USER GUIDE

Ruckus
Unleashed Multi-Site Manager User Guide

Supporting Software Release 2.0

Part Number: 800-71640-001
Publication Date: 1 February 2018

Copyright Notice and Proprietary Information

Destination Control Statement

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, RUCKUS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. Ruckus does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. Ruckus does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to Ruckus that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL RUCKUS, ARRIS, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIES, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF RUCKUS HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS.

If you are dissatisfied with the Materials or with the associated terms of use, your sole and exclusive remedy is to discontinue their use.

Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

Contents

Preface

Document Conventions

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

TABLE 1 Text conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples.	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *Ruckus Small Cell Release Notes* for more information

Notes, Cautions, and Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE

A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

CAUTION

A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.

Convention	Description
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Document Feedback

Ruckus is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to Ruckus at: docs@ruckuswireless.com

When contacting us, please include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)
- For example:
  - Ruckus Small Cell Alarms Guide SC Release 1.3
  - Part number: 800-71306-001
  - Page 88

Ruckus Product Documentation Resources

Visit the Ruckus website to locate related documentation for your product and additional Ruckus resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate documentation by product or perform a text search. Access to Release Notes requires an active support contract and Ruckus Support Portal user account. Other technical documentation content is available without logging into the Ruckus Support Portal.

White papers, data sheets, and other product documentation are available at https://www.ruckuswireless.com.

Online Training Resources

To access a variety of online Ruckus training modules, including free introductory courses to wireless networking essentials, site surveys, and Ruckus products, visit the Ruckus Training Portal at https://training.ruckuswireless.com.

Contacting Ruckus Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their Ruckus Networks products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the Support Portal using https://support.ruckuswireless.com, or go to https://www.ruckuswireless.com and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Request for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.

Self-Service Resources

The Support Portal at https://support.ruckuswireless.com/contact-us offers a number of tools to help you to research and resolve problems with your Ruckus products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://forums.ruckuswireless.com/ruckuswireless/categories
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/software
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management

About This Guide

Introduction

This *Unleashed Multi-Site Manager User Guide* describes how to install, configure, and manage the Unleashed Multi-Site Manager application or software.

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 Support website at

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

Related Documentation

In addition to this *User Guide*, each Unleashed Multi-Site Manager 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*: Provides information about the current software release, including new features, enhancements, and known issues.

Introducing Ruckus Unleashed Multi-Site Manager

Unleashed Multi-Site Manager Overview

Ruckus Unleashed Multi-Site Manager software is an intelligent, scalable network management system designed to facilitate administration of your dispersed ZoneDirector devices and Unleashed networks.

The software offers a dashboard displaying device views, alarms and events: Processes notifications received from managed Ruckus devices and displays them in an easy-to-understand and easy-to-use graphical user interface accessible via a Web browser.

NOTE

Unleashed Multi-Site Manager 2.0 does not support solo APs.

ATTENTION

By downloading this software and subsequently upgrading ZoneDirector, please be advised that:

- The ZoneDirector periodically connects to Ruckus, and Ruckus collects the ZoneDirector serial number, software version and build number. Ruckus transmits a file back to the ZoneDirector and this is used to display the current status of the ZoneDirector Support Contract.
- Please be advised that this information may be transferred and stored outside of your country of residence where data protection standards may be different.

Management Software and Server

The software is installed on a Linux-based server. The installation includes Web server and MariaDB database components for communicating with and tracking your dispersed Ruckus devices.

For the specific installation steps, refer to Installing the Software on page 22.

Event Times

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

NOTE

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

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

Management Protocol

Ruckus Unleashed Multi-site supports the Technical Report 069 (TR-069) CPE WAN Management Protocol (CWMP) as defined by the DSL Forum (http://www.dslforum.org).

Internet Accessibility

The software requires an Internet-accessible interface to:

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

Where Should You Place Unleashed Multi-Site Manager?

Since you want Unleashed Multi-Site Manager to be as available as possible to the remote devices being managed, you should place it in your network accordingly.

NOTE
Make sure that the software's IP address is reachable via HTTPS from outside of your internal network. This allows managed devices to call home.

Key Terms

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

TABLE 2 Key terms

Term	Description
Device Registration	Enable software management on the Unleashed/ZD devices and then they will register to Unleashed Multi-Site Manager automatically.
Periodic Inform Interval	This is the frequency at which managed Ruckus devices must synchronize with the application. When Ruckus devices call home periodically, the software can verify proper operation of managed devices.
Group	Grouping devices physically and assigning them various permissions/control and reporting.
Default Mail to	This phrase refers to the email address which is sent messages from the system based on various events. You enter this email address either during the installation procedure or in the **To** field on the **Administer** > **System Settings** > **SMTP Settings** page.

TABLE 2 Key terms (continued)

Term	Description
	You must specify an SMTP server to send email notifications to this user. Refer to SMTP Settings on page 97.

Installing and Upgrading the Software

Firewall Ports that Must be Open for Communications

CAUTION

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.

Depending on how your network is designed, you may need to edit the iptables file and open communication ports on any firewalls located between Unleashed Multi-Site Manager and Ruckus devices. Refer to the following URLs which include information about how to edit the iptables file.

- http://en.wikipedia.org/wiki/Iptables
- http://www.thegeekstuff.com/2010/07/list-and-flush-iptables-rules
- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/index.html and read all the IP Tables information under the Firewall section.

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

TABLE 3 Firewall ports that must be open for Unleashed Multi-Site Manager communications

Communication	Ports
MariaDB	
Unleashed Multi-Site Manager > MariaDB communications	TCP destination port 3306
ZoneDirector and Unleashed (Device)	
Device > Unleashed Multi-Site Manager registration and periodic inform	TCP destination port 443 (HTTPS)
Unleashed Multi-Site Manager > Device	TCP destination port 443 (HTTPS)
Device > Unleashed Multi-Site Manager SNMP traps	UDP destination port 161 (SNMP)
Unleashed Multi-Site Manager > TACACS+ server	TCP destination port 49 (TACACS+)
Unleashed Multi-Site Manager > Device	TCP destination port 8082 (ZD wakeup)
Device > Unleashed Multi-Site Manager firmware upgrade	TCP destination port 80 (HTTP)
Device > Unleashed Multi-Site Manager template configuration upgrade	TCP destination port 80 and 443 (HTTP and HTTPS)
Device >Unleashed Multi-Site Manager SMTP traps	TCP destination port 25 (SMTP)
Unleashed Multi-Site Manager to FTP server	TCP destination port 21 (FTP)

NOTE

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

Administering a Linux Server

Ruckus recommends that you use the following OS:

- CentOS release 6.5 (64 bit)
- CentOS release 7.1 (64 bit)
- Red Hat Enterprise Linux Server release 6.5 (64 bit)
- Red Hat Enterprise Linux Server release 7.1 (64 bit)

NOTE
Unleashed Multi-Site Manager is generally only installed on VMware/CentOS/ESXi servers for limited installations, as the software database in this environment cannot support larger Ruckus networks. (For VMware system information, contact your sales representative.)

NOTE
Existing customers may not want to switch from the software installed on a VMware server to an RHEL server, as the data will have to be extensively modified for migration.

Continue with the following sections to install the software on a Linux server.

Preparing the Server for Software Installation

Before installing the software, make sure your environment, including the target Linux server, meets all the requirements. This section details preparation of the host server for Unleashed Multi-Site Manager installation and operation.

What You Will Be Doing

- Preparing a clean Linux server according to the minimum system requirements.
- Placing the server on a subnet that is reachable by the Ruckus devices to be managed.
- Customizing your DHCP server.
- You must install jemalloc before installing the software.

  Following are the sample steps to install jemalloc:

  1. Download jemalloc based on your linux version from http://pkgs.org/download/libjemalloc.so.1()(64bit)
  2. Upload jemalloc to the software server and install it issuing this command:

```
rpm -Uvh jemalloc-3.6.0-1.el6.x86_64.rpm
```

Server System Requirements

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

- CPU and RAM: Depends on the number of managed ZoneDirector devices and Unleashed APs, on the purge policy, and whether the software is installed in a Linux or a VMware virtual machine.
- Ruckus recommends that you use the following OS:
  - CentOS release 6.5 (64 bit)
  - CentOS Linux release 7.1 (64 bit)
  - Red Hat Enterprise Linux Server release 6.5 (64 bit)

  - Red Hat Enterprise Linux Server release 7.1 (64 bit)
- HDD: 30GB dedicated to Unleashed Multi-Site Manager, minimum for 10 licenses.
- RAM: 8GB dedicated to Unleashed Multi-Site Manager, minimum.
- CD-ROM device if you choose to use this method of installation.
- Mouse.
- Network adapter.

Refer to the most recent *Unleashed Multi-Site Manager Release Notes* for detailed information.

CAUTION
To ensure that normal software operations run smoothly, make sure that the target Linux server has at least 160GB of free disk space dedicated to it.
The software disk space requirement is doubled when it is being updated.
Database backups also consume extra disk space. The required extra disk space is determined by the number of database backups.
If the software does not have sufficient disk space, then the MariaDB server for it may encounter errors.

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

Web Browser Requirements

The software web interface works with the latest version of Firefox and Chrome web browsers. It is optimized for 1280 x 1024 (and higher) screen resolution.

Editing the Server Hosts File

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

NOTE
If you are planning to enable SMTP notification on the software, then you need to add another line in the hosts file for your SMTP server's DNS information. For more details, refer to SMTP Settings on page 97.

NOTE
If you use "." in the hostname to separate hostname.domainname, then you are not allowed to use a digit-only domainname. For instance, `UMM.ruckus` and `UMM.98ABC` are allowed, and `UMM.98` and `Localhost.12345` are not allowed.

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.

Installing the Software

You can install the software via CD-ROM or via FTP on a Linux workstation that meets the system requirements listed in Server System Requirements on page 20.

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

CAUTION
If your Linux server contains an instance of MariaDB before the software installation, then that MariaDB instance and all dependent packages must be uninstalled before initializing the software installation.

Continue with the following sections:

- Installing from a CD-ROM
- Installing from an FTP Download

Installing from a CD-ROM

1. Log in to the host server as `root`.
2. Insert the software CD into the CD-ROM drive.
3. If the software server does not automatically mount the 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
```

Continue with the figure in Step 7 and then Step 8 in the next task, Installing from an FTP Download.

Installing from an FTP Download

Before performing this task, learn about roles at Understanding User Roles and Privileges on page 104.

1. Log in to the host server as **root**.
2. Upload the *.ISO file (or patch file) to somewhere on the hard drive, such as `/tmp`.
3. Make sure that the *.ISO file owner is `root:root`:

```
# chown root:root *.ISO
```

4. Make a directory for the mount:

```
# mkdir ISO
```

5. Mount the *.ISO file:

```
# mount -o loop *.ISO ISO
```

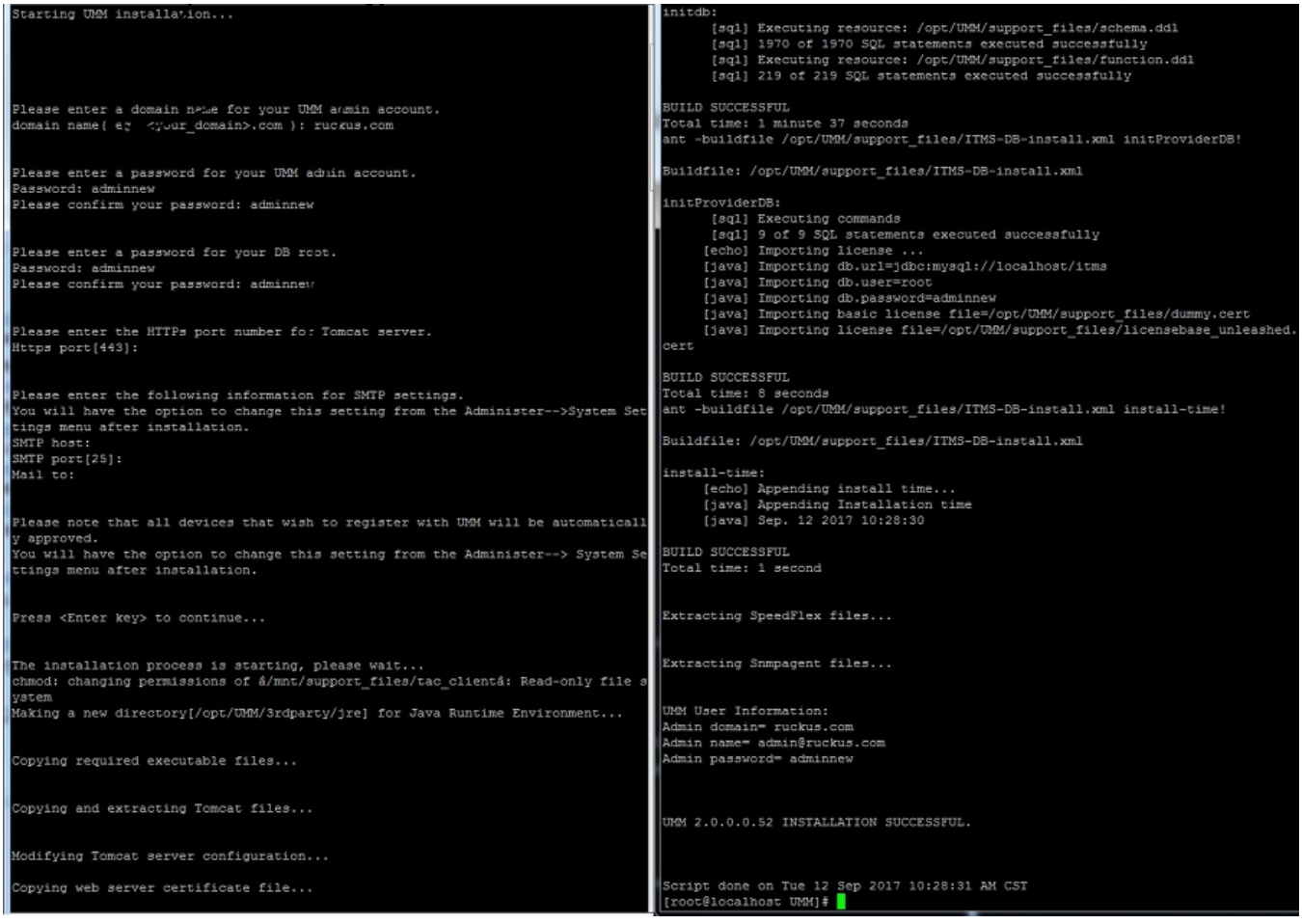
6. Change to the ISO directory:

```
# cd ISO
```

7. Execute the install script `install.sh`.

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

FIGURE 1 Partial software installation including program location, domain identification, and admin password configuration



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 software. A default location is provided. Press **<Enter>** to accept the default location.

```
Location[/opt/UMM]:
```

11. Enter your organization's domain name. By default, the domain name is appended to the word "admin", creating the default Unleashed Multi-Site Manager user account: `admin@domain.com`. The `admin@domain.com` user account is a Super User in the software system and cannot be deleted.

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

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

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

13. Enter a password for the MariaDB 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 software system events are sent.

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

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

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

    FIGURE 2 Configuring the SMTP settings

When the installation completes, a success message appears.

You have completed installing the Unleashed Multi-Site Manager software. You can now log in to the Web interface and configure the software settings. For more information, refer to Logging into Unleashed Multi-Site Manager on page 29.

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

Notable Files in the Software Root Directory

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

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

Upgrading the Software

Ruckus releases Unleashed Multi-Site Manager software updates that contain feature enhancements or fixes for known issues. These software updates are made available on the Ruckus Support Web site or released through authorized channels. Update files typically use `{version number}.patch.tar` for their file naming convention (for example, `9.12.0.0.11.patch.tar`).

Refer to the latest *Unleashed Multi-Site Manager Release Notes* for detailed upgrade information.

CAUTION
Although the software update process has been designed to preserve all software configuration settings, Ruckus strongly recommends that you back up the software database, in case the update process fails for any reason. For information on how to back up the database, refer to Backing Up the Database from the Command Line Interface on page 26 and Backing Up and Restoring the Database from the Web Interface on page 117.

NOTE
After completing the software update, Ruckus recommends backing up the software database so that you have a backup of the updated database schema. For instructions on how to back up the database, refer to Backing Up the Database from the Command Line Interface on page 26 and Backing Up and Restoring the Database from the Web Interface on page 117.

NOTE
The software `/etc/hosts` and `/etc/sysconfig/network` file host names do not support special characters, such as '.'. If special characters are used in these files, then ZoneDirector servers are unable to register with Unleashed Multi-Site Manager.

Uninstalling the Software

1. Execute the sofwtare uninstall script.

```
# [root@umm UMM]# ./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 MariaDB server.
   c) It deletes the configuration files, and uninstalls the software 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/UMM` directory.

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

Backing Up the Database from the Command Line Interface

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

Unleashed Multi-Site Manager includes `backup.sh`, a script for backing up the software database, which is located in its root directory.

Follow these steps to back up the software database.

1. On the Linux server, go to the software root directory (`/opt/UMM`).

2. Execute the database backup script. You can either specify the file path and file name of the backup file, or you can let Unleashed Multi-Site Manager automatically set the path.
   - To back up the software 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 software root directory with the file name `Mybackup.tgz`, then enter the following command:

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

   - To back up the software 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/UMM/dbBackup` folder, and the file name is automatically assigned based on the date and time when the backup script was executed (for example, `DB_2017-09-20_10h26m.cli`).

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

For more information about backing up and restoring the database via the Web interface, see Backing Up the Database from the Web Interface on page 118

Restoring the Database from the Command Line Interface

Unleashed Multi-Site Manager provides `restore.sh`, a script for restoring a backup copy of the software database located in the software root directory.

CAUTION
Before starting this procedure, take note of the file path and file name of the software 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 software database.

1. On the Linux server, go to the software root directory (`/opt/UMM`).
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 software root directory, then enter the following command:

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

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

What's Next?

With Unleashed Multi-Site Manager now installed, you can log in and configure the software to manage your Ruckus devices. The chapters that follow guide you through all of these configuration tasks.

Getting Started with Unleashed Multi-Site Manager

Logging into Unleashed Multi-Site Manager

Use one of the Web browsers described in Web Browser Requirements on page 21 to access the software Web interface:

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

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

   `https://<ipaddress>`

   --OR--

   `https://umm`

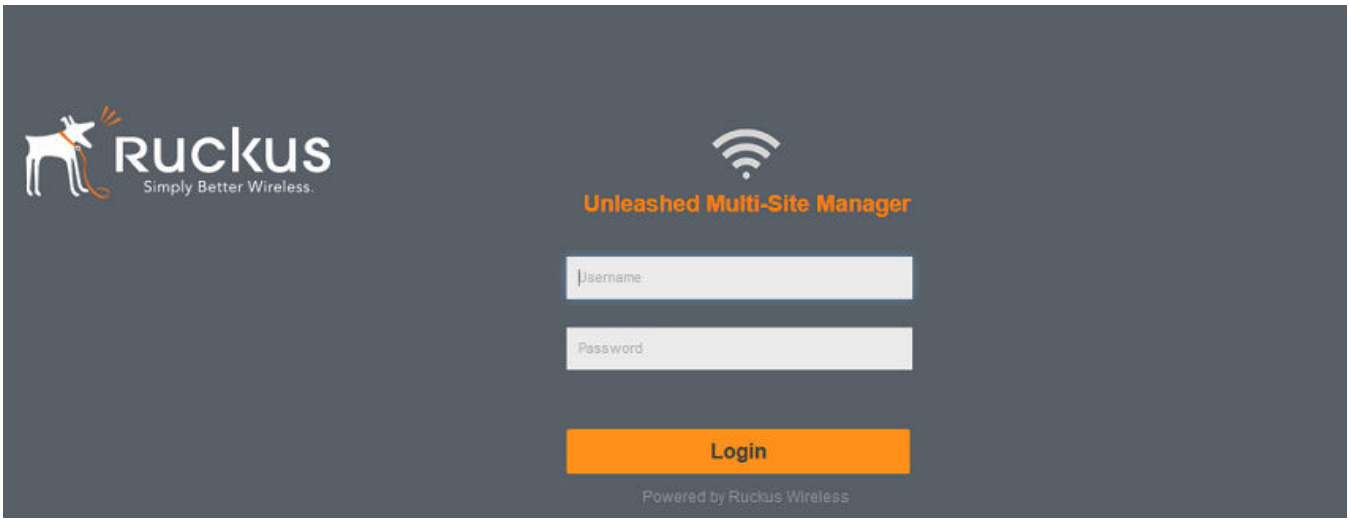
3. Press **<Enter>** to initiate the connection.

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

   > NOTE
   > By default, Unleashed Multi-Site Manager uses a Ruckus 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 the software using HTTPS, then you can install a certificate issued by a recognized certificate authority such as VeriSign. For information, refer to Managing SSL Certificates on page 108.

   The **Ruckus Admin** login page appears.

FIGURE 3 The 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 the software installation (refer to Installing the Software on page 22). 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 on page 99.

   > NOTE
   > If you log in using the TACACS+ server, then your user name appears in the top right of the Unleashed Multi-Site Manager page followed by *(Tacacs+)*.

6. Click **Log In**. The Web interface appears in the browser window. The **Dashboard** workspace appears by default.
   For more on the Dashboard, refer to Getting to Know the Dashboard on page 32.

> **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 software configuration.

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

Features of the Web Interface

FIGURE 4 The Web interface

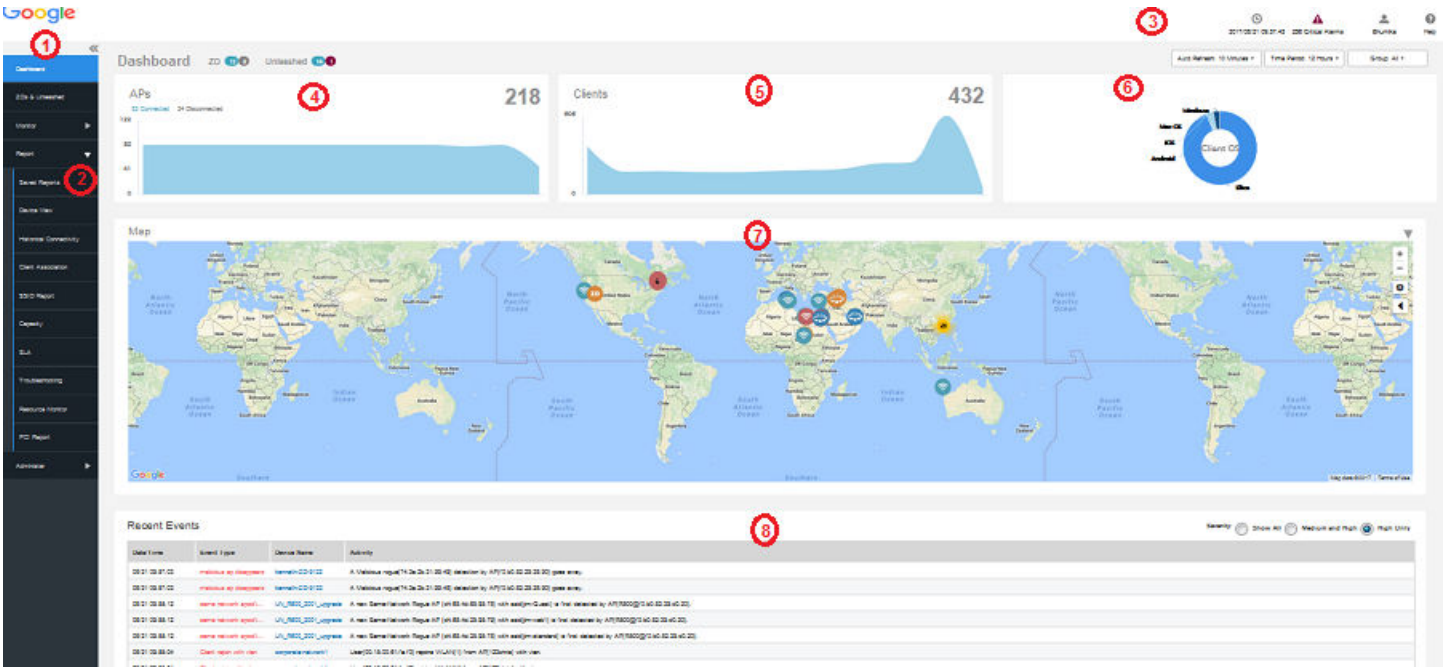


TABLE 4 Web interface elements

No.	Interface Element	Interface Element Description
1	Main Menu	Five tabs group related tasks that you can perform in Unleashed Multi-Site Manager . These tabs include: • Dashboard • ZDs & Unleashed • Monitor • Report • Administer

TABLE 4 Web interface elements (continued)

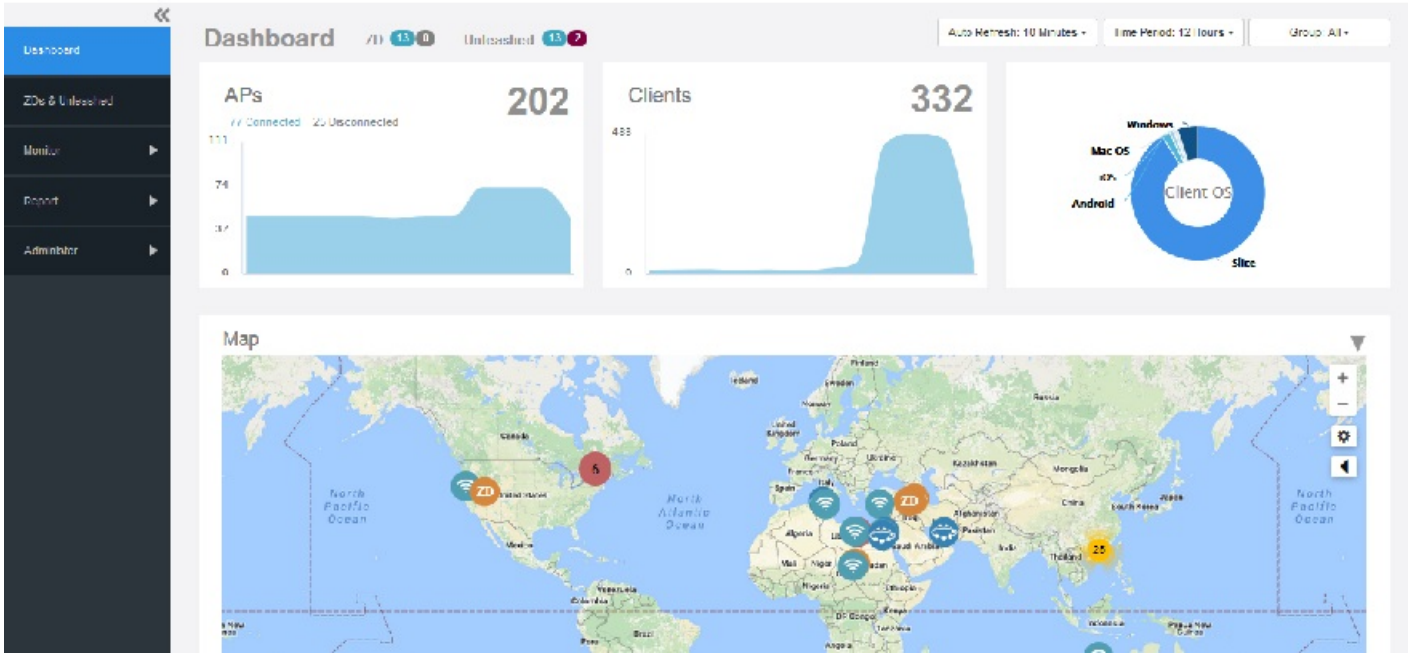
No.	Interface Element	Interface Element Description
2	Submenu	On each tab are second level menu items that, when clicked, display related options in the content area to the right.
3	Alarms, Help and Log Out	• Alarm severity is classified into the order of **Critical**, **Major**, **Minor** and **Warning**. It shows the number of alarms triggered based on the severity. For example, if **Critical** alarms are generated, it will show the number of critical alarms. If there aren't any critical alarms, then it will show the number of alarms in the next severity type - the number of **Major** alarms. • Shows the major alarms (if enabled in **Monitor** > **Alarm Settings**). • Shows the current software date and time. • Click the **Help** link to open the online help. • Click the **Log Out** link to log out of the software. The user name identifies the user who is logged in. • If Unleashed Multi-Site Manager has an active *trial* license file, then a notice appears that the software is using the trial license file and when the trial license file expires. When the trial license file expires, Unleashed Multi-Site Manager deletes devices for which there are not enough licenses.
4	APs panel	Displays the number of APs that are connected and disconnected for a period of time. Above this panel you can also see the number of ZoneDirector controllers and Unleashed APs that are connected and disconnected in real time.
5	Clients panel	Displays the number of clients that are connected and disconnected for a period of time.
6	OS panel	Displays the OS utilization by the clients. You can modify the dashboard view by selecting the following options present above this panel: • Auto Refresh • Time Period • Group All
7	Map	Displays information about the APs deployed in the Goggle map.
8	Recent Events	Displays the events that were recently triggered for the device (ZoneDirector or Unleashed APs). You can also sort the events to view them by severity type.

Getting to Know the Dashboard

After you log in to the Web interface, the Dashboard is the first page that appears. The Dashboard provides a quick summary of what is happening on Unleashed Multi-Site Manager and its managed devices.

The **Auto Refresh** option allows you to select the time interval for the page to auto refresh an display the latest information. The **Time Period** option allows you to select the period of time for which data must be displayed in the dash board. You have the option to select 12 hours, 24 hours, 7 days and 31 days and the time period. The **Group All** option allows you to select what data which you need to display on the dash board. You can choose to select **All**, **ZD**, or select based on user.

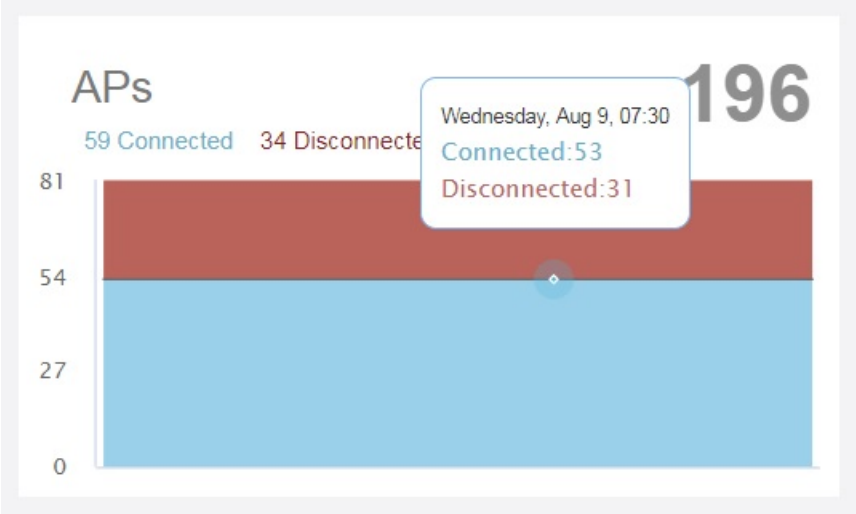
FIGURE 5 Dashboard



It displays at-a-glance information about the following:

- The number of ZDs and Unleashed, which are connected and disconnected.
- The number of APs that are registered with ZoneDirector and Unleashed devices (which, in turn, are being managed by Unleashed Multi-Site Manager).

FIGURE 6 APs

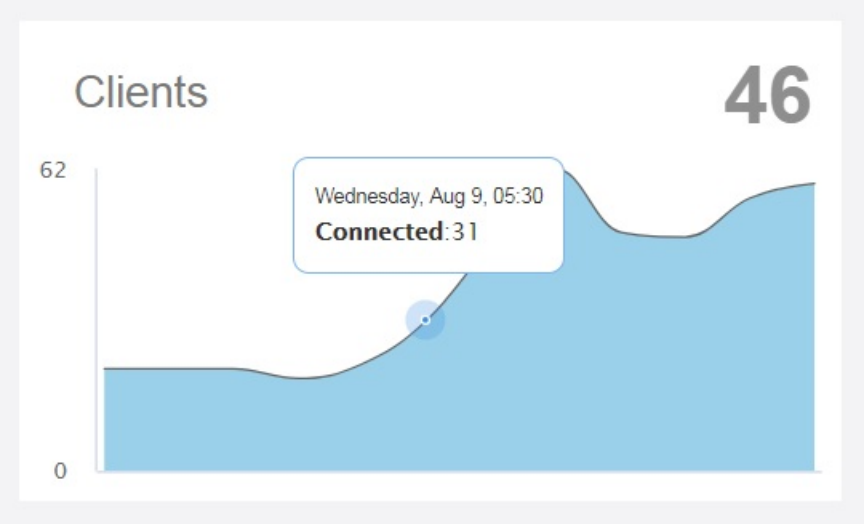


The graph displays the number of connected and disconnected APs depend on the time period option selected. For example, if you select 12 hours, then the graph displays trends for devices connected or disconnected for the last 12 hours. Mouse-over

along the graph to display the connected and disconnected AP statistics at any time withing the select time range to view the respective statistics.

- The number of clients that are associated with the currently connected APs.

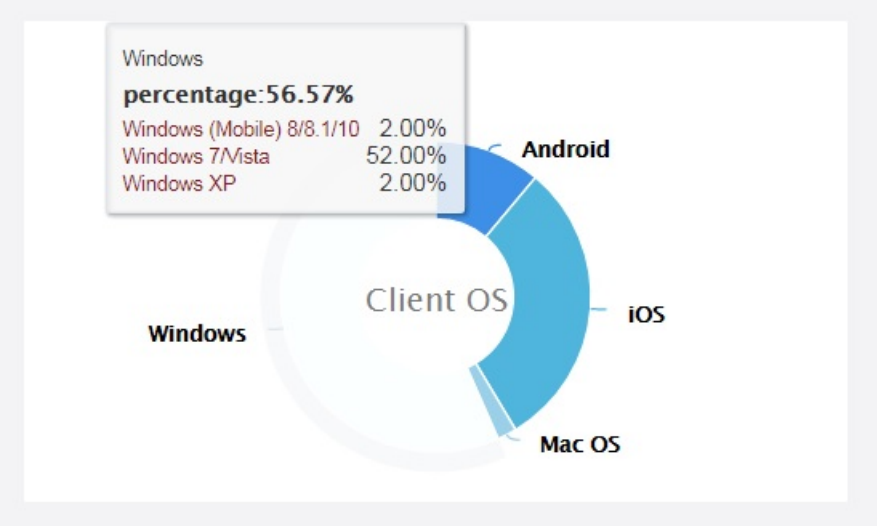
FIGURE 7 Clients



Mouse-over along the graph to display the connected clients at any time withing the select time range.

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

FIGURE 8 Client OS



Mouse-over the graph to see the percentage share of OS used by client devices. For example, a 56% for windows means, out of the total client devices accessing the server, 56% of those devices are having Windows Operating System. Further, it also displays the percentage of various versions of each OS, accessing the server.

- Map which displays the various AP and Device information across the globe. Mouse over the AP or device to see the respective statistics.

  FIGURE 9 Maps

- The **Recent Events** panel displays information about events that have occurred on Unleashed Multi-Site Manager, on managed ZoneDirector devices, and on clients.

  The following table describes the information that you can find on the **Recent Events** panel.

TABLE 5 Columns on the Recent Events Panel

Column Name	Description
Date / Time	Displays the event time stamp.
Event Type	Displays the name of the event (as assigned by Ruckus).
Device Name	Name of device reporting the event. Click this link to go to an **Inventory** > **Reports** view of the devices reporting the specific event.
Activity	Events description.

The information in the **Recent Events** can be displayed based on the severity (**Show All**, **Medium and High** and **High Only**), which you can select form the tope right corner of the panel.

Getting Started Tasks

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

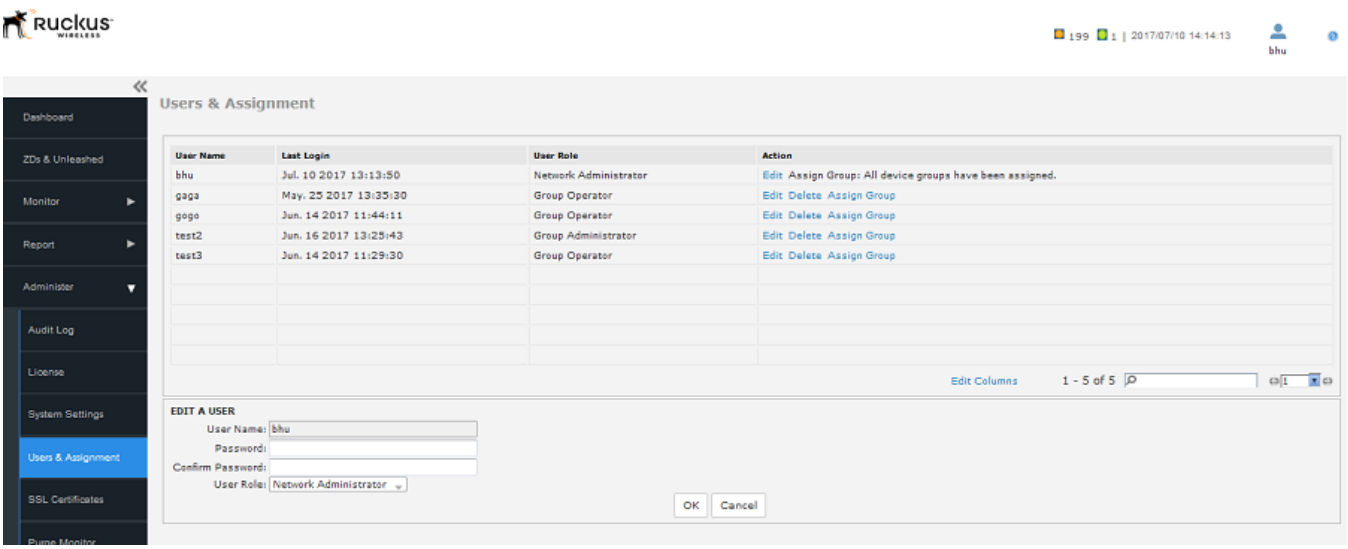
- Changing the Default Administrative Password
- Pointing A ZoneDirector and Unleashed device to Unleashed Multi-Site Manager
- Checking Your software License

Changing the Default Administrative Password

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

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

FIGURE 10 Editing User Password



4. Type a new password in the **Password** field.
   - Passwords must be between 6 and 32 characters long, and must be comprised of letters and numbers only.
   - Passwords are case-sensitive.
   - Do not use spaces.

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

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

Pointing a ZoneDirector or Unleashed Network to Unleashed Multi-Site Manager

If you want to use Unleashed Multi-Site Manager to monitor and administer ZoneDirectors or an Unleashed network, then follow the procedures listed in the Enabling Management via Unleashed Multi-Site Manager section in the *ZoneDirector User Guide* and *Unleashed Quick Start Guide*. For more information, see Appendix on page 125

NOTE
Make sure that the required communication ports are open between the ZoneDirector or Unleashed network and Unleashed Multi-Site Manager as described in Firewall Ports that Must be Open for Communications on page 19.

Checking Your Software License

A fresh Unleashed Multi-Site Manager installation provides only 1 Unleashed license by default. When you upgrade the software from a FlexMaster version to Unleashed Multi-Site Manager, it provides 100 ZoneDirector licenses and 1 Unleashed license, by default. For additional Unleashed AP management, you must buy the paid license and upload them. Unleashed networks consume license numbers by the 'active AP number' under it.

When you are managing ZoneDirector using Unleashed Multi-Site Manager, 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 APs), for example, consumes 250 license seats.

The Unleashed license is updated when Unleashed Multi-Site Manager receives a message from Unleashed, however the Unleashed AP connection status is updated every 15 mins. Therefore, there is an inherent difference or delay between when Unleashed Multi-Site Manager updates the Unleashed license (every 1~60 mins), and its AP connection status (15 mins). This may cause inconsistences between the connected AP and license on the user interface.

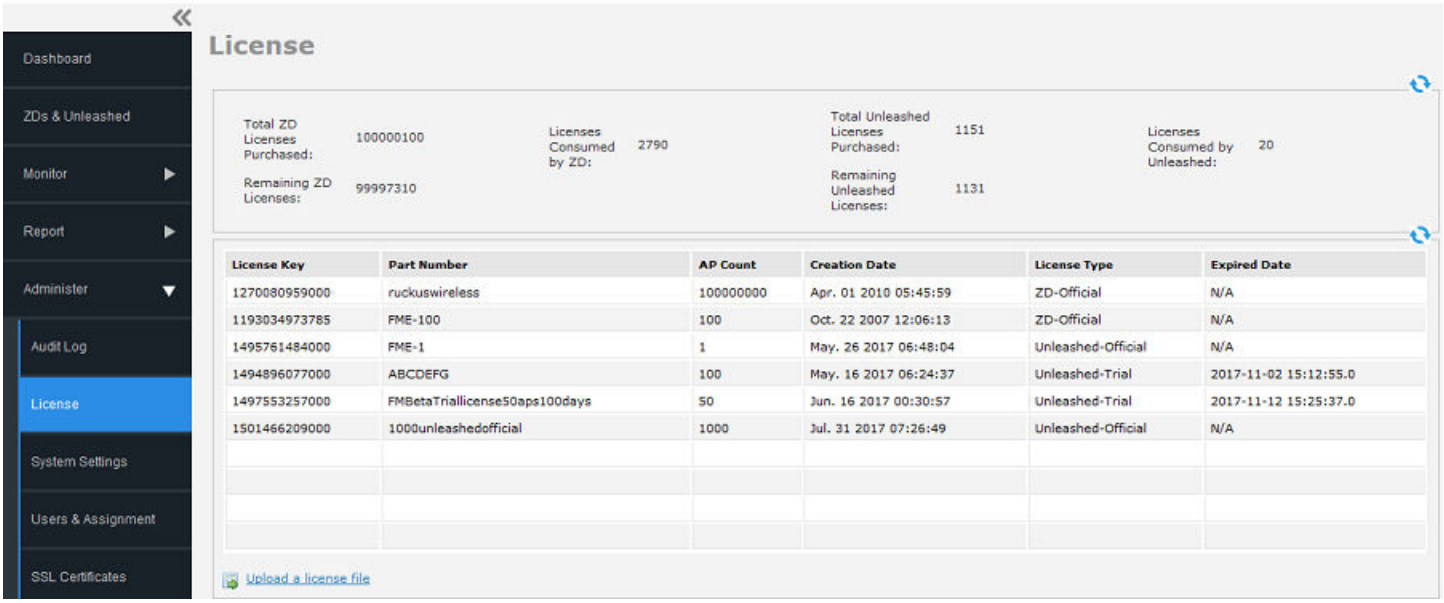
When trial licenses expire, Unleashed Multi-Site Manager checks the license number and deletes the device(s) as necessary. It does not monitor this device anymore.

NOTE
When the Smart Redundancy feature is enabled, the Smart Redundant pair of ZDs consume one extra ZoneDirector license.

When this seat limit is reached, no additional devices are able to register with Unleashed Multi-Site Manager until a license file that provides additional license seats is uploaded.

Before using Unleashed Multi-Site Manager to manage Ruckus devices, Ruckus recommends that you check how many ZoneDirector devices and Unleashed 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 Unleashed APs.

FIGURE 11 License Details



If the number of devices that you plan to manage exceeds the number of devices supported by the license file, then you need to contact Ruckus Sales representative, obtain a license file for additional devices, and upload it to Unleashed Multi-Site Manager.

Working with ZoneDirector Controllers and Unleashed APs

Viewing Devices Managed by the Software

The ZDs & Unleashed page of the Web interface displays information about devices that the Unleashed Multi-Site Manager software manages. These devices include ZoneDirector controllers, Unleashed APs and Clients.

Follow these steps to view the devices manage by the software:

After you to login to the web interface, select **ZDs & Unleashed** from the menu in the left.

The **ZDs & Unleashed** page appears listing all the devices managed by the software.

You can use **View Mode**, to select how you want the device information to be presented.

- List: Displays the list of all devices irrespective of the Group they belong to.

  Group: Displays the list of devices in a hierarchical format.

FIGURE 12 Page listing devices managed by Unleashed Multi-Site Manager - List View

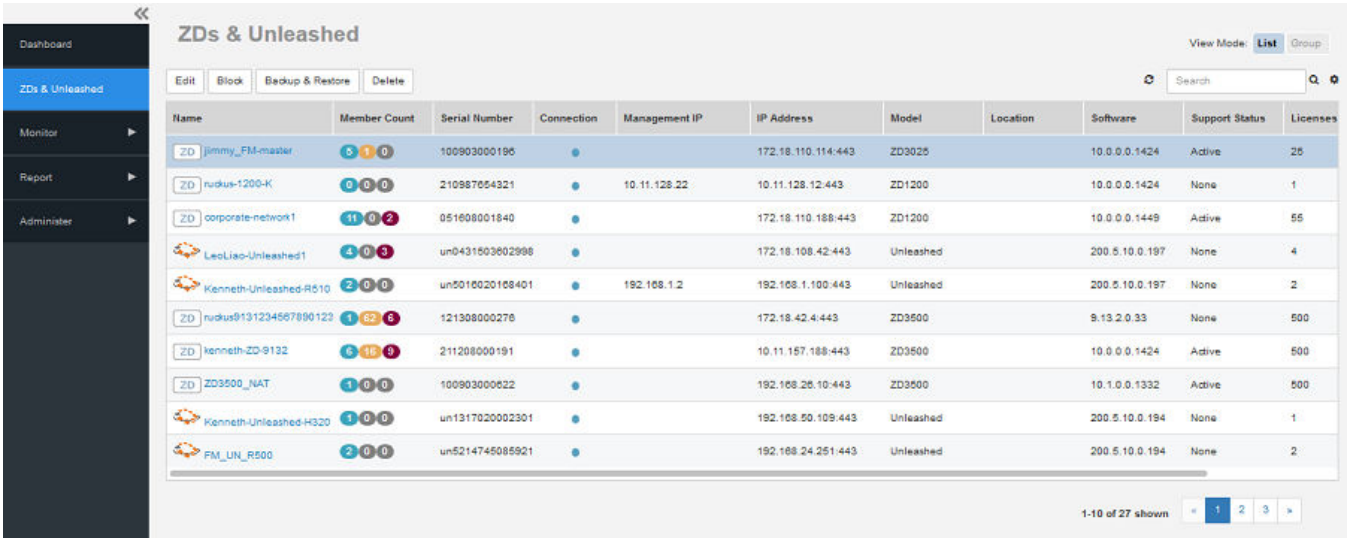
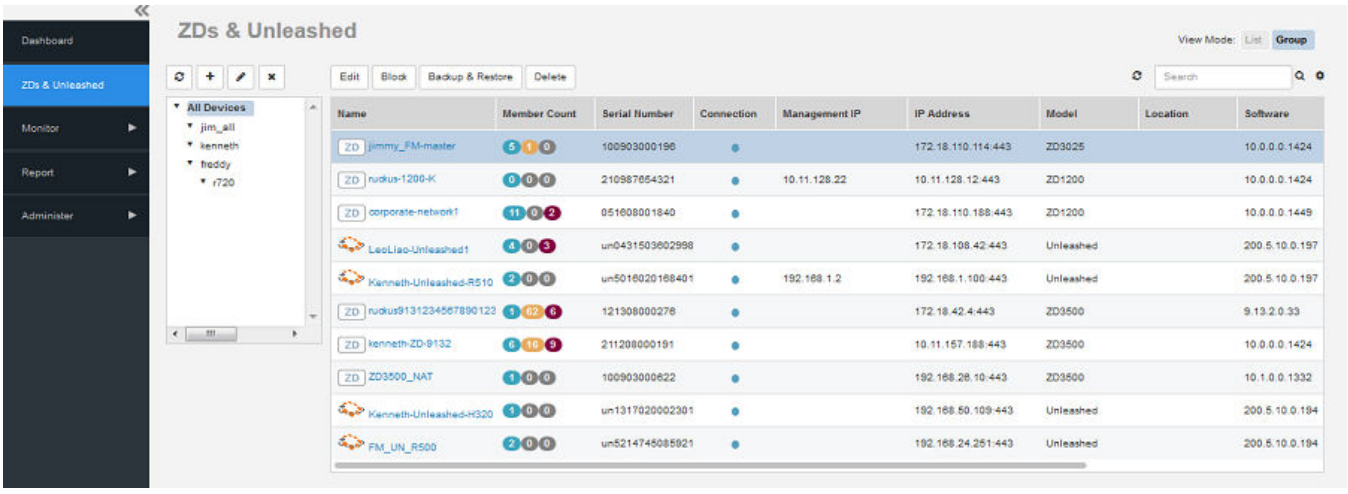


FIGURE 13 Page listing devices managed by Unleashed Multi-Site Manager - Group View



Click the icon to refresh the contents of the table.

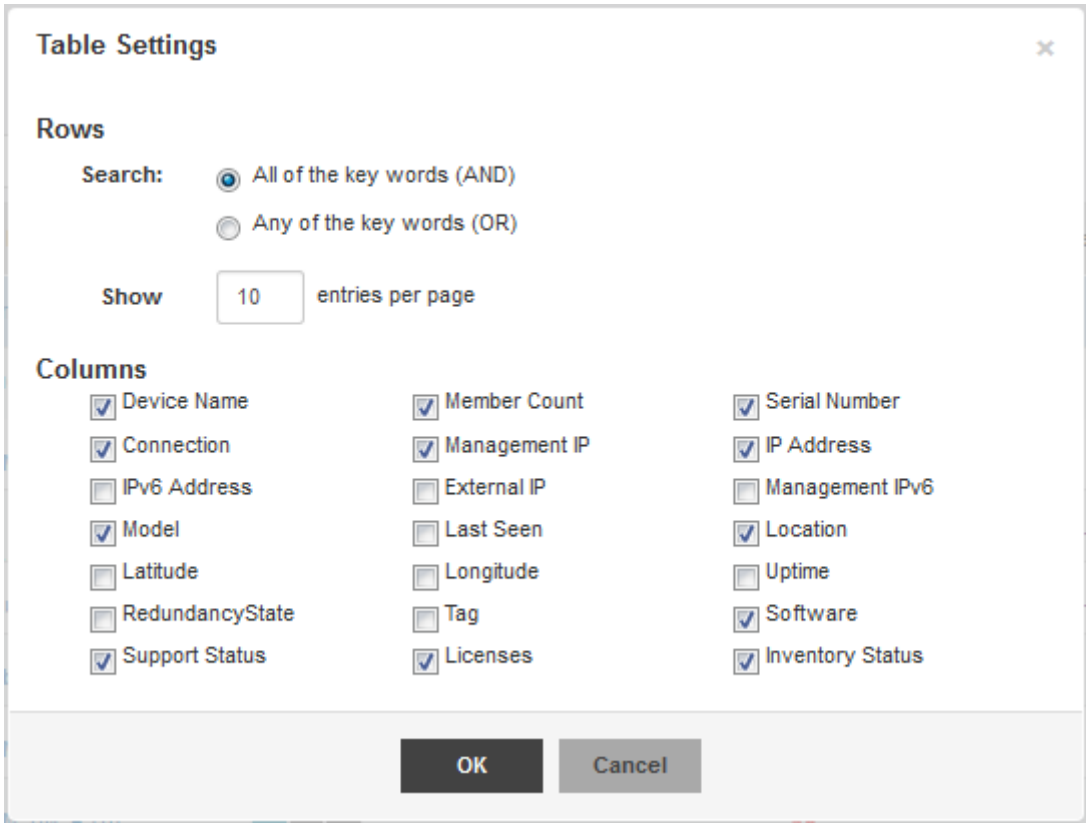
The following table list some of the fields and table columns that appear by default:

Field/Column	Description
Device Name	Displays the name of the device - it could be a ZD controller or an Unleashed network that software manages.

Field/Column	Description
	Clicking the device name hyperlink opens the dashboard of the controller in a new page.
Member Count	Displays the status of the members managed by the ZD controller or the Unleashed network, namely **Connected**, **Disconnected** and **Pending**.
Serial Number	Displays the serial number of the device.
Connection	Indicates whether the device is currently online ( ) or offline ( ) or online with some APs disconnected ( ).
External IP	Displays the IP address of the device when it is behind the NAT server. Unleashed Multi-Site Manager uses this IP address to manage the device. For ZoneDirector or Unleashed which are behind NAT, include port 443 for port forwarding.
Tag	When configured, this column shows a generic attribute (Device Tag) that can be used to identify the device. For example, when this AP device is located in main office, you can assign the tag “Main” to it.
IP Address	Displays the IP address assigned to the device. **NOTE** The port number after the IP address indicates the protocol that you can use to gain access to the device’s Web interface. If `:443` appears after the port number, you can access the device’s Web interface using: `https://{device-IP-address}.`
IPv6 Address	Displays the IPv6 address of the device.
Model	Displays the Model of the managed Ruckus device.
Uptime	Displays how long since the device was last rebooted.
Latitude	Displays the latitude (North-South position) of the device.
Longitude	Displays the longitude (East-West position) of the device.
Location	Displays the Location of the device (if provided).
Software	Displays the software version that is installed on the device.
Support Status	Displays the support status for the device.
Licenses	Displays the number of licenses consumed by the device.
Inventory Status	Displays the permission that is assigned to the device such as Permitted, License Exceeded and Lost Device

By clicking , you can customize the table settings that are displayed. You must select the check boxes to display the columns in the table and enter the number of rows you want to display in the table, in addition to specifying the search criteria.

FIGURE 14 Customizing the Table Settings



Type a word or phrase that you want to search for within the **Search box**, and then wait for a second or two. The software refreshes the page and displays devices with attributes that matched your search keyword or keyphrase. The matching attributes are highlighted and Unleashed Multi-Site Manager displays up to ten search results on each page by default. The number of rows is however customizable. When your search generates more results than the number of rows set, use the left arrow and right arrow icons after the search box to display the previous page or next page, respectively.

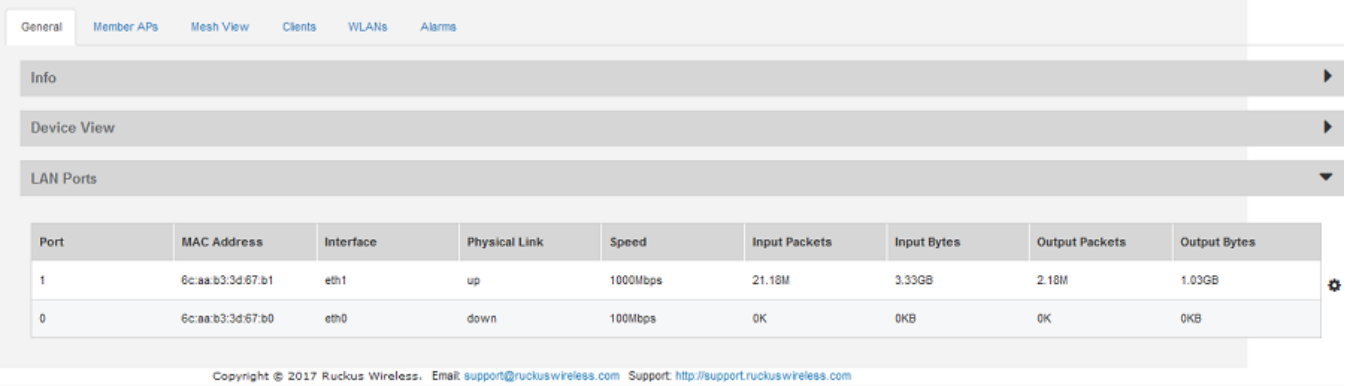
Viewing Device Configuration

You can view the configuration details of the devices managed by Unleashed Multi-Site Manager.

After you login to the Web interface, select **ZDs & Unleashed** from the menu in the left.

The **ZDs & Unleashed** page appears listing all the devices managed by the software. The lower panel of this page displays the configuration details of the device which are organized into tabs as described in the table.

FIGURE 15 Viewing device configuration details



Configuration Tabs	Description
General	This tab displays the following: • **Info**: provides basic device information including the number of data bytes and packets transmitted and received by the device. • **Device View**: provides detailed information about the clients and APs associated with the device. • **LAN Ports**: provides detailed information about the ports open to the device, speed of data transfer/reception, and the number of data packets and bytes transmitted and received.
Member APs	Displays a table with detailed information about the APs associated with the device, such as the number of authorised clients associated with the AP, software version, model number, uptime, IP address and current status of the AP.
Mesh View	Displays a table that lists the mesh details of the device such as the mesh topology, signal strength, MAC address, IP address, channel used and number of authorised clients.
Clients	Displays a table detailing information about the AP associated with the client such as the MAC address of the wireless client, IP address assigned to the client, Radio channel the client uses, Signal strength, VLAN ID assigned to the client, Uplink and Downlink traffic, and client connection status.
WLANs	Displays a table that lists the WLANs configured on the device, including the WLAN names, ESSIDs, authentication and encryption methods, and the number of clients associated with each WLAN, Tx/Rx of bytes and packets.
Alarms	Displays a table that lists information about the typ of alarm that was triggered, the time and date when the alarm was generated, severity and activity associate with the alarm.

Click the icon to refresh the contents of the tables within these tabs. You can also customize the tables by clicking the icon. You can also make use of the **Search** box to look for specific information within the tables.

Creating and Managing Groups

Unleashed Multi-Site Manager allows you to create and edit device groups, and to assign devices to existing device groups. Each device can be assigned to a single device group at a time, and can be moved to a different device group at any time.

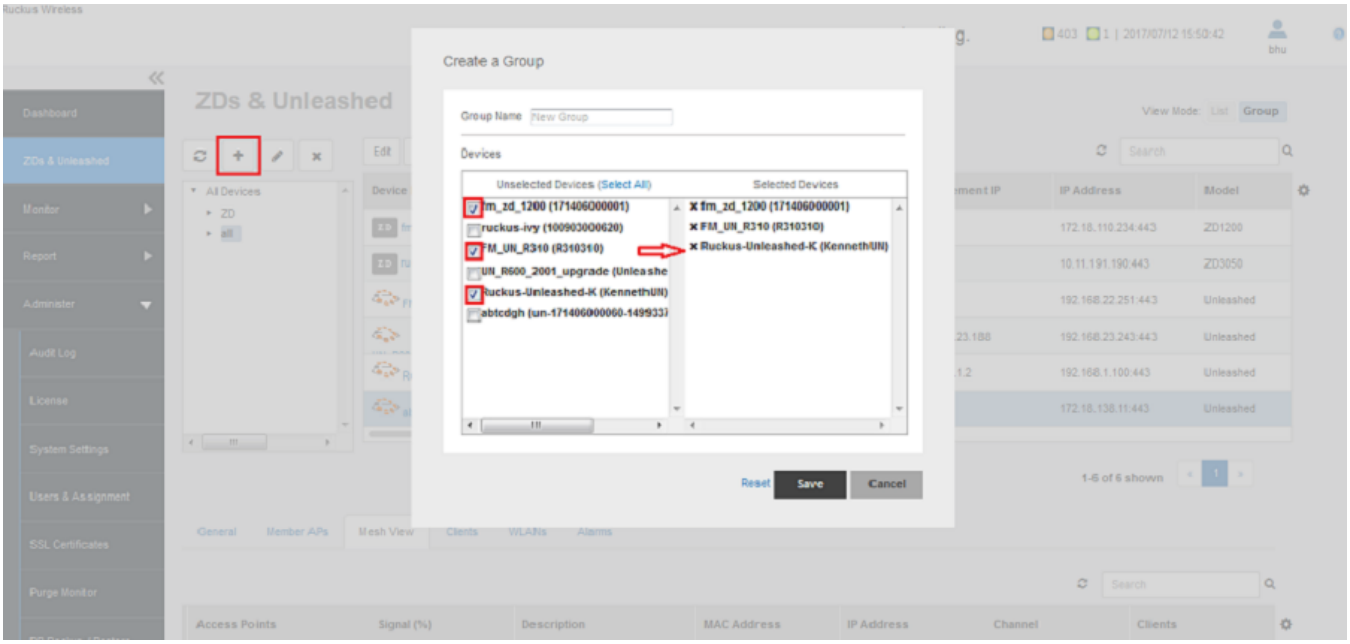
1. After you to login to the Web interface, select **ZDs & Unleashed** from the menu in the left.

   The **ZDs & Unleashed** page appears listing all the devices managed by the software.

2. From the device group hierarchy, select device under which you want to create the group and click the + icon.

   The **Create a Group** page appears.

FIGURE 16 Creating a Group



3. In **Group Name**, type the name of the group you want to create.
4. In **Devices**, under the *Unselected Devices* section, select the devices that you want to group by checking the box against the device. Those selected are populated under the *Selected Devices* section.
5. Click **Save** to confirm the grouping.

   A success message is displayed after the group is created.

6. Click **OK**.

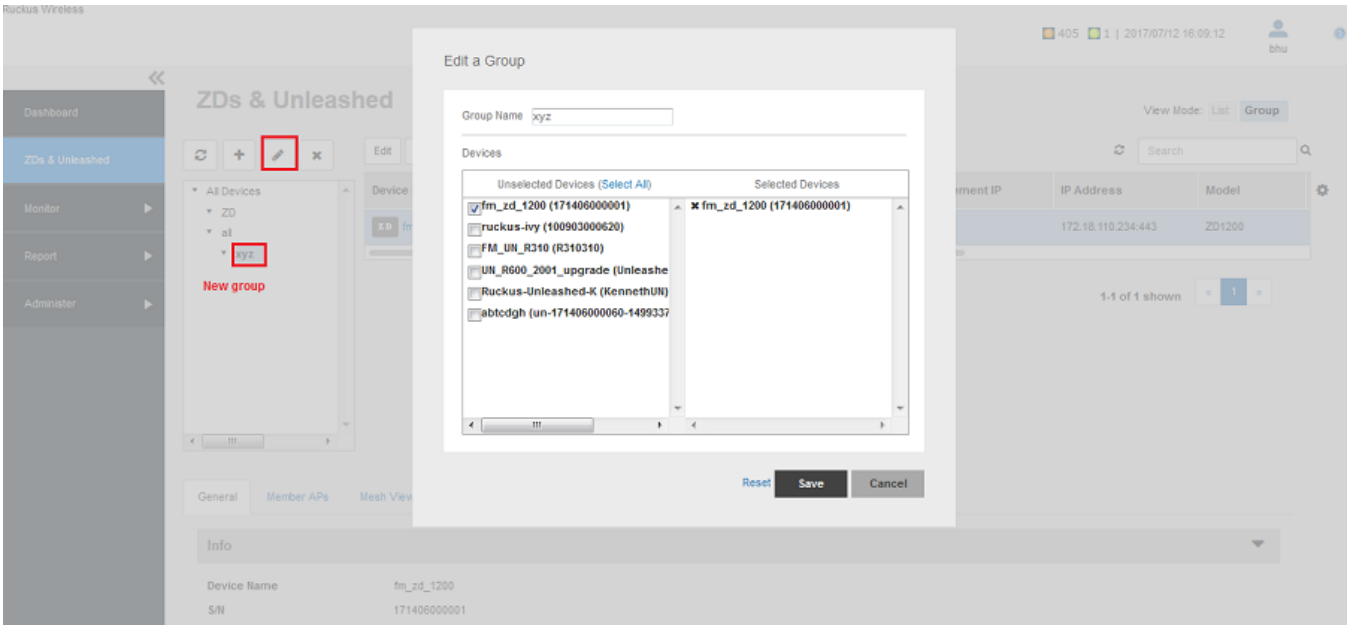
   The newly created group is listed under the device hierarchy.

Editing a Group

7. Select the group and click the icon.

   The **Edit a Group** page appears.

   FIGURE 17 Editing a Group



8. Make the necessary changes and click **Save**.

You have successfully edited the group.

To delete a group, select it and click the icon above the device hierarchy tree.

Editing Device Properties

You can edit a device's tag name, location, GPS coordinates and Web port mapping.

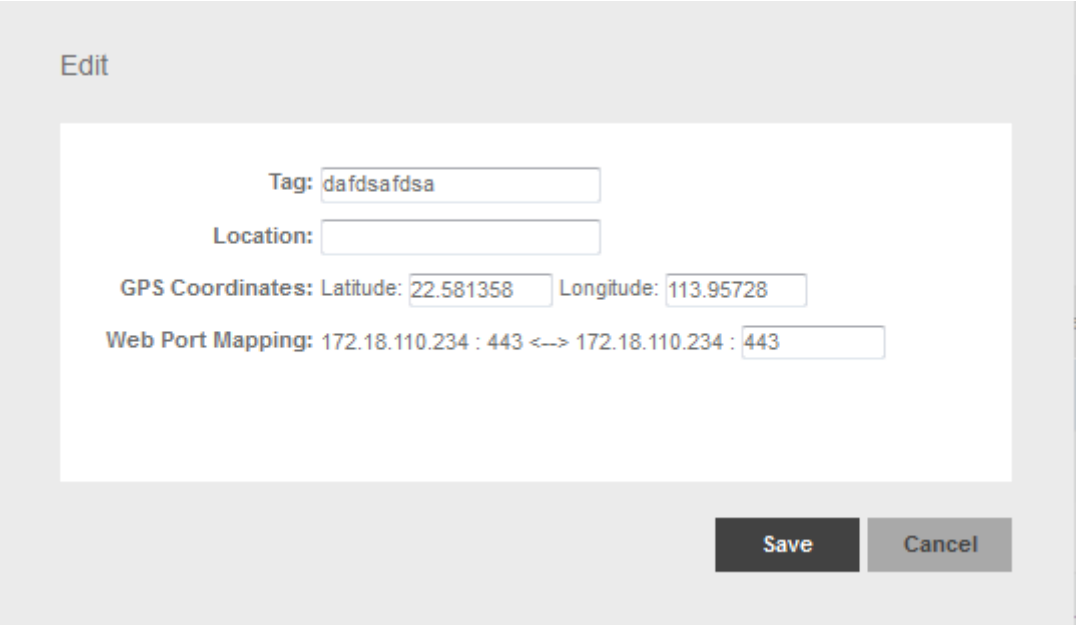
1. After you to login to the Web interface, select **ZDs & Unleashed** from the menu in the left.

   The **ZDs & Unleashed** page appears listing all the devices managed by the software.

2. From the list of devices, select the device for which you want to edit the propertied, then click **Edit**.

   The **Edit** dialog box appears.

   FIGURE 18 Edit dialog box



3. Modify the following configuration settings:
   - Tag: Type the device tag name.
   - Location: Type the location of the device.
   - GPS Coordinates (Latitude and Longitude): the software uses these to position the device icon on the map.
   - Web Port Mapping: The port number after the IP address indicates the protocol that you can use to gain access to the device's Web interface. Default port number is 433 for HTTPS protocol.
4. Click **Save**.

   A success message is displayed after the device properties are saved.
5. Click **OK**.

   The new configuration changes for the device are saved and refreshed in the table.

Blocking Devices from the Software

If devices within the network seem unauthorized or are a threat to security, you can use the software Web interface to block the device. You can block one or more devices at a time.

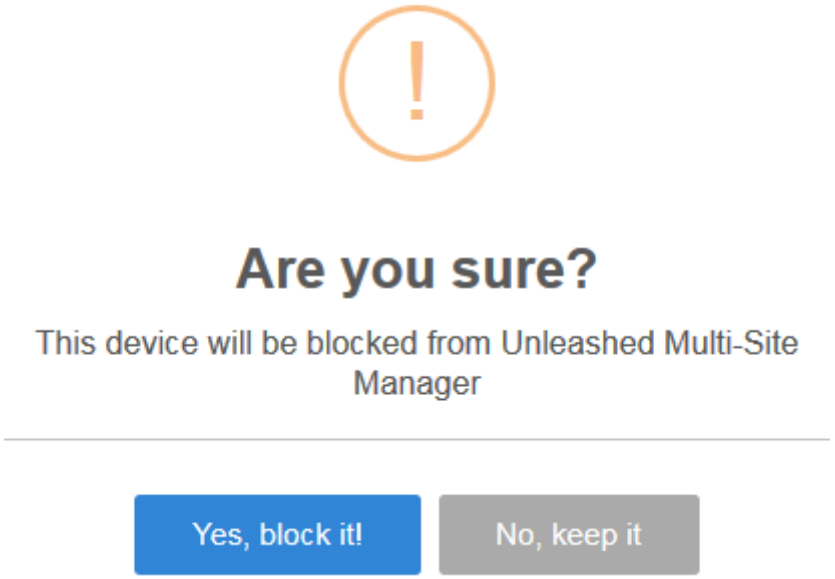
1. After you to login to the Web interface, select **ZDs & Unleashed** from the menu in the left.

   The **ZDs & Unleashed** page appears listing all the devices managed by the software.

2. From the list of devices, select the device you want to block and then click **Block**.

   A confirmation message appears asking if you want to block the devices from the software.

FIGURE 19 Block screen



3. Click **Yes, block it!**.

   The device is blocked, and Unleashed Multi-Site Manager no longer manages the device.

Backing Up Device Configuration Files

You can create configuration backup files for all the devices managed by the software, to recover configuration settings in the event of a device failure. The backup files can be created for single or multiple devices.

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

NOTE
The number of ZoneDirector (ZD) and Unleashed configuration backups to retain in the software database for each ZD and Unleashed is limited to 10.

1. After you to login to the Web interface, select **ZDs & Unleashed** from the menu in the left.

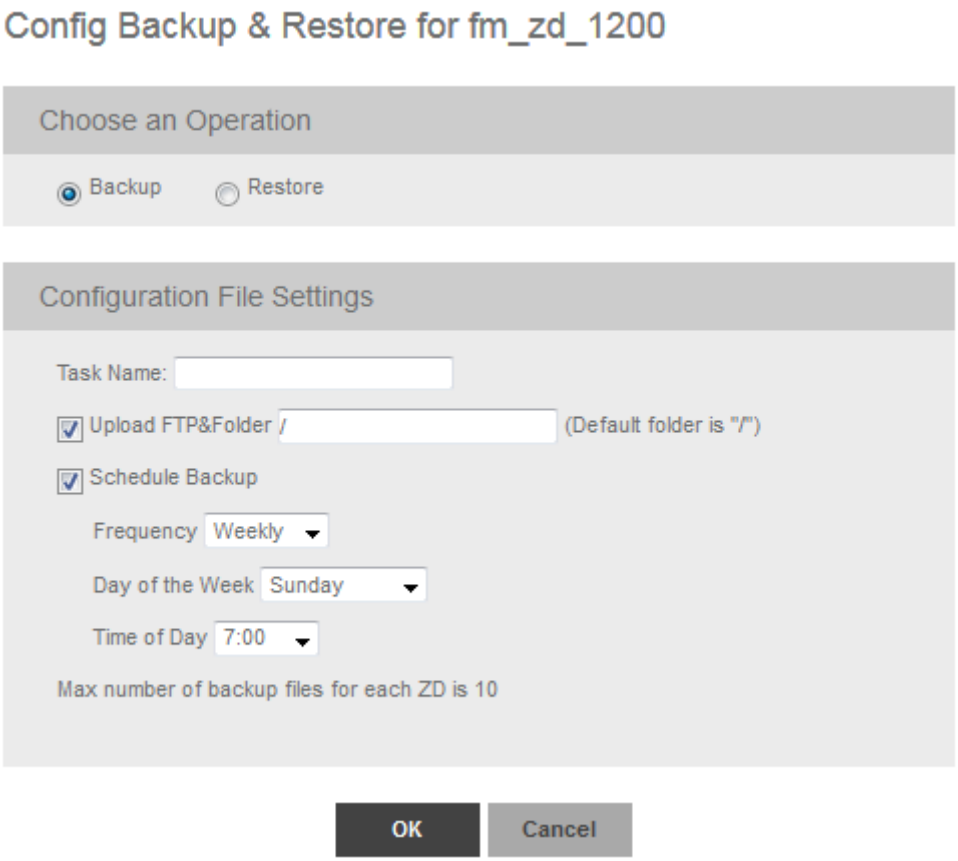
   The **ZDs & Unleashed** page appears listing all the devices managed by the software.

2. From the list of devices, select the device for which you want to back up the configuration values and then click **Backup & Restore**.

   The **Configuration Backup & Restore** form for the device appears.

   You can select multiple devices by pressing CTRL + click the device.

   FIGURE 20 Backing Up Configuration



3. In **Choose and Operation**, select **Backup**.
4. In **Configuration File Settings**, enter the following:
   - Task Name: type the name of the backup file. Use a descriptive name that helps you identify this backup configuration
   - Upload FTP & Folder: select the check box and type the workstation folder and the software will upload the backup file to the FTP server.
   - Schedule Backup: select the check box to schedule when you want to back up of the configuration.

     After you select the check box, the **Frequency** and **Time of Day** options are displayed. Select the options from the drop-down menu as appropriate. In **Frequency**, if you select Weekly or Monthly, the corresponding **Day of the Week** or **Day of the Month** options are displayed, respectively.
5. Click **OK**.

   A success message is displayed after the task is created.

   You can view the created task from **Monitor** > **Task**.

6. Click **OK**.

   The schedule to backup the device configuration is created.

Restoring Device Configuration

Unleashed Multi-Site Manager enables you to restore device settings easily from a backup file. You have the option to perform full restore, failover restore or a policy-level restore to another device.

Before performing a restore procedure for the device, make sure that you have at least one backup file that you can use to restore the device settings.

Restoring device 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.

Also ensure that you are selecting the appropriate restore type. For example, when you only want to restore the wireless, access control, and user settings, make sure you select *Policy Restore*. Selecting *Full Restore* overwrites all existing device settings, including the IP address, system name, user name, and password.

An 'Unleashed ID' is automatically generated by the system for each unleashed network. This ID is reset when the device is set to factory default, and may be overwritten when device configuration is restored (depend on which restore option are selected).

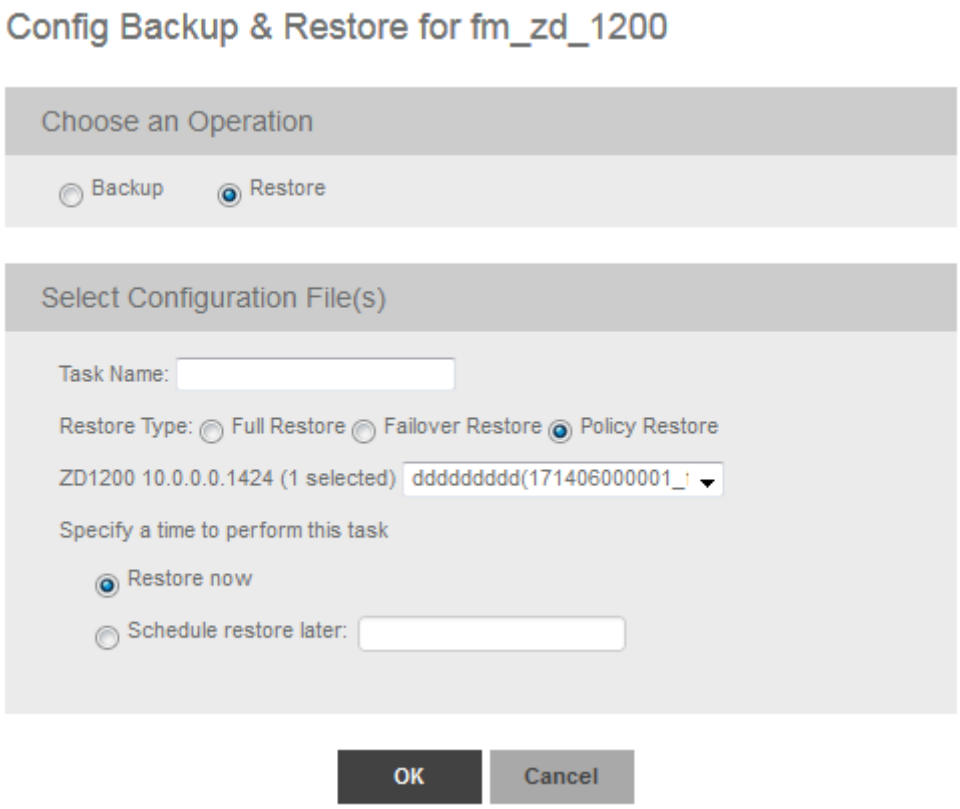
NOTE
The number of ZoneDirector (ZD) and Unleashed configuration backups to retain in the software database for each ZD and Unleashed is limited to 10.

1. After you to login to the Web interface, select **ZDs & Unleashed** from the menu in the left.

   The **ZDs & Unleashed** page appears listing all the devices managed by the software.

2. From the list of devices, select the device for which you want to restore the configuration values and then click **Backup & Restore**. The **Configuration Backup & Restore** form appears.

FIGURE 21 Restoring the Configuration



3. In **Choose and Operation**, select **Restore**.

4. In **Configuration File Settings**, enter the following:
   - Task Name: type the name of the restore task the you want to create. Use a descriptive name that helps you identify this task.
   - Restore Type: choose one of the following
     - *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 device with those from the backup file. For example, if the configuration file of a device becomes corrupted, then you can use full restore to recover the device.
     - *Failover Restore*: Restores all settings from the backup file, except the system name, IP address, user name, and password. Use this restore type when you want to configure a secondary device as a failover unit. After configuring the secondary device, deploy it to the same network as the primary device. If the primary device fails for any reason, then all APs managed by the primary device are able to report to the secondary device automatically. If you choose this restore type, then you need to manually configure the IP address, system name, user name and password of the secondary device.
     - *Policy Restore*: Restores only the wireless, access control, role, and user settings from the backup file. Use this restore type when you want to apply the same set of common settings to multiple devices. You need to first configure one device with your preferred wireless, access control, role, and user settings, back up these settings, and then restore them onto the target devices.
   - Device Selection (ZD or Unleashed): from the drop-down menu, choose the target configuration file to restore.
   - In **Specify time for this task**, specify when you want the task to run. To run the task immediately, click **Restore now**. To schedule the task, click **Schedule restore later** and then select the date and time.
5. Click **OK**.

   A success message is displayed after the task is created.

   You can view the created task from **Monitor** > **Task**.
6. Click **OK**.

   The configuration restore task is created.

Deleting Devices Managed by the Software

If you do not want Unleashed Multi-Site Manager to manage a device(s), you can delete it. You can delete one or more devices at a time.

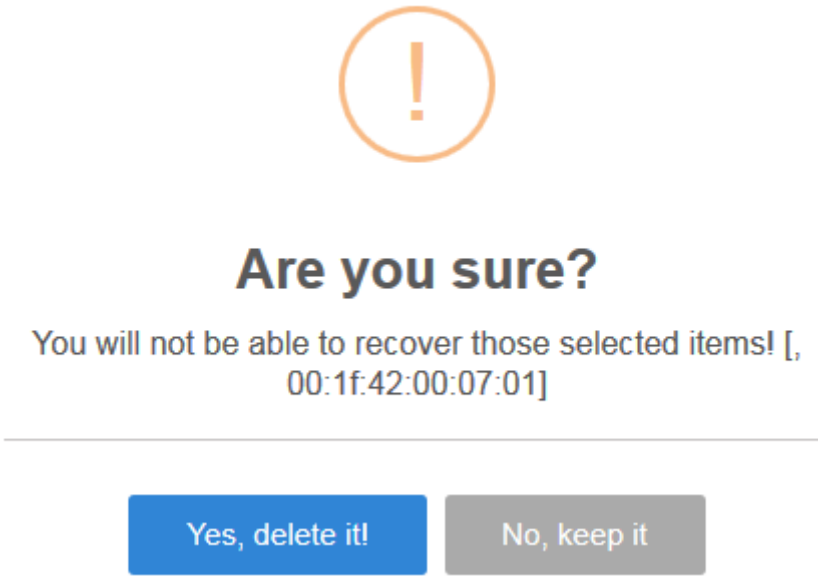
1. After you to login to the Web interface, select **ZDs & Unleashed** from the menu in the left.

   The **ZDs & Unleashed** page appears listing all the devices managed by the software.

2. From the list of devices, select the device or set of devices you want to delete, and then click **More** > **Delete**.

   A confirmation message appears asking if you want to delete the device(s) from Unleashed Multi-Site Manager.

   FIGURE 22 Delete screen



3. Click **Yes, delete it!**.

   The device(s) is deleted, and the software no longer manages it.

Monitoring Events and Network Activities

About the Monitor Page

The **Monitor** page allows you to view events that have occurred on the software and managed devices, and to configure alert notifications for connectivity issues that occur on various device views. It also provides SpeedFlex, which you can use to measure the throughput from one device to another, and to view basic information about a specific client.

About User Customized Alarms

The operator can define customized threshold crossing alarms (alerts) for various events crossing operator-defined thresholds. These alarms can be sent as SNMP traps to SNMP servers, and/or via an email to a group or user, and/or to a syslog event. Refer to Configuring Alarm Settings on page 56 for configuration instructions.

Setting user customized alerts requires defining two thresholds per event type, and then activating the corresponding alarms for the event type.

For instance, if the event type is *AP # of clients* and the thresholds are 100 and 200 clients, then Unleashed Multi-Site Manager can send alarms:

- When the client count goes up to 100 (send *low-threshold alarm set TCA*)
- When the client count goes up to 200 (send *high-threshold alarm set* TCA)
- When the client count goes down to 200 (send *high-threshold alarm clear* TCA)
- When the client count goes down to 100 (send *low-threshold alarm clear* TCA)

NOTE

For any alarms to be sent, the SNMP server information and/or email system information must be configured as described in Configuring Alarm Settings on page 56 before Unleashed Multi-Site Manager can send the alarms.

Available Alarm Event Types

- AP *# of channel changes* (number of channel changes in the last hour)
- AP *# of clients* (number of concurrently connected clients)
- AP # of reboot (number of times in the last hour that the AP has rebooted)
- AP *lost connection* (number of hours the AP has been continuously disconnected)
- AP *traffic* (AP traffic, megabytes for the last hour)

- *Unleashed Multi-Site Manager server CPU usage* (Software CPU usage exceeds the threshold X percent 3 times continuously)
- *ZD CPU usage* (ZoneDirector CPU usage exceeds the threshold X percent 3 times continuously)

Monitoring Alarms

Alarms are a type of event that typically warrants your attention. Alarms are generated by managed access points and ZoneDirector devices and the software server.

Alarms vary in severity. The following are the four alarm severity levels in Unleashed Multi-Site Manager (from highest severity to lowest severity):

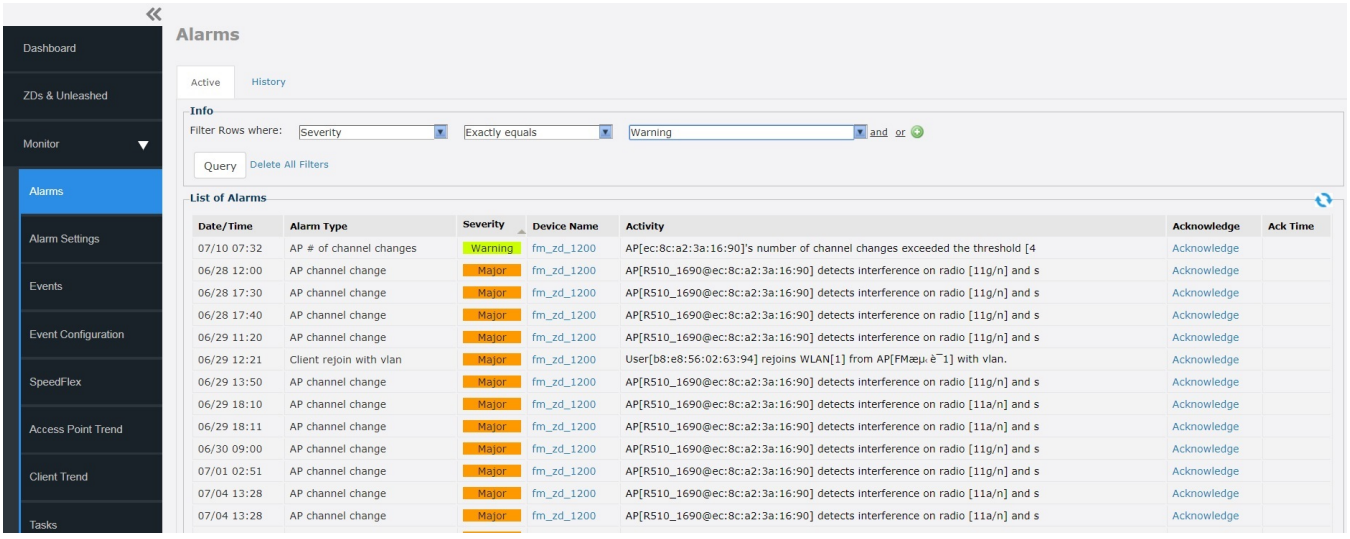
- Critical
- Major
- Minor
- Warning

Viewing and Acknowledging Alarms

Acknowledging an alarm lets other Unleashed Multi-Site Manager administrators know that someone is already looking into the issue.

1. Go to **Monitor** > **Alarms**. The **Active** tab, which lists the most recent alarms, appears by default. The **History** tab displays older alarms that have been acknowledged.

   FIGURE 23 The Alarms page



2. To acknowledge an alarm, click the alarm **Acknowledge** link.

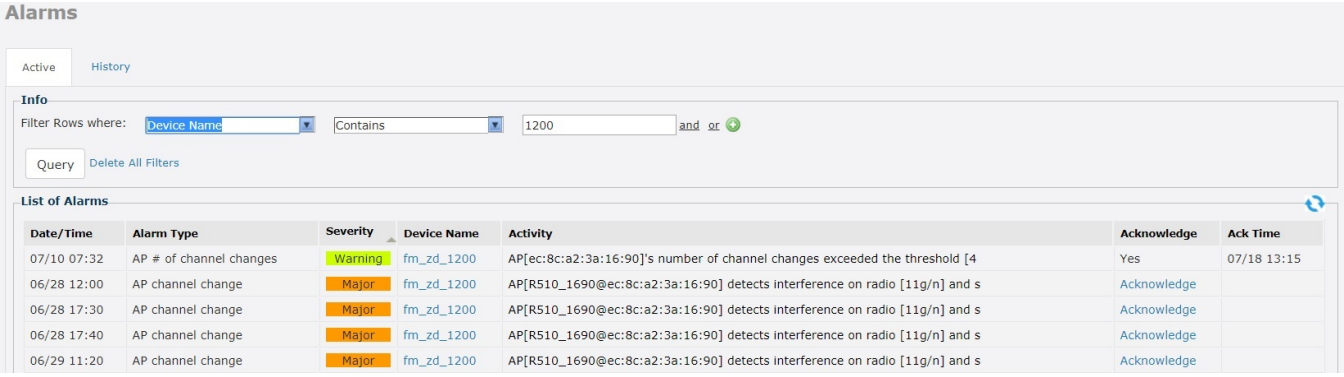
   The software moves the alarm to the **History** tab, the **Acknowledge** column displays `Yes`, and the **Ack Time** column displays the date and time when the alarm was acknowledged.
3. To view other alarms that have already been acknowledged, click the **History** tab.

Filtering Alarms

Use the **Info** section on the **Active** and **History** tabs to filter alarms based on a set of criteria.

1. On either the **Active** or **History** tab, go to the **Info** section. To search for alarms, you need to specify the criteria of the alarms that you want to display.

   FIGURE 24 Creating a filter for ZD 1200 alarms



2. In the first drop-down list box after **Filter Rows where**, select the filter attribute that you want to use. Options include *Date/Time*, *Alarm Type*, *Severity*, *Device Name*, and *Acknowledge* status.
3. In the second drop-down list box, select the filter operator that you want to use. Available filter operators include:
   - *Exactly equals*: Filter alarms with attributes that exactly match the filter parameter you entered. For example, if you selected **Severity** as the attribute and you entered `Critical` as the filter parameter, then only critical alarms appear in the filter results.
   - *Contains* (available only if **Device Name** is selected in the first drop-down list): Filter devices with attributes that include the filter parameter you entered. For example, if you entered `Ruckus` as the **Device Name** filter parameter, then all devices with "ruckus" in the device name (for example, **`ruckus`**`AP` and `AP`**`ruckus`**) appear in the filter results.
   - *Starts with* (available only if **Device Name** is selected in the first drop-down list): Filter devices with attributes that start with the filter parameter you entered. For example, if you entered `Ruckus` as the **Device Name** filter parameter, then only devices with device names that begin with "ruckus" (for example, **`ruckus`**`AP1`, **`ruckus`**`AP2`) appear in the filter results.
   - *Ends with* (available only if **Device Name** is selected in the first drop-down list): Filter devices with attributes that end with the filter parameter you entered. For example, if you entered `AP` as the **Device Name** filter parameter, then only devices with device names that end in "AP" (for example, `ruck- us`**`AP`**, `lobby`**`AP`**) appear in the filter results.
   - *Later than or Earlier than* (available only if **Date/Time** is selected in the first drop-down list): Filter alarms based on the specified date and time.

   After you select a filter operator, a third (text) box appears.
4. In the text box, type the filter parameter that you want to use with the attribute and operator that you selected. The required filter parameter depends on the attribute that you selected in the first drop-down list box.
   - If you selected **Date/Time**, then select a date and time in the text box.
   - If you selected **Alarm Type**, then select a specific alarm that you want to filter.
   - If you selected **Severity**, then select a severity level (Warning, Minor, Major, Critical) that you want to filter.
   - If you selected **Device Name**, then type the partial or full string of the device name that you want to filter.
   - If you selected **Acknowledge**, then select the acknowledgment status (No, Yes, Recovered, Duplicate) that you want to filter.

5. If you want to add another filter, then click . A second filter layer appears below the first. Complete the filter options as in the first filter. You can add up to three additional filters.
6. When you complete setting up the search filters, click **Query**.

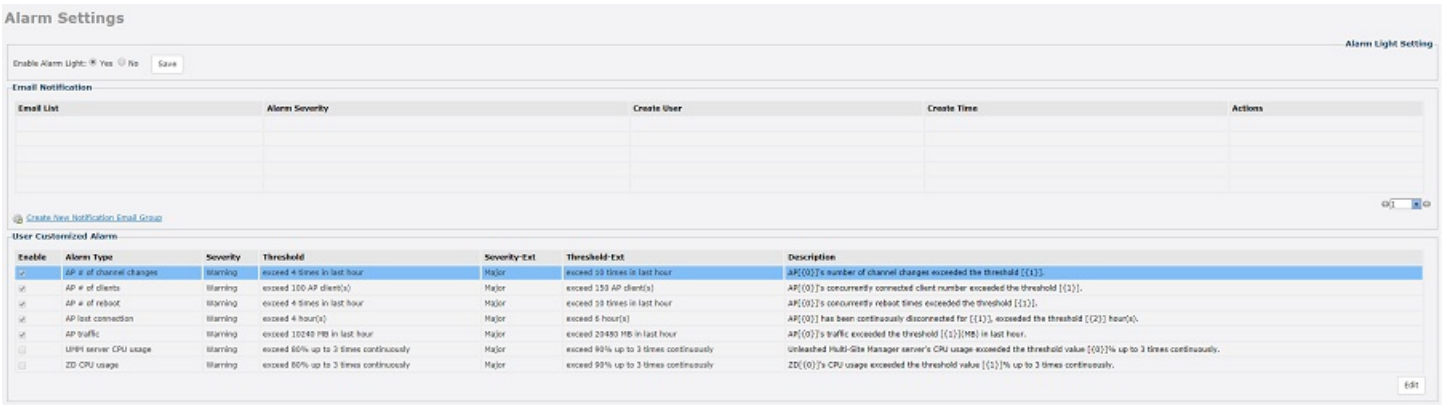
   The software displays the alarms that match the filter criteria.

You have completed filtering alarms.

Alarm Settings

The **Alarms Settings** page allows you to configure email notification for user defined alarms, edit user defined alarms and events. These functionalities are captured under three sections, namely **Email Notification**, **User Customized Alarm** and **Event Selection**.

FIGURE 25 Alarm Settings



The **Email Notification** section displays the users and their respective email addresses to which email notification are send when alarms are generated. The section also displays the severity level of those alarms which you have opted to be notified to each user along with the time when each user was created to receive the notification.

All the available user defined alarms are displayed under the **User Customized Alarm** section.

The **Event Selection** section displays all the events which triggers the alarm. These events are categorized under the following five tabs.

- System Admin
- Mesh
- Configuration
- Client
- AP Admin
- Performance

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), select **Yes**.
   - To disable the alarm lights, select **No**.

   Click the **Save** button in the **Enable Alarm Light** section.
3. In the **Email Notification** section, configure the email alarm groups, including email addresses to which alarm notifications are sent and alarm severities.
   - To create a new email notification, click **Create New Notification Email Group** link under the **Email Notification** section and then:
     - In **Severity Criteria**, select the check boxes for the alarm severity that you want to send notifications for: options include *All*, *Critical*, *Major*, *Minor* and *Warning*.
     - Enter the email addresses to send notifications to; use a semi-colon (;) to separate multiple email addresses.

     NOTE
     To edit an existing email notification entry, in **Email Addresses**, click **Edit** and then in **Severity Criteria**, select the check boxes for the alarm severity for which you want to send notifications: options include *All*, *Critical*, *Major*, *Minor* and *Warning*. Also enter the email addresses to send notifications to; use a semi-colon (;) to separate multiple email addresses. Click the **Save** button in the Email Notification section the changes.
4. From the **Select Zone Director** tab, select the device to be monitored from the list so that email notifications are sent for the alarms generated for these devices and click **Save**.
5. From the **Select Alarm Type** tab, select the alarm types which you want to generate for the selected devices and click **Save**.
6. Click **Edit** and then configure the alarm types in the **User Customized Alarm** section by assigning a severity level and setting a threshold value to each alarm type.

   Among others, these alarms include:
   - *AP # of channel changes*: Triggered when the number of channel changes per AP crosses either of the specified thresholds.
   - *AP # of clients*: Triggered when the number of clients per AP crosses either of the specified thresholds.
   - *AP # of reboot*: Triggered when the number of reboots per AP crosses either of the specified thresholds.
   - *AP lost connection*: Triggered when an AP is continuously disconnected for the either of the specified thresholds (numbers of hours).
   - *AP traffic*: Triggered when traffic on an AP crosses either of the specified thresholds (traffic in MB).
   - *Unleashed Multi-Site Manager server CPU usage*: Triggered when CPU usage on Unleashed Multi-Site Manager crosses either of the specified thresholds (CPU usage percentage).
   - *ZD CPU usage*: Triggered when CPU usage on a ZoneDirector crosses either of the specified thresholds (CPU usage percentage).

   Click the **Save** button in the User Customized Alarm section.

7. Configure the **Event Selection** section by selecting (enabling) events that trigger alarms.

   Events are categorized into the following tabs:

   - *System Admin*
   - *Mesh*
   - *Configuration*
   - *Client*
   - *AP Admin*
   - *Performance*
8. Select each tab under the **Event Selection** section, 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.
9. Then click the **Save** button in the **Event Selection** section.

You have completed configuring the alarm settings.

Monitoring Events

Unleashed Multi-Site Manager keeps a record of all events that occur on the server and managed ZoneDirector devices.

The Events section displays system events that have been reported by the managed Ruckus devices. The **List of Events** table columns include:

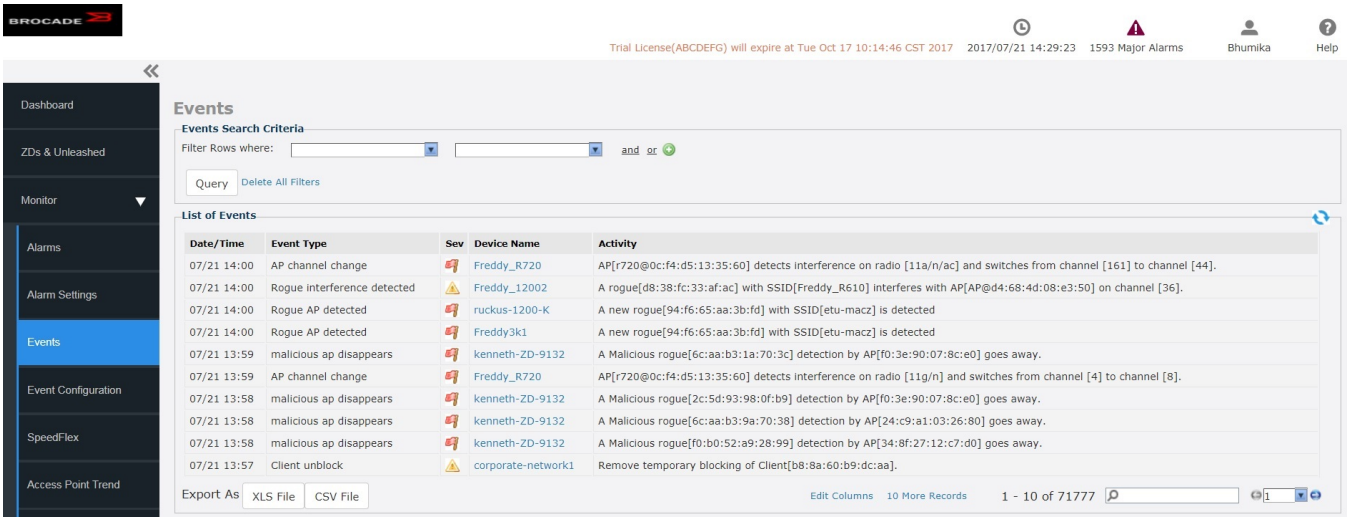
- **Date/Time**: When the event occurred.
- **Event Type**: Ruckus designated event title.
- **Sev**: Severity of the event.
- **Device Name**: Name of the device.
- **Activity**: A description of the event.

Search Using the Events Search Criteria

NOTE
When you save your query parameters as a view, any new events that occur after you create the view and meet the query criteria are automatically added to the saved view.

1. Go to **Monitor** > **Events**.

FIGURE 26 Using Search Criteria to search for an event



2. Look for the **Events Search Criteria** section. To search for events, you need to specify the criteria of the devices that you are looking for.
3. In the first drop-down list box after **Filter Rows** where, select the search attribute that you want to use. Options include *Date/Time*, *Event Type*, *Sev(erity)* and *Device Name.*
4. In the second drop-down list box, select the search operator that you want to use. Available search operators include:
   - *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **Model** as the attribute and you entered `ZD3250` as the search parameter, then only devices of this model appear in the search results.
   - *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered `100` as the search parameter, then all devices with "100" in the serial number (for example, **100**903000031 and 11090**100**0282) appear in the search results.
   - *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered `3208` as the query parameter, then only devices with serial numbers that begin with "3208" (for example, 320833000219) appear in the search results.
   - *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered `011` as the query parameter, then only devices with model names that end in "001" (for example, 100903000**001**) appear in the search results.
   - *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 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 **and** or **or**, and then click . A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.
7. When you complete setting up the search filters, click **Query**. The software displays the devices that match the search criteria.

Search Using the Search Box

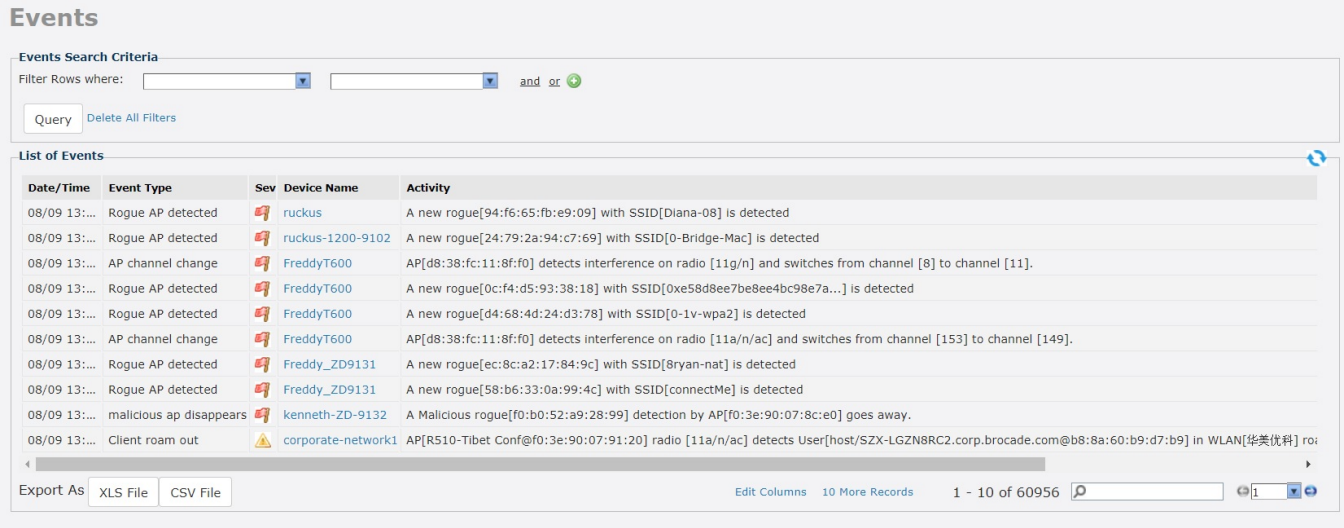
A search box exists at the bottom right area of the **List of Events** section. You can use this search box to search for events that have occurred on Unleashed Multi-Site Manager or any of the managed devices.

NOTE
When you save your query parameters as a view, any new events that occur after you create the view and meet the query criteria are automatically added to the saved view.

1. Type a search string into the box.

   The search string could be a partial or full string and can consist of numbers or letters or a combination of both.

FIGURE 27 The device property that matches the search string is highlighted in the search results



2. Press **<Enter>**.

Unleashed Multi-Site Manager 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.

Additional Search 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 download is complete, open the file and use**Save As** option to save the XSL file to the desired location.

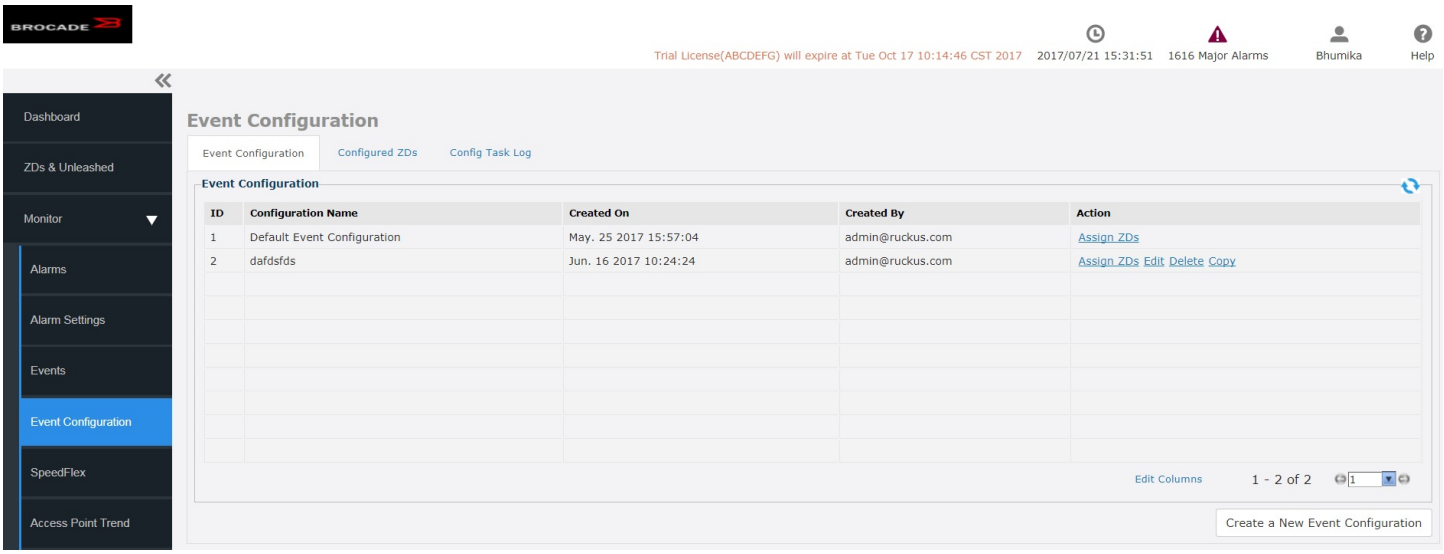
- Save the search results as CSV (comma-separated value file): In **Export As**, click **CSV File**. When the download is complete, use the **Save As** option to save the CSV file to the desired location.

Event Configuration

This page displays the configured events, configured ZDs and configured task logs.

> **NOTE**
> Events can be configured only for ZD. Unleashed does not support event configuration.

FIGURE 28 Event Configuration



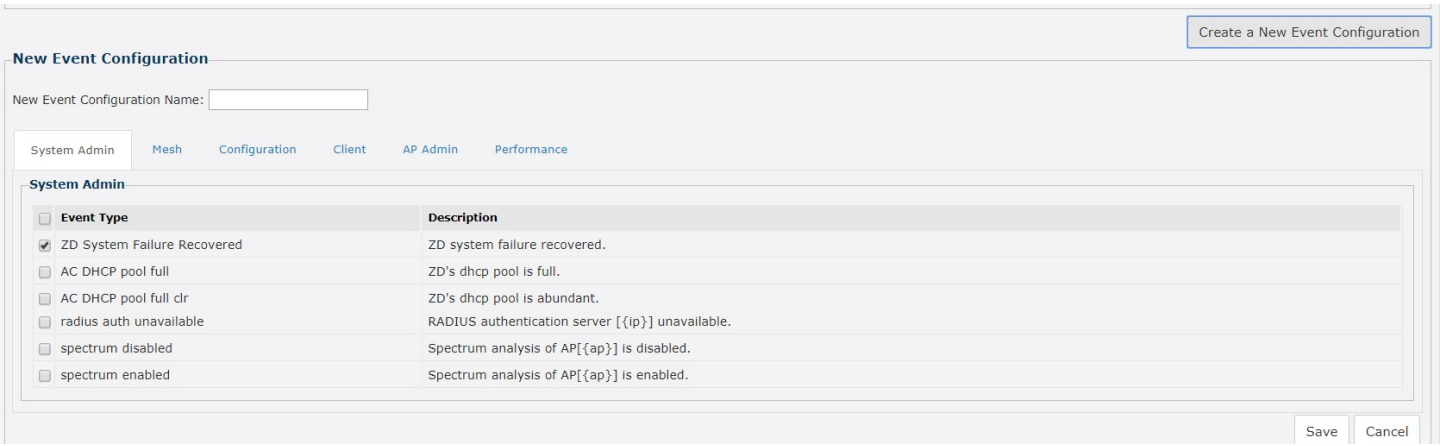
The **Event Configuration** tab list all the configured events. The **Configured ZDs** tab displays all existing Zone Director devices. You can filter the displayed out put based on the selection you make from the **Select a ZD view** drop-down. This can be further filtered by creating a raw based filter query based on IP Address, IPV6 Address, Controller name, Model, and Serial Number.

Multiple filter queries can be clubbed by clicking the "+" sign against each query row. Once all your filter queries are entered, click te **Query** button on the bottem right corner of the page to run the query and fetch the result. The result is displayed in the **List of ZDs** section.

FIGURE 29 Filtering Configured ZDs

To create a new event configuration, click the **Create a New Event Configuration** button. The poge gets refreshed to display the **New Event Configuration** section.

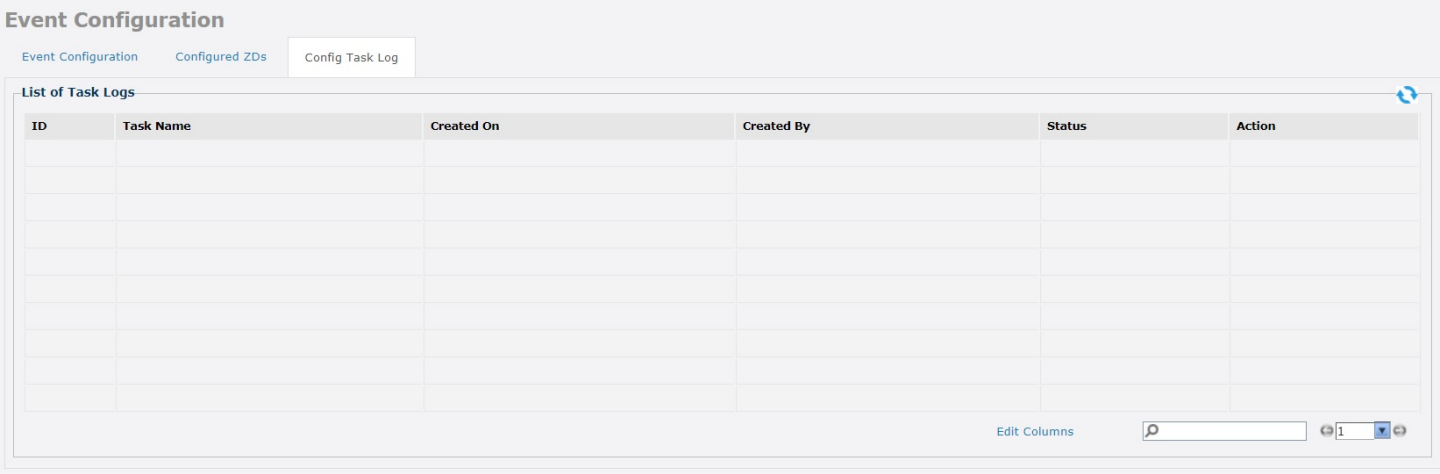
FIGURE 30 New Event Configuration



Enter a name for the configuration in the **New Event Configuration Name** text field. All available event types are calcified under the **System Admin**, **Mesh**, **Configuration**, **Client**, **AP Admin** and **Performance** tabs. Make selections as required under these tabs and click the **Save** button on the bottom right corner of the page, to save the new configuration. The newly created configuration will now appear under the **Event Configuration** tab.

The list of task logs are displayed under the **Config Task Log** tab.

FIGURE 31 Task Logs



Measuring Throughput Using SpeedFlex

Unleashed Multi-Site Manager includes a wireless performance tool called SpeedFlex that you can use to measure the downlink and uplink throughput between any of the following devices:

- ZD or Unleashed
- An AP that ZD or Unleashed is managing
- A wireless client that is associated with ZD-managed AP or unleashed-managed AP.

NOTE
When performing a site survey, you can use SpeedFlex to help find the optimum location for APs on the network with respect to user locations.

CAUTION
For SpeedFlex to work, the devices that you are testing must not be behind a NAT server. If one of the devices is behind a NAT server, then the test fails because SpeedFlex is unable to communicate with the device behind the NAT server.

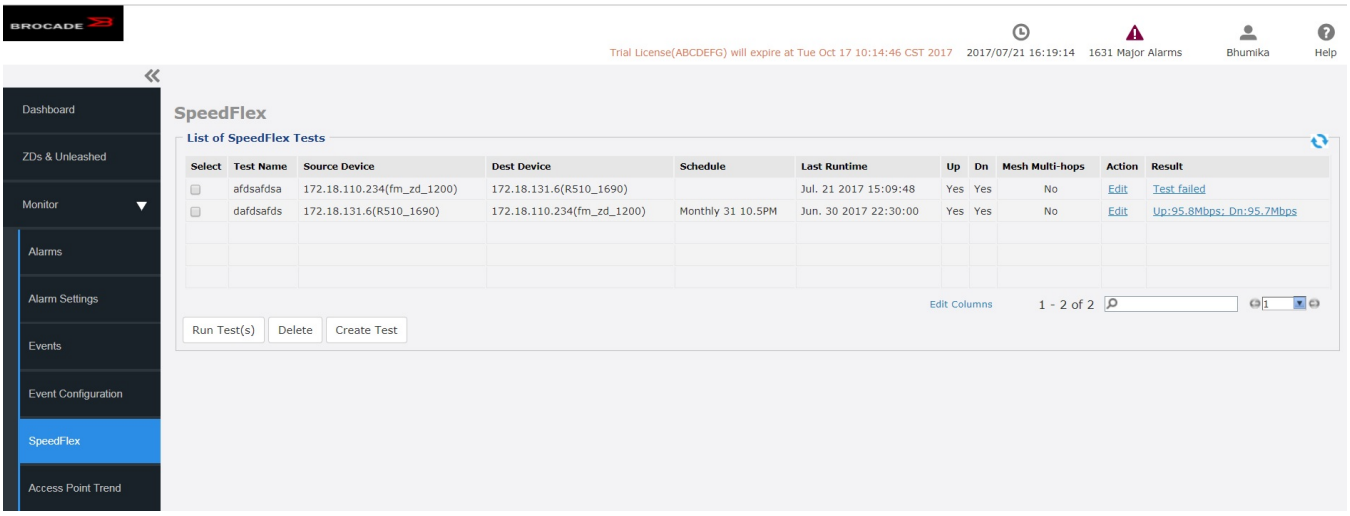
To use SpeedFlex, you must first create a SpeedFlex task to assign the destination and source devices. When you create the task, you can also set it to run based on a recurring schedule.

Creating a SpeedFlex Task

Creating a SpeedFlex task requires that you specify the destination and source devices for running the test.

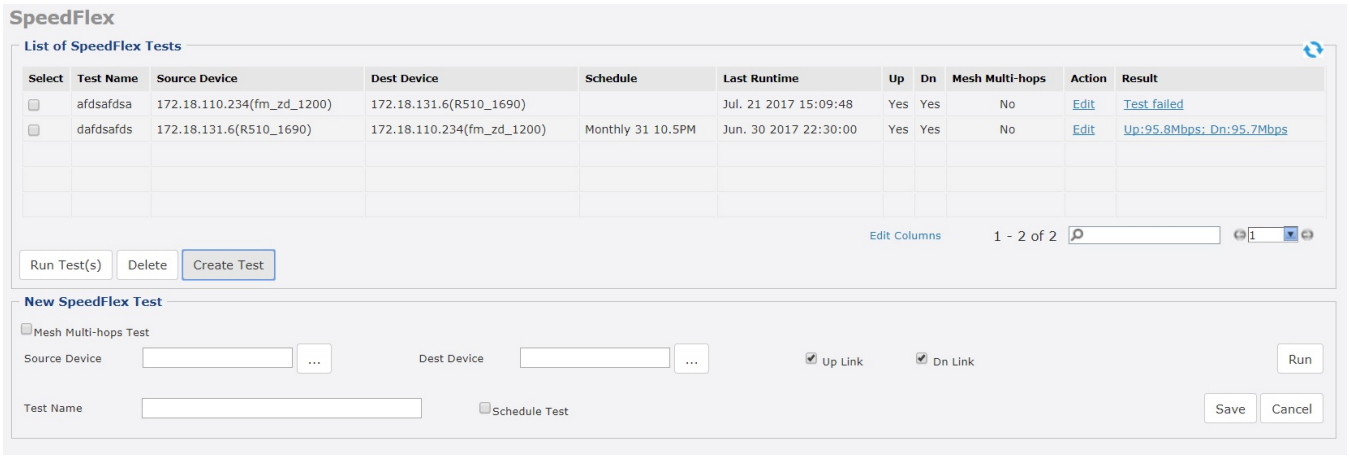
1. Go to **Monitor** > **SpeedFlex**.

FIGURE 32 SpeedFlex Window



2. Click the **Create Test** button.

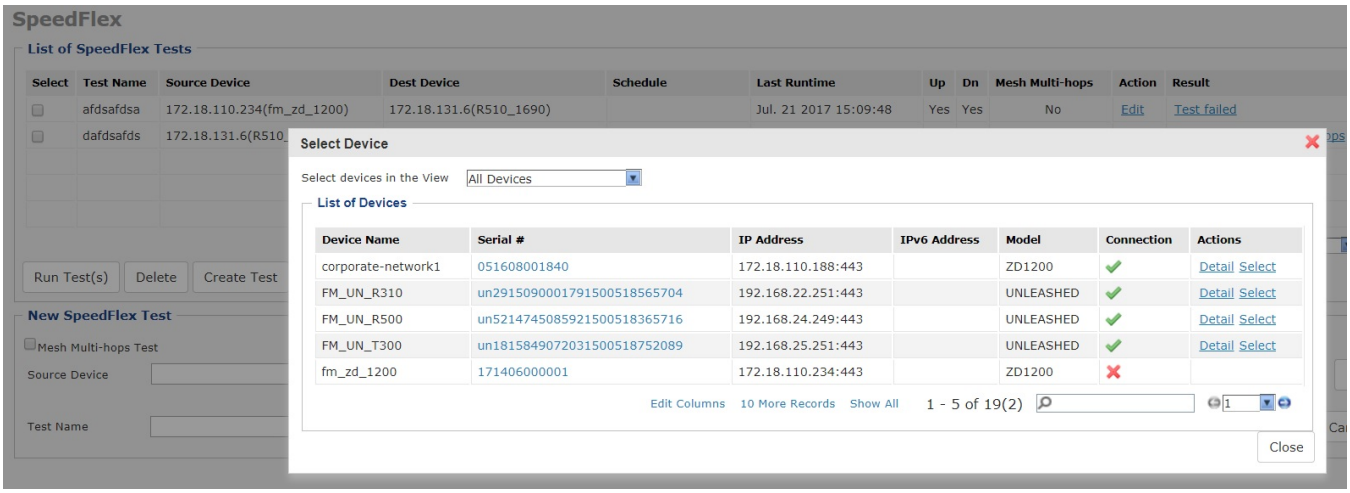
   The **New SpeedFlex Test** form appears.



3. If you want to measure the throughput between hops (devices between the source and destination devices) in a mesh topology, then select the **Mesh Multi- hops Test** check box. If you want to measure the throughput between the source and destination devices only, then make sure that the **Mesh Multi-hops Test** check box is clear.

4. In **Source Device**, click the button with the ellipsis (...). The **Select Device** window appears.

FIGURE 33 Select Device



a) In **Select devices in the View**, select the device view to which the source device belongs.

The **List of Devices** table refreshes, and displays the devices that belong to the selected view.

b) Look for the device that you want to assign as the source device, and then click the **Select** link (in the **Actions** column) that is in the same row as the device name. The software returns you to the **Monitor** > **SpeedFlex** window.

> NOTE
> You can only run SpeedFlex tests on devices that support the SpeedFlex feature and that are currently online. If the **Select** link does not appear in the same row as a particular device, then that device may be offline (check the **Connection** column) or may not support the SpeedFlex feature.

5. In **Dest Device**, repeat the steps your performed in Step 4, but this time, select the destination device.
6. Specify the traffic direction (uplink and downlink) for which you want to perform the throughput test. By default, both **Up Link** and **Dn Link** check boxes are selected, which means that Unleashed Multi-Site Manager tests the throughput for both directions.

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

7. In **Test Name**, type a name that you want to use for this SpeedFlex test.

After you save this test, it appears in the **List of SpeedFlex Tests** with the test name that you assigned.

8. If you want this test to run automatically based on a recurring schedule, then do the following:
   a) Select the **Schedule Test** check box. The **Schedule** form appears below.
   b) In **Frequency**, select how often you want this test to run.
   c) In **Time of Day**, select the time when this test runs.
   d) In **Email report to**, type the email address to which the SpeedFlex test results are sent. When you want to send the report to multiple email addresses, use a comma (,) or semicolon (;) to separate the email addresses.
9. Click **Save**.

The **List of SpeedFlex Tests** table refreshes, and then the test that you created appears in the table.

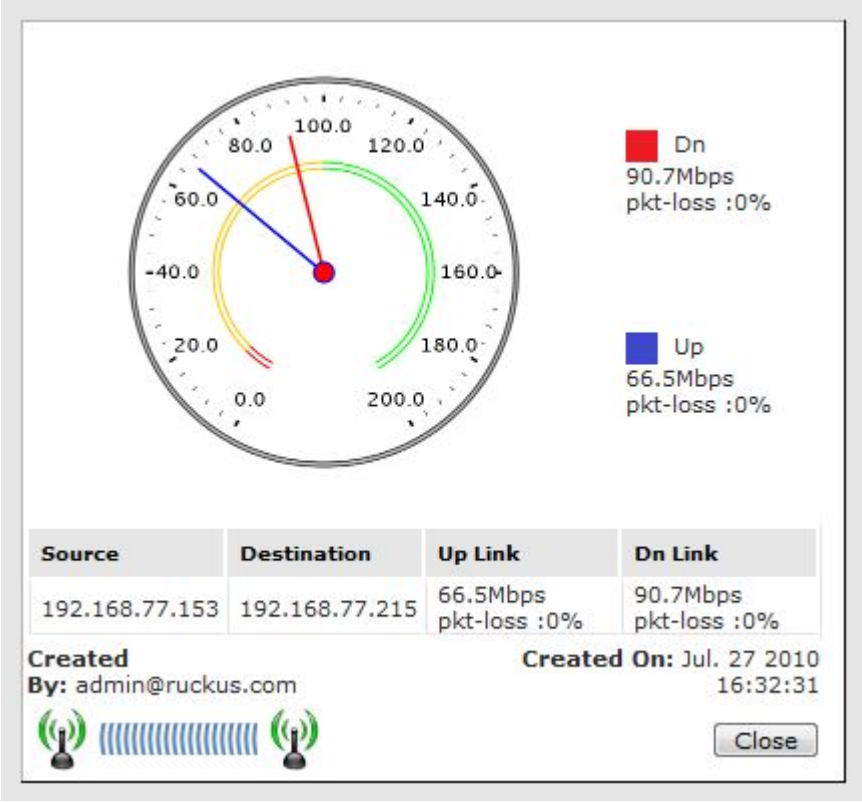
Running a SpeedFlex Task

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

1. Go to **Monitor** > **SpeedFlex**.
2. In **List of SpeedFlex Tests**, select the check box for the SpeedFlex test that you want to run. When you want to run multiple tests at the same time, select the check boxes for all the SpeedFlex tests that you want to run.
3. Click **Run Test(s)**. The SpeedFlex **Performance Test** window appears and displays a speedometer that indicates the downlink and uplink throughput detected by Unleashed Multi-Site Manager. When both downlink and uplink throughput values appear, the SpeedFlex test is complete.

   If you selected multiple SpeedFlex tests to run, then the software runs the tests sequentially and shows all test results on the same page.

FIGURE 34 SpeedFlex test result sample



Editing a SpeedFlex Test

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

1. In **List of SpeedFlex Tests**, look for the SpeedFlex test that you want to edit.
2. Click the **Edit** link that is in the same row as the test name.

   The **New SpeedFlex Test form** appears below.
3. Edit the test details as required.

4. Click **Save**.

Deleting a SpeedFlex Test

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

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

   You can select more than one test name to delete at the same time.
3. Click **Delete**.

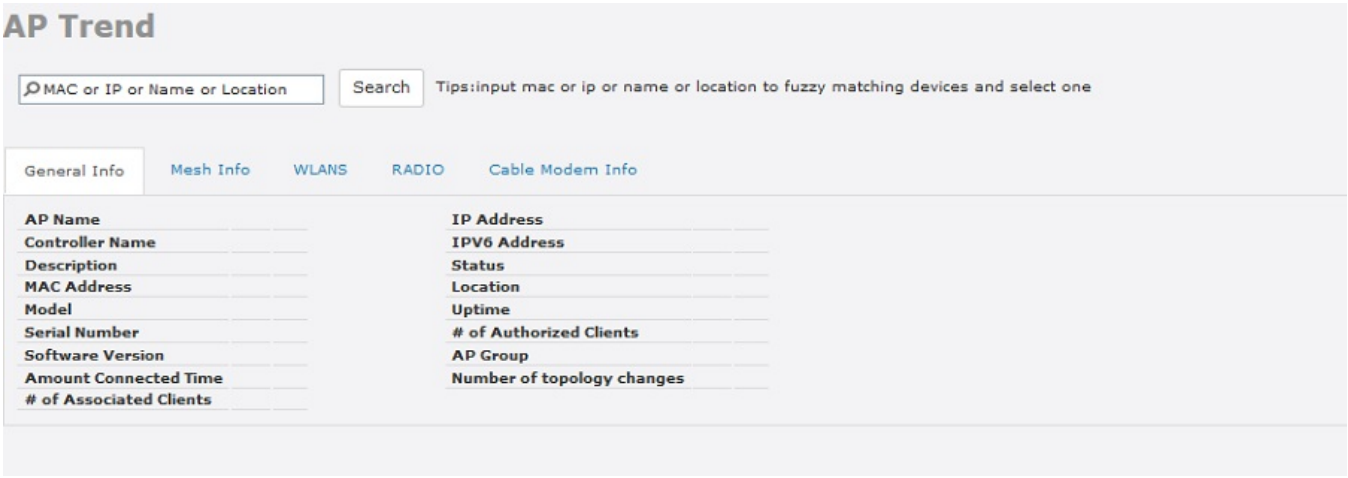
The **List of SpeedFlex Tests** refreshes, and then the SpeedFlex test that you deleted disappears from the list.

Monitoring Access Point Trends

The **Access Point Trend** page on the **Monitor** tab allows you to display basic information about a Ruckus AP. You need to know the AP's MAC address to be able to run a query on it.

1. Go to the **Monitor** > **AP Trend** page.

FIGURE 35 Access Point Trend



2. In the text box, type the AP MAC address, IP address, name or location, and then select the AP from the list. Click **Search**. The software displays the AP's basic information under four or five tabs:
   - **General Info**: The name and other information about the AP.
   - **Mesh Info**: The mesh type and other information about this AP, when the AP is part of a mesh network.
   - **WLANs**: The Name/ESSID of WLANs, and other information about this AP.
   - **Radio**: The Current Channel used by this AP's radio.
   - **Cable Modem Info**: When the AP is equipped with an integral cable modem (for instance, ZF7761-CM or ZF7781-CM), clicking this tab takes you to a cable modem Trends page.

3. To display trending graphs for the AP:
   a) Select a **Sampling Period**.
   b) Click **Generate Graphs**.

      The software displays the AP's trends information at the bottom of the page:

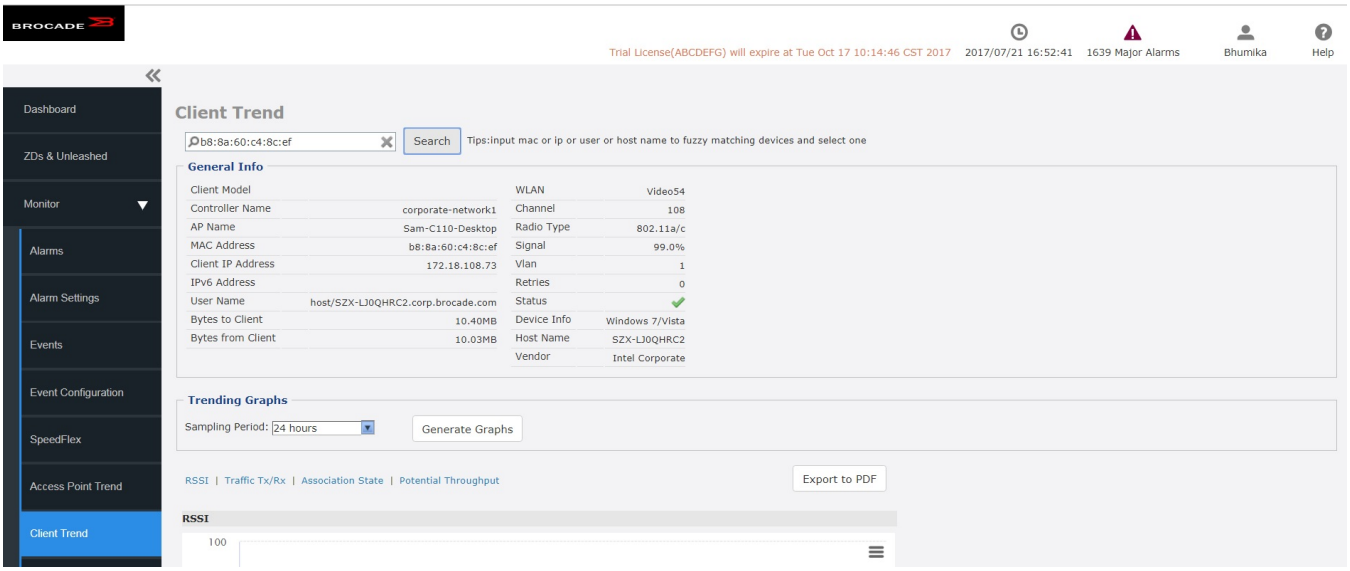
      - Associated Clients
      - Traffic Tx and Rx
      - Association State
4. To save AP trending graphs:
   a) Click **Export to PDF**.
   b) The software prints the information on the screen to a PDF file on your workstation.

Monitoring Client Trends

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

1. Go to the **Monitor** > **Client Trend** page.
2. In the text box, type the MAC address, IP address, user name or host name of the client which you want to query for basic information.

FIGURE 36 Client Trend



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.
   - *Client IP Address*: The IP address assigned to the client.
   - *WLAN*: The SSID or wireless network name with which the client is associated.
   - *Channel*: The wireless channel used by the WLAN.
   - *Radio Type*: The wireless radio used by the WLAN.
   - *Signal*: The RSSI strength of the WLAN.
   - *Status*:
     – A green check mark indicates that the client is currently connected
     – A red cross mark indicates that is it disconnected.

     .

4. To display trending graphs for the client:

   a) Select a **Sampling Period**.

   b) Click **Generate Graphs**.

   The software displays the client's trends information at the bottom of the page:

   - RSSI
   - Traffic
   - Association State

     NOTE
     This is applicable only for ZD. For Unleashed, it is not supported.

   - Potential Throughput

5. To save client trending graphs, Click **Export to PDF.**

   The software prints the information on the screen to a PDF file on your workstation.

Working with Reports

Available Report Types

The following table lists the different report types that you can generate in Unleashed Multi-Site Manager. For instructions on how to generate each type of report, refer to the succeeding sections.

TABLE 6 Available reports in the software

Report Name	Description
Device View	View current status of controller, AP and clients.
Historical Connectivity	View the connection statuses of managed devices at different periods.
Client Association	View the connected client at different periods.
SSID Report	View the number of 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.
Capacity	Displays device capacity data based on associated clients and traffic, among others.
SLA	Displays SLA related information, including connection time, and potential throughput.
Troubleshooting	Generate various graphs that are useful for troubleshooting, including number of child APs, number of Hops, Mesh RSSI, and number of Reboot.
Resource Monitor	View CPU, memory, and disk usage on ZoneDirector devices. NOTE This is applicable only for ZD. Unleashed does not support this report.
PCI Report	Display SSID and rogue AP information.

Hiding and Showing Columns in Reports

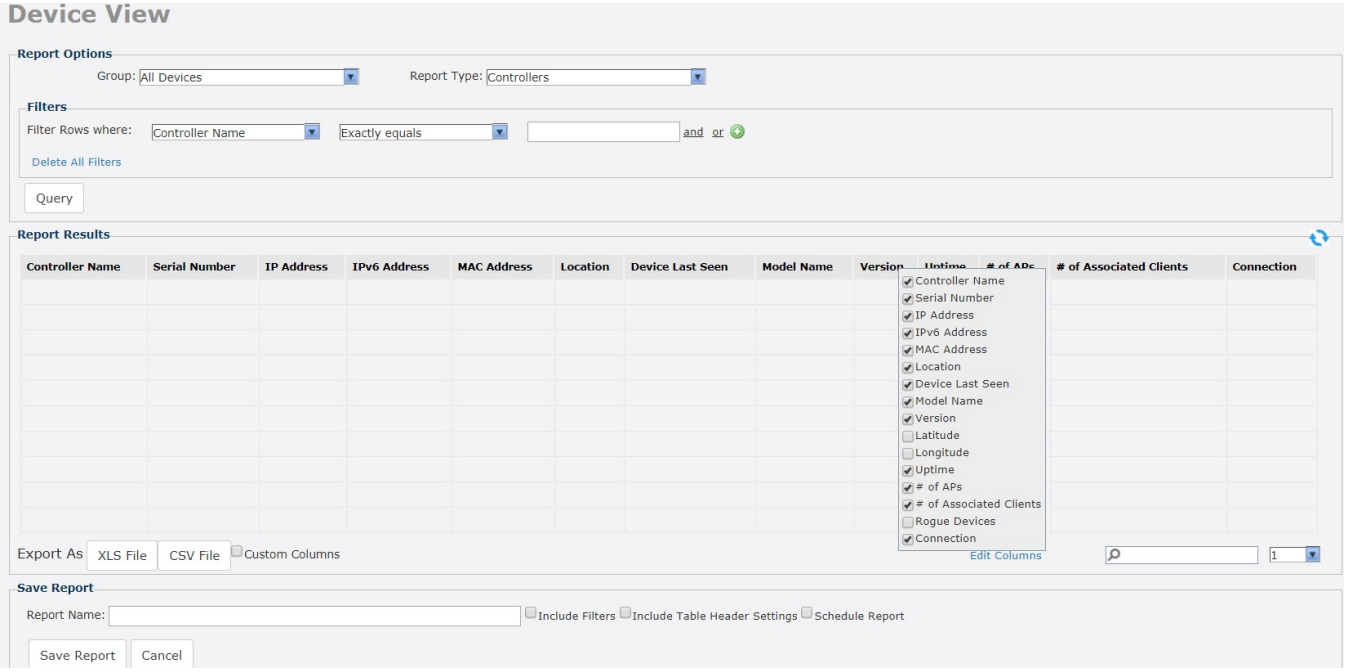
By default, all columns that are available for a particular report are displayed. When you want the report to show only specific columns, you can hide the columns that you do not want to display.

1. Right-click any of the column headings in the report that you have generated.

   A pop-up menu appears, displaying all the column headings that are available for that particular report.

2. Clear the check boxes for the column headings that you want to hide. As soon as you clear a check box, the corresponding column disappears from the report.

FIGURE 37 Clear the check boxes for the columns that you want to hide



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.
4. 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.

Generating a Device View Report

A device view report includes device information such as, connected and disconnected devices and APs, and connected wireless clients.

1. Go to **Reports** > **Device View**.
2. In **Device View**, select the group for which you want to generate a report.

   Options include:

   - All devices
   - Specified device

3. Select one of the following options in **Report Type**:
   - *Controllers*: Shows all controllers.
   - *All Access Points*: Shows all ZoneDirector-managed APs.

     Also select:

     – *AP Type*: *APs*, *Root APs*, *Mesh APs*, or *eMesh APs*, and
     – *Period* (for the report): between *1 hour* and *24 hours*, or *Greater than 24 hours*.
   - *Connected Clients*: Shows all currently-connected ZD and Unleashed managed clients.
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 *controller name*, *AP name*, *AP serial number*, *Description*, *Location*, *Model name*, *AP IPv6 address* and others.

   b) In the second drop-down list box, select the search operator that you want to use. Available search operators include:
      - *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered **`172.17.16.176`** as the search parameter, then only devices with this IP address appear in the search results.
      - *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered **`100`** as the search parameter, then all devices with "100" in the IP address (for example, `172.17.16.`**`100`** and **`100`**`.1.10.13`) appear in the search results.
      - *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered **`3908`** as the query parameter, then only devices with serial numbers that begin with "3908" (for example, `390801005202`) appear in the search results.
      - *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected **IP address** as the attribute and you entered **`13`** as the query parameter, then only devices with model names that end in "13" (for example, `100.1.10.`**`13`**) appear in the search results.

   c) In the third text box, type the search parameter that you want to use with attribute and operator that you selected.

      The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.

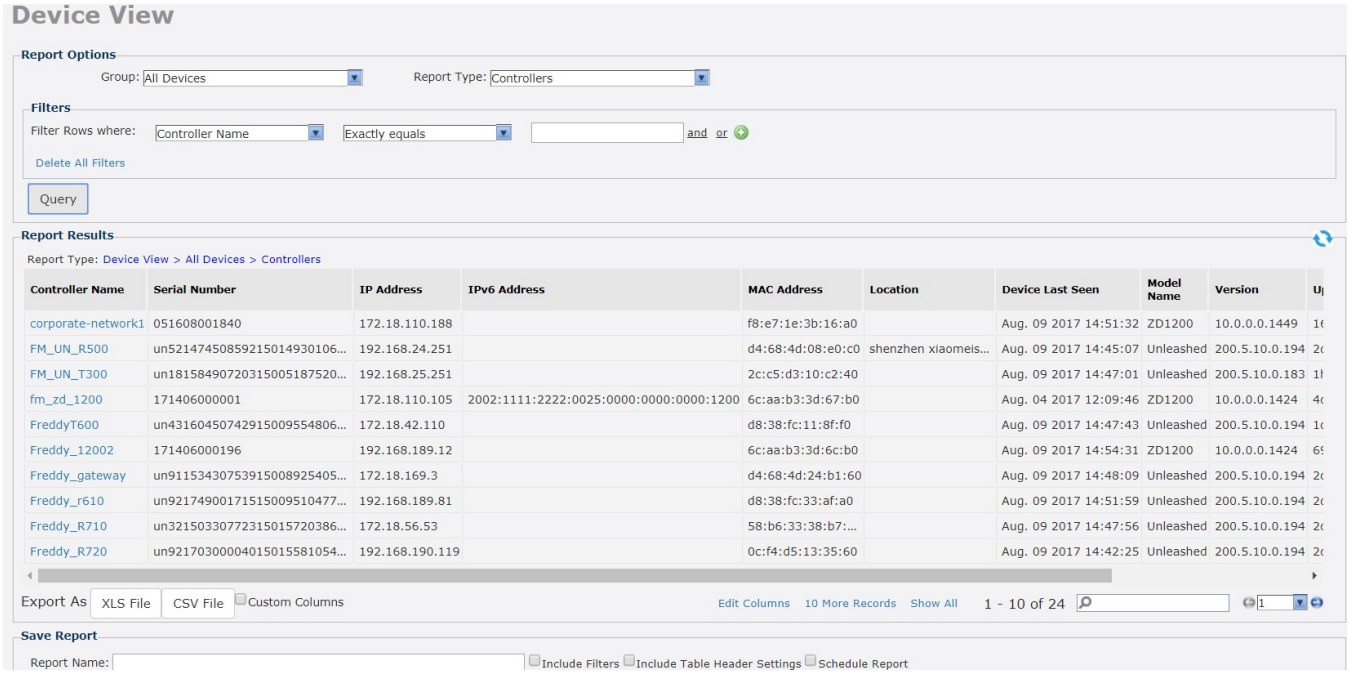
   d) If you want to add another search filter, click **and** or **or**, and then click  .

      A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.

5. Click **Query**. The page refreshes, and then a list of devices that belong to the device view that you specified appears on the page.
   Device details that are shown on the Reports page can include:
   - AP Name
   - Controller Name
   - AP Serial Number
   - AP MAC
   - AP IP Address
   - AP IPv6 Address
   - Model Name
   - Last Seen
   - Connection
   - Connection Mode
   - Radio/Channel/Mode
   - Max Number of Associated Clients
   - Min Number of Associated Clients
   - Mesh Uplink RSSI
   - Mesh Downlink RSSI
   - Details

     NOTE
     In any device view report, if you click an **AP MAC** Address hyperlink, then the software displays the **ZoneDirector** > **Monitor** > **Access Point Trend** window. Refer to Monitoring Access Point Trends on page 67.
     If you click a **Client MAC** address hyperlink, then the software displays the **ZoneDirector** > **Monitor** > **Currently Active Clients** screen in another window. The **Currently Active Clients** screen includes the OS or Type (if known), the authorization method, the WLAN and VLAN used, the client IP address, and the AP MAC address, among others.

FIGURE 38 A sample device view report

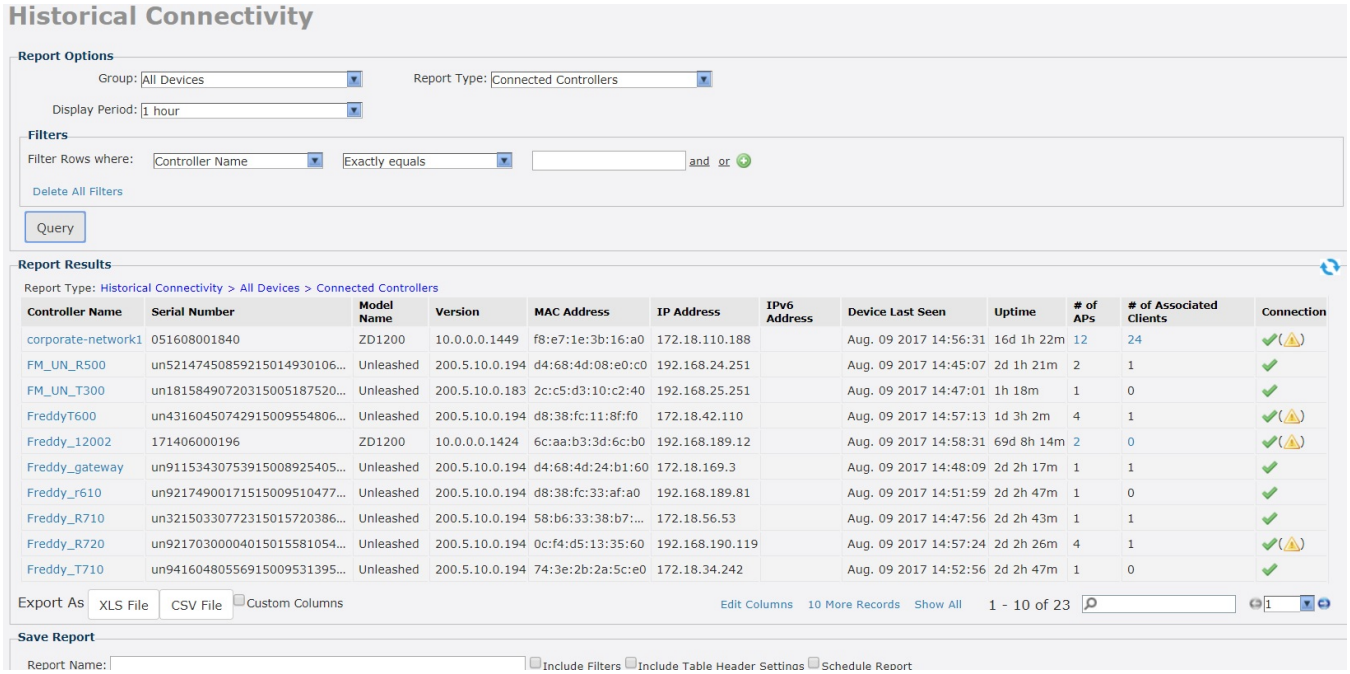


Generating a Historical Connectivity Report

A historical connectivity report allows you to view the connection statuses of managed devices at different periods.

1. Go to **Reports** > **Historical Connectivity**.

FIGURE 39 Sample historical connectivity report



2. In **Group**, select the device view for which you want to generate a report.

   Default device views include:

   - All devices
   - Specified device

3. In **Report Type**, configure the type of report that you want to view:
   - Select one of the following options in **Report Type:**
     - *Connected Controllers*: Shows all controller devices that communicated with Unleashed Multi-Site Manager at the last inform interval
     - *Disconnected Controllers*: Shows all controller devices that did not communicate with Unleashed Multi-Site Manager 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.
4. In *Display Period*, select the report interval from 1 hour to 31 days, or for an operator-selected date range.

5. (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 *Controller Name*, *Serial Number*, *IP address*, *Model Name*, *Device Last Seen*, and others.

   b) In the second drop-down list box, select the search operator that you want to use. Available search operators include:
      - *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered **`172.17.16.176`** as the search parameter, then only devices with this IP address appear in the search results.
      - *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered **`100`** as the search parameter, then all devices with "100" in the IP address (for example, 172.17.16.**100** and **100**.1.10.13) appear in the search results.
      - *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered **`3908`** as the query parameter, then only devices with serial numbers that begin with "3908" (for example, 390801005202) appear in the search results.
      - *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected IP address as the attribute and you entered **`13`** as the query parameter, then only devices with model names that end in "13" (for example, `100.1.10.`**`13`**) appear in the search results.

   c) In the third text box, type the search parameter that you want to use with attribute and operator that you selected.

      The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.

   d) If you want to add another search filter, click **and** or **or**, and then click  .

      A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.

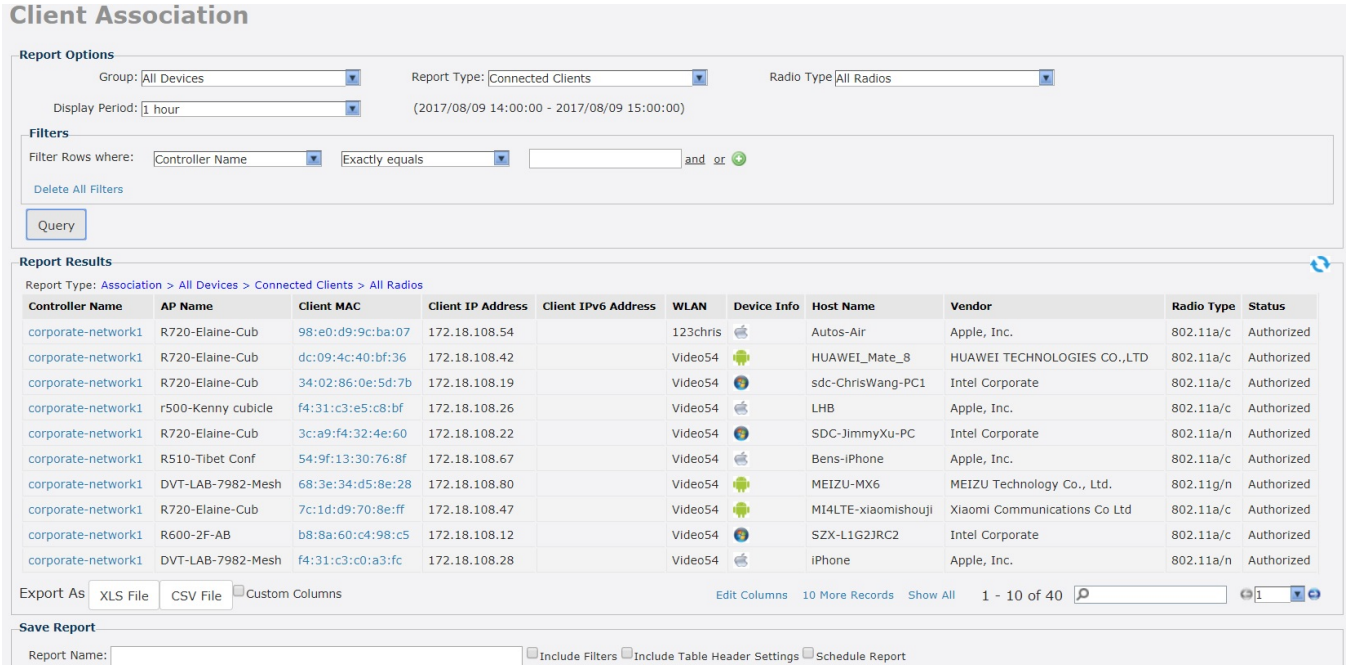
6. Click **Query**. The software displays the requested report results.

Generating a Client Association Report

A client association report identifies the clients that have been associated with managed APs during an operator-defined time.

1. Go to **Reports** > **Client Association**.

FIGURE 40 Sample client association report



2. In **Group**, select the device for which you want to generate a report.

   Default groups include:

   - All Devices
   - Specified device

3. Perform the following:

   a) Select one of the following options in **Radio Type**: *All Radios*, *802.11b/g*, *802.11a/n*, *802.11g/n*, *802.11a/c*, or *802.11a*.

   b) In **Display Period**, select the report interval from 1 hour to 31 days, or for an operator-selected date range.

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 *Controller Name*, *Client IP address*, *AP Name*, and others.
   b) In the second drop-down list box, select the search operator that you want to use.
      Available search operators include:
      - *Exactly equals*: Search for devices with attributes that exactly match the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered **`172.17.16.176`** as the search parameter, then only devices with this IP address appear in the search results.
      - *Contains*: Search for devices with attributes that include the query parameter you entered. For example, if you selected **IP Address** as the attribute and you entered **`100`** as the search parameter, then all devices with "100" in the IP address (for example, `172.17.16.`**`100`** and **`100`**`.1.10.13`) appear in the search results.
      - *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered **`3908`** as the query parameter, then only devices with serial numbers that begin with "3908" (for example, `390801005202`) appear in the search results.
      - *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected **IP address** as the attribute and you entered **`13`** as the query parameter, then only devices with model names that end in "13" (for example, `100.1.10.`**`13`**) appear in the search results.
   c) In the third text box, type the search parameter that you want to use with attribute and operator that you selected.
      The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
   d) If you want to add another search filter, click **and** or **or**, and then click  .
      A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.
5. Click **Query**. The software refreshes the page and displays the report that you selected.

NOTE
The software provides options for filtering the devices that are included in the report. Options for saving the generated report, automating report generation, and saving the report as an Excel file are also available. For more information, refer to Using Advanced Report Options on page 86.

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** > **SSID Report**.
2. In **SSID Report**, select the group for which you want to generate a report.
   The default device view is **All devices**.
   When there are custom device views, they also appear in the list of options.

3. In **Report Type**, configure the type of report that you want to view.

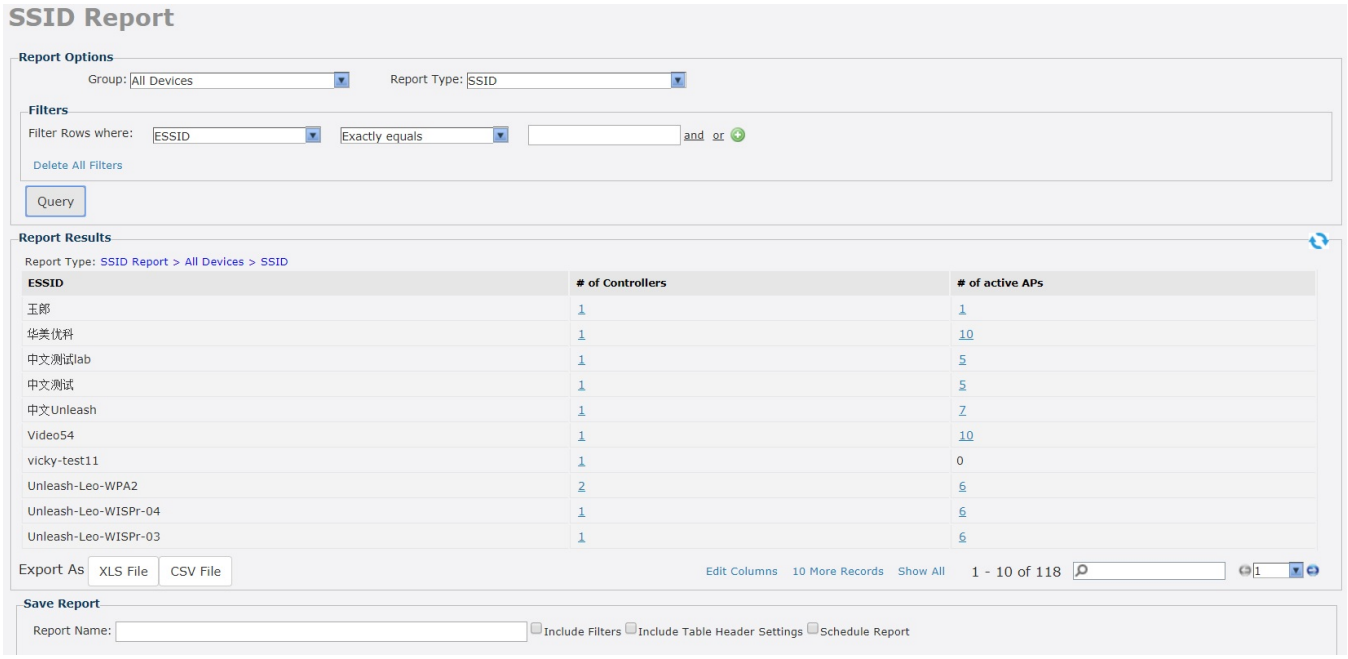
   The available report options depend on the device view that you selected in the previous step.

   - *SSID*: Shows the number of APs that are configured to use a particular SSID and the number of ZoneDirector devices that are managing these APs.
   - *Top Bar-Graph*: Can show the Client's number, Tx traffic or Rx traffic.
   - *Time Line Graph*: Can show the # of Associated Clients, Traffic-Tx+Rx, Traffic- Rx, Peak-Tx or Peak-Rx.

4. Click **Query**. If you selected report type that generates a graph, then click **Generate Graph**. The page refreshes, and then displays the SSID report that you queried or graph that you generated.

   NOTE
   When reading the SSID report, the **Clients** column includes the online and offline clients during the last 15 minutes. The **Tx (Mbytes)** and **Rx (Mbytes)** columns list the number of megabytes transmitted and received during the last 15 minutes, respectively. The **Peak Tx (Mbytes)** and **Peak Rx (Mbytes)** columns list the max number of data + management megabytes transmitted in 10 samples collected during the last 15 minutes (the APs send statistics to the ZD every 90 seconds, and the peaks are the max values of those samples).

FIGURE 41 Sample SSID report



Generating a Capacity Report

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

1. Go to **Reports** > **Capacity.**.

2. In **Group**, select the device view for which you want to generate a report.

   Default device views include:

   - All Devices
   - Specified devices

3. In **Report Type**, select the type of report that you want to generate.

   IThe following report type options appear:

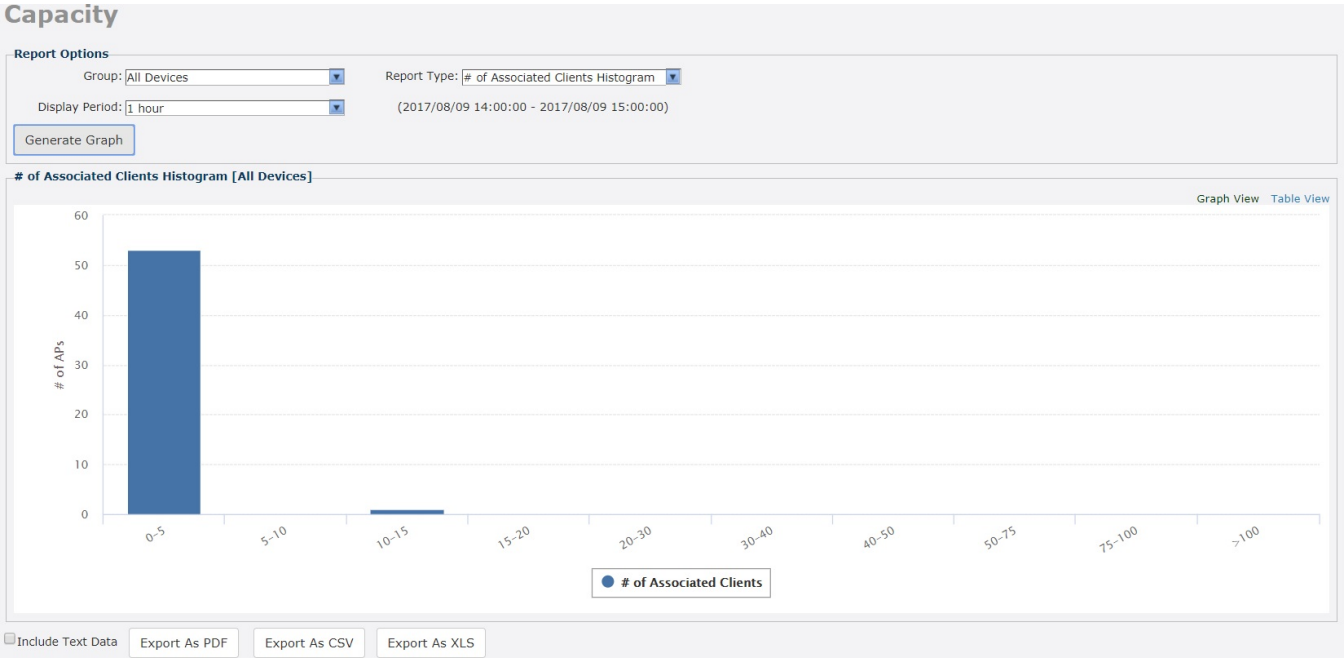
   - *# of Associated Clients Histogram*
   - *AP Traffic -Tx/Rx Histogram*
   - *Client Traffic -Tx/Rx*
   - *Network Capacity*

4. In **Display Period**, select the time period for which you want to generate the report. Options range from 1 hour to 31 days.
5. Click **Generate Graph**.

   The page refreshes and the graph appears.

   To view the report in a tabular format, click **Table View**. To save a PDF version of the report, click **Export As PDF**, and then save the PDF file to your local computer when the browser prompt appears. To save a comma-separated variables version of the report, click **Export As CSV**, and then save the *.csv file to your local computer when the browser prompt appears. To save an Excel version, click **Export As XLS**.

FIGURE 42 A sample capacity report



NOTE

A report bar graph can include both Tx and Rx information on the same report, such as **All Devices** > **AP Traffic - Tx/Rx**. When the report contains Tx and Rx selections at the bottom of the report, you can control whether the Tx and/ or Rx information is displayed. Click the **(TX)** and **(RX)** icons to toggle on and off the Tx and Rx displays, respectively.

Generating an SLA Report

Generate various graphs that display service-level agreement (SLA) related information, including AP connection time, client potential throughput, and client associated time.

1. Go to **Reports** > **SLA**.
2. In **Group**, select the device view for which you want to generate a report.

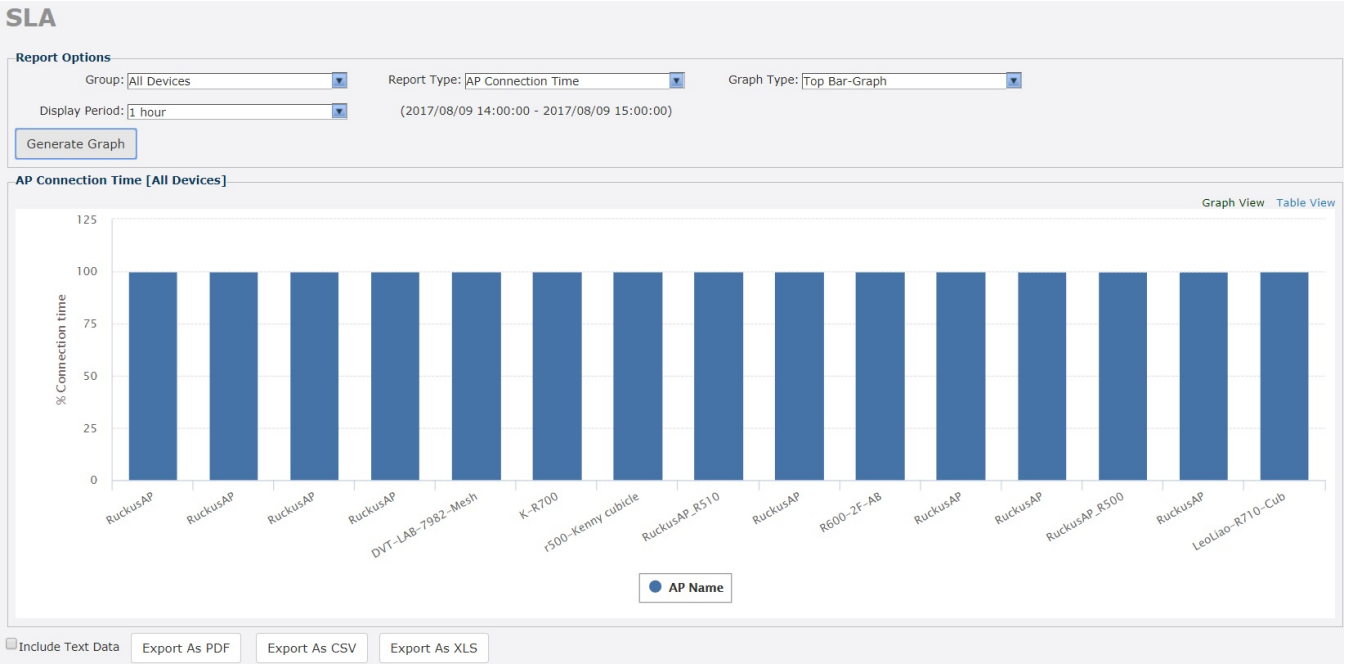
   Default device views include:

   - All Devices
   - Specified Device
3. In **Report Type**, select the type of report that you want to generate. The following report type options appear:
   - *AP Connection Time*
   - *Client Potential Throughput*
   - *Client Associated Time*
4. In **Graph Type**, select the type of graph to use in the report. Options include:
   - *Top Bar-Graph*: Displays the top devices for the selected report type.
   - *Histogram*: Displays the density of managed devices against a specific variable (report type).
5. In **Display Period**, select the time period for which you want to generate the report. Options range from 1 hour to 31 days.
6. Click **Generate Graph**. The page refreshes, and the graph appears.

   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 **Table View**.

FIGURE 43 Sample SLA report



Generating a Troubleshooting Report

Generate various graphs that are useful for troubleshooting.

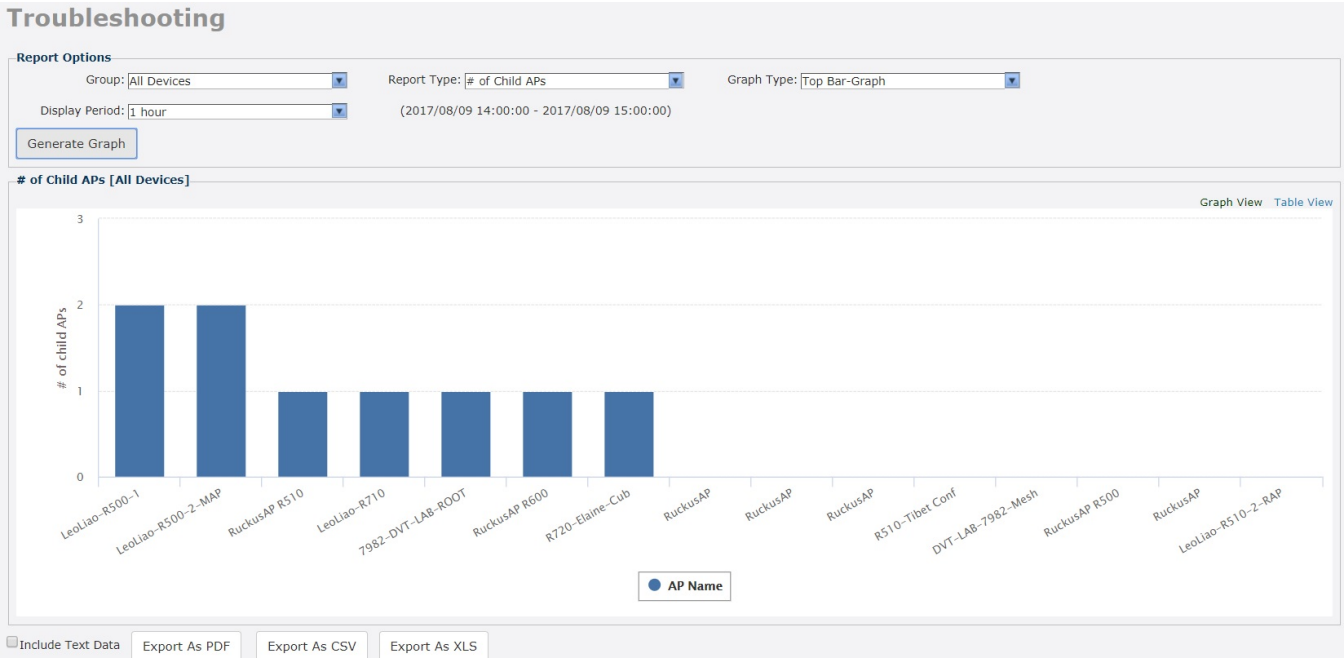
1. Go to **Reports** > **Troubleshooting**.
2. In **Group**, select the device view for which you want to generate a report.

   Default device views include:

   - All Devices
   - Specified Device
3. In **Report Type**, select the type of report that you want to generate. The following report type options appear:
   - # of Child APs
   - # of Hops
   - Mesh RSSI
   - # of Reboot
4. In **Graph Type**, select the type of graph to use in the report. Options include:
   - Top Bar-Graph: Displays the top devices for the selected report type.
   - Histogram: Displays the density of managed devices against a specific variable (report type).
5. In **Display Period**, select the time period for which you want to generate the report. Options range from 1 hour to 31 days.
6. Click **Generate Graph**. The page refreshes, and the graph appears.

   To view the report in a tabular format, click **Table View**.

FIGURE 44 A sample troubleshooting report



Generating a Resource Monitor Report

Generate a resource monitor report to view CPU, memory, and disk usage on managed ZoneDirector devices.

NOTE
This report is supported only for ZD. Unleashed is not supported.

1. Go to **Reports** > **Resource Monitor**.

   The **Report Type** parameter has only one selection (**CPU/Mem/Disk Usage**), which cannot be changed.
2. In **Group**, select the device view for which you want to generate a report.

   The default device view is **All Devices**.

   When there are custom device views, they also appear in the list of options.
3. (Optional) If you want to add a search filter to your query, then configure the options in the Filters section.
   a) In the first drop-down list box after **Filter Rows where**, select the search attribute that you want to use. Options include *Controller name*, *Model Name*, *Serial Number*, *IP Address*, *%CPU*, *%Mem* and *%Disk* .
   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 param- eter, then only devices with this IP address appear in the search results.
      - *Contains*: Search for devices with attributes that include the query param- eter you entered. For example, if you selected **IP Address** as the attribute and you entered **`100`** as the search parameter, then all devices with "100" in the IP address (for example, `172.17.16.`**`100`** and **`100`**`.1.10.13`) appear in the search results.
      - *Starts with*: Search for devices with attributes that start with the query parameter you entered. For example, if you selected **Serial Number** as the attribute and you entered **`3908`** as the query parameter, then only devices with serial numbers that begin with "3908" (for example, `390801005202`) appear in the search results.
      - *Ends with*: Search for devices with attributes that end with the query parameter you entered. For example, if you selected **IP address** as the attribute and you entered **`13`** as the query parameter, then only devices with model names that end in "13" (for example, `100.1.10.`**`13`**) appear in the search results.

      After you select a search operator, a third (text) box appears.
   c) In the text box, type the search parameter that you want to use with attribute and operator that you selected.

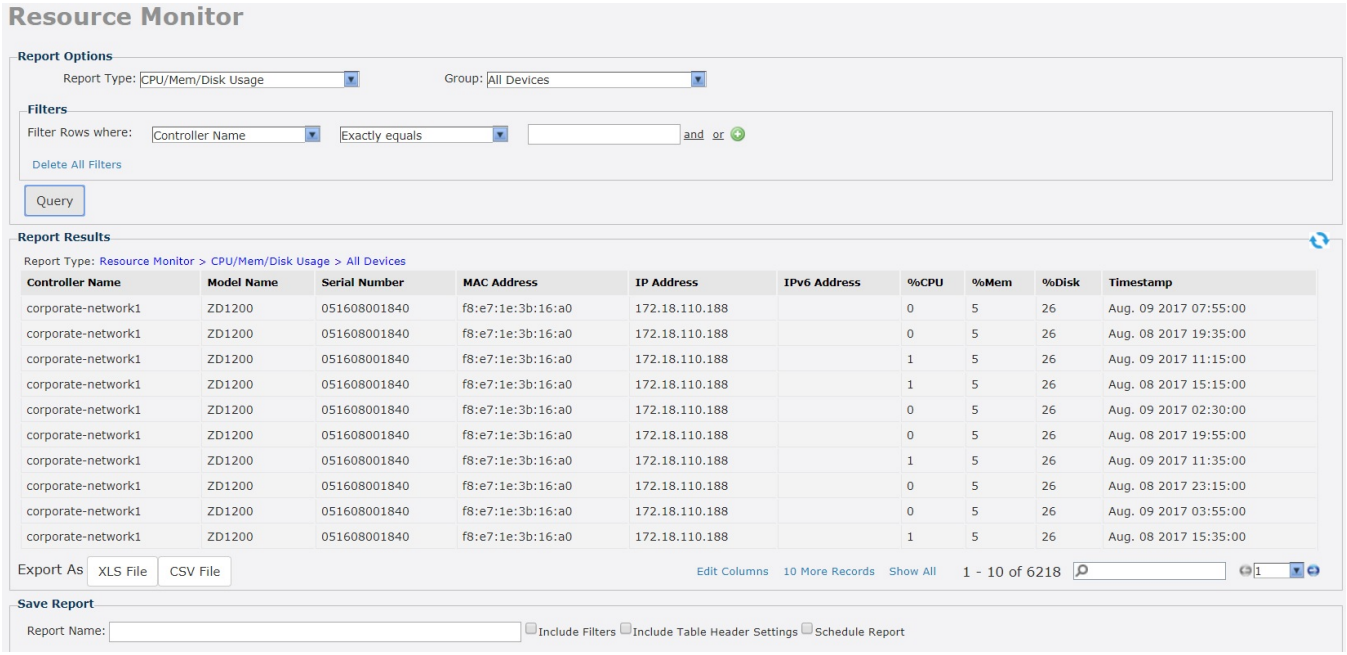
      The search parameter can consist of numbers or letters (depending on the attribute that you selected in the first drop-down list box) and can be a partial or full string. Refer to the previous step for search examples.
4. If you want to add another search filter, click **and** or **or**, and then click  .

   A second filter layer appears below the first. Complete the search filter options as in the first filter. You can add up to three additional search filters.

5. Click **Query**. The page refreshes, and then displays the current resource usage (CPU, memory, and disk) of all ZoneDirector devices in the selected device view.

> NOTE
> The software provides options for filtering the devices that are included in the report. Options for saving the generated report, automating report generation, and saving the report as an Excel file are also available. For more information, refer to Using Advanced Report Options on page 86.

FIGURE 45 Sample resource monitor report



Generating a PCI Report

Generate a PCI report, showing all current and past detected Rogue devices over the report period, as follows:

1. Go to **Reports** > **PCI Report**.
2. In **Controllers**, select the device view for which you want to generate a report.
3. In **Period**, select the time period for which you want to generate the report.

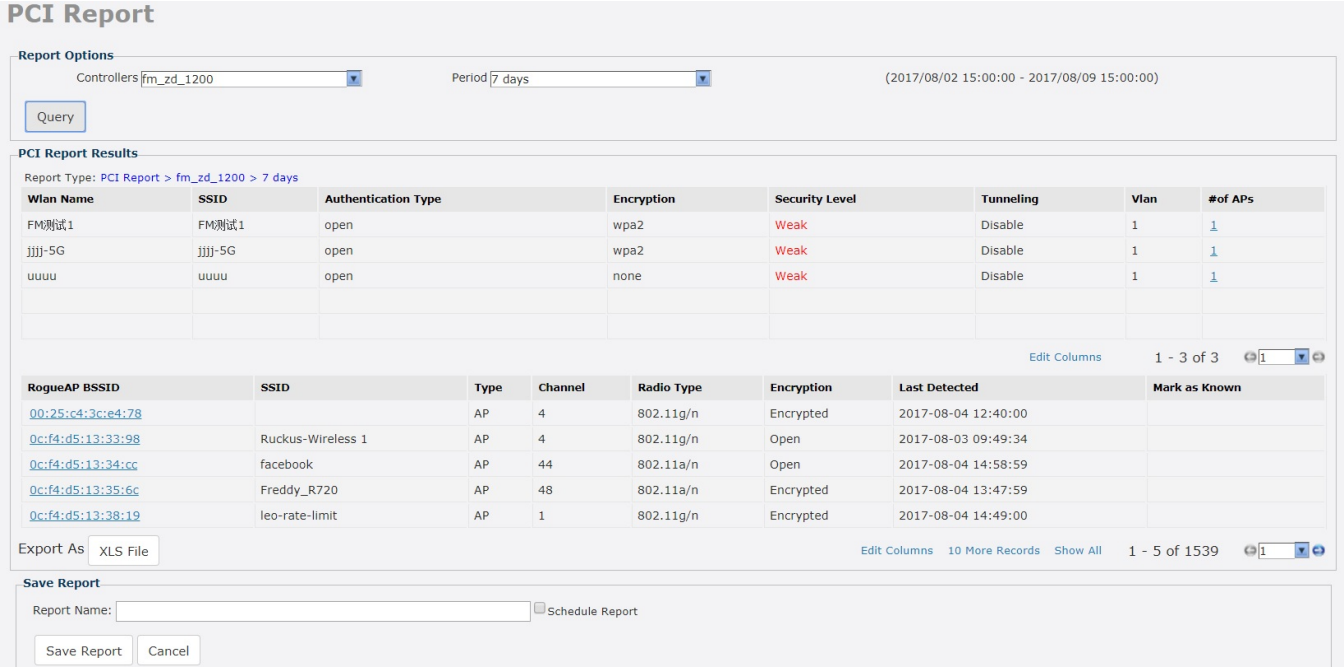
   Options range from 15 minutes to 31 days.

4. Click **Query**.

   The page refreshes, and displays the selected PCI report.

   NOTE
   The software provides options for filtering the devices that are included in the report. Options for saving the generated report, automating report generation, and saving the report as an Excel file are also available. For more information, refer to Using Advanced Report Options on page 86.

FIGURE 46 Sample PCI report



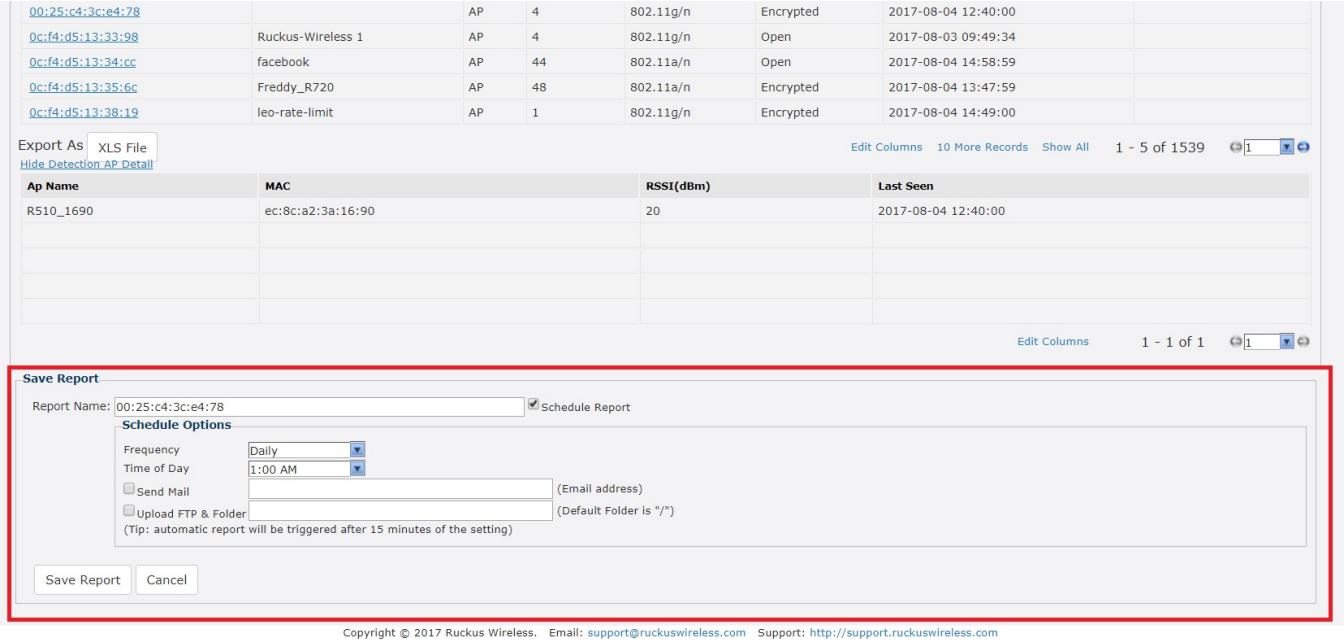
Using Advanced Report Options

You can configure the options of a report, so you can easily generate the report anytime without having to reconfigure the report options. You can even configure the software 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. Configure the required report.

4. Go to the **Save Report** section.

FIGURE 47 Saving a report and automating report generation



5. In **Report Name**, type a descriptive name for the report that you are saving.
6. Configure the following settings:
   - **Schedule Report**: Select this check box when you want the software 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 the software to generate this report. Options include **Daily**, **Weekly** and **Monthly**. If you selected **Weekly**, then select the **Day of the Week** when the software generates the report. If you selected **Monthly**, then select the **Day of the Month** when the software generates the report.
   - *Time of Day*: Set the time when the software generates the report.
   - *Email report to*: Type the email address to which the report is sent. When you are sending the report to multiple email addresses, use a comma to separate the email addresses.
   - *Send Mail*: Type the email address to which the report is sent. When you are sending the report to multiple email addresses, use a comma to separate the email addresses.
   - *Upload FTP & Folder*: Enter the workstation folder for the software to write the FTP files to.
7. Click **Save Report**.

You have completed configuring Unleashed Multi-Site Manager to generate and email this report automatically. The report should now appear on the **Saved Reports** page. For more information on working with saved report, refer to Managing Saved Reports on page 88.

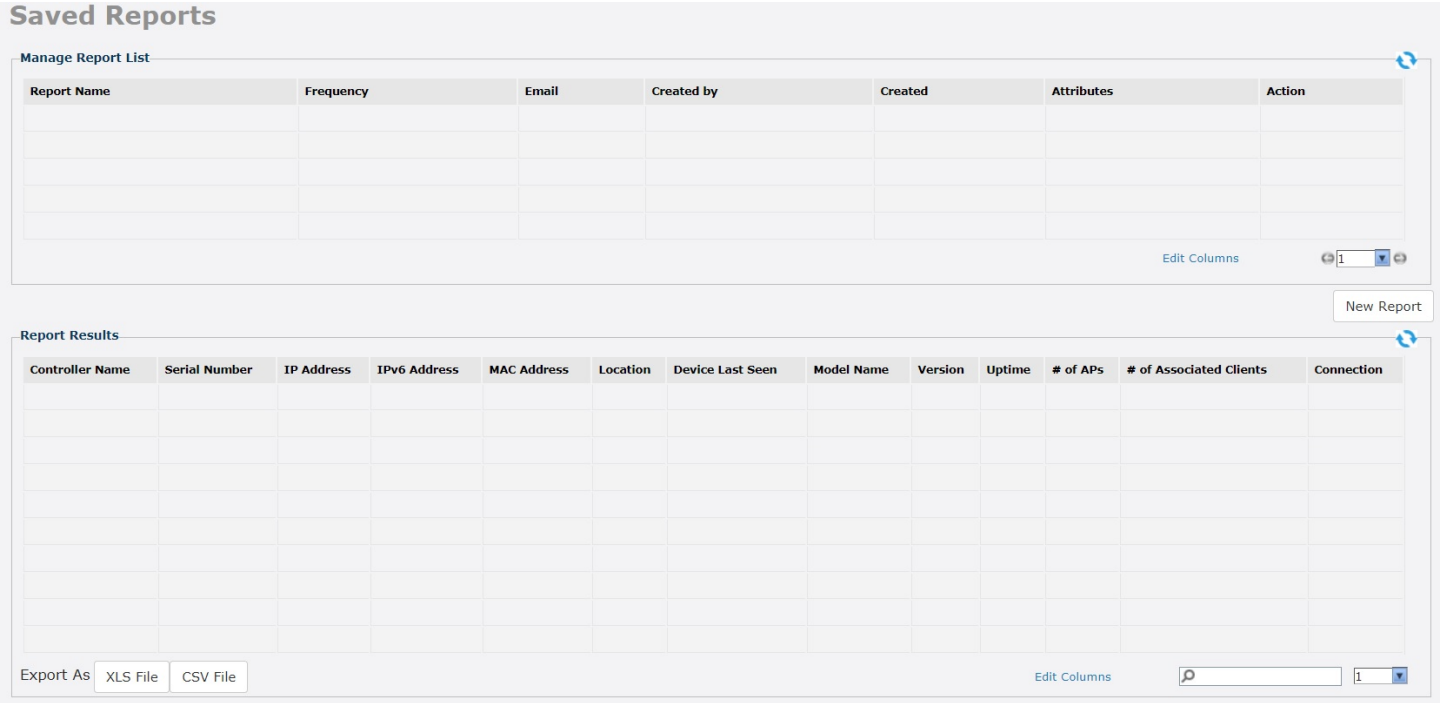
Managing Saved Reports

The **Saved Reports** page displays reports that you have previously configured and saved. There are three tasks that you can perform on the **Report** > **Saved Reports** 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 48 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** > **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 in the **Report Results** section.

Editing a Report

When you need to change the report options, you can edit the report settings from the **Saved Reports** page.

1. Go to **Reports** > **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.
4. Update the report options as needed.
5. Click **Save Report**.

You have completed editing a report.

Deleting a Report

When you no longer want a report to appear on the **Saved Reports** page, you can delete it.

1. Go to **Reports** > **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

About the Administer Tab

The **Administer** tab provides options for viewing audit logs, updating the software license file, configuring system settings, and other administration functions.

Viewing Audit Logs

Audit logs describe configuration actions that were performed on the software 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 7 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 software Web interface.
User logged out	User log out of the software 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.

TABLE 7 Audit log entries (continued)

Audit Type	Description
Audit log emailed	User sent out software's audit log via email.
License file verification	The maximum number of devices supported by your software license has been reached. To manage additional devices, please contact Ruckus Sales representative and obtain a license for additional devices.
License file uploaded	User uploaded a new license file into the software.
Device registered	A device registered with the software.
Inventory file imported	User imported an inventory file (XLS) into the software.
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 the software.
Inventory status created	User created an inventory status.
Inventory status modified	User updated an inventory status.
Inventory status assigned	User changed a n AP's inventory status.
Inventory comment assigned	User edited an AP's comment on the **Inventory** page.
Inventory status deleted	User deleted an inventory status.
ZoneDirector configuration cloned	User created a "Clone ZoneDirector" task.
Managed group created	User created a group for delegated management.
Managed group updated	User updated a group for delegated management.
Managed group deleted	User deleted a group for delegated management.
Managed group device(s) added	User assigned devices to a managed group.
Managed group device(s) removed	User removed devices from a managed group.
User group mapping updated	User changed the "user account" and "managed group" mapping.
User logged in via the Northbound interface	A 3rd party system logged into the software via the Northbound interface.
User logged out via the Northbound interface	A 3rd party system logged out of the software 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 software server.
Upgrade successful	User patched the software successfully.
Upgrade failed	User patch for the software failed.
ZoneDirector could not be r eached	The software 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 the software three times.
Automatic report emailed	Automatic report has been sent out.

Managing Software Licenses

The number of Ruckus AP devices that the software can manage is limited by one or more license files. The AP devices can be ZD or Unleashed. Once the limit is reached, no additional devices are able to register with the software (and none appear on the **Inventory** page) until another license file is added to the software server. Refer to the **Administer** > **License** page to see how many APs are currently licensed.

There are 2 kinds of software licenses file, one is for ZD and the other one is for unleashed. By default, there are zero ZoneDirector licenses and one Unleashed license. ZoneDirector license consumes Unleashed Multi-Site Manager license according to it's AP license. For example, ZD3500 will consume 500 licenses even when the 500 APs are not managed by Zone Director.

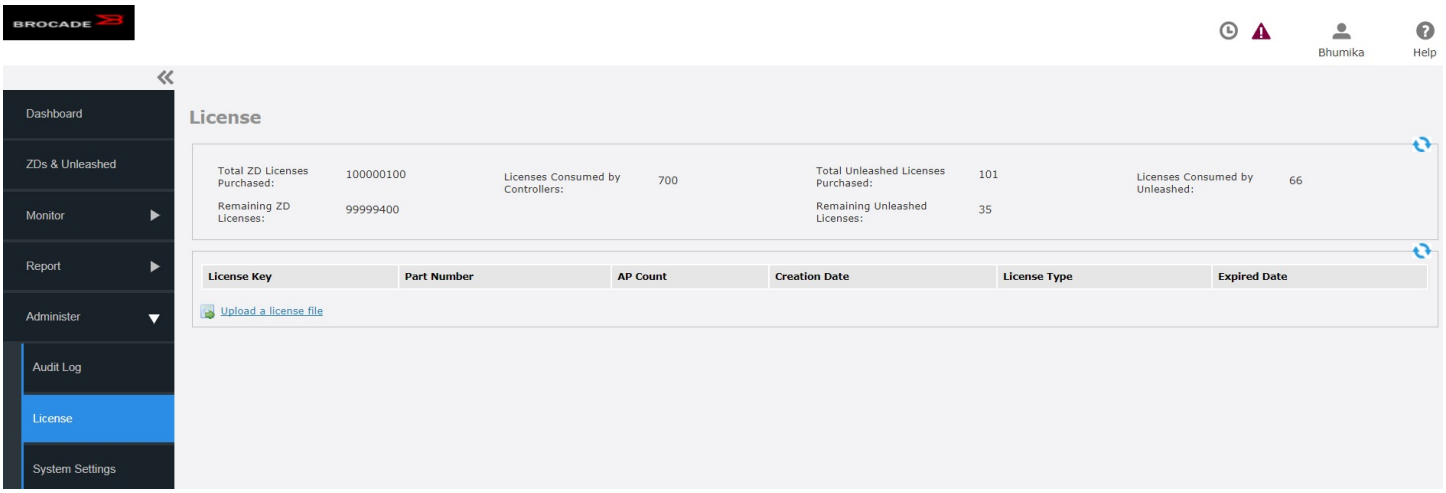
Unleashed license consumes software license according to its connected AP number. The unleashed license is updated whenever the software receives the information message from unleashed but the unleashed AP connect status is updated every 15 mins. So, there is a gap between the software update the Unleashed license (every 1 to 60 mins) and it's AP connected status (15 mins). This may cause an inconsistence between connected AP and license on the web user interface.

When a trial license expires, the software checks the licenses number and will delete the devices if the license is lacking.

To enable Unleashed Multi-Site Manager to manage additional APs, you need to upload at least one more license file. Use the **License** page in **Administer** > **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 License page.

FIGURE 49 The License page



The page displays the total ZD and Unleashed Licences available and the unused ZD and Unleashed licences.

> **NOTE**
> **Licenses Consumed by ZoneDirectors** indicates the total number of AP devices that your ZoneDirector licenses can support, not the number of APs that your ZoneDirector devices are currently managing.

When your total inventory nears the total licences purchased, you can buy a new license to add on to the maximum number; that is, a new license adds on to the previous license, and it does not overwrite the previous license. Thus, the total licenses purchased is the sum of AP counts within each license file.

NOTE
If your inventory count reaches your license total, then any new devices attempting to register are denied (and do not appear in your Inventory) until your license situation is resolved.

Uploading a License File

You can update your current software license by uploading additional license files using the Web interface.

1. Once you obtain a new license file from Ruckus, log in to the Unleashed Multi-Site Manager Web interface.
2. Go to **Administer** > **License**.
3. Click the **Upload a license file** link. The **UPLOAD A LICENSE FILE** form opens below the link.
4. Click the **Choose File** button next to **Select file to upload**.
5. Select the license file, and then click **Return** within the dialog to close the **Open** window.
6. Click **OK** to upload the license file to Unleashed Multi-Site Manager.

Configuring System Settings

The System Settings option allows you to specify an SMTP server and a support- level user for sending the software 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 the software-generated files (such as logs, events, and graph data) should be maintained on the software. Once the configured length of time has been reached, files/items older than the date are purged from the software to save disk space. This prevents those files from growing interminably.

FIGURE 50 System Settings page (part 1 of 4)

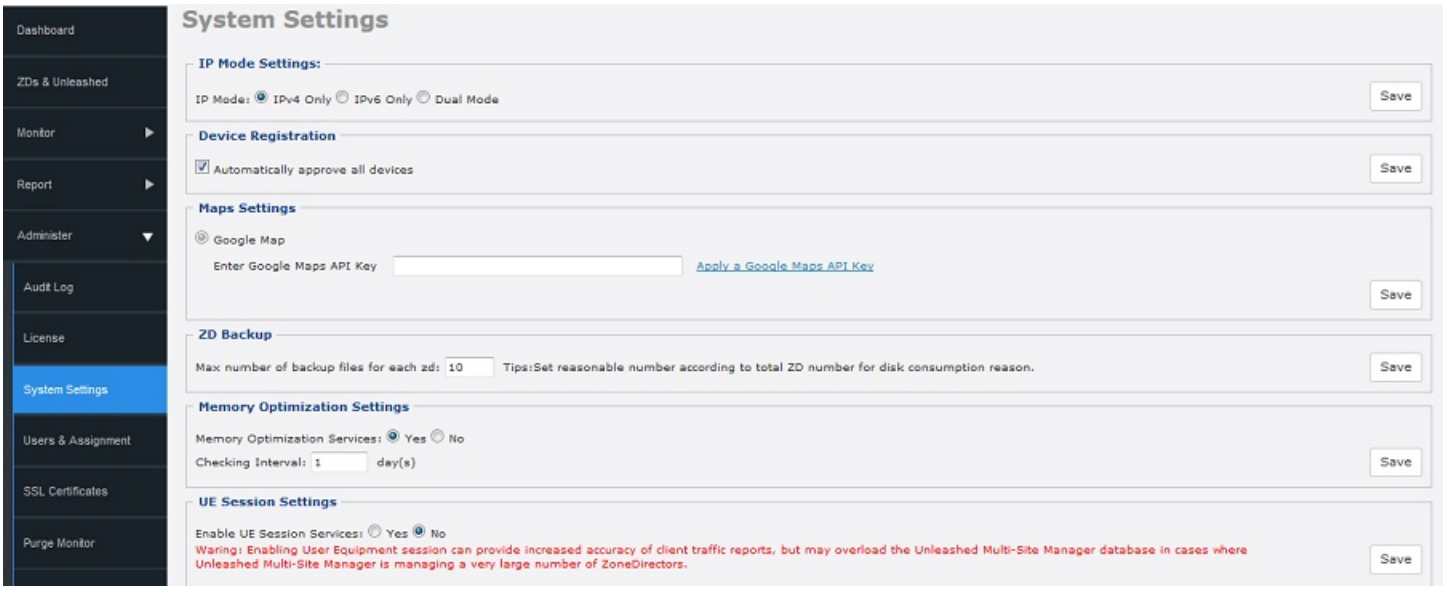


FIGURE 51 System Settings page (part 2 of 4)

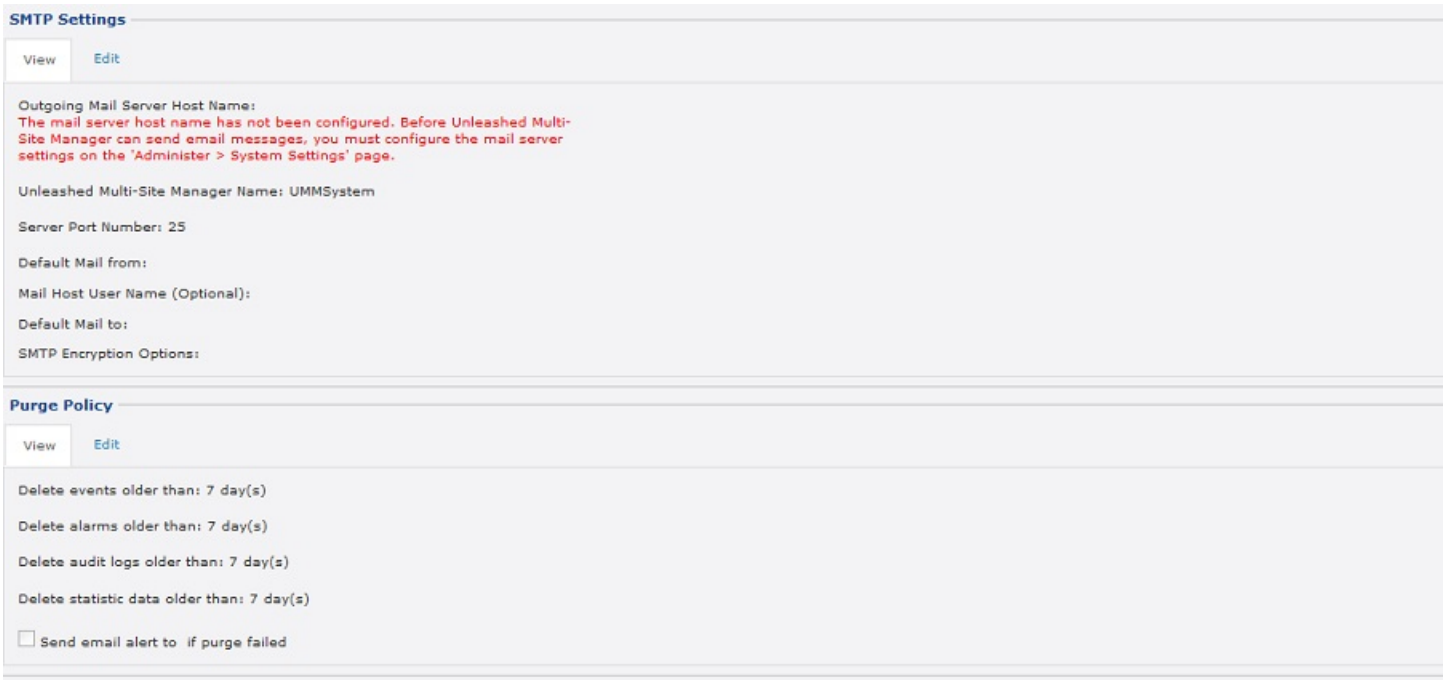


FIGURE 52 System Settings page (part 3 of 4)

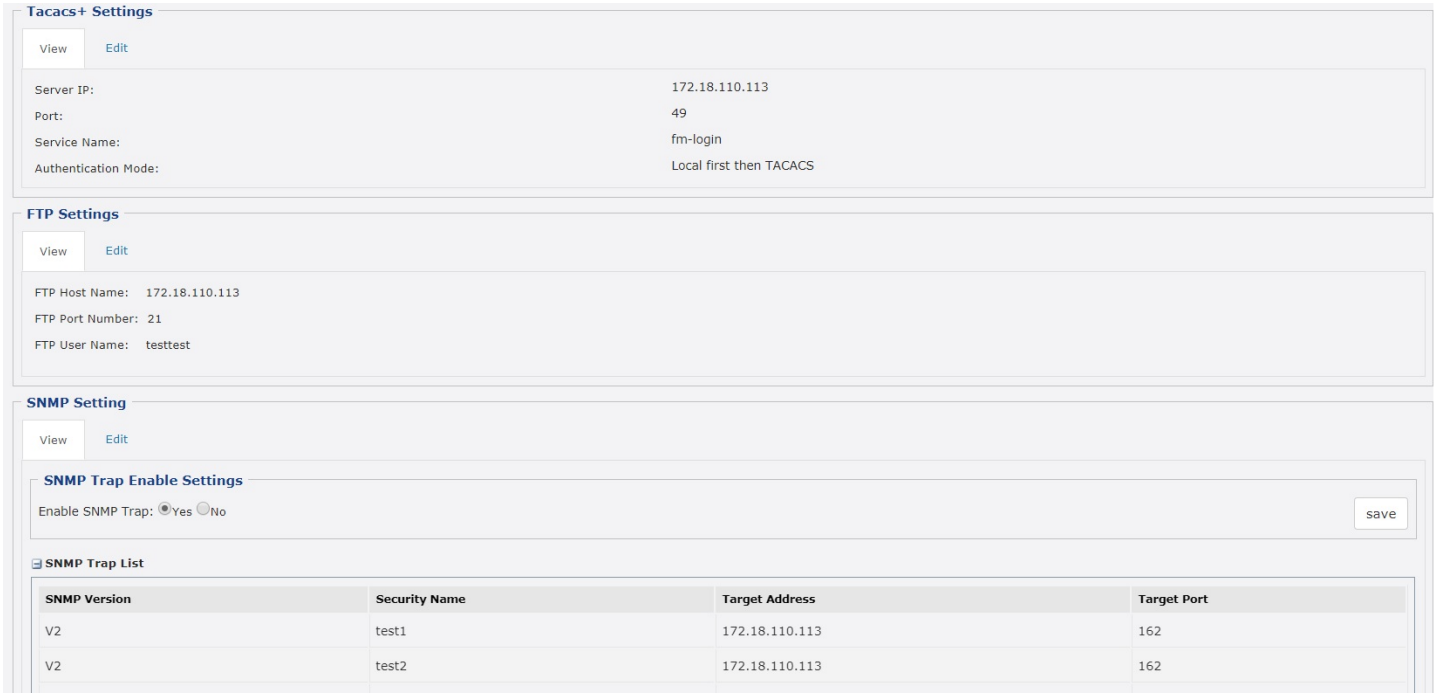
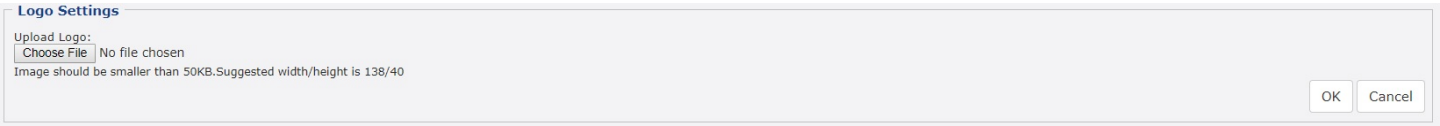


FIGURE 53 System Settings page (part 4 of 4)



IP Mode Settings

Unleashed Multi-Site Manager supports IPv4, IPv6, and dual IPv4/IPv6 operation modes. If dual mode is used, then the software keeps both IPv4 and IPv6 IP addresses. By default, the software operates in IPv4 mode. When you want to change the IP mode, follow the procedure below.

1. Go to **Administer** > **System Settings**.
2. Under **IP Mode Settings**, select the mode that you want the software to use.

   Options include **IPv4 Only**, **IPv6 Only** and **Dual Mode**.
3. Click the **Save** button that is in the same section.

Device Registration

This settings allows you to automatically approve all the newly added devices. Check the **Automatically approve all devices** check box and click **Save** to save the configuration.

Map Settings

To use the Google Maps API, you must register the software on the Google API Console and get a Google API key which you can add to the software. If you already have a Google API Map Key, type the key to establish a connection with Google Maps. You can click the **Apply a Google Maps API Key** to generate a key.

Memory Optimization Settings

To help ensure that the software 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 the software clears its memory cache. When you are done, click the **Save** button in the **Memory Optimization Settings** section.

> NOTE
> Memory optimization requires that your the software 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.

UE Session Settings

User Equipment session services provide better accuracy of client traffic reports. However, if the Unleashed Multi-Site Manager is managing many ZD and Unleashed controllers, then the software database can become overloaded with inputs.

Follow these steps to enable User Equipment sessions.

1. Go to **Administer** > **System Settings**.

2. Scroll down to the **UE Session Settings** section.
3. In **Enable UE Session Services**, select **Yes** or **No** to enable or disable User Equipment sessions, respectively.
4. Click the **Save** button that is in the same section.

SMTP Settings

You must configure the software'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 preconfigured recipient (**Default Mail To**) specified on the **SMTP Settings** page.

> **NOTE**
> You may have already configured the SMTP settings during the software installation.

For the email functionality to work, you need either [1] a DNS server that can supply the IP address of the SMTP server, or [2] the correct mapping to the SMTP server in your hosts file (located in the `/etc` directory). If you choose the second option, then you need to add lines similar to the following in your `/etc/hosts` file:

```
127.0.0.1 fully.qualified.domain.name localhost
123.123.123.123 fully.qualified.smtpdomain.name smtp- server_hostname
```

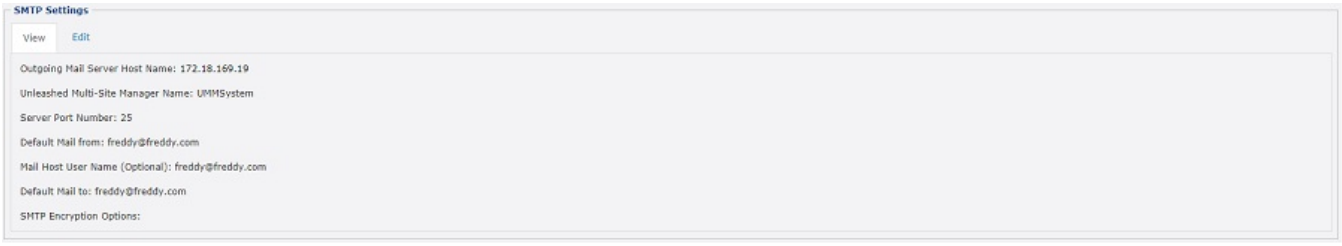
> **NOTE**
> If you use "." in the hostname to separate `hostname.domainname`, then you are not allowed to use a digit-only domain name. For instance, `umm.ruckus` and `umm.98ABC` are allowed, and `umm.98` and `Localhost.12345` are not allowed.

> **NOTE**
> If you edited the hosts file before you installed the software (as described in Editing the Server Hosts File on page 21, then the first line should already exist in the hosts file; you do not need to add the same line again.

Follow these steps to edit the SMTP settings.

1. Go to **Administer** > **System Settings**.
2. Scroll down to the **SMTP Settings** section.
3. Click the **Edit** tab.

FIGURE 54 Editing SMTP Settings



4. In **Outgoing Mail Server Host Name**, type the host name of the outgoing SMTP server.
5. (optional) In **UMM Name**, enter a new name for the the software server.

6. In **Server Port Number**, type the SMTP server's listening port number.

   The default SMTP port number is 25.

   > **NOTE**
   > If you select TLS or STARTTLS SMTP Encryption Options, then define a different port number, because different SMTP server protocols do not support port 25. For example, the Gmail server uses 587 as its STARTTLS port and 465 as the TLS port, and the QQ server uses 25 as its non-SSL port and 465 as its TLS port.
   > If your port number setting and protocol setting do not match, emails cannot be sent successfully. For example, if you select port 25 and select STARTTLS for a QQ server, testing will fail. Emails do not automatically revert to the non-TLS protocol.

7. In **Default Mail from**, type the email address that appears as the sender of the email.
8. In **Mail Host User Name (Optional)**, type the SMTP user name for the email account that you are using to send email notifications.
9. In **Mail Host Password (Optional)**, type the SMTP password for the email account.
10. In **Default Mail to**, type the email address of the user to whom you want to send email notifications.
11. In **SMTP Encryption Options**:
    - Check the **TLS** box if you want the software to use Transport Layer Security cryptographic protocol.
    - Also check the **STARTTLS** box if you want the software to use the STARTTLS extension to upgrade plain email connections to encrypted TLS connections instead of using a separate port for encrypted communication.
12. Click **Test** to verify that the software is able to use the SMTP settings that you configured to send email notifications. If an error appears, then check your settings and update them with the correct settings.
13. Click the **Save** button that is in the same section.

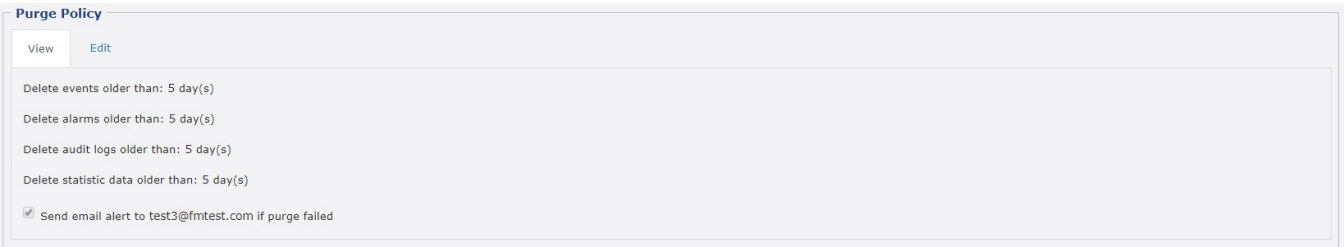
Purge Policy

Use Purge Policy to automatically delete the software event logs, audit logs, and graph data after they age past a certain number of days. This helps ensure that the software has sufficient disk space to perform tasks.

Note that if the operator defines too many SSIDs on a ZD, then this impacts the the software capacity. So when the software is configured for maximum capacity, Ruckus recommends that the operator does not implement the '64 SSID' feature on the ZDs. Refer to Server System Requirements on page 20 for minimum system CPU and RAM requirements.

1. Go to **Administer** > **System Settings**.
2. Scroll down to the **Purge Policy** section.
3. Click the **Edit** tab.

FIGURE 55 Editing Purge Policy settings



4. Type a numerical value (all values are number of days) for one or more of the following:
   - **Delete events older than:** default is 7 days
   - **Delete alarms older than:** default is 7 days
   - **Delete audit logs older than:** default is 7 days
5. Click **Save**.

TACACS+ Settings

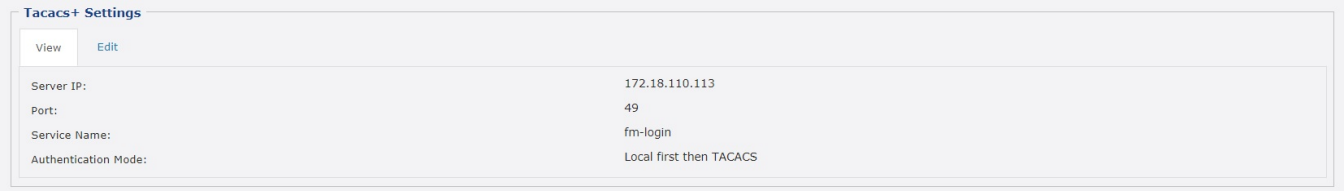
TACACS+ is an access control network protocol that provides separate authentication, authorization and accounting services.

NOTE
Only the Admin user is permitted to change the **Authentication Mode** during installation. Authentication has four modes:

- Only local (TACACS user cannot log in.)
- Only TACACS (Except the Admin user who was created when the software was installed.)
- First local then TACACS (Both of them can log in.)
- First TACACS then local (Both of them can log in.) The **Authentication Mode** affects the user login process.

1. Go to **Administer** > **System Settings**.
2. Scroll down to the **Tacacs+ Settings** section.
3. Click the **Edit** tab.

FIGURE 56 Editing TACACS+ settings



4. Enter the TACACS+ parameters:
   - *Server* - IPv4 or IPv6 server address.
   - *Port* can be set to any available TCP port.
   - *Service Name*.
   - *Secret*.
   - *Confirmed Secret*.
5. Click **Test** to verify that the software is able to use the TACACS+ settings that you configured.
   If an error appears, then check your settings and update them with the correct settings.
6. Click **Save**.

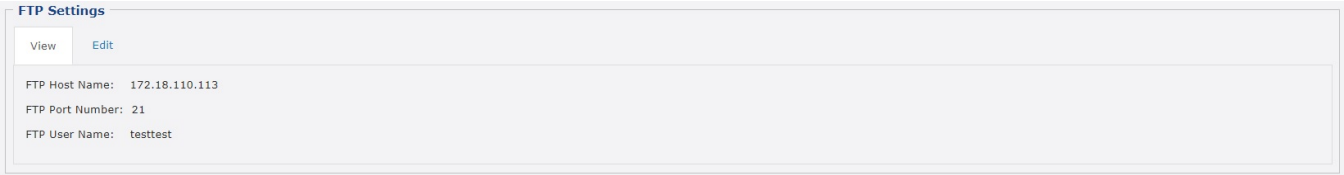
FTP Server Settings

You must configure FTP server settings for your Ruckus devices to communicate with an FTP server.

1. Go to **Administer** > **System Settings**.

2. Scroll down to the **FTP Settings** section.
3. Click the **Edit** tab.

FIGURE 57 Editing FTP server settings



4. Enter the FTP parameters:
   - *FTP Host Name* - IPv4 or IPv6 server address.
   - *FTP Port Number* - 21 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 the software is able to use the FTP server settings that you configured.

   If an error appears, then check your settings and update them with the correct settings.
6. Click **Save**.

SNMP Server Settings

If you have an SNMP trap receiver on the network, then you can configure the software to send SNMP trap notifications to the server. Enable this feature if you want to automatically receive notifications for ZD, Unleashed, 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 **Edit** tab.

FIGURE 58 SNMP configuring settings

4. In **Enable SNMP Trap**, click **Yes** or **No**.
5. Click **save**.
6. Continue with Configuring SNMP Settings.

Configuring SNMP Settings

After you enable SNMP trap, you need to configure the SNMP V2/V3 settings, depending on the SNMP version that the SNMP trap receiver is using.

If Your Network Uses SNMP v2

1. Click the **Administer** > **System Settings** > **SNMP Settings** > **Edit** tab.
2. Under **SNMP v2 Settings**, configure the following settings:
   a) *Community:* Enter the SNMP v2 community string.
   b) *Read:* Select this check box to enable SNMP read access.
   c) *Trap:* Select this check box to send SNMP traps to the trap server on the network.

   NOTE

   To add another SNMP v2 community string, click the icon, and then configure the community string and read and trap privileges.

3. Click **save** to save your changes.
4. Under **SNMP Trap**, configure the following settings:
   a) *SNMP Version:* Select V2.
   b) *Security Name:* Enter the security name.
   c) *Target Address:* Enter the IP address of the SNMP trap receiver.
   d) *Target Port:* Enter the SNMP port number on the SNMP trap receiver.
5. Click **save** to save your changes.

If Your Network Uses SNMPv3

1. Click the **Administer** > **System Settings** > **SNMP Settings** > **Edit** tab.
2. Under **SNMP v3 Settings**, configure the following settings:
   a) *User Name*: Enter a user name between 1 and 31 characters long.
   b) *Auth Protocol* Select **MD5**, **SHA** or **NONE** authentication method (default is MD5).
      - *MD5* (Message-Digest algorithm 5) is a message hash function with 128- bit output.
      - *SHA* (Secure Hash Algorithm) is a message hash function with 160-bit output.
   c) *Auth Password*: Enter a passphrase between 8 and 32 characters long.
   d) Priv Protocol: Select **DES**, **AES** or **NONE**.
      - *DES* (Data Encryption Standard), data block cipher.
      - *AES* (Advanced Encryption Standard), data block cipher.
      - *NONE*: No Privacy passphrase is required.
   e) *Priv Password*: If either **DES** or **AES** is selected, then enter a Privileged Password between 8 and 32 characters long.
   f) *Read*: Select this check box to enable SNMP read access.
   g) *Trap*: Select this check box to send SNMP traps to the trap server on the network.

      NOTE

      To add another SNMP v3 community string, click the  icon, and then configure the community string and read and trap privileges.

3. Click **save** to save your changes.
4. Under SNMP Trap, configure the following settings:
   a) *SNMP Version*: Select **V3**.
   b) *Security Name*: Enter the security name.
   c) *Target Address*: Enter the IP address of the SNMP trap receiver.
   d) *Target Port*: Enter the SNMP port number on the SNMP trap receiver.
5. Click **save** to save your changes.

Default Events for Which the Software Sends Trap Notifications

There are several event types for which the software sends trap notifications to the SNMP server that you specified.

The default event types include:

- System administration events
- Mesh events
- Configuration events
- Client events
- AP admin events
- Performance events
- Device status events
- Alarm events

Default **System Admin trap** notifications:

- ZD System Failure Recovered
- Admin restart
- Admin shutdown
- Admin upgrade
- System cold restarted
- System warm restarted

Default **AP Admin trap** notifications:

- AP delete
- AP joined
- AP joined with reason
- AP lost
- AP lost heartbeat

Default **Device status events** trap notifications:

- Connectivity problem
- Device rebooted
- Device recovers from disconnect state
- Firmware successfully written to flash

Setting Events and Alarms for Which the Software Sends Trap Notifications

If you want the software to send trap notifications for non-default events, then you need to enable trap notifications for these events.

1. In the **SNMP Settings** section, scroll down to the **Events & Alarms selection** section (under **SNMP Trap**).
2. If the Events & Alarms selection section is collapsed, then click the  icon to expand it. The configuration tabs for the various event types appear.
3. Click the tab names to view the list of events from event types, and then select the check box for each event type that you want the software to send trap notifications.
4. Repeat as required.
5. Click **Save** to save your changes.

Setting User Customized Alarms

Refer to About User Customized Alarms on page 53 and Configuring Alarm Settings on page 56 for information about user-customized threshold-crossing alarms.

Logo Settings

You can change the Ruckus logo that appears up on the upper-left corner of the Unleashed Multi-Site Manager 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 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.

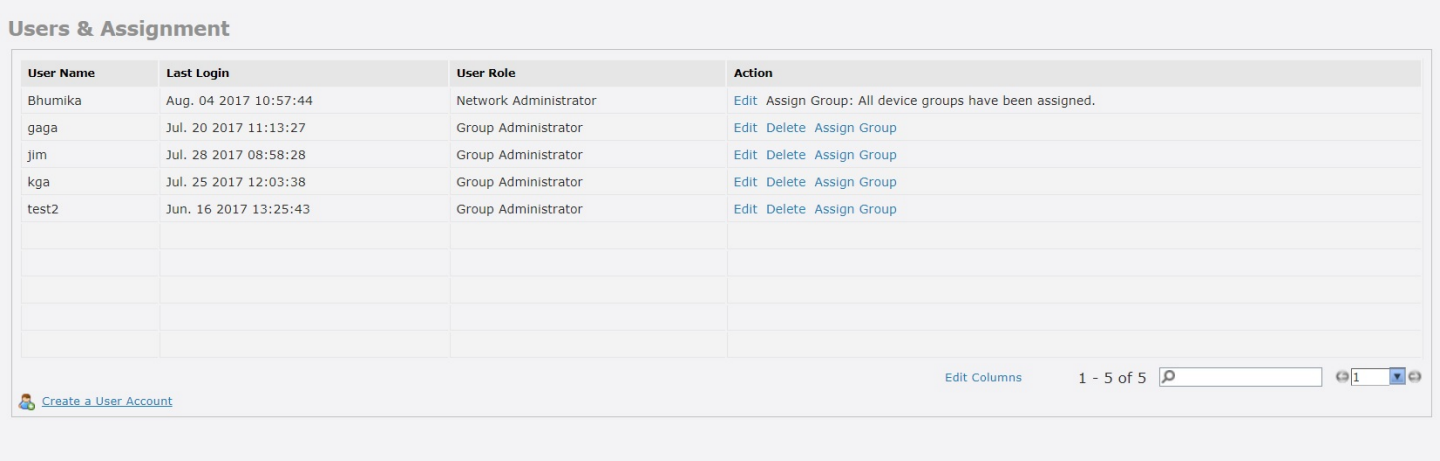
2. Go to **Administer** > **System Settings**.
3. Scroll down to the **Logo Settings** section.
4. Click the **Choose File** button.
5. When the **Open/Browse** dialog box appears, browse to the location where you saved the custom logo that you want to upload, and then select it.
6. Click **Open** to save your selection.
7. Click **OK** to finish uploading the custom logo file.

The Web interface refreshes, and the custom logo that you uploaded appears in place of the default Ruckus logo.

Managing User Accounts

When you want to share or delegate device management and monitoring tasks with other users in your organization, the software allows you to create additional user accounts. You should create a new user account and assign an appropriate role for each person who uses the software. Ruckus recommends against using one login account for multiple users as doing this may not produce useful audit log results.

FIGURE 59 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 Unleashed Multi-Site Manager 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 Unleashed Multi-Site Manager system. The following are the roles that you can assign in Unleashed Multi-Site Manager:

- Network Administrator
- Group Administrator

Network Administrator

The Network Administrator role grants full read and write privileges to the entire Unleashed Multi-Site Manager system. The installation process creates one default Network Administrator (admin) account; this default admin account cannot deleted or renamed.

> NOTE
> The default Network Administrator (also called Super User) has the highest account privilege and can 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 user accounts for a Group 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
- Assign devices to device management groups
- View Dashboard and Inventory information related to the assigned devices
- Provision configuration upgrade tasks for assigned devices

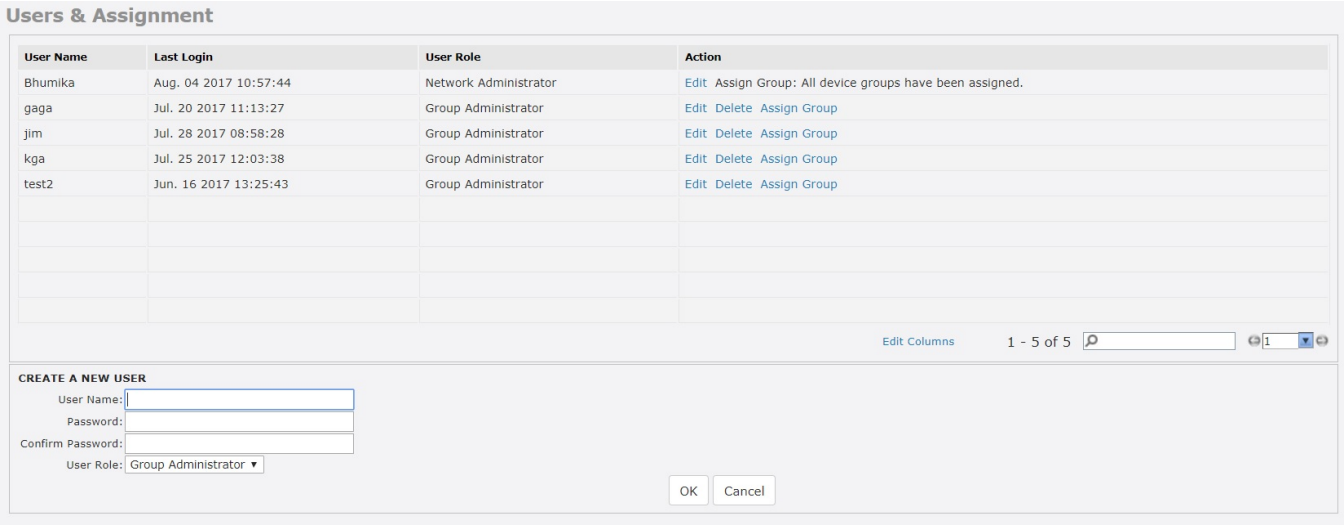
Creating a New User Account

When you want to delegate the responsibility of managing the software and its managed devices to other authorized users in your organization, you can create a user account for each of them. There is no limit to the number of user accounts that you can create.

1. Go to **Administer** > **Users & Assignment**.

2. Click **Create a User Account**. Unleashed Multi-Site Manager displays the **CREATE A NEW USER** pane.

FIGURE 60 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, then the following user roles appear on the menu: **Network Administrator**, **Group Administrator**.

   For more information on user roles, refer to Understanding User Roles and Privileges on page 104.
7. Click **OK** to create the account.

The page refreshes, and then the user account you have created appears in the **Users** list.

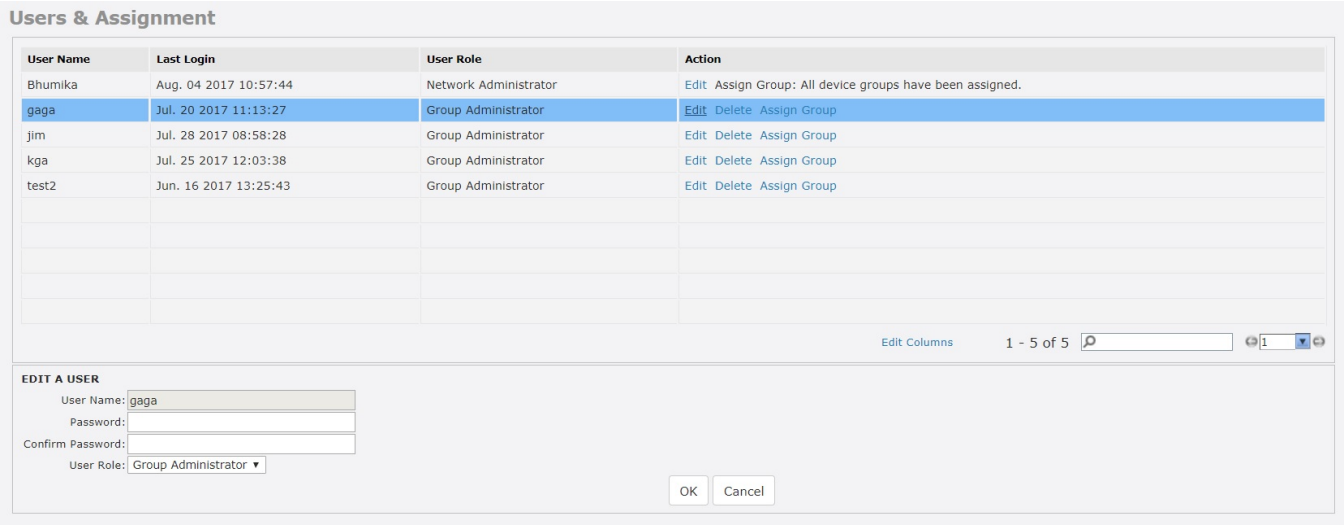
Editing a User Account

Edit a user account if you need to make account changes, such as the user password or the user role.

1. Go to **Administer** > **Users & Assignment**.

2. Find the row in the **Users** table for the desired user account to edit, and then click **Edit** in the **Action** column.

FIGURE 61 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 software database and prevent unauthorized users from gaining access to the the software Web interface.

1. Go to **Administer** > **Users & Assignment**.
2. Find the row in the **Users** table for the desired user account to delete, and then click **Delete** in the Action column.

The page refreshes, and then the user account you deleted is removed from the **Users** list.

Assigning Users to Manage Device Groups

1. Create a User account as described in Creating a New User Account on page 105.

   NOTE
   The User account must have **Group Administrator** privileges to manage a Device Group, as described in Understanding User Roles and Privileges on page 104.

2. Create a Device Group as described in the **Creating and Managing Groups** section Creating and Managing Groups on page 44.
3. Go to **Administer** > **Users & Assignment**.

4. Find the entry for the user account that you want to assign as group owner.
5. 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 62 Assigning a user to manage the group

6. Select the check box for each managed group that you want to assign to the user account
7. Click **Apply** to save your changes.

When the group owner logs into the the software 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 the software 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 the software is using for HTTPS communication is signed by Ruckus and is not recognized by most Web browsers.

If you want to prevent these security warnings from appearing, then you need to import an SSL certificate that was issued by a recognized certificate authority such as VeriSign.

NOTE
Unleashed Multi-Site Manager 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 the software.

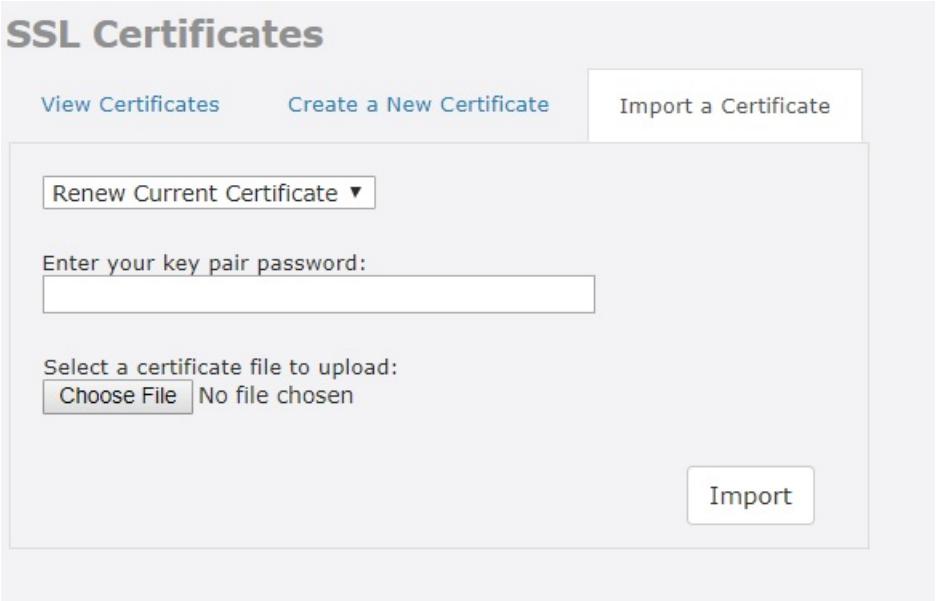
Importing an SSL Certificate

When you already have an SSL certificate issued by VeriSign, you can import it into Unleashed Multi-Site Manager 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 software Web interface.
2. Go to **Administer** > **SSL Certificates**.

3. On the SSL Certificates page, click the **Import a Certificate** tab.

FIGURE 63 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 Current Certificates on page 115.
8. After you verify that the new certificate has been imported successfully, shut down the software service by executing the following script:

   ```
   # /opt/UMM/shutdown.sh
   ```

9. Restart the software service by executing the following script:

```
# /opt/UMM/startup.sh
```

FIGURE 64 Shutting down and restarting the software service

```
[root@localhost UMM]# ./shutdown.sh
shutdown_pid=21797
Shutting down Tomcat server...

Using CATALINA_BASE:   /opt/UMM/3rdparty/tomcat/fm-tomcat
Using CATALINA_HOME:   /opt/UMM/3rdparty/tomcat/fm-tomcat
Using CATALINA_TMPDIR: /opt/UMM/3rdparty/tomcat/fm-tomcat/temp
Using JRE_HOME:        /opt/UMM/3rdparty/jre/fm-jre
Using CLASSPATH:       /opt/UMM/3rdparty/tomcat/fm-tomcat/bin/bootstrap.jar:/opt/UMM/3rdparty/tomc
at/fm-tomcat/bin/tomcat-juli.jar
Going to kill UMM process.
Done.
Going to kill UMM process.
killing HttpShellProxy process pid=11010
Done.
Going to kill Snmpagent process.
killing Snmpagent process pid=10909
Done.
Current path = /opt/UMM/support_files
waiting...test -e /opt/UMM/3rdparty/mysql/fm-mysql/data/localhost.localdomain.pid
file check=not
[root@localhost UMM]# ./startup.sh


Linux version [x86_64]

JAVA_OPTS=-server -Xms2253m -Xmn1971m -Xmx5258m -XX:MetaspaceSize=256m -XX:MaxMetaspaceSize=384m -
XX:+HeapDumpOnOutOfMemoryError -XX:-UseGCOverheadLimit -Djava.awt.headless=true -Xss2m -Dsun.secur
ity.ssl.allowUnsafeRenegotiation=false -Dhttps.protocols=TLSv1.2
startup_pid=21913
Starting DB server.

170915 10:27:57 mysqld_safe Logging to '/opt/UMM/3rdparty/mysql/fm-mysql/data/localhost.localdomai
n.err'.
170915 10:27:57 mysqld_safe Starting mysqld daemon with databases from /opt/UMM/3rdparty/mysql/fm-
mysql/data
Detecting MySQL status...
MySQL start successfully!
Starting ActiveMQ.

nohup: appending output to ânohup.outâ
Starting Tomcat server.

Using CATALINA_BASE:   /opt/UMM/3rdparty/tomcat/fm-tomcat
Using CATALINA_HOME:   /opt/UMM/3rdparty/tomcat/fm-tomcat
Using CATALINA_TMPDIR: /opt/UMM/3rdparty/tomcat/fm-tomcat/temp
Using JRE_HOME:        /opt/UMM/3rdparty/jre/fm-jre
Using CLASSPATH:       /opt/UMM/3rdparty/tomcat/fm-tomcat/bin/bootstrap.jar:/opt/UMM/3rdparty/tomc
at/fm-tomcat/bin/tomcat-juli.jar
Tomcat started.
Using CATALINA_BASE:   /opt/UMM/3rdparty/tomcat/httpshellproxy
Using CATALINA_HOME:   /opt/UMM/3rdparty/tomcat/httpshellproxy
Using CATALINA_TMPDIR: /opt/UMM/3rdparty/tomcat/httpshellproxy/temp
Using JRE_HOME:       /opt/UMM/3rdparty/jre/fm-jre
Starting snmpagent at port 161.

SNMP agent starts up successfully.


[root@localhost UMM]#
```

You have completed importing a VeriSign-issued SSL certificate.

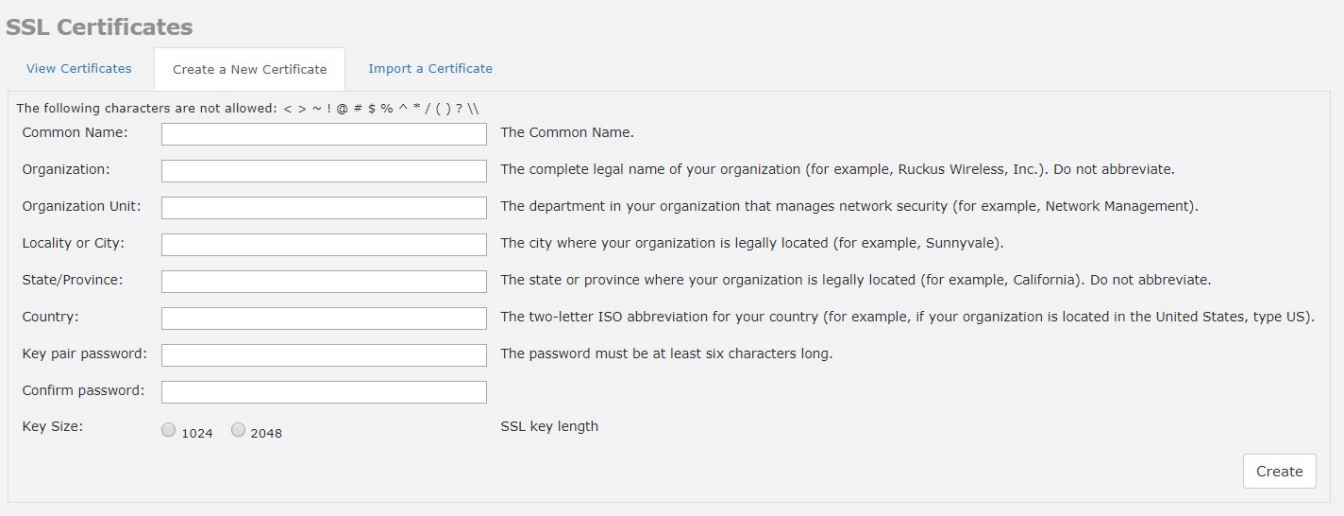
Try connecting to the software Web interface using HTTPS. The security alert should no longer appear.

Creating a Certificate Signing Request File for VeriSign

When you do not have a VeriSign certificate, you need to create a certificate signing request (CSR) file and send it to VeriSign to purchase an SSL certificate. The the software 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.

FIGURE 65 Fill in the boxes to create the Certificate Signing Request



2. In the text boxes provided, fill in the following information:
   a) **Common Name**: Type the fully qualified domain name of your Web server.

      This must be an exact match (for example, `www.ruckuswireless.com`).

   b) **Organization**: Type the complete legal name of your organization (for example, `Ruckus Wireless, Inc.`).

      Do not abbreviate your organization name.

   c) **Organization Unit**: Type the name of the division, department, or section in your organization that manages network security (for example, `Network Management`).

   d) **Locality or City**: Type the city where your organization is legally located (for example,).

   e) **State/Province**: Type the state or province where your organization is legally located (for example, California). Do not abbreviate the state or province name.

   f) **Country**: Type the two-letter ISO abbreviation for your country (for example, if your organization is located in the United States, type `US`).

   g) **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.

   h) **Confirm password**: Retype the key pair password to confirm.

   i) **Key Size**: Select the required key size--1024 or 2048.

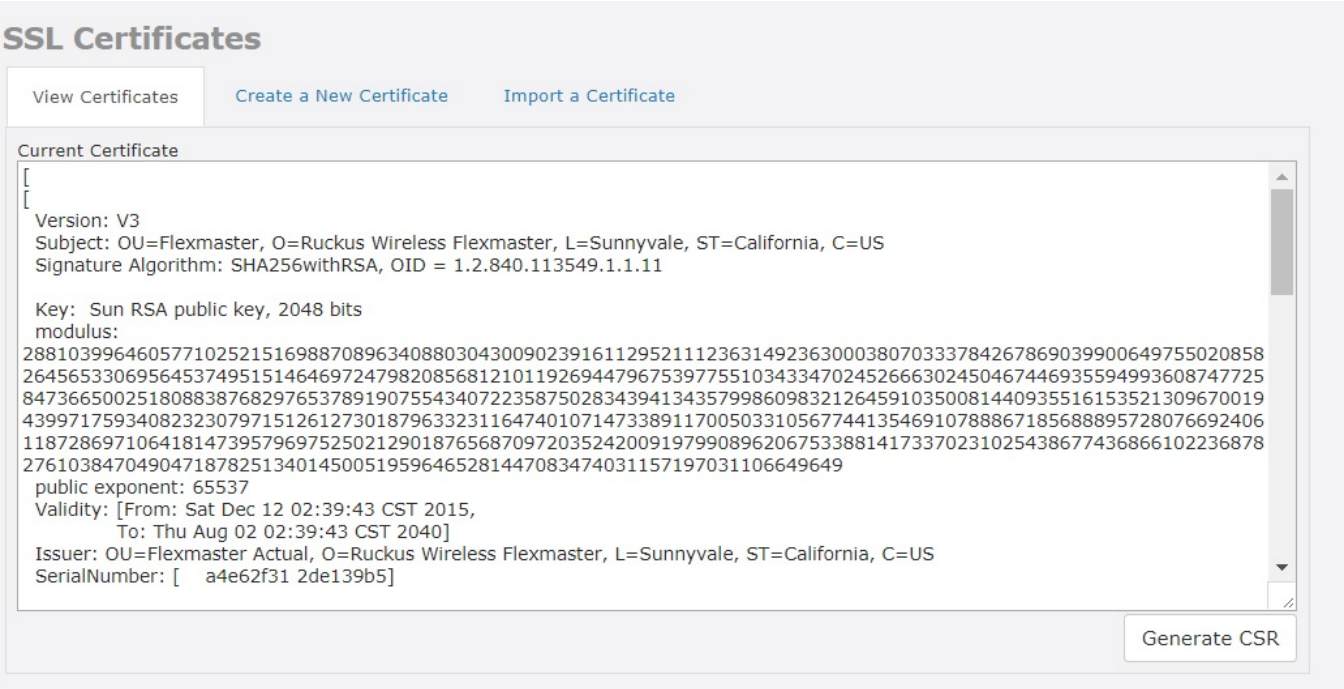
      ATTENTION
      Remember the key pair password that you set in this procedure. You need to enter this password when you import the SSL certificate that VeriSign sends you into Unleashed Multi-Site Manager.

3. Click **Create**.

   The **New Certificate Information** page appears, displaying a summary of the certificate information that you entered. If you find any incorrect information or if you want to edit the certificate information, then click **Remove Certificate**, and then start over with Step 1. If the certificate information is correct, then continue to Step 4.

4. Click **Generate CSR**. The page refreshes, and then displays the content of the CSR.

FIGURE 66 The default SSL certificate on the software



5. Copy the complete content of the CSR request, and then paste it into a text editor (for example, Notepad). Save the file.
6. Go to the VeriSign Web site and follow the instructions for purchasing an SSL certificate.

   For more information, visit: www.verisign.com/ssl/buy-ssl-certificates/index.html
7. When the VeriSign Web site prompts for the certificate signing request, copy and paste the content of the text file that you saved in Step 5, and then complete the certificate purchase.

   After VeriSign approves your CSR, you receive the VeriSign-signed certificate via email. The following is a sample signed certificate that you receive from VeriSign:

```
-----BEGIN CERTIFICATE-----
MIIFVjCCBD6gAwIBAgIQLfaGuqKukMumWhbVf5v4vDANBgkqhkiG9w0BAQUFADCB
sDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
BgEFBQcBAQRtMGswJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlzaWduLmNv
bTBDBggrBgEFBQcwAoY3aHR0cDovL1NWUlNlY3VyZS1haWEudmVyaXNpZ24uY29t
L1NWUlNlY3VyZTIwMDUtYWlhLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFowWDBW
FglpbWFnZS9naWYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEFGDAm
FiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZIhvcN AQEFBQADggEBAI/S2dmm/
kgPeVAlsIHmx751o4oq8+fwehRDBmQDaKiBvVXGZ5ZM noc3DMyDjx0SrI9lkPsn223CV3UVBZo385g1T4iKwXgcQ7/
WF6QcUYOE6HK+4ZGc HermFf3fv3C1FoCjq+zEu8ZboUf3fWbGprGRA+MR/dDI1dTPtSUG7/zWjXO5jC// 0pykSldW/
q8hgO8kq30S8JzCwkqrXJfQ050N4TJtgb/YC4gwH3BuB9wqpRjUahTi K1V1ju9bHB
+bFkMWIIMIXc1Js62JClWzwFgaGUS2DLE8xICQ3wU1ez8RUPGnwSxA YtZ2N7zDxYDP2tEiO5j2cXY7O8mR3ni0C30=
-----END CERTIFICATE-----
```

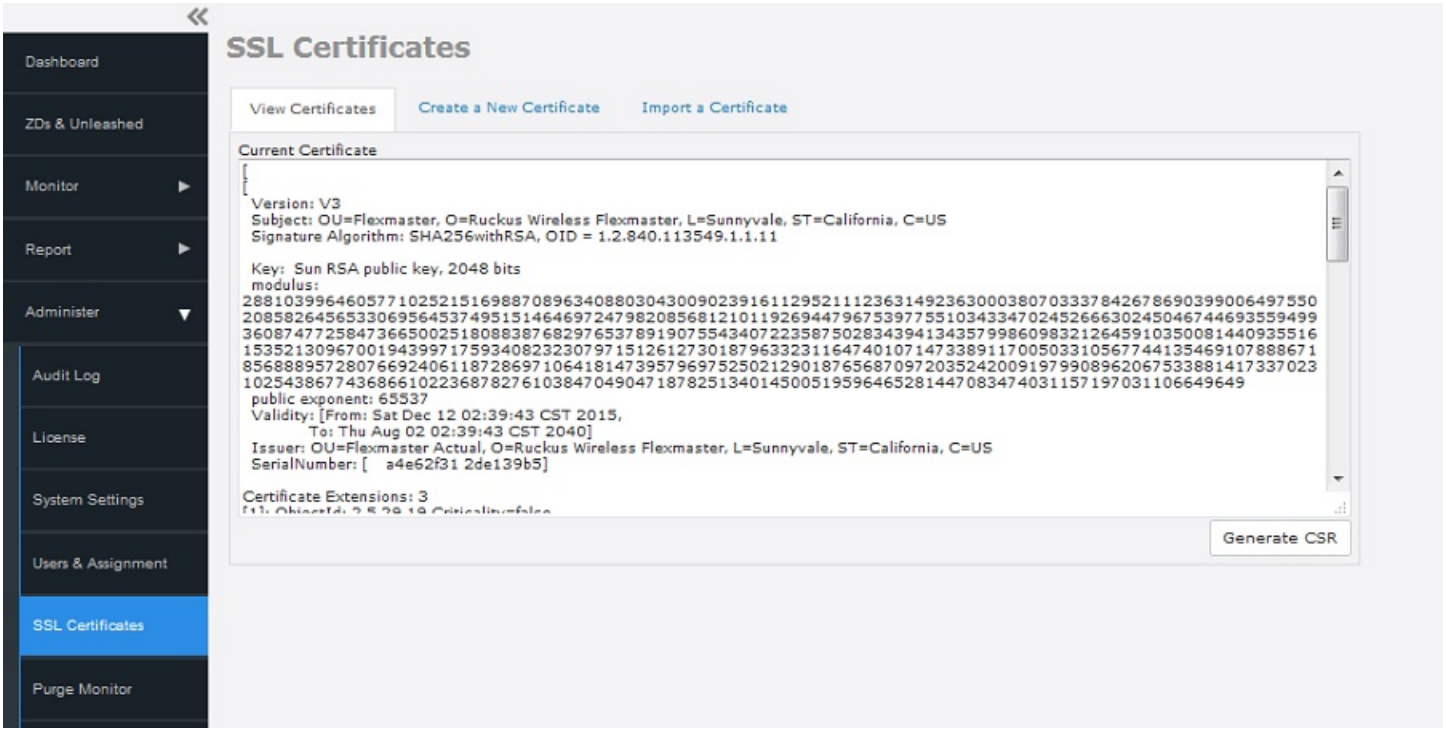
8. Copy the content of the signed certificate, and then paste it into a text file. Save the file.

You can now import the signed certificate from VeriSign into your the software server. For instructions, refer to Importing an SSL Certificate on page 108.

Viewing Current Certificates

To view the details of the certificate file that the software is currently using, click the **View Certificates** tab on the **SSL Certificates** page. If you imported a VeriSign- signed SSL certificate, then the current certificate should show VeriSign as the certificate issuer.

FIGURE 67 The default SSL certificate on the software



Upgrading the Software

Ruckus may periodically release the software updates that contain feature enhancements or fixes for known issues. These software updates are made available on the Ruckus Support Web site or released through authorized channels.

Update files typically use `{version number}.patch` for their file naming convention (for example, `9.12.0.0.11.patch`).

ATTENTION
Although the software update process has been designed to preserve all software configuration settings, Ruckus strongly recommends that you back up the software database, in case the update process fails for any reason.

NOTE
After you upgrade your software 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 software version and delete the old templates.

1. Log in to the host server as root.
2. Insert the Unleashed Multi-Site Manager upgrade CD into the CD-ROM drive.
3. If the software server does not automatically mount the software 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, `9.12.0.0.11.patch.tar`) to the software server.
7. Copy the patch file to the Unleashed Multi-Site Manager folder `/opt/UMM/`:

```
# cp 9.12.0.0.11.patch.tar /opt/UMM/
```

8. Untar the patch file with following command:

```
# tar -vxf 9.12.0.0.11.patch.tar
```

9. Make sure that the `{version number}.patch` file, such as `9.12.0.0.11.patch`, has been extracted from the tar file.
10. Upgrade Unleashed Multi-Site Manager with following command:

```
# ./upgrade.sh 9.12.0.0.11
```

11. If the software upgrade fails for any reason, then send the upgrade log file, `/opt/UMM/9.12.0.0.11.patch`, and the screen dump to Ruckus Support.

    ATTENTION
    After installing a software update, Ruckus recommends backing up the software database so you have a backup of the updated database schema. Refer to Backing Up and Restoring the Database from the Web Interface on page 117 or Backing Up the Database from the Command Line Interface on page 26 for more information.

Recovering Unleashed Multi-Site Manager from an Unsuccessful Software Update

If the software update fails for any reason, then the software update script is designed to automatically recover and restore your previous software installation. If the auto restore process also fails, then you can still restore your previous software installation manually from the database that you backed up.

To recover your software installation manually, do the following:

1. Remove the Unsuccessful Unleashed Multi-Site Manager Installation.
2. Reinstall the Previous Unleashed Multi-Site Manager Software Version.
3. Restore the Backup Unleashed Multi-Site Manager Database.

Step 1: Remove the Unsuccessful Software Installation

1. Log in to the Unleashed Multi-Site Manager server.
2. Execute the Unleashed Multi-Site Manager 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 software 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/UMM` directory.

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

Step 2: Reinstall the Previous Software Version

Follow the Unleashed Multi-Site Manager installation instructions described in Installing the Software on page 22.

Step 4: Restore the Backup Software Database

Before starting this procedure, take note of the file path to the software 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 software database.

.

1. On the Linux server, go to the software root directory (`/opt/UMM`), 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 software database backup file that you want to restore.

   For example, when you want to restore a backup file named `Mybackup.tgz` that is located in the software 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 software database that you specified has been restored successfully.

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 software database from a backup file.

Backing Up the Database from the Web Interface

ATTENTION
This procedure halts the software operation. Do not perform this procedure when you need the software to be operating properly.

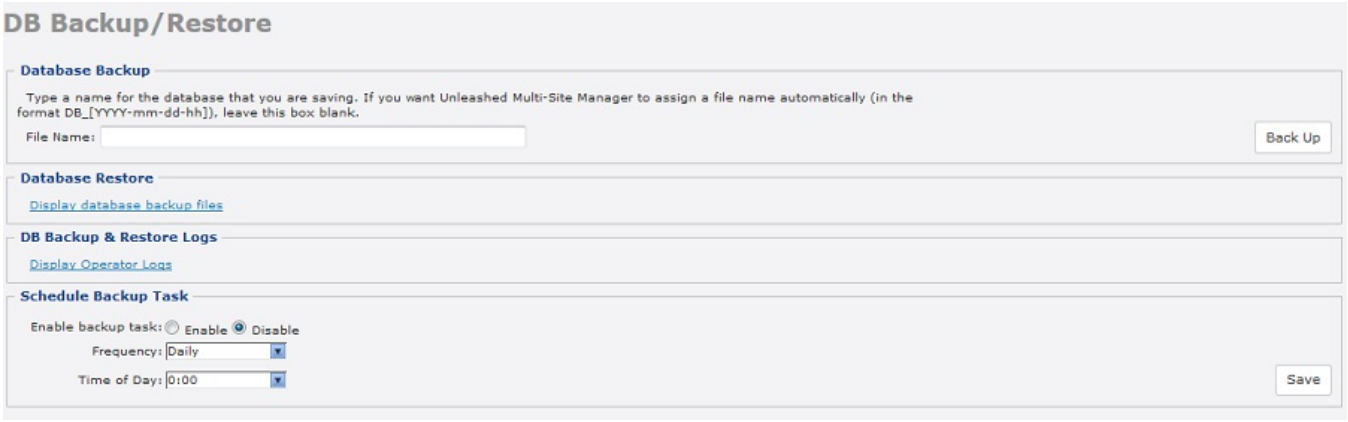
1. Go to **Administer** > **Support** and record the software version number (such as 9.12.0.0.11).
2. Go to **Administer** > **DB Backup/Restore.**.
3. Look for the **Database Backup** section.
4. In **File Name**, type a name that you want to assign to the backup file, using the format `DB_[Unleashed Multi-Site Manager version number]_[YYYY-mm-dd-hh]`. For example, the backup file name might be `DB_9.12.0.0.11 2015-06-21-02`. (Including the software version number version number can make it easier to upgrade and downgrade the software database files.)

   Do not allow software to automatically assign a file name (in the format `DB_[YYYY-mm-dd-hh]`, because the automatically assigned file name does not include the software version number.

   ATTENTION
   This procedure halts software operation. Do not perform this procedure when you need the software to be operating properly.

5. Click **Back Up**. The **BACKUP STATUS AREA** window appears and displays the progress of the backup process.

FIGURE 68 The Backup Status Area shows the progress of the backup process



6. Unleashed Multi-Site Manager backs up its database and reboots its server. Wait for this reboot to complete, and then log back into the software web interface.

   ATTENTION
   Do not navigate away from the **DB Backup/Restore** page while the backup process is in progress. Doing so cancels the backup process.

You have backed up the software database.

Scheduling Database Backup

You can also configure the software 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 the software to automatically back up the database. Options include **Daily**, **Weekly**, and **Monthly**.
5. Configure additional options for the **Frequency** option that you clicked.
   - If you clicked **Daily**, then set the **Time of Day** when you want the software to back up the database.
   - If you clicked **Weekly**, then set the **Day of the Week** and **Time of Day** when you want the software to back up the database.
   - If you clicked **Monthly**, then set the **Day of the Month** and **Time of Day** when you want the software to back up the database.
6. Click **Save**.

You have completed configuring the software to back up its database automatically.

Viewing and Deleting Database Backup Files

1. Go to **Administer** > **DB Backup/Restore.**.
2. Look for the **Database Restore** section.
3. Click the **Display database backup files** link.

   A table appears, displaying the file names of the database backup files and the dates when they were created.
4. To delete a database backup file, click the option button next to the database file name, and then click **Delete**.

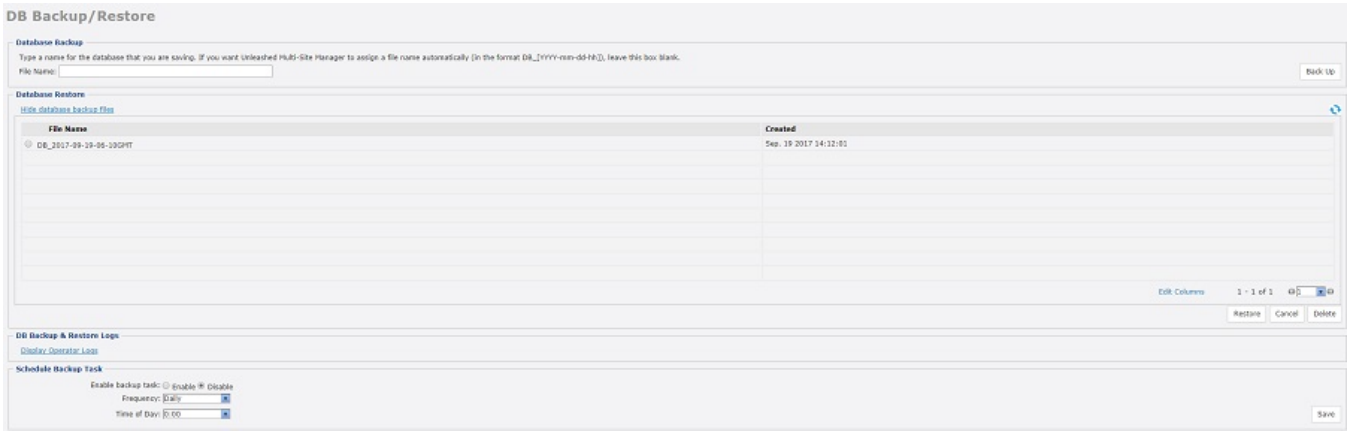
Restoring a Backup Copy of the Database

1. Go to **Administer** > **DB Backup/Restore.**.
2. Look for the Database Restore section.
3. Click the **Display database backup files** link.

   A table appears and displays the file names of the database backup files and the dates when they were created.

4. Click the **option** button next to the database file name that you want to restore.

FIGURE 69 The Database Restore screen



5. Click **Restore**.

   The **Restore Status Area** window appears and displays the progress of the restore process.

6. Check the **Restore Status Area** window for the following message:

```
restore db completed...success. Please wait for system restart automatically.
Unleashed Multi-Site Manager DB has been restored with {UMM-database-file-name}.tgz
```

7. Wait for the software login page to appear.

When the login page appears, you have completed restoring the backup database.

Generating Support Information

When you request technical support from Ruckus, you may be asked to collect information about Unleashed Multi-Site Manager that may help Ruckus troubleshoot the issue. You need to generate system logs.

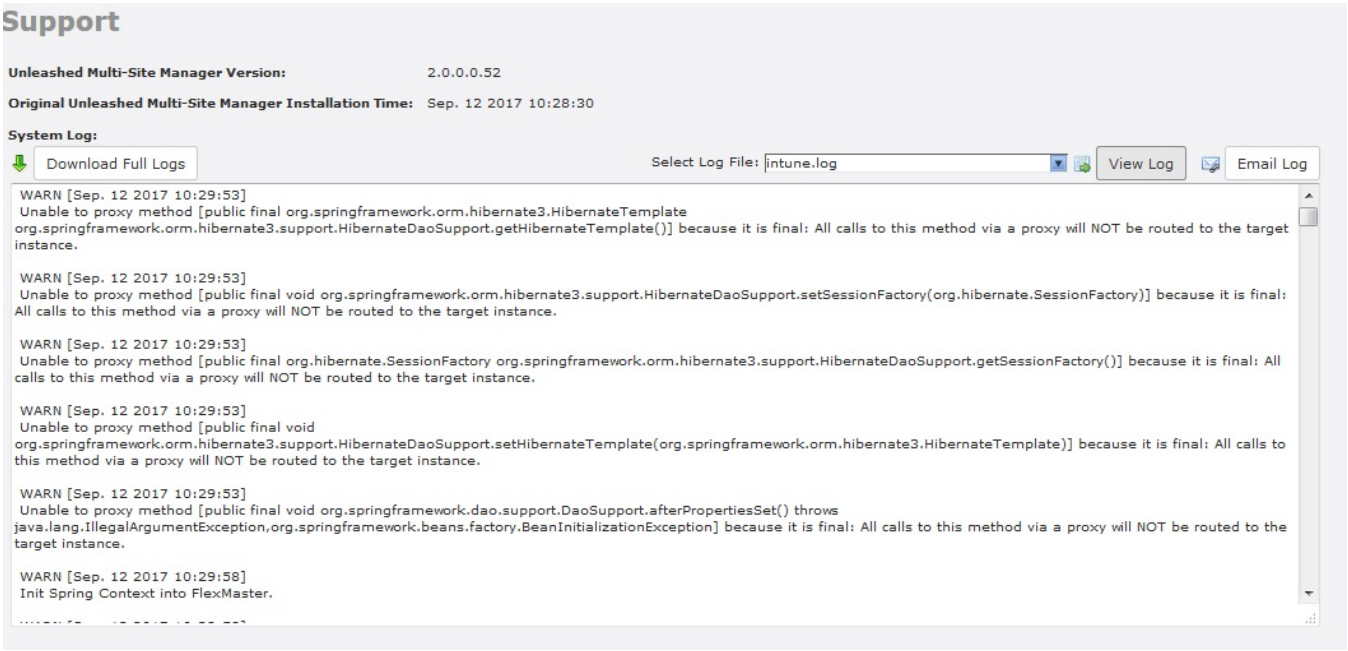
Viewing System Logs

The system log captures information in 12-hour sets. After 12 hours, the “expired” log is backed up and a new log is started. This log rotation prevents the system log from becoming too long. New logs start at midnight (12:00 AM or 0:00) and midday (12:00 PM).

1. Go to **Administer** > **Support**.
2. In **Select Log File**, select the required log file.

3. Click **View Log**. The log displays information from either midnight to the current time or midday to current time.

FIGURE 70 Viewing a system log file



Downloading System Logs

1. Go to **Administer** > **Support**.
2. Click **Download Full Logs**.

Unleashed Multi-Site Manager zips all the existing log files and downloads the `umm_logs.zip` file to your client workstation.

NOTE
If the software web page is not available, please retrieve the log file from `/opt/UMM/3rdparty/tomcat/apache-tomcat-6.0.18/webapps/intune/WEB-INF/logs/`. Backed-up logs appear as (midnight) `Unleashed Multi-Site Manager.log.yyyy-mm-dd-AM` or (midday) `Unleashed Multi-Site Manager.log.yyyy-mm-dd-PM`.

Emailing a Copy of the System Log File

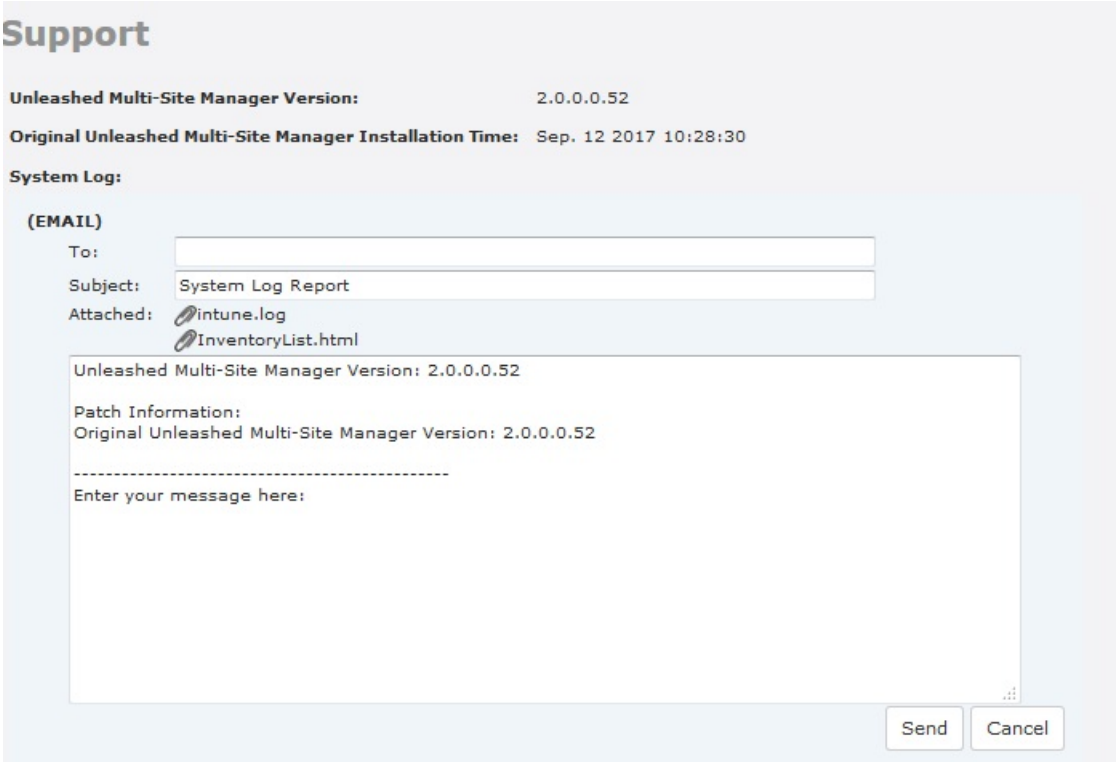
1. Go to **Administer** > **Support**.
2. Click the **Email Log** button. The **System Log** form appears.

   The **To** and **Subject** fields are filled out, and the system log has been added as attachment.

   The **To** address must be previously configured in the System Settings. Please refer to Configuring System Settings on page 94.
3. Type any information you want to highlight in the message box.

4. Click **Send** to send the email message.

FIGURE 71 Sending the system log via email



NOTE
If the software web page is not available, please send the log file from `/opt/UMM/3rdparty/tomcat/apache-tomcat-6.0.18/ webapps/intune/WEB-INF/logs/`. Backed-up logs appear as (midnight) `Unleashed Multi-Site Manager.log.yyyy-mm-dd-AM` or (midday) `Unleashed Multi-Site Manager.log.yyyy-mm-dd-PM`.

Manually Transferring Files

There may be times when you would like to manually transfer log and other files between a Windows workstation and a software server. Ruckus recommends that you use a free Windows file transfer tool, **WinSCP**, or equivalent, to simplify the file transfers. WinSCP can be downloaded from https://winscp.net/eng/download.php and installed on your Windows workstation.

To transfer files to the Windows workstation:

1. Launch WinSCP and log in with the following selections:
   - *File Protocol*: **SFTP**, **SCP** or **FTP**
   - *Encryption*: **None**, **SSL/TLS Implicit**, **SSL Explicit** or **TLS Explicit**
   - *Host Name*
   - *Port number*
   - *User name*
   - *Password*
   - *Account*
   - *Anonymous login*
2. In the WinSCP window, find the required files and transfer them to the Windows workstation.

   The most common software log files are:
   - `/opt/UMM/<version number>.patch.log`
   - `/opt/UMM/install.log`
   - `/opt/UMM/3rdparty/tomcat/apache-tomcat-<version>/webapps/intune/WEB-INF/logs/Unleashed Multi-Site Manager.log`
   - `/opt/UMM/3rdparty/tomcat/apache-tomcat- <version>/webapps/intune/WEB-INF/logs/Intune.log`
   - `/tmp/<ZD log file name>.xml`
   - `/opt/UMM/3rdparty/tomcat/httpshellproxy/logs/<logname>.log`
   - `/opt/UMM/3rdparty/tomcat/apache-tomcat-<version>/webapps/intune/WEB-INF/ZDWebUtils/instances/$<instance_port_number>/webs.log`

After you have transferred the file(s), you can use them as directed by Ruckus Support.

Appendix

Enabling Unleashed Multi-Site Manager Management on Unleashed Devices

To allow Unleashed Multi-Site Manager to monitor and manage Unleashed devices, you must enable software management in the Unleashed device and register the device with Unleashed Multi-Site Manager.

1. Upload the Unleashed license as described in Uploading a License File on page 94.

2. Generate and Apply the Unleashed ID: Each unleashed network has an ID which is automatically generated by the system. You can renew this ID by clicking **Generate** from the Unleashed web interface and then apply it to the network. The 'Unleashed ID' is reset during set factory, and overwritten when the configuration is restored (when you choose the restore option as Restore everything). Unleashed Multi-Site Manager uses the 'Unleashed ID' to identify the unleashed network, and whenever the 'Unleashed ID' is renewed or reset, Unleashed Multi-Site Manager regards it as a new unleashed device.

FIGURE 72 Generating Unleashed ID

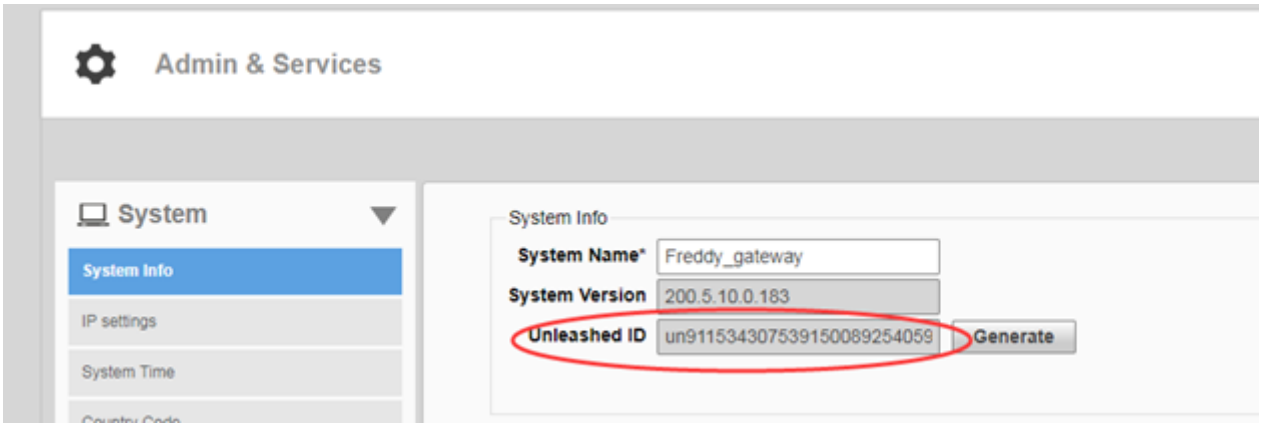
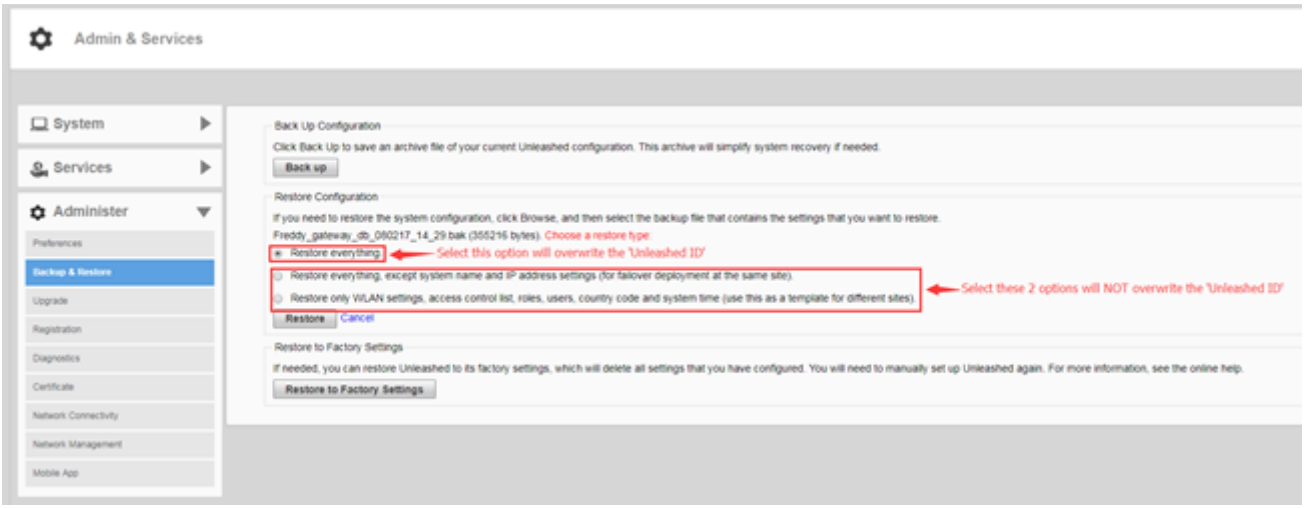


FIGURE 73 Unleashed - Restore Configuration

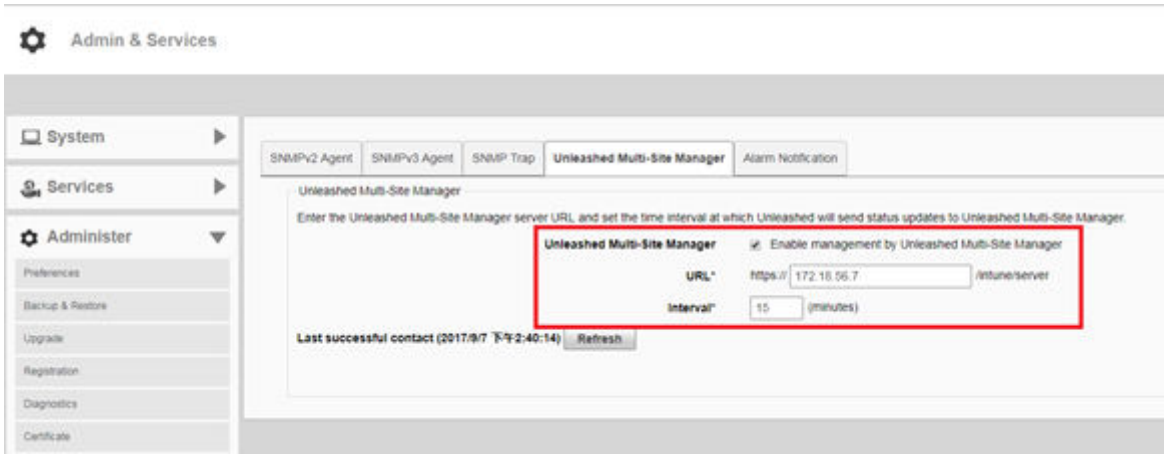


3. Enable software management from Unleashed web interface:
   a) Go to **Admin & Services** > **Administer** > **Network Management** > **Unleashed Multi-Site Manager Management**.
   b) Select the **Enable management by Unleashed Multi-Site Manager** check-box.

      Configure the following:

      - URL: The IP address or URL of the software server.
      - Interval: the time interval (in minutes) within which the Unleashed device sends the TR069 information to Unleashed Multi-Site Manager. It is recommended that you configure this interval according to your network capacity.

FIGURE 74 Enabling Unleashed Multi-Site Manager Management



4. Login to the Unleashed Multi-Site Manager web interface and go to **ZDs & Unleashed**. The Unleashed device will be registered and displayed.

You have successfully enabled software management in the Unleashed network, and registered the Unleashed device for Unleashed Multi-Site Manager to monitor.

Enabling Unleashed Multi-Site Manager Management on ZoneDirector

To allow Unleashed Multi-Site Manager to monitor and manage ZoneDirector devices, you must enable software management in the ZoneDirector device and register the device with Unleashed Multi-Site Manager.

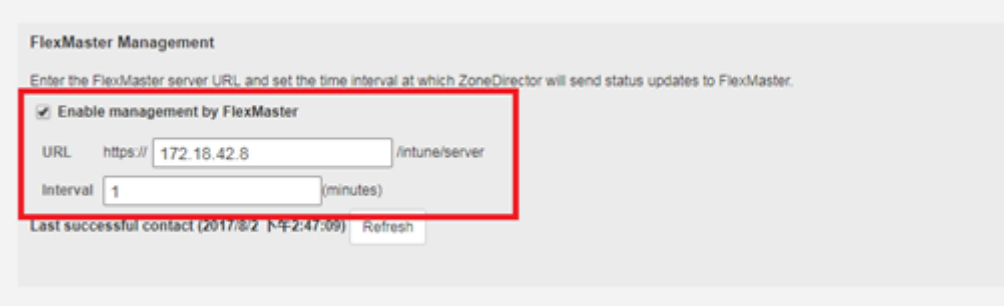
1. Upload the ZoneDirector license as described in Uploading a License File on page 94.

2. Enable Unleashed Multi-Site Manager management from ZoneDirector web interface:
   a) Go to **Configure** > **System** > **Network Management**.
   b) In **FlexMaster Management**, select the **Enable management by FlexMaster** check-box.

      Configure the following:

      - URL: The IP address or URL of the software server.
      - Interval: the time interval (in minutes) within which the ZoneDirector device sends the TR069 information to the Unleashed Multi-Site Manager. It is recommended that you configure this interval according to your network capacity.

FIGURE 75 Enabling Unleashed Multi-Site Manager Management



3. Login to the software web interface and go to **ZDs & Unleashed**. The ZoneDirector device will be registered and displayed.

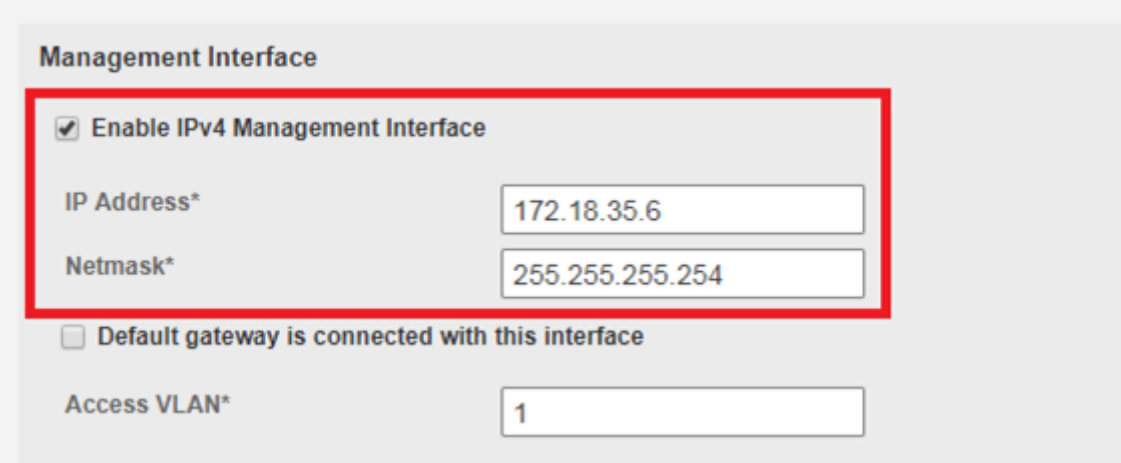
You have successfully enabled software management in the ZoneDirector device, and registered the ZoneDirector device for Unleashed Multi-Site Manager to monitor.

Managing Devices behind the NAT Server

You can manage ZoneDirector and Unleashed devices behind the NAT server by enabling managing these devices from the web interface and configuring ports for communication.

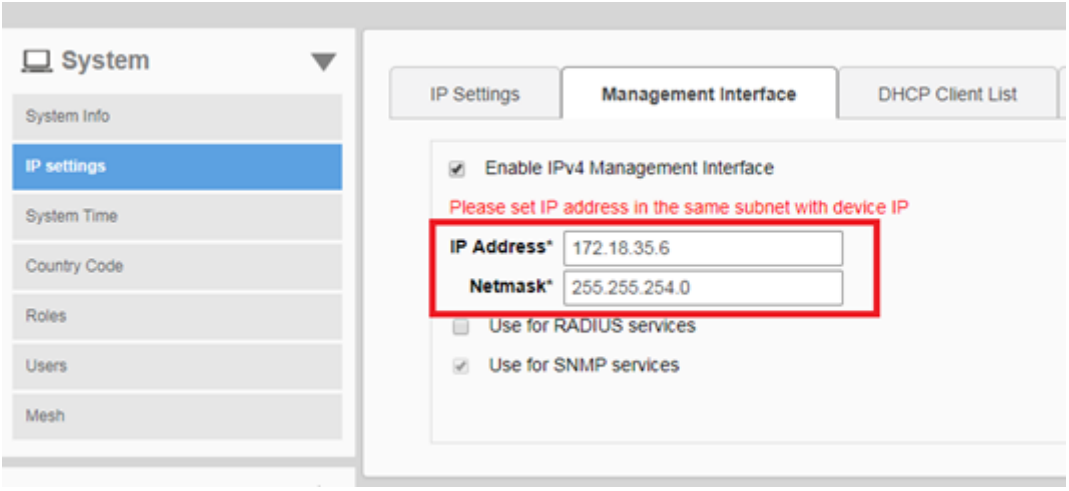
1. From the web interface of the device, configure the management interface according to your network.
   - From the ZoneDirector web interface, go to **Configure** > **System** > **Management Interface**.

     FIGURE 76 Management Interface - ZoneDirector Web Interface



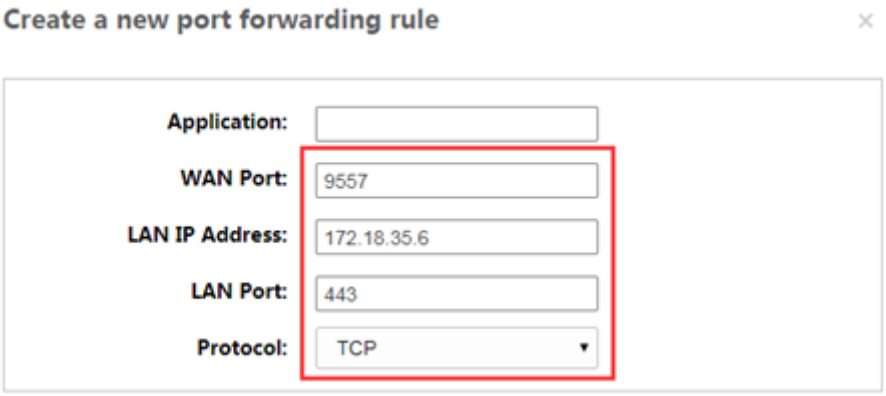
   - If you are accessing the Unleashed web interface, then go to **Admin & Services** > **System** > **IP Setting** > **Management Interface**.

     FIGURE 77 Management Interface - Unleashed Web Interface



2. Login to the NAT server and map the LAN port to 443.

FIGURE 78 Sample Port Mapping



3. Enable Unleashed Multi-Site Manager management. Refer to Enabling Unleashed Multi-Site Manager Management on Unleashed Devices on page 125 or Enabling Unleashed Multi-Site Manager Management on ZoneDirector on page 127 as appropriate.
4. From the software web interface, select the device behind the NAT server and edit the port number based on the settings configured in step 2. For more information, see Editing Device Properties on page 45.

350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com