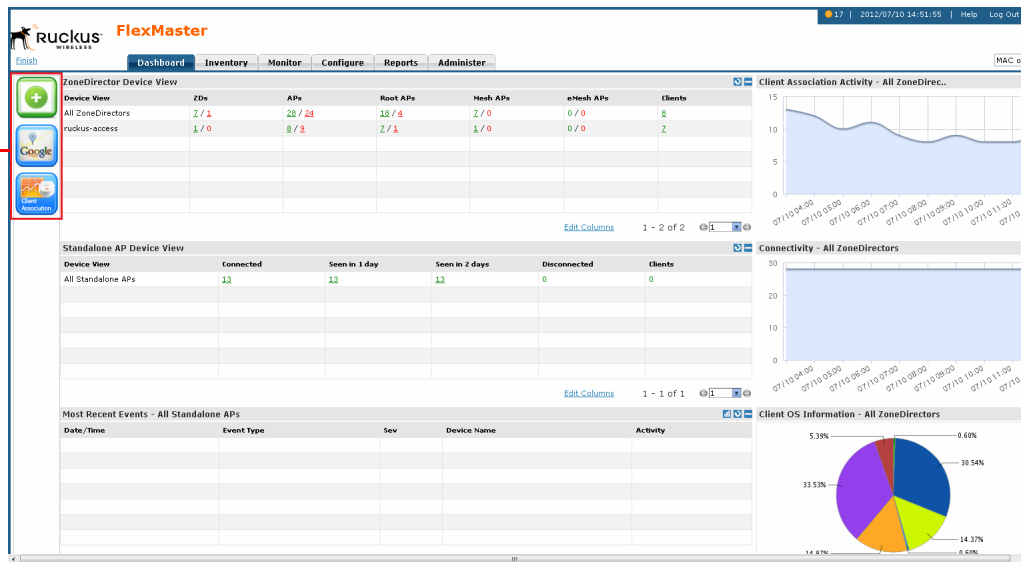
NOTE: If you are unable to place a widget in a slot, verify that the slot is empty. Also, some widgets (for example, the ZoneDirector Device View widget) are wider and require more than one slot. Make sure that there are enough slots for the widget that you are adding.

Getting Started with FlexMaster

Getting to Know the Dashboard and Its Widgets


Figure 26. A mini sidebar appears on the left side

Mini sidebar that displays widgets 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](#).

- 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.

- 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 Work with TACACS+](#)
- [Configuring Your Devices to Communicate with FlexMaster over L2TP](#)

Changing the Default Password

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

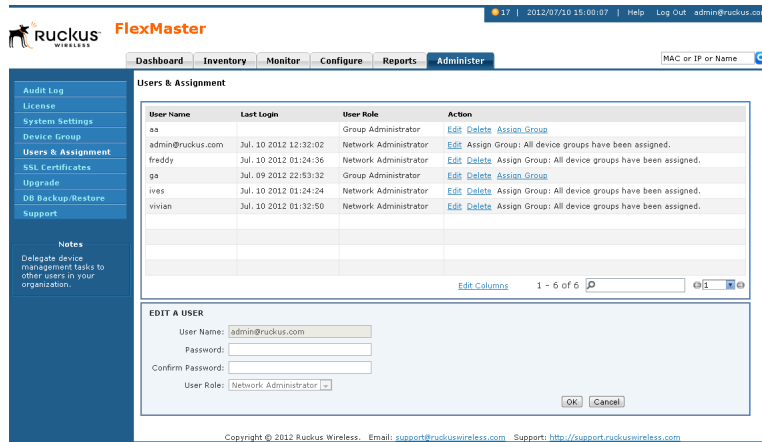
1. After logging in to the FlexMaster Web interface, go to **Administer > Users & Assignments**.
2. In the *Users* table, look for the admin user account that you used to log in to the FlexMaster Web interface.
3. Click the **Edit** link (in the *Action* column) that is in the same row as the user account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



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

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

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 is available over the Internet.

Take note of the following:

- ZoneFlex APs shipped with this version are preconfigured with the URL of your FlexMaster server (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

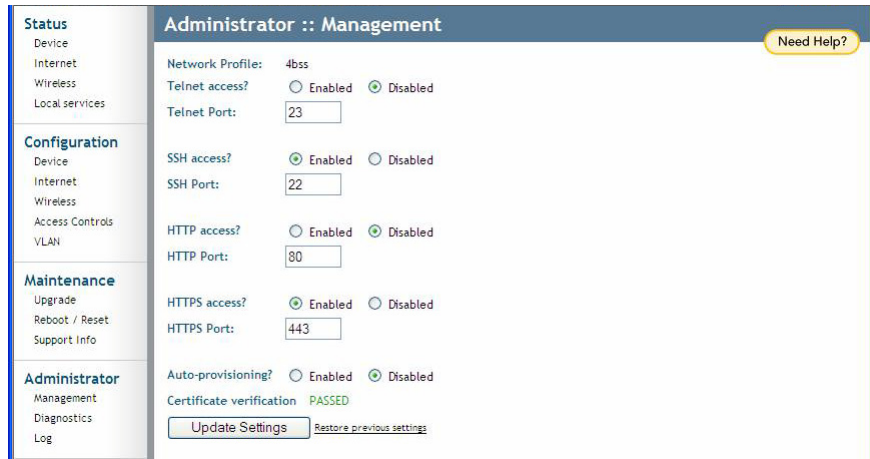
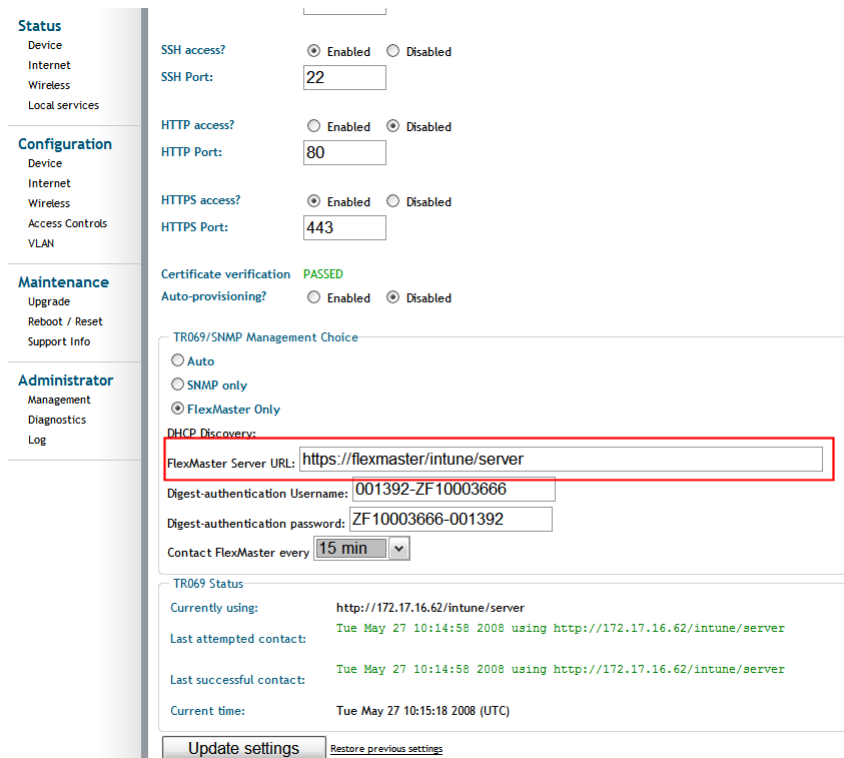


Figure 29. The ZF2942 Administrator > Management page after upgrading to 6.0



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

1. Log in to your Ruckus Wireless AP's Web interface.
2. Go to **Administrator > Management**. See [Figure 29](#).
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 are also managing ZoneDirector using FlexMaster, then note that the number of license seats that ZoneDirector consumes depends on the maximum number of APs that it can support. ZoneDirector 3250 (which supports up to 250 clients), for example, consumes 250 license seats.



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

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

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

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

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

Figure 30. The Administer > License page

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 'License' and displays the following information:

- Total Licenses Purchased: 100100100
- Remaining Licenses: 100099924
- Licenses Consumed by Standalone APs: 14
- Licenses Consumed by ZoneDirectors: 1162

Below this summary is a table with the following columns: License Key, Part Number, AP Count, and Creation Date.

License Key	Part Number	AP Count	Creation Date
1193034973785	FME-100	100	Oct. 21 2007 23:36:13
1270080959000	ruckuswireless	100000000	Mar. 31 2010 17:15:59
1196089018000	ABC	100000	Nov. 26 2007 06:56:58

At the bottom of the license table, there is a link: [Upload a license file](#). The footer of the page contains the copyright information: Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com. Support: <http://support.ruckuswireless.com>.

Configuring Your Devices to Work with TACACS+

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

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



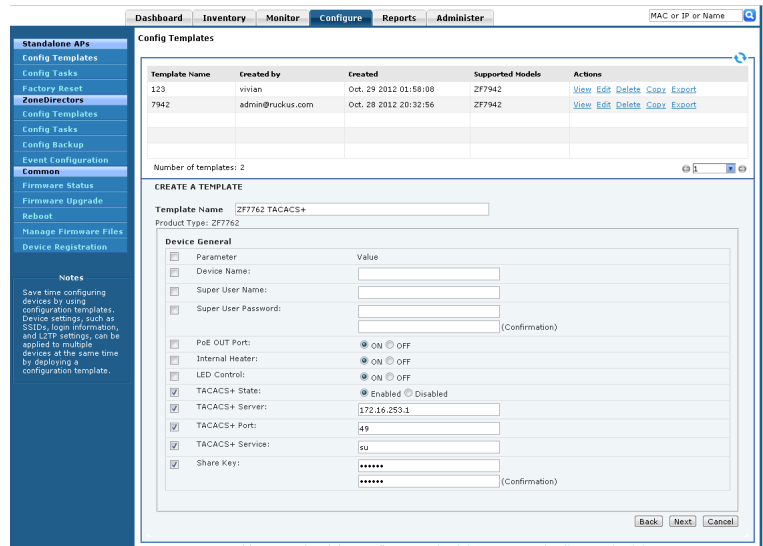
NOTE: If the Ruckus Wireless ZD is behind a firewall/NAT device, then port 49 (TACACS+ port) may need to be forwarded through the firewall/NAT device for FM to communicate with the ZD and AP devices. For more information, refer to [Firewall Ports that Must be Open for Communications](#).

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

Creating the TACACS+ Configuration Template

1. Go to **Configure > Config Templates**.
2. Click **Create a template**. The “Create a Template” configuration form opens at the bottom of the page.
3. In **Template Name**, type a name for this TACACS+-specific template. For example, if you are creating a TACACS+ configuration template for ZoneFlex 7762, you can type **ZF7762 TACACS**.
4. In **Select Product Type**, select the product model for which you are creating an L2TP configuration template (**ZF7762**).
5. Under **Select the configuration options that you want to modify**, select the **Device General** check box.
6. Click **Next**. The Device General page appears.
7. Click the **Enabled TACACS+ State** button. FlexMaster displays the remaining TACACS+ parameters.
8. Enter the TACACS+ parameters:
 - TACACS+ Server - IPv4 or IPv6 server address.
 - TACACS+ Port - 49 is the default, but it can be set to any available TCP port.
 - TACACS+ Service - Login.
 - Share Key - TACACS+ Password.

Figure 31. Required TACACS+ settings

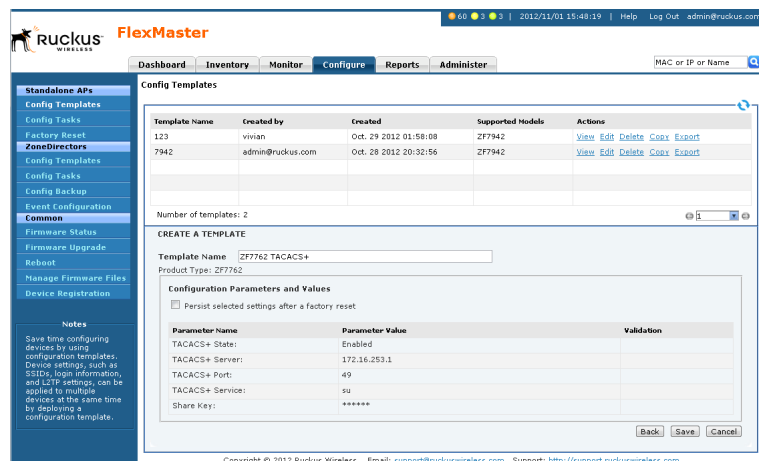


9. Click **Next**.

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

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

Figure 32. Verify that the TACACS+ settings are correct



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

Continue with [Creating the TACACS+ Configuration Task](#).

Creating the TACACS+ Configuration Task

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

Figure 33. Creating the TACACS+ configuration task

The screenshot shows the 'CREATE A TASK' form in FlexMaster. On the left is a navigation sidebar with options like 'Event Configuration', 'Common', 'Firmware Status', 'Firmware Upgrade', 'Reboot', 'Manage Firmware Files', and 'Device Registration'. The main form area is titled 'CREATE A TASK' and contains the following sections:

- Task Settings:** A text field for 'Specify a task name:' containing 'ZF7762 TACACS+'. Below it is a dropdown for 'Select a configuration template:' set to 'ZF7762 TACACS+ (ZF7762)', with a 'View Parameters' link.
- Select the devices to be provisioned:** Includes tabs for 'Select View' and 'Advanced Settings'. A dropdown for 'Select a view of devices to perform configuration update:' is set to 'All Standalone APs', with a 'View Details' link.
- Device List:** A table with columns: Device Name, Serial #, MAC Address, IP Address, IPv6 Address, and External IP Address. The table lists several Ruckus devices including APs and WBs.
- Specify time for this task:** Radio buttons for 'Perform this task now' (selected) and 'Schedule this task for later:'. A 'Date:' field is present.
- Buttons for 'Save' and 'Cancel' at the bottom right.

3. In *Specify a task name*, type a name for this TACACS+-specific configuration task. For example, if this TACACS+ configuration task is for ZoneFlex 7762 APs, you can type **7762 TACACS+**.
4. Toggle the *Select the Configuration Template* drop-down list to select the previously configured TACACS+ configuration template.
5. (Optional) Under the *Select View* tab, toggle the *Select a view of devices to perform configuration update* drop-down list to filter the list of devices based on a device view. For example, if the configuration template is for ZoneFlex 7762, select the device view that contains ZF7762 models.
6. Under *Specify time for the task*, click when you want to perform this task:
 - Perform this task now
 - Schedule this task for later: Specify the desired Date and Time
7. Click **Save**.

Configuring Your Devices to Communicate with FlexMaster over L2TP

If your network prevents FlexMaster from initiating communication across the Internet to managed devices, 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 task to push the update with the L2TP settings to your managed devices. When the devices next “call home”, they receive this update and register with the LNS. This allows FlexMaster to initiate future connections.



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

Creating the L2TP Configuration Template

1. Go to **Configure > Config Templates**.
2. Click **Create a template**. The “Create a Template” configuration form opens at the bottom of the page.
3. In **Template Name**, type a name for this L2TP-specific template. For example, if you are creating an L2TP configuration template for ZoneFlex 2925, you can type **L2TP for 2925**.
4. In **Select Product Type**, select the product model for which you are creating an L2TP configuration template.
5. Under **Select the configuration options you would like to modify**, select the **Internet** and **VLAN & LAN Port Setting** check boxes.



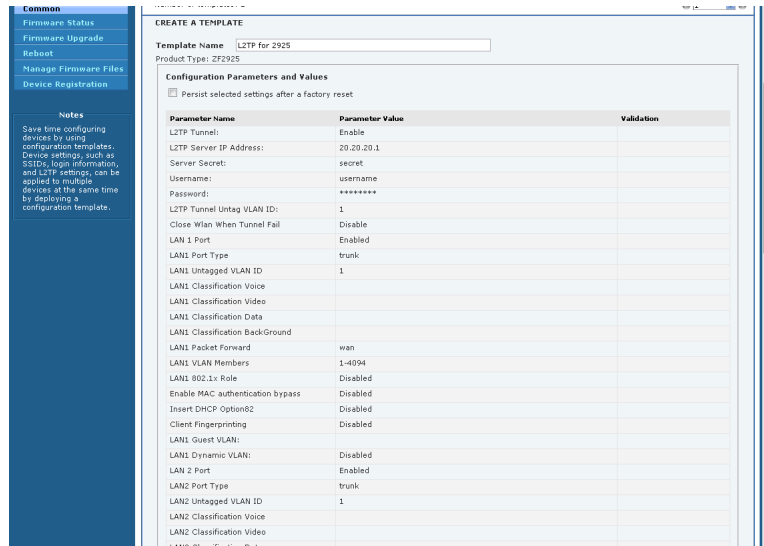
NOTE: You must select both the Internet and VLAN Setting check boxes to create an L2TP configuration template successfully. If you only select the Internet check box, you are able to create the configuration template, but it is not applied.

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

The following LNS values are required:

- L2TP Server IP Address
- Server Secret
- L2TP Username

Figure 35. Verify that the L2TP settings are correct



12. On the *Configuration Parameters and Values* page, click **Save** to save the template. Continue with [Creating the L2TP Configuration Task](#).

Creating the L2TP Configuration Task

1. Go to **Configure > Config Tasks**.
2. Click **Create a task**. The CREATE A TASK form appears at the bottom of the page.
3. In *Specify a task name*, type a name for this L2TP-specific configuration task. For example, if this L2TP configuration task is for ZoneFlex 2925 APs, you can type **L2TP Upgrade for 2925**.
4. Toggle the *Select the Configuration Template* drop-down list to select the previously configured L2TP configuration template.
5. (Optional) Under the *Select View* tab, toggle the *Select a view of devices to perform configuration update* drop-down list to filter the list of devices based on a device view. For example, if the configuration template is for ZoneFlex 2925, select the device view that contains ZF2925 models.
6. Under *Specify time for the task*, click when you want to perform this task:
 - Perform this task now
 - Schedule this task for later: Specify the desired Date and Time
7. Click **Save**.

Figure 36. Creating the L2TP configuration task

CREATE A TASK

Task Settings

Specify a task name:

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

Select the devices to be provisioned

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

Device Name	Serial #	MAC Address	IP Address	External IP Address	Model	Connection	Uptime	Software	Tag
RuckusAP	001002000010	40:44:00:00:00:80	192.168.22.136:443	192.168.22.136:443	UNKNOWN	✓	17h 26m	9.5.0.0.5	
7025	121102000243	C4:10:8A:0C:5C:A0	192.168.22.55:443		ZF7025	✓	1d 15h 21m	9.5.0.0.5	
RuckusAP	131204010729	C0:8A:DE:03:2D:A0	192.168.22.142:443	192.168.22.142:443	ZF7762	✓	14h 1m	9.1.2.0.8	
RuckusAP	131204010760	C0:8A:DE:03:2F:90	192.168.22.141:443	192.168.22.141:443	ZF7762	✓	1d 13h 52m	9.1.2.0.8	
RuckusAP	131204010763	C0:8A:DE:03:2F:A0	192.168.22.143:443	192.168.22.143:443	ZF7762	✓	14h 4m	9.1.2.0.8	
ZF7363	161203002768	58:93:96:2D:2C:D0	192.168.22.123:443	192.168.22.123:443	ZF7363	✓	5d 18h 34m	0.0.0.99.279	
RuckusAP	161205001949	C0:8A:DE:1D:82:F0	192.168.22.147:443	192.168.22.147:443	ZF7321	✓	15h 14m	9.4.0.0.103	
RuckusAP	280901001853	00:25:C4:19:FF:20	192.168.22.140:443	192.168.22.140:443	ZF7942	✓	1d 13h 46m	9.5.0.0.5	
7025	381102000054	C4:10:8A:10:15:40	192.168.22.111:443	192.168.22.111:443	ZF7025	✓	1d 12h 37m	9.5.0.0.5	
RuckusWB	501055004323	74:91:1A:10:88:80	192.168.20.60:443	192.168.20.60:443	ZF7731	✓	15d 14h 15m	9.2.0.0.156	

Number of devices: 14

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

Specify time for this task :

Perform this task now

Schedule this task for later:

Date:

Working with Device Inventory

In This Chapter

About the Inventory Page	70
Working with ZoneDirector Inventory	87
Working with Standalone APs Inventory	101
Working with Client Inventory	113

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

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

ZoneDirector Inventory Pages

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

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

Field/Column	Description
ZD Search Criteria section	Use these filters to search for specific ZoneDirector devices. You can save the search results as a new ZoneDirector view. See Searching for ZoneDirector Devices .
Text View/Map View	By default, the page displays a Text View 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 Map View . See Text View and Map View .
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 appear in this table. For information on the columns that appear in this table, refer to the following table.
Export As XLS File or CSV File	If you want to save the devices that currently appear in the table to an XLS file, click the XLS File button. To save them to a CSV file, click the CSV File 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 Search Using the ZD Search Criteria .

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



NOTE: By default, ZoneDirector only displays a few of the available columns on the ZoneDirector Inventory page. If you want to display additional columns, refer to [Displaying and Hiding Columns on the ZoneDirector Inventory Page](#) for information.

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

Column	Description
ZD Name	Name assigned to the device
Serial Number	Serial number of the device. Clicking this link opens a new browser window specific to the device. This is the device view as if you logged into the device's Web interface. NOTE: Use the opened ZoneDirector web interface to configure features such as Hotspot 2.0. Refer to the <i>Ruckus Wireless ZoneDirector User Guide</i> to create a Hotspot 2.0 service on a ZoneDirector.
MAC Address	MAC address of the device
External IP	IP address assigned to the device NOTE: <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> <ul style="list-style-type: none"> If :443 appears after the port number, you can access the device's Web interface using <code>https://{device-IP-address}</code>. If :80 appears after the IP address, you can access the device's Web interface using <code>http://{device-IP-address}</code>. <p>If both HTTPS and HTTP management options are enabled, only :443 appears 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
Location	Location of the device (if provided)
Connection	Indicates whether the device is currently online (✔) or offline (✘).

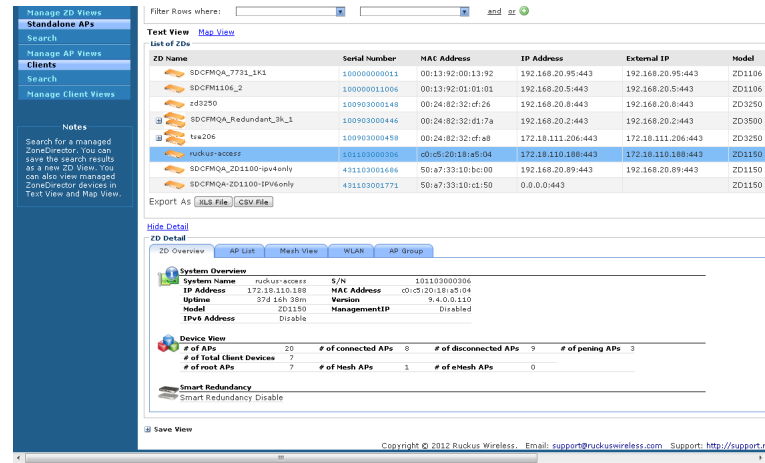
Table 13. Columns that appear in the List of ZDs table

Column	Description
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"> • Active: This device is part of a Smart Redundancy deployment and is currently the active ZoneDirector device. • Standby: This device is part of a Smart Redundancy deployment and is currently the backup ZoneDirector device. • Standalone: This device is not part of a Smart Redundancy deployment. <p>NOTE: When Smart Redundancy is enabled, the Smart Redundant pair of ZDs consume one extra ZoneDirector license. Refer to Checking Your FlexMaster License for more information on ZD licenses.</p>
Tag	<p>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.</p>
Software	Shows the software version that is installed on the device
Actions	<p>Displays actions you can take on the device, including:</p> <ul style="list-style-type: none"> • Edit: Allows you change the tag name assigned to the device, as well as its location, GPS coordinates, and Web port mapping. • View More ZD Info: Clicking this link displays the ZD detail table below the List of ZDs table. See Viewing the ZD Detail Section.

Viewing the ZD Detail Section

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

Figure 37. The ZD Detail section



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

Table 14. Information that appears in the ZD Detail table

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

Displaying and Hiding Columns on the ZoneDirector Inventory Page

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

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

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

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

The screenshot shows the FlexMaster interface with the 'Inventory' tab selected. A table lists ZoneDirector devices with columns for ZD Name, Serial Number, MAC Address, IP Address, and External IP. A 'Text View' pop-up window is open, showing a list of columns with checkboxes to toggle their visibility. The 'Model' checkbox is checked, while others like 'Last Seen', 'Location', 'Latitude', 'Longitude', 'Uptime', 'Connection', 'Redundancy State', 'Tag', 'Software', and 'Actions' are unchecked.

ZD Name	Serial Number	MAC Address	IP Address	External IP
SDCFMQA_7731_1K1	100000000011	00:13:92:00:13:92	192.168.20.95:443	192.168.20.95:443
SDCFM1106_2	100000011006	00:13:92:01:01:01	192.168.20.5:443	192.168.20.5:443
r43290	100903000148	00:24:82:32:cf:26	192.168.20.8:443	192.168.20.8:443
SDCFMQA_Redundant_3k_1	100903000446	00:24:82:32:d1:7a	192.168.20.2:443	192.168.20.2:443
tr4204	100903000458	00:24:82:32:cf:a8	172.18.111.206:443	172.18.111.206:443
nvd-kvr-access	101103000306	00:c5:20:18:a5:04	172.18.110.188:443	172.18.110.188:443
SDCFMQA_ZD1100-IPv6only	431103001686	50:a7:33:10:bc:00	192.168.20.89:443	192.168.20.89:443
SDCFMQA-ZD1100-IPv6only	431103001771	50:a7:33:10:c1:50	0.0.0.0:443	

Standalone APs Inventory Pages

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

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

Field/Column	Description
AP Search Criteria	Use these filters to search for specific standalone APs. You can save the search results as a new AP view. See Searching for Standalone APs .
Text View/Map View	By default, the page displays a Text View 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 Map View . See Text View and Map View .
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 appear in this table. For information on the columns that appear in this table, refer to the following table.
Export as XLS File or CSV File	If you want to save the devices that currently appear in the table to an XLS file, click the XLS File button. To save them to a CSV file, click the CSV File 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 Search Using the AP Search Criteria .

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

Column	Description
AP Name	Name assigned to the device
Serial Number	Serial number of the device. Clicking this link opens a new browser window specific to the device. This is the device view as if you logged into the device's Web interface.

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

Column	Description
IP Address	<p>IP address assigned to the device</p> <p>NOTE: 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"> If :443 appears after the port number, you can access the device's Web interface using <code>https://{device-IP-address}</code>. If :80 appears after the IP address, you can access the device's Web interface using <code>http://{device-IP-address}</code>. <p>If both HTTPS and HTTP management options are enabled, only :443 appears after the IP address.</p>
External IP	<p>If the device is behind a NAT server, this is the IP address and port number that FlexMaster uses to communicate with the device.</p> <p>NOTES:</p> <ul style="list-style-type: none"> If the device is not behind a NAT server, the values for IP Address (above) and External IP Address are the same. 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 Edit link on this page that is in the same row as the device name, and then enter the port number that you assigned to the device on the NAT server.
IPv6	<p>If the network supports IPv6, this is the IPv6 address that is assigned to the AP.</p>
Model	<p>Model of the managed Ruckus Wireless device</p>
Last Seen	<p>Date and time when FlexMaster last communicated with the device</p>
Location	<p>If configured, this column shows the location of the device.</p>
Uptime	<p>Shows how long since the device was last rebooted</p>
Connection	<p>Indicates whether the device is currently online (🟢) or offline (🔴).</p>
Tag	<p>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.</p>

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

Column	Description
Software	Shows the software version that is installed on the device
Actions	Clicking Edit allows you change the tag name assigned to the device, as well as its location, GPS coordinates, and Web port mapping.

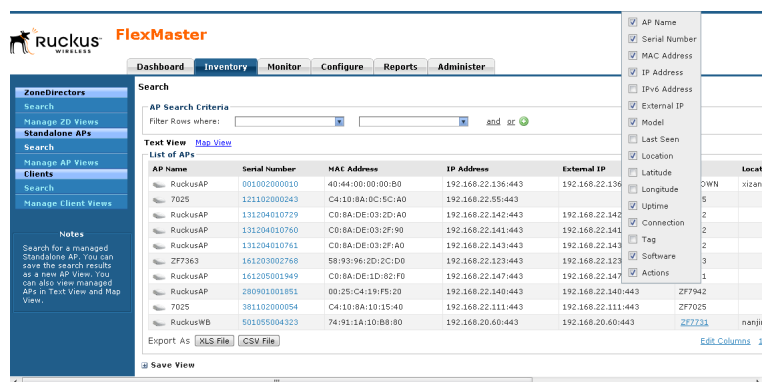
Displaying and Hiding Columns on the Standalone AP Inventory Page

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

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

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

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



Client Inventory Pages

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

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

Field/Column	Description
Clients Search Criteria section	Use these filters to search for specific clients. You can save the search results as a new client view. See Searching for Clients .
Text View/Map View	By default, the page displays a Text View 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 Map View . See Text View and Map View .

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

Field/Column	Description
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 appear in this table. For information on the columns that appear in this table, refer to the following table.
Export as XLS File or CSV File	If you want to save the devices that currently appear in the table to an XLS file, click the XLS File button. To save them to a CSV file, click the CSV File 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 Search Using the Client Search Criteria .

Table 18. 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
Connection	Indicates whether the client is currently online (☑) or offline (☒).

Displaying and Hiding Columns on the Client Inventory Page

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

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

You have completed hiding columns from the Client Inventory page.

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

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

The screenshot shows the Ruckus FlexMaster interface. The main table displays client information with columns: ZD Name, AP Name, Client MAC, Client IP Address, WLAN, Device Info, Host Name, and Radio Type. A 'List of Clients' dialog box is open, showing a search criteria section and a table of clients. On the right side of the dialog, there is a 'Columns' section with a list of columns and their corresponding checkboxes for visibility. The 'Client IPv6 Address' checkbox is unchecked, while others are checked.

ZD Name	AP Name	Client MAC	Client IP Address	WLAN	Device Info	Host Name	Radio Type
ruckus-access	RuckusAP	00:13:e8:38:0f:fb	172.18.111.63	ruckus-access	BoboMeow		802.11a/n
ruckus-access	SDC-ZF7962	00:16:eaf5:8c:e8	172.18.111.74	ruckus-access	QAAuto-Jacky		802.11a/n
tse206	7762-lab	00:16:65:76:e0:4a		ro-wlan			802.11a
ruckus-access	SDC-ZF7962	00:1e:e5:e1:38:02	172.18.110.254	fortest	DELL-PC		802.11g/n
tse206	7025-cubic	00:22:68:a7:22:bf	172.18.110.147	wlan-hotspot	tues		802.11b/g
ruckus-access	SDC-ZF7962	00:22:fb:4e:9f:22	172.18.110.203	ruckus-access	SDC-LISA		802.11g/n
ruckus-access	SDC-ZF7962	00:22:fb:5d:5e:3e	172.18.110.199	video54.local			802.11a/n
ruckus-access	SDC-ZF7962	00:22:fb:ad:03:a6	172.18.111.90	ruckus-access	sdc-szhou		802.11a/n
ruckus-access	RuckusAP	00:22:fb:ad:12:52	172.18.110.106	ruckus-access	Ann-PC		802.11a/n
ruckus-access	SDC-ZF7962	00:22:fb:ad:30:1e	172.18.111.91	ruckus-access	ruckus-7d5f882		802.11a/n

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

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




NOTE: The GPS coordinates of standalone APs can be set either from their native Web interface or from the FlexMaster Web interface. The GPS coordinates of ZoneDirector devices, on the other hand, can only be configured from the FlexMaster Web interface. GPS coordinates cannot be assigned to clients. To set the coordinates of a standalone AP or ZoneDirector from the FlexMaster Web interface, search for the device on the Inventory page, and then click the **Edit** link 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**.

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

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

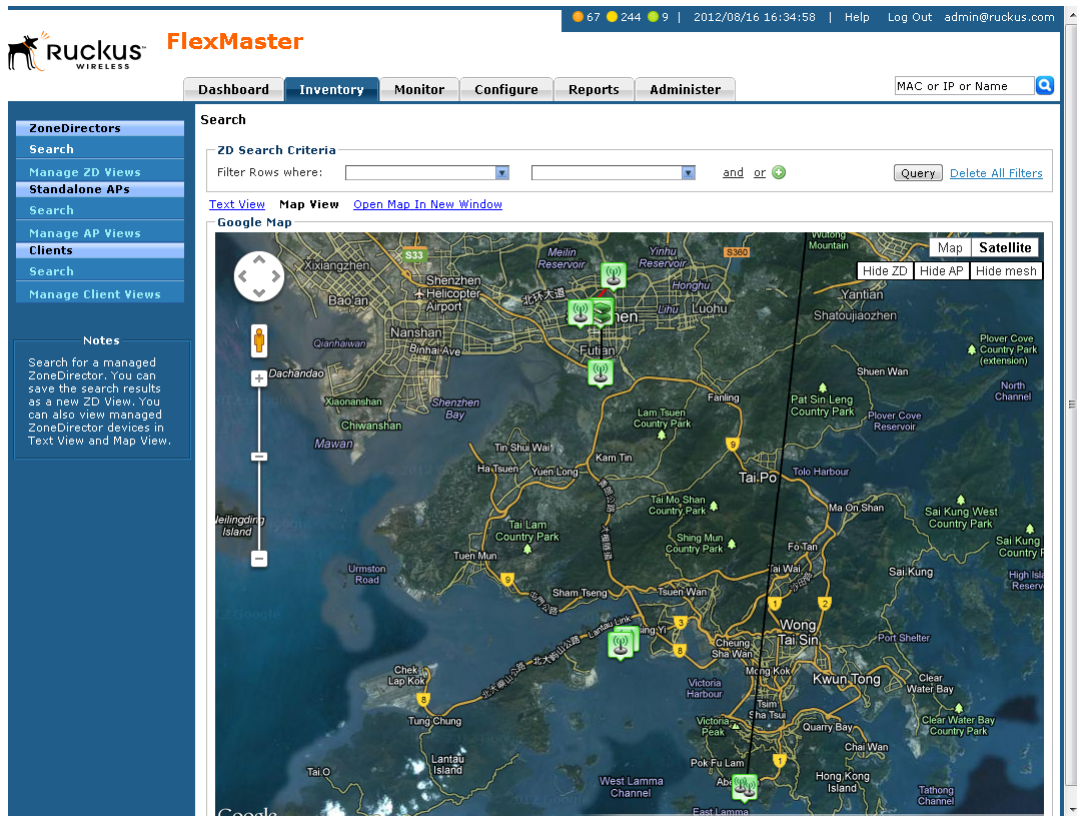
- *Map*: Standard flat globe view
- *Satellite*: Satellite view of the globe



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

- The ZD Map View includes three buttons in the top-right corner:
 - **Show ZD/Hide ZD**: Click to show or hide all ZoneDirector devices
 - **Show ZD/Hide AP**: Click to show or hide all APs
 - **Show Mesh/Hide Mesh**: Click to show or hide all mesh network links

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

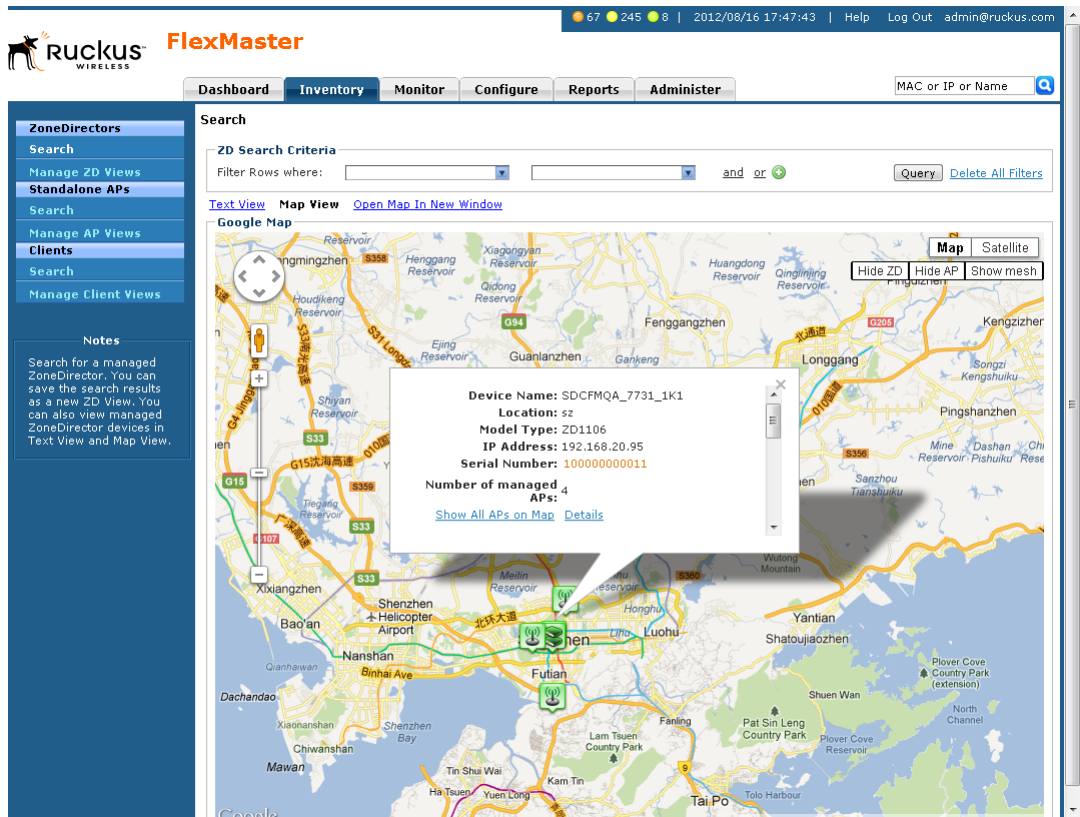


ZD Icons

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

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

Figure 42. Map View showing ZD basic information



AP Icons

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

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

Figure 43. Map View showing AP basic information

The screenshot displays the Ruckus FlexMaster web interface. At the top, the navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The 'Inventory' tab is active. On the left, a sidebar contains 'ZoneDirectors' and 'Clients' sections. The main content area is titled 'Search' and shows 'ZD Search Criteria' with filter options. Below this, there are links for 'Text View', 'Map View', and 'Open Map In New Window'. The 'Map View' is selected, showing a Google Map of Hong Kong. A pop-up window displays the following information for a selected AP:

- Status:** Connected
- Broadcast:** SDC_FMQA_ZD3K_Guest(2.4GHz); SDCFMQA_Redundant_3k(5.0GHz); SDC_FMQA_ZD3K_Hotspot(5.0GHz); SDC_FMQA_ZD3K_Guest(5.0GHz); SDC_FMQA_ZD3K_STD(5.0GHz); SDC_FMQA_ZD3K_Hotspot(2.4GHz); SDCFMQA_Redundant_3k(2.4GHz); SDC_FMQA_ZD3K_STD(2.4GHz)
- AP Serial Number:** 280901001379
- Model Name:** zf7962
- IP Address:** 192.168.22.115

The map shows various locations in Hong Kong, including Kowloon, Hong Kong Island, and Lantau Island. A search bar at the top right contains 'MAC or IP or Name'.

Viewing ZoneDirector Devices on the Map View

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

- Device name
- Location (if configured)
- Model type
- IP address
- Tag
- Serial number (hyperlink): Clicking this link opens the ZoneDirector Web interface.
- Number of managed APs
- **Show All APs on Map** (hyperlink): Clicking this link displays the Ruckus Wireless APs on the Map View. After clicking this link, the **Show/Hide ZD**, **Show/Hide AP**, and **Show/Hide Mesh** buttons appear in the upper-right corner of the Map View.
- **Details** (hyperlink): Clicking this link displays associated AP details in a pop-up table ([Figure 44](#)).

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

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

The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. A search bar is located at the top right. The left sidebar contains navigation options for 'ZoneDirectors', 'Search', 'Manage ZD Views', 'Standalone APs', 'Manage AP Views', 'Clients', and 'Manage Client Views'. The main content area is titled 'Search' and includes 'ZD Search Criteria' with filter options and a 'Query' button. Below this, there are tabs for 'Text View', 'Map View', and 'Open Map In New Window'. The 'Map View' is active, displaying a Google Map. A pop-up window is overlaid on the map, showing details for a specific AP. The pop-up window contains the following information:

Serial Number: 100903000446 [Show mesh data](#)

Number of managed APs : 6 Number of connected APs : 6 Number of disconnected APs: 0
 Number of pending APs : 0 Number of connected clients: 0

Serial Number	MAC Address	Model Name	IP Address	External IP	Connection Mode	# of Clients	Uptime
280901000824	00:25:c4:19:e5:30	zf7962	192.168.22.57	192.168.22.57:12223	L3	0	2d 20h
280901001379	00:25:c4:19:e2:e0	zf7962	192.168.22.115	192.168.22.115:12223	L3	0	2d 20h
280901001393	00:25:c4:19:e4:b0	zf7962	192.168.22.83	192.168.22.83:12223	L3	0	2d 20h
301003002070	74:91:1a:1f:ed:b0	zf7962	192.168.22.116	192.168.22.116:12223	L3	0	2d 20h
301003002290	74:91:1a:1f:fb:90	zf7962	192.168.22.117	192.168.22.117:12223	L3	0	2d 20h
VF40010099	ac:67:06:1b:fa:00	zf7962	192.168.22.102	192.168.22.102:12223	L3	0	2d 20h

At the bottom of the pop-up window, there is a pagination control showing '1 - 6 of 6' and a search input field.

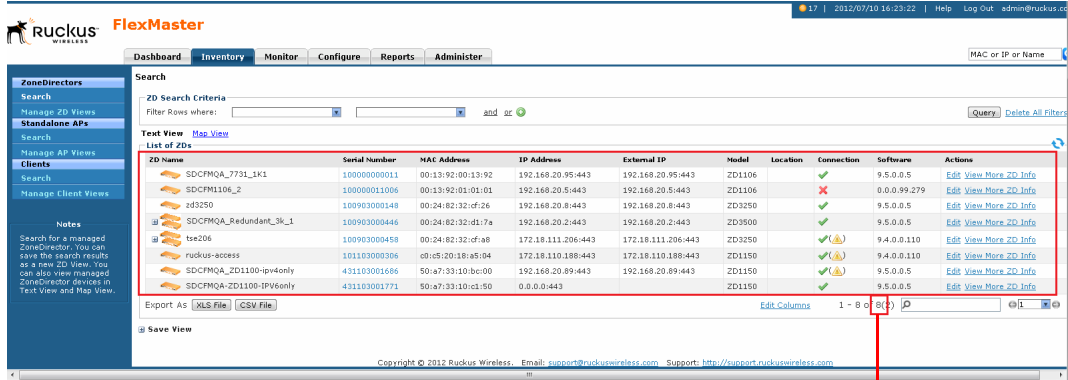
Working with ZoneDirector Inventory

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 45](#). The total number of managed ZoneDirector devices is indicated below the table, right next to the device search box.

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



Total number of managed ZoneDirector devices

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 > ZoneDirectors > Search**.
2. Look for the **ZD Search Criteria** section. To search for ZoneDirector devices, you need to specify the criteria of the devices that you are looking for.
3. In the first drop-down list box after **Filter Rows where**, select the search attribute that you want to use. Options include name, serial number, 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 appears in the search results.
 - *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered 100 as the search parameter, all devices with "100" in the IP address (for example, 172 . 17 . 16 . **100** and **100** . 1 . 10 . 13) appears in the search results.
 - *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered 3208 as the query parameter, only devices with serial numbers that begin with "3208" (for example, 320833000219 appear in the search results.
 - *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected **IP address** as the attribute and you entered 13 as the query parameter, only devices with model names that end in "13" (for example, 100 . 1 . 10 . **13**) appear in the search results.

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


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

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

The screenshot shows the FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The left sidebar has 'ZoneDirectors' selected, with sub-options for 'Search', 'Manage ZD Views', 'Standalone APs', 'Clients', and 'Manage Client Views'. The main content area is titled 'Search' and contains 'ZD Search Criteria' with filters for Model (2D3250) and MAC Address (26). Below the search criteria is a table titled 'List of ZDs' with columns for ZD Name, Serial Number, MAC Address, IP Address, External IP, Model, Location, Connection, Software, and Actions. One device is listed: 'zd3250' with serial number '100903000148', MAC address '00:24:82:32:cf:26', IP address '192.168.20.8-443', and external IP '192.168.20.8-443'. The interface also includes an 'Export As' section with options for 'XLS File' and 'CSV File', and a 'Save View' button.



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

Additional Tasks That You Can Perform

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

- Save the search results as XLS (Microsoft[®] Excel[®] file format): In *Export As*, click **XLS File**. When the *Save As* dialog box appears, click **Save File**, and then click **OK**. Use Microsoft Excel to open the file.
- Save the search results as CSV (comma-separated value file): In *Export As*, click **CSV File**. When the *Save As* dialog box appears, click **Save File**, and then click **OK**. You can use any spreadsheet application (such as Microsoft Excel) to open the file.
- Save the results as a ZD view: 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 are automatically added to the saved view.

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

FlexMaster searches all its database columns for a match to the string that you entered, and then displays the results in the *List of ZDs* table. The device property that matches the search string is highlighted in the table. In [Figure 47](#), the search string '291' matched part of a ZoneDirector device's serial number and, therefore, is highlighted in yellow.

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

The screenshot shows the FlexMaster web interface. The search criteria are set to Model: 203250 and MAC Address: 26. The search results table is as follows:

ZD Name	Serial Number	MAC Address	IP Address	External IP	Model	Location	Connection	Software	Actions
	1009030-0146	00:24:82:32:cf:26	192.168.20.8-443	192.168.20.8-443	203250		✓	9.5.0.0.5	Edit View More ZD Info

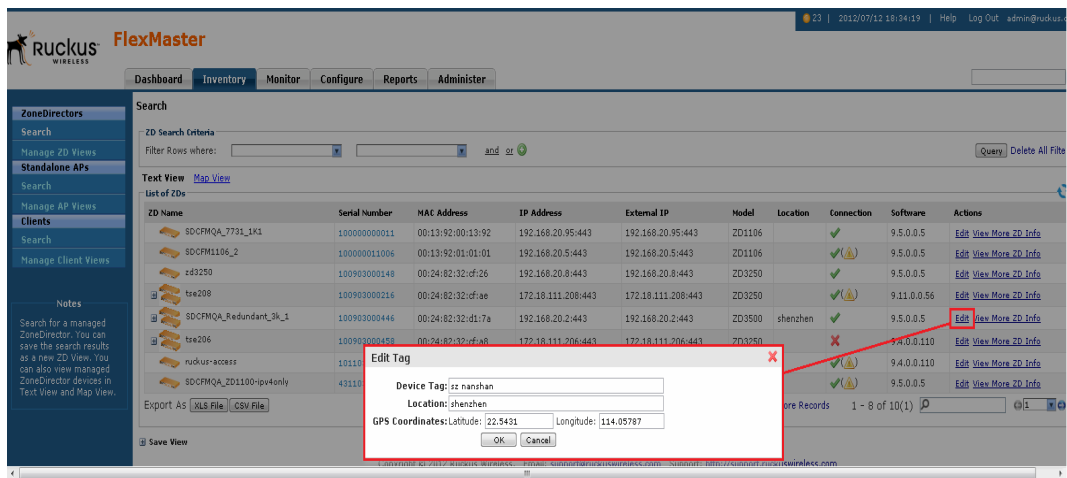
At the bottom right of the interface, there is a search box containing 'D146'. A red arrow points from this search box to the highlighted serial number '1009030-0146' in the table.

Editing a ZoneDirector Tag

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

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

Figure 48. Editing ZoneDirector tag details



Viewing ZoneDirector APs

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

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

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

The screenshot shows the FlexMaster interface with the following components:

- Navigation Menu (Left):** ZoneDirectors, Search, Manage ZD Views, Stand-alone APs, Search, Manage AP Views, Clients, Manage Client Views, Notes.
- Search Bar (Top):** ZD Search Criteria, Filter Rows where: [dropdown], [add or] [clear], [Query] Delete All Filters.
- Main Content Area:**
 - List of ZDs Table:**

ZD Name	Serial Number	MAC Address	IP Address	External IP	Model	Location	Connection	Software	Actions
SDCFMQA_7731_SK1	10000000011	00:13:92:00:13:92	192.168.20.95:443	192.168.20.95:443	ZD1106		✓	9.5.0.0.5	Edit View More ZD Info
SDCFMQA_1006	10000001006	00:13:92:01:01:01	192.168.20.5:443	192.168.20.5:443	ZD1106		✓	9.5.0.0.5	Edit View More ZD Info
z3250	100903000148	00:24:82:32:cf:26	192.168.20.8:443	192.168.20.8:443	ZD3250		✓	9.5.0.0.5	Edit View More ZD Info
txe200	100903000216	00:24:82:32:cf:a8	172.18.111.208:443	172.18.111.208:443	ZD3250		✓	9.11.0.0.56	Edit View More ZD Info
SDCFMQA_#redundant_3K_1	100903000446	00:24:82:32:d1:7a	192.168.20.2:443	192.168.20.2:443	ZD3500	shenzhen	✓	9.5.0.0.5	Edit View More ZD Info
tre206	100903000458	00:24:82:32:cf:a8	172.18.111.206:443	172.18.111.206:443	ZD3250		✗	9.4.0.0.110	Edit View More ZD Info
ruckus-access	101103000306	c0:c5:20:18:a5:04	172.18.110.188:443	172.18.110.188:443	ZD1150		✓	9.4.0.0.110	Edit View More ZD Info
SDCFMQA_ZD1100-ipv6only	431103001666	50:a7:33:10:bc:00	192.168.20.89:443	192.168.20.89:443	ZD1150		✓	9.5.0.0.5	Edit View More ZD Info
 - ZD Detail Section:**
 - Buttons: ZD Overview, **AP List**, Mesh View, WLAN, AP Group
 - ZD AP List Table:**

AP Name	Description	Serial Number	AP MAC	Model Name	IP Address	External IP	Connection Mode	# of clients	Uptime	Status
RuckusAP		921001013734	04:ef:aa:2a:ccc:b0	z77942	192.168.22.92	192.168.22.92:12223	L3	0		✗
		301003000244	ac:67:06:1e:45:30	z77962	192.168.22.108	192.168.22.108:12223	L3	0	17h 49m	✓

Viewing ZoneDirector Mesh Connections

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

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

Figure 50. ZoneDirector Mesh View

The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The left sidebar contains navigation options for 'ZoneDirectors', 'Standalone APs', 'Clients', and 'Notes'. The main content area displays a 'List of ZDs' table with columns for ZD Name, Serial Number, MAC Address, IP Address, External IP, Model, Location, Connection, Software, and Actions. Below the table, the 'ZD Detail' section is visible, with the 'Mesh View' tab selected. The 'ZD Mesh View' table shows details for an access point, including AP Name, Description, IP Address, Channel, Model Name, Uptime, RSSI, and # of Clients.

ZD Name	Serial Number	MAC Address	IP Address	External IP	Model	Location	Connection	Software	Actions
SDFMQA_7791_3K1	100903000011	00:13:92:00:13:92	192.168.20.95-443	192.168.20.95-443	ZD1106		✓	9.5.0.0.5	Edit View More ZD Info
SDFM1106_2	1009030011006	00:13:92:01:01:01	192.168.20.5-443	192.168.20.5-443	ZD1106		✓	9.5.0.0.5	Edit View More ZD Info
z63250	100903000149	00:24:82:32:cf:26	192.168.20.8-443	192.168.20.8-443	ZD3250		✓	9.5.0.0.5	Edit View More ZD Info
ts4208	100903000216	00:24:82:32:cf:a6	172.18.111.208-443	172.18.111.208-443	ZD3250		✓	9.11.0.0.56	Edit View More ZD Info
SDFMQA_#-fundant_3k_1	100903000446	00:24:82:32:d1:7a	192.168.20.2-443	192.168.20.2-443	ZD3500	shenzhen	✓	9.5.0.0.5	Edit View More ZD Info
ts4206	100903000459	00:24:82:32:cf:a8	172.18.111.206-443	172.18.111.206-443	ZD3250		✗	9.4.0.0.110	Edit View More ZD Info
ruckus-access	110110300036	00:c5:20:18:a5:04	172.18.110.188-443	172.18.110.188-443	ZD1150		✓	9.4.0.0.110	Edit View More ZD Info
SDFMQA_ZD1100-ipv6only	431103001686	50:a7:33:10:bc:00	192.168.20.89-443	192.168.20.89-443	ZD1150		✓	9.5.0.0.5	Edit View More ZD Info

Access Points	AP Name	Description	IP Address	Channel	Model Name	Uptime	RSSI	# of Clients
	ac:67:06:1a:e5:30	RuckusAP	192.168.22.108	157 (11a/n=40)	rF962	17h 49m		0

Viewing ZoneDirector WLANs and WLAN Groups

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

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

Figure 51. ZoneDirector WLANs and WLAN groups

The screenshot shows the ZoneDirector interface. The top section displays a table of ZD devices. The bottom section shows the 'ZD Detail' view with the 'WLAN' tab selected, displaying details for WLANs and WLAN Groups.

ZD Name	Serial Number	MAC Address	IP Address	External IP	Model	Location	Connection	Software	Actions
SDCFMQA_7731_1K1	10090300011	00:13:92:00:13:92	192.168.20.95-443	192.168.20.95-443	ZD1106		✓	9.5.0.0.5	Edit View More ZD Info
SDCFM1106_2	100903001000	00:13:92:01:01:01	192.168.20.8-443	192.168.20.8-443	ZD1106		✓	9.5.0.0.5	Edit View More ZD Info
k32250	100903000149	00:24:82:32:cf:26	192.168.20.8-443	192.168.20.8-443	ZD3250		✓	9.5.0.0.5	Edit View More ZD Info
tra200	100903000216	00:24:82:32:cf:a6	172.18.111.208-443	172.18.111.208-443	ZD3250		✓	9.11.0.0.56	Edit View More ZD Info
SDCFMQA_Redundant_3A_1	100903000446	00:24:82:32:d1:7a	192.168.20.2-443	192.168.20.2-443	ZD3500	shenzhen	✓	9.5.0.0.5	Edit View More ZD Info
tra206	100903000459	00:24:82:32:cf:a0	172.18.111.206-443	172.18.111.206-443	ZD3250		✗	9.4.0.0.110	Edit View More ZD Info
radius-access	101103000306	c0:e5:20:18:a5:04	172.18.110.180-443	172.18.110.180-443	ZD1150		✓	9.4.0.0.110	Edit View More ZD Info
SDCFMQA_ZD1100-ipv4only	431103001686	50:a7:33:10:bc:00	192.168.20.89-443	192.168.20.89-443	ZD1150		✓	9.5.0.0.5	Edit View More ZD Info

Name	ESSID	Authentication	Encryption	Clients
SDCFM1106_2	SDCFM1106_2	open	wpa	0

Name	Description	WLANs
Default	Default WLANs for Access Points	SDCFM1106_2

Viewing ZoneDirector AP Groups

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

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

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

The screenshot displays the FlexMaster interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The left sidebar contains navigation options for 'ZoneDirectors', 'Clients', and 'Notes'. The main content area shows a 'List of ZDs' table with columns for ZD Name, Serial Number, MAC Address, IP Address, External IP, Model, Location, Connection, Software, and Actions. The selected row is 'SDCFMQA_Radumiant_3k_1'. Below the table, the 'ZD Detail' section is visible, with the 'AP Group' tab selected. This tab displays a table of AP groups with columns for Member, Device Name, Description, Model, and Status. The 'System Default' group is expanded, showing several RuckusAP devices with their respective MAC addresses and connection statuses.

ZD Name	Serial Number	MAC Address	IP Address	External IP	Model	Location	Connection	Software	Actions
SDCFMQA_7731_1K1	100000000011	00:13:92:00:13:92	192.168.20.95:443	192.168.20.95:443	ZD1106		✓	9.5.0.0.5	Edit View More ZD Info
SDCFM1106_2	100000011006	00:13:92:01:01:01	192.168.20.5:443	192.168.20.5:443	ZD1106		✓	9.5.0.0.5	Edit View More ZD Info
ed3250	100903000149	00:04:82:32:cf:26	192.168.20.8:443	192.168.20.8:443	ZD3250		✓	9.5.0.0.5	Edit View More ZD Info
tre200	100903000216	00:04:82:32:cf:ae	172.18.111.208:443	172.18.111.208:443	ZD3250		✓	9.11.0.0.56	Edit View More ZD Info
SDCFMQA_Radumiant_3k_1	100903000446	00:04:82:32:d1:7a	192.168.20.2:443	192.168.20.2:443	ZD3500	shenzhen	✓	9.5.0.0.5	Edit View More ZD Info
tre206	100903000458	00:04:82:32:cf:a8	172.18.111.206:443	172.18.111.206:443	ZD3250		✗	9.4.0.0.110	Edit View More ZD Info
ruckus-access	101103000306	c0:c5:20:18:a5:04	172.18.110.188:443	172.18.110.188:443	ZD1150		✓	9.4.0.0.110	Edit View More ZD Info
SDCFMQA_ZD1100-ipvonly	431103002166	50:a7:33:10:bc:00	192.168.20.89:443	192.168.20.89:443	ZD1150		✓	9.5.0.0.5	Edit View More ZD Info

Member	Device Name	Description	Model	Status
System Default				
80:25:c4:19:a4:b0	RuckusAP	System default group for Access Point	r7962	✓
74:93:1a:1f:fb:90	RuckusAP		r7962	✓
74:93:1a:1f:ed:b0	RuckusAP		r7962	✓
ac:67:06:1b:fa:00	RuckusAP		r7962	✓
00:25:c4:19:a2:a0	RuckusAP		r7962	✓
00:25:c4:19:a5:30	Kannath7962		r7962	✓
ac:67:06:1e:45:30	RuckusAP		r7962	✗

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 you want to deploy tasks to a group of devices.

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

1. Perform a search for clients using one of these search methods:
 - [Search Using the ZD Search Criteria](#), or
 - [Search Using the Search Box](#)
2. When the search results appear, scroll down to the Save as View section.
3. In **View Name**, type a name that you want to assign to the view.
4. In **Description**, type a description for the view that you are saving. For example, if the view contains only ZoneDirector 3250 devices, you can type **ZD3250s only**.
5. Click **Save**.

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

Figure 53. Creating a ZD view that contains only ZoneDirector 3250 devices

The screenshot shows the FlexMaster interface with a search for 'ZD3250' devices. The search results table is as follows:

ZD Name	Serial Number	MAC Address	IP Address	External IP	Model	Location	Connection	Software	Actions
zdz250	100903000148	00:24:82:32:cf:26	192.168.20.8:443	192.168.20.8:443	ZD3250		✓	9.5.0.0.5	Edit View More ZD Info
tsa208	100903000214	00:24:82:32:cf:ae	172.18.111.208:443	172.18.111.208:443	ZD3250		✓ (A)	9.11.0.0.56	Edit View More ZD Info
tsa206	100903000458	00:24:82:32:cf:a8	172.18.111.206:443	172.18.111.206:443	ZD3250		✗	9.4.0.0.110	Edit View More ZD Info

The 'Save as View' dialog box is open, showing the following fields:

- View Name: ZD3250
- Description: ZD3250s only
- Buttons: Save, Cancel

Managing ZD Views

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

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

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

View Name	Created by	Created On	Criteria	View Description	Actions
All ZoneDirectors	admin@ruckus.com	2012-07-06 18:03:13		All ZoneDirectors	Set Tags Query
ruckus-access	admin@ruckus.com	2012-07-10 10:21:19	DeviceName Equals To ruckus-access		Edit Delete Set Tags Query
SDCFMQA_Redundant_3k_1	freddy	2012-07-11 17:18:19	DeviceName Equals To SDCFMQA_Redundant_3k_1	SDCFMQA_Redundant_3k_1	Edit Delete Set Tags Query
zdsK	freddy	2012-07-12 15:05:40	ModeName Equals To ZDS100		Edit Delete Set Tags Query

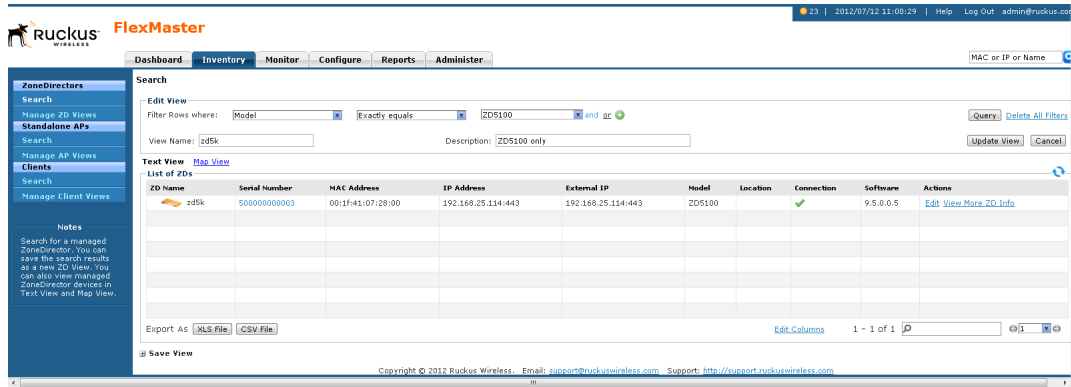
At the bottom of the table, there is a pagination control showing '1 - 4 of 4' and a search input field.

Editing a ZD View

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

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

Figure 55. Editing a ZD view



Deleting a ZD View

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

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

Editing a ZD View Tag

If you have a ZD view with all the devices in the same location, you can create a ZD view tag that FlexMaster uses to display the devices in *Map View*.

1. In the *List of ZD Views* table, display the ZD view you want to edit. If the ZD view you want to edit does not appear on the table, search for it using the search box.
2. Click the ZD view **Set Tags** link. FlexMaster displays the *Edit Tag* menu at the bottom of the window.
3. Edit the ZD view tag properties that you want to update. Properties that you can edit include:
 - ZD view tag name.
 - Location -- text string that appears in the *Text View* and the *Map View*.
 - GPS Coordinates (Latitude and Longitude) -- FlexMaster uses these to position the ZD view icon on the *Map View*.
 - Device Web Port Number Mapping -- maps the device web port for this ZD view.
 - Device Wakeup Port Number Mapping -- maps the device wakeup port for this ZD view; normally 8082.
4. After you make changes, click **OK**.

Figure 56. Editing ZoneDirector View tag details

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

View Name	Created by	Created On	Criteria	View Description	Actions
All ZoneDirectors	admin@ruckus.com	2012-06-06 16:44:57		All ZoneDirectors	Set Tags Query
Roxie Networks	dstff@ruckus.com	2012-06-01 10:52:41	DeviceName Contains roxie	David Stiff's home network	Edit Delete Set Tags Query
RuckusChicagoDemo	John	2012-07-10 22:06:33	DeviceName Equals To RuckusChicagoDemo	Trial/PoC ZD	Edit Delete Set Tags Query

Below the table is the 'Edit Tag' form with the following fields:

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

Buttons for 'OK' and 'Cancel' are at the bottom of the form.

Viewing Devices That Belong to a ZD View

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

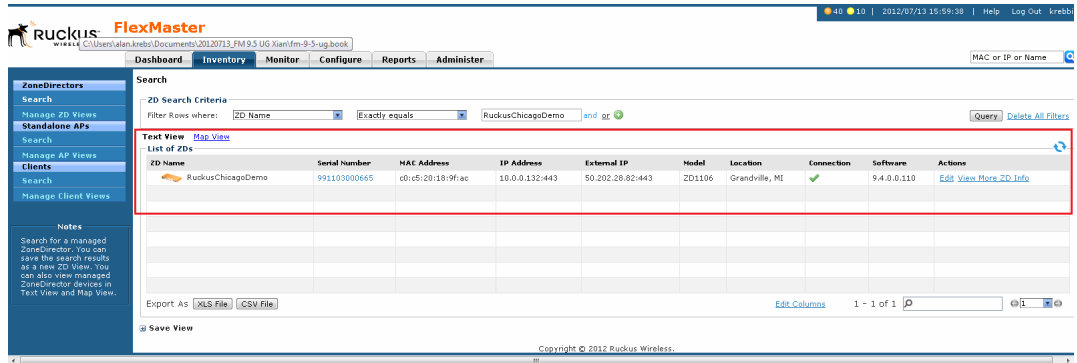
1. Go to the **Inventory > ZoneDirectors > Manage ZD Views** page.
2. Look for the ZD view on which you want to run a query.

Working with Device Inventory

Working with ZoneDirector Inventory

3. Click the ZD view **Query** link. The ZoneDirector Search page appears, and the devices that belong to the ZD view appear in the *List of ZDs* section ([Figure 57](#)).

Figure 57. After you click the Query link, devices that belong to the view appear in the List of ZDs section



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 'ZoneDirectors' section with options for 'Search', 'Manage ZD Views', 'Standalone APs', 'Manage AP Views', 'Clients', and 'Manage Client Views'. The main content area is titled 'Search' and contains a search criteria section with a filter for 'ZD Name' set to 'RuckusChicagoDemo'. Below this is a 'List of ZDs' table with one row of data. The table has columns for ZD Name, Serial Number, MAC Address, IP Address, External IP, Model, Location, Connection, Software, and Actions. The data row shows 'RuckusChicagoDemo' with serial number 991103000665, MAC address c0:c5:20:18:9f:ac, IP address 10.0.0.132:443, and external IP 50.202.28.82:443. The table also includes an 'Export As' section with 'XLS File' and 'CSV File' options, and a 'Save View' button.

ZD Name	Serial Number	MAC Address	IP Address	External IP	Model	Location	Connection	Software	Actions
RuckusChicagoDemo	991103000665	c0:c5:20:18:9f:ac	10.0.0.132:443	50.202.28.82:443	ZD1106	Grandville, MI	✓	9.4.0.0.110	Edit View More ZD Info

Working with Standalone APs Inventory

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



NOTE: To view a list of APs that are reporting to managed ZoneDirector devices, refer to [Viewing ZoneDirector APs](#).

Viewing a Summary of Standalone APs

To view APs that have registered with FlexMaster, click **Inventory > Standalone APs > Search**. A list of APs appears in the **List of APs** section as shown in [Figure 58](#). The total number of managed APs is indicated below the table, right next to the device search box.

Figure 58. A list of APs that have registered with FlexMaster appears in the List of APs section

The screenshot shows the FlexMaster web interface. The 'Standalone APs' section is active, displaying a 'List of APs' table. The table has columns for AP Name, Serial Number, MAC Address, IP Address, External IP, Model, Location, Uptime, Connection, Software, and Actions. Three APs are listed: kenoyw_AP, RuckusAP, and Eric7962. Below the table, there is an 'Export As' section with 'XLS File' and 'CSV File' options, and a pagination control showing '1 - 3 of 3'.

AP Name	Serial Number	MAC Address	IP Address	External IP	Model	Location	Uptime	Connection	Software	Actions
kenoyw_AP	161055002718	AC:67:06:33:7F:10	192.168.1.24:443	115.66.30.19:443	ZF7363	Singapore	23d 8h 56m	✓	9.4.0.0.110	Edit
RuckusAP	481102001114	50:A7:33:28:5D:20	10.0.1.142:443	67.8.165.142:443	ZF7025		11d 3h 1m	✓	9.4.0.0.111	Edit
Eric7962	501003003115	CO:C5:20:12:31:40	10.0.1.105:443	67.8.165.142:443	ZF7962		18h 35m	✗	9.4.0.0.103	Edit

Total number of managed APs

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 Standalone APs

There are two ways to search for APs:

- [Search Using the AP Search Criteria](#)
- [Search Using the Search Box](#)

Search Using the AP Search Criteria

1. Go to the **Inventory > Standalone APs > Search**.
2. Look for the **AP Search Criteria** section. To search for APs, you need to specify the criteria of the devices that you are looking for.
3. In the first drop-down list box after **Filter Rows where**, select the search attribute that you want to use. Options include AP name, serial number, MAC address, IP address, external IP address, model, and last seen (among others).
4. In the second drop-down list box, select the search operator that you want to use. Available search operators include:
 - *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered 172 . 17 . 16 . 176 as the search parameter, only devices with this IP address appear in the search results.
 - *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered 100 as the search parameter, all devices with "100" in the IP address (for example, 172 . 17 . 16 . **100** and **100** . 1 . 10 . 13) appear in the search results.
 - *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered 3908 as the query parameter, only devices with serial numbers that begin with "3908" (for example, 390801005202) appear in the search results.
 - *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected **IP address** as the attribute and you entered 13 as the query parameter, only devices with model names that end in "13" (for example, 100 . 1 . 10 . **13**) appear in the search results.

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


5. In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
6. If you want to add another search filter, 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 59. 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'. A search bar at the top right contains 'MAC or IP or Name'. The left sidebar has a 'Search' section with options for 'ZoneDirectors', 'Standalone APs', and 'Clients'. The main content area is titled 'Search' and shows 'AP Search Criteria' with a filter 'Filter Rows where: IP Address [v] [Ends with] [v] 1.142 and or [v]'. Below this is a 'Text View' section with a 'List of APs' table. The table has columns for AP Name, Serial Number, MAC Address, IP Address, External IP, Model, Location, Uptime, Connection, Software, and Actions. One row is visible for 'RuckusAP' with serial number '491102001114', MAC address '50:A7:33:28:5D:20', IP address '10.0.1.142:443', and external IP '67.8.165.142:443'. At the bottom, there are options to 'Export As' (XLS File, CSV File) and a 'Save View' button.



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

Additional Tasks That You Can Perform

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

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

Search Using the Search Box

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



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

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

FlexMaster searches all its database columns for a match to the string that you entered, and then displays the results in the *List of APs* table. The device property that matches the search string is highlighted in the table. In [Figure 60](#), the search string 3908 matched part of two APs's serial numbers and, therefore, are highlighted in yellow.

Figure 60. The device property that matches the search string is highlighted in the search results

The screenshot shows the FlexMaster web interface. The 'List of APs' table is displayed with the following data:

AP Name	Serial Number	MAC Address	IP Address	External IP	Model	Location	Uptime	Connection	Software	Actions
RuckusAP	481102001114	90:A7:33:20:5D:20	10.0.1.142:443	67.8.165.142:443	277025		11d 5h 16m	✓	9.4.0.0.111	Edit
Eric7962	501003003115	C0:15:20:12:31:40	10.0.1.195:443	67.8.165.142:443	277962		18h 35m	✗	9.4.0.0.103	Edit

The search criteria at the top of the table is '3908'. The 'External IP' column for both rows is highlighted in yellow. A red box highlights the search input field at the bottom right, which contains '3908'. A red arrow points from the search input field to the highlighted 'External IP' cells in the table.

Editing a Standalone AP Tag

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

1. On the *List of APs* table, look for the device that you want to edit. 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 tag properties that you want to update. Properties that you can edit include:
 - Standalone AP tag name.
 - Location -- text string that appears in the *Text View* and the *Map View*.
 - GPS Coordinates (Latitude and Longitude) -- FlexMaster uses these to position the standalone AP icon on the *Map View*.
 - Device Wakeup Port Number Mapping -- maps the device wakeup port for this standalone AP; normally 8082.



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

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

Figure 61. Editing standalone AP tag details

The screenshot shows the Ruckus FlexMaster interface. A modal dialog box titled "Edit Tag" is open, allowing for the configuration of a standalone AP's tag details. The dialog includes the following fields:

- Device Tag:
- Location:
- GPS Coordinates: Latitude: Longitude:
- Device Wakeup Port Number Mapping:

Buttons for "OK" and "Cancel" are at the bottom of the dialog. In the background, a table lists APs with columns for AP Name, Serial #, Uptime, Connection, Software, and Actions. The "Edit" link in the Actions column for the AP "RuckusAP" is highlighted with a red box.

AP Name	Serial #	Uptime	Connection	Software	Actions
kennyw_AP	141055	23d 9h 48m	✓	9.4.0.0.110	Edit
RuckusAP	481102	15d 2h 21m	✓	9.4.0.0.111	Edit
Eric7962	501003	18h 35m	✗	9.4.0.0.103	Edit

Creating a Standalone AP View

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

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**.

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

Figure 62. 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 options for ZoneDirectors, Standalone APs, Clients, and Notes. The main content area displays search results for APs. A 'Save View' dialog box is open at the bottom, with a red border. The dialog box contains the following information:

- View Name: Ruckus AP
- Description: Ruckus APs with 1.142
- Buttons: Save, Cancel

The background shows a table of APs with the following columns: AP Name, Serial Number, MAC Address, IP Address, External IP, Model, Location, Uptime, Connection, Software, and Actions. The table contains one row of data for a Ruckus AP.

AP Name	Serial Number	MAC Address	IP Address	External IP	Model	Location	Uptime	Connection	Software	Actions
RuckusAP	481102001114	50:A7:33:28:5D:20	10.0.1.142/443	67.8.145.142/443	ZF7025		114 4h 17m	✓	9.4.0.0.111	Edit

Managing Standalone AP Views

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

Figure 63. The *Manage AP Views* page lists all existing AP views

The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The left sidebar contains navigation options: 'ZoneDirectors', 'Manage 2D Views', 'Standalone APs', 'Manage AP Views', 'Clients', and 'Notes'. The main content area is titled 'Manage AP Views' and contains a table with the following data:

View Name	Created by	Created On	Criteria	View Description	Actions
All Standalone APs	admin@ruckus.com	2012-06-06 16:44:57		All Standalone APs	Set Tags Query
Ruckus AP	krebbis	2012-07-13 17:15:39	IPAddress Ends With 1.142	Ruckus APs with 1.142	Edit Delete Set Tags Query

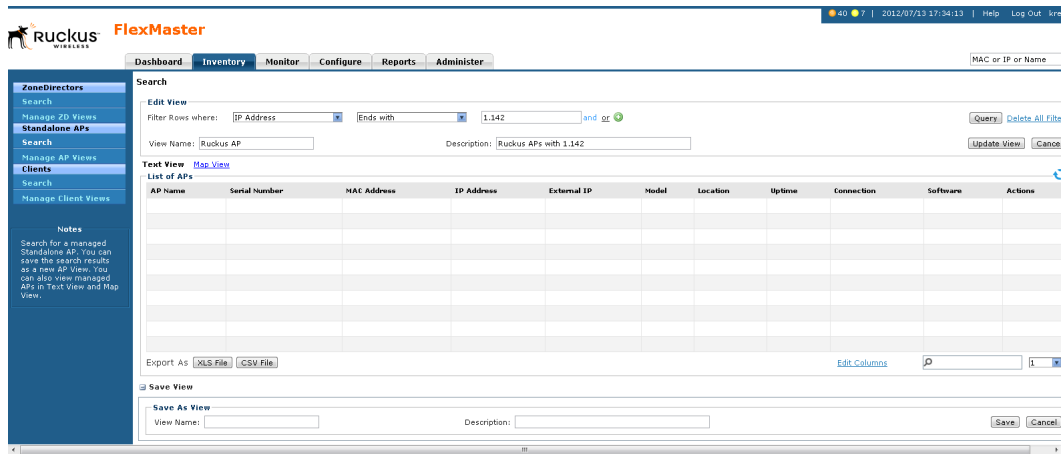
At the bottom of the table, there is a search bar labeled 'New Search' and a footer that reads 'Copyright © 2012 Ruckus Wireless.' The page also shows '1 - 2 of 2' items and pagination controls.

Editing an AP View

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

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

Figure 64. Editing an AP view



Deleting an AP View

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

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

Setting Tags

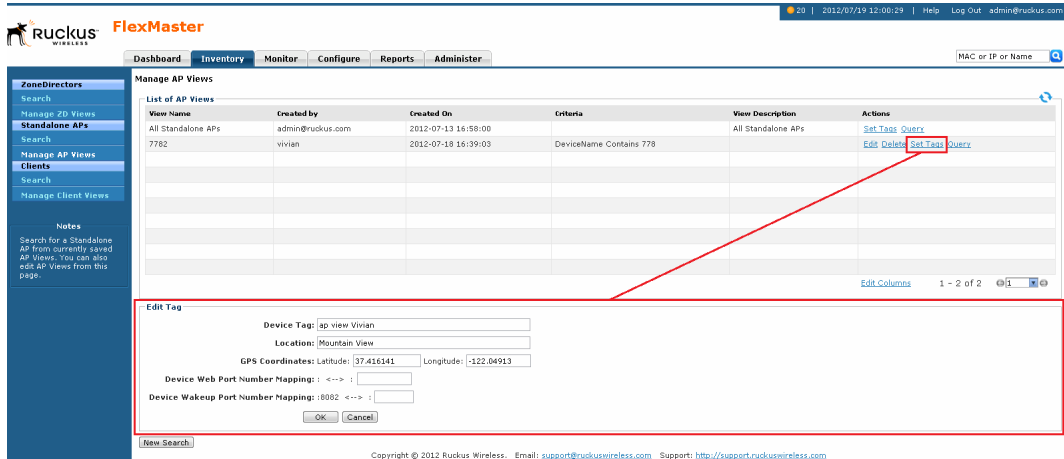
If you have a view with all the devices in the same location, you can use the geographical location of those devices as the tag to enable FlexMaster to display the devices on the *Map View*.

Follow these steps to assign a tag to an AP view.

1. Go to the **Inventory > Standalone APs > Manage Views** page.
2. Look for the to which you want to assign a tag.
3. Click the AP view **Set Tags** link. The *Edit Tag* section appears at the bottom of the page.
 - a. In **Device Tag**, type the tag name that you want to assign to the AP view.
 - b. In **Location**, type a text string that appears in the *Text View* and the *Map View*.
 - c. In **GPS Coordinates**, enter the Latitude and Longitude of the view; FlexMaster uses these to position the AP view icon on the *Map View*.
 - d. In **Device Web Port Number Mapping**, enter the device web port map for this AP view.

- e. In Device Wakeup Web Port Number Mapping, enter the device wakeup port map for this AP view; normally 8082.
4. Click **OK** to save your changes.

Figure 65. Assigning a tag to an AP view

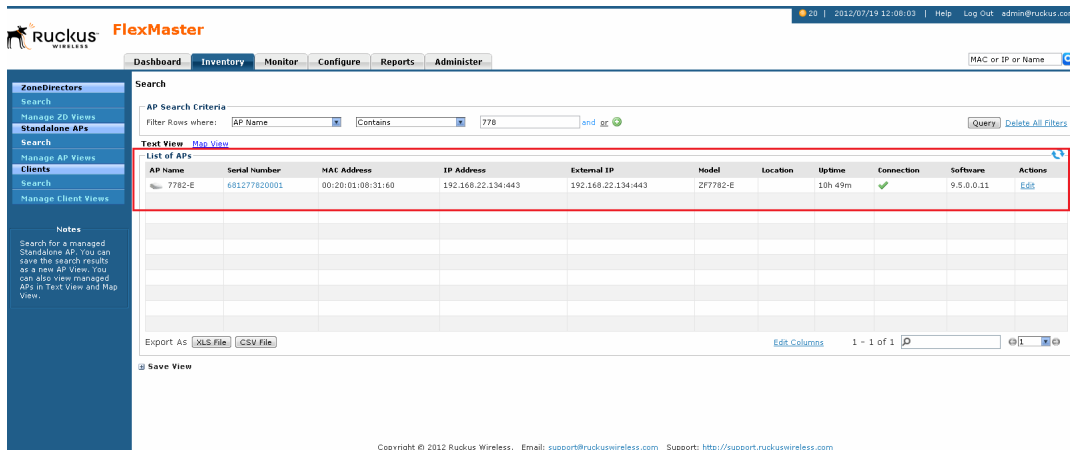


Viewing Devices That Belong to a View

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


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

Figure 66. After you click the Query link, devices that belong to the view appear in the List of APs section



Viewing 7731 Bridge Relationships

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

1. Go to the **Inventory** page.
2. Under Standalone APs, click **Search**.
3. In **Filter Rows where**, select the following:
 - First drop-down menu: Model
 - Second drop-down menu: Exactly equals
 - Third drop-down menu: ZF7731
4. Click **Query**. The 7731 devices on the network appear under *List of APs*.
5. Click the **Map View** link to view the locations of the 7731 devices on the map. The map view displays the 7731 devices (denoted by the  icon) on the map.


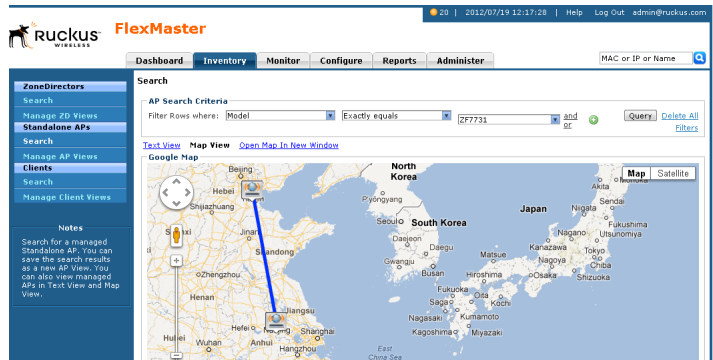
The Map View also displays the bridge relationships of these 7731 devices, as well as the ZoneDirector devices (denoted by the  icon) to which they report.

Figure 67. The map view shows the relationships of the 7731 Bridge devices and the ZoneDirector to which they report.

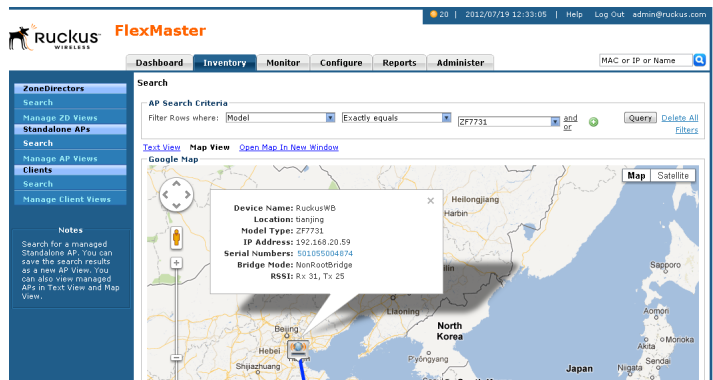


Viewing 7731 AP Bridge Summary Information

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


- Device Name
- Location
- Model Type
- IP Address
- Serial Numbers
- Bridge Mode
- RSSI

Figure 68. Click the device icon to view summary information about the device



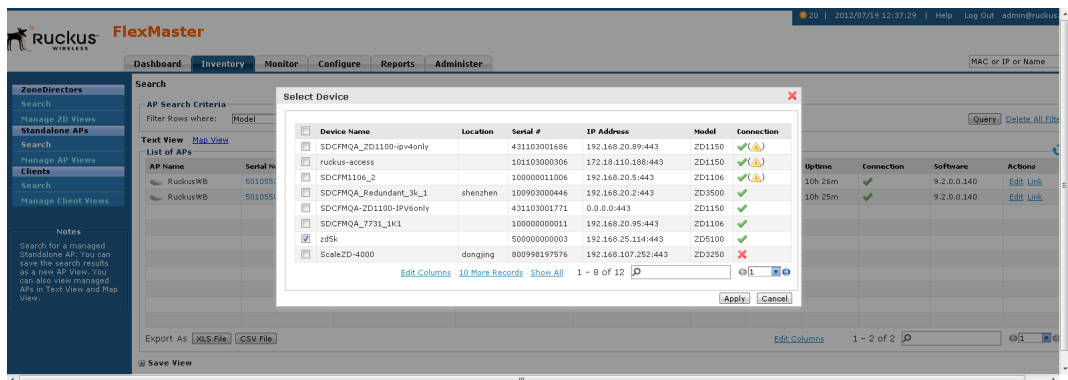
Updating the Parent ZoneDirector of a 7731 Bridge Device

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

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

You have completed updating the parent ZoneDirector of the 7731 Bridge.

Figure 69. Select the check box for the ZoneDirector device to which you want the 7731 Bridge to report



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 70](#). The total number of clients (associated with APs reporting to managed ZoneDirector devices) is indicated below the table, right next to the device search box.

Figure 70. A list of clients appears in the List of Clients section

ZD Name	AP Name	Client MAC	Client IP Address	WLAN	Device Info	Host Name	Associated Time	Channel	Radio Type	Signal	Rx	Tx	Vlan	Retries	Connection	Authentication
ruckus-access	RuckusAP 00:27:bb:3c:9f:34	172.18.111.50	ruckus-access	video54.local	edwardu-PC	17h 3m	165	802.11a/h	79.2%	90.33MB	6.93MB	1	6182	✓	✓	✓
ruckus-access	RuckusAP 00:24:d7:36:a6:70	172.18.112.90	ruckus-access	video54.local		17h 43m	1	802.11g/h	96.5%	176.93MB	34.40MB	1	3162	✓	✓	✓
ruckus-access	RuckusAP 00:24:5a:44:39:e4	172.18.110.145	ruckus-access	video54.local	jiangw	1d 18h 19m 11	11	802.11n/g	99.0%	154.88MB	8.45MB	1	150986	✓	✓	✓
ruckus-access	RuckusAP 00:24:d7:dd:63:e4	172.18.111.112	ruckus-access	video54.local		1d 11h 27m	165	802.11a/h	99.0%	921.11MB	136.39MB	1	2656	✓	✓	✓
SDCFMQA_Redundant_3k_1	RuckusAP 00:26:c6:3c:99:12	192.168.22.134	SDC-FMQA-ZD3K_STD		lenovo-c913ae4f	4h 56m	149	802.11a/h	99.0%	9.91MB	1.02MB	1	6	✓	✓	✓
SDCFMQA_ZD1100-IP6only	RuckusAP 00:26:c6:3c:97:80	192.168.22.93	SDC-FMQA-ZD1104_STD			12h 10m	4	802.11b/g	17.3%	17.56MB	46.10MB	1	45	✓	✓	✓
ruckus-access	RuckusAP 04:77:83:2f:6c:d0	172.18.112.113	ruckus-access		cherry-AP-01-PC	12h 12m	1	802.11g/h	61.9%	17.65MB	315.18KB	1	2596	✓	✓	✓
SDCFMQA-ZD1100-IP6only	RuckusAP 58:94:6b:24:62:f6	192.168.22.120	SDC-FMQA-ZD1116_STD		SDC-FREDDYCHEN	52m	157	802.11a/h	69.1%	1.15MB	144.33KB	1	18	✓	✓	✓
ruckus-access	RuckusAP 00:24:d7:2e:ac:04	172.18.110.180	ruckus-access		SDC-Wind-PC	2h 11m	165	802.11a/h	91.6%	5.43MB	69.44KB	1	1	✓	✓	✓
ruckus-access	RuckusAP f4:6d:04:3a:e8:b0	172.18.111.24	ruckus-access		android-699f1836229a592a	7h 18m	11	802.11g/h	61.9%	18.33MB	34.16KB	1	7495	✗	✓	✓

Total number of clients

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

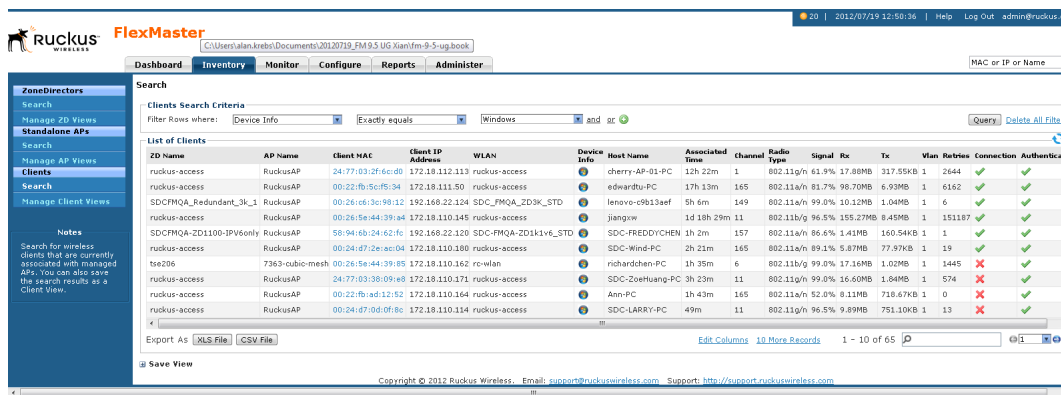
There are two ways to search for clients:

- [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 need to specify the criteria of the devices that you are looking for.


Figure 71. Using Search Criteria to search for a client



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 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) 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) 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) appear in the search results.

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

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



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

Additional Tasks That You Can Perform

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

- Save the search results as XLS (Microsoft[®] Excel[®] file format): In *Export As*, click **XLS File**. When the *Save As* dialog box appears, click **Save File**, and then click **OK**. Use Microsoft Excel to open the file.
- Save the search results as CSV (comma-separated value file): In *Export As*, click **CSV File**. When the *Save As* dialog box appears, click **Save File**, and then click **OK**. You can use any spreadsheet application (such as Microsoft Excel) to open the file.
- Save the results as a client view: 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 are automatically added to the saved view.

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

FlexMaster searches all its database columns for a match to the string that you entered, and then displays the results in the *List of Clients* table. The device property that matches the search string is highlighted in the table. In [Figure 72](#), the search string 00 : 16 matched part of a client's MAC address and, therefore, is highlighted in yellow.

Figure 72. The device property that matches the search string is highlighted in the search results

The screenshot shows the FlexMaster interface with a search filter applied to the 'List of Clients' table. The search criteria are 'Device Info' and 'Exactly equals' with the search string '00:16'. The table lists various clients, and the 'Client MAC' column for the 'cherry-AP-01-PC' entry is highlighted in yellow, indicating a match with the search string. The 'Host Name' column for the same entry is also highlighted in red.

ZD Name	AP Name	Client MAC	Client IP Address	WLAN	Device Info	Host Name	Associated Time	Channel	Radio Type	Signal	Rx	Tx	Vlan	Rebtes	Connection	Authentication
ruckus-access	RuckusAP	00:24:d7:2e:ac:04	172.18.110.180	ruckus-access	SDC-Wind-PC	cherry-AP-01-PC	2h 25m	165	802.11a/n	91.6%	6.05MB	78.87KB	1	19	✓	✓
ruckus-access	RuckusAP	24:77:03:2f:6c:d0	172.18.112.113	ruckus-access	cherry-AP-01-PC	edwardu-PC	12h 25m	1	802.11g/n	66.8%	17.98MB	319.21KB	1	2663	✓	✓
ruckus-access	RuckusAP	00:22:fb:5c:f5:34	172.18.111.50	ruckus-access	richardhen-PC	richardhen-PC	17h 17m	165	802.11a/n	69.3%	99.03MB	6.94MB	1	6162	✓	✓
tse206	7363-cubio-mesh	00:26:5e:44:39:85	172.18.110.162	ro-wlan	SDC-ZeeHuang-PC	SDC-ZeeHuang-PC	1h 35m	6	802.11b/g	99.0%	17.16MB	1.02MB	1	1445	✗	✓
ruckus-access	RuckusAP	24:77:03:38:09:e8	172.18.110.171	ruckus-access	SDC-ZeeHuang-PC	SDC-ZeeHuang-PC	1h 23m	11	802.11g/n	99.0%	16.60MB	1.64MB	1	574	✗	✓
ruckus-access	RuckusAP	00:22:fb:ad:12:52	172.18.110.164	ruckus-access	Ann-PC	Ann-PC	1h 43m	165	802.11a/n	52.0%	6.11MB	716.67KB	1	0	✗	✓
ruckus-access	RuckusAP	00:24:d7:0d:0f:6c	172.18.110.114	ruckus-access	SDC-LARRY-PC	SDC-LARRY-PC	49m	11	802.11g/n	94.5%	9.89MB	751.10KB	1	13	✗	✓
ruckus-access	RuckusAP	00:24:d7:0c:06:94	172.18.110.149	ruckus-access	CherryYuang-PC	CherryYuang-PC	1h 15m	165	802.11g/n	71.8%	6.02MB	1.54MB	1	263	✗	✓
ruckus-access	RuckusAP	00:24:d7:36:af:40	172.18.112.107	ruckus-access	liuhuo-PC	liuhuo-PC	9h 23m	2	802.11b/g	88.7%	4.64MB	802.44KB	1	91	✗	✓
ruckus-access	RuckusAP	00:24:d7:35:f4:a4	172.18.112.89	ruckus-access	stevezheng-PC	stevezheng-PC	9h 59m	2	802.11b/g	86.6%	9.30MB	1.03MB	1	1611	✗	✓

Creating a Client View

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

1. Perform a search for clients through one of these search methods:
 - [Search Using the Client Search Criteria](#), or
 - [Search Using the Search Box](#)
2. When the search results appear, scroll down to the *Save as View* section.
3. In **View Name**, type a name that you want to assign to the view.
4. In **Description**, type a description for the view that you are saving. For example, if the view contains only clients with "PC" in the Host Name, you can enter **PC in Host Name**.
5. Click **Save**.

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

Figure 73. Creating a client view that consists of clients with PC in the Host Name

The screenshot shows the FlexMaster interface with the 'Save as View' dialog box open. The dialog box is highlighted with a red border and contains the following text:

Save as View

View Name:

Description:

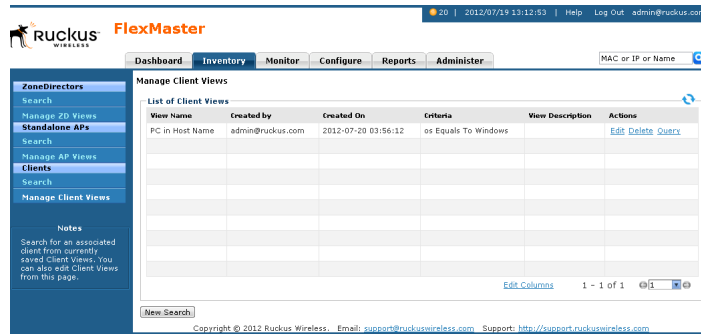
Below the dialog box, a table of client search results is visible. The table has the following columns: ZD Name, AP Name, Client MAC, Client IP Address, WLAN, Device Info, Host Name, Associated Time, Channel, Radio Type, Signal, Rx, Tx, Vlan, Retries, Connection, and Authentication. The table contains 10 rows of client data.

ZD Name	AP Name	Client MAC	Client IP Address	WLAN	Device Info	Host Name	Associated Time	Channel	Radio Type	Signal	Rx	Tx	Vlan	Retries	Connection	Authentication
ruckus-access	RuckusAP	00:24:d7:2e:ac:04	172.18.110.180	ruckus-access	SDC-Wind-PC	SDC-Wind-PC	2h 33m	165	802.11a/h	89.1%	6.28MB	82.02KB	1	19	✓	✓
ruckus-access	RuckusAP	24:77:03:2f:6c:60	172.18.112.113	ruckus-access	cherry-AP-01-PC	cherry-AP-01-PC	12h 34m	1	802.11g/n	69.3%	18.14MB	325.80KB	1	2688	✓	✓
ruckus-access	RuckusAP	00:22:fb:5c:fb:34	172.18.111.50	ruckus-access	edwardbu-PC	edwardbu-PC	17h 25m	165	802.11a/h	66.8%	99.26MB	6.94MB	1	6162	✓	✓
tsx206	7363-cubic-mesh	00:26:5e:44:39:95	172.18.110.162	rc-wlan	richardchen-PC	richardchen-PC	1h 35m	6	802.11b/g	99.0%	17.16MB	1.02MB	1	1445	✗	✓
ruckus-access	RuckusAP	24:77:03:38:09:e0	172.18.110.171	ruckus-access	SDC-Zoethuang-PC	SDC-Zoethuang-PC	3h 23m	11	802.11g/n	99.0%	16.60MB	1.84MB	1	574	✗	✓
ruckus-access	RuckusAP	00:22:fb:ad:12:52	172.18.110.114	ruckus-access	Ann-PC	Ann-PC	1h 43m	165	802.11a/h	52.0%	8.11MB	718.67KB	1	0	✗	✓
ruckus-access	RuckusAP	00:24:d7:06:0f:8c	172.18.110.114	ruckus-access	SDC-LARRY-PC	SDC-LARRY-PC	49m	11	802.11g/n	96.5%	9.89MB	751.10KB	1	13	✗	✓
ruckus-access	RuckusAP	00:24:d7:dc:06:84	172.18.110.149	ruckus-access	CherryYuang-PC	CherryYuang-PC	1h 15m	165	802.11a/h	71.8%	6.02MB	1.54MB	1	203	✗	✓
ruckus-access	RuckusAP	00:24:d7:36:af:40	172.18.112.187	ruckus-access	leishuo-PC	leishuo-PC	9h 23m	2	802.11b/g	86.6%	3.46MB	802.44KB	1	51	✗	✓
ruckus-access	RuckusAP	00:24:d7:35:ff:94	172.18.112.89	ruckus-access	stevezheng-PC	stevezheng-PC	9h 59m	2	802.11b/g	86.6%	9.30MB	1.03MB	1	1611	✗	✓

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

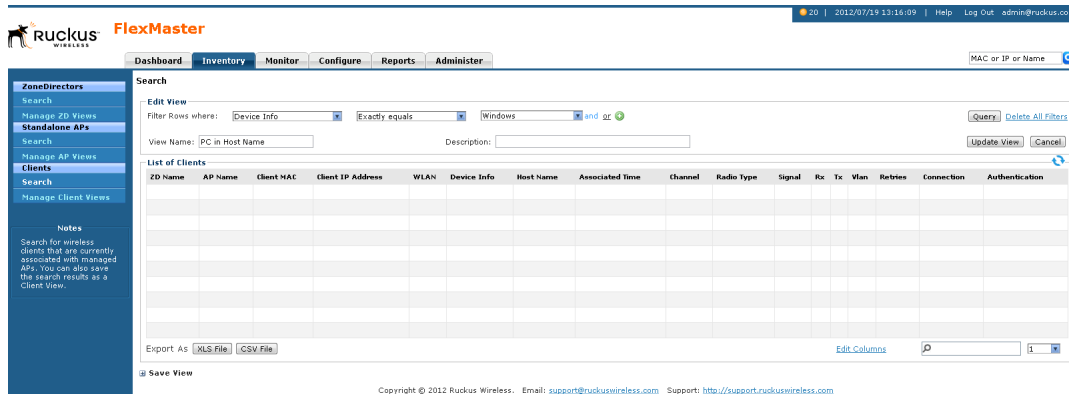


Editing a Client View

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

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



Deleting a Client View

1. Go to the **Inventory > Clients > Manage Client Views** page.
2. Look for the client view that you want to delete.
3. Click the **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.

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 76. 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 interface with the 'List of Clients' table. The table contains the following data:

ZD Name	AP Name	Client MAC	Client IP Address	WLAN	Device Info	Host Name	Associated Time	Channel	Radio Type	Signal	Rssi	Tx	Vlan	Metrics	Connection	Authentication
ruckus-access	RuckusAP	24:77:03:0f:6c:d0	172.18.112.113	ruckus-access	📶	cherry-AP-01-PC	12h 51m	1	802.11g/n	59.4%	18.48MB	330.43KB	1	2792	✓	✓
ruckus-access	RuckusAP	00:22:b9:5c:f5:34	172.18.111.50	ruckus-access	📶	edward@PC	17h 42m	165	802.11a/n	71.0%	99.96MB	6.99MB	1	5162	✓	✓
SDCFMQA_Redundant_3k_1	RuckusAP	00:26:cb:3c:99:12	192.168.22.124	SDC-FMQA_ZD3K_STD	📶	lenovo-e913sef	5h 35m	149	802.11a/n	98.0%	10.84MB	1.22MB	1	6	✓	✓
ruckus-access	RuckusAP	00:26:5e:44:39:04	172.18.110.145	ruckus-access	📶	jiangpw	1d 18h 58m	11	802.11b/g	99.0%	156.36MB	0.46MB	1	151861	✓	✓
SDCFMQA-ZD1100-IPV6only	RuckusAP	58:94:6b:24:62:f0	192.168.22.120	SDC-FMQA-ZD114v6_STD	📶	SDC-FREDDYCHEN	1h 51m	157	802.11a/n	84.2%	2.06MB	231.53KB	1	1	✓	✓
ruckus-access	RuckusAP	00:24:d7:2e:ac:d4	172.18.110.180	ruckus-access	📶	SDC-Wind-PC	2h 58m	165	802.11a/n	84.2%	6.84MB	87.03KB	1	22	✓	✓
ts6296	7363-oubo-mesh	00:26:5e:44:39:05	172.18.110.162	rw-lan	📶	richardchen-PC	1h 35m	6	802.11b/g	99.0%	17.16MB	1.02MB	1	1445	✗	✓
ruckus-access	RuckusAP	24:77:03:39:09:48	172.18.110.171	ruckus-access	📶	SDC-ZoeHuang-PC	3h 23m	11	802.11g/n	99.0%	16.60MB	1.84MB	1	574	✗	✓
ruckus-access	RuckusAP	00:22:fb:ad:12:52	172.18.110.164	ruckus-access	📶	Ann-PC	1h 43m	165	802.11a/n	82.0%	8.11MB	718.67KB	1	0	✗	✓
ruckus-access	RuckusAP	00:24:d7:0d:0f:8c	172.18.110.114	ruckus-access	📶	SDC-LARRY-PC	49m	11	802.11g/n	96.5%	9.89MB	751.10KB	1	13	✗	✓

Managing a Single Standalone Access Point

In This Chapter

Device View	122
Viewing Device Summary	125
Viewing and Editing Device Details	127
Performing Device Diagnostics	130



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

Device View

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



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



NOTE: To manage a Ruckus Wireless AP with FlexMaster, the management server URL must be configured on the AP. The default URL is <https://flexmaster/intune/server>. To change the URL, a provisioning template must be used. Another way to configure this URL is from the device's embedded Web management user interface. For more information, refer to [Ensuring That APs Can Connect to FlexMaster](#).

Figure 77. Clicking a standalone AP's serial number opens the AP Device View

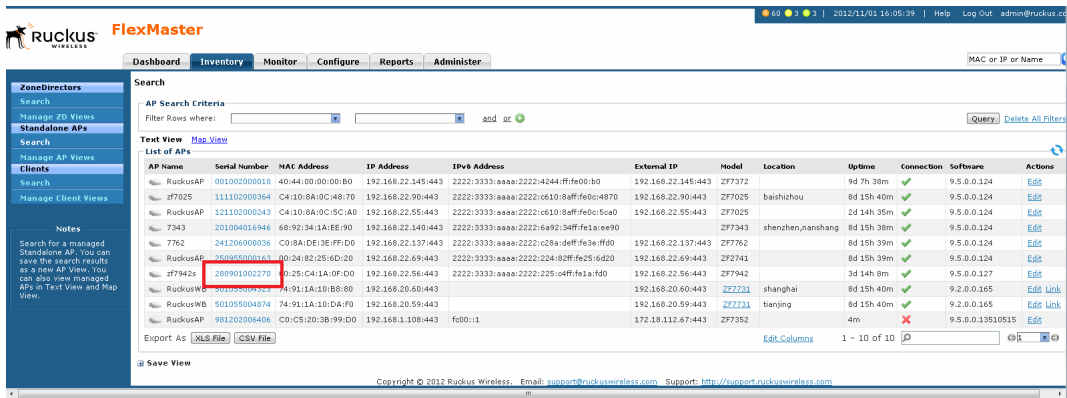
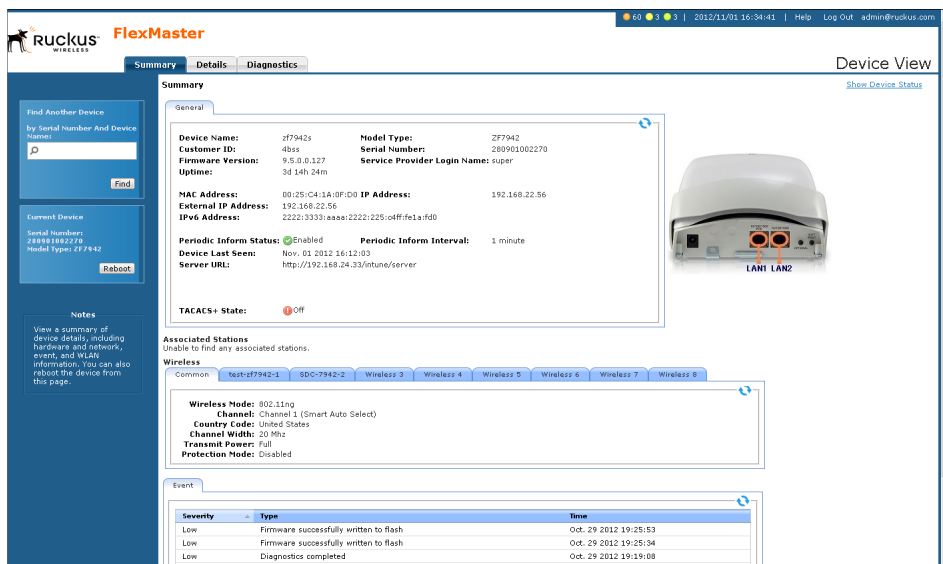


Figure 78. The AP Device View opens in a new browser window



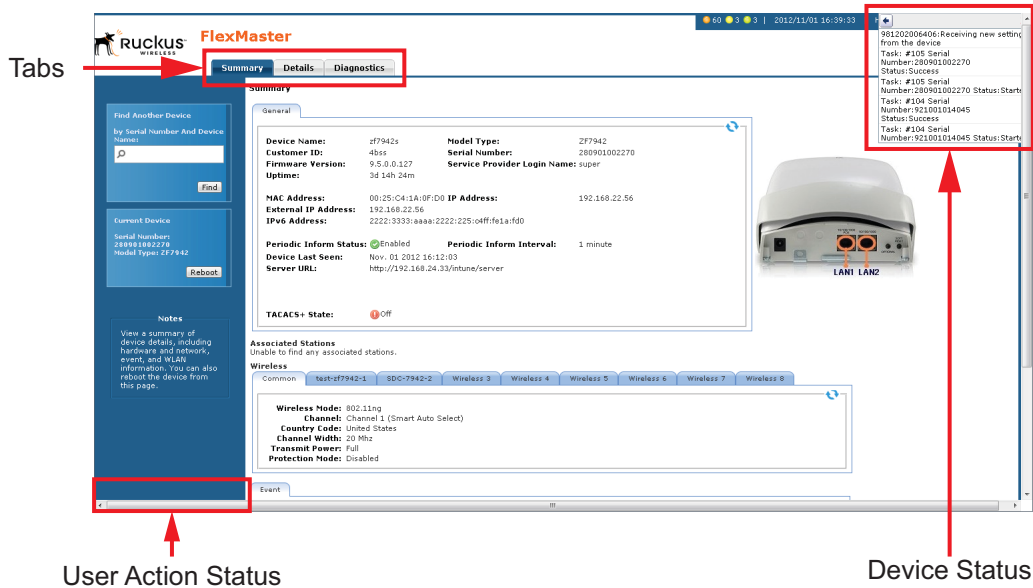
Device View Tabs and Status Boxes

The Device View contains three tabs that you can use to view information about the standalone AP, configure its settings, and run diagnostic tests on it. The following table lists the tabs that are available on the Device View. [Figure 79](#) shows the ZoneFlex 7942 Device View.

Table 19. Tabs on the Device View

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

Figure 79. ZoneFlex 7942 Device View



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

- 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 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.
- 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 shows if a matching device has been found.

Viewing Device Summary

The *Summary* tab offers a quick look at general details of the device, including a picture of the device, the device name, IP address, and available SSIDs. The following table lists the tasks that you can perform on the Summary tab. [Figure 80](#) and [Figure 81](#) show the ZoneFlex 7942 Device View Summary.

Table 20. Tasks you can perform on the Summary tab

Task	How To Do It
Find another device	In the <i>Find Another Device</i> box in the upper left corner of the page, type the serial number or MAC address of another device, and then click Find to find matching devices.
Reboot the device	Under <i>Current Device</i> , click Reboot to reboot the device.
View device details	(Default View) Shows a picture of the device model and high-level device details.
View device events	Clicking the Events tab opens a summary of device events.

NOTE: Some APs have two built-in radios. In those Summary pages, details are shown about two radios.

Figure 80. ZoneFlex 7942 Device View Summary tab, Part 1

The screenshot displays the Ruckus FlexMaster web interface. The top navigation bar includes 'Summary', 'Details', and 'Diagnostics' tabs. The main content area is titled 'Device View' and shows the following information:

- Find Another Device:** A search box with a 'Find' button.
- Current Device:** Shows 'Serial Number: 28981282279' and 'Model Type: ZF7942' with a 'Reboot' button.
- Summary:**
 - General:**
 - Device Name: zf7942s
 - Model Type: ZF7942
 - Customer ID: 4866
 - Serial Number: 28991002270
 - Firmware Version: 9.5.0.0.127
 - Service Provider Login Name: super
 - Uptime: 3d 14h 24m
 - MAC Address: 00:25:C4:1A:0F:D0
 - IP Address: 192.168.22.56
 - External IP Address: 192.168.22.56
 - IPv6 Address: 2222:3333:aaaa:2222::225:0aff:fe1a:f00
 - Periodic Inform Status: Enabled
 - Periodic Inform Interval: 1 minute
 - Device Last Seen: Nov. 01 2012 16:12:03
 - Server URL: http://192.168.24.33/intune/server
 - TACACS+ State: Off
 - Associated Stations:** Unable to find any associated stations.
 - Wireless:**
 - Wireless Node: 802.11ng
 - Channel: Channel 1 (Smart Auto Select)
 - Country Code: United States
 - Channel Width: 20 MHz
 - Transmit Power: Full
 - Protection Mode: Disabled
 - Event:**

Severity	Type	Time
Low	Firmware successfully written to flash	Oct. 29 2012 19:25:53
Low	Firmware successfully written to flash	Oct. 29 2012 19:25:34
Low	Diagnostics completed	Oct. 29 2012 19:19:00

Managing a Single Standalone Access Point

Viewing Device Summary

Figure 81. ZoneFlex 7942 Device View Summary tab, Part 2

Find Another Device
by Serial Number And Device Name:

Find

Current Device
Serial Number: 289861862778
Model Type: ZF7942

Reboot

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

General

Device Name: zf7942s	Model Type: ZF7942
Customer ID: 4bss	Serial Number: 280901002270
Firmware Version: 9.5.0.0.127	Service Provider Login Name: super
Uptime: 36 14h 24m	

MAC Address: 00:25:C4:1A:0F:DD **IP Address:** 192.168.22.56

External IP Address: 192.168.22.56

IPv6 Address: 2222:3333:aaaa::2222:225:0aff:fe1a:f60

Periodic Inform Status: Enabled **Periodic Inform Interval:** 1 minute

Device Last Seen: Nov. 05 2012 16:12:03

Server URL: http://192.168.24.25/mnuh/server

TACACS+ State: Off


Associated Stations
Unable to find any associated stations.

Wireless

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

Event

Severity	Type	Time
Low	Firmware successfully written to flash	Oct. 29 2012 19:25:53
Low	Firmware successfully written to flash	Oct. 29 2012 19:25:34
Low	Diagnostics completed	Oct. 29 2012 19:19:08
Low	Device recovers from disconnect state	Oct. 29 2012 02:55:34
Low	Device rebooted	Oct. 29 2012 01:49:50
Low	Firmware successfully written to flash	Oct. 29 2012 01:49:50
Low	Device rebooted	Oct. 29 2012 01:31:36
Low	Firmware successfully written to flash	Oct. 29 2012 01:31:36
Medium	Connectivity problem	Oct. 29 2012 02:00:01



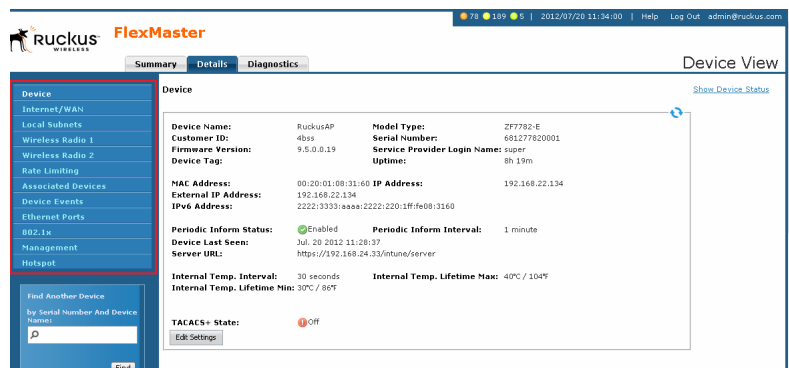
Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com

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 view-only static view of the details for that option. Click the **Edit Settings** button to edit option details.

Figure 82. Typical Details Menu Options



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

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

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



NOTE: Managed devices attempt to contact FlexMaster at the specified inform interval. If an AP is unable to contact FlexMaster after one hour, then it automatically extends the periodic inform interval by a random number of minutes. For example, if you set the inform interval to 5 minutes and the AP is unable to contact FlexMaster, it may extend the inform interval to 15 minutes. The AP continues to extend the interval until it is able to contact FlexMaster successfully (in which case the periodic inform interval reverts to the original setting) or it stops attempting to contact FlexMaster.



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

Figure 83. To change the device settings, click Edit Settings

The screenshot shows the FlexMaster web interface. The left sidebar contains navigation menus for Device, Internet/WAN, Local Subnets, Wireless, Rate Limiting, Associated Devices, Device Events, Ethernet Ports, 802.11e, Management, and Hotspot. The main content area is titled 'Device View' and shows configuration details for a device with ID '4b45'. The details include:

Device Name:	d77942s	Model Type:	ZF7942
Customer ID:	4b45	Serial Number:	2809631002270
Firmware Version:	9.5.0.0.127	Service Provider Login Name:	super
Uptime:	3d 15h 43m		
MAC Address:	00:25:C4:1A:0F:D0	IP Address:	192.168.22.56
External IP Address:	192.168.22.56		
IPv6 Address:	2222:3333:aaaa:2222::225::c4ff:fe1a:fd0		
Periodic Inform Status:	Enabled	Periodic Inform Interval:	1 minute
Device Last Seen:	Nov. 01 2012 17:31:30		
Server URL:	http://192.168.24.33/rtune/server		

At the bottom of the configuration details, there is a 'TACACS State' set to 'Off' and a red box highlighting the 'Edit Settings' link.



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

Configuring Replacement Options for ZoneFlex 7731 Wireless Bridge

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



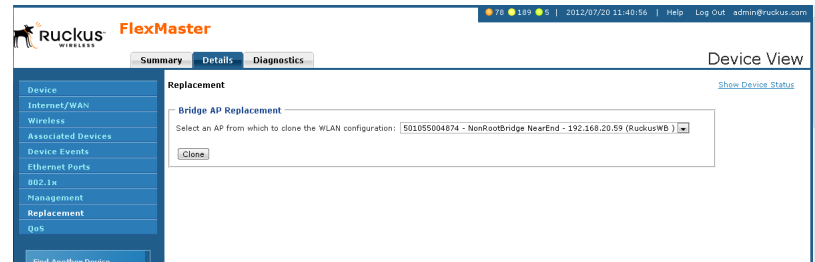
NOTE: This option is only available on the Device View of ZoneFlex 7731 Wireless Bridge.

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

1. Register the new ZoneFlex 7731 Wireless Bridge (replacement unit) with FlexMaster.
2. Access the Device View of the new ZoneFlex 7731 Wireless Bridge.
3. Click the **Details** tab, and then click the **Replacement** option on the left-side menu.
4. In *Select one AP to clone WLAN configurations*, select the wireless bridge that you are replacing.
5. Click **Clone**. FlexMaster queries its database for the settings of wireless bridge for replacement, and 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 84. The Replacement page for ZoneFlex 7731 Wireless Bridge



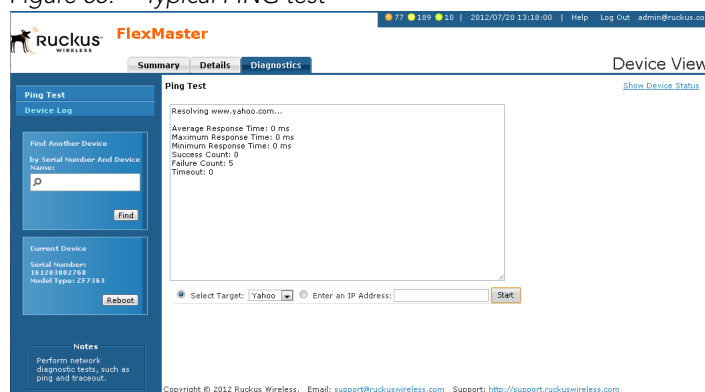
Performing Device Diagnostics

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. Ping the destination address by clicking **Start**. When the test is completed, FlexMaster displays the results in the *Ping Test* box.

Figure 85. Typical PING test

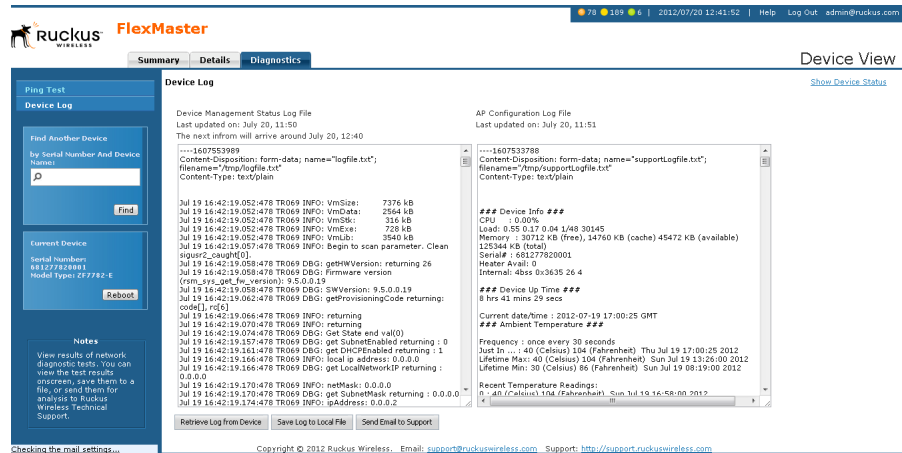


Viewing the Device Log

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

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

Figure 86. The Device Log page



FlexMaster retrieves two types of logs from the device:

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



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



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



NOTE: If a managed AP is behind a NAT server and you click the Retrieve Log from Device button, FlexMaster is able to retrieve the log from the managed AP only at the next inform interval. To determine if a managed AP is behind a NAT server, 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.*

Managing a Single Standalone Access Point

Performing Device Diagnostics

Provisioning Tasks to Managed Devices

In This Chapter

About Provisioning Tasks	134
Provisioning Tasks to Standalone APs	137
Provisioning Tasks to ZoneDirector Devices	164
Provisioning Common Tasks	178
Configuring VLAN and LAN Port Settings	196

About Provisioning Tasks

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

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

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

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

Provisioning Conventions and Recommended Practices

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

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



NOTE: When scheduling tasks, make sure that there is adequate time interval between tasks that target the same devices. For example, 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 fails or expires.

Understanding the Status of a Task

When you deploy a configuration upgrade, firmware upgrade, or reboot task, the task status appears in the task table, 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 can 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 see the following statuses (hyperlinks):

`8#Success 2#Failed`

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

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

Table 21. 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 Restart link under the Actions column.
Canceled	The scheduled task has been canceled.
Success	The task has completed successfully.
Failed	The task failed because these devices did not respond to FlexMaster. To see which target devices failed to complete the task, click the failed status link. To restart this task on the devices that failed, click the Restart link under the Actions column.

Provisioning Tasks to Managed Devices

About Provisioning Tasks

Figure 87. The task status column (in red box) on the Firmware Upgrade page

The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The left sidebar contains various configuration options like 'Standalone APs', 'ZoneDirectors', and 'Common'. The main content area is titled 'Firmware Upgrade' and contains a table with the following data:

ID	Task Name	Schedule	Created	Created by	Actions	Status
19	Upgrade Roxie Net to 9.4 GA	Perform now	Jun. 01 2012 10:53:24	dstiff@ruckus.com	Delete	1#Success
9	Eric SA 7962	Perform now	Apr. 26 2012 04:31:40	admin@ruckus.com	Delete	1#Success

Below the table, it indicates 'Number of tasks: 2' and provides a 'Create a task' button. A red box highlights the 'Status' column in the table, showing '1#Success' for both tasks.

Copyright © 2012 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 task (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 is 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.

1. Go to **Configure > Standalone APs > Config Templates**.
2. Click **Create a template**. The "Create a Template" configuration wizard opens at the bottom of the page.

Provisioning Tasks to Managed Devices

Provisioning Tasks to Standalone APs

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.

Figure 88. Select the check boxes for the options that you want to configure - Part 1

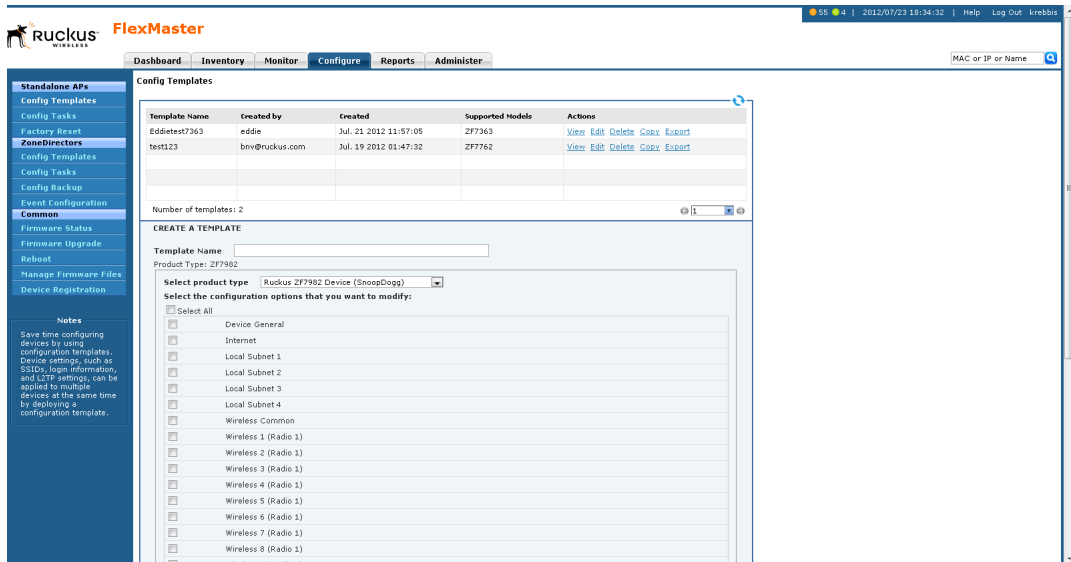


Figure 89. Select the check boxes for the options that you want to configure - Part 2



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](#).
 - For TACACS+ settings, refer to [Configuring Your Devices to Work with TACACS+](#).

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

Table 22. Configuration categories and example parameters

Category	Example Parameters
Device General	Device Name, Super User Name, Super User Password, TACACS+ State, Internal Heater, Temperature Update Interval
Internet	NTP Server, Management VLAN, Internet Connection Type, IP address, Mask, Gateway, DNS Server List, IPv6 settings, L2TP Tunnel
Local Subnet	Subnet, Access VLAN, Local IP Address, Subnet Mask, DHCP Server, Starting Address, Maximum DHCP Users
Wireless Common	Country Code, Wireless Radio Mode, Radio Channel Width, Channel, Radio Transmit Power, Radio Protection Mode, 5.8 GHz Channels, Data Rate, External Antenna Gain
Wireless setting (wireless bridge only)	Enable Pairing, Wireless Bridge Availability, Wireless Bridge Broadcast SSID, Wireless Bridge Name, Wireless Bridge SSID, Wireless Bridge Encryption Method, Country Code, Wireless Radio Mode, Radio Channel Width, Channel, Radio Transmit Power, Radio Protection Mode, Antenna
Wireless (number)	Wireless Availability, Broadcast SSID, Client Isolation, Name, SSID, RTS/CTS Threshold, Rate limiting, Encryption Method, Packet Forwarding, Hotspot Service, Access VLAN, Insert DHCP option 82, Client Fingerprinting
Management	SSH Access, HTTP/HTTPS Access, Telnet Access, Telnet Port, SSH Access, SSH Port, HTTP Access, HTTP Port, HTTPS Access, HTTPS Port, System Log Access, Log Server IP, Log Server Port, Remote Management Mode
Device Registration Settings	Server URL, Server Registration User Name, Server Registration Password, Periodic Inform Interval (for more on these settings, see Creating an AP Configuration Task)
QoS Global, Ethernet, and Wireless Configuration (wireless bridge only)	TOS settings, Dot1p settings, QoS settings
VLAN & LAN Port Settings	LAN port and WLAN settings, VLAN based QoS settings
802.1X Settings	LAN1 802.1X settings

Provisioning Tasks to Managed Devices

Provisioning Tasks to Standalone APs

Table 22. Configuration categories and example parameters

Category	Example Parameters
Hotspot Basic Settings, Walled Garden, MAC Address Pass-Through, Advanced Setting	Hotspot Service, UAM IP Address, Redirect URL, After Login, Primary RADIUS Server, Secondary RADIUS Server, RADIUS Shared Secret, Set Host List, Set MAC Address List, Login Retry Times, Blocked User URL, MAC Authentication, NAS ID, WISPr Location ID, WISPr Location Name, Location Description, Accounting Update Interval (minute(s)), Interim Redirection Frequency (minute(s)), Maximum Session Time (minute(s)), Grace Period (minute(s)), COA Port, Swap Input and Output Counters, Encode User Password, UAM Server Secret
LED Diagnostics	(per device)



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

Figure 90. Enter the values for the parameters that you want to modify

The screenshot shows the FlexMaster web interface. The main navigation bar includes Dashboard, Inventory, Monitor, Configure, Reports, and Administer. The left sidebar lists various configuration options for Standalone APs, including Config Templates, Factory Reset, Zone Directors, Config Tasks, Config Backup, Event Configuration, and Common. The 'CREATE A TEMPLATE' form is displayed, showing the following details:

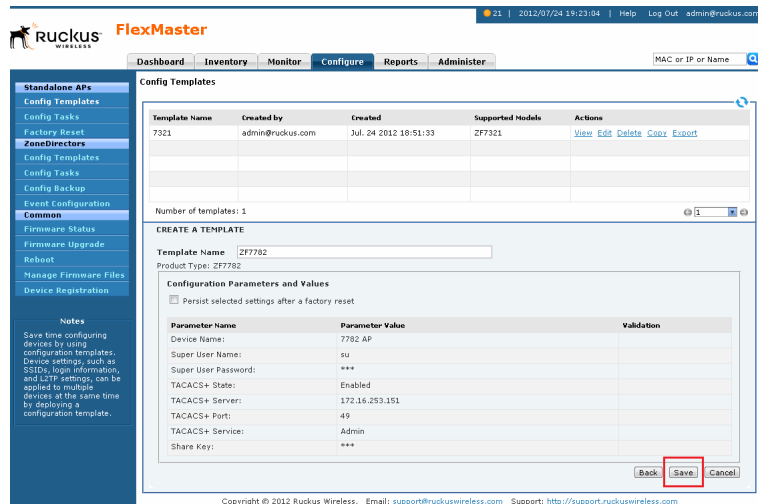
- Template Name: ZF7782
- Product Type: ZF7782
- Number of templates: 0
- Device General settings:
 - Parameter
 - Device Name: 7782 Outdoor AP
 - Super User Name: su
 - Super User Password: ***** (Confirmation)
 - TACACS+ State: Enabled Disabled
 - TACACS+ Server: 172.16.253.1
 - TACACS+ Port: 49
 - TACACS+ Service: ZD7782
 - Share Key: ***** (Confirmation)



NOTE: If you modify any of the values in the template or click any option or text box, then FlexMaster assumes that you want to change this parameter and automatically selects the check box in the Checked column.

6. Click **Next**.
 7. Depending on the check boxes you selected in [Step 5](#), selection and configuration parameters appear based on the category. Select the *Checked* column check box for a parameter and configure the value (for example, type an IP address or click an **Enable** button) for that parameter as part of the template. If the check box under the *Checked* column is not selected, then that parameter is not provisioned as part of the template.
 8. Click **Next** after each category selection and configuration.
 9. When you reach the *Configuration Parameters and Values* page, a summary of the configurations you have specified are displayed. If FlexMaster detected any errors, the corresponding fields are 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, then all attributes that are provisioned to one or more devices have precedence over the factory default settings, even if the device is reset to factory defaults. If this check box is cleared, then the parameters provisioned in this template reverts to factory defaults after a factory reset.
10. Click **Save** to save your configuration template.

Figure 91. Click **Save** to save the configuration template that you are creating



NOTE: After you click **Save**, if any of the values that you entered in the configuration template is invalid, then an error message appears under the Validation column. You need to correct invalid values before the template can be saved.

The only configuration template that does not provide the validation feature is the VLAN Settings template. This is because there is no way for FlexMaster to check if the VLAN settings you configured are correct. To view the status of a VLAN configuration template, check the Configuration Upgrade page.

Since multiple templates with varying attributes can be applied to a given device and the persist flag can be set on a per template basis, the last template that is applied overwrites the previous persist flag. Furthermore, if the same parameters are set in multiple templates, the value set in the last template takes precedence.

Viewing the Settings of an AP Configuration Template

1. Go to **Configure** > **Standalone APs** > **Config Templates**. A list of templates that you have created appears on the page.
2. Look for the 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

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 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

1. Go to **Configure > Standalone APs > Config Templates**. A list of templates that you have created appears on the page.
2. Look for the configuration template that you want to delete.
3. Click the **Delete** link that is in the same row as the template name. A confirmation message appears.
4. Click **OK**.

The page refreshes and the configuration task that you deleted disappears from the list.

Copying an AP Configuration Template

In addition to creating and editing configuration templates, you can also copy an existing template and save it under a different template name. This feature is useful when you want to apply a similar set of configuration settings to another group of devices. Note that when you copy or clone a template, you can only apply it to devices of the same model.

1. Go to **Configure > Standalone APs > Config Templates**. A list of templates that you have created appears on the page.
2. Look for the configuration template that you want to copy.
3. Click the **Copy** link that is in the same row as the template name. The Copy pane appears at the bottom of the page.
4. In **New template name**, type the name that you want to assign to the new configuration template.
5. Click **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

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”.

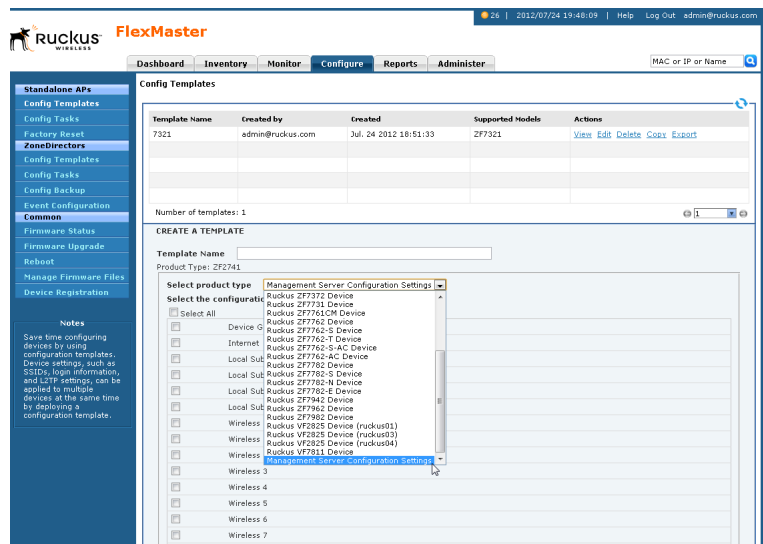
When configured, these settings are provisioned to *all* managed standalone APs, regardless of the product model.

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](#).

Follow these steps to create a management server configuration template.

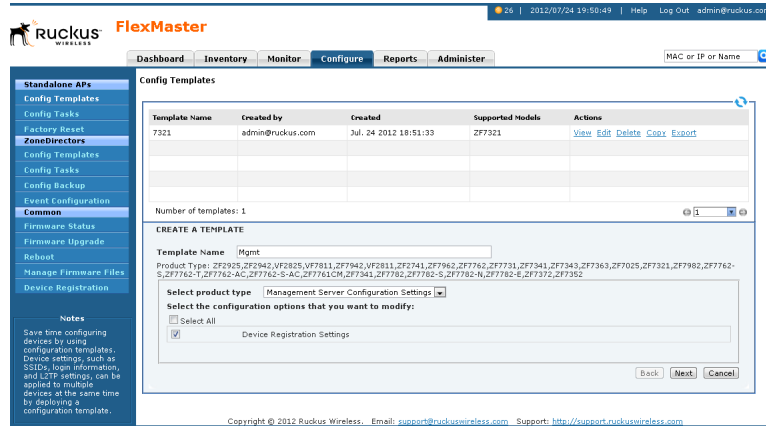
1. Go to **Configure > Standalone APs > Config Templates**.
2. Click **Create a template**. The *CREATE A TEMPLATE* configuration form appears at the bottom of the page.
3. In *Template Name*, type a name for the template that you are creating.
4. (Optional) Toggle the *Select product type* drop-down list to select the Management Server Configuration Settings option.

Figure 92. Select the target product type



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

Figure 93. Select Device Registration Settings



6. Click **Next**.

7. Under *Device Registration Settings*, change the required parameters.

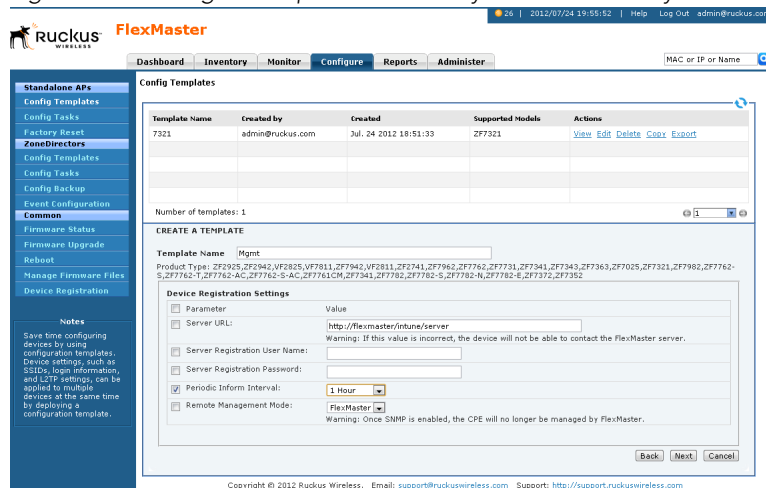
Table 23. Parameters included in registration settings

Parameter	Description
Server URL	Type the URL to FlexMaster's management service. The URL value must be a full URL starting with "http://" or "https://" followed by the FlexMaster server host name or IP address, and must end with "/intune/server". The default value is "http://flexmaster/intune/server".
Server Registration User Name	Type the user name for logging into the FlexMaster server
Server Registration Password	Type the password appropriate to the user name for logging into the FlexMaster server
Periodic Inform Interval	Select the time interval at which the device must synchronize with FlexMaster NOTE: The shortest inform interval that APs with 7.0 and later software support is one (1) minute, while APs with pre-7.0 software support five (5) minutes. If you set 1 minute as the periodic inform interval in your template, it is provisioned successfully to APs running on pre-7.0 software, but the interval that they use is 5 minutes (the shortest interval that they can support).

Table 23. Parameters included in registration settings

Parameter	Description
Remote Management Mode	<p>Select the remote management option that you want to apply to the device:</p> <ul style="list-style-type: none"> • AUTO to allow the device to be managed via SNMP or TR-69 (FlexMaster) • SNMP to allow only SNMP management • TR-69 to allow only FlexMaster management <p>NOTE: If you enable SNMP management, FlexMaster is no longer able to manage the device.</p>

Figure 94. Configure the parameters that you want to modify



8. Click **Next**.

Figure 95. Review your configuration settings, and then click Save

The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The left sidebar contains various menu items such as 'Standalone APs', 'Config Templates', 'Factory Reset', 'ZoneDirectors', 'Common', and 'Notes'. The main content area is titled 'Config Templates' and features a table with the following data:

Template Name	Created by	Created	Supported Models	Actions
7321	admin@ruckus.com	Jul. 24 2012 10:51:33	ZF7321	View Edit Delete Copy Export

Below the table, there is a 'CREATE A TEMPLATE' section with a form. The 'Template Name' field contains 'Nght'. The 'Product Type' field contains a long alphanumeric string. The 'Configuration Parameters and Values' section includes a checkbox for 'Persist selected settings after a factory reset' and a table with the following data:

Parameter Name	Parameter Value	Validation
Periodic Inform Interval:	1 Hour	

At the bottom of the form, there are 'Back', 'Save', and 'Cancel' buttons. The footer of the page contains copyright information for Ruckus Wireless.

9. After saving the template, create an AP configuration task that provisions 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 can manage many Ruckus Wireless devices, creating configuration upgrade tasks consolidates necessary configurations across one or more devices as defined by a device view.

AP Configuration Upgrade tasks require a configuration template that specifies the settings to be updated. Since configuration templates are specific to a product model, it is possible that not all devices in a device view are provisioned based on product model. For example, if you grouped multiple devices according to their common location (for example, Los Angeles, CA) and called that view "LA Devices", and the view consisted of three ZF 7942s and two VF 2825s, then you need to create two (or more) separate configuration templates and configuration upgrade tasks to configure all of the devices in the view.



WARNING! Deploying a template that changes the device's country code or 802.11 radio mode settings causes the Ruckus Wireless device to reboot. The reboot may take up to two minutes. Ruckus Wireless recommends applying such configuration changes during periods when service level agreement (SLA) downtime is permitted.



NOTE: Before you create a configuration upgrade task, you need to create a configuration template. To create a configuration template, refer to [Creating an AP Configuration Template](#).

Creating an AP Configuration Task

An AP configuration task enables FlexMaster to deploy a configuration template that you have already created.



NOTE: Configuration, firmware, reboot, and factory reset tasks cannot be deleted. Tasks that have not yet started, however, can be cancelled, although they remain in the FlexMaster database. By keeping all of the user actions in the database, FlexMaster can produce accurate audit logs of system configuration activities.

1. Go to **Configure > Standalone APs > Config Tasks**.
2. Click **Create a task**. The *Create Task* form appears at the bottom of the page.
3. In the *Task Settings* section, do the following:
 - In *Specify a task name*, type a name that you want to assign to this configuration upgrade task.
 - In *Select a configuration template*, select the configuration template that you want to use. If you want to view the parameters and settings that are included in the configuration template, select the template, and then click the View Parameters link.

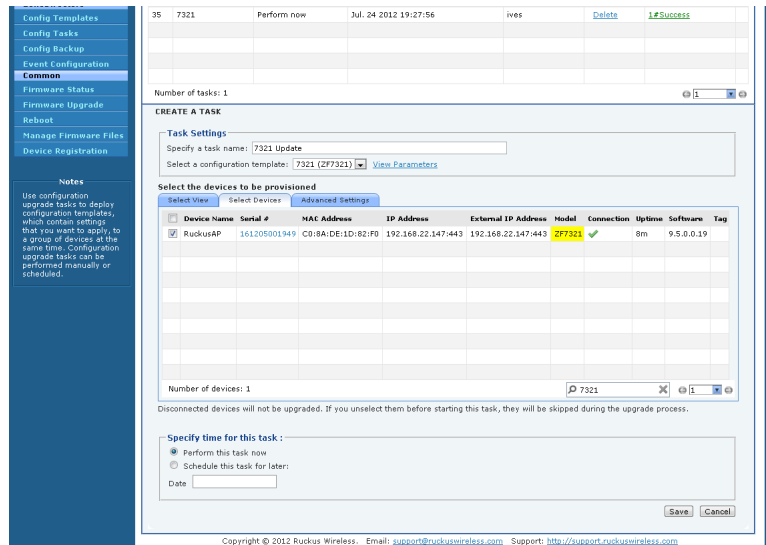
4. In **Select the devices to be provisioned**, choose the target devices.
 - To apply the selected configuration template to all standalone APs, select **All Standalone APs**.
 - To apply the selected configuration template to an existing AP view, select the **AP View** name.

Note that if the template is model-specific, then the settings in the template are only applied to devices that match the model.

 - To apply all settings in the configuration template to a device group or to specific devices,
 - Click the **Select Devices** tab.
 - In the **Select Devices** tab, search for and select the target devices.

Note that if the template is model-specific, then the settings in the template are only applied to devices that match the model.

Figure 96. Selecting the configuration template and target devices



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

- To apply different parameter settings to target devices, click the **Advanced Settings** tab, and then do the following:
 - In *Serial Number*, enter the serial number of the device that you want to configure.

- Select the check boxes for the parameters that you want to configure for the device, and then configure the settings.
For example, if the configuration template includes IP address settings and you want to assign the IP address 192 . 68 . 100 . 13 to this device, select the *IP Address* check box, and then type 192 . 68 . 100 . 13 in the box provided.
 - Click the **Add** link to add this configuration to the task.
NOTE: Clicking Add does not save the task itself. To save the configuration upgrade task, after you done configuring the task, click the *Save* button at the bottom of the page.
 - Repeat these steps for each device that you want to configure.
5. In **Specify time for this task**, specify when you want the task to run.
 - To run the task immediately, click **Perform this task now**.
 - To schedule the task, click **Schedule this task for later**, and then enter the date and time.
 6. Click **Save** to save the configuration upgrade task.



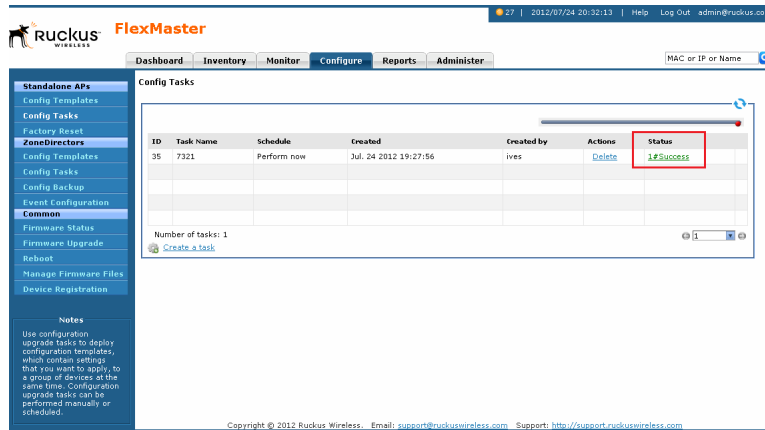
NOTE: If FlexMaster detects a problem in the configuration upgrade task that you are saving, an error message appears.

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

Viewing the Status of an AP Configuration Upgrade Task

1. Go to **Configure > Standalone APs > Config Tasks**. A list of upgrade tasks that you have created appears on the page.
2. Look for the upgrade task for which status you want to view.
3. 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.
 - *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 can appear under the **Status** column. For a complete list of all statuses, see [Understanding the Status of a Task](#).

Figure 97. Viewing the status of a configuration upgrade task

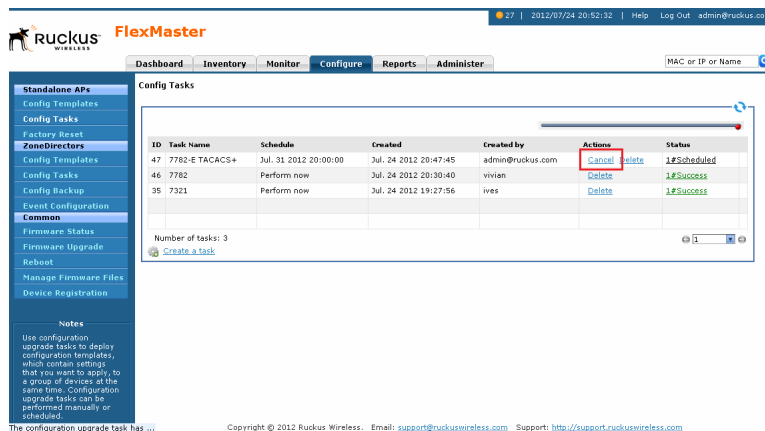


Canceling a Scheduled Configuration Upgrade Task

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

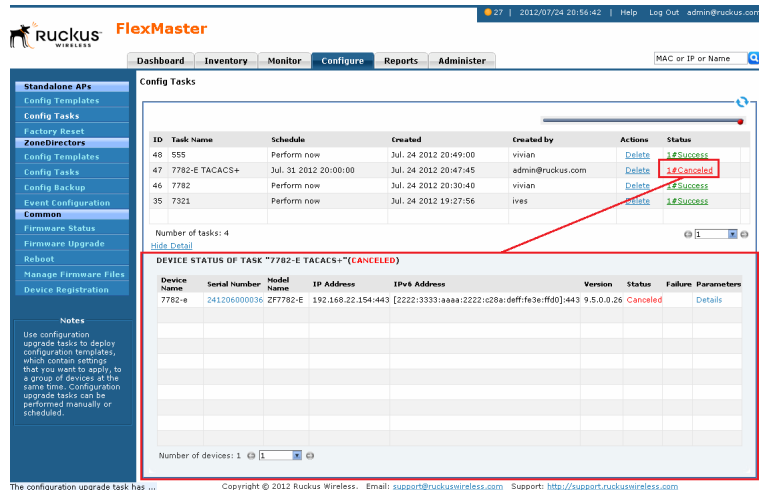
1. Go to **Configure > Standalone APs > Config Tasks**.
2. Locate the upgrade task you want to cancel in the *Config Tasks* table.
3. Click **Cancel** under the *Actions* column.

Figure 98. 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 "Canceled" in the *Status* column.
5. Click the **Canceled** link for the canceled upgrade to view all task details.

Figure 99. Viewing details of the canceled task

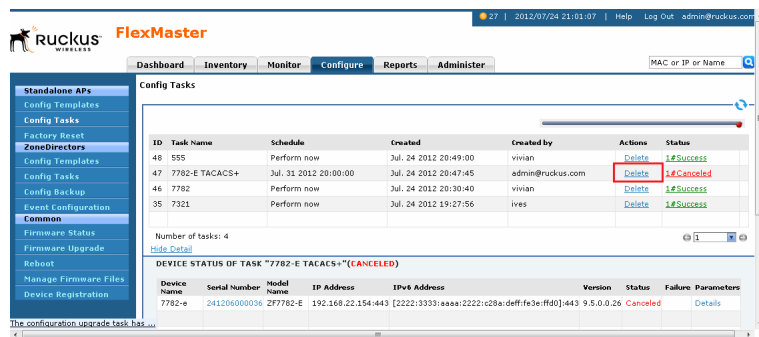


Deleting a Configuration Upgrade Task

1. Go to **Configure > Standalone APs > Config Tasks**.
2. Locate the task you want to delete.
3. Click the **Delete** link that is in the same row as the task name. A confirmation message appears.
4. Click **OK** to delete the scheduled task.

The page refreshes, and then the task that you deleted disappears from the list of configuration upgrade tasks.

Figure 100. Click Delete to delete the configuration upgrade task



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 are not affected by the restart task option.

1. Go to **Configure > Standalone APs > Config Tasks**.
2. Locate the task you want to restart.
3. Click the **Restart** link that is in the same row as the task name. A confirmation message appears.
4. Click **OK** to restart the task.

The page refreshes and the Status column for the task shows *Started*.



NOTE: In addition to restarting a single task manually, FlexMaster provides a way to automatically restart all failed tasks. To configure this setting, go to **Administer > System Settings**, and then click the **Yes** option in Task Restart Services.

Performing an AP Factory Reset

The Factory Reset option resets devices to their factory defaults, immediately or at the specified time. Resetting to factory defaults may be necessary when repurposing devices, thus requiring a new configuration for each device. A reset causes a reboot; thus, the devices go out of service for a period of time (approximately one to two minutes).

Note that FlexMaster can reset APs to factory defaults, but not ZoneDirector devices. This is because resetting ZoneDirector to factory defaults affects all APs that are connected to it and may cause parts of (if not the entire) network to go offline.



WARNING! If you changed the Management Server Configuration Settings (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 erases all configuration settings, except those that you chose to make persistent. When you create a new configuration template, you can make the settings in the template persistent by selecting the *Persist selected settings after a factory reset* check box. For more information, refer to [Creating an AP Configuration Task](#).

Creating an AP Factory Reset Task

1. Go to **Configure > Standalone APs > Factory Reset**.
2. Click **Create a task**. The *Create A Task* form appears at the bottom of the page.
3. In *Specify a task name*, type a name for your reboot task.
4. If you want this task that you are creating to reset all settings on the target devices to factory default, including those settings that have been made persistent, select the *Clear post factory persistent configuration changes* check box.
5. Select the *Reboot device after Factory Reset* check box to reboot all group devices after sending the factory reset task. A reboot is required to complete the factory reset process, therefore Ruckus Wireless recommends selecting this check box.
6. Under *Select a view of devices to perform factory default*, select the target devices. Do one of the following:
 - On the **Select View** tab, select an existing device view.
 - On the **Select Devices** tab, select the check box for each device that you want to reset to factory default.
7. Under *Specify a time to perform this task*, click when you want to perform this task:
 - **Perform this task now:** Run the task immediately after clicking **Save**.
 - **Schedule this task for later:** Specify the Date (yyyy-mm-dd) and Time (hh:mm:ss [AM|PM]) on which the task should run.
8. Click **Save**.

Figure 101. Creating a factory reset task

Factory Reset

- Zones/Devices
- Config Templates
- Config Tasks
- Config Backup
- Event Configuration
- Common**
- Firmware Status
- Firmware Upgrade
- Reboot
- Manage Firmware Files
- Device Registration

Notes

Create a factory reset task to reset a group of devices to factory default settings at the same time. Factory reset tasks can be performed manually or scheduled. **WARNING!** Resetting a device to factory default will erase all device settings that you have previously configured.

ID	Task Name	Schedule	Created	Created By	Actions	Status

Number of tasks: 0

CREATE A TASK

Task Settings

Specify a task name: 7782-E Reset

Clear post factory persistent configuration changes

Reboot device after factory reset

Select a view to reset to factory default:

Select View: [Select Devices](#)

Select a view of devices to perform factory reset: 7782 [View Details](#)

Device Name	Serial #	MAC Address	IP Address	External IP Address	Model	Connection	Uptime	Software	Tag
7782-e1	241206000036	C0-8A-DE:9E:FF:D0	192.168.22.154-443	192.168.22.154-443	ZF7782-E	X	1m	9.5.0.0.26	

Number of devices: 1

Specify a time to perform this task:

Perform this task now

Schedule this task for later:

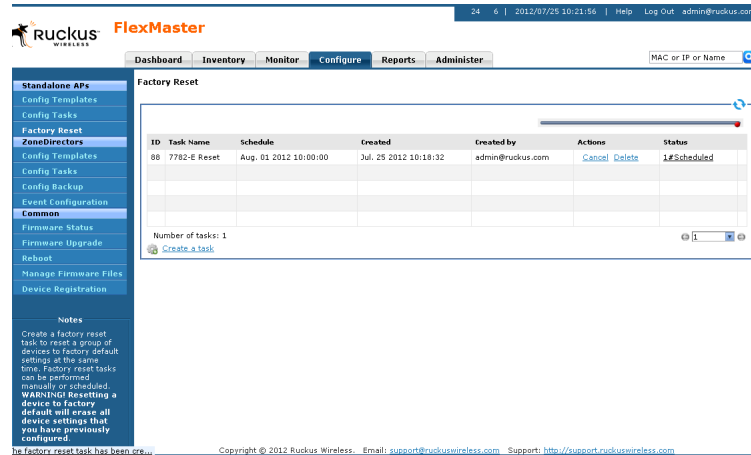
Date: 2012-08-01 10:00

[Save](#) [Cancel](#)

Viewing Existing AP Factory Reset Tasks

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

Figure 102. The *Factory Reset* page lists that factory reset tasks that have been created



Canceling an AP Factory Reset Task

1. Go to **Configure > Standalone APs > Factory Reset**. The *Factory Reset* page displays the factory reset tasks that have been created.
2. Look for the factory reset task that you want to cancel, and then click the **Cancel** link that is in the same row as the task name. A confirmation dialog appears.
3. Click **OK** to continue.

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

Deleting an AP Factory Reset Task

1. Go to **Configure > Standalone APs > Factory Reset**. The *Factory Reset* page displays the factory reset tasks that have been created.
2. Look for the factory reset task that you want to delete, and then click the **Delete** link that is in the same row as the task name. A confirmation dialog appears.
3. Click **OK** to continue.

The page refreshes, and then the task disappears from the *Factory Reset* table. You have completed deleting the AP factory reset task.

Creating an Auto Configuration Task

New devices that are registering with FlexMaster can also be automatically provisioned with settings preconfigured by the administrator for a specific group of devices (for example, all ZoneFlex 2942 devices). Auto configuration enables you to ensure that newly registered devices can be made operational immediately, without having to wait for you to configure them.

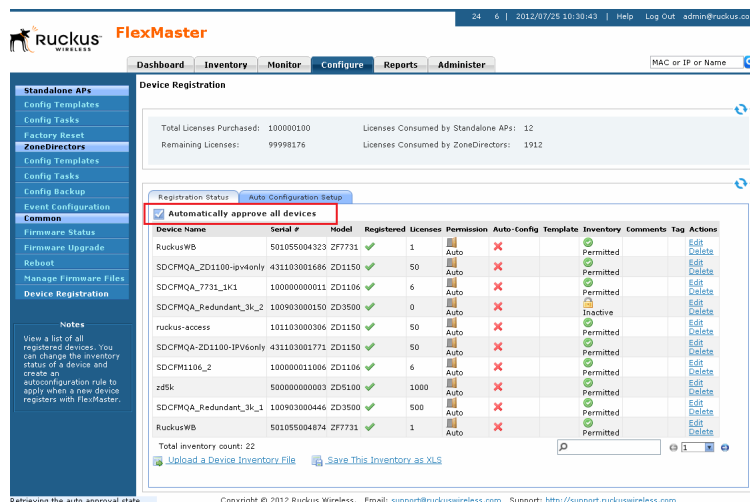
Note that auto configuration is only for devices that have not registered with FlexMaster. When a device is already registered with FlexMaster, its settings are not updated by the auto configuration task, even if it is part of the target device view for auto configuration.

Step 1: Before You Begin

Before creating an auto configuration task, verify that device registration is set to Auto (this is the default setting). Follow these steps to check if device registration is set to auto approve.

1. Go to **Configure > Common > Device Registration**.
2. 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 enable automatic approval of devices.

Figure 103. Verify that device registration is set to Auto



If you intentionally disabled automatic device registration, then you can still run auto configuration tasks, but you need to list the devices that you want to auto configure in an inventory file. For instructions on how to create an inventory file, refer to [Option 2: Upload an Inventory File of Devices to Auto Configure](#).

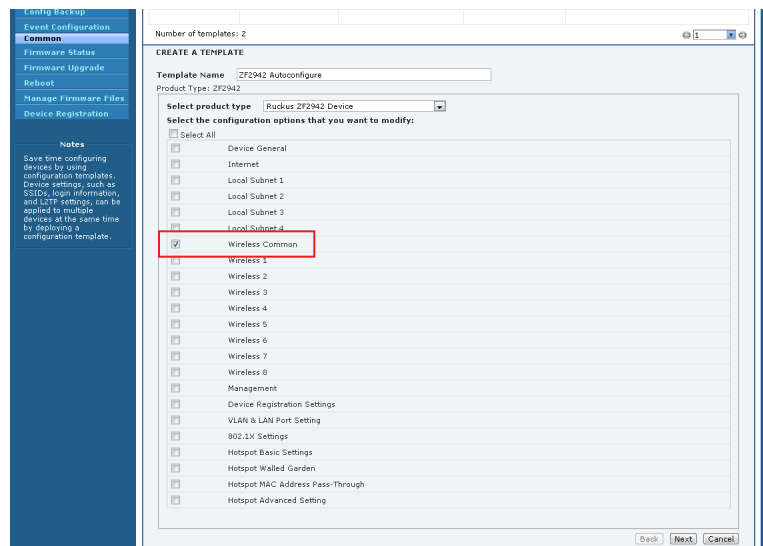
Step 2: Create a Configuration Template

Create a configuration template that defines the settings that you want to provision to new devices. For more information on creating templates, refer to [Creating an AP Configuration Template](#).

For example, if you want to auto configure the Wireless Common settings of all ZoneFlex 2942 access points that register with FlexMaster:

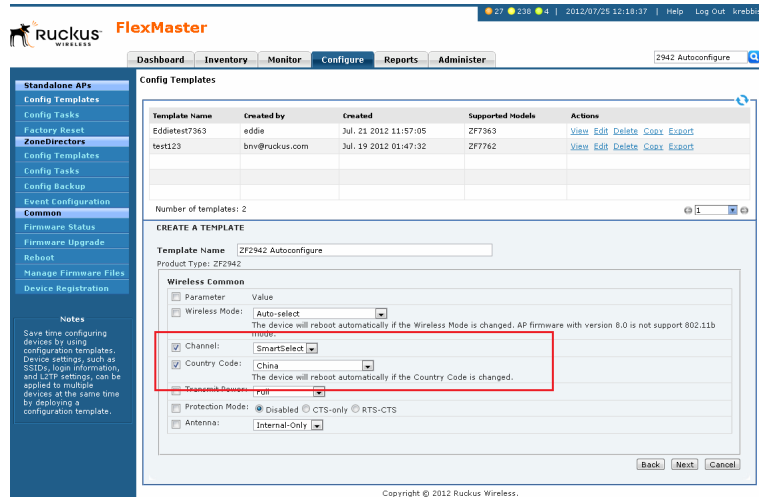
1. Go to **Configure > Standalone APs > Config Templates**.
2. Click **Create a template**. The *Create a Template* configuration wizard opens at the bottom of the page.
3. In *Template Name*, type a name for the template, such as **2942 Autoconfigure**.
4. Select **Ruckus ZF2942 Device** in *Select product type*.
5. Select the **Wireless Common** check box ([Figure 104](#)) when you create it.

Figure 104. Example: Creating a basic Wireless Common auto configuration template for ZoneFlex 2942 access points



6. Click **Next**. FlexMaster displays the *Create a Template Wireless Common* page.

Figure 105. Example: Enter the Wireless Common values for the parameters that you want to auto configure



NOTE: When you are creating a configuration template that includes wireless radio settings, make sure that the radio channel you select is authorized in your country. To ensure that you are using an authorized radio channel, select the correct Country Code for the location in which you operate the access points, and then select **SmartSelect** for the channel.



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

7. Click **Next**.
8. When you reach the *Configuration Parameters and Values* page, a summary of the configurations you have specified are displayed. If FlexMaster detected any errors, the corresponding fields are flagged in red.

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

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

Step 3: Define the Target Devices for Auto Configuration

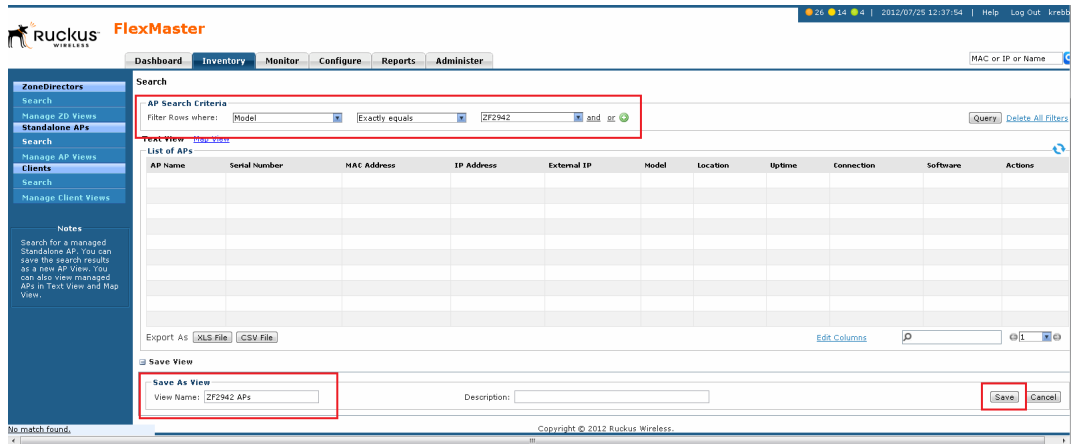
The next step is to specify the devices that are automatically configured when they register with FlexMaster. You can either create a device view and use that as the target group for auto configuration, or upload an inventory file that lists the target devices.

Option 1: Search and Save As a Device View

The easiest way to create a device view is to perform a search based on a specific attribute, and then save the search results as a device group. For example, 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 select this name as the target view later when you create an auto configuration task.

Figure 106. Running a search for ZoneFlex 2942 devices



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

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 need to upload an inventory file for FlexMaster to auto configure devices.

Follow these steps to create and upload an inventory file.

1. Open a blank Microsoft Excel sheet.
2. In Column A, type the serial numbers of all Ruckus Wireless devices that you want to include in the inventory file.
3. In Column B, assign a tag to each device in the list. These tags function as the group names for the devices in the list.

Figure 107. Sample inventory file

	A	B
1	999789098765	880 W. Maude Ave, Sunnyvale, CA
2	888960533566	Rome, Italy
3	777576467888	New York, NY
4	555432109876	Los Angeles Region Access Points
5	677576467823	San Jose, CA

4. Save the file in .XLS format.
5. On the FlexMaster Web interface, go to the **Configure > Common > Device Registration** page.
6. On the *Registration Status* tab, click the **Upload a Device Inventory File** link at the bottom of the page.
7. In *Pre-Registration Data*, click **Choose File**.
8. Go to the location of the inventory file (in .XLS format) that you saved earlier, and then click **Open**.
9. Click **OK**.

The Web interface refreshes and a message appears at the top of the page, informing you that the inventory file has been uploaded successfully. The tags that you assigned to each device appear under the **Auto-Config** column on the *Registration Status* tab.

Step 4: Create the Auto Configuration Task

1. Go to the **Configure > Common > Device Registration** page.
2. On the **Device Registration** page, click the **Auto Configuration Setup** tab.
3. Click **Create a rule**.
4. In **Enter an AutoConfiguration Name**, type a name that you want to assign to the auto configuration task.
5. In **Device View**, select the device view to which you want to deploy the auto configuration task. Options include the default device view, *All Standalone APs*, as well any device views you have created. If you uploaded an inventory file, 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:

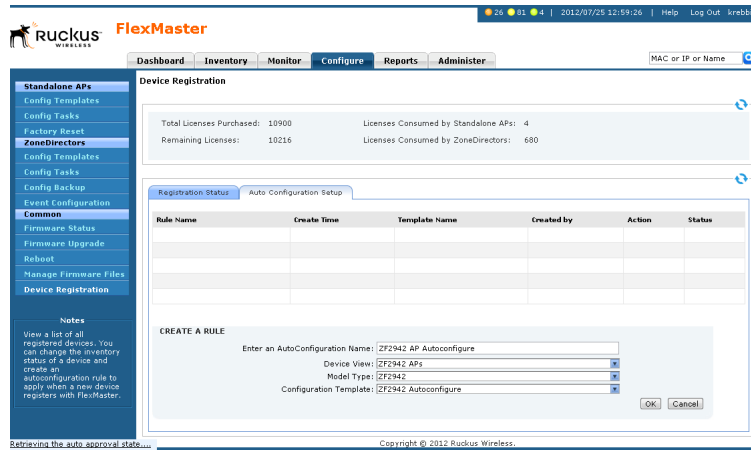
- VF2811 (MediaFlex 2811 Adapter)
- VF2825 (MediaFlex 2825 AP)
- VF7811 (MediaFlex 7811 Adapter)
- ZF2741 (ZoneFlex 2741 Outdoor AP)
- ZF2925 (ZoneFlex 2925 802.11g AP)
- ZF2942 (ZoneFlex 2942 802.11g AP)
- ZF7025 (ZoneFlex 7025 Multiservice 802.11n Wired/Wireless Wall Switch)
- ZF7321 (ZoneFlex Smart Dual-Band Selectable 802.11n Access Point)
- ZF7341 (ZoneFlex 7341 2.4GHz 802.11n Smart Wi-Fi AP)
- ZF7341-U (ZoneFlex 7300 Series Dual Band 802.11n Indoor AP with USB)
- ZF7343 (ZoneFlex 7363 802.11n Indoor Single-Band AP)
- ZF7343-U (ZoneFlex 7300 Series Dual Band 802.11n Indoor AP with USB)
- ZF7352 (ZoneFlex 7352 Indoor Single-Band AP)
- ZF7363 (ZoneFlex 7363 802.11n Indoor Dual-Band AP)
- ZF7363-U (ZoneFlex 7300 Series Dual Band 802.11n Indoor AP with USB)
- ZF7372 (ZoneFlex 7372 Indoor Dual-Band AP)
- ZF7731 (ZoneFlex 7731 802.11n Bridge AP)
- ZF7761-CM (ZoneFlex 7761-CM Cable Modem AP)
- ZF7762 (ZoneFlex 7762 802.11n Outdoor AP)
- ZF7762-AC (ZoneFlex 7762-AC 802.11n Outdoor AP)
- ZF7762-N (ZoneFlex 7762-N 802.11n Outdoor AP)
- ZF7762-S (ZoneFlex 7762-S 802.11n Outdoor Sector AP)
- ZF7762-S-AC (ZoneFlex 7762-S-AC 802.11n Outdoor Sector AP)
- ZF7762-T (ZoneFlex 7762-T Dual Band 802.11n Outdoor AP)
- ZF7942 (ZoneFlex 7942 Smart Wi-Fi 802.11n AP)
- ZF7962 (ZoneFlex 7962 Dual-Band 802.11n Smart Wi-Fi AP)
- ZF7982 (ZoneFlex 7982 Dual-Band 802.11n Smart Wi-Fi AP)

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 are unable to save the auto configuration task.

Figure 108. Creating an auto configuration task for ZoneFlex 2942 access points



8. Click **OK**.

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

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



- To view the task status, click the **View** link on the Device Registration page.
- To stop the task, click the **Stop** link. The page refreshes, and the task status changes to *Cancelled*. To start the task again, click the **Restart** link.
- To delete the task, click the **Delete** link. The page refreshes, and the task status changes to *Cancelled*. To start the task again, click the **Restart** link.

You have completed creating an auto configuration task. To create another auto configuration task (for example, for a different device view or with a different set of settings), repeat the same procedure.

How to Tell Which Devices Were Auto Configured

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-Config* column shows two types of icons that indicate the auto registration status of a device:

-  means auto configured
-  means not auto configured

If a template was used to auto-configure a device, then the Template Name appears in the *Template* column.

Provisioning Tasks to ZoneDirector Devices

This section describes how to create ZoneDirector configuration templates and provision these to ZoneDirector devices. It also describes how to back up ZoneDirector settings and restore them to the original ZoneDirector device or another ZoneDirector device of the same model.

Working with ZoneDirector Configuration Templates

ZoneDirector configuration templates 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 provision with a template, standby ZoneDirector devices are automatically filtered from the list. Once the active ZoneDirector device is provisioned, it automatically synchronizes its settings with the standby ZoneDirector device.

Creating a ZoneDirector Configuration Template



NOTE: Before creating a ZoneDirector configuration template, you must have saved at least one configuration file for the target ZoneDirector. For information on how to back up ZoneDirector configuration, see [Immediately Backing Up ZoneDirector Configurations](#).

1. Go to **Configure > ZoneDirectors > Config Templates**.
2. Click **Create a template**. The *CREATE A TEMPLATE* configuration form opens at the bottom of the page.
3. In *Template Name*, type a name for the configuration template that you are creating.
4. In *ZoneDirector Backup Configuration*, select a backup configuration that you use as base configuration for the template that you are creating. You need to make modifications to the backup configuration to create your ZoneDirector configuration template.
5. Click **Next**. FlexMaster displays the *WLANs*, *Access Point Policies*, *Hotspot Services*, *AAA Servers*, and *System* tabs.
6. Under each of the *WLANs*, *Access Point Policies*, *Hotspot Services*, *AAA Servers*, and *System* tabs, make required changes to the device parameters. After making changes, click **Apply** or **OK** to save your changes to the template.



NOTE: For instructions on how to configure the ZoneDirector settings (for example, WLAN settings), refer to the *ZoneDirector User Guide* or *ZoneDirector Online Help*.

7. After you have made all required changes, click **Save** to finish creating the ZoneDirector configuration template.

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

Editing a ZoneDirector Configuration Template

1. Go to **Configure > ZoneDirectors > Config Templates**. A list of templates that you have created appears on the page.
2. Click the ZoneDirector configuration template **Edit** link. The *EDIT* pane appears at the bottom of the page, displaying the *WLANs*, *Access Point Policies*, *Hotspot Services*, *AAA Servers*, and *System* tabs.
3. Under each of the *WLANs*, *Access Point Policies*, *Hotspot Services*, *AAA Servers*, and *System* tabs, make changes to the device parameters as required. After making changes, click **Apply** or **OK** to save your changes to the template.



NOTE: For instructions on how to configure the ZoneDirector settings (for example, WLAN settings), refer to the *ZoneDirector User Guide* or *ZoneDirector Online Help*.

4. After you have made all required changes, click **Save** to finish creating the ZoneDirector configuration template.

Deleting a ZoneDirector Configuration Template

1. Go to **Configure > ZoneDirectors > Config Templates**. A list of templates that you have created appears on the page.
2. Click the ZoneDirector configuration template **Delete** link. A confirmation message appears.
3. Click **OK**.

The page refreshes, and the configuration task that you deleted disappears from the list.

Working with ZoneDirector Event Configuration

Managed ZoneDirector devices generate a significant number of events, which makes the task of monitoring critical ZoneDirector events challenging. To ensure that you are notified about ZoneDirector events that are critical to your organization, you can define the events that you want to show on the Events widget on the Dashboard.

Creating a ZoneDirector Event Configuration

A ZoneDirector event configuration named *Default Event Configuration* exists. This default event configuration includes all important ZoneDirector events 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.

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 event type tabs, and then select the check boxes for the ZoneDirector events that you want to include in the new event configuration.
5. Click **Save**. The event configuration that you created appears in the Event Configuration table.

You have completed creating a new ZoneDirector event configuration. To apply this event configuration to ZoneDirector devices, refer to [Assigning an Event Configuration to ZoneDirector Devices](#).

Figure 109. The New Event Configuration form appears at the bottom of the page

ID	Configuration Name	Created On	Created By	Action
1	Default Event Configuration	Jul 30 2012 16:04:10	admin@ruckus.com	Assign ZDs

New Event Configuration

New Event Configuration Name:

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

Event Type	Description
<input type="checkbox"/> AP speedflex to AP	SpeedFlex: AP{{ap}} to AP{{apto}} - downlink {{downlink}} uplink {{uplink}}
<input type="checkbox"/> AP speedflex to AP downlink	SpeedFlex: AP{{ap}} to AP{{apto}} - downlink {{downlink}}
<input type="checkbox"/> AP speedflex to AP uplink	SpeedFlex: AP{{ap}} to AP{{apto}} - uplink {{uplink}}
<input type="checkbox"/> AP speedflex to ZD	SpeedFlex: AP{{ap}} to ZoneDirector - downlink {{downlink}} uplink {{uplink}}
<input type="checkbox"/> AP speedflex to ZD downlink	SpeedFlex: AP{{ap}} to ZoneDirector - downlink {{downlink}}
<input type="checkbox"/> AP speedflex to ZD uplink	SpeedFlex: AP{{ap}} to ZoneDirector - uplink {{uplink}}
<input type="checkbox"/> Admin speedflex to AP	SpeedFlex: AP [[dap]] to AP [[uap]] - downlink {{downlink}} uplink {{uplink}}
<input type="checkbox"/> Admin speedflex to AP downlink	SpeedFlex: AP [[dap]] to AP [[uap]] - downlink {{downlink}}
<input type="checkbox"/> Admin speedflex to AP uplink	SpeedFlex: AP [[dap]] to AP [[uap]] - uplink {{uplink}}
<input type="checkbox"/> Admin speedflex to ZD	SpeedFlex: AP [[dap]] to ZoneDirector - downlink {{downlink}} uplink {{uplink}}
<input type="checkbox"/> Admin speedflex to ZD downlink	SpeedFlex: AP [[dap]] to ZoneDirector - downlink {{downlink}}
<input type="checkbox"/> Admin speedflex to ZD uplink	SpeedFlex: AP [[dap]] to ZoneDirector - uplink {{uplink}}

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

Assigning an Event Configuration to ZoneDirector Devices

After you create an event configuration, you need to assign it to the ZoneDirector devices that you want to send notifications for the events that you defined in the event configuration template. Assigning an event configuration creates a provisioning task that deploys that particular event configuration to the target ZoneDirector devices.



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

1. Go to **Configure > ZoneDirectors > Event Configuration**.
2. On the *Event Configuration* tab, look for the event configuration that you want to assign to ZoneDirector devices.
3. Click the **Assign ZDs** link that is in the same row as the event configuration that you want to assign. The *Assign ZDs with {Event Configuration Name}* form appears at the bottom of the page.

- In *Select a View*, select the ZoneDirector view from which you want to select ZoneDirector devices. 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.

- Select the check boxes for the ZoneDirector devices to which you want to assign the event configuration. To select all ZoneDirector devices that are currently displayed on the page, click the check box next to the *ZD Name* column header.

Note that this only selects the devices on the current page. If there are devices listed on other pages, you need to go to those pages to select the devices.



NOTE: The *List of ZoneDirectors* table can show up to ten ZoneDirector devices at a time. 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.

- 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 110. Assigning an event configuration to ZoneDirector devices

The screenshot shows the 'Event Configuration' interface. At the top, there are tabs for 'Event Configuration', 'Configured ZDs', and 'Config Task Log'. Below the tabs is a table with the following data:

ID	Configuration Name	Created On	Created By	Action
1	Default Event Configuration	Jul. 30 2012 16:04:10	admin@ruckus.com	Assign ZDs
2	Test Event Config	Jul. 31 2012 03:41:17	admin@ruckus.com	Assign ZDs Edit Delete Copy
3	Test Event Config 2	Jul. 31 2012 03:52:31	admin@ruckus.com	Assign ZDs Edit Delete Copy

Below this table is a section titled 'Assign ZDs with Test Event Config 2'. It includes a dropdown menu for 'Select a ZD View:' set to 'All ZoneDirectors'. Below that is a table titled 'List of Zone Directors' with the following data:

<input type="checkbox"/>	ZD Name	Model	Event Configuration	Serial Number	IP	Connection
<input type="checkbox"/>	SDCFM1106_2	ZD1106	Default Event Configuration	100000011006	192.168.20.5	
<input type="checkbox"/>	SDCFMQA-ZD1100-IPV6only	ZD1150	Default Event Configuration	431103001771	0.0.0.0	
<input checked="" type="checkbox"/>	SDCFMQA_7731_1k1	ZD1106	Test Event Config	100000000011	192.168.20.95	
<input type="checkbox"/>	SDCFMQA_Redundant_3k_1	ZD3500	Default Event Configuration	100903000446	192.168.20.2	
<input type="checkbox"/>	SDCFMQA_ZD1100-ipv4only	ZD1150	Default Event Configuration	431103001686	192.168.20.89	
<input type="checkbox"/>	ruckus-access	ZD1150	Default Event Configuration	101103000306	172.18.110.188	
<input type="checkbox"/>	z8250	ZD3250	Default Event Configuration	100903000148	192.168.20.8	
<input type="checkbox"/>	z8K	ZD9100	Default Event Configuration	500000000003	192.168.25.114	

At the bottom of the interface, there are 'Save' and 'Cancel' buttons, and a copyright notice: 'Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com. Support: http://support.ruckuswireless.com'.

Viewing the Status of an Event Configuration Task

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

1. Go to **Configure > ZoneDirectors > Event Configuration**.
2. Click the **Config Task Log** tab.
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 111. Check the *Status* column for the status of the event configuration task

The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The 'Configure' tab is active, and the 'Event Configuration' sub-tab is selected. The 'Config Task Log' sub-tab is also active, displaying a table of task logs. The table has columns for ID, Task Name, Created On, Created By, Status, and Action. Two entries are visible, both with a 'Success' status. A sidebar on the left contains various navigation options like 'Standalone APs', 'ZoneDirectors', and 'Common'. A footer note explains how to create an event configuration.

ID	Task Name	Created On	Created By	Status	Action
42	[Test Event Config 2] assignment changed	Jul. 31 2012 03:57:06	admin@ruckus.com	Success	Details
41	[Test Event Config] assignment changed	Jul. 31 2012 03:46:50	admin@ruckus.com	Success	Details

Viewing the Event Configuration Assigned to a ZoneDirector Device

1. Go to **Configure > ZoneDirectors > Event Configuration**.
2. Click the *Configured ZDs* tab.
3. In *Select a ZD View*, select the view from which to search for ZoneDirector devices.
4. View all devices in the view or create a filter to search for specific ZoneDirector devices.
 - To display all ZoneDirector devices within the selected view, click **Query**. The *List of ZDs* table appears and lists ZoneDirector details. The *Configuration* column displays the event configuration that is currently assigned to each ZoneDirector device.

- To search for specific ZoneDirector devices, configure the filter settings by doing the following:
 - i. In the first drop-down list box after **Filter Rows where**, select the search attribute that you want to use. Options include name, serial number, IP address, external IP address, model, and last seen (among others).
 - ii. In the second drop-down list box, select the search operator that you want to use. Available search operators include:
 - *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered 172 . 17 . 16 . 176 as the search parameter, only devices with this IP address appear in the search results.
 - *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered 100 as the search parameter, all devices with “100” in the IP address (for example, 172 . 17 . 16 . **100** and **100** . 1 . 10 . 13) appear in the search results.
 - *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered 3208 as the query parameter, only devices with serial numbers that begin with “3208” (for example, 320833000219) appear in the search results.
 - *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected **IP address** as the attribute and you entered 13 as the query parameter, only devices with model names that end in “13” (for example, 100 . 1 . 10 . **13**) appear in the search results.After you select a search operator, a third (text) box appears.
 - iii. In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
 - iv. If you want to add another search filter, 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 user actions on the database, FlexMaster can produce accurate audit logs of system configuration activities.

Creating a ZoneDirector Configuration Upgrade Task

1. Go to **Configure > ZoneDirectors > Config Tasks**.
2. Click **Create a task**. The *CREATE A TASK* pane opens at the bottom of the page.
3. In the *Task Settings* section, do the following:
 - In *Specify a task name*, type a name that you want to assign to this ZoneDirector configuration task.
 - In *Select configuration type*, click **Configuration**.



NOTE: A **Restore** option, which allows you to restore the backup settings to a ZoneDirector device, appears next to **Configuration**. For information on how to use the Restore option, see [Restoring ZoneDirector Configuration](#).

- In *Select configuration file*, select the ZoneDirector configuration template that you want to deploy.
4. In *Select ZoneDirectors to restore*, choose the target ZoneDirector devices.
 - 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 are only 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 are only applied to ZoneDirector devices that match the model. If you select a device of a different model, an error message appears when you save the configuration upgrade task.



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

5. In *Specify a time to perform this task*, specify when you want the task to run.
 - To run the task immediately, click **Perform this task now**.
 - To schedule the task, click **Schedule this task for later**, and then select the date and time.
6. Click **Save** to save the ZoneDirector configuration task.

If FlexMaster detects a problem in the configuration upgrade task that you are saving, then an error message appears.

Backing Up and Restoring ZoneDirector Configuration

This section describes how to create and restore ZoneDirector device configuration backup files. The backup files can be created for single or multiple ZoneDirector devices. The following sections detail how to schedule automatic backups, create an immediate backup, and how to restore backups.

Ruckus Wireless strongly recommends that you periodically back up the settings of your ZoneDirector devices, to make sure that you can easily recover the configuration settings if they ever become corrupted.



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

Scheduling Automatic ZoneDirector Configuration Backups

1. Go to **Configure > ZoneDirectors > Config Backup**.
2. On the *Config Backup* page, click **Create a task**. FlexMaster displays the *Saved Views* tab.
3. Select the *Actions* check box(es) for the ZoneDirector device(s) to be backed up. The names of the targeted ZoneDirectors appear in the **Selected ZoneDirector** list at the bottom of the screen.
4. When you have completed the list of targeted ZoneDirector devices, type a name for the backup task in the **Enter a description for the Configuration** box. Use a descriptive name that helps you identify this backup configuration (especially if you are backing up multiple ZoneDirector configurations).
5. Select the *Schedule BackUp* check box. FlexMaster displays the *Schedule* dialog at the bottom of the screen.
6. In the *Schedule* dialog, select the **Frequency** and **Time of Day** for the automatic backups.
7. Click **Save**.
FlexMaster saves your selections, and performs your backups as scheduled.
8. At any time, you can check your backup task in the *List of Backup Results* at the bottom of the screen. The list displays the status of your backup task.

Immediately Backing Up ZoneDirector Configurations

1. Go to **Configure > ZoneDirectors > Config Backup**.
2. On the *Config Backup* page, click **Create a task**. FlexMaster displays the *Saved Views* tab.
3. Select the *Actions* check box(es) for the ZoneDirector device(s) to be backed up. The names of the targeted ZoneDirectors appear in the **Selected ZoneDirector** list at the bottom of the screen.
4. When you have completed the list of targeted ZoneDirector devices, type a name for the backup task in the **Enter a description for the Configuration** box. Use a descriptive name that helps you identify this backup configuration (especially if you are backing up multiple ZoneDirector configurations).
5. Click **Save**.
FlexMaster saves your selections, and immediately performs your backup.
6. After a few moments, check the *List of Backup Results* for your backup task. The list displays the status of your backup task.

Restoring 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 managed by the primary ZoneDirector device are able to report to the secondary ZoneDirector device automatically. If you choose this restore type, you need to manually configure the IP address, system name, user name and password of the secondary ZoneDirector device.

- *Policy Restore*: Restores only the wireless, access control, role, and user settings from the backup file. Use this restore type if you want to apply the same set of common settings to multiple ZoneDirector devices. You need to first configure one ZoneDi-

rector device with your preferred wireless, access control, role, and user settings, back up these settings, and then restore them onto the target ZoneDirector devices. Note that guest access settings and dynamic pre-shared key (PSK) data is not exported to the target devices. The target devices also retain their original IP address, system name, user name and password.

Performing the Restore Procedure

Before performing a restore procedure for ZoneDirector, make sure that you have at least one backup file that you can use to restore the ZoneDirector settings. If you have not created a backup file, refer to [Backing Up and Restoring ZoneDirector Configuration](#) for more information.

Restoring ZoneDirector settings from a backup file overwrites the current settings with those contained in the backup file. When performing the restore procedure, make sure that:

- You are restoring the correct backup file.
- You are selecting the appropriate restore type. For example, if you only want to restore the wireless, access control, and user settings, make sure you select *Policy Restore*. Selecting *Full Restore* overwrites all existing ZoneDirector settings, including the IP address, system name, user name, and password.

Follow these steps to restore ZoneDirector settings from a backup file.

1. Go to **Configure > ZoneDirectors > Config Tasks**.
2. Click **Create a task**. The *CREATE A TASK* pane opens at the bottom of the page.
3. In the *Task Settings* section, do the following:
 - In *Specify a task name*, type a name that you want to assign to this ZoneDirector configuration task.
 - In *Select configuration type*, click **Restore**.
 - In *Select a configuration file*, select the ZoneDirector backup file that you want to use for the restore procedure. The settings (partial or complete, depending on the restore type) in this backup file are copied to the target ZoneDirector devices.
 - In *Specify restore type*, select the type of restore that you want to perform. FlexMaster provides three restore types: **Full Restore**, **Failover Restore**, and **Policy Restore**. For help in deciding which restore type to choose, 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 are only 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

Provisioning Tasks to Managed Devices

Provisioning Tasks to ZoneDirector Devices

settings in the template are only applied to ZoneDirector devices that match the model. If you select a device of a different model, an error message appears when you save the configuration upgrade task.



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

5. In *Specify time for this task*, specify when you want the task to run.
 - To run the task immediately, click **Perform this task now**.
 - To schedule the task, click **Schedule this task for later**, and then select the date and time.
6. Click **Save** to save the ZoneDirector restore task. 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](#)
- [Releasing Device Licenses](#)

Working with Device Firmware

This section describes how to view firmware that is currently installed on managed devices and how to upgrade firmware on these devices.



NOTE: 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 the following table for descriptions of the columns that appear on the page.

Figure 112. The Firmware Status page displays the firmware versions that are installed on managed devices

Model Type	Software Version	Date	Number of Devices	Actions
ZD1106	9.5.0.0.34	Jul. 29 2012	2	Save as a View
ZD1150	9.4.0.0.110	May. 23 2012	1	Save as a View
ZD1150	9.5.0.0.34	Jul. 29 2012	2	Save as a View
ZD3250	9.5.0.0.34	Jul. 29 2012	1	Save as a View
ZD3500	9.5.0.0.34	Jul. 29 2012	2	Save as a View
ZD5100	9.5.0.0.34	Jul. 29 2012	1	Save as a View
ZF2942	9.5.0.0.34	Jul. 29 2012	1	Save as a View
ZF732L	9.5.0.0.34	Jul. 29 2012	1	Save as a View




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 24. Columns on the Firmware Status table

Column Name	Description
Model Type	Model of the device.
Software Version	Version of the software/firmware that is currently installed on a device.
Date	Date when the firmware was uploaded to FlexMaster.
Number of Devices	Number of devices that are using this firmware.
Actions	Shows the Save as a View link. Clicking this link shows options for saving devices in this group as a view, based on their firmware version.

Displaying and Hiding Columns

By default, FlexMaster displays all the available columns on the Firmware Status page. If you want to hide some of these columns, do the following:

1. Click the **Edit Columns** link at the bottom of the table. A box appears and displays check boxes for the table columns. By default, all check boxes are selected, which means all available columns are visible in the table.
2. To hide a column, clear the check box for that column. For example, to hide the date column, clear (or uncheck) the **Date** check box.
3. Click anywhere outside the box with check boxes when you are done.

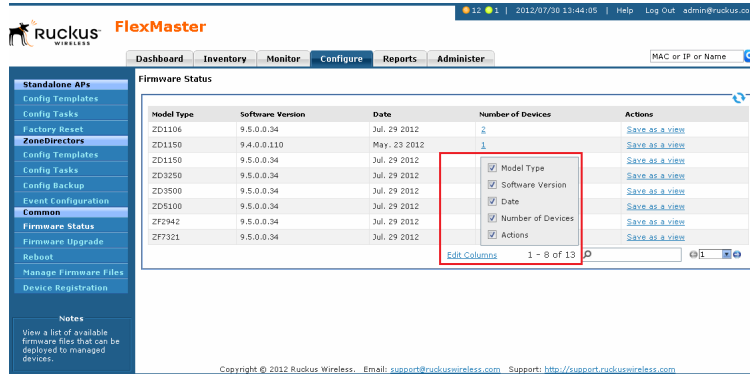
You have completed hiding columns from the Firmware Status page.

Provisioning Tasks to Managed Devices

Provisioning Common Tasks

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

Figure 113. To hide a column, clear or uncheck the check box for that column



The screenshot shows the Ruckus FlexMaster web interface. The main content area displays a table titled "Firmware Status" with the following data:

Model Type	Software Version	Date	Number of Devices	Actions
ZD1106	9.5.0.0.34	Jul. 29 2012	2	Save as a view
ZD1150	9.4.0.0.110	May. 23 2012	1	Save as a view
ZD1150	9.5.0.0.34	Jul. 29 2012		Save as a view
ZD3250	9.5.0.0.34	Jul. 29 2012		Save as a view
ZD3500	9.5.0.0.34	Jul. 29 2012		Save as a view
ZD5100	9.5.0.0.34	Jul. 29 2012		Save as a view
ZF2942	9.5.0.0.34	Jul. 29 2012		Save as a view
ZF7321	9.5.0.0.34	Jul. 29 2012		Save as a view

Below the table, there is an "Edit Columns" link and a list of columns with checkboxes:

- Model Type
- Software Version
- Date
- Number of Devices
- Actions

The "Edit Columns" link is highlighted with a red box. Below the list, it says "1 - 6 of 13".

Creating a Firmware Upgrade Task

The Firmware Upgrade option enables the creation of tasks that upgrade the firmware of managed devices at a specified time. The task defines the devices to be upgraded, the firmware files to provision, and the time at which to perform the upgrade.



NOTE: Before creating a firmware upgrade task, you first need to upload one or more firmware files to FlexMaster by following the steps in [Uploading a Firmware File](#).



NOTE: You need not accompany a firmware upgrade task with a reboot task. However, the new firmware does not become active until the next reboot. For more on rebooting, 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 user actions in the database, FlexMaster can produce accurate audit logs of system configuration activities.

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

Figure 114. The **CREATE A TASK** form

Device Name	Serial #	Software	Model	Connection	IP Address
ZF7363	161203002768	9.5.0.0.34	ZF7363	✓	192.168.22.123:443
RuckusAP	161205001949	9.5.0.0.34	ZF7321	✓	192.168.22.147:443
ZF742	201055001440	9.5.0.0.34	ZF7742	✓	192.168.22.91:443
RuckusAP	294212345578	9.5.0.0.34	ZF2942	✓	192.168.22.70:443
RuckusWB	501055004323	9.2.0.0.140	ZF7731	✓	192.168.20.60:443
RuckusWB	501055004874	9.2.0.0.140	ZF7731	✓	192.168.20.59:443
RuckusAP	92101013734	9.5.0.0.34	ZF7942	✓	192.168.22.92:443
RuckusAP	92101013880	9.5.0.0.34	ZF7942	✓	192.168.22.144:443
RuckusAP	92101014045	9.5.0.0.34	ZF7942	✓	192.168.22.145:443
RuckusAP	991155001182	9.5.0.0.34	ZF7761CM	✓	192.168.22.109:443

3. In *Specify a task name*, type a name for the firmware upgrade task that you are creating.
4. Under *Select the view to upgrade*, do one of the following:

- Click the **Select View** tab, and then toggle the *Select a view of devices to perform firmware upgrade* drop-down list to filter the list of devices based on a device view.
 - Click the **Select Devices** tab. And then, under the *Select* column, select the check box for each device you want to update.
5. Under *Select the firmware file for each model*, select the firmware file for each device type by selecting the desired firmware file from the drop-down list. Different types of devices require different firmware files. If a device in the group does not have a suitable firmware file, that device is not updated.
 6. (Optional) Mark the **Reboot device after firmware upgrade** check box to reboot all groups of devices after firmware upgrade. You may choose to upgrade devices without immediate reboot, and then reboot them later, such as during an SLA-defined maintenance interval.



NOTE: You do not need to force a reboot with a firmware upgrade. However, the new firmware does not become active until the devices are rebooted.

7. Under *Specify a time to perform this task*, click when you want to perform this task:
 - **Perform this task now:** Run the task immediately after clicking **Save**.
 - **Schedule this task for later:** Specify the *Date* (yyyy-mm-dd) and *Time* (hh:mm) when the task should run.
8. Click **Save**. A pop-up window appears.
9. Click **OK** in the pop-up window to confirm the task.

Deleting a Firmware Upgrade Task

If you no longer use an existing firmware upgrade task, you can delete it.

1. Go to the **Configure > Common > Firmware Upgrade** page.
2. Look for the firmware upgrade task that you want to delete.
3. Click the **Delete** link that is in the same row as the task name. A confirmation message appears.
4. Click **OK** to continue.

The page refreshes, and the task that you deleted disappears from the list.

Working with Reboot Tasks

The Reboot option enables creation of tasks that reboot devices at a specified time. For example, your Change Management Policy may require a specific time window within which devices can be rebooted. Your service agreement specifies that on Sundays at 3:00 AM devices may be taken out of service for maintenance 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 115. The **CREATE A TASK** form appears at the bottom of the page

Device Name	Serial #	Model	IP Address	Uptime	Connection	Software
ZF7363	161203002768	ZF7363	192.168.22.123:443	19h 43m	✓	9.5.0.0.34
RuckusAP	161205001949	ZF7321	192.168.22.147:443	12h 51m	✓	9.5.0.0.34
7762	281055001440	ZF7762	192.168.22.91:443	12h 32m	✓	9.5.0.0.34
RuckusAP	294212345678	ZF2942	192.168.22.70:443	19h 41m	✓	9.5.0.0.34
RuckusWB	501055004323	ZF7731	192.168.20.60:443	11d 13h 30m	✓	9.2.0.0.140
RuckusWB	501055004074	ZF7731	192.168.20.59:443	7d 16h 40m	✓	9.2.0.0.140
RuckusAP	921001013734	ZF7942	192.168.22.92:443	19h 42m	✓	9.5.0.0.34
RuckusAP	921001013880	ZF7942	192.168.22.144:443	19h 42m	✓	9.5.0.0.34
RuckusAP	921001014045	ZF7942	192.168.22.145:443	19h 42m	✓	9.5.0.0.34
RuckusAP	991155001182	ZF7761CM	192.168.22.109:443	20h 9m	✓	9.5.0.0.34

3. Type a name for your reboot task at *Specify a task name*.
4. Under *Select the view to reboot*, do the following:
 - Click the **Select View** tab, and then toggle the *Select a view of devices to perform reboot* drop-down list to filter the list of devices based on a device view. Default view include *All Standalone APs* and *All ZoneDirectors*.

- Click the **Select Devices** tab, and then select the check box in the *Select* column for each device you want to update.
5. Under *Specify time to perform this task*, click when you want to perform this task:
 - **Perform this task now**: Run the task immediately after clicking **Save**.
 - **Schedule this task for later**: Specify the *Date* (yyyy-mm-dd) and *Time* (hh:mm) when the task should run.
6. Click **Save**.

Viewing the Status of a Reboot Task

View the status of the reboot task to check if it has started, completed successfully, or failed.

1. Go to **Configure > Common > Reboot**. A list of reboot tasks that you have created appears on the page.
2. Look for the reboot 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#Scheduled*: Indicates that the configuration task has been successfully scheduled for n number of devices. To view the list of devices that have been scheduled, click **n#Scheduled** (hyperlink). The Device Status pane appears at the bottom of the page, displaying scheduled task information.
 - *n#Success*: Indicates that the configuration task has been provisioned successfully to n number of devices that have this status. To view the list of devices that have been provisioned successfully, click **n#Success** (hyperlink). The Device Status pane appears at the bottom of the page, displaying task details, device details, and task status.
 - *n#Fail*: Indicates that the configuration task failed on n number of devices. To view the list of devices on which provisioning failed, click **n#Fail** (hyperlink). The Device Status pane appears at the bottom of the page, displaying task details, device details, and task status. If the task failed, click the **Detail** link under the **Failure** column to see what may have caused the task failure.

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

Deleting a Reboot Task

1. Go to the **Configure > Common > Reboot** page.
2. Look for the that you want to delete.
3. Click the reboot task **Delete** link. A confirmation message appears.
4. Click **OK** to continue.

The page refreshes, and 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

Follow these steps to upload a firmware file to FlexMaster.

1. Go to **Configure > Common > Manage Firmware Files**.
2. Click **Upload new firmware file**. The **UPLOAD NEW FIRMWARE FILE** form appears at the bottom of the page.

Figure 116. The **UPLOAD NEW FIRMWARE FILE** form appears at the bottom of the page

The screenshot shows the 'Manage Firmware Files' page in FlexMaster. On the left is a navigation menu with options like 'Standalone APs', 'Config Templates', 'Config Tasks', 'Factory Reset', 'ZoneDirectors', 'Event Configuration', 'Common', 'Firmware Status', 'Firmware Upgrade', 'Reboot', 'Manage Firmware Files', and 'Device Registration'. The 'Manage Firmware Files' option is selected.

The main content area is titled 'Manage Firmware Files' and contains a table of existing files:

Firmware Name	Description	Created By	Actions
2741_9.5.0.0.34.BIT	2741_9.5.0.0.34.BIT	admin@ruckus.com	Edit Delete
2942_9.5.0.0.34.BIT	2942_9.5.0.0.34.BIT	admin@ruckus.com	Edit Delete
7025_9.5.0.0.34.BIT	7025_9.5.0.0.34.BIT	admin@ruckus.com	Edit Delete
7321_9.5.0.0.34.BIT	7321_9.5.0.0.34.BIT	admin@ruckus.com	Edit Delete
7321_9.5.0.0.5.BIT	7321_9.5.0.0.5.BIT	admin@ruckus.com	Edit Delete
7942_9.5.0.0.34.BIT	7942_9.5.0.0.34.BIT	admin@ruckus.com	Edit Delete
7962_9.5.0.0.34.BIT	7962_9.5.0.0.34.BIT	admin@ruckus.com	Edit Delete
7982_9.5.0.0.34.BIT	7982_9.5.0.0.34.BIT	admin@ruckus.com	Edit Delete
ed1100_9.5.0.0.19.ap_9.5.0.0.19.img	ed1100_9.5.0.0.19.ap_9.5.0.0.19.img	admin@ruckus.com	Edit Delete
ed1100_9.5.0.0.34.ap_9.5.0.0.34.img	ed1100_9.5.0.0.34.ap_9.5.0.0.34.img	admin@ruckus.com	Edit Delete

Below the table, it says 'Number of files: 12' with a search box.

The 'UPLOAD NEW FIRMWARE FILE' form is open, showing the following sections:

- Select the device model for this firmware file:** A grid of checkboxes for various device models including MediaFlex (VF2611, VF2025, VF7611), ZoneFlex (ZF2741, ZF2925, ZF2942, ZF7025, ZF7321, ZF7341, ZF7343-U, ZF7343, ZF7352, ZF7363, ZF7372, ZF7731, ZF7761CM, ZF7762, ZF7762-AC, ZF7762-M, ZF7762-S, ZF7762-S-AC, ZF7762-T, ZF7762-E, ZF7782, ZF7782-N, ZF7782-S, ZF7782, ZF7982), ZoneDirector 1000, ZoneDirector 1100, ZoneDirector 3000, and ZoneDirector 5000.
- Specify firmware description:** A text input field.
- Select firmware file:** A 'Choose File' button with the text 'No file chosen'.
- Buttons for 'OK' and 'Cancel'.

At the bottom of the page, there is a copyright notice: 'Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com'.

3. Under *Specify the device model for this firmware file*, select the check box before the Ruckus Wireless device to specify the product and model to which the firmware applies. Device models are grouped according to product names: MediaFlex, ZoneFlex, and ZoneDirector.
4. In *Specify firmware description*, type a description of the firmware file. Ruckus Wireless recommends using a name that readily identifies the firmware.
5. In *Select firmware file*, click **Choose File** to search your client workstation or other reachable location for the firmware file.
6. Click **OK** to upload the firmware file for storage on FlexMaster.

Editing a Firmware File

After you upload a firmware file, you can edit it to define the product models on which the firmware is installed.



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

1. Go to **Configure > Common > Manage Firmware Files**.
2. Click a firmware file **Edit** link. The *EDIT* form appears below the table.
3. Edit the firmware details as required. You can select the product models on which FlexMaster attempts to provision the firmware. You can also edit the firmware description.
4. Click **OK** to save your changes.

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

Deleting a Firmware File

1. Go to **Configure > Common > Manage Firmware Files**.
2. Look for the firmware file that you want to delete.
3. Click the **Delete** link that is in the same row as the firmware name. A confirmation message appears.
4. Click **OK** to confirm.

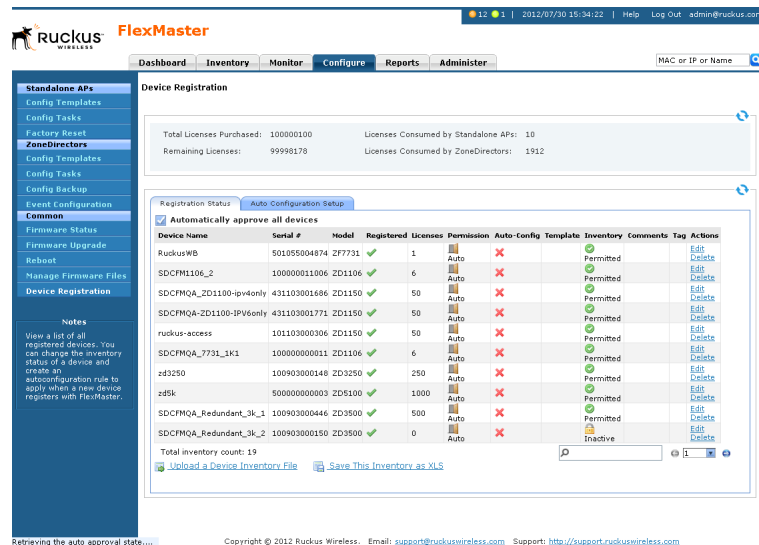
The page refreshes, and then the firmware file that you deleted disappears from the list.

Managing Device Registration

By default, compatible Ruckus Wireless devices attempt to register with FlexMaster upon boot up. The Device Registration option offers management of each join request sent by your devices. Thus, you can permit or deny devices from joining FlexMaster. All device registration requests are accepted by default.

A key feature of Device Registration is the ability to import a list of devices into the FlexMaster inventory before actual device registration, which occurs when the devices boot up. This enables you to stay ahead of your dispersal of Ruckus Wireless APs and keep track of each device's details (for example, serial number and MAC address), as well as automatically permit or deny the device to register with FlexMaster upon power up.

Figure 117. The Device Registration page



The table below describes the columns that appear in the Device Registration table.

Table 25. 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 #	Serial number of a registering device.
Model	Model of device.
Registered	<p>✓ indicates that the device has registered with FlexMaster.</p> <p>✗ indicates that the device has not yet registered with FlexMaster.</p>
Licenses	How many licenses this device consumes.

Table 25. Table columns on the Device Registration page

Column	Description
Permission	Mode of acceptance as <i>Auto</i> (permission automatically assigned, no manual intervention) or <i>Manual</i> (permission requires manual assignment).
Auto-Config	<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>
Template	(to be determined)
Inventory	<ul style="list-style-type: none"> • <i>Permitted</i>: The device is allowed to register with FlexMaster. • <i>Inactive</i>: The device is currently inactive.
Comments	Shows any notes that you have entered about the device. To add comments, click the Edit link that is in the same row as the device name, and then enter your comments in the EDIT form that appears below the table.
Tag	If you assigned a tag to the device in the auto configuration inventory file, that tag appears here.
Actions	<p>Clicking the Edit 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.</p> <p>Clicking the Delete link allows you to delete a Ruckus Wireless device registration from the FlexMaster database. Deleting the device registration also releases the consumed license or licenses.</p>
Status	<p>Shows the permission status of the device. Default permission statuses include:</p> <ul style="list-style-type: none"> • <i>Admin Denied</i>: The device not receive configuration and firmware upgrades from FlexMaster. • <i>Permitted</i>: The device is allowed to register with FlexMaster. • <i>RMA</i>: The device is currently being repair or replaced. RMA stands for Return Merchandise Authorization. • <i>Unavailable</i>

Setting Device Registration Permissions

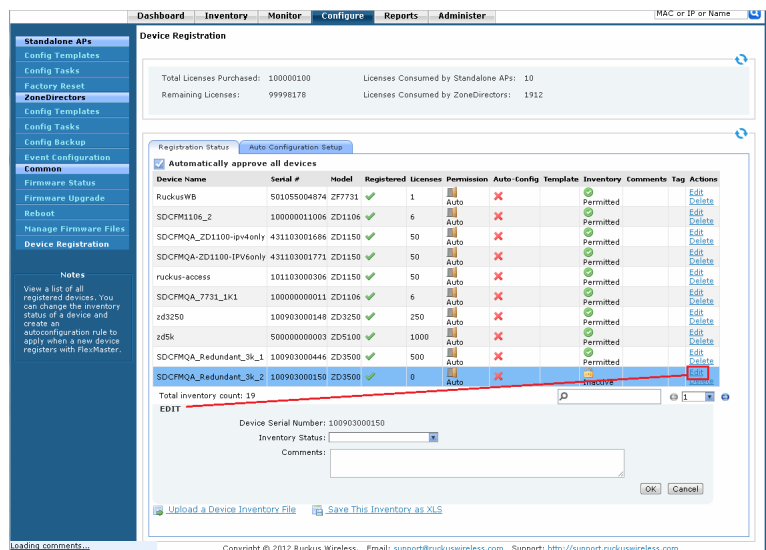
By default, Permission Mode is set to *Automatically approve all devices*, which allows all supported Ruckus Wireless devices to register with FlexMaster automatically. If there is a specific device that you want to prevent from registering with FlexMaster, you need to manually change the permission for that device to *Admin Denied*.

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 no longer receives configuration and firmware upgrades from FlexMaster after you save the new permission.
 - *Permitted*: Click this option to allow the device to register with FlexMaster.
 - *RMA*: Click this option is the device is currently being repair or replaced. RMA stands for Return Merchandise Authorization.
 - *Unavailable*: Click this option if you want to designate this device as unavailable.

If you created any custom statuses on the **Administer > View Management > Inventory Status** tab, they also appear as options when you are editing the inventory status of a device.

4. Enter optional comments in **Comments**.
5. Click **OK** to save your changes.

Figure 118. Editing a device's registration settings



NOTE: If you deny a device that is already registered, it remains in the inventory but FlexMaster no longer honors requests from that device.



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



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



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

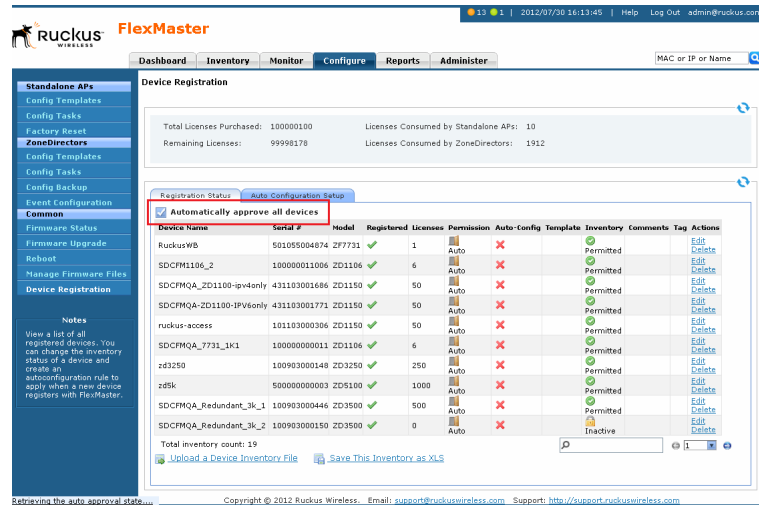


NOTE: Only devices in **Permitted** status consume licenses; devices in other statuses do not consume any licenses.

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 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 119. Enabling auto approval



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 26. 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> is able to register successfully if licenses are available. Device status is set to Permitted
Added via inventory file	Any	Permitted (or any user-defined status)	Licenses exceeded	Fail	Device status appears as <i>License Exceeded</i> . The license held by the device is released.

Provisioning Tasks to Managed Devices

Provisioning Common Tasks

Table 26. 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	If a standalone AP becomes managed by ZoneDirector, its status changes to <i>Managed by ZoneDirector</i> . If a ZoneDirector device becomes managed by another FlexMaster server or the TR069 function is disabled, its status changes to <i>Lost ZoneDirector</i> . If the ZoneDirector device is managed by another FlexMaster server, the license held by the device is released on the original FlexMaster server. However, if the TR069 function is disabled, the license status remains the same until the inventory status is changed to a status other than "Permitted".
Added via inventory file	Any	Admin Denied, RMA, or Unavailable	Any	Fail	The license held by the device is zero.
Auto registration (call home)	Enabled	Any	Licenses available	Success	Device status is set to <i>Permitted</i> . The auto registration state of the device is set to <i>Enabled</i> .
Auto registration (call home)	Enabled	Any	Licenses exceeded	Fail	Device status is set to <i>License Exceeded</i> and the license held by the device is released. The auto registration state of the device is set to <i>Enabled</i> .
Auto registration (call home)	Disabled	Any	Any	Fail	Device status is set to <i>Admin Denied</i> and the license held by the device is released. The auto registration state of the device is 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 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 are able to register with FlexMaster even when automatic device approval is disabled.
- You can also upload an inventory file when you want to automatically configure a number of unregistered Ruckus Wireless devices when they register with FlexMaster.

Preparing a Device Inventory File

A device inventory file is a Microsoft Excel file with the same entries as the *Device Registration* table. After you upload the device inventory file with the pre-registration data, you need to create an auto-configuration task using the tag to select the target devices.

Figure 120. An example of a device inventory file

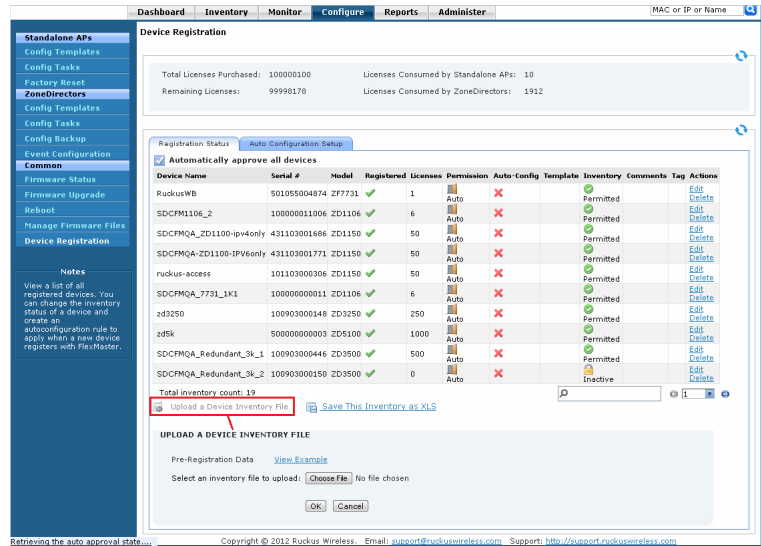
	A	B	C	D	E	F	G	H	I	J	K	L
	Device Name	Serial #	Model	Registered	Licenses	Permission	Auto-Config	Template	Inventory	Comments	Tag	
1	RuckusWB	501055004874	ZF7731	Yes	1	Auto	No		Permitted			
2	SDCFM1106_2	100000011006	ZD1106	Yes	6	Auto	No		Permitted			
3	SDCFMQA_ZD1100-ipv4only	431103001686	ZD1150	Yes	50	Auto	No		Permitted			
4	SDCFMQA_ZD1100-IPV6only	431103001771	ZD1150	Yes	50	Auto	No		Permitted			
5	ruckus-access	101103000306	ZD1150	Yes	50	Auto	No		Permitted			
6	SDCFMQA_7731_1K1	100000000011	ZD1106	Yes	6	Auto	No		Permitted			
7	zd3250	100903000148	ZD3250	Yes	250	Auto	No		Permitted			
8	zd5k	500000000003	ZD5100	Yes	1000	Auto	No		Permitted			
9	SDCFMQA_Redundant_3k_1	100903000446	ZD3500	Yes	500	Auto	No		Permitted			
10	SDCFMQA_Redundant_3k_2	100903000150	ZD3500	Yes	0	Auto	No		Inactive			
11	RuckusAP	921001014045	ZF7942	Yes	1	Auto	No		Permitted			
12	RuckusAP	921001013734	ZF7942	Yes	1	Auto	No		Permitted			
13	RuckusAP	294212345678	ZF2942	Yes	1	Auto	No		Permitted			
14	RuckusAP	921001013880	ZF7942	Yes	1	Auto	No		Permitted			
15	ZF7363	161205002768	ZF7363	Yes	1	Auto	No		Permitted			
16	RuckusAP	991155001182	ZF7761CM	Yes	1	Auto	No		Permitted			
17	RuckusWB	501055004323	ZF7731	Yes	1	Auto	No		Permitted			
18	7762	281055001440	ZF7762	Yes	1	Auto	No		Permitted			
19	RuckusAP	161205001949	ZF7321	Yes	1	Auto	No		Permitted			
20												
21												
22												

Uploading a Device Inventory File

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

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.

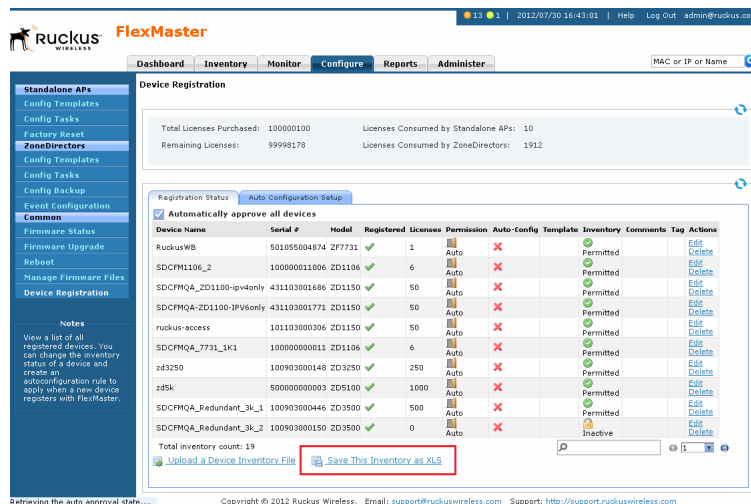
Figure 121. The Upload a Device Inventory File form



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 122. Click the Save This Inventory as XLS link



1. On the *Device Registration* page, click the **Save This Inventory as XLS** link at the bottom of the page. FlexMaster saves the *inventory.xls* file to your workstation.

2. If necessary, click **Save**, and then select the location where you want to save the file.

You have completed exporting the device list to an Excel file. Go to the location where you exported the Excel file to verify that the file was saved successfully, and then use Microsoft Excel to open the file.

Releasing Device Licenses

Devices can be released on a per-serial number basis:

1. Go to **Configure > Common > Device Registration**.
2. Click **Registration Status**.
3. Find the required *Device Name* in the table. Note the number of licenses consumed in the *Licenses* column.
4. Click **Delete** in the *Actions* column and respond to the confirmation prompt.
FlexMaster deletes the device, releases the consumed license or licenses, and returns you to the **Registration Status** page.
5. In the **Registration Status** page, verify that the device entry is deleted.

Configuring VLAN and LAN Port Settings

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



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



NOTE: 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 are unable to set it as the hotspot interface and the following message appears:

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

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 need to edit one or more of these VLAN profiles.
- The Management VLAN cannot be renamed or deleted.
- When the AP is in its factory default state, all physical interfaces on the AP are untagged and all wireless interfaces are connected to the Management VLAN.

- By default, L2TP feature and L2TP tunnel state are both disabled on the AP.
- FlexMaster only uses the Tunnel Management VLAN when L2TP is enabled.
- VLANs with the same ID must have the same tunneled state.
- A physical interface can be configured as untagged on only one VLAN, and wireless interfaces cannot be configured as tagged on a ZoneFlex AP.
- A wireless interface can be connected to only one VLAN.
- Ethernet ports are defined as Trunk Ports, Access Ports, or General Ports. Trunk links pass VLAN information between switches. Access ports provide access to the network and can be configured as members of specific VLANs, thereby separating the traffic on these ports from traffic on other VLANs. General Ports are user-defined ports that can have any combination of up to 20 VLAN IDs assigned. At least one port on each AP must be designated as a Trunk Port.
- By default, all ports are enabled as Trunk Ports with Untagged VLAN set as 1 (except for ZoneFlex 7025, whose front ports are enabled as Access Ports by default). If configured as an Access Port, all untagged ingress traffic is the configured Untagged VLAN, and all egress traffic is untagged. If configured as a Trunk Port, all untagged ingress traffic is the configured Untagged VLAN (by default, 1), and all VLAN-tagged traffic on VLANs 1-4094 will be seen when present on the network.
Trunking is a function that must be enabled on both sides of a link. If two switches are connected together, for example, both switch ports must be configured as trunk ports. The Trunk Port is a member of all the VLANs that exist on the AP/switch and carries traffic for all those VLANs between switches.
- All Access Ports are set to Untagged VLAN 1 by default. This means that all Access Ports belong to the native VLAN and are all part of a single broadcast domain. To remove ports from the native VLAN and assign them to specific VLANs, select Access Port and enter any valid VLAN ID in the VLAN ID field (valid VLAN IDs are 2-4094). The following table describes the behavior of incoming and outgoing traffic for Access Ports with VLANs configured.

VLAN Settings	Incoming Traffic (from the client)	Outgoing Traffic (to the client)
Access Port, Untag VLAN 1	All incoming traffic is native VLAN (VLAN 1).	All outgoing traffic on the port is sent untagged.
Access Port, Untag VLAN [2-4094]	All incoming traffic is sent to the VLANs specified.	Only traffic belonging to the specified VLAN is forwarded. All other VLAN traffic is dropped.

- General ports are user-specified ports that can have any combination of up to 20 VLAN IDs assigned. Enter multiple valid VLAN IDs separated by commas or a range separated by a hyphen.

Provisioning Tasks to Managed Devices

Configuring VLAN and LAN Port Settings

- Using Port-Based 802.1X: 802.1X authentication provides the ability to secure the network and optionally bind service policies for an authenticated user. 802.1X provides logical port control and leverages the EAP authentication and RADIUS protocols to allow the network policy to be effectively applied in real time, no matter where the user connects to the network.
AP Ethernet ports can be individually configured to serve as either an 802.1X supplicant (authenticating the AP to an upstream authenticator switch port), or as an 802.1X authenticator (receiving 802.1X authentication requests from downstream supplicants). A single port can not provide both supplicant and authenticator functionality at the same time.
- If mesh mode is enabled on ZoneDirector, then the 802.1X port settings are unavailable for any APs that support mesh. The ZoneFlex 7025 does not support mesh, so 802.1X settings are available for those access points even when mesh is enabled. However, the 802.1X settings are only available from the Editing [Access Point] dialogue, not from AP Groups. Therefore if you want to use 802.1X on ZoneFlex 7025 ports when mesh is enabled, you must configure each AP individually.
- Ethernet port as authenticator: The Access Point is fundamentally a wireless switch. On APs with two or more wired ports, the AP acts as a network edge switch and can be configured to authenticate downstream wired stations (which can even be another edge switch). When the AP Ethernet port is configured as an 802.1X authenticator, it can be further defined as either Port-based or MAC-based. MAC-based authenticator mode is only supported if the port is an Access Port.

	Trunk Port	Access Port	General Port
Port-based authenticator support	Yes	Yes	Yes
MAC-based authenticator support	No	Yes	No

- Ethernet port as supplicant: You can also configure a port to act as a supplicant and force it to authenticate itself to an upstream authenticator port. Until the AP has successfully done so, the state of the authenticator port is closed and packets from the AP or stations behind it will be dropped at the authenticator port.
In this configuration, it is expected that the connected authenticator port is configured as a Trunk Port to pass all VLAN packets, and in port-based authentication mode. Each AP is allowed to configure a maximum of one Ethernet port as an 802.1X supplicant, and the supplicant port must be a Trunk Port.
- In 802.1X port-based authenticator mode, only a single MAC host must be authenticated for all hosts to be granted access to the network.
- In 802.1X MAC-based authenticator mode, each MAC host is individually authenticated. Each newly-learned MAC address triggers an EAPOL request-identify frame.
 - Guest VLAN: (Default disabled). When a station fails to authenticate to this port, it will be assigned to this "guest" VLAN, with access to Internet but not to internal resources.

- Dynamic VLAN: (Default disabled). Dynamically assign VLANs based on the policies set on the RADIUS server.
- Authenticator: Select the RADIUS server from the list. A RADIUS server must be selected to set this port as a MAC-based authenticator.

General Configuration Procedures

The specific procedures for configuring the VLAN settings of an AP depend on several factors in your network environment. These factors include the number of physical and wireless interfaces that you want to segment and the number of VLANs to which you want these interfaces to be connected. Since VLAN configuration procedures typically differ from one network to another, this guide only provides high-level steps for configuring VLANs.

1. Launch the VLAN configuration page for the AP.

VLAN settings need to be configured on a per-device basis. Log on to the FlexMaster Web interface, find the AP that you want to configure, and then launch the device view for that AP. You can find the VLAN-related settings by clicking VLAN on the Device Interface menu.

2. Remove the physical and wireless interfaces that you want to connect to the wired VLAN from the default Management VLAN.

By default, all physical and wireless interfaces on the AP belong to the Management VLAN. This default configuration allows any client connected to any of the AP's interfaces to communicate with other clients that are connected to the same AP. Before you can connect a physical or wireless interface to another VLAN, you first need to disconnect it from the Management VLAN.

3. Edit a VLAN profile to connect the physical and wireless interfaces to the wired VLAN.

Edit one of the available VLAN profiles on the AP to enable it to forward traffic to the target VLAN on the wired network, and then add the physical and wireless interfaces that you want to connect to that VLAN.

These are the three general steps for configuring the VLAN settings on an AP. For an example of specific configuration procedures, refer to the following sample scenario.

How Dynamic VLAN Works

By default, all wireless clients associated with Ruckus Wireless APs are segmented into a single VLAN (with VLAN ID 1, unless otherwise configured). If you want to individually assign wireless clients into specific VLANs (for example, for increased security), you can enable dynamic VLAN.

Dynamic VLAN allows ZoneDirector to separate wireless clients into different network segments based on the VLAN ID that is assigned to each wireless user on the RADIUS server. As such, dynamic VLAN is implemented on a per-user basis, typically by MAC address.

Priority of Dynamic VLAN, VLAN, and Tunnel Mode

If the VLAN, Dynamic VLAN and Tunnel Mode features are all enabled and they have conflicting rules, ZoneDirector prioritizes and applies these three features in the following order:

1. Dynamic VLAN (top priority)
2. VLAN
3. Tunnel Mode

How it Works for Assigned Clients

When a client is dynamically assigned to a VLAN in the RADIUS server database, this is how it works:

1. Client associates with a WLAN on which Dynamic VLAN has been enabled.
2. The AP requires the client to authenticate with the RADIUS server.
3. When the RADIUS server completes the client authentication process, it sends the join approval and the VLAN ID that has been assigned to the AP.
4. Client joins the AP and is segmented to the assigned VLAN ID.

How it Works for Unassigned Clients

When a client is not assigned to a VLAN in the RADIUS server database, this is how it works:

1. Client associates with a WLAN on which Dynamic and Guest VLANs have been enabled. The client is currently blocked from access.
2. The RADIUS server notifies the AP that the client is not dynamically assigned to a VLAN.
3. Client joins the AP and is segmented to the Guest VLAN.

Sample Dynamic VLAN Scenario

Your wired LAN is segmented into several VLANs, including one called *Sales VLAN* (VLAN 10) and one called *Guest VLAN* (VLAN 11). You assign the Sales clients in a RADIUS (or other) server to VLAN 10, so the Sales clients stay on the same VLAN, no matter which AP they are using to access the wired network. The dynamic VLAN feature can also allow the Sales clients to roam across multiple APs without re-authenticating.

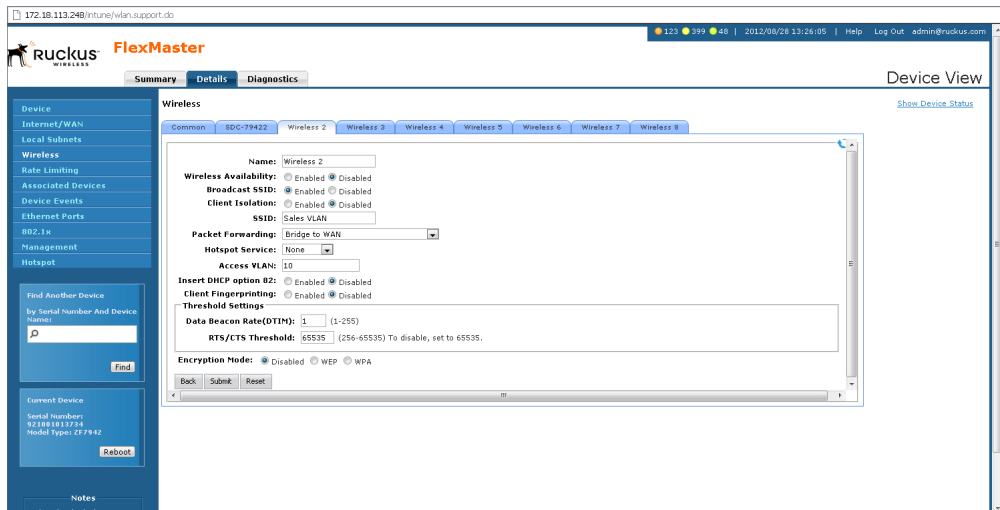
In this scenario, you have a ZoneFlex 7942 device deployed on the network and you want its Port 2 and a wireless interface to join the Sales VLAN on the wired LAN. Specifically, you want its physical ports Port 2 and Wireless 2 interface to be part of the Sales VLAN.

The Sales VLAN is assigned VLAN ID 10 and associated Guest VLAN is assigned VLAN ID 11.

Step 1: Configuring the Wireless LAN

1. Launch the Device View for the AP that you want to manage, click the **Details** tab, and then click **Wireless** on the menu. FlexMaster displays the *Wireless* page.
2. In the *Wireless* page, click the desired **Wireless #** tab, and then click **Edit Settings**. FlexMaster displays the *Edit Wireless LAN* page.
3. In the *Edit Wireless LAN* page, edit the following:
 - (optional) *SSID* -- what the wireless clients will see when they search for the Sales VLAN.
 - *Access VLAN* -- set to VLAN ID **10**.
4. In the *Edit Wireless LAN* page, click **Submit** to save your changes.

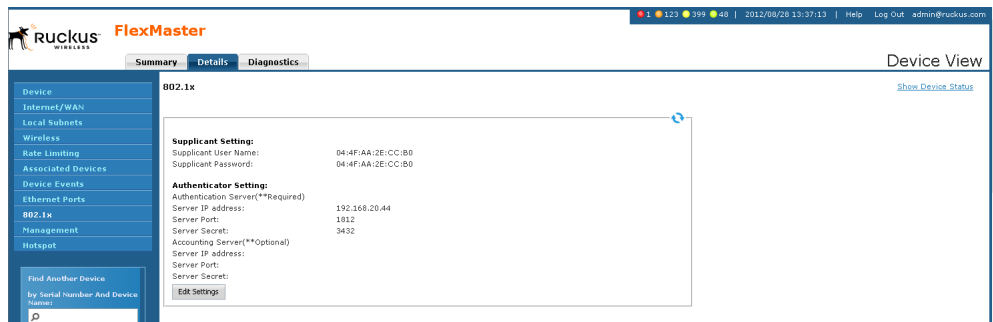
Figure 123. *Edit Wireless LAN* page



Step 2: Verifying 802.1X Configuration

1. In the *Wireless* page, click **802.1x** on the menu.
2. Using the recommendations in "[Configuring VLAN and LAN Port Settings](#)" on [page 196](#), make sure that the 802.1X server settings are correct.

Figure 124. Verifying 802.1X server settings



Step 3: Configuring the Ethernet Port

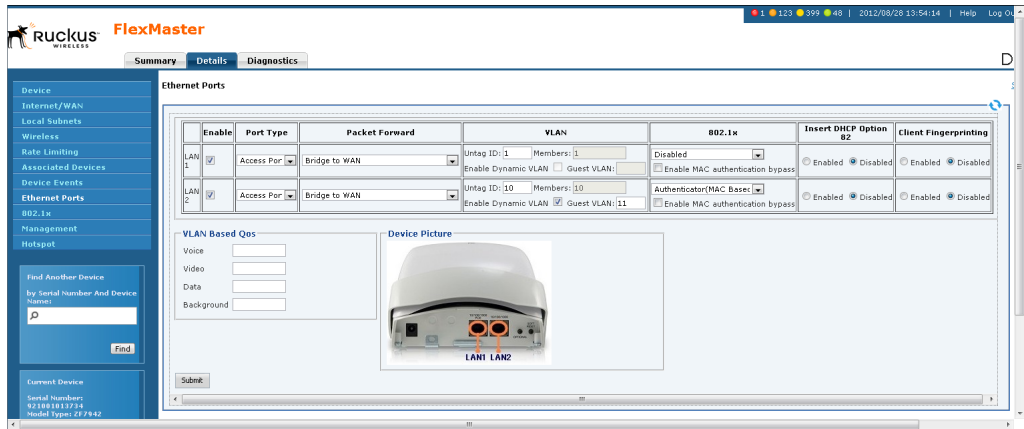
For this example, we are configuring LAN Port 2 to support *Sales VLAN 10* and *Guest VLAN 11* as part of a dynamic VLAN.

1. In the *Wireless* page, click **Ethernet Ports** on the menu. FlexMaster displays the *Ethernet Ports* page.
2. In the Port 2 *Port Type* entries, select **Access Port**.
3. In the Port 2 *VLAN* entries:
 - Select the **Enable Dynamic VLAN** box.
 - Enter VLAN ID **10** in the *Untag ID* box.
 - Enter VLAN ID **11** in the *Guest VLAN* box.
4. In the Port 2 *802.1x* entries, select **Authenticator (MAC Based)**.
5. If this ethernet port is to support MAC authentication bypass, then select the **Enable MAC authentication bypass** box.

Enabling this option allows users with registered MAC addresses to be transparently authorized without having to log in. A user entry on the RADIUS server needs to be created using the client MAC address as both the username and password. (The MAC address format is a single string of characters without punctuation.) If MAC authentication is unsuccessful, the normal 802.1X authentication exchange is attempted.

6. In the *Ethernet Ports* page, click **Submit** to save your changes.

Figure 125. Ethernet Ports page



Step 4: Configuring the RADIUS Server

For dynamic VLAN to work, you must configure the following RADIUS attributes for each user:

- *Tunnel-Type*: Set this attribute to **VLAN**.
- *Tunnel-Medium-Type*: Set this attribute to **IEEE-802**.
- *Tunnel-Private-Group-ID*: Set this attribute to the VLAN ID to which you want to segment this user.



NOTE: Some RADIUS servers may also require the *User-Name* attribute to be configured.

Table 27. RADIUS user attributes required by dynamic VLAN

Attribute	Type ID	Expected Value (Numerical)
Tunnel-Type	64	VLAN (13)
Tunnel-Media-Type	65	802 (6)
Tunnel-Private-Group-ID	81	VLAN ID

Sample FreeRADIUS Entries

0018ded90ef3 (MAC address)

User-Name = user1,
Tunnel-Type = VLAN,
Tunnel-Medium-Type = IEEE-802,
Tunnel-Private-Group-ID = 0010

00242b752ec4 (MAC address)

User-Name = user2,
Tunnel-Type = VLAN,
Tunnel-Medium-Type = IEEE-802,
Tunnel-Private-Group-ID = 0012

In this scenario, when user1 client associates with the WLAN, the RADIUS server authenticates user1, and user1 joins the AP and is segmented to VLAN 10 which has been assigned by the RADIUS server.

However, when user2 client associates with the WLAN, the RADIUS server authenticates user2 and returns VLAN ID 12 to the AP, and because user2 is not assigned to VLAN 10, user2 is assigned to the Guest VLAN.

Creating a Hotspot

A hotspot is a venue or area that provides wireless Internet access to devices with wireless networking capability, such laptops, PDAs, and other portable devices. Hotspots are usually available in public venues such as hotels, airports, restaurants, and shopping malls.



NOTE: The hotspot feature is only available on ZoneFlex 2942 APs that are running on software version 5.1 and later.

Your ZoneFlex 2942 AP has a built-in hotspot feature that you can enable and configure to provide hotspot service to users in your environment. In addition to your ZoneFlex 2942 AP, you need the following to deploy a hotspot:

- **Web Server:** You need a Web server that can host the external portal/login page that clients use to gain access to the hotspot service. More information in the Web server requirements is available in the *ZoneFlex 2942 Hotspot Application Notes* (see note below).
- **RADIUS Server:** A Remote Authentication Dial-In User Service (RADIUS) through which users can authenticate.

For installation and configuration instructions for the captive portal and RADIUS server software, refer to the documentation that was provided with them.



NOTE: If you need additional information on how to deploy a hotspot with ZoneFlex 2942, contact Ruckus Wireless Support at support@ruckuswireless.com and request 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 are using for your hotspot deployment.
- Have the following information ready:
 - Redirect URL for the captive portal (the Web page where clients log on to gain access to the hotspot service)
 - RADIUS server IP address
 - RADIUS server shared secret

Decide on which wireless interface you want to use for the hotspot. ZoneFlex 2942 has four wireless interfaces; you can use any of these. You should also verify that Wireless Availability is enabled on that wireless interface.

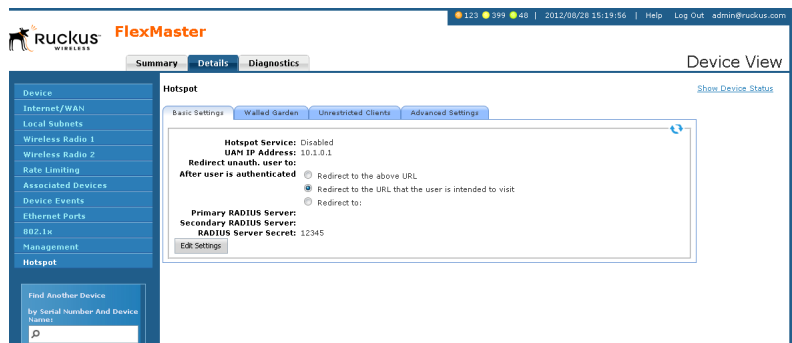


NOTE: A wireless interface must be part of either the Management VLAN or Available Wireless Interfaces before you can set it as the hotspot interface. If the wireless interface belongs to any VLAN other than the Management VLAN, you are unable to set it as the hotspot interface and the following message appears: `The specified wireless interface is not available for the hotspot service.`

Configuring Basic Hotspot Settings

Basic hotspot settings cover the essential configuration that you need to perform to make your hotspot operational. In this procedure, you need to configure the settings shown in [Figure 126](#).

Figure 126. Hotspot page Basic Settings tab



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 can select any of these.



NOTE: By default, client isolation is enabled on the hotspot interface. This means wireless clients that are connected to the same hotspot service are unable to communicate with each other.

5. In **Hotspot Wired Interface**, select the wired interfaces that you want to include in the hotspot service. Any device (for example, a network printer) connected to a wired interface that is part of the hotspot is accessible to hotspot users.



NOTE: 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 can appear:

Interface {name or number} is already being used in a VLAN

To switch to another interface, do the following:

1. Disable the hotspot service.
2. Switch to another wired or wireless interface.
3. Enable the hotspot service.

6. In **Redirect URL**, type the URL to which users are redirected after they associate with the hotspot and launch their Web browser. This is the URL of the captive portal that you have set up, where users need to enter their user name and password to access the Internet service that your hotspot provides.
7. In **Primary RADIUS Server**, type the IP address of the RADIUS server on the network. Users logging on to the hotspot authenticate with this RADIUS server.
8. In **RADIUS Server Secret**, type the shared secret that you have configured on the RADIUS server. The shared secret is a password that is used to secure the communication between the AP and the RADIUS server.
9. Click **Submit**. The message "Task #{N} is submitted. Please check the status area." appears.
10. Check the Status Area at the 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 a Walled Garden

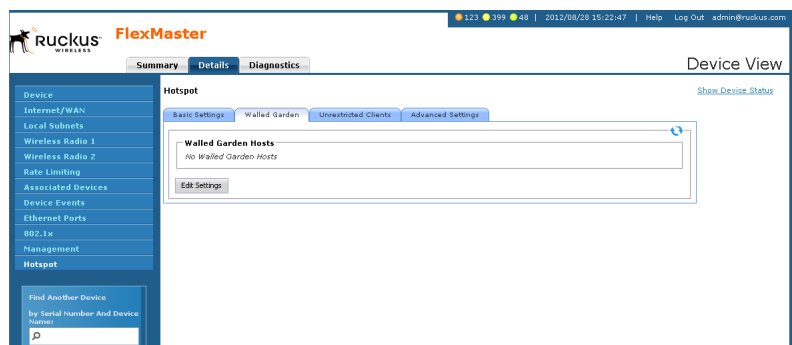
The term *walled garden* refers to a list of URLs that users (who are associated with your hotspot) can access without providing a user name and password. If you are operating the hotspot in a hotel, for example, you can include the hotel's Web site in the walled garden. A walled garden for a corporate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

You can add up to 64 entries to the Walled Garden hosts list. The following are the types of entries that are supported:

- IP address (for example, 10.1.1.1)
- IP address/network mask (for example, 1.1.1.1/24)
- Domain name (for example, mydomainname.com)

You can also append a port number to any of these entries (for example, mydomainname.com:80).

Figure 127. Hotspot page Walled Garden tab



Follow these steps to add an entry to the walled garden list.

1. On the Hotspot page, click the **Walled Garden** tab. The Walled Garden Hosts page appears.
2. Click 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.

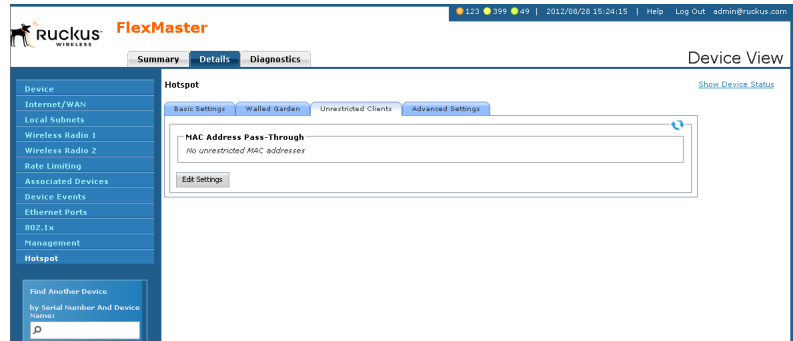
Repeat the same procedure for each entry that you want to add to the list.

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 128. Hotspot page Unrestricted Clients tab



Follow these steps to add a MAC address to the pass-through list.

1. On the *Hotspot* page, click the **Unrestricted Clients** tab. The MAC Address Pass-Through 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.

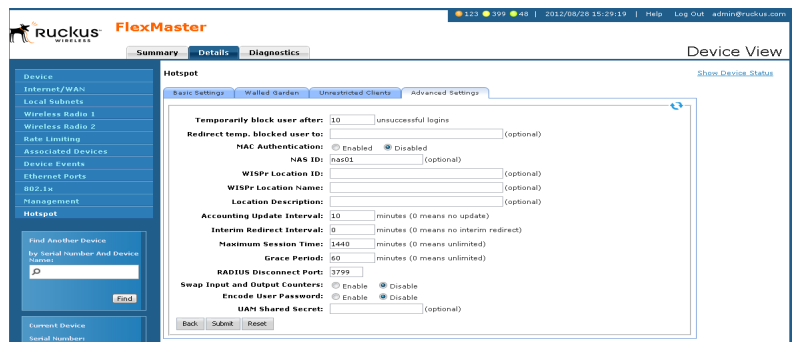
Repeat the same procedure for each entry that you want to add to the pass-through list.

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 129. Hotspot page Advanced Settings tab



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 also functions as a backup server in case the primary server becomes unavailable.
 - **NAS ID**: Type the name which the RADIUS server uses to 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 uses to access the ChilliSpot login CGI (`hotspot.login.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 automatically authenticates these devices with the RADIUS server using their MAC addresses.



NOTE: Before these portable devices can access the hotspot service, you need to manually add their MAC addresses to the database of pre-approved devices on the RADIUS server. For information on how to do this, refer to the documentation provided with your RADIUS server software.

4. If your ISP is blocking outgoing SMTP messages to control spam, then you can redirect your SMTP traffic to an external mail server (not within your ISP's domain) to ensure that hotspot users are 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 is 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 assigns 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 assigns 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, these attributes identify this specific hotspot location in the RADIUS data, which may be helpful for accounting.

Figure 130. Hotspot page Advanced Settings tab

The screenshot shows the Ruckus FlexMaster web interface. The left sidebar contains a navigation menu with categories like Device, Internet/WAN, Local Subnets, Wireless Radio 1, Rate Limiting, Associated Devices, Device Events, Ethernet Ports, 802.1x, Management, and Hotspot. The main content area is titled 'Hotspot' and has tabs for Basic Settings, Walled Garden, Unrestricted Clients, and Advanced Settings. The Advanced Settings tab is active, displaying various configuration fields for a hotspot. The fields include: 'Temporarily block user after' (10), 'Redirect temp. blocked user to' (unsuccessful logins), 'NAC Authentication' (Enabled/Disabled), 'NAS ID' (nas01), 'WISPr Location ID', 'WISPr Location Name', 'Location Description', 'Accounting Update Interval' (10), 'Interim Redirect Interval' (0), 'Maximum Session Time' (1440), 'Grace Period' (60), 'RADIUS Disconnect Port' (3799), 'Swap Input and Output Counters' (Enable/Disable), 'Encode User Password' (Enable/Disable), and 'UAM Shared Secret'. A 'Find' button is visible in the bottom left of the main content area.

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:
 - *isocc* (ISO-country-code) – The ISO country code that the AP includes in RADIUS authentication and accounting requests.
 - *cc* (country-code) – The ITU country code that the AP includes in RADIUS authentication and accounting requests.
 - *ac* (area-code) – The ITU area code that the AP includes in RADIUS authentication and accounting requests.
 - *network* - (to be determined)

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

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

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.

Monitoring Events and Network Activities

In This Chapter

About the Monitor Page	214
Monitoring Alarms	214
Configuring Alarm Settings	217
Monitoring Events	219
Creating an Event View	222
Managing Event Views	223
Viewing the Event TimeLine	225
Configuring Alert Properties	228
Measuring Throughput Using SpeedFlex	230
Monitoring Access Point Trends	233
Monitoring Client Trends	234

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 Alarms

Alarms are a type of event that typically warrants your attention. Alarms are generated by managed access points and ZoneDirector devices and the FlexMaster server.

Alarms vary in severity. The following are the four alarm severity levels in FlexMaster (from highest severity to lowest severity):

- Critical
- Major
- Minor
- Warning

Viewing and Acknowledging Alarms

Acknowledging an alarm lets other FlexMaster administrators know that someone is already looking into the issue.

1. Go to **Monitor > Alarms**. The **Active** tab, which lists the most recent alarms, appears by default. The **History** tab displays older alarms that have been acknowledged.

2. To acknowledge an alarm, click the alarm **Acknowledge** link.

FlexMaster moves the alarm to the History tab, the *Acknowledge* column displays Yes, and the *Ack Time* column displays the date and time when the alarm was acknowledged.

3. To view other alarms that have already been acknowledged, click the **History** tab.

Figure 131. The Alarms page

The screenshot shows the FlexMaster Alarms page. The interface includes a navigation bar with tabs for Dashboard, Inventory, Monitor, Configure, Reports, and Administer. The left sidebar contains links for Alarms, Alarm Settings, Events, Manage Event Views, Event TimeLine, Alert Properties, SpeedFlex, Access Point Trend, Client Trend, and Notes. The main content area is titled 'Alarms' and has tabs for Active and History. Below the tabs is an 'Info' section with a 'Filter Rows where:' dropdown menu and a search input field. The 'List of Alarms' table contains the following data:

Date/Time	Alarm Type	Severity	Device Name	Activity	Acknowledge	Ack Time
07/30 18:28	AP lost connection	Major	SDCFMQA_Redundant_	AP[6c:67:06:1e:45:30] has been continuously disconnected for [7 day(s) 16 h	Acknowledge	
07/30 18:28	AP lost connection	Major	SDCFMQA_ZD1100-IPV	AP[00:20:01:08:31:60] has been continuously disconnected for [12 day(s) 23	Acknowledge	
07/30 18:28	AP lost connection	Major	ruckus-access	AP[04:10:8a:10:15:40] has been continuously disconnected for [125 day(s) 22	Acknowledge	
07/30 18:28	AP lost connection	Major	ruckus-access	AP[00:24:82:24:61:20] has been continuously disconnected for [115 day(s) 15	Acknowledge	
07/30 18:28	AP lost connection	Major	ruckus-access	AP[68:92:34:1b:6b:00] has been continuously disconnected for [21 day(s) 23	Acknowledge	
07/30 18:28	AP lost connection	Major	ruckus-access	AP[0c:c5:20:04:be:b0] has been continuously disconnected for [24 day(s) 15	Acknowledge	
07/30 18:28	AP lost connection	Major	ruckus-access	AP[04:10:8a:20:e9:20] has been continuously disconnected for [24 day(s) 19	Acknowledge	
07/30 18:28	AP lost connection	Major	ruckus-access	AP[68:92:34:1b:6a:80] has been continuously disconnected for [24 day(s) 18	Acknowledge	
07/30 18:28	AP lost connection	Major	ruckus-access	AP[68:92:34:29:17:90] has been continuously disconnected for [35 day(s) 15	Acknowledge	
07/30 18:28	AP lost connection	Major	SDCFMQA_7731_1K1	AP[60:44:00:00:00:80] has been continuously disconnected for [5 day(s) 17 h	Acknowledge	
07/30 18:28	AP lost connection	Major	SDCFMQA_7731_1K1	AP[00:8a:da:1d:82:60] has been continuously disconnected for [3 day(s) 8 h	Acknowledge	
07/30 18:28	AP lost connection	Major	SDCFMQA_7731_1K1	AP[00:24:82:25:6d:20] has been continuously disconnected for [5 day(s) 22 h	Acknowledge	
07/30 18:21	AP lost heartbeat	Major	SDCFMQA_Redundant_	AP[74:91:1a:1f:fb:90] heartbeats lost	Acknowledge	
07/30 02:12	Admin upgrade	Warning	SDCFMQA_7731_1K1	System is upgraded.	Acknowledge	

Filtering Alarms

Use the *Info* section on the **Active** and **History** tabs to filter alarms based on a set of criteria.


1. On either the **Active** or **History** tab, look for the *Info* section. To search for alarms, you need to specify the criteria of the alarms that you want to display.
2. In the first drop-down list box after **Filter Rows where**, select the filter attribute that you want to use. Options include Date/Time, Alarm Type, Severity, Device Name, and Acknowledge status.
3. In the second drop-down list box, select the filter operator that you want to use. Available filter operators include:
 - **Exactly equals**: Filter alarms with attributes that exactly match the filter parameter you entered. For example, if you selected **Severity** as the attribute and you entered **Critical** as the filter parameter, only critical alarms appear in the filter results.
 - **Contains** (available only if **Device Name** is selected in the first drop-down list): Filter devices with attributes that include the filter parameter you entered. For example, if you selected **Device Name** as the attribute and you entered **Ruckus** as the filter parameter, all devices with "ruckus" in the device name (for example, **ruckusAP** and **APruckus**) appear in the filter results.
 - **Starts with** (available only if **Device Name** is selected in the first drop-down list): Filter devices with attributes that start with the filter parameter you entered. For example, if you selected **Device Name** as the attribute and you entered **Ruckus** as the filter parameter, only devices with device names that begin with "ruckus" (for example, **ruckusAP1**, **ruckusAP2**) appear in the filter results.

Monitoring Events and Network Activities

Monitoring Alarms

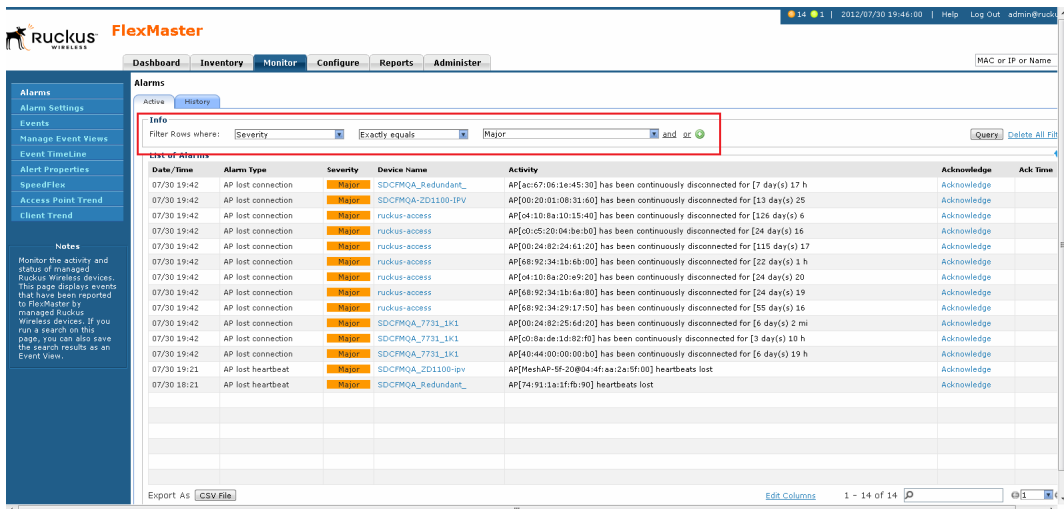
- **Ends with** (available only if **Device Name** is selected in the first drop-down list): Filter devices with attributes that end with the filter parameter you entered. For example, if you selected **Device Name** as the attribute and you entered **AP** as the filter parameter, only devices with device names that end in "AP" (for example, **ruckusAP**, **lobbyAP**) appear in the filter results.
- **Later than** or **Earlier than** (available only if **Date/Time** is selected in the first drop-down list): Filter alarms based on the specified date and time.

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

4. In the text box, type the filter parameter that you want to use with the attribute and operator that you selected. The required filter parameter depends on the attribute that you selected in the first drop-down list box.
 - If you selected **Date/Time**, select a date and time in the text box.
 - If you selected **Alarm Type**, select a specific alarm that you want to filter.
 - If you selected **Severity**, select a severity level (Warning, Minor, Major, Critical) that you want to filter.
 - If you selected **Device Name**, type the partial or full string of the device name that you want to filter.
 - If you selected **Acknowledge**, select the acknowledgement status (No, Yes, Recovered, Duplicate) that you want to filter.
5. If you want to add another filter, click . A second filter layer appears below the first. Complete the filter options as in the first filter. You can add up to three additional filters.
6. When you complete setting up the search filters, click **Query**. FlexMaster displays the alarms that match the filter criteria.

You have completed filtering alarms.

Figure 132. Creating a filter for major alarms



The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes Dashboard, Inventory, Monitor, Configure, Reports, and Administer. The left sidebar contains various monitoring tools like Alarms, Alarm Settings, Events, and Event Timeline. The main content area is titled "Alarms" and shows a table of active alarms. A filter is applied to the "Severity" column, set to "Exactly equals" and "Major". The table lists various alarms, including "AP lost connection" and "AP lost heartbeat", with columns for Date/Time, Alarm Type, Severity, Device Name, Activity, Acknowledge, and Ack Time. The bottom of the interface shows an "Export As" option set to "CSV File" and a page indicator "1 - 14 of 14".

Date/Time	Alarm Type	Severity	Device Name	Activity	Acknowledge	Ack Time
07/30 19:42	AP lost connection	Major	SDCFMQA_Redundant_	AP[ac:47:06:1e:45:30] has been continuously disconnected for [7 day(s) 17 h	Acknowledge	
07/30 19:42	AP lost connection	Major	SDCFMQA_ZD1100-IPV	AP[00:20:01:06:31:60] has been continuously disconnected for [13 day(s) 25	Acknowledge	
07/30 19:42	AP lost connection	Major	ruckus-access	AP[04:10:8a:10:15:49] has been continuously disconnected for [126 day(s) 6	Acknowledge	
07/30 19:42	AP lost connection	Major	ruckus-access	AP[00:20:04:3e:bb] has been continuously disconnected for [24 day(s) 16	Acknowledge	
07/30 19:42	AP lost connection	Major	ruckus-access	AP[00:24:82:24:61:20] has been continuously disconnected for [115 day(s) 17	Acknowledge	
07/30 19:42	AP lost connection	Major	ruckus-access	AP[68:92:34:1b:6b:00] has been continuously disconnected for [22 day(s) 1 h	Acknowledge	
07/30 19:42	AP lost connection	Major	ruckus-access	AP[04:10:8a:20:e9:20] has been continuously disconnected for [24 day(s) 20	Acknowledge	
07/30 19:42	AP lost connection	Major	ruckus-access	AP[68:92:34:1b:6a:80] has been continuously disconnected for [24 day(s) 19	Acknowledge	
07/30 19:42	AP lost connection	Major	ruckus-access	AP[68:92:34:29:17:50] has been continuously disconnected for [55 day(s) 16	Acknowledge	
07/30 19:42	AP lost connection	Major	SDCFMQA_7731_1K1	AP[00:24:82:25:6d:20] has been continuously disconnected for [3 day(s) 2 mi	Acknowledge	
07/30 19:42	AP lost connection	Major	SDCFMQA_7731_1K1	AP[00:8a:1d:1d:82:ff] has been continuously disconnected for [3 day(s) 10 h	Acknowledge	
07/30 19:42	AP lost connection	Major	SDCFMQA_7731_1K1	AP[40:44:00:00:00:80] has been continuously disconnected for [6 day(s) 19 h	Acknowledge	
07/30 19:21	AP lost heartbeat	Major	SDCFMQA_ZD1100-IPV	AP[MeshAP-5F-20@04:4f:ea:2a:5f:00] heartbeats lost	Acknowledge	
07/30 18:21	AP lost heartbeat	Major	SDCFMQA_Redundant_	AP[74:91:1a:1f:fb:90] heartbeats lost	Acknowledge	

Configuring Alarm Settings

1. Go to **Monitor > Alarm Settings**. The Alarm Settings page appears.
2. Configure the *Enable Alarm Light* section. When the alarm lights are enabled, they appear on the Help and Logout bar in the upper right corner of the Web interface.
 - To enable the alarm lights (default), click **Yes**.
 - To disable the alarm lights, click **No**.

Click the **Save** button in the *Enable Alarm Light* section.

3. In the *Email Notification* section, configure the email address to which alarm notifications are sent. You also need to define the alarm severity for which to send notifications.
 - In *Email Addresses*, click **Edit**, and then type the email address to which to send notifications. Use a semi-colon (;) to separate multiple email addresses.
 - In *Severity Criteria*, select the check boxes for the alarm severity for which you want to send notifications. Options include *All*, *Warning*, *Minor*, *Major* and *Critical*.

Click the **Save** button in the *Email Notification* section.

4. Configure the alarm types in the *User Customized Alarm* section by assigning a severity level and setting a threshold value to each alarm type. These alarms include:
 - *AP # of clients*: Triggered when the number of clients per AP exceeds the specified threshold.
 - *AP lost connection*: Triggered when an AP is continuously disconnected for the specified threshold (number of hours).
 - *AP traffic*: Triggered when traffic on an AP exceeds the specified threshold (traffic in MB).
 - *FlexMaster server CPU usage*: Triggered when CPU usage on FlexMaster exceeds the specified threshold (CPU usage percentage).
 - *ZD CPU usage*: Triggered when CPU usage on a ZoneDirector device exceeds the specified threshold (CPU usage percentage).

Click the **Save** button in the *User Customized Alarm* section.

5. Configure the *Event Selection* section by selecting (enabling) events that trigger alarms. Events are categorized into the following groups:
 - System Admin
 - Mesh
 - Configuration
 - Client
 - AP Admin
 - Performance

Click the tab for an event group, click the **Edit** button at the bottom of the section, and then select the check boxes for events that trigger alarms. You can also change the severity level that is assigned to each event.

Click the **Save** button that is in the *Event Selection* section.

You have completed configuring the alarm settings.

Monitoring Events and Network Activities

Configuring Alarm Settings

Figure 133. The Alarm Settings page

FlexMaster

Dashboard | Inventory | Monitor | **Configure** | Reports | Administer

MAC or IP or Name

Alarm Settings

Enable Alarm Light: Yes No [Save](#)

Email Notification

Severity Criteria: All Warning Minor Major Critical

E-Mail Addresses: [Edit](#)

(Note: If input two or more E-mail addresses, please separate each address by a semicolon.)

User Customized Alarm

Enable	Severity	Alarm Type	Threshold	Description
<input checked="" type="checkbox"/>	Major	AP # of clients	exceed 100 AP client(s)	AP[{}]'s concurrently connected client number exceeded the threshold [{}]
<input checked="" type="checkbox"/>	Major	AP lost connection	exceed 4 hour(s)	AP[{}]'s has been continuously disconnected for [{}], exceeded the threshold
<input checked="" type="checkbox"/>	Major	AP Traffic	exceed 10240 MB in last hour	AP[{}]'s traffic exceeded the threshold [{}](MB) in last hour.
<input type="checkbox"/>	Critical	FlexMaster server CPU usage	exceed 80% up to 3 times continuously	FlexMaster server's CPU usage exceeded the threshold value [{}]% up to 3 t
<input type="checkbox"/>	Critical	ZD CPU usage	exceed 80% up to 3 times continuously	ZD[{}]'s CPU usage exceeded the threshold value [{}]% up to 3 times cont

[Edit](#)

Event Selection(Select miscellaneous event type to trigger the alarm)

System Admin | Mesh | configuration | Client | ap admin | **Performance**

Enable	Severity	Alarm Type	Description
<input checked="" type="checkbox"/>	Major	ZD System Failure Recovered	ZD system failure recovered.
<input type="checkbox"/>	Warning	AC license AP different	ZoneDirector and redundancy ZoneDirector have different licensed APs.
<input type="checkbox"/>	Warning	AC working mode	ZoneDirector automatically swaps working mode to [{}](mode)
<input type="checkbox"/>	Minor	AP 80211 DOS mgmt flood	AP[{}] detects excessive 802.11 management frames on radio [{}](radio).
<input type="checkbox"/>	Minor	AP 80211 DOS probe req flood	AP[{}] detects excessive probe requests on radio [{}](radio).
<input type="checkbox"/>	Warning	AP management URL changed	AP management URL changed
<input type="checkbox"/>	Minor	Ad hoc network detected	A new ad-hoc network [{}](ad-hoc) with SSID[{}](ssid) is detected
<input type="checkbox"/>	Minor	Ad hoc interference detected	An ad-hoc network [{}](ad-hoc) with SSID[{}](ssid) interferes with AP[{}](ap) on

Monitoring Events

FlexMaster keeps a record of all events that occur on the server, managed ZoneDirector devices, standalone APs, and even on clients that associated with managed APs.

The Events section displays system events that have been reported by the managed Ruckus Wireless devices. The *List of Events* table columns include:

- *Date/Time*: When the event occurred.
 - *Event Type*: Ruckus Wireless-designated event title.
 - *Sev*: Severity of the event.
 - *Device Name*: Name of the device.
 - *Activity*: A description of the event.
1. Go to **Monitor > Events**. The *List of 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 need to specify the criteria of the devices that you are looking for.
3. In the first drop-down list box after **Filter Rows where**, select the search attribute that you want to use. Options include Date/Time, Event Type, Sev(erity), and Device Name.
4. In the second drop-down list box, select the search operator that you want to use. Available search operators include:
 - *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **Model Name** as the attribute and you entered zD3250 as the search parameter, only devices of this model appear in the search results.
 - *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered 100 as the search parameter, all devices with "100" in the serial number (for example, **100**903000031 and 11090**100**0282) appear in the search results.

- **Starts with:** Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered 3208 as the query parameter, only devices with serial numbers that begin with “3208” (for example, 320833000219) appear in the search results.
- **Ends with:** Search for devices with attributes that end with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered 011 as the query parameter, only devices with model names that end in “001” (for example, 100903000001) appear in the search results.

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


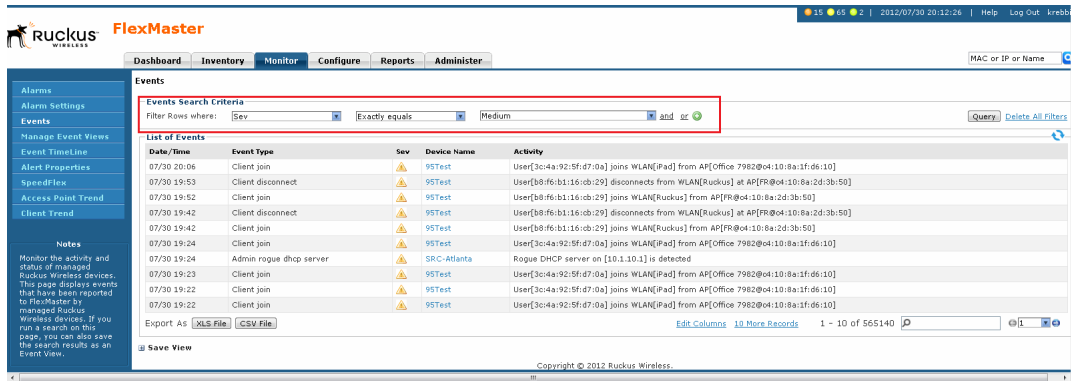
5. In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
6. If you want to add another search filter, 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 134. Using Search Criteria to search for an event



The screenshot shows the FlexMaster interface with the 'Events' section active. The 'Events Search Criteria' section is highlighted with a red box, showing a filter for 'Sev' with the operator 'Exactly equals' and the value 'Medium'. Below this, the 'List of Events' table displays the following data:

Date/Time	Event Type	Sev	Device Name	Activity
07/30 20:06	Client join	95Test	User[3c4a:92:5f:07:0a]	joins WLAN[Pad] from AP[Office 7982@04:10:8a:1f:d6:10]
07/30 19:53	Client disconnect	95Test	User[b8:f6:b1:16:cb:29]	disconnects from WLAN[Ruckus] at AP[FR@04:10:8a:2d:3b:50]
07/30 19:52	Client join	95Test	User[b8:f6:b1:16:cb:29]	joins WLAN[Ruckus] from AP[FR@04:10:8a:2d:3b:50]
07/30 19:42	Client disconnect	95Test	User[b8:f6:b1:16:cb:29]	disconnects from WLAN[Ruckus] at AP[FR@04:10:8a:2d:3b:50]
07/30 19:42	Client join	95Test	User[b8:f6:b1:16:cb:29]	joins WLAN[Ruckus] from AP[FR@04:10:8a:2d:3b:50]
07/30 19:24	Client join	95Test	User[3c4a:92:5f:07:0a]	joins WLAN[Pad] from AP[Office 7982@04:10:8a:1f:d6:10]
07/30 19:24	Admin rogue dhcp server	SR-C-Atlanta		Rogue DHCP server on [10.1.10.1] is detected
07/30 19:23	Client join	95Test	User[3c4a:92:5f:07:0a]	joins WLAN[Pad] from AP[Office 7982@04:10:8a:1f:d6:10]
07/30 19:22	Client join	95Test	User[3c4a:92:5f:07:0a]	joins WLAN[Pad] from AP[Office 7982@04:10:8a:1f:d6:10]
07/30 19:22	Client join	95Test	User[3c4a:92:5f:07:0a]	joins WLAN[Pad] from AP[Office 7982@04:10:8a:1f:d6:10]



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 are automatically added to the saved view.

Additional Tasks That You Can Perform

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

- Save the search results as XLS (Microsoft[®] Excel[®] file format): In **Export As**, click **XLS File**. When the Save As dialog box appears, click **Save File**, and then click **OK**. Use Microsoft Excel to open the file.

- Save the search results as CSV (comma-separated value file): In *Export As*, click **CSV File**. When the *Save As* dialog box appears, click **Save File**, and then click **OK**. You can use any spreadsheet application (such as Microsoft Excel) to open the file.
- Save the results as an event view: 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 are automatically added to the saved view.

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

FlexMaster searches all its database columns for a match to the string that you entered, and then displays the results in the *List of Events* table. The event property that matches the search string is highlighted in the table. In [Figure 135](#), the search string '95' matched part of devices names and are highlighted in yellow.

Figure 135. The device property that matches the search string is highlighted in the search results

The screenshot shows the FlexMaster web interface. The top navigation bar includes Dashboard, Inventory, Monitor, Configure, Reports, and Administer. The main content area is titled 'Events' and contains an 'Events Search Criteria' section with a search box and filters. Below this is a table with the following columns: Date/Time, Event Type, Sev, Device Name, and Activity. The 'Device Name' column is highlighted in yellow for several rows, indicating a search match. At the bottom right of the table, there is a search box containing the text '95'. The interface also includes a sidebar with navigation options like Alarms, Alarm Settings, Events, and Notes, and a footer with the copyright notice 'Copyright © 2012 Ruckus Wireless'.

Date/Time	Event Type	Sev	Device Name	Activity
07/30 20:11	Client join	▲	95Test	User[3c:4a:92:5f:d7:0a] joins WLAN[Pad] from AP[Office 7982@04:10:8a:1f:d6:10]
07/30 20:06	Client join	▲	95Test	User[3c:4a:92:5f:d7:0a] joins WLAN[Pad] from AP[Office 7982@04:10:8a:1f:d6:10]
07/30 19:53	Client disconnect	▲	95Test	User[b8:f6:b1:16:cb:29] disconnects from WLAN[Ruckus] at AP[FR@04:10:8a:2d:3b:50]
07/30 19:52	Client join	▲	95Test	User[b8:f6:b1:16:cb:29] joins WLAN[Ruckus] from AP[FR@04:10:8a:2d:3b:50]
07/30 19:42	Client disconnect	▲	95Test	User[b8:f6:b1:16:cb:29] disconnects from WLAN[Ruckus] at AP[FR@04:10:8a:2d:3b:50]
07/30 19:42	Client join	▲	95Test	User[b8:f6:b1:16:cb:29] joins WLAN[Ruckus] from AP[FR@04:10:8a:2d:3b:50]
07/30 19:24	Client join	▲	95Test	User[3c:4a:92:5f:d7:0a] joins WLAN[Pad] from AP[Office 7982@04:10:8a:1f:d6:10]
07/30 19:23	Client join	▲	95Test	User[3c:4a:92:5f:d7:0a] joins WLAN[Pad] from AP[Office 7982@04:10:8a:1f:d6:10]
07/30 19:22	Client join	▲	95Test	User[3c:4a:92:5f:d7:0a] joins WLAN[Pad] from AP[Office 7982@04:10:8a:1f:d6:10]
07/30 19:22	Client join	▲	95Test	User[3c:4a:92:5f:d7:0a] joins WLAN[Pad] from AP[Office 7982@04:10:8a:1f:d6:10]

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 you want to view events that have occurred on a group of devices.

1. Perform a search for event using 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.
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 136. Saving search results as an event view

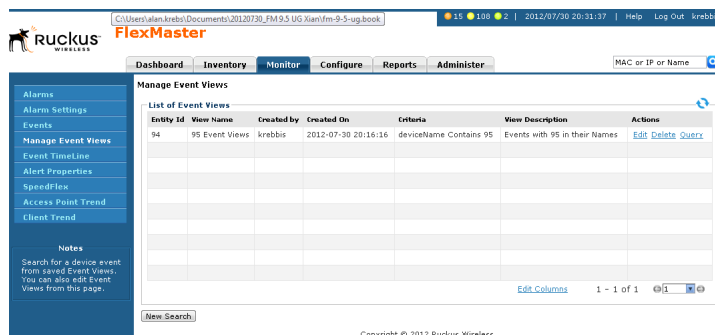
The screenshot shows the Ruckus FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The left sidebar contains various menu items like 'Alarms', 'Alarm Settings', 'Events', 'Manage Event Views', 'Event TimeLine', 'Alert Properties', 'SpeedFlea', 'Access Point Trend', 'Client Trend', and 'Notes'. The main content area is titled 'Events' and shows 'Events Search Criteria' with a search filter and a 'Query' button. Below this is a table of search results with columns for Date/Time, Event Type, Sev, Device Name, and Activity. The 'Save As View' section is highlighted with a red box, showing a 'View Name' field containing '95 Device Names' and a 'Description' field containing 'Devices with 95 in the Name'. There are 'Save' and 'Cancel' buttons next to the description field.

Date/Time	Event Type	Sev	Device Name	Activity
07/30 20:11	Client join	▲	95Test	User[3c:4a:92:5f:d7:0a] joins WLAN[Pad] from AP[Office 7982@04:10:8a:1f:d6:10]
07/30 20:06	Client join	▲	95Test	User[3c:4a:92:5f:d7:0a] joins WLAN[Pad] from AP[Office 7982@04:10:8a:1f:d6:10]
07/30 19:53	Client disconnect	▲	95Test	User[b8:f6:b1:16:cb:29] disconnects from WLAN[Ruckus] at AP[FR@04:10:8a:2d:3b:50]
07/30 19:52	Client join	▲	95Test	User[b8:f6:b1:16:cb:29] joins WLAN[Ruckus] from AP[FR@04:10:8a:2d:3b:50]
07/30 19:42	Client disconnect	▲	95Test	User[b8:f6:b1:16:cb:29] disconnects from WLAN[Ruckus] at AP[FR@04:10:8a:2d:3b:50]
07/30 19:42	Client join	▲	95Test	User[b8:f6:b1:16:cb:29] joins WLAN[Ruckus] from AP[FR@04:10:8a:2d:3b:50]
07/30 19:24	Client join	▲	95Test	User[3c:4a:92:5f:d7:0a] joins WLAN[Pad] from AP[Office 7982@04:10:8a:1f:d6:10]
07/30 19:23	Client join	▲	95Test	User[3c:4a:92:5f:d7:0a] joins WLAN[Pad] from AP[Office 7982@04:10:8a:1f:d6:10]
07/30 19:22	Client join	▲	95Test	User[3c:4a:92:5f:d7:0a] joins WLAN[Pad] from AP[Office 7982@04:10:8a:1f:d6:10]
07/30 19:22	Client join	▲	95Test	User[3c:4a:92:5f:d7:0a] joins WLAN[Pad] from AP[Office 7982@04:10:8a:1f:d6:10]

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

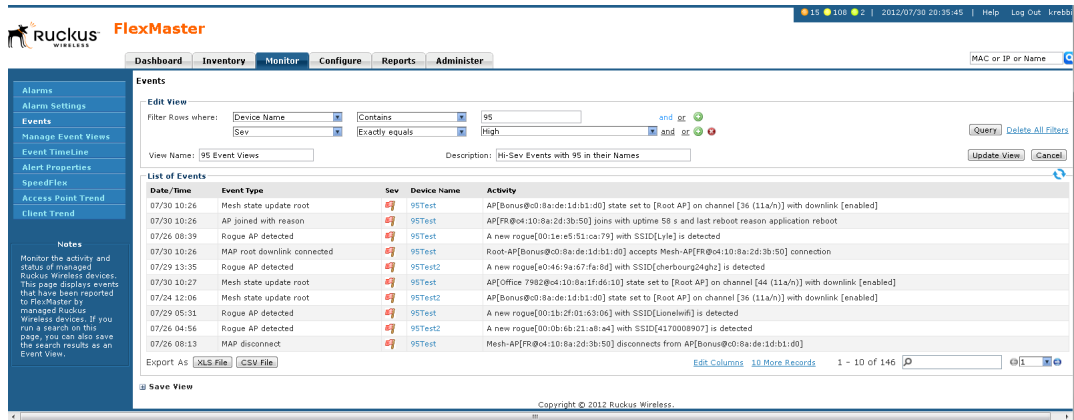


Editing an Event View

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

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



Deleting an Event View

1. Go to the **Inventory > ZoneDirector > Manage Views** page.
2. Click the event view **Delete** link. A confirmation message appears.
3. Click **OK** to confirm.

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

Viewing the Event Timeline

The Event Timeline chart displays the events that have occurred on FlexMaster and its managed devices. Events are displayed per severity and include one- or two-word descriptions. The Event Timeline chart is 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.

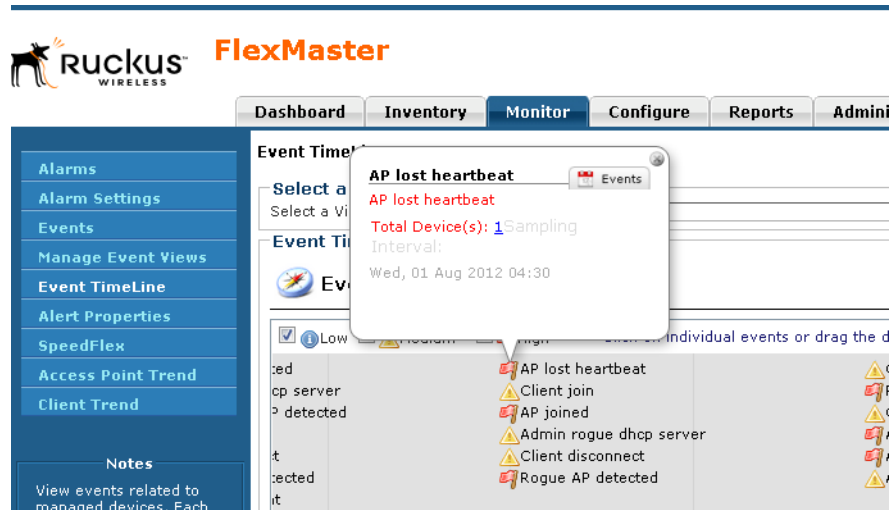
Figure 139. The Event Timeline widget



The Event Timeline widget uses the following conventions:

Device View widget	Click the Event Timeline 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"> • <i>Informational</i> events are lowest in severity, and are typically associated with configuration changes or device boot up. • <i>Warnings</i> events relate to device connectivity and communication. • <i>Errors</i> are critical events affecting the device's functionality.
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 Monitor > Reports view of the selected event. As the event may cover multiple devices, each device is displayed individually in the report.

Figure 140. The Event Detail pop-up window

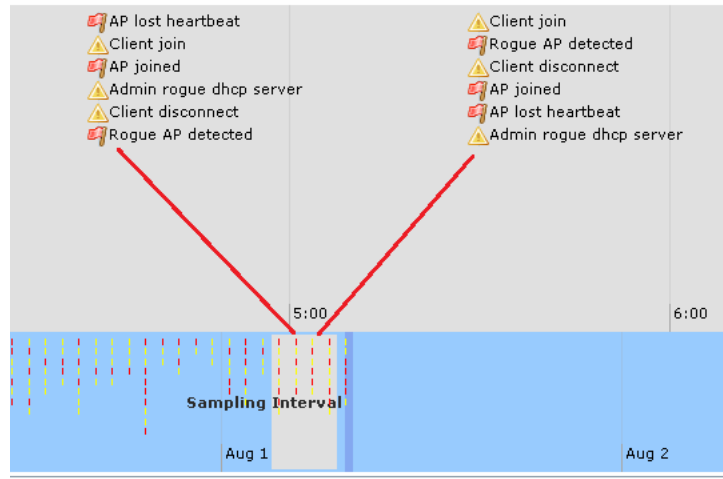


Colored Segments

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 141. Colored segments on the Events TimeLine widget

Horizontal bars or drag the day or hour bands to scroll through the events over a period of time.



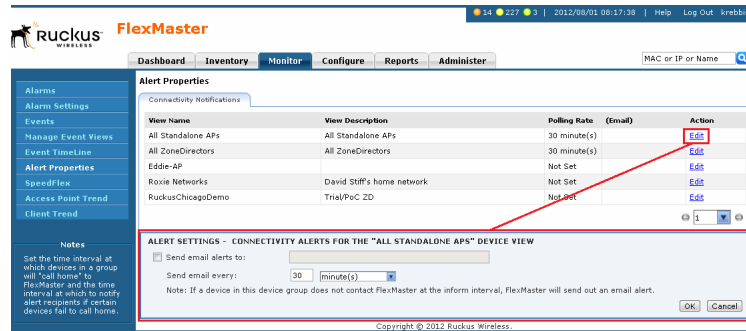
Hold and Drag

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 142. Editing the alert property of a group



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 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 143](#) 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 143. 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 144. Click the Cancel link to disable alert notifications for the device group

The screenshot shows the FlexMaster web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Monitor', 'Configure', 'Reports', and 'Administer'. The left sidebar contains various menu items like 'Alarms', 'Alarm Settings', 'Events', 'Manage Event Views', 'Event TimeLine', 'Alert Properties', 'SpeedFlex', 'Access Point Trend', and 'Client Trend'. The main content area is titled 'Alert Properties' and shows a table of 'Connectivity Notifications'. The table has columns for 'View Name', 'View Description', 'Polling Rate', 'Email', and 'Action'. The first row, 'All Standalone APs', has a 'Cancel' link in the Action column, which is highlighted with a red box. Other rows include 'All ZoneDirectors', 'Eddie-AP', 'Roxie Networks', and 'RuckusChicagoDemo'. A 'Notes' section is visible at the bottom left of the main content area.

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 fails because SpeedFlex is unable to communicate with the device behind the NAT server.

To use SpeedFlex, you must first create a SpeedFlex task to assign the destination and source devices. When you create the task, you can also set it to run based on a recurring schedule.

Creating a SpeedFlex Task

Creating a SpeedFlex task requires that you specify the destination and source devices for running the test.

1. Go to **Monitor > SpeedFlex**.
2. Click the **Create Test** button. The *New SpeedFlex Test* form appears.
3. If you want to measure the throughput between hops (devices between the source and destination devices) in a mesh topology, 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 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 tests 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. 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 runs.
 - d. In *Email report to*, type the email address to which the SpeedFlex test results are sent. If you want to send the report to multiple email addresses, use a comma (,) or semicolon (;) to separate the email addresses.
8. In *Test Name*, type a name that you want to use for this SpeedFlex test. After you save this test, it appears in the *List of SpeedFlex Table* with the test name that you assigned.
9. Click **Save**. The *List of SpeedFlex Test* table refreshes, and then the test that you created appears in the table.

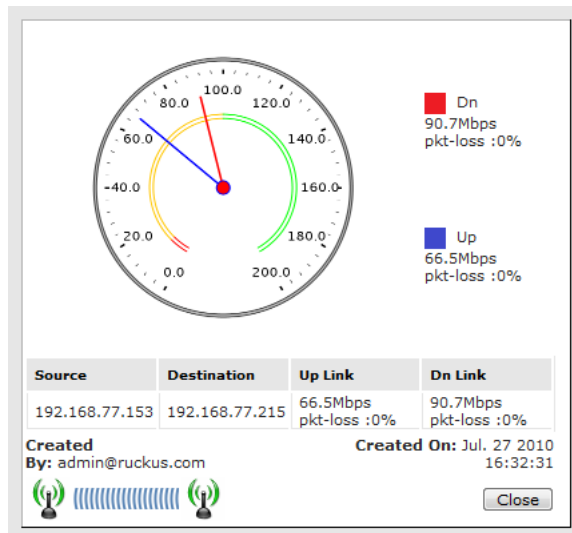
Running a SpeedFlex Task

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

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 145. 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.

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.

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 Access Point Trends

The *Access Point Trend* page on the *Monitor* tab allows you to display basic information about a Ruckus Wireless AP. You need to know the AP's MAC address to be able to run a query on it.

1. Go to the **Monitor > Access Point Trend** page.
2. In **MAC**, type the AP MAC address and click **Search**.

FlexMaster displays the AP's basic information under four tabs:

- *General Info*: The name and other information about the AP.
- *Mesh Info*: The mesh type and other information about this AP, when the AP is part of a mesh network.
- *WLANs*: The Name/ESSID of WLANs, and other information about this AP.
- *Radio*: The Current Channel used by this AP's radio.

3. To display trending graphs for the AP:

- Select a **Sampling Period**.
- Click **Generate Graphics**.

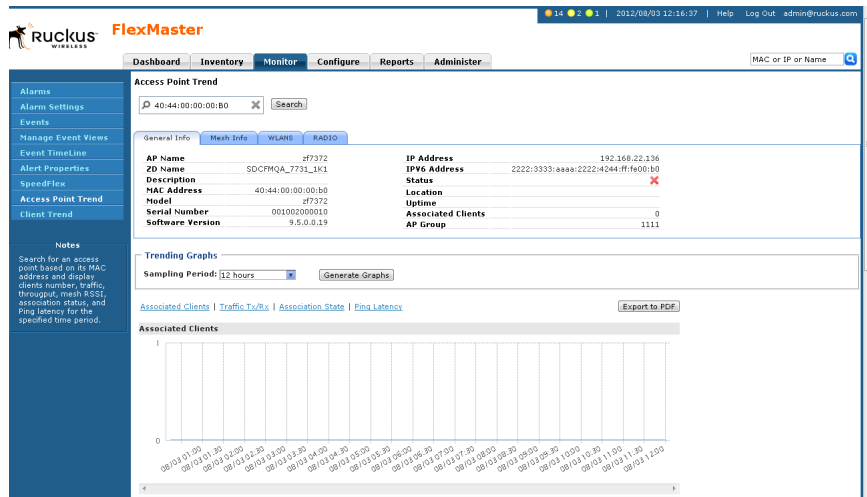
FlexMaster displays the AP's trends information at the bottom of the page:

- *Associated Clients*
- *Traffic Tx and Rx*
- *Association State*
- *Ping Latency*

Saving the AP Trends to PDF

- Click *Export to PDF*.
- FlexMaster prints the information on the screen to a PDF file on your workstation.

Figure 146. Access Point Trends page

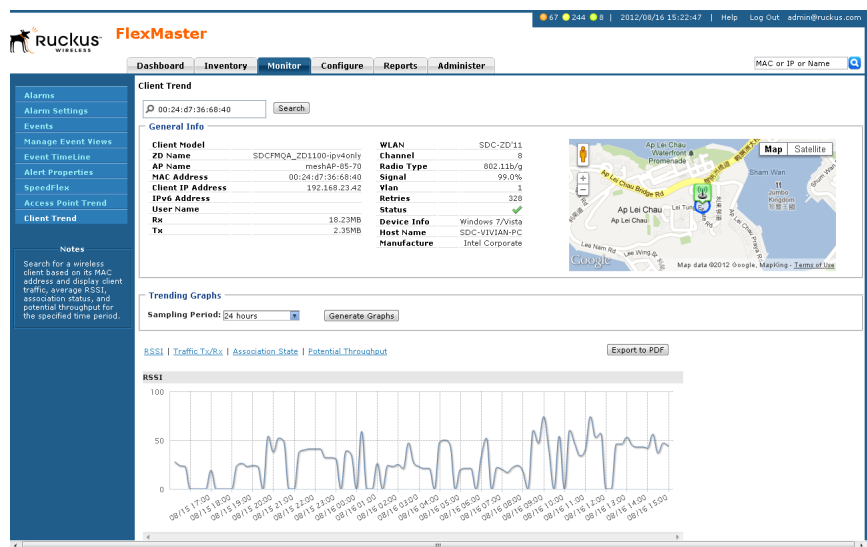


Monitoring Client Trends

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 need to know the wireless client's MAC address to be able to run a query on it.

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

Figure 147. Client Trend page



3. Click **Search**. The page refreshes, and then displays the client's basic information, including but not limited to:
 - **ZD Name**: The name of ZoneDirector device that is managing the client's parent AP.
 - **AP Name**: The name of the client's parent AP.
 - **User IP**: The IP address assigned to the client.
 - **WLAN**: The SSID or wireless network name with which the client is associated.
 - **Channel**: The wireless channel used by the WLAN.
 - **Radio**: The wireless radio used by the WLAN.
 - **Signal**: The RSSI strength of the WLAN.
 - **Status**: A green check mark indicates that the client is currently connected. A red cross mark indicates that it is disconnected.

The right side of the page also displays a map with the client location indicated by a blue circle. The client location is determined by the AP.

4. 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 Graphs**.

FlexMaster displays graphs of the client's RSSI, traffic, association state, and potential throughput.

Monitoring Events and Network Activities

Monitoring Client Trends

Working with Reports

In This Chapter

Available Report Types	238
Generating a Device View Report	239
Generating an Active Firmware Report	242
Generating a Historical Connectivity Report	244
Generating a Client Association Report	246
Generating an SSID Report	248
Generating a Provision Report	250
Generating Events-Related Reports	252
Generating a SpeedFlex Report	257
Generating a Capacity Report	258
Generating an SLA Report	260
Generating a Troubleshooting Report	261
Generating a Resource Monitor Report	263
Hiding and Showing Columns in Reports	265
Using Advanced Report Options	265
Managing Saved Reports	267

Available Report Types

The following table lists the different report types that you can generate in FlexMaster. For instructions on how to generate each type of report, refer to the succeeding sections.

Table 28. 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	View a list of devices that are currently using the selected firmware.
Historical Connectivity	View the connection statuses of managed devices in different device views.
Client Association	Identify clients that are currently associated with managed APs and managed APs are currently reporting to managed ZoneDirector devices.
SSID Report	View the number of ZoneDirector devices and APs on which a particular SSID is configured. You can also view graphs of associated clients, received traffic, and transmitted traffic per SSID.
Provision	List the statuses of all tasks that you have provisioned, categorized based on task types.
Events	List all events that match the selected event category, device category, and event type.
SpeedFlex	View completed throughput test results based on the test name, source or destination IP address, date executed, user, etc.
Capacity	Display device capacity data based on throughput, associated clients, airtime utilization, and traffic, among others.
SLA	Display SLA related information, including uptime, downtime, and potential throughput.
Troubleshooting	Generate various graphs that are useful for troubleshooting, including # of Child APs, # of Hops, Change of Topology of Mesh, Client Phy Rate, Client RSSI, Mesh RSSI, Physical Link Distance and Ping Test.
Resource Monitor	View CPU, memory, and disk usage on ZoneDirector devices.

Generating a Device View Report

A device view report includes device information such as, connected and disconnected devices and APs, connected wireless clients, wireless mesh report, connectivity report, diagnostic report, and bridge AP report.



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

1. Go to **Reports > Report Categories > Device View**.
2. Go to the *Report Options* section.
3. 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, then they also appear in the list of options.




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

4. 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
 - *All 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.
 - *Rogue APs*: Shows detected rogue access points.
 - 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).
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 device name, serial number, MAC address, IP address, model name, and last seen (among others).
 - b. In the second drop-down list box, select the search operator that you want to use. Available search operators include:
 - *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered 172 . 17 . 16 . 176 as the search parameter, then only devices with this IP address appear in the search results.
 - *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered 100 as the search parameter, all devices with “100” in the IP address (for example, 172 . 17 . 16 . **100** and **100** . 1 . 10 . 13) appear in the search results.
 - *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered 3908 as the query parameter, only devices with serial numbers that begin with “3908” (for example, 390801005202) appear in the search results.
 - *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected **IP address** as the attribute and you entered 13 as the query parameter, only devices with model names that end in “13” (for example, 100 . 1 . 10 . **13**) appear in the search results.

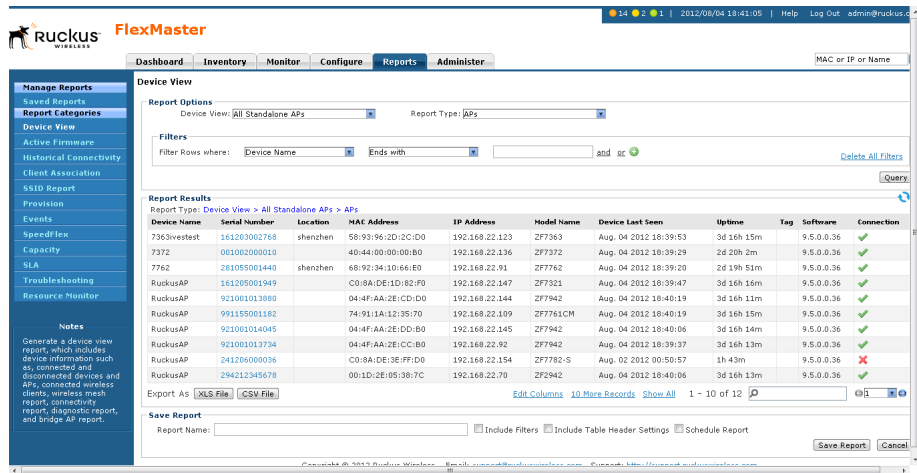
After you select a search operator, a third (text) box appears.

- c. In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
 - 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 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 148. An example of a device view report



The screenshot shows the Ruckus FlexMaster interface. The 'Reports' tab is active, and the 'Device View' report is displayed. The report is filtered for 'Standalone APs' and shows a list of devices with their details. The table below represents the data shown in the report.


Device Name	Serial Number	Location	MAC Address	IP Address	Model Name	Device Last Seen	Uptime	Tag	Software	Connection
7363vestest	161203002768	shenzhen	58:93:96:2D:2C:D0	192.168.22.123	ZF7363	Aug. 04 2012 18:39:53	3d 16h 15m		9.5.0.0.36	✓
7372	001002000010		40:44:00:00:00:80	192.168.22.136	ZF7372	Aug. 04 2012 18:39:29	2d 20h 2m		9.5.0.0.36	✓
7762	281058001440	shenzhen	68:92:34:10:66:E0	192.168.22.91	ZF7762	Aug. 04 2012 18:39:20	2d 19h 51m		9.5.0.0.36	✓
RuckusAP	161205001949		C0:8A:DE:1D:82:F0	192.168.22.147	ZF7321	Aug. 04 2012 18:39:47	3d 16h 15m		9.5.0.0.36	✓
RuckusAP	921001011380		04:4F:AA:2E:CD:D0	192.168.22.144	ZF7942	Aug. 04 2012 18:40:19	3d 16h 11m		9.5.0.0.36	✓
RuckusAP	991155001182		74:91:1A:12:35:70	192.168.22.109	ZF7761CM	Aug. 04 2012 18:40:19	3d 16h 15m		9.5.0.0.36	✓
RuckusAP	921001014045		04:4F:AA:2E:DD:80	192.168.22.145	ZF7942	Aug. 04 2012 18:40:06	3d 16h 14m		9.5.0.0.36	✓
RuckusAP	921001013734		04:4F:AA:2E:CC:80	192.168.22.92	ZF7942	Aug. 04 2012 18:39:37	3d 16h 13m		9.5.0.0.36	✓
RuckusAP	241084000056		C0:8A:DE:3E:FF:D0	192.168.22.154	ZF7762-S	Aug. 02 2012 00:50:57	11h 43m		9.5.0.0.36	✓
RuckusAP	294212345678		00:1D:2E:05:36:7C	192.168.22.70	ZF2942	Aug. 04 2012 18:40:06	3d 16h 13m		9.5.0.0.36	✓

Generating an Active Firmware Report

An active firmware report shows the firmware versions that are currently installed on APs or ZoneDirector devices that FlexMaster is managing.

1. Go to **Reports > Report Categories > Active Firmware**.
2. Go to the *Report Options* section.
3. In *Firmware*, click the device model–firmware version combination that you want to search for. The options that appear on this menu correspond to the firmware files that you uploaded to FlexMaster on the **Configure > Common > Manage Firmware Files** page.
4. (Optional) If you want to add a search filter to your query, then configure the options in the **Filters** section.
 - a. In the first drop-down list box after **Filter Rows where**, select the search attribute that you want to use. Options include device name, serial number, MAC address, IP address, model name, 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 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) 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) 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**) appear in the search results.

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

 - c. In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
 - 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.
5. 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 149. An example of an active firmware report

The screenshot shows the Ruckus FlexMaster web interface. The main content area displays an 'Active Firmware' report. The report options are set to 'Firmware: Model ZF7942; Firmware 9.5.0.0.36'. The report results table is as follows:

Device Name	Serial Number	MAC Address	IP Address	Model Name	Device Last Seen	Uptime	Tag	Software	Connection
RuckusAP	921001013734	04:4F:AA:2E:CC:B0	192.168.22.92	ZF7942	Aug. 04 2012 20:07:28	3d 17h 41m		9.5.0.0.36	✓
RuckusAP	921001013880	04:4F:AA:2E:CD:D8	192.168.22.144	ZF7942	Aug. 04 2012 20:07:02	3d 17h 38m		9.5.0.0.36	✓
RuckusAP	921001014045	04:4F:AA:2E:DD:B0	192.168.22.145	ZF7942	Aug. 04 2012 20:07:27	3d 17h 41m		9.5.0.0.36	✓

At the bottom of the report, there are options to 'Export As' (XLS File, CSV File), 'Save Report' (with a text field for the report name), and checkboxes for 'Include Filters', 'Include Table Header Settings', and 'Schedule Report'.

Generating a Historical Connectivity Report

A historical connectivity report displays the connection statuses of managed devices in different device views.

1. Go to **Reports > Report Categories > Historical Connectivity**.
2. Go to the *Report Options* section.
3. 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, then they also appear in the list of options.




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

4. 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.
 - *Continuously Disconnected APs*: Shows all APs that have continuously 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
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 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) 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) 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**) appear in the search results.

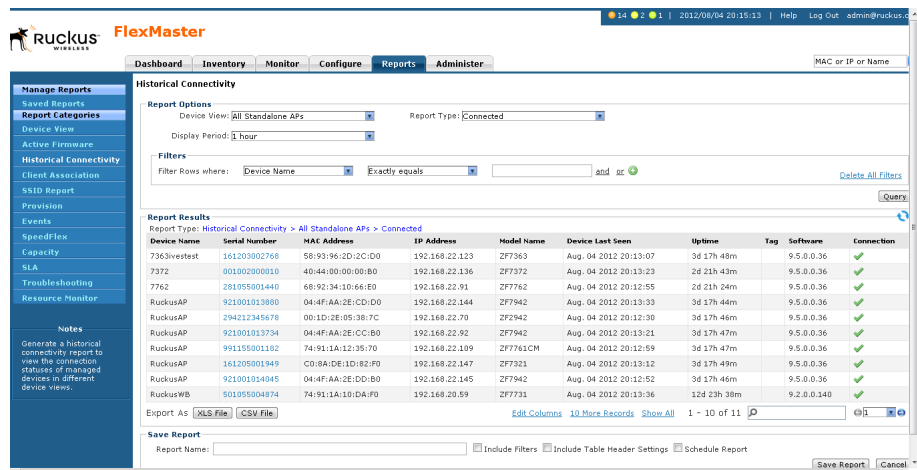
After you select a search operator, a third (text) box appears.

- c. In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
- 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 devices that have not called home to FlexMaster within the defined inform interval.

Figure 150. An example of a connectivity report



The screenshot shows the Ruckus FlexMaster interface. The 'Reports' tab is active, and the 'Historical Connectivity' report is displayed. The report options show 'Device View' set to 'All Standalone APs' and 'Report Type' set to 'Connected'. The display period is set to 'hour'. A search filter is applied: 'Filter Rows where: Device Name Exactly equals'. The report results table is as follows:

Device Name	Serial Number	MAC Address	IP Address	Model Name	Device Last Seen	Uptime	Tag	Software	Connection
7363vestest	161203002768	58-93-96:2D:2C:D0	192.168.22.123	ZF7363	Aug. 04 2012 20:13:07	3d 17h 48m		9.5.0.0.36	✓
7372	001002000010	40-44-00:00:00:B0	192.168.22.136	ZF7372	Aug. 04 2012 20:13:23	2d 21h 43m		9.5.0.0.36	✓
7762	281055001440	68-92:34:10:66:E0	192.168.22.91	ZF7762	Aug. 04 2012 20:12:55	2d 21h 24m		9.5.0.0.36	✓
RuckusAP	921001013800	04:4F:AA:2E:CD:D0	192.168.22.144	ZF7942	Aug. 04 2012 20:13:33	3d 17h 44m		9.5.0.0.36	✓
RuckusAP	294211345678	00:1D:2E:05:3B:7C	192.168.22.70	ZF2942	Aug. 04 2012 20:12:30	3d 17h 46m		9.5.0.0.36	✓
RuckusAP	921001013734	04:4F:AA:2E:CC:B0	192.168.22.92	ZF7942	Aug. 04 2012 20:13:21	3d 17h 47m		9.5.0.0.36	✓
RuckusAP	991155001182	74-91:1A:12:35:70	192.168.22.109	ZF7761CM	Aug. 04 2012 20:12:59	3d 17h 47m		9.5.0.0.36	✓
RuckusAP	161205001949	C0:8A:DE:1D:82:F0	192.168.22.147	ZF7321	Aug. 04 2012 20:13:12	3d 17h 49m		9.5.0.0.36	✓
RuckusAP	921001014045	04:4F:AA:2E:DD:B0	192.168.22.145	ZF7942	Aug. 04 2012 20:12:52	3d 17h 46m		9.5.0.0.36	✓
RuckusWB	501955004874	74-91:1A:10:DA:F0	192.168.20.59	ZF7731	Aug. 04 2012 20:13:36	12d 23h 38m		9.2.0.0.148	✓

Generating a Client Association Report

A client association report identifies the clients that are currently associated with managed APs and the managed APs that are currently reporting to managed ZoneDirector devices.

1. Go to **Reports > Report Categories > Client Association**.
2. Go to the *Report Options* section.
3. 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 also appear in the list of options.




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

4. In **Report Type**, configure the type of report that you want to view. The available report options depend on the device view that you selected in the previous step.
 - If you selected **All ZoneDirectors**, then select one of the following options in **Report Type**:
 - *Connected Clients*: Shows all clients that communicated with FlexMaster at the last inform interval
 - If you selected **All Standalone APs**, then select one of the following options in **Report Type**:
 - *APs*: Shows all directly-managed APs that communicated with FlexMaster at the last inform interval.
 - *Connected Clients*: Shows all clients that communicated with FlexMaster at the last inform interval.
5. In **Radio Type**, select the radio for which you want to display association information. Options include **All Radios**, **802.11b/g**, **802.11a/n**, **802.11g/n**, and **802.11a**.
6. In **Display Period**, select the period for this report.
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 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) 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) 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**) 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 can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
- 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.

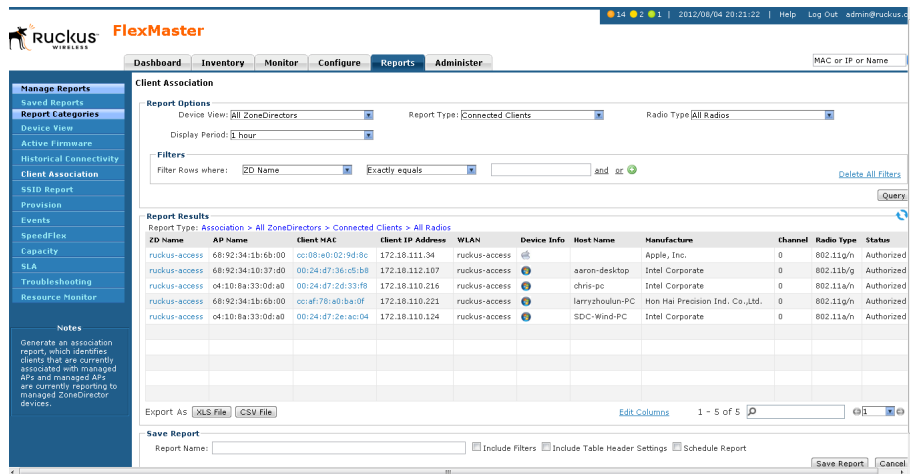
8. Click Query.

The page refreshes, and then displays client 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 151. An example of a client association report



Generating an SSID Report

An SSID report displays the number of ZoneDirector devices and APs on which a particular SSID is configured. You can also view graphs of associated clients, received traffic, and transmitted traffic per SSID.

1. Go to **Reports > Report Categories > SSID Report**.
2. In *Device View*, select the device view for which you want to generate a report. Default device views include:
 - All ZoneDirectors

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



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

3. In *Report Type*, configure the type of report that you want to view. The available report options depend on the device view that you selected in the previous step.
 - *SSID*: Shows the number of APs that are configured to use a particular SSID and the number of ZoneDirector devices that are managing these APs.
 - *# of Associated Clients*: Shows a graph (either top N bar graph or time line graph) of the number of wireless clients that were associated with SSIDs in the selected device view for a given period of time.
 - *Traffic - Tx*: Shows a graph (either top N bar graph or time line graph) of the amount of traffic (in bytes) that were transmitted per SSID in the selected device view for a given period of time.


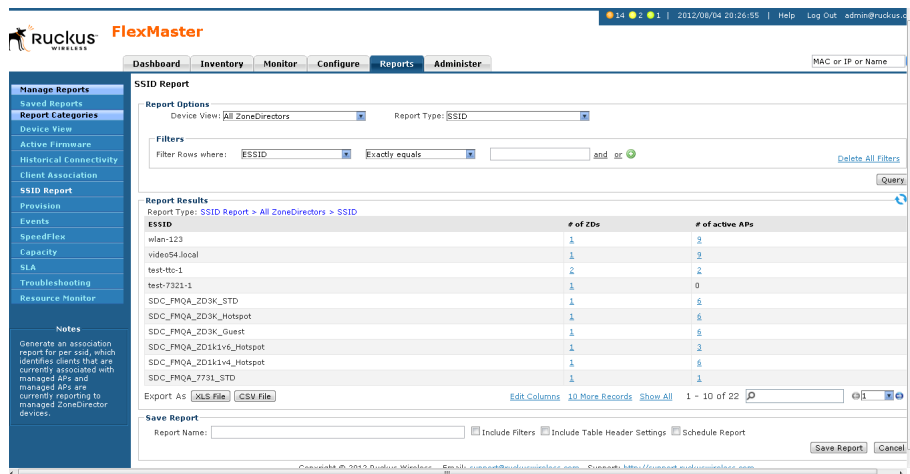
- *Traffic - Tx*: Shows a graph (either top N bar graph or time line graph) of the amount of traffic (in bytes) that were received per SSID in the selected device view for a given period of time.
4. (Optional) If you selected **SSID** as the report type and you want to add a search filter to your query, configure the options in the **Filters** section.
 - a. In the first drop-down list box after **Filter Rows where**, verify that **ESSID** is selected.
 - b. In the second drop-down list box, select the search operator that you want to use. Available search operators include:
 - *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered.
 - *Contains*: Search for devices with attributes that include the query parameter you entered.
 - *Starts with*: Search for devices with attributes that start with the query parameter you entered.
 - *Ends with*: Search for devices with attributes that end with the query parameter you entered.After you select a search operator, a third (text) box appears.
 - c. In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
 - 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.
 5. Click **Query**. If you selected report type that generates a graph, click **Generate Graph**. The page refreshes, and then displays the SSID report that you queried or graph that you generated.

Figure 152. An example of an SSID report




Generating a Provision Report

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

1. Go to **Reports > Report Categories > Provision**.
2. Go to the *Report Options* section.
3. 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
4. (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 can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
- 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.

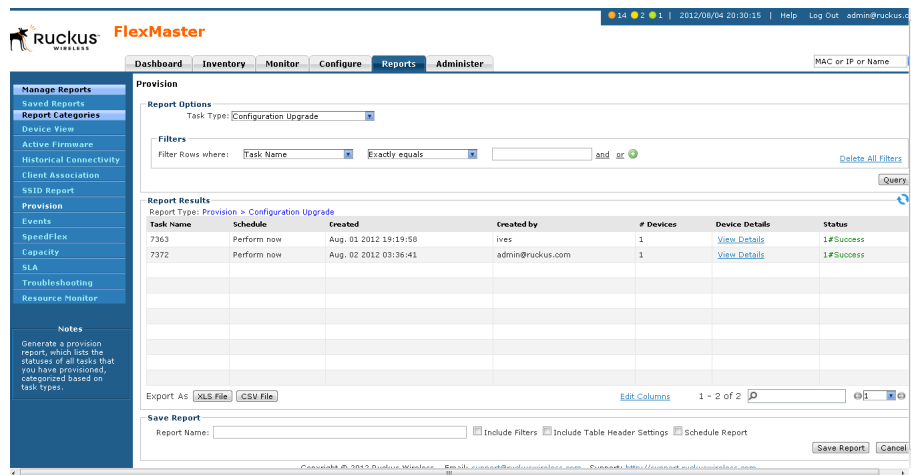
5. Click **Query**.

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 153. An example of a provision 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, and the Provision report is displayed. The report shows two tasks:

Task Name	Schedule	Created	Created by	# Devices	Device Details	Status
7363	Perform now	Aug. 01 2012 19:19:50	ives	1	View Details	1#Success
7372	Perform now	Aug. 02 2012 03:36:41	admin@ruckus.com	1	View Details	1#Success

Below the table, there are options to export the report as an XLS file or CSV file, and a Save Report section with fields for Report Name and checkboxes for Include Filters, Include Table Header Settings, and Schedule Report.

Generating Events-Related Reports

Events-related reports displays a list of events that match the selected event category, device category, and event type. There are four types of events-related report.

- An events report shows a summary of devices on which a particular event (for example, connectivity problem) has occurred.
- An event timeline report shows devices on which a specific event occurred (similar to an events report), but based on a configurable time period. For example, if you want to view a list of devices on which the “Connectivity problem” event occurred within the last seven days, you can set the start time and end time ranges to cover the previous week.
- Similar to an events report, a detailed events report lists devices on which a particular event (for example, connectivity problem) has occurred, including all instances when the event occurred on each device. For example, if the “Connectivity problem” event occurred 10 times on a particular device, the detailed events report will show details of all 10 occurrences, including the dates and times when the events occurred.
- An event plot report displays a graph version of five specific connectivity events that occurred on APs that are reporting to managed ZoneDirector devices.



NOTE: An events report does not indicate the number of times a particular event occurred on a device. If you need to know how frequently the event occurred on a device, generate a detailed events report instead.


Follow these steps to generate an events-related report.

1. Go to **Reports > Report Categories > Events**.
2. Go to the *Report Options* section.
3. In *Event Category*, click **Events**, **Event Timeline**, **Detailed Events** or **Event Plot**.
4. If you selected **Events** or **Detailed Events**, then in *Device Category*, click the type of managed device for which you want to generate the report. Options include **ZoneDirectors** and **Standalone APs**.
5. If you selected **Event Timeline** or **Event Plot**, then in *Device Category*, click the device view for which you want to generate a report. Default device views include:
 - All Standalone APs
 - All ZoneDirectorsIf you created custom device views, then they also appear in the list of options.
6. If you selected **Events**, **Event Timeline** or **Detailed Events**, then in *Event Type*, select the type of event for which you want a report.
7. If you selected **Event Timeline** or **Event Plot**, then in *Display Period*, select the period for this report.

Note that the time period covered by the report depends on the availability of events data on the FlexMaster database. If the events log has been purged recently, then the events report only displays events that occurred after the last purge. For more information, see [Purge Policy](#).



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

8. (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 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) 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) 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**) appear in the search results.After you select a search operator, a third (text) box appears.
 - c. In the text box, type the search parameter that you want to use with attribute and operator that you selected. The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
 - 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.
9. If you selected **Events**, **Event Timeline** or **Detailed Events**, then click **Query**. See [Figure 154](#), [Figure 155](#), or [Figure 156](#).
10. If you selected **Event Plot**, then click **Generate Graph**. See [Figure 157](#).

The page refreshes, and then displays your report.

If you generated an event plot report, the five types of events that are plotted on the graph include:

- Ping loss
- AP lost heartbeat
- AP joined
- AP lost
- AP rebooted

To hide an event from the graph, go to the *Plot Options* section, clear the check box before the event name, and then click *Filter*.



NOTE: FlexMaster provides options for filtering the devices that are included in the report. Options for saving the generated report, automating report generation, and saving the report as an Excel or .CSV file are also available. For more information, see [Using Advanced Report Options](#).

Figure 154. An example of an events report

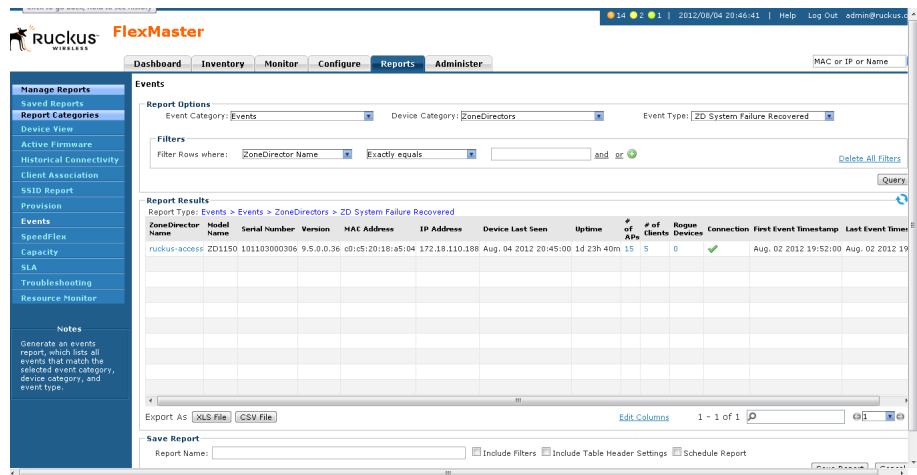


Figure 155. An example of an event timeline report

The screenshot shows the Ruckus FlexMaster interface with the 'Reports' tab selected. The 'Events' section is active, displaying a report for 'Event Category: Event Timeline'. The report options include 'Device View: All Standalone APs' and 'Event Type: Connection request'. The display period is set to 51 days. The filters section shows 'Filter Rows where: Device Name Exactly equals'. The report results table is as follows:

Device Name	Serial Number	MAC Address	IP Address	Model Name	Device Last Seen	Uptime	Tag	Software	Connection	First Event Timestamp	Last Event Timestamp
7363vestest	161203002760	58:93:96:2D:0C:00	192.168.22.123	ZF7363	Aug_04_2012_20:52:50	3d 18h 26m	9.5.0.0.36	✓		Aug_01_2012_19:20:05	Aug_01_2012_19:20:05
7372	001002001017	48:44:00:00:00:80	192.168.22.136	ZF7372	Aug_04_2012_20:52:24	2d 22h 25m	9.5.0.0.36	✓		Aug_02_2012_03:36:45	Aug_02_2012_03:36:45
7762	201055001440	68:92:34:10:66:ED	192.168.22.91	ZF7762	Aug_04_2012_20:52:04	2d 22h 4m	9.5.0.0.36	✓		Aug_02_2012_00:29:33	Aug_02_2012_02:27:17
RuckusAP	241206000036	C0:8A:DE:13:FF:00	192.168.22.154	ZF7782-S	Aug_02_2012_00:50:57	1h 43m	9.5.0.0.36	✗		Aug_01_2012_18:53:19	Aug_01_2012_19:31:00

The interface also includes options to export the report as XLS or CSV, and a 'Save Report' section with fields for report name and checkboxes for 'Include Filters', 'Include Table Header Settings', and 'Schedule Report'.

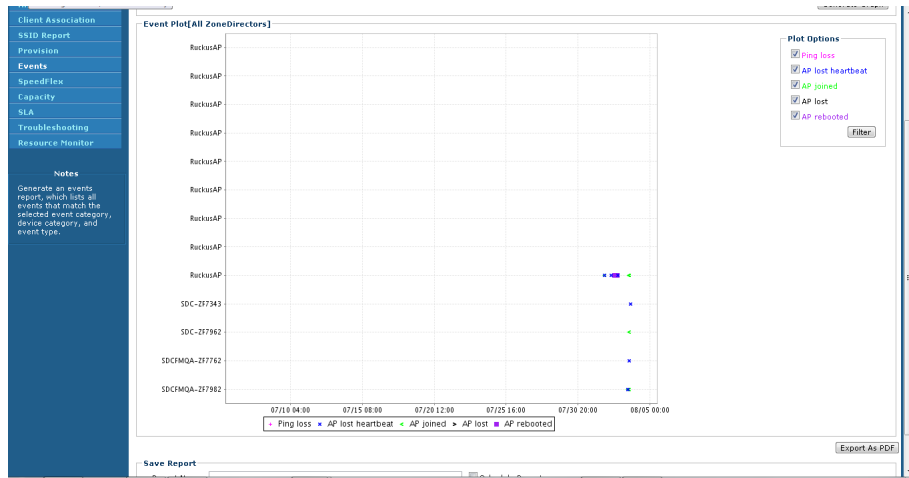
Figure 156. An example of a detailed events report

The screenshot shows the Ruckus FlexMaster interface with the 'Reports' tab selected. The 'Events' section is active, displaying a report for 'Event Category: Detailed Events'. The report options include 'Device Category: ZoneDirectors' and 'Event Type: ZD System Failure Recovered'. The filters section shows 'Filter Rows where: ZD Name Exactly equals'. The report results table is as follows:

ZD Name	ZD MAC	ZD IP Address	ZD Model Name	Timestamp	Detail
ruckus-access	01:05:20:18:a5:04	172.18.110.188	ZD1150	Aug_02_2012_19:50:41	time:Aug_02_2012_19:50:41

The interface also includes options to export the report as XLS or CSV, and a 'Save Report' section with fields for report name and checkboxes for 'Include Filters', 'Include Table Header Settings', and 'Schedule Report'.

Figure 157. 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, and so on.

1. Go to **Reports > Report Categories > SpeedFlex**.
2. Go to the *Filters* section in *Report Options*.
3. To search for previously run SpeedFlex tests to include in the SpeedFlex report, specify the criteria of the SpeedFlex tests that you are looking for.



NOTE: If you want to display *all* SpeedFlex tests that have been run, skip the *Filters* section (steps 4 to 8), and simply click the **Query** button.

4. In the first drop-down list box after *Filter Rows where*, select the search attribute that you want to use. Options include name, serial number, IP address, external IP address, model, and last seen (among others).
5. In the second drop-down list box, select the search operator that you want to use. Available search operators include:
 - *Exactly equals:* Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered 172 . 17 . 16 . 176 as the search parameter, only devices with this IP address appear in the search results.
 - *Contains:* Search for devices with attributes that include the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered 100 as the search parameter, all devices with "100" in the IP address (for example, 172 . 17 . 16 . **100** and **100** . 1 . 10 . 13) appear in the search results.
 - *Starts with:* Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered 3908 as the query parameter, only devices with serial numbers that begin with "3908" (for example, 390801005202) appear in the search results.
 - *Ends with:* Search for devices with attributes that end with the query parameter you entered. For example, if you selected **IP address** as the attribute and you entered 13 as the query parameter, only devices with model names that end in "13" (for example, 100 . 1 . 10 . **13**) appear in the search results.

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

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

The page refreshes, and then displays all the SpeedFlex tests that match the filter criteria that you specified. If you did not specify any filter criteria, FlexMaster displays all SpeedFlex tests that have been run and stored on the FlexMaster database.

Figure 158. An example of a SpeedFlex report

Test Name	Src.Device	Dest.Device	Src.IP	Dest.IP	Src.Model	Dest.Model	Mesh Test	Execute Time	Executor	Status	Finish Time	Details
test	ruckus-access	SDCPMQA_7731_SK1	172.18.110.188	192.168.20.95	ZD1150	ZD1106	No	Aug. 01 2012 19:37:34	ives	Success	Aug. 01 2012 19:37:53	View Details
Test Test	ruckus-access	SDCPM106_2	172.18.110.188	192.168.20.5	ZD1150	ZD1106	No	Aug. 05 2012 19:00:00	SYSTEM_USER	Success	Aug. 05 2012 19:00:19	View Details
Test Test	ruckus-access	SDCPM106_2	172.18.110.188	192.168.20.5	ZD1150	ZD1106	No	Aug. 04 2012 19:00:00	SYSTEM_USER	Success	Aug. 04 2012 19:00:19	View Details

Generating a Capacity Report

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

1. Go to **Reports > Report Categories > Capacity**.
2. Go to the *Report Options* section.
3. 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 also appear in the list of options.



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

4. 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 Associated Clients

- Air-Time Utilization
- AP Actual Throughput
- AP Traffic
- Client Actual Throughput
- Client Traffic

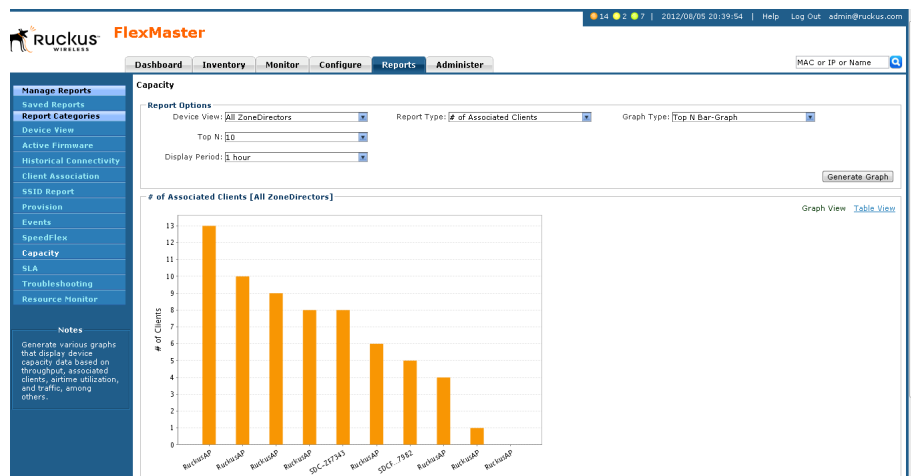
If you selected a device view consisting of Standalone APs, *Backhaul Throughput* is the only report type option that appears.

5. 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).
6. In *Display Period*, select the time period for which you want to generate the report. Options range from 1 hour to 31 days.
7. 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 159. 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.

1. Go to **Reports > Report Categories > SLA**.
2. Go to the *Report Options* section.
3. 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 also appear in the list of options.



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

4. 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
- AP Uptime
- Client Potential Throughput
- Client Associated Time

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

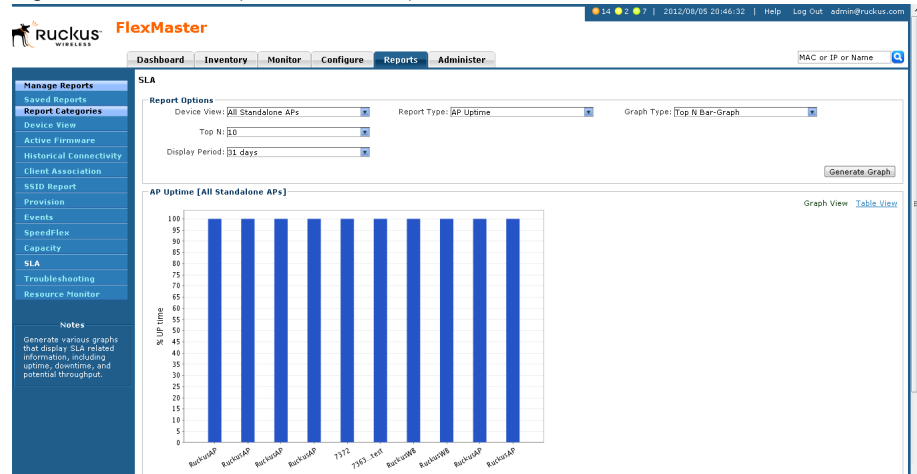
- AP Downtime
- AP Uptime
- Backhaul Link Uptime

5. 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).
6. In *Display Period*, select the time period for which you want to generate the report. Options range from 1 hour to 31 days.
7. 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 160. An 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.

1. Go to **Reports > Report Categories > Troubleshooting**.
2. Go to the *Report Options* section.
3. 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 also appear in the list of options.



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

4. 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
- # of Reboot
- Physical Link Distance
- Ping Test

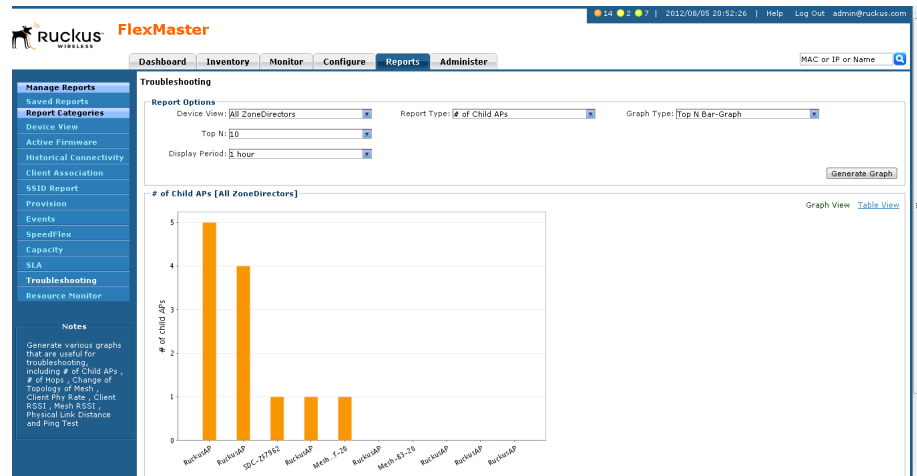
If you selected a device view consisting of Standalone APs, *Backhaul Change of State* is the only report type option that appears.

5. 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).
6. In *Display Period*, select the time period for which you want to generate the report. Options range from 1 hour to 31 days.
7. 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 161. An example of a troubleshooting report



Generating a Resource Monitor Report

Generate a resource monitor report to view CPU, memory, and disk usage on managed ZoneDirector devices.

1. Go to **Reports > Report Categories > Resource Monitor**.
2. Go to the *Report Options* section.
3. In *Device View*, select the device view for which you want to generate a report. Default device views include:
 - All ZoneDirectorsIf you created custom ZoneDirector device views, they also appear in the list of options.
4. (Optional) If you want to add a search filter to your query, configure the options in the **Filters** section.
 - a. In the first drop-down list box after **Filter Rows where**, select the search attribute that you want to use. Options include ZoneDirector name, model name, serial number, IP address, %CPU, %Mem, and %Disk (among others).
 - b. In the second drop-down list box, select the search operator that you want to use. Available search operators include:
 - *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered 172.17.16.176 as the search parameter, only devices with this IP address appear in the search results.
 - *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered 100 as the search parameter, all devices with “100” in the IP address (for example, 172.17.16.100 and 100.1.10.13) appear in the search results.

- *Starts with:* Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered 3908 as the query parameter, only devices with serial numbers that begin with “3908” (for example, 390801005202) appear in the search results.
- *Ends with:* Search for devices with attributes that end with the query parameter you entered. For example, if you selected **IP address** as the attribute and you entered 13 as the query parameter, only devices with model names that end in “13” (for example, 100.1.10.13) appear in the search results.

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

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

The page refreshes, and then displays the current resource usage (CPU, memory, and disk) of all ZoneDirector devices in the selected device view.



NOTE: FlexMaster provides options for filtering the devices that are included in the report. Options for saving the generated report, automating report generation, and saving the report as an Excel file are also available. For more information, see [Using Advanced Report Options](#).

Figure 162. An example of a resource monitor report

The screenshot shows the FlexMaster web interface. The 'Reports' tab is active, and the 'Resource Monitor' report is displayed. The report type is 'CPU/Mem/Disk Usage' and the device view is 'All ZoneDirectors'. The report results table is as follows:

ZoneDirector Name	Model Name	Serial Number	MAC Address	IP Address	%CPU	%Mem	%Disk	Timestamp
SDCFMQA_Redundant_3k_1	ZD3500	100903000466	00:24:82:32:d1:7a	192.168.20.2	0	5	9	Aug. 05 2012 20:50:00
SDCFMQA_ZD1100-ipv4only	ZD1150	431103001686	50:a7:33:10:bc:00	192.168.20.89	1	21	7	Aug. 05 2012 20:50:00
SDCFM106_2	ZD1106	100000011006	00:13:92:01:01:01	192.168.20.5	1	23	20	Aug. 05 2012 20:50:00
SDCFMQA_7731_1K1	ZD1106	100000000011	00:13:92:00:13:92	192.168.20.95	0	18	20	Aug. 05 2012 20:50:00
SDCFMQA_Redundant_3k_1	ZD3500	100903000466	00:24:82:32:d1:7a	192.168.20.2	0	5	9	Aug. 05 2012 20:45:00
SDCFMQA_ZD1100-ipv4only	ZD1150	431103001686	50:a7:33:10:bc:00	192.168.20.89	1	21	7	Aug. 05 2012 20:45:00
SDCFM106_2	ZD1106	100000011006	00:13:92:01:01:01	192.168.20.5	0	23	20	Aug. 05 2012 20:45:00
SDCFMQA_7731_1K1	ZD1106	100000000011	00:13:92:00:13:92	192.168.20.95	0	18	20	Aug. 05 2012 20:45:00
ruckus-access	ZD1150	101103000306	e8:05:20:18:a5:04	172.16.110.188	5	25	20	Aug. 05 2012 20:45:00
SDCFMQA_ZD1100-ipv4only	ZD1150	431103001686	50:a7:33:10:bc:00	192.168.20.89	0	21	7	Aug. 05 2012 20:40:00

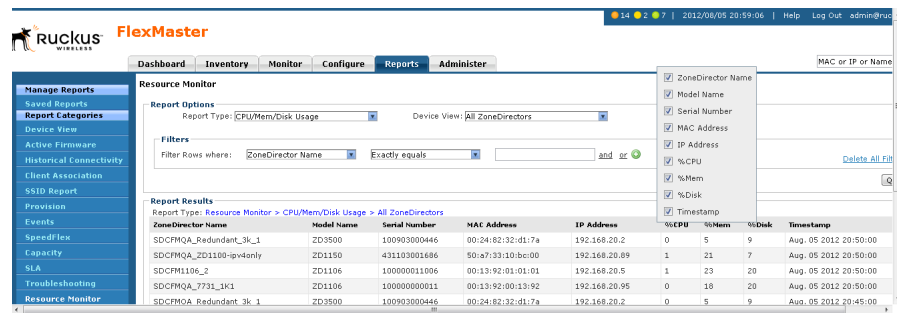
Hiding and Showing Columns in Reports

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.

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 163. 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.

1. Click the **Reports** tab.
2. On the *Report Categories* menu, click the name of the report that you want to configure.
3. Go to the *Save Report* section.
4. In *Report Name*, type a descriptive name for the report that you are saving.

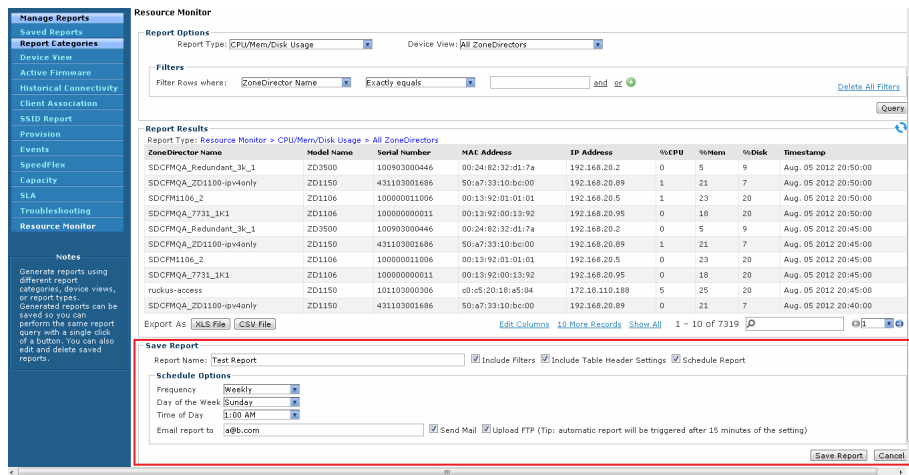
5. Configure the following settings:

- **Include Filters:** Select this check box 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, with a display period as short as once per hour. After you select this check box, the *Schedule Options* section appears below. Configure the following settings:
 - *Frequency:* Specify how often you want FlexMaster to generate this report. Options include **Daily**, **Weekly**, and **Monthly**. If you selected **Weekly**, select the **Day of the Week** when FlexMaster generates the report. If you selected **Monthly**, select the **Day of the Month** when FlexMaster generates the report.
 - *Time of Day:* Set the time when FlexMaster generates the report.
 - *Email report to:* Type the email address to which the report is sent. If you are sending the report to multiple email addresses, use a comma to separate the email addresses.
 - Select *Send Mail* and/or *Upload FTP*, as required.

6. Click **Save Report**.

You have completed configuring FlexMaster to generate and email this report automatically. The report should now appear on the *Saved Reports* page. For more information on working with saved reports, refer to [Managing Saved Reports](#).

Figure 164. Saving a report and automating report generation



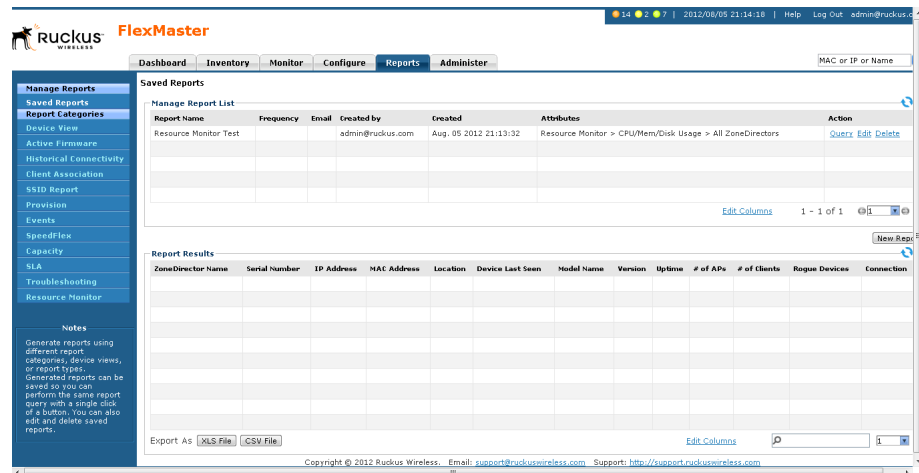
Managing Saved Reports

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:

- [Querying a Report](#)
- [Editing a Report](#)
- [Deleting a Report](#)

NOTE: A button named **New Report** appears below the Manage Report List section. You can click the button to save a new report. Other than the *Select a Report Category* option (which you use to select the type of report to save), the procedure for configuring and saving a report from the *Saved Reports* page is essentially the same as when doing it from the main page for the specific report.

Figure 165. The Saved Reports page



Querying a Report

Querying a report refers to manually generating the report using the options that you configured when you saved the report.

1. Go to **Reports > Manage Reports > Saved Reports**.
2. In the *Manage Report List* section, look for the report that you want to query.
3. Click the **Query** link that is in the same row as the name of the saved report.

The page refreshes, and then the report that you queried appears below, in the *Report Results* section.

Editing a Report

If you need to change the report options, you can edit the report settings from the Saved Reports page.

1. Go to **Reports > Manage Reports > Saved Reports**.
2. In the *Manage Report List* section, look for the report that you want to edit.
3. Click the **Edit** link that is in the same row as the name of the saved report. The Edit Report section appears below.
4. Update the report options as needed.
5. Click **Save Report**.

You have completed editing a report.

Deleting a Report

If you no longer want a report to appear on the Saved Reports page, you can delete it.

1. Go to **Reports > Manage Reports > Saved Reports**.
2. In the *Manage Report List* section, look for the report that you want to delete.
3. Click the **Delete** link that is in the same row as the name of the saved report. A confirmation message appears.
4. Click **OK** to confirm that you want to delete the report.

The page refreshes, and then the report that you deleted disappears from the *Manage Report List* section.

Performing Administrative Tasks

In This Chapter

About the Administer Tab	270
Viewing Audit Logs	270
Managing FlexMaster Licenses	272
Configuring System Settings	274
Managing Device Groups	286
Managing User Accounts	288
Assigning Users to Manage Device Groups	292
Managing SSL Certificates	293
Upgrading the FlexMaster Software	298
Backing Up and Restoring the Database from the Web Interface	302
Generating Support Information	305

About the Administer Tab

The *Administer* tab provides options for viewing audit logs, updating the FlexMaster license file, configuring system settings, and managing users.

Viewing Audit Logs

Audit logs describe configuration actions that were performed on the FlexMaster and identify the users who initiated each action. Auditing is an important function that can help you determine when a configuration change was made and by whom in order to troubleshoot possible issues.

The following table lists the entries that can appear in the audit logs.

Table 29. Audit log entries

Audit Type	Description
Task creation error occurred	User created a provisioning task but it failed.
Configuration upgraded	User created a configuration upgrade task.
Firmware upgraded	User created a firmware upgrade task.
Device rebooted	User created a reboot task.
Device reset to factory default	User created a factory reset task.
Configuration settings updated	User updated a device's configuration from the Device View.
User logged in	User logged into the FlexMaster Web interface.
User logged out	User log out of the FlexMaster Web interface.
User account created	Administrator created a new user account.
User account updated	Administrator updated a user account.
User account deleted	Administrator deleted a user account.
Device log file retrieved	User retrieved an AP's log file from the Device View.
Device log file emailed	User sent out an AP's log file via email.
Device ping test performed	User performed a PING test from the Device View.
VLAN settings updated	User updated the AP's VLAN settings from the Device View.
Audit log emailed	User sent out FlexMaster's audit log via email.
License file verification	The maximum number of devices supported by your FlexMaster license has been reached. To manage additional devices, please contact Ruckus Wireless Support and obtain a license for additional devices.

Table 29. Audit log entries

Audit Type	Description
License file uploaded	User uploaded a new license file into FlexMaster.
Device registered	A device registered with FlexMaster.
Inventory file imported	User imported an inventory file (XLS) into FlexMaster.
Firmware file imported	User uploaded new firmware image files.
Configuration template created or updated	User edited the configuration template.
Device group created or updated	User created or updated the device group.
Device tag created or updated	User created or updated a tag name.
Task canceled	A user-created task has been canceled.
Approval mode updated	User updated the AP approval mode on the Inventory page.
Auto configuration rule created	User created a new auto-configuration rule.
ZoneDirector configuration obtained	User performed "obtain ZD configuration" from a ZoneDirector device.
SSL certificate uploaded	User uploaded an SSL certificate to FlexMaster.
Inventory status created	User created an inventory status.
Inventory status modified	User updated an inventory status.
Inventory status assigned	User changed an AP's inventory status.
Inventory comment assigned	User edited an AP's comment on the Inventory page.
Inventory status deleted	User deleted an inventory status.
ZoneDirector configuration cloned	User created a "Clone ZoneDirector" task.
Managed group created	User created a group for delegated management.
Managed group updated	User updated a group for delegated management.
Managed group deleted	User deleted a group for delegated management.
Managed group device(s) added	User assigned devices to a managed group.
Managed group device(s) removed	User removed devices from a managed group.

Table 29. Audit log entries

Audit Type	Description
User group mapping updated	User changed the "user account" and "managed group" mapping.
User logged in via the Northbound interface	A 3rd party system logged into FlexMaster via the Northbound interface.
User logged out via the Northbound interface	A 3rd party system logged out of FlexMaster via the Northbound interface.
Northbound interface operation invoked	A 3rd party system invoked the Northbound interface.
Upgrade script started	User installed a patch on the FlexMaster server.
Upgrade successful	User patched FlexMaster successfully.
Upgrade failed	User patch for FlexMaster failed.
ZoneDirector could not be reached	FlexMaster could not reach a managed ZoneDirector.
Task deleted	User deleted a task.
Task restarted	User restarted a failed task.
Automatic report created or updated	User created an automatic report.
User failed to log in.	User used an incorrect password to log in to FlexMaster three times.
Automatic report emailed	Automatic report has been sent out.

Managing FlexMaster Licenses

After you install FlexMaster, the number of Ruckus Wireless APs that FlexMaster can manage is limited to 100. Once this limit is reached, no additional devices are able register with FlexMaster (and none appear on the Inventory page). To enable FlexMaster to manage additional APs, you need to upload at least one license file. Use the License page in **Management > License** to upload a license file.



NOTE: When managed devices consume all the available license seats that the current license file supports, an alert message appears on the Dashboard.

Total AP count represents the total number of Ruckus Wireless APs that can be managed by your FlexMaster according to the installed licenses. Each FlexMaster license enables management of a maximum number of Ruckus Wireless APs. When your total inventory

nears the total in your initial license, you buy a new license to add on to the maximum number; that is, a new license adds on to the previous license, it does not overwrite the previous license. Thus, *Total AP count* is the sum of AP counts within each license file.

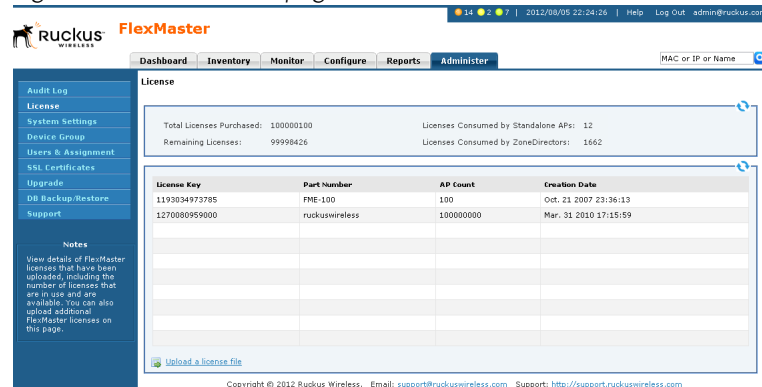


NOTE: If your inventory count reaches your license total, any new devices attempting to register are denied (and do not appear in your Inventory) until your license situation is resolved.



NOTE: **Licenses Consumed by ZoneDirectors** indicates the total number of APs that your ZoneDirector licenses can support, not the number of APs that your ZoneDirector devices are currently managing.

Figure 166. The License page



Uploading a License File

You can update your current FlexMaster license by uploading additional license files using the FlexMaster Web interface.

1. Once you obtain the license file from Ruckus Wireless, log in to the FlexMaster Web interface.
2. Go to **Administer > License**.
3. Click the **Upload a license file link** located below the *License* table. The *Upload a License File* form opens below the link.
4. Click the **Browse** button next to *Select file to be uploaded*.
5. Select the license file, and then click **OK** within the dialog box to close the *Browse* window.
6. Click **Upload** to upload the license file to FlexMaster.

Configuring System Settings

The System Settings option allows you to specify an SMTP server and a support-level user for sending FlexMaster system email messages. Audit and system logs are sent to the specified email address when initiated from those respective areas.

It also enables configuration of a purge policy. A purge policy establishes a length of time FlexMaster-generated files (such as logs, events, and graph data) should be maintained on FlexMaster. Once the configured length of time has been reached, files/items older than the date are purged from FlexMaster to save disk space. This prevents those files from growing interminably.

You can also change the display language settings on the System Settings page and enable or disable Google Maps.

This section describes how to configure the following settings:

- [Language Settings](#)
- [IP Mode Settings](#)
- [Google Maps Settings](#)
- [Task Restart Settings](#)
- [Device Ping Settings](#)
- [Memory Optimization Settings](#)
- [Dashboard Settings](#)
- [SMTP Settings](#)
- [Purge Policy](#)
- [TACACS+ Settings](#)
- [FTP Server Settings](#)
- [Logo Settings](#)

Figure 167. System Settings page (part 1 of 3)

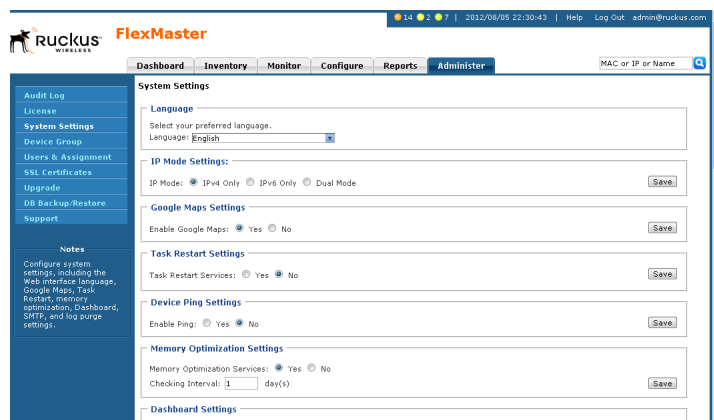


Figure 168. System Settings page (part 2 of 3)

Checking Interval: 1 day(s)

Dashboard Settings

Auto Refresh Interval: 10 minutes

Management mode: 2 Tiers 3 Tiers

SMTP Settings

View

Outgoing Mail Server Host Name: smtp.qq.com

Server Port Number: 25

Default Mail From: 9136469@qq.com

Mail Host User Name (Optional): 9136469

Default Mail to: 9136469@qq.com

Purge Policy

View

Delete events older than: 7 day(s)

Delete alarms older than: 7 day(s)

Delete audit logs older than: 7 day(s)

Delete statistic data older than: 7 day(s)

Tacacs+ Settings

View

Server IP: 192.168.22.130

Port: 49

Figure 169. System Settings page (part 3 of 3)

Delete statistic data older than: 7 day(s)

Tacacs+ Settings

View

Server IP: 192.168.22.130

Port: 49

Service Name: fm-login1

FTP Settings

View

FTP Host Name:

FTP Port Number: 21

FTP User Name:

SNMP Setting

View

SNMP Trap Enable Settings

Enable SNMP Trap: Yes No

ND SNMP Trap List.

Logo Settings

Upload Logo: No file chosen Image should be smaller than 500k. Suggested width/height is 138/40

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

Language Settings

The FlexMaster Web interface supports five display languages:

- English (default)
- Chinese Simplified
- Japanese
- Spanish
- Arabic

You can switch to any of these languages 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.

1. Go to **Administer > System Settings**.
2. In **Language**, select the language to which you want to change the Web interface display. The Web interface refreshes, and then changes the display to the language you selected.

IP Mode Settings

FlexMaster supports IPv4, IPv6, and dual IPv4/IPv6 operation modes. If dual mode is used, FlexMaster keeps both IPv4 and IPv6 IP addresses. By default, FlexMaster operates in IPv4 mode. If you want to change the IP mode, follow the procedure below.

1. Go to **Administer > System Settings**.
2. Under *IP Mode Settings*, select the mode that you want FlexMaster to use. Options include **IPv4 Only**, **IPv6 Only** and **Dual Mode**.
3. Click the **Save** button that is in the same section.

Google Maps Settings

FlexMaster uses Google Maps to show the geographical locations of managed devices. This requires FlexMaster to have active connection to Google Maps via the Internet and for Google Maps to be enabled on FlexMaster. By default, Google Maps is enabled on FlexMaster.

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.

1. Go to **Administer > System Settings**.
2. Under *Google Maps Settings*, click **No** to disable Google Maps.
3. Click the **Save** button that is in the same section.

Task Restart Settings

If you want FlexMaster to automatically restart failed configuration upgrade or firmware upgrade tasks, click the **Yes** option, and then click the **Save** button in the *Task Restart Settings* section. By default, automatic task restart is disabled.

Device Ping Settings

FlexMaster managed devices have a built-in ping feature that can be used to test the connection status between two devices. You can enable and disable ping on these managed devices from the FlexMaster Web interface.

1. Go to **Administer > System Settings**.
2. Under *Enable Ping*, click either **Yes** or **No**. Ping is enabled by default.
3. Click the **Save** button that is in the same section.

Memory Optimization Settings

To help ensure that FlexMaster has enough memory resources to process tasks, you can configure the system settings to clear its memory cache periodically.

Do this by clicking **Yes**, and then setting the interval (in days) at which FlexMaster clears its memory cache. When you are done, click the **Save** button in the Memory Optimization Settings section.



NOTE: Memory optimization requires that your FlexMaster server is running on Linux kernel 2.6.16 or later version. If your Linux kernel version is older, then the memory optimization settings that you configure are not applied.

Dashboard Settings

Dashboard settings include options for configuring the refresh rate of information that is displayed on the Dashboard and device management mode that you want to display on the Dashboard.

Follow these steps to configure the refresh rate of the Dashboard data.

1. Go to **Administer > System Settings**.
2. Scroll down to the *Dashboard Settings* section.
3. In *Auto Refresh Interval*, type refresh interval (in minutes) that you want to set for the Dashboard data. The default refresh interval is 10 minutes.
4. Click the **Save** button that is in the same section.

To select the device management mode that you want to display on the Web interface:

1. Go to **Administer > System Settings**.
2. Scroll down to the *Dashboard Settings* section.
3. In *Management mode*, select one of the following options:
 - *2 Tiers*: Shows data related to FlexMaster and APs only. Click this option if APs on the network are being managed directly by FlexMaster.

- *3 Tiers* (default): Shows data related to FlexMaster, ZoneDirector devices, and APs. Click this option if APs on the network are being managed by ZoneDirector devices (which, in turn, are being managed by FlexMaster).

4. Click the **Save** button that is in the same section.

SMTP Settings

You must configure FlexMaster's host server to enable it to send email notifications. For example, the Audit Log and System Log menu items offer email options. When sending logs via email, the entire contents of these log files are sent to the pre-configured recipient (*Default Mail To*) specified on the *SMTP Settings* page.



NOTE: You may have already configured the SMTP settings during FlexMaster installation.

For the email functionality to work, you need either [1] a DNS server that can supply the IP address of the SMTP server, or [2] the correct mapping to the SMTP server in your hosts file (located in the `/etc` directory). If you choose the second option, 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.

Follow these steps to edit the SMTP settings.

1. Go to **Administer > System Settings**.
2. Scroll down to the *SMTP Settings* section.

Figure 170. Editing SMTP Settings

The screenshot shows a web-based configuration interface for SMTP settings. At the top, there is a 'Management mode' section with radio buttons for '2 Tiers' and '3 Tiers', and a 'Save' button. Below this is the 'SMTP Settings' section, which has 'View' and 'Edit' tabs. The 'Edit' tab is active, and the form contains the following fields: 'Outgoing Mail Server Host Name' (smtp.qq.com), 'Server Port Number' (25), 'Default Mail from' (9136469@qq.com), 'Mail Host User Name (Optional)' (9136469), 'Mail Host Password (Optional)' (masked with dots), and 'Default Mail to' (9136469@qq.com). At the bottom right of the form are 'Test', 'Save', and 'Cancel' buttons. Below the SMTP settings is a 'Purge Policy' section with 'View' and 'Edit' tabs.

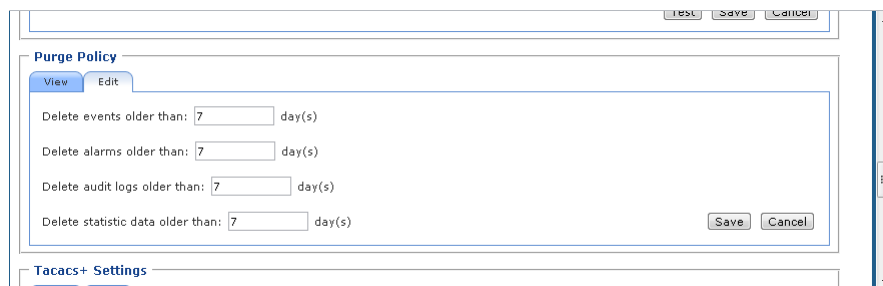
3. Click the **Edit** tab.
4. In *Outgoing Mail Server Host Name*, type the host name of the outgoing SMTP server.
5. In *Server Port Number*, type the SMTP server's listening port number. The default SMTP port number is 25.
6. In *Default Mail from*, type the email address that appears as the sender of the email.
7. In *Mail Host User Name (Optional)*, type the SMTP user name for the email account that you are using to send email notifications.
8. In *Mail Host Password (Optional)*, type the SMTP password for the email account.
9. In *Default Mail to*, type the email address of the user to whom you want to send email notifications.
10. Click **Test** to verify that FlexMaster is able to use the SMTP settings that you configured to send email notifications. If an error appears, check your settings and update them with the correct settings.
11. Click the **Save** button that is in the same section.

Purge Policy

Use Purge Policy to automatically delete FlexMaster event logs, audit logs, and graph data after they age past a certain number of days. This helps ensure that FlexMaster has sufficient disk space to perform tasks.

1. Go to **Administer > System Settings**.
2. Scroll down to the *Purge Policy* section.

Figure 171. Editing Purge Policy settings



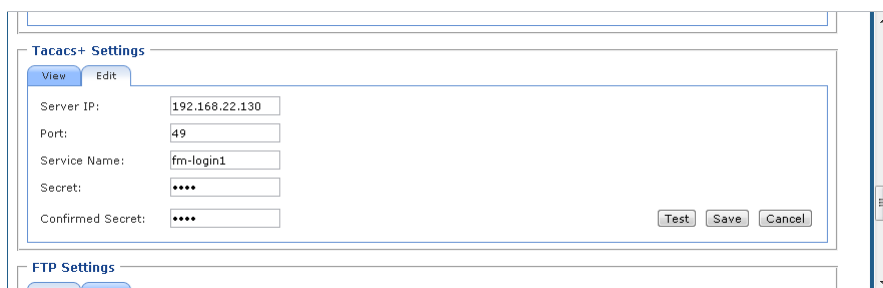
3. Click the **Edit** tab.
4. Type a numerical value (all values are number of days) for one or more of the following:
 - Delete events older than: default is 30 days
 - Delete alarms older than: default is 30 days
 - Delete audit logs older than: default is 30 days
 - Delete statistic data older than: default is 7 days
5. Click **Save**.

TACACS+ Settings

TACACS+ is an access control network protocol that provides separate authentication, authorization and accounting services. For your Ruckus Wireless devices, you must configure the devices to communicate with the TACACS+ server.

1. Go to **Administer > System Settings**.
2. Scroll down to the *Tacacs+ Settings* section.

Figure 172. Editing TACACS+ settings



3. Click the **Edit** tab.
4. Enter the TACACS+ parameters:
 - *Server* - IPv4 or IPv6 server address.
 - *Port* - 49 is the default, but it can be set to any available TCP port.

- *Service Name.*
 - *Secret.*
 - *Confirmed Secret.*
5. Click **Test** to verify that FlexMaster is able to use the TACACS+ settings that you configured. If an error appears, check your settings and update them with the correct settings.
 6. Click **Save**.

FTP Server Settings

You must configure FTP server settings for your Ruckus Wireless devices to communicate with an FTP server.

1. Go to **Administer > System Settings**.
2. Scroll down to the *FTP Settings* section.

Figure 173. Editing FTP server settings

The screenshot shows a web-based configuration interface for FTP settings. At the top, there are two tabs: 'View' (which is active) and 'Edit'. Below the tabs, there are four text input fields: 'FTP Host Name', 'FTP Port Number' (containing the value '21'), 'FTP User Name', and 'FTP User Password'. To the right of these fields are two buttons: 'Test' and 'save'. Below the main form area, there is a link labeled 'SNMP Setting'.

3. Click the **Edit** tab.
4. Enter the FTP parameters:
 - *FTP Host Name* - IPv4 or IPv6 server address.
 - *FTP Port Number* - 49 is the default, but it can be set to any available TCP port.
 - *FTP User Name* - Login.
 - *FTP User Password* - Server password.
5. Click **Test** to verify that FlexMaster is able to use the FTP server settings that you configured. If an error appears, check your settings and update them with the correct settings.
6. Click **Save**.

SNMP Server Settings

If you have an SNMP trap receiver on the network, you can configure FlexMaster to send SNMP trap notifications to the server. Enable this feature if you want to automatically receive notifications for ZoneDirector, AP, and client events that indicate possible network issues.

Enabling SNMP Traps

Before you can send SNMP trap notifications, you must enable SNMP trap notifications.

1. Go to **Administer > System Settings**.
2. Scroll down to the SNMP Settings section.
3. Click the **View** tab.
4. In *Enable SNMP Trap*, click **Yes** or **No**.
5. Click **Save**.


Configuring SNMP Settings

After you enable SNMP trap, you need to configure the SNMP V2/V3 settings, depending on the SNMP version that the SNMP trap receiver is using.

If Your Network Uses SNMP v2

1. Click the **Edit** tab.
2. Under *SNMP v2 Settings*, configure the following settings:
 - *Community*: Enter the SNMP v2 community string.
 - *Read*: Select this check box to enable SNMP read access.
 - *Trap*: Select this check box to send SNMP traps to the trap server on the network.



NOTE: To add another SNMP v2 community string, click the  icon, and then configure the community string and read and trap privileges.


3. Under *SNMP Trap*, configure the following settings:
 - *SNMP Version*: Select **V2**.
 - *Security Name*: Enter the security name.
 - *Target Address*: Enter the IP address of the SNMP trap receiver.
 - *Target Port*: Enter the SNMP port number on the SNMP trap receiver.
4. Click **Save** to save your changes.

If Your Network Uses SNMPv3

1. Click the **Edit** tab.
2. Under *SNMP v3 Settings*, configure the following settings:
 - *User Name*: Enter a user name between 1 and 31 characters.

- *Auth Protocol*: Select either **MD5** or **SHA** or **NONE** authentication method (default is MD5).
 - MD5 (Message-Digest algorithm 5) is a message hash function with 128-bit output.
 - SHA (Secure Hash Algorithm) is a message hash function with 160-bit output.
- *Auth Password*: Enter a passphrase between 8 and 32 characters in length.
- *Priv Protocol*: Select either DES, AES or None.
 - DES (Data Encryption Standard), data block cipher.
 - AES (Advanced Encryption Standard), data block cipher.
 - NONE: No Privacy passphrase is required.
- *Priv Password*: If either DES or AES is selected, enter a Priv Password between 8 and 32 characters in length.
- *Read*: Select this check box to enable SNMP read access.
- *Trap*: Select this check box to send SNMP traps to the trap server on the network.



NOTE: To add another SNMP v3 community string, click the  icon, and then configure the community string and read and trap privileges.

3. Under *SNMP Trap*, configure the following settings:
 - *SNMP Version*: Select **V3**.
 - *Security Name*: Enter the security name.
 - *Target Address*: Enter the IP address of the SNMP trap receiver.
 - *Target Port*: Enter the SNMP port number on the SNMP trap receiver.
4. Click **Save** to save your changes.

Events for Which FlexMaster Sends Trap Notifications

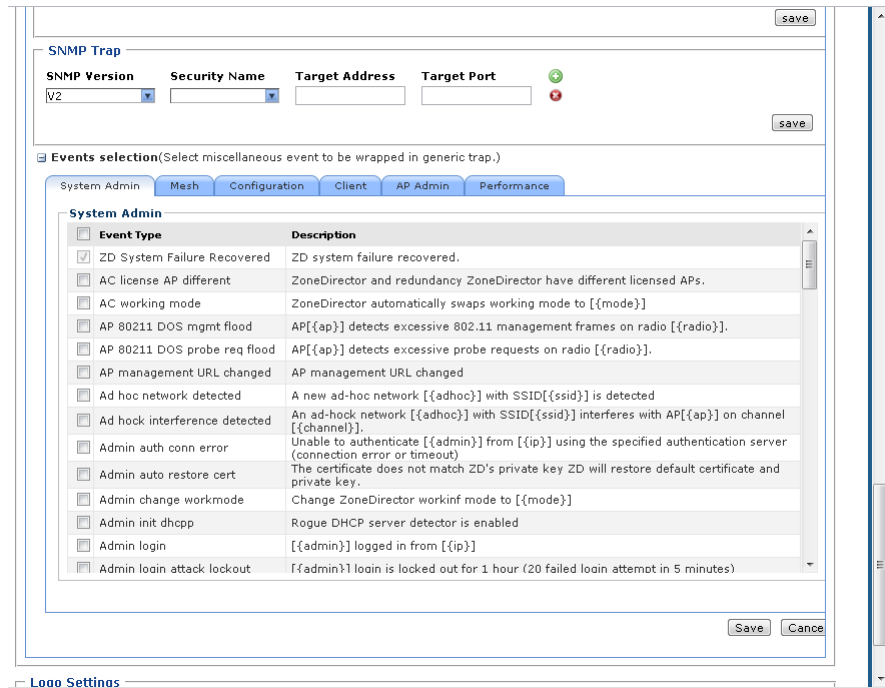
There are several event types for which FlexMaster sends trap notifications to the SNMP server that you specified. These event types include:


- System admin events
- Mesh events
- Configuration events
- Client events
- AP admin events
- Performance events

By default, FlexMaster only sends trap notifications when the event “ZD System Failure Recovered” (a system admin event) occurs. If you want FlexMaster to send trap notifications for other events, you need to enable trap notifications for these events.

1. In the *SNMP Settings* section, scroll down to the *Events selection* section (under SNMP Trap).

Figure 174. Events selection



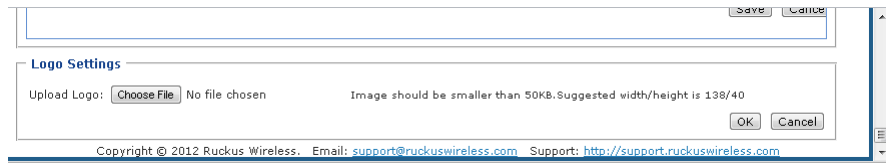
2. If the *Events selection* section is collapsed, click the  icon to expand it. The configuration tabs for the various event types appear.
3. Select the check box for each event type that you want FlexMaster to send trap notifications. Click the tab names to view the list of events from event types.
4. Click **Save** to save your changes.

Logo Settings

You can change the Ruckus Wireless logo that appears up on the upper-left corner of the FlexMaster Web interface to a different image (for example, your company logo). To do this, you need to upload an image file to replace the Ruckus Wireless logo. The image file must be smaller than 50kb, with a recommended size of 138px by 40px.

1. Prepare a 138px by 40px version of your logo.
2. Go to **Administer > System Settings**.
3. Scroll down to the *Logo Settings* section.

Figure 175. Logo settings



4. Click the **Choose File** button.
5. When the Open/Browse dialog box appears, browse to the location where you saved the custom logo that you want to upload, and then select it.
6. Click **Open** to close the dialog box.
7. Click **OK** to finish uploading the custom logo file.

The FlexMaster Web interface refreshes, and the custom logo that you uploaded appears in place of the default Ruckus Wireless logo.

Managing Device Groups

FlexMaster allows you to create and edit device groups, and to assign devices to existing device groups.

- [Creating a Device Group](#)
- [Assigning Devices to a Device Group](#)
- [Editing a Device Group Name](#)
- [Deleting a Device Group](#)

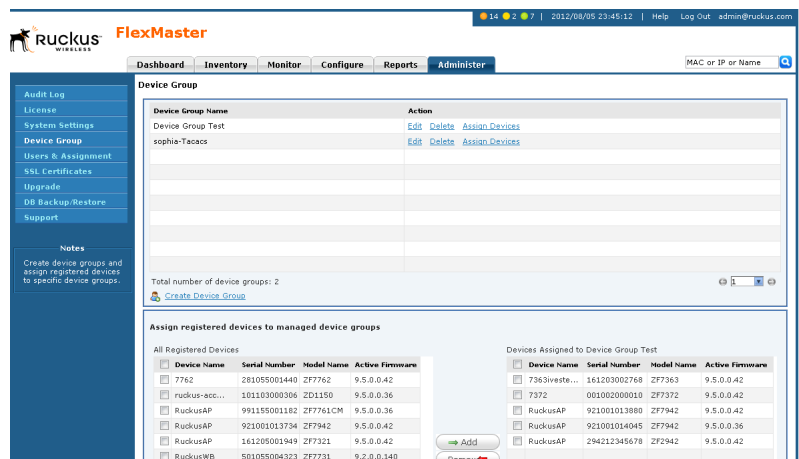
Creating a Device Group

1. Go to **Administer > Device Group**.
2. Click **Create Device Group**.
3. In the *CREATE DEVICE GROUP* section, enter the new device group name in *Device Group Name*.
4. Click **OK**.

Assigning Devices to a Device Group

1. Go to **Administer > Device Group**.
2. Click **Assign Devices** on the same line as the target device group name.

Figure 176. Assigning devices to a device group



3. In the *CREATE DEVICE GROUP* section, enter the new device group name in *Device Group Name*. FlexMaster displays the *Assign registered devices to managed device groups* panel.

4. In the *Assign registered devices to managed device groups* panel, the left pane lists all the registered devices. The right pane lists all of the devices assigned to this device group.
5. Select the individual device check boxes and use the **Add** and **Remove** buttons to move devices to and from the right and left panes.
6. As you add devices to the right pane, FlexMaster assigns them to the target device group.

Editing a Device Group Name

1. Go to **Administer > Device Group**.
2. Click **Edit** on the same line as the target device group name.
3. In the *EDIT DEVICE GROUP* section, change the device group name in *Device Group Name*.
4. Click **OK**.

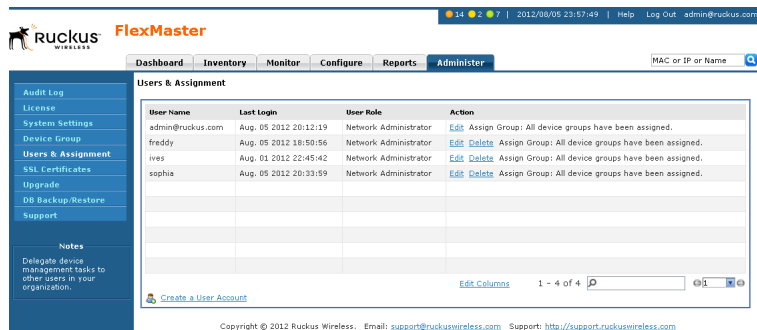
Deleting a Device Group

1. Go to **Administer > Device Group**.
2. Click **Delete** on the same line as the target device group name.
3. In the verification dialog, click **OK**. FlexMaster deletes the device group.

Managing User Accounts

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 uses FlexMaster. Ruckus Wireless recommends against using one login account for multiple users as doing this may not produce useful audit log results.

Figure 177. Users list on the Administer > Users & Assignment page



Understanding User Roles and Privileges

By default, the built-in admin account is listed; this account cannot be deleted or the User Name or User Role changed, but the password can be changed. User roles determine privileges and views available to a user within the FlexMaster system.



NOTE: There is no limit to the number of accounts that you can create for each user role.

User roles determine privileges and views available to a user within the FlexMaster system. The following are the roles that you can assign in FlexMaster:

Network Administrator

The Network Administrator role grants full read and write privileges to the entire FlexMaster system. The installation process creates one default Network Administrator (admin) account; this default admin account cannot 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 managements.

Group Administrator

The Group Administrator role grants full read and write privileges to the assigned devices. A Group Administrator can perform the following tasks:

- Manage devices that belong to assigned groups
- Create Group Operator and Operator accounts
- Assign devices to device management groups
- View Dashboard and Inventory information related to the assigned devices
- Create configuration templates for assigned devices
- Provision configuration upgrade tasks for assigned devices

Group Operator

The Group Operator role grants read privileges only to the assigned devices. A Group Operator can perform the following tasks:

- View Dashboard information related to the assigned devices
- View Inventory information related to the assigned devices
- Only assigned devices appear on the Inventory page
- Only assigned devices appear in the search results
- Reports are only generated for assigned devices
- Receive system alerts for assigned devices. (**Note:** The Group Administrator defines the system alerts that a Group Operator can receive.)



NOTE: A Group Operator does not have Configure and Administer privileges. Although the Configure and Administer tabs still appear on the Web interface, changes to these by the Group Operator cannot be saved.

Device Operator

A Device Operator has read/write access at the device level only. Upon login, a Device Operator sees the Device View page without content. The Device Operator must enter the serial number or MAC address of a managed device to view details for that device. A Device Operator role is typically assigned to customer support personnel; the Operator can only see details once the customer provides the device information.

3rd Party Partner

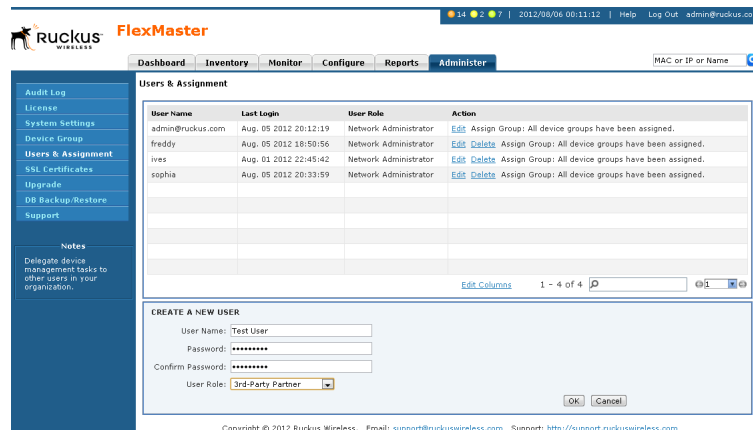
You can assign a 3rd-party partner as a device operator. The 3rd party system logs into FlexMaster via the Northbound interface.

Creating a New User Account

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.

1. Go to **Administer > Users & Assignment**.
2. Click the **Create a User Account** link below the *Users & Assignment* table. The **CREATE A NEW USER** pane appears below the link.

Figure 178. Creating a user account



3. In **User Name**, type a name that you want to assign to this user account. For example, you can type john or john doe. The user name is not case-sensitive and can contain up to 45 alphanumeric characters and spaces.
4. In **Password**, type a password for the account. The password is case-sensitive and can contain up to 45 alphanumeric characters.
5. Repeat the password in **Confirm Password**.
6. In **User Role**, select the role that you want to assign to this user. The options that appear on the User Role menu depends on your own user role. If you are a Network Administrator, the following user roles appear on the menu: **Network Administrator**, **Group Administrator**, **Group Operator**, **Device Operator** and **3rd Party Partner**.

For more information on user roles, see [Understanding User Roles and Privileges](#).

6. Click **OK** to create the account.

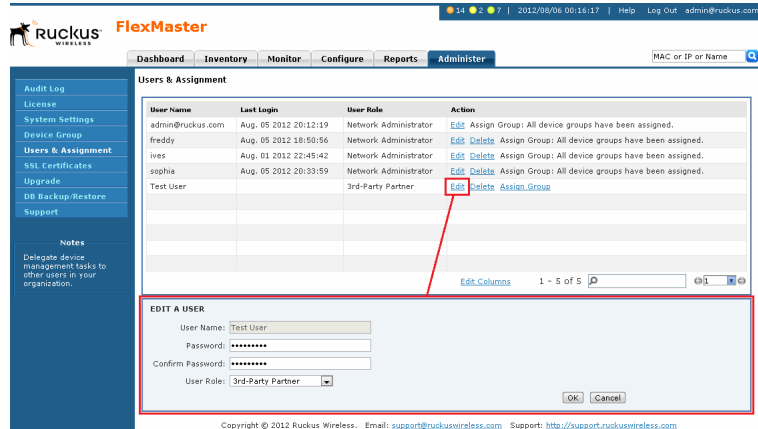
The page refreshes, and then the user account you have created appears in the *Users* list.

Editing a User Account

Edit a user account if you need to make account changes, such as the user password or the user role.

1. Go to **Administer > Users & Assignment**.
2. Find the row in the Users table for the desired user account to edit, and then click **Edit** under the *Action* column.

Figure 179. Editing a user account



3. Edit the following options as required:
 - User Name
 - Password
 - Confirm Password
 - User Role (except for default "admin" account)
4. Click **OK** to save your changes.

Deleting a User Account

Delete user accounts that you no longer need to save space on the FlexMaster database and prevent unauthorized users from gaining access to the FlexMaster Web interface.

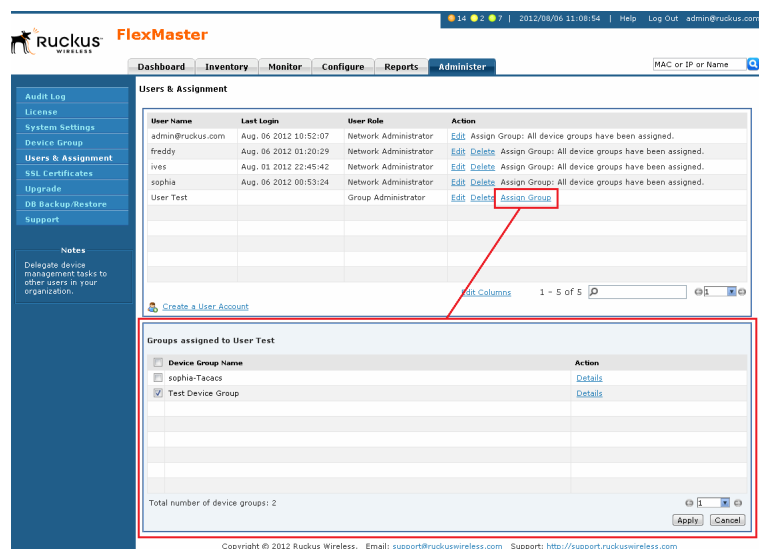
1. Go to **Administer > Users & Assignment**.
2. Find the row in the *Users* table for the desired user account to delete, and then click **Delete** under the *Action* column.

The page refreshes, and then the user account you deleted disappears from the Users list.

Assigning Users to Manage Device Groups

1. Create a User account as described in [Creating a New User Account](#).
2. Create a Device Group as described in [Creating a Device Group](#).
3. Assign devices to a Device Group as described in [Assigning Devices to a Device Group](#).
4. Go to **Administer > Users & Assignment**.
5. Find the entry for the user account that you want to assign as group owner.
6. Click the **Assign Group** link that is in the same row as the user name. The Groups Assigned to {User Name} pane appears, displaying the names of existing device groups.

Figure 180. Assigning a user to manage the group



7. Select the check box for each managed group that you want to assign to the user account.
8. Click **Apply** to save your changes.

When the group owner logs into the FlexMaster Web interface, he or she is able to view and manage the devices that belong to the assigned group.

Managing SSL Certificates

When you use HTTPS to connect to the FlexMaster Web interface, a security warning appears every time you connect to the Web interface. This is because the default SSL certificate (or security certificate) that FlexMaster is using for HTTPS communication is signed by Ruckus Wireless and is not recognized by most Web browsers.

If you want to prevent these security warnings from appearing, you need to import an SSL certificate that was issued by a recognized certificate authority such as VeriSign.



NOTE: FlexMaster currently supports only VeriSign security certificates.

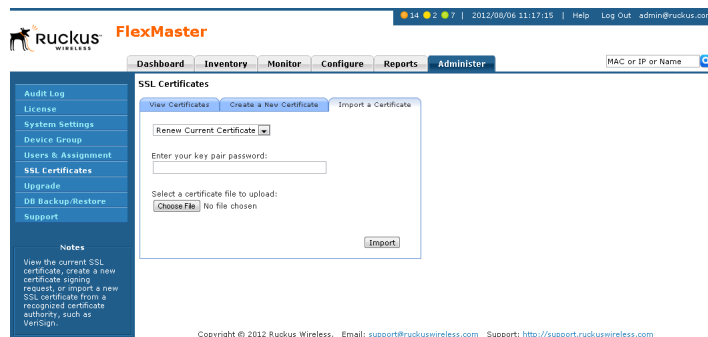
This section describes how to generate a certificate request file to obtain an SSL certificate from VeriSign and how to import a VeriSign SSL certificate into FlexMaster.

Importing an SSL Certificate

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 need the SSL certificate file and the key pair password that you set when you created the certificate signing request (CSR) file.

1. Copy the certificate file to location (either on the local drive or a network share) that you can access from the FlexMaster Web interface.
2. Go to **Administer > SSL Certificates**.
3. On the SSL Certificates page, click the **Import a Certificate** tab.

Figure 181. Importing an SSL certificate



4. In **Enter your key pair password**, type the key pair password that was set when you created the CSR file.
5. In **Select a certificate file to upload**, click **Choose file**, and then go to the location where you saved the certificate file. Select the certificate file, and then click **Open**.

6. Click **Import**. A message appears, informing you that the certificate has been imported successfully.
7. Click the **View Certificates** tab, and check the value for *Issuer* in the current certificate file. Verify that it shows the following:

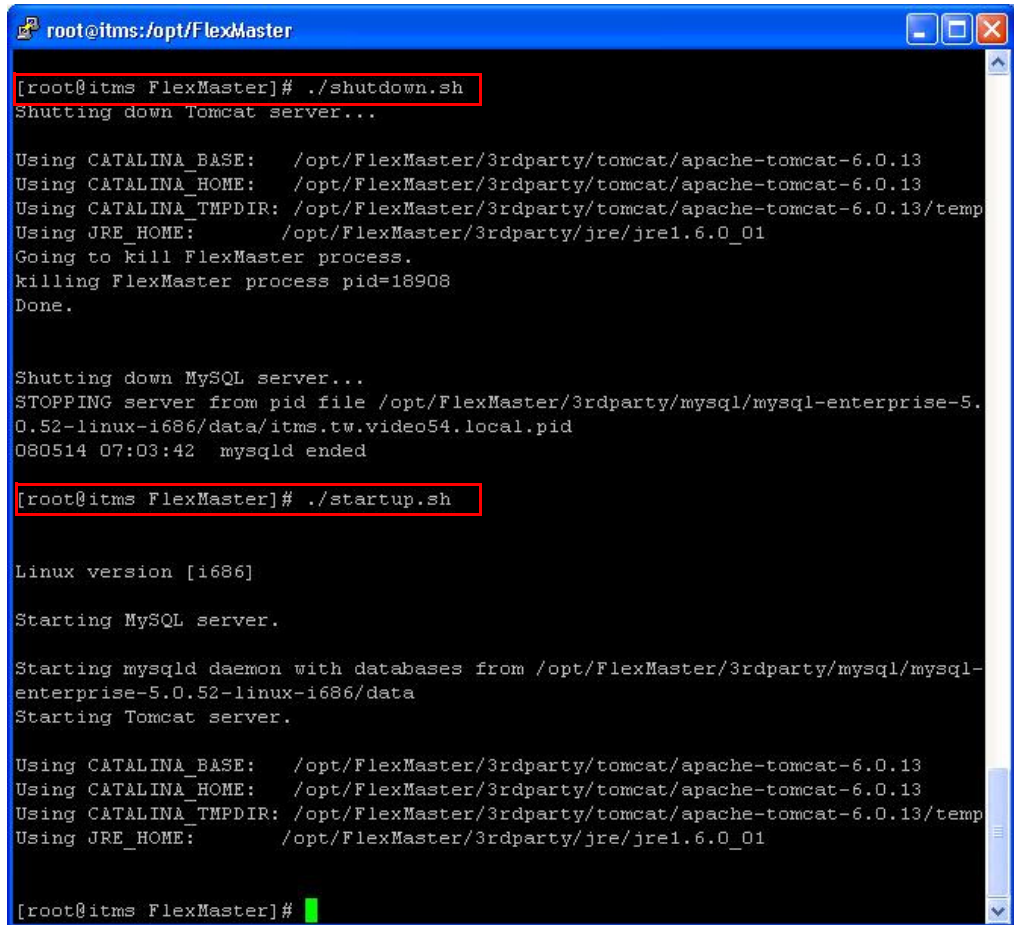
```
Issuer: CN:VeriSign Class 3 Secure Server CA
```

For more information, refer to [Viewing the Current Certificates](#).
8. After you verify that the new certificate has been imported successfully, shut down the FlexMaster service by executing the following script:

```
# /opt/FlexMaster/shutdown.sh
```
9. Restart the FlexMaster service by executing the following script:

```
# /opt/FlexMaster/startup.sh
```

Figure 182. 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 need to create a certificate signing request (CSR) file and send it to VeriSign to purchase an SSL certificate. The FlexMaster Web interface provides a form that you can use to create the CSR file.

1. On the *SSL Certificates* page, click the **Create a New Certificate** tab.
2. In the boxes provided, fill in the following information:
 - **Common Name:** Type the fully qualified domain name of your Web server. This must be an exact match (for example, `www.ruckuswireless.com`).
 - **Organization:** Type the complete legal name of your organization (for example, `Ruckus Wireless, Inc.`). Do not abbreviate your organization name.
 - **Organization Unit:** Type the name of the division, department, or section in your organization that manages network security (for example, `Network Management`).
 - **Locality or City:** Type the city where your organization is legally located (for example, `Sunnyvale`).
 - **State/Province:** Type the state or province where your organization is legally located (for example, `California`). Do not abbreviate the state or province name.
 - **Country:** Type the two-letter ISO abbreviation for your country (for example, if your organization is located in the United States, type `US`).
 - **Key pair password:** Type the password that you want to use for the SSL certificate. The key pair password must consist of at least six characters.
 - **Confirm password:** Retype the key pair password to confirm.

Figure 183. 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 left sidebar has a 'Notes' section with instructions: 'View the current SSL certificates, create a new certificate signing request, or import a new SSL certificate from a recognized certificate authority, such as VeriSign.' The main content area is titled 'SSL Certificates' and has two tabs: 'View Certificates' and 'Create a New Certificate'. The 'Create a New Certificate' tab is active, showing a form with the following fields and labels:

- Common Name:** (Label: ???admin.administration.sslcert.message.createnewkeypair.commonname???)
- Organization:** (Label: The complete legal name of your organization (for example, Ruckus Wireless, Inc.). Do not abbreviate.)
- Organization Unit:** (Label: The department in your organization that manages network security (for example, Network Management).)
- Locality or City:** (Label: The city where your organization is legally located (for example, Sunnyvale).)
- State/Province:** (Label: The state or province where your organization is legally located (for example, California). Do not abbreviate.)
- Country:** (Label: The two-letter ISO abbreviation for your country (for example, if your organization is located in the United States, type US).)
- Key pair password:** (Label: The password must be at least six characters long.)
- Confirm password:**

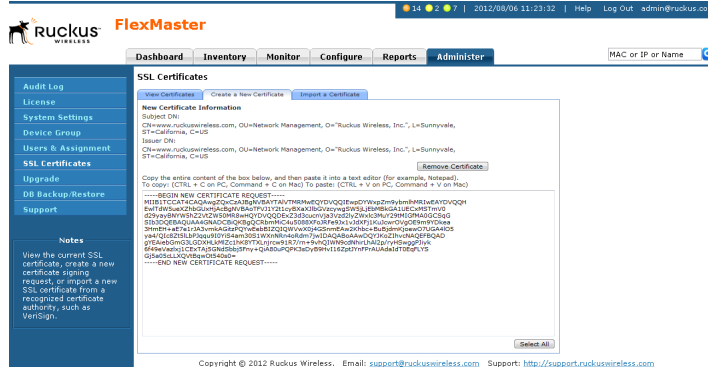
A 'Create' button is located at the bottom right of the form. The footer of the page reads: 'Copyright © 2012 Ruckus Wireless. Email: support@ruckuswireless.com Support: http://support.ruckuswireless.com'



WARNING! Remember the key pair password that you set in this procedure. You need to enter this password when you import the SSL certificate (that VeriSign sends you) into FlexMaster.

3. Click **Create**. The New Certificate page appears, displaying a summary of the certificate information that you entered. If you find any incorrect information or if you want to edit the certificate information, click *Remove Certificate*, and then go back to [Step 1](#). If the certificate information is correct, continue to [Step 4](#).
4. Click **Generate CSR**. The page refreshes, and then display the content of the CSR.

Figure 184. Copy the content of the CSR and save it to a text file



5. Copy the complete content of the CSR request, and then paste it into a text editor (for example, Notepad). Save the file.
6. Go to the VeriSign Web site and follow the instructions for purchasing an SSL certificate. For more information, visit:
www.verisign.com/ssl/buy-ssl-certificates/index.html
7. When the VeriSign Web site prompts for the certificate signing request, copy and paste the content of the text file that you saved in [Step 5](#), and then complete the certificate purchase.

After VeriSign approves your CSR, you receive the VeriSign-signed certificate via email. The following is an example of a signed certificate that you receive from VeriSign:

```
-----BEGIN CERTIFICATE-----
MIIFVjCCBD6gAwIBAgIQLfAGuqKukMumWhbVf5v4vDANBgkqhkiG9w0BAQUFADCB
sDELMaKGA1UEBhMVCVVMxZjZAVBgnVBAoTDLZlcm1TaWduLCBjbmuMR8wHQYDVQQL
BgEFPQcBAQRtMGswJAYIKwYBBQUHMAggGh0dHA6Ly9vY3NwLnZlcm1zaWduLmNv
bTBDBggrBgEFBQcwAoY3AHR0cDovL1NWU1NlY3VyZS1haWEudmVyaXNpZ24uY29t
L1NWU1NlY3VyZTIwMDUuYWhLmNlcnJlbnBgcggrBgEFBQcBDARiMGChXqBcMFowDBW
FglpbWFnZS9S9naWYwITAFMACBBSsOAwIaBBRLA7kolgYMu9BSOJsprEshiyEFGDAm
FiRodHRWoi8vbG9nb3552ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZIhvcN
AQEFBQADggEBAl/S2dmm/kgPeValSIHmx751o4oq8+fwehRDBMqDaKiBvVXGZ5ZM
noc3DMYDjx0SrI9l1kPsn223CV3UVBZ0385g1T4iKwXgcQ7/WF6BQCUYOE6HK+4ZGc
HermFf3fv3C1FoCjq+zEu8ZboUf3fWbGprGRA+MR/dDI1dTPtSUG7/zWjX05jC//
0pykSlDw/q8hg08kq30S8JzCwkqrXJfQ050N4TJtgb/YC4gwh3BuB9wqprjUahTi
```

```
K1V1ju9bHB+bFkMWIIMIXc1Js62JC1WzwFgaGUS2DLE8xICQ3wU1ez8RUPGnwSxA  
YtZ2N7zDxYDP2tEiO5j2cXY7O8mR3ni0C30=  
-----END CERTIFICATE-----
```

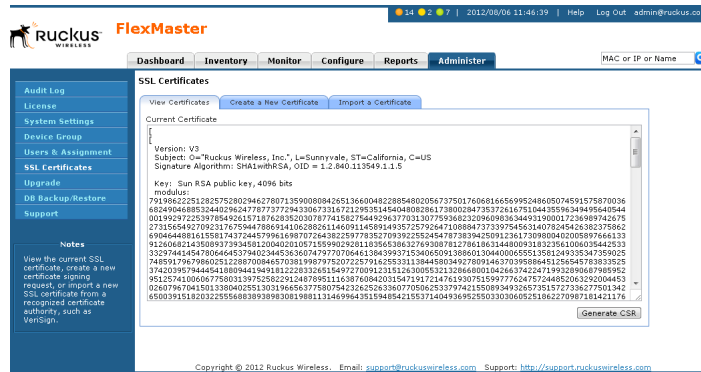
8. Copy the content of the signed certificate, and then paste it into a text file. Save the file.

You can now import the signed certificate from VeriSign into your FlexMaster server. For instructions, refer to [Importing an SSL Certificate](#).

Viewing the Current Certificates

To view the details of the certificate file that FlexMaster is currently using, click the **View Certificates** tab on the SSL certificate page. If you imported a VeriSign-signed SSL certificate, the current certificate should show VeriSign as the certificate issuer.

Figure 185. The default SSL certificate on 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 are made available on the Ruckus Wireless support Web site or released through authorized channels.

Update files typically use {version number}.patch for their file naming convention (for example, 9.5.0.0.11.patch).



WARNING! Although the software update process has been designed to preserve all FlexMaster configuration settings, Ruckus Wireless strongly recommends that you back up the FlexMaster database, in case the update process fails for any reason.

For information on how to back up and restore FlexMaster database, refer to the man pages located in <FlexMaster_installation_directory>/3rdparty/mysql/mysql-enterprise-5.0.52-linux-i686 or the MySQL AB Web documentation located at <http://dev.mysql.com/doc version 5.0>.



NOTE: After you upgrade your FlexMaster server, some of the configuration templates that you created using the previous version may no longer provision successfully. To help ensure successful provisioning, recreate the templates using the new FlexMaster version and delete the old templates.

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

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

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

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

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

6. Upload the patch file (for example, *9.5.0.0.11.patch.tar*) to the FlexMaster server.

7. Copy the patch file to the FlexMaster folder */opt/FlexMaster/*:

```
# cp 9.5.0.0.11.patch.tar /opt/FlexMaster/
```

8. Untar the patch file with following command:

```
# tar -vxf 9.5.0.0.11.patch.tar
```

9. Make sure that the *{version number}.patch* file, such as *9.5.0.0.11.patch*, has been extracted from the tar file.

10. Upgrade FlexMaster with following command:

```
# ./upgrade.sh 9.5.0.0.11
```



WARNING! After installing a software update, Ruckus Wireless recommends backing up the FlexMaster database so you have a backup of the updated database schema. Refer to [Backing Up and Restoring the Database from the Web Interface](#) or [Backing Up the Database from the Command Line Interface](#) for more information.

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 auto restore 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 in to the FlexMaster server.
2. Execute the FlexMaster uninstall script.

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

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

Step 2: Reinstall the Previous FlexMaster Software Version

Follow the FlexMaster installation instructions described in [Installing the FlexMaster Software](#).

Step 3: Shut Down the FlexMaster Service

After you install the FlexMaster software update, you need to shut down the FlexMaster service in preparation for restoring the backup FlexMaster database. Shut down the FlexMaster service by running the following script in the FlexMaster root directory:

```
# shutdown.sh
```

Step 4: Restore the Backup FlexMaster Database

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

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

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

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

where `{file path and file name of the backup file that you want to restore}` is the file path and name of the FlexMaster database backup file that you want to restore.

For example, 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.

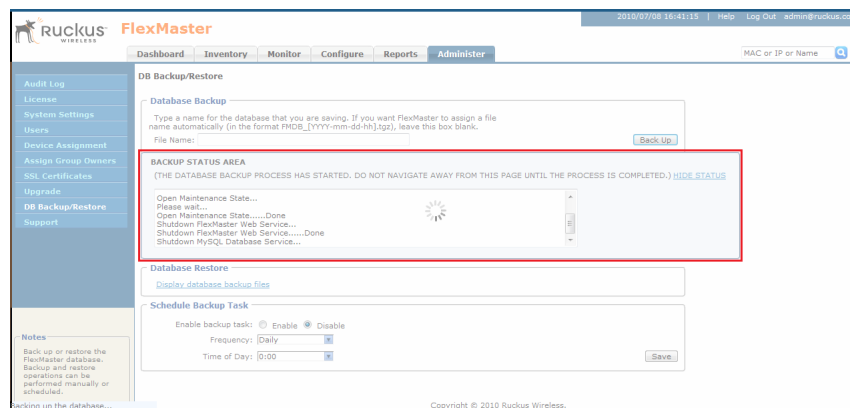
Backing Up the Database from the Web Interface



CAUTION! This procedure halts the FlexMaster operation. Do not perform this procedure when you need FlexMaster to be operating properly.

1. Go to **Administer > DB Backup/Restore**.
2. Look for the *Database Backup* section.
3. In *File Name*, type a name that you want to assign to the backup file. If you want FlexMaster to automatically assign a file name (in the format FMDB_ [YYYY-mm-dd-hh] . tgz), skip this step.
4. Click **Back Up**. The Backup Status Area window appears and displays the progress of the backup process.

Figure 186. The Backup Status Area shows 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.



CAUTION! Do not navigate away from the *DB Backup/Restore* page while the backup process is in progress. Doing so cancels the backup process. Wait for the Backup Status window to display the message that the process is complete.

Scheduling Database Backup

You can also configure FlexMaster to back up its database automatically based on a schedule that you set.

1. Go to **Administer > DB Backup/Restore**.
2. Look for the *Schedule Backup Task* section.
3. In *Enable backup task*, click **Enable**.
4. In *Frequency*, specify how often you want FlexMaster to automatically back up the database. Options include **Daily**, **Weekly**, and **Monthly**.
5. Configure additional options for the *Frequency* option that you clicked.
 - If you clicked **Daily**, 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

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 **Delete**.

Restoring a Backup Copy of the Database

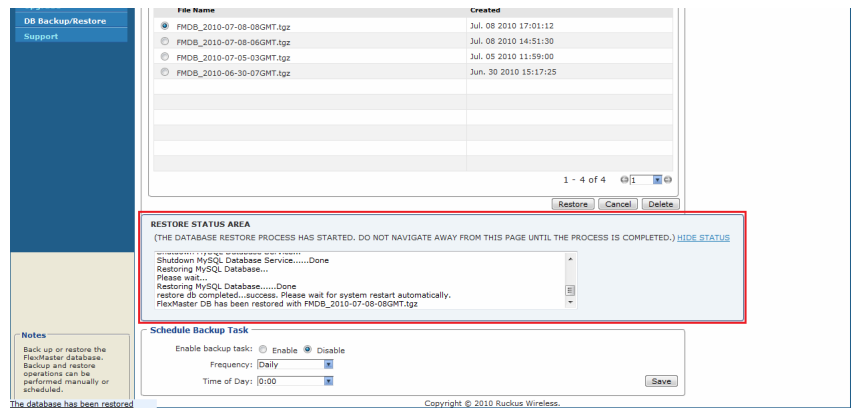
1. Go to **Administer > DB Backup/Restore**.
2. Look for the *Database Restore* section.
3. Click the **Display database backup files** link. A table appears and displays the file names of the database backup files and the dates when they were created.
4. Click the option button next to the database file name that you want to restore.

Performing Administrative Tasks

Backing Up and Restoring the Database from the Web Interface

5. Click **Restore**. The *Restore Status Area* window appears and displays the progress of the restore process.

Figure 187. The *Restore Status Area* shows 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.

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 need to generate system logs.

The System Log is a low level system server log which is useful to support personnel.

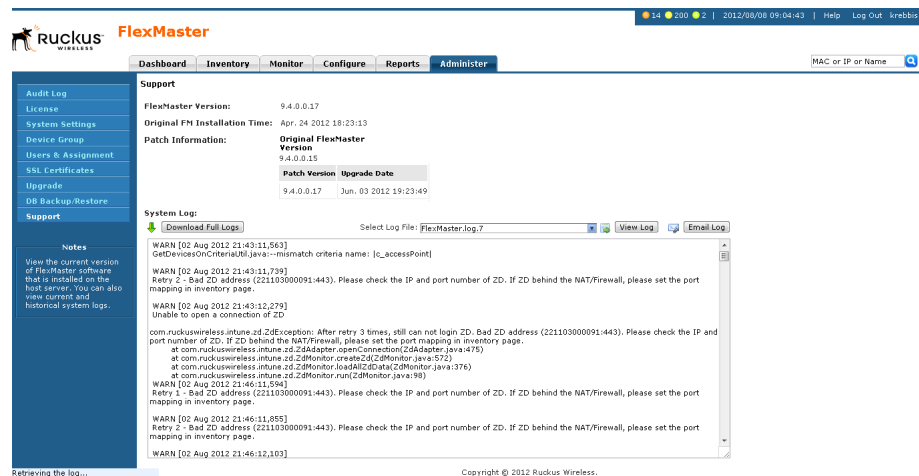
Viewing System Logs

The system log captures information in 12-hour sets. After 12 hours, the “expired” log is backed up and a new log is started. This log rotation prevents the system log from becoming too long. New logs are started at midnight (12:00 AM or 0:00) and midday (12:00 PM).

The system logs are located in the FlexMaster installation directory under `3rdparty/tomcat/apache-tomcat-6.0.13/webapps/intune/WEB-INF/logs/`. Backed-up logs appear as (midnight) FlexMaster.log.yyyy-mm-dd-AM or (midday) FlexMaster.log.yyyy-mm-dd-PM.

1. Go to **Administer > Support**.
2. In *Select Log File*, select the required log file.
3. Click **Retrieve Log**. The log displays information from either midnight to the current time or midday to current time.

Figure 188. Viewing a system log file



Downloading System Logs

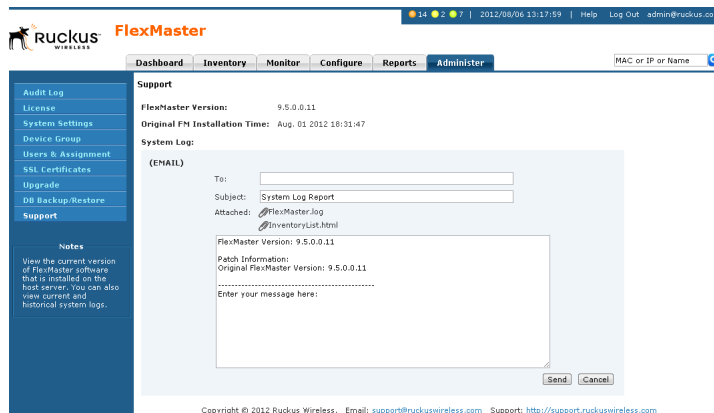
1. Go to **Administer** > **Support**.
2. Click **Download Full Logs**.

FlexMaster zips all the existing log files and downloads the `fm_logs.zip` file to your client workstation.

Emailing a Copy of the System Log File

1. Go to **Administer** > **Support**.
2. Click the **Email Log** button. The *System Log* form appears.
The *To* and *Subject* fields are filled out, and the system log has been added as attachment.
The *To* address must be previously configured in the System Settings. [Configuring System Settings](#)
3. Type any information you want to highlight in the message box.
4. Click **Send** to send the email message.

Figure 189. Sending the system log via email



Index

Symbols

- # of child APs
 - report, 261
- # of hops
 - report, 261
- # of reboot
 - report, 261

Numerics

- 2- and 3-tier management mode
 - Dashboard, 277
- 2741 AP, 162
- 2925 AP, 162
- 2942 AP, 162
- 7025 wall switch, 162
- 7321 AP, 162
- 7341 AP, 162
- 7341-U AP, 162
- 7343 AP, 162
- 7343-U AP, 162
- 7352 AP, 162
- 7363 AP, 162
- 7363-U AP, 162
- 7372 AP, 162
- 7731 AP, 162
- 7731 bridge
 - replacing, 129
- 7761-CM cable modem AP, 162
- 7762 AP, 162
- 7762-AC AP, 162
- 7762-N AP, 162
- 7762-S AP, 162
- 7762-S-AC AP, 162
- 7762-T AP, 162
- 7942 AP, 162
- 7962 AP, 162
- 7982 AP, 162
- 802.1X

- dynamic VLAN example, 202
- 802.1X authentication, 198
- 802.1X authenticator
 - dynamic VLAN, 199
 - guest VLAN, 198
 - MAC-based mode, 198
 - port-based mode, 198
 - RADIUS, 199

A

- access point
 - see AP
- access ports
 - ethernet, 197
 - VLANs, 197
- accounts
 - user, 288
- acknowledging alarms, 214
- active firmware report, 242
- adapter
 - VF 2811, 162
 - VF 7811, 162
- Admin Denied, 188
- advanced features and functions
 - Device View, 127
- alarm
 - acknowledging, 214
 - AP # of clients, 217
 - AP lost connection, 217
 - AP traffic, 217
 - email notification, 217
 - event trigger
 - AP admin, 217
 - client, 217
 - configuration, 217
 - mesh, 217
 - performance, 217
 - system admin, 217

- filtering, 215
- FlexMaster server CPU usage, 217
- light summary, 217
- monitoring, 214
- ZD CPU usage, 217
- alert
 - configuring, 228
 - disabling, 229
- allowing FM ping test, 277
- AP
 - # of clients alarm, 217
 - advanced features and functions, 127
 - factory reset, 153
 - canceling task, 156
 - deleting task, 156
 - viewing task, 156
 - lost connection alarm, 217
 - standalone
 - Device View, 122
 - details, 127
 - ping test, 130
 - summary, 125
 - managing, 121
 - traffic alarm, 217
 - trends, monitoring, 233
 - VF 2825, 162
 - wakeup port 8082, 8
 - wakeup port 8082 mapping, 9, 105, 109
 - ZF 2741, 162
 - ZF 2925, 162
 - ZF 2942, 162
 - ZF 7321, 162
 - ZF 7341, 162
 - ZF 7341-U, 162
 - ZF 7343, 162
 - ZF 7343-U, 162
 - ZF 7352, 162
 - ZF 7363, 162
 - ZF 7363-U, 162
 - ZF 7372, 162
 - ZF 7731, 162
 - ZF 7761-CM, cable modem, 162
 - ZF 7762, 162
 - ZF 7762-AC, 162
 - ZF 7762-N, 162
 - ZF 7762-S, 162
 - ZF 7762-S-AC, 162
 - ZF 7762-T, 162
 - ZF 7942, 162
 - ZF 7962, 162
 - ZF 7982, 162
 - approving, device registration, 191
 - authentication
 - 802.1X, 198
 - authenticator support
 - MAC-based, 198
 - port-based, 198
 - auto configuration
 - task, 157
 - approving, 157
 - creating, 161
 - verifying, 163
 - template
 - creating, 158
 - defining targets, 160
 - auto refresh interval
 - Dashboard, 277
 - automatic file purging, 279
 - automatically restart tasks, 276

B

 - backing up database
 - CLI, 35
 - HDD requirements, 14
 - scheduling, 303
 - web interface, 302
 - backing up ZoneDirector configuration
 - about, 173
 - immediate, 174
 - scheduling, 173

C

 - cable modem AP
 - ZF 7761-CM, 162
 - call home, 2
 - capacity report, 258
 - certificates
 - certificate signing request, 296
 - SSL, 293
 - change of mesh topology
 - report, 261

- changing
 - display language, 275
 - IPv4/6 mode, 276
 - password, 57
- child
 - # of APs report, 261
- client
 - association report, 246
 - Phy Rate report, 261
 - RSSI report, 261
 - trends, monitoring, 234
- common tasks
 - provisioning
 - device firmware, 178
 - creating, 181
 - deleting, 182
 - viewing, 178
 - firmware files
 - deleting, 186
 - editing, 186
 - overview, 185
 - uploading, 185
 - overview, 178
 - reboot, 183
 - creating, 183
 - deleting, 184
 - status, 184
 - see also ZoneDirector and standalone AP provisioning
- configuring
 - alert properties, 228
 - auto configuration
 - task, 157
 - approving, 157
 - creating, 161
 - verifying, 163
 - template
 - creating, 158
 - defining targets, 160
 - dynamic VLAN, 200
 - email notifications, 278
 - FTP server settings, 281
 - hotspot 2.0, 71
 - L2TP communication, 65
 - management server template, 144
 - RADIUS server, 212
 - SNMP server settings, 282
 - standalone AP task
 - cancelling, 151
 - creating, 148
 - deleting, 152
 - restarting, 153
 - viewing status, 150
 - standalone AP template, 137
 - copying, 143
 - creating, 137
 - deleting, 143
 - editing, 142
 - exporting, 143
 - viewing, 142
 - TACACS+, 62
 - unrestricted clients, 209
 - VLAN and LAN port, 196
 - walled garden, 207
 - ZoneDirector task
 - creating, 171
- connectivity
 - historical report, 244
- CPU usage
 - FlexMaster alarm, 217
 - ZD alarm, 217
- CSR
 - certificate signing request, 296
- customizing reports, 265

D

- Dashboard
 - 2- and 3-tier management mode, 277
 - auto refresh interval, 277
 - configuring, 277
 - description, 42
- database backup
 - CLI, 35
 - HDD requirements, 14
 - scheduling, 303
 - web interface, 302
- database restore
 - CLI, 36
 - web interface, 303
- deleting a device, 195
- deleting reports, 268
- deployment scenarios, 6

- hotspot, 7
- hotspot 2.0, 7
- service provider, 6
- detailed events report, 252
- device
 - advanced features and functions, 127
 - unregistering, 195
- device group
 - assigning users to manage, 292
 - managing, 286
- device inventory, 69
- device inventory file
 - exporting, 194
 - overview, 192
 - preparing, 193
 - uploading, 193
 - when to upload, 193
- device licenses
 - releasing, 195
- device log
 - Device View, 130
- device operator, 289
- device registration, 10
 - approval, 191
 - permissions, 189
 - removing, 195
- Device View, 10–11
 - advanced features and functions, 127
 - device log, 130
 - diagnostics, 130
 - report, 239
 - standalone AP, 122
 - details, 127
 - ping test, 130
 - summary, 125
 - widget, 46
- device web port mapping, 9, 99, 108
- DHCP Option 43, 16
- DHCP server, 16
- diagnostics
 - Device View, 130
- disabling an alert, 229
- DNS server, 16
- downloading system logs, 306
- dynamic VLAN
 - 802.1X authenticator, 199
 - 802.1X configuration, 202
 - ethernet port configuration, 202
 - ethernet port MAC auth bypass, 202
 - operation, 200
 - RADIUS server configuration, 203
 - RADIUS server configuration example, 204
 - scenario, 201
 - WLAN configuration, 201

E

- editing reports, 268
- email settings
 - alarms, 217
- email SMTP notifications, 278
- emailing
 - reports, 266
 - system logs, 306
- ethernet port
 - authenticator, 198
 - dynamic VLAN example, 202
 - dynamic VLAN MAC auth bypass example, 202
 - supplicant, 198
- ethernet port types
 - access ports, 197
 - general ports, 197
 - trunk ports, 197
- event
 - monitoring, 219
 - plot report, 252
 - search box, 221
 - searching for, 219
 - timeline, 225
 - timeline report, 252
 - traps, SNMP, 283
- Event View
 - creating, 222
 - managing, 223
- events report, 252
- events search criteria, 219
- Events widget, 47
- events-related reports, 252

F

- factory reset
 - AP, 153
 - canceling AP task, 156
 - deleting AP task, 156
 - viewing AP task, 156
 - ZoneDirector, 153
- filtering alarms, 215
- firmware upgrade
 - creating a task, 181
 - deleting a task, 182
- FlexMaster
 - communicating with managed devices, 4
 - deployment location, 5
 - getting started tasks, 57
 - installation, 13
 - installation procedure, 25
 - key terms, 10
 - L2TP communication, 65
 - licenses, 60
 - software upgrade recovering, 300
 - software upgrading, 298
 - uninstalling, 31
- FlexMaster server CPU usage alarm, 217
- FlexMaster time, 2
- FTP
 - server settings, 281
- FTPing reports, 266

G

- general ports
 - ethernet, 197
 - VLANs, 197
- generating support information, 305
- getting started, 57
- Google Maps, 3
 - enabling, 276
- group
 - device managing, 286
- group administrator, 289
- group operator, 289
- guest VLAN
 - 802.1X authenticator, 198

H

- HDD requirements
 - database backup, 14
- historical connectivity report, 244
- hosts file, 24
- hotspot
 - scenario, 7
- hotspot 2.0
 - configuring, 71
 - scenario, 7
- HTTP port 80, 8
- HTTPS port 443, 8

I

- incoming VLAN traffic, 197
- inform interval, 11
- installation, 13
 - overview, 14
 - preparing, 14
 - root directory files, 31
 - system requirements, 14
- IPv4/6 mode
 - changing, 276

K

- key terms, 10

L

- L2TP communication, 65
- L2TP tunneling, 4
- language
 - changing the display, 275
- licenses, 60
 - releasing, 195
- logging in, 38
- logo
 - changing, 284
- logs, system, 305

M

- MAC authentication bypass, 202
- MAC-based authenticator support, 198
- management mode
 - 2- and 3-tier, 277

- management server
 - provisioning
 - configuration template, 144
- managing Event View, 223
- managing saved reports, 267
- measuring throughput
 - SpeedFlex, 230
- MediaFlex
 - advanced features and functions, 127
 - VF 2811 adapter, 162
 - VF 2825 AP, 162
 - VF 7811 adapter, 162
- memory optimization, 277
- mesh
 - RSSI report, 261
 - topology change report, 261
- monitor
 - alarm acknowledging, 214
 - alarm email notification, 217
 - alarm filtering, 215
 - alarm light summary, 217
 - alarms, 214
 - AP trends, 233
 - client trends, 234
 - events, 219

N

- network administrator, 288
- notifications
 - SMTP emails, 278

O

- optimization
 - memory, 277
- outgoing VLAN traffic, 197

P

- password, 39
 - changing, 57
- permissions, device registration, 189
- Permitted, 188
- Phy Rate
 - client report, 261
- physical link distance
 - report, 261

- ping test
 - FM report, 261
 - FM report, allowing, 277
 - standalone AP, 130
- port
 - 443 (HTTPS), 8
 - 49 (TACACS+), 8
 - 80 (HTTP), 8
 - 8082 (AP wakeup), 8
 - 8082 (ZD wakeup), 8–9
 - device web mapping, 9
- port mapping
 - 8082 AP wakeup, 9, 105, 109
 - 8082 ZD wakeup, 99
 - device web, 99, 108
- port-based 802.1X, 198
- port-based authenticator support, 198
- ports, ethernet, 197
- provisioning, 11, 134
 - AP factory reset, 153
 - canceling, 156
 - deleting, 156
 - viewing, 156
 - common tasks
 - device firmware, 178
 - creating, 181
 - deleting, 182
 - viewing, 178
 - firmware files
 - deleting, 186
 - editing, 186
 - overview, 185
 - uploading, 185
 - overview, 178
 - reboot, 183
 - creating, 183
 - deleting, 184
 - status, 184
 - see also ZoneDirector and standalone AP provisioning
 - conventions, 134
 - hotspot, 204
 - management server
 - configuration
 - template, 144
 - Port-Based 802.1X, 198

- RADIUS server, 212
- report, 250
- standalone AP
 - configuration task
 - cancelling, 151
 - creating, 148
 - deleting, 152–153
 - viewing status, 150
 - template, 137
 - copying, 143
 - creating, 137
 - deleting, 143
 - editing, 142
 - exporting, 143
 - viewing, 142
 - status, 135
- VLAN and LAN Port
 - configuration rules, 196
 - overview, 196
 - procedures, 199
- ZoneDirector
 - backing up configuration
 - about, 173
 - configuration task
 - creating, 171
 - configuration template
 - assigning to a ZoneDirector, 167
 - creating, 166
 - overview, 164
 - status, 169
 - viewing, 169
 - restoring configuration
 - about, 173
 - upgrading configuration, 171
- purge policy, 279

Q

- querying reports, 267

R

- RADIUS
 - 802.1X authenticator, 199
- RADIUS server
 - configuring, 212
 - dynamic VLAN entry example, 204
 - dynamic VLAN example, 203
- reboot
 - # of report, 261
- releasing device licenses, 195
- removing a device registration, 195
- replacing 7731 bridge, 129
- report
 - # of child APs, 261
 - # of hops, 261
 - # of reboot, 261
 - active firmware, 242
 - capacity, 258
 - change of mesh topology, 261
 - client association, 246
 - client Phy Rate, 261
 - client RSSI, 261
 - customizing, 265
 - deleting, 268
 - Device View, 239
 - editing, 268
 - emailing, 266
 - events-related
 - detailed events, 252
 - event plot, 252
 - event timeline, 252
 - events, 252
 - FM ping test, 261
 - FM ping test, allowing, 277
 - FTPing, 266
 - historical connectivity, 244
 - managing saved, 267
 - mesh RSSI, 261
 - physical link distance, 261
 - provisioning, 250
 - querying, 267
 - resource monitor, 263
 - scheduling, 266
 - SLA, 260
 - SpeedFlex, 257
 - SSID, 248
 - troubleshooting, 261
- resource monitor report, 263
- restart tasks, 276
- restoring database
 - CLI, 36

- web interface, 303
- restoring ZoneDirector configuration
 - about, 173
- RMA, 188
- RSSI
 - client report, 261
 - mesh report, 261

S

- saved reports
 - managing, 267
- scheduling reports, 266
- search box, events, 221
- searching for events, 219
- service provider scenario, 6
- SLA report, 260
- Smart Redundancy, 72
- SMTP
 - email notifications, 278
- SNMP
 - event traps, 283
 - server settings, 282
- software
 - upgrade recovering, 300
 - upgrading, 298
- SpeedFlex, 230
 - report, 257
- SSID report, 248
- SSL certificates, 293
 - certificate signing request, 296
- standalone AP
 - Device View, 122
 - details, 127
 - ping test, 130
 - summary, 125
 - managing, 121
 - provisioning
 - configuration task
 - creating, 148, 150–152
 - restarting, 153
 - configuration template, 137
 - copying, 143
 - creating, 137
 - deleting, 143
 - editing, 142
 - exporting, 143

- viewing, 142
- upgrading, 148
- support information, generating, 305
- system logs, 305
- system requirements, 14
 - CPU, 15
 - RAM, 15
 - Web browser, 15

T

- TACACS+, 280
 - configuration, 62
 - port 49, 8
- tag, 11
- task
 - auto configuration, 157
 - approving, 157
 - creating, 161
 - template
 - creating, 158
 - defining targets, 160
 - verifying, 163
 - automatic restart, 276
 - canceling AP factory reset, 156
 - deleting AP factory reset, 156
 - provisioning, 134
 - conventions, 134
 - status, 135
 - standalone AP
 - provisioning
 - cancelling, 151
 - creating, 148
 - deleting, 152
 - restarting, 153
 - viewing status, 150
 - status box, 41
 - viewing AP factory reset, 156
 - ZoneDirector
 - provisioning, creating, 171
- TCP ports, 8
- template
 - management server
 - provisioning, 144
 - standalone AP
 - provisioning, 137
 - copying, 143

- creating, 137
- deleting, 143
- editing, 142
- exporting, 143
- viewing, 142

throughput

- measuring with SpeedFlex, 230

timeline

- event, 225

topology

- change of mesh report, 261

TR-069, 3

trends

- monitoring AP, 233
- monitoring client, 234

troubleshooting report, 261

trunk ports

- ethernet, 197
- VLANs, 197

U

Unavailable, 188

uninstalling, 34

unregistering a device, 195

unrestricted clients

- configuring, 209

untagged

- VLAN, 197

upgrading, 32

- FlexMaster software, 298
- recovering, 300
- standalone AP, 148

user

- assigning to device group, 292

user accounts

- managing, 288

user name, 39

user roles, 288

- device operator, 289
- group administrator, 289
- group operator, 289
- network administrator, 288

V

VF

- 2811 adapter, 162
- 2825 AP, 162
- 7811 adapter, 162

viewing system logs, 305

VLAN

- access ports, 197
- ethernet ports, 197
- general ports, 197
- incoming and outgoing traffic, 197
- trunk ports, 197
- untagged, 197

VLAN and LAN Port settings

- configuration rules, 196
- overview, 196
- procedures, 199

W

wall switch

- ZF 7025, 162

walled garden

- configuring, 207

Web browser, 15

Web interface

- session timeout mechanism, 39
- widgets, 43

web interface

- Dashboard, 42
- features, 40

widgets, 43

WLAN

- dynamic VLAN example, 201

Z

ZD CPU usage alarm, 217

ZD wakeup port 8082, 8–9

- mapping, 99

ZF

- 2741 AP, 162
- 2925 AP, 162
- 2942 AP, 162
- 7025 wall switch, 162
- 7321 AP, 162
- 7341 AP, 162
- 7341-U AP, 162

- 7343 AP, 162
- 7343-U AP, 162
- 7352 AP, 162
- 7363 AP, 162
- 7363-U AP, 162
- 7372 AP, 162
- 7731 AP, 162
- 7731 bridge
 - replacing, 129
- 7761-CM cable modem AP, 162
- 7762 AP, 162
- 7762-AC AP, 162
- 7762-N AP, 162
- 7762-S AP, 162
- 7762-S-AC AP, 162
- 7762-T AP, 162
- 7942 AP, 162
- 7962 AP, 162
- 7982 AP, 162
- advanced features and functions, 127
- ZoneDirector
 - Device View widget, 47
 - factory reset, 153
 - provisioning
 - backing up configuration
 - about, 173
 - immediate, 174
 - scheduling, 173
 - configuration task
 - creating, 171
 - configuration template
 - assigning to a ZoneDirector, 167
 - creating, 166
 - overview, 164
 - status, 169
 - viewing, 169
 - restoring
 - about, 173
 - upgrading configuration, 171- ZoneFlex
 - see ZF