USER GUIDE

Ruckus Unleashed Multi-Site Manager User Guide, 2.1

Supporting Unleashed Multi-Site Manager Release 2.1

Part Number: 800-71846-001 Rev B
Publication Date: 27 July 2018

Copyright, Trademark and Proprietary Rights Information

© 2018 ARRIS Enterprises LLC. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from ARRIS International plc and/or its affiliates ("ARRIS"). ARRIS reserves the right to revise or change this content from time to time without obligation on the part of ARRIS to provide notification of such revision or change.

Export Restrictions

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, ARRIS 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. ARRIS 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. ARRIS 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 ARRIS 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 ARRIS, ARRIS AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF ARRIS 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. 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

ARRIS, the ARRIS logo, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface **7**
- Document Conventions 7
  - Notes, Cautions, and Warnings 7
- Command Syntax Conventions 8
- Document Feedback 8
- Ruckus Product Documentation Resources 8
- Online Training Resources 9
- Contacting Ruckus Customer Services and Support 9
  - What Support Do I Need? 9
  - Open a Case 9
  - Self-Service Resources 9

About This Guide **11**
- Introduction to Unleashed Multi-Site Manager 11
- Related Documentation 11

Introducing Ruckus Unleashed Multi-Site Manager **13**
- Unleashed Multi-Site Manager Overview 13
- Management Software and Server 13
  - Event Times 13
  - Management Protocol 14
  - Internet Accessibility 14
- Where Should You Place Unleashed Multi-Site Manager? 14
- Key Terms 14

Installing and Upgrading Unleashed Multi-Site Manager **15**
- Firewall Ports that Must Be Open for Communications 15
- Administering a Linux Server 16
  - Preparing the Server for Software Installation 16
  - Editing the Server Hosts File 17
  - Installing the Software 18
  - Notable Files in the Software Root Directory 21
  - Upgrading the Software 21
  - Uninstalling the Software 22
  - Backing Up the Database from the Command Line Interface 22
  - Restoring the Database from the Command Line Interface 23
- After Installation 23

Getting Started with Unleashed Multi-Site Manager **25**
- Logging In to Unleashed Multi-Site Manager 25
- Features of the Web Interface 27
- Getting to Know the Dashboard 28
- Getting Started Tasks 32
  - Changing the Default Administrative Password 32
  - Pointing a ZoneDirector or Unleashed Network to Unleashed Multi-Site Manager 33
  - Checking Your Software License 34

Working with ZoneDirector Controllers and Unleashed APs **35**
- Viewing Devices Managed by the Software 35

Viewing the Device Configuration....39
Creating and Managing Groups....40
Viewing Group Details....41
Editing the Device Properties....42
Editing WLAN SSID....44
Blocking Devices from the Software....44
Backing Up Device Configuration Files....45
Restoring the Device Configuration....47
Deleting Devices Managed by the Software....49
Managing Tasks....51

Working with Reports....53
Available Report Types....53
Configuring Report Options....54
Saving Reports....55
Generating Reports....56
Generating an AP Report....56
Generating a WLAN Report....57
Generating a Client Report....58
Generating Reports for Rogue Devices....59
Viewing Saved Reports....60

Performing Administrative Tasks....63
The Administer Tab....63
Viewing Audit Logs....63
Managing Software Licenses....65
Uploading a License File....66
Managing User Accounts....67
User Roles and Privileges....67
Creating a New User Account....68
Editing a User Account....69
Deleting a User Account....70
Assigning Users to Manage Device Groups....70
Managing SSL Certificates....71
Importing an SSL Certificate....71
Creating a Certificate Signing Request File for VeriSign....76
Viewing Current Certificates....79
Upgrading the Software....81
Recovering Unleashed Multi-Site Manager from an Unsuccessful Software Update....81
Backing Up and Restoring the Database from the Web Interface....83
Backing Up the Database from the Web Interface....83
Scheduling Database Backup....84
Viewing and Deleting Database Backup Files....85
Restoring a Backup Copy of the Database....85
Generating Support Information....86
Viewing System Logs....86
Downloading System Logs....87
Emailing a Copy of the System Log File....87
Manually Transferring Files....88

System....91
Configuring System Settings....91

General Settings....93
SMTP Settings....94
Purge Policy....96
TACACS+....98
FTP Server Settings....98
SNMP Server Settings....99
Alarm Settings....103
Configuring Alarm Settings....103
User-Customized Alarms....105
Monitoring Events....106
Event Configuration....106
Appendix....111
Configuring Unleashed Multi-Site Manager Behind the NAT Server....111
Configuring Unleashed Multi-Site Manager In Front of NAT Server....112
Configuring the 200.6 Unleashed Setup....113
Configuring ZoneDirector & 200.5 Unleashed Behind NAT Server....115
Configuring ZoneDirector & 200.5 Unleashed In Front of the NAT Server....120
Setting Up Unleashed Multi-Site Manager as a Virtual Machine....122
Hardware Requirements and Specifications....133
Changing the Login Information for the Virtual Machine....133
Changing the Linux Password....133
Changing the Login Credentials to Access the Database....134

Preface

- Document Conventions 7
- Command Syntax Conventions 8
- Document Feedback 8
- Ruckus Product Documentation Resources 8
- Online Training Resources 9
- Contacting Ruckus Customer Services and Support 9

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.
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 to Unleashed Multi-Site Manager 11
- Related Documentation 11

Introduction to Unleashed Multi-Site Manager

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..... 13
- Management Software and Server..... 13
- Where Should You Place Unleashed Multi-Site Manager?..... 14
- Key Terms..... 14

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
This release of Unleashed Multi-Site Manager does not support solo APs except P300.

ATTENTION
By downloading this software and subsequently upgrading ZoneDirector, 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.
- 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, MariaDB and Elasticsearch database components for communicating with and tracking your dispersed Ruckus devices.

For the specific installation steps, refer to Installing the Software on page 18.

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

Unleashed Multi-Site Manager 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 in to 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?

Because 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.

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. You must specify an SMTP server to send email notifications to this user. Refer to SMTP Settings on page 94.

Installing and Upgrading Unleashed Multi-Site Manager

- Firewall Ports that Must Be Open for Communications....15
- Administering a Linux Server....16
- After Installation....23

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
ZoneDirector and Unleashed (Device)	
HTTPS	TCP destination port 443
HTTP	TCP destination port 80
SSH	TCP destination port 22
SSH Tunnel (nginx)	TCP destination port 9443

NOTE
If Unleashed Multi-Site Manager is behind the Nat server, you must map TCP 22, 80, 443 and 9443 ports to the Unleashed Multi-Site Manager server

NOTE
For ZD and 200.5 Unleashed devices, port 80 is used to download the configuration file from Unleashed Multi-Site Manager. Therefore, ensure port 80 is open in the firewall, otherwise, the restore task will continue to displays the status as Applying.

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)

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
     ```

  3. Before you install Unleashed Multi-Site Manager, ensure that you upgrade openssl and its lib according to their Linux version:

     RedHat/CentOS 6.x: Openssl 1.0.1 +

     RedHat/CentOS 7.x: Openssl 1.0.2 +

     A sample to upgrade Openssl version with linux yum:

     ```
     yum upgrade openssl 1.0.2
     ```

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: 30 GB dedicated to Unleashed Multi-Site Manager, minimum for 10 licenses
- RAM: 8 GB 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 160 GB 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 10 GB 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 94.

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 16.

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.

Installing from a CD-ROM

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

   If the software server does not automatically mount the CD-ROM, then continue with Step 3. If the server automatically mounts the CD-ROM, then continue with Step 5.
3. Enter the following command to create a mount point (or directory where you want to mount the CD-ROM):

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

   ```
   # mount /dev/cdrom /mnt/cdrom
   ```
5. Change directory (`cd`) to the mount point for the CD-ROM.
6. 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 User Roles and Privileges on page 67.

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:

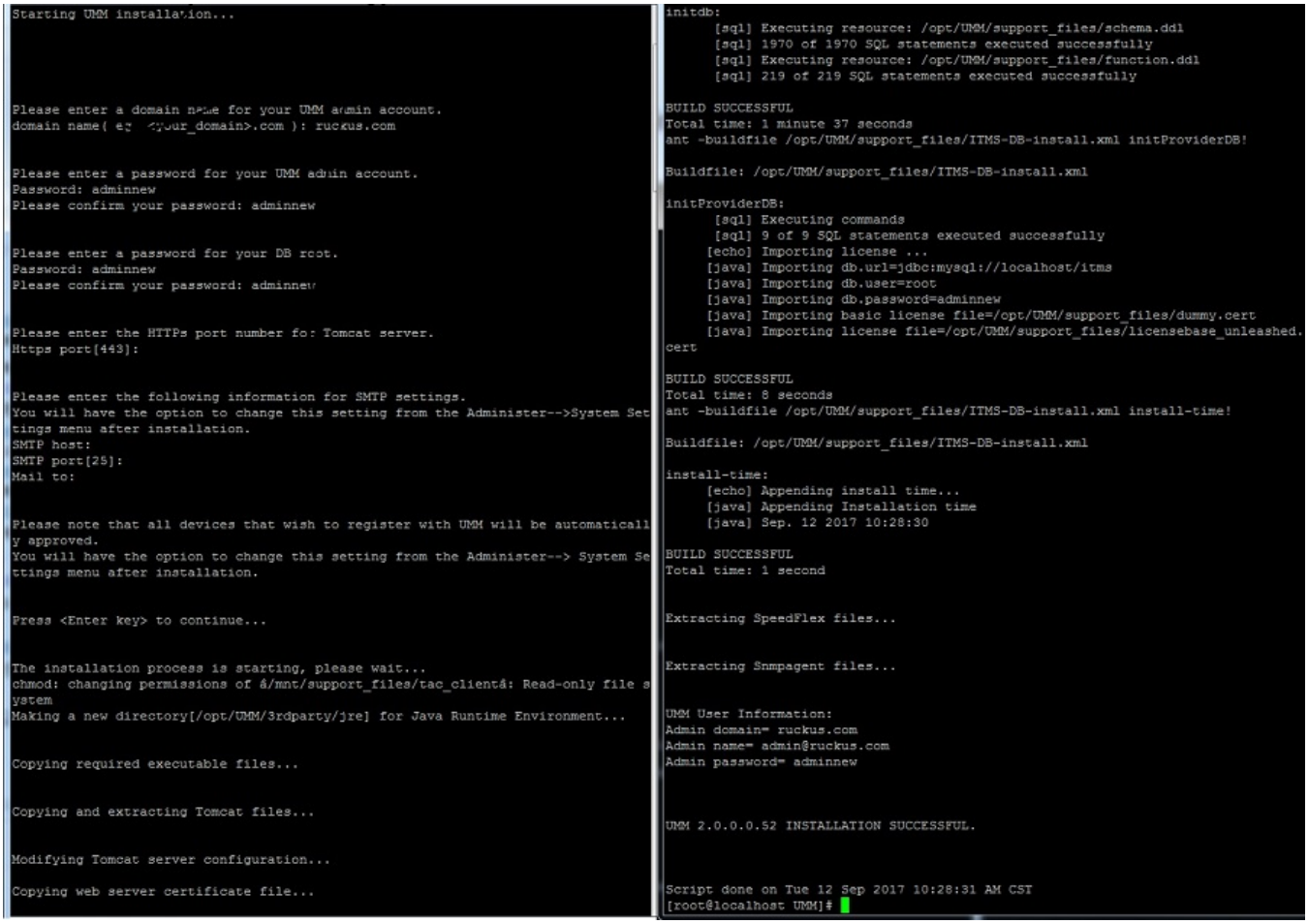
   ```
   # mount -o loop *.ISO ISO
   ```
6. Change to the ISO directory:

   ```
   # 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)



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
```

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
```

8. 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]:
```

9. 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
```

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

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

11. Enter a password for the MariaDB root account.

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

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

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

13. 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 In to Unleashed Multi-Site Manager on page 25.

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 website 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 22 and Backing Up and Restoring the Database from the Web Interface on page 83.

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 22 and Backing Up and Restoring the Database from the Web Interface on page 83.

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

Execute the software uninstall script.

```
# [root@umm UMM]# ./uninstall.sh
```

After you execute the uninstall script, it performs the following steps:

1. It shuts down the Tomcat server.
2. It shuts down the MariaDB and Elasticsearch server.
3. It deletes the configuration files, and uninstalls the software services.
4. It restores the original `/etc/my.cnf` file.
5. It finds `/etc/my.cnf.ruckus`, and then renames it to `/etc/my.cnf`.
6. 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 83

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.

After Installation

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 In to Unleashed Multi-Site Manager....25
- Features of the Web Interface....27
- Getting to Know the Dashboard....28
- Getting Started Tasks....32

Logging In to Unleashed Multi-Site Manager

Use one of the Web browsers described in Web Browser Requirements on page 17 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`

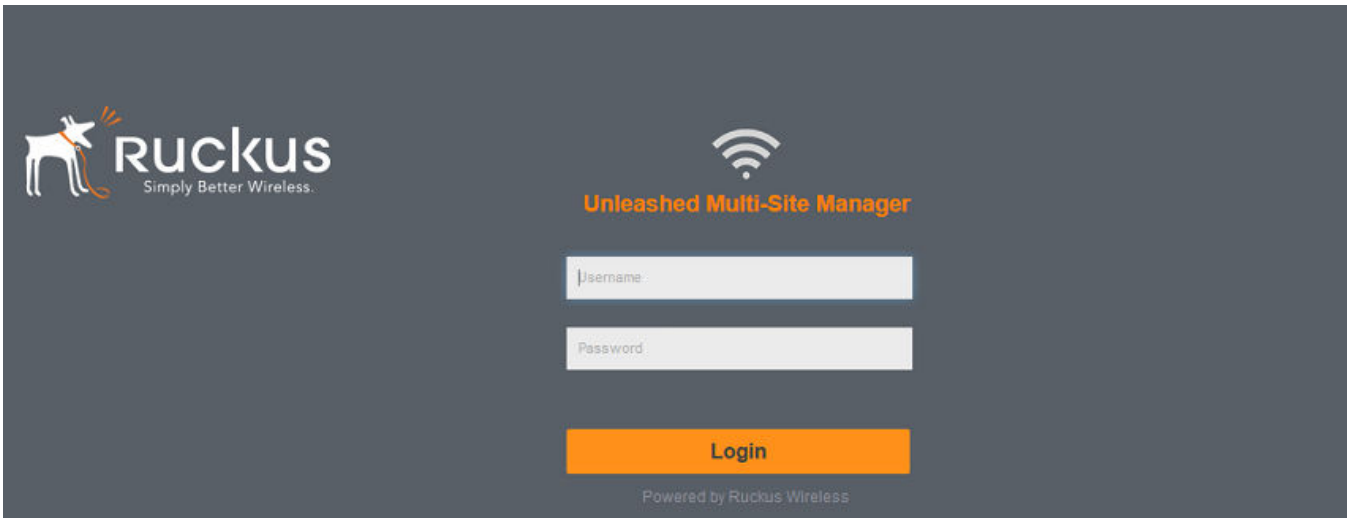
3. Press **Enter** to initiate the connection.

   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 71.

   The **Ruckus Admin** login page appears.

   FIGURE 3 Ruckus Admin 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 18). For example:

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

   Password: **`admin`**

5. If you are using remote authentication, then log in using the TACACS+ server configured in TACACS+ on page 98.

   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 28.

   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 in to 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

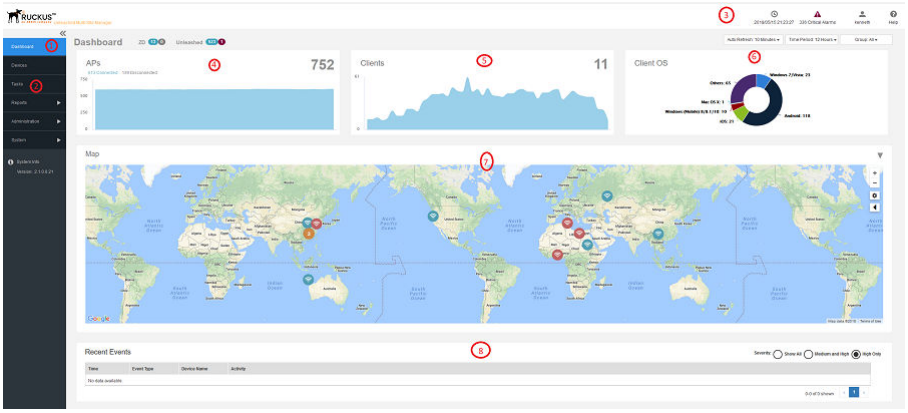


TABLE 4 Web Interface Elements

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 • Devices • Tasks • Reports • Administration • System
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.

TABLE 4 Web Interface Elements (continued)

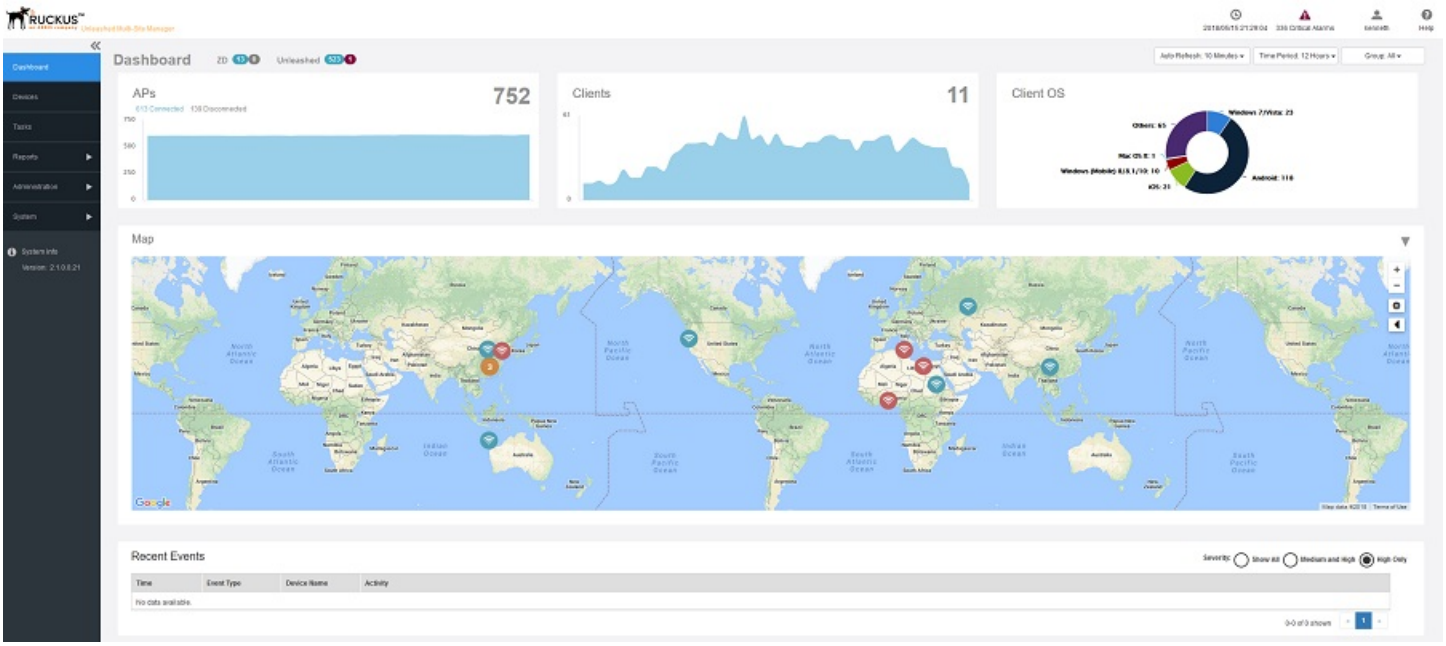
No.	Interface Element	Interface Element Description
		• Click the **Help** link to open the online help. • Click the **Log Out** link to log out of the software. The user name identifies the user who is logged in. • If Unleashed Multi-Site Manager has an active *trial* license file, then a notice appears 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 for a period of time.
6	Clients 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** or select other group which created by user.

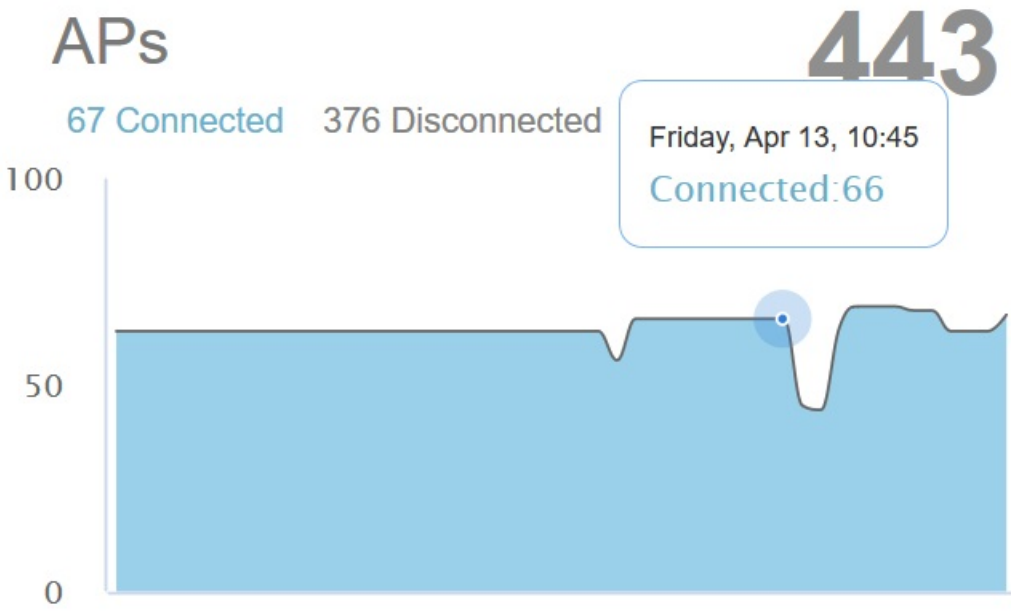
FIGURE 5 The Dashboard



The Dashboard 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).

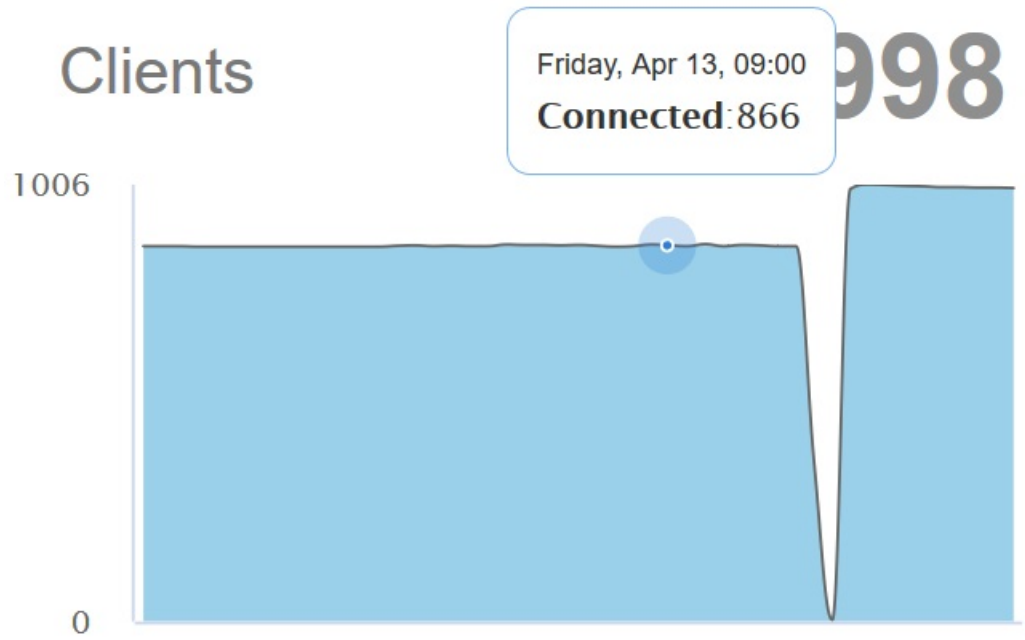
FIGURE 6 APs Graph



The graph displays the number of connected APs depending on the time period option selected. For example, if you select 12 hours, then the graph displays trends for devices connected for the last 12 hours. Pause the pointer along the graph to display the connected AP statistics at any time within the selected time range to view the respective statistics.

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

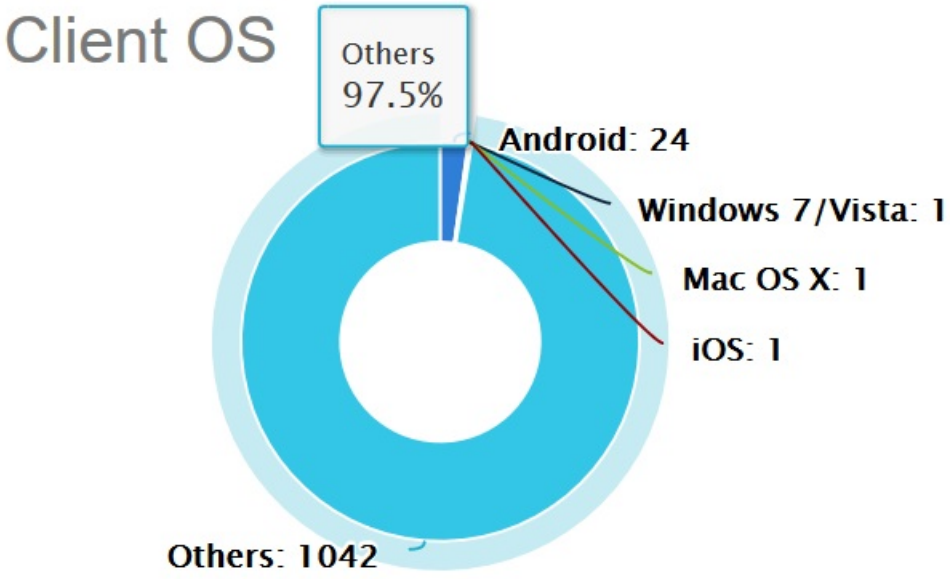
FIGURE 7 Clients Graph



Pause the pointer along the graph to display the connected clients at any time within the selected 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.

FIGURE 8 Client OS Graph



Pause the pointer on 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 percent of those devices are using the Windows operating system. Further, it also displays the percentage of various versions of each OS accessing the server.

- A map which displays the AP and device information across the globe. Pause the pointer on the AP or device to see the respective statistics.

FIGURE 9 AP and Device Information Map



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

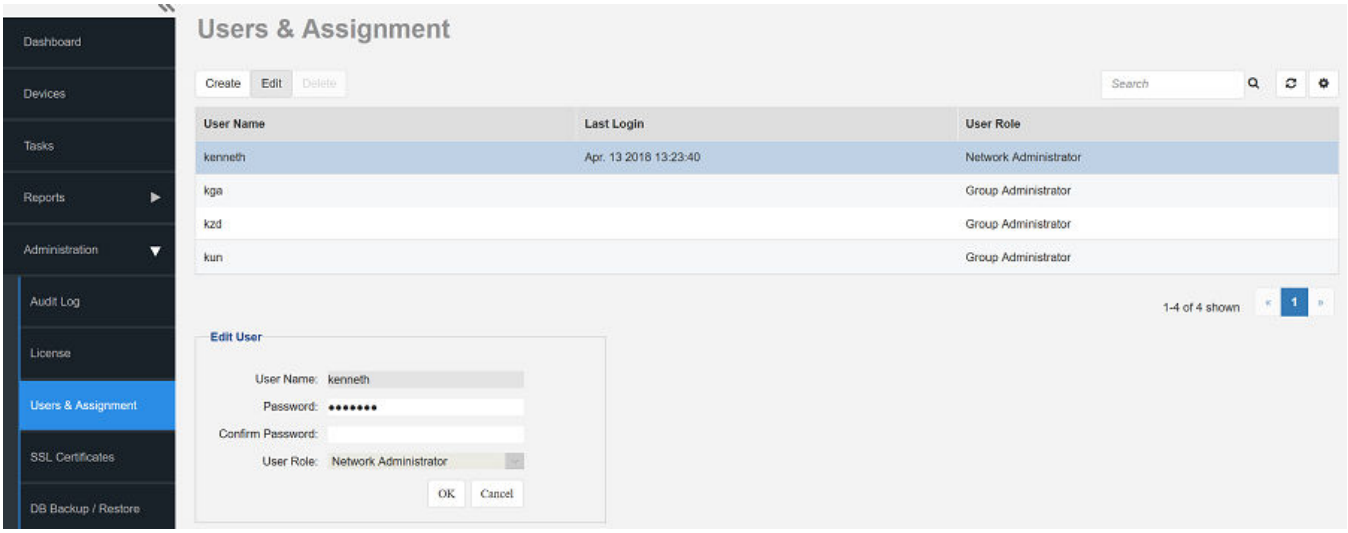
Changing the Default Administrative Password

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 **Administration** > **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 User** form appears below the table.

FIGURE 10 Editing the 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. Select the **User Role** form the drop-down menu.
7. 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 111

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 15.

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.

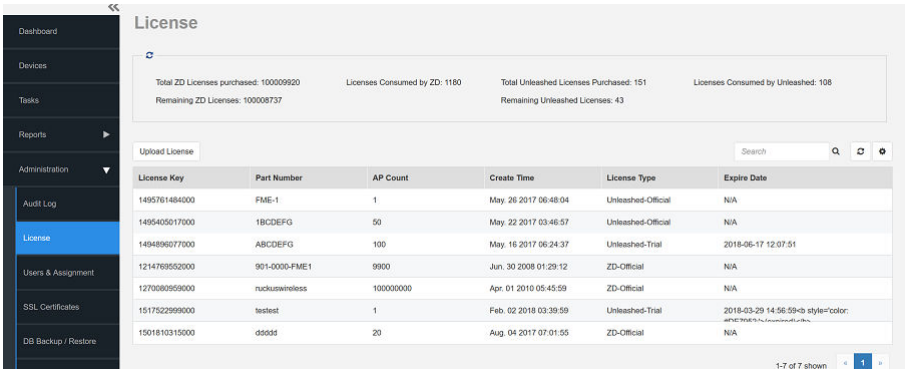
When trial licenses expire, Unleashed Multi-Site Manager checks the license number and deletes the device(s) as necessary. It does not monitor this device anymore.

> **NOTE**
> A standby ZoneDirector device will not occupy any license but on some web interfaces, the standby ZoneDirector license is displayed as 1.

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....35
- Viewing the Device Configuration....39
- Creating and Managing Groups....40
- Editing the Device Properties....42
- Editing WLAN SSID....44
- Blocking Devices from the Software.... 44
- Backing Up Device Configuration Files.... 45
- Restoring the Device Configuration.... 47
- Deleting Devices Managed by the Software....49
- Managing Tasks.... 51

Viewing Devices Managed by the Software

The **Devices** 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 log in to the web interface, select **Devices** from the menu in the left.

The **Devices** 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 Devices Managed by Unleashed Multi-Site Manager - List View

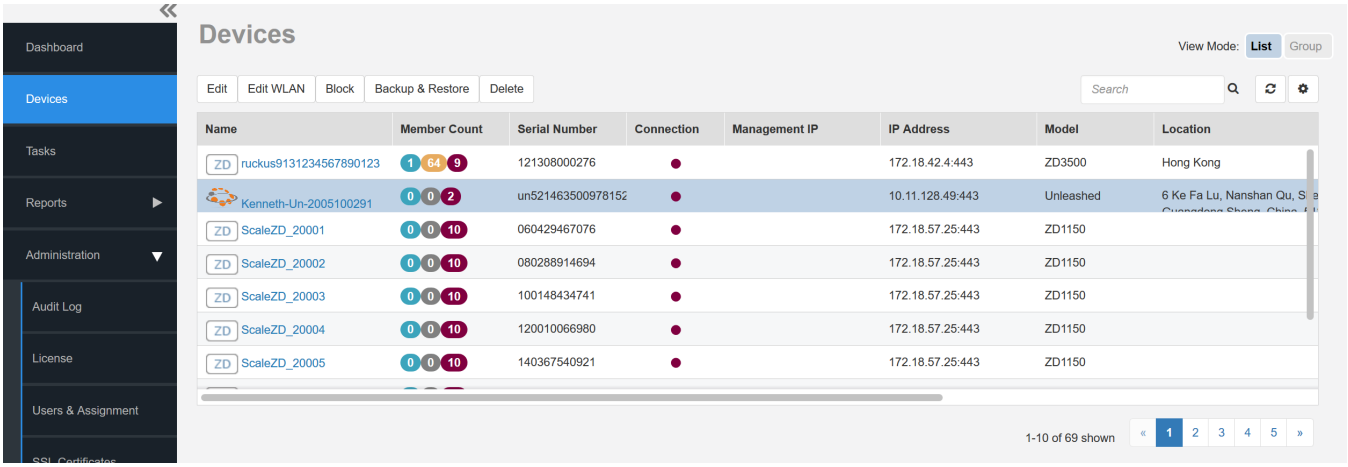
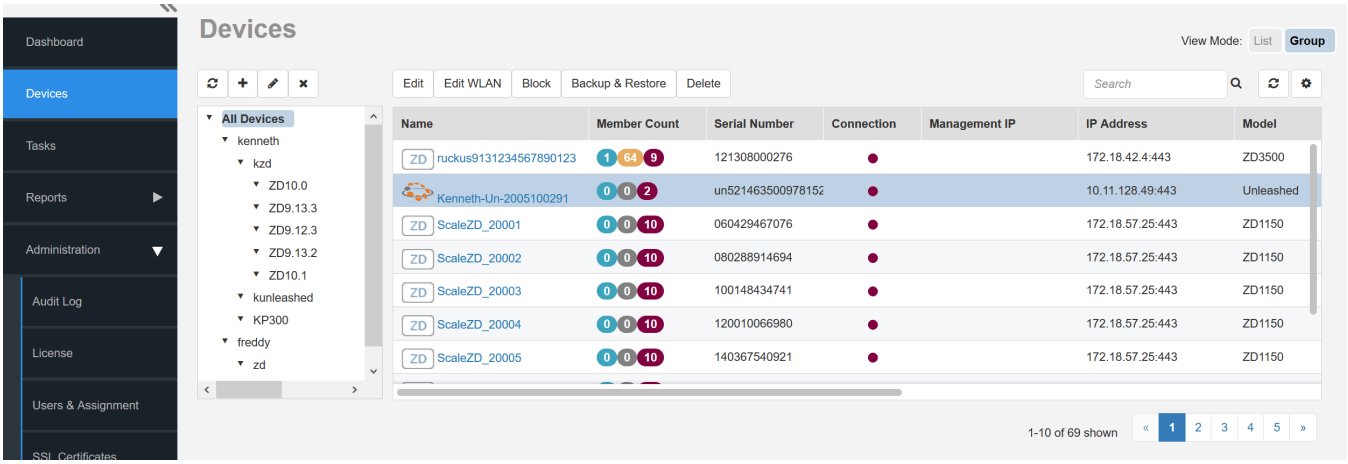


FIGURE 13 Devices Managed by Unleashed Multi-Site Manager - Group View



Click the icon to refresh the contents of the table.

The following table lists some of the fields and table columns that appear by default.

TABLE 6 Configuring Device Management

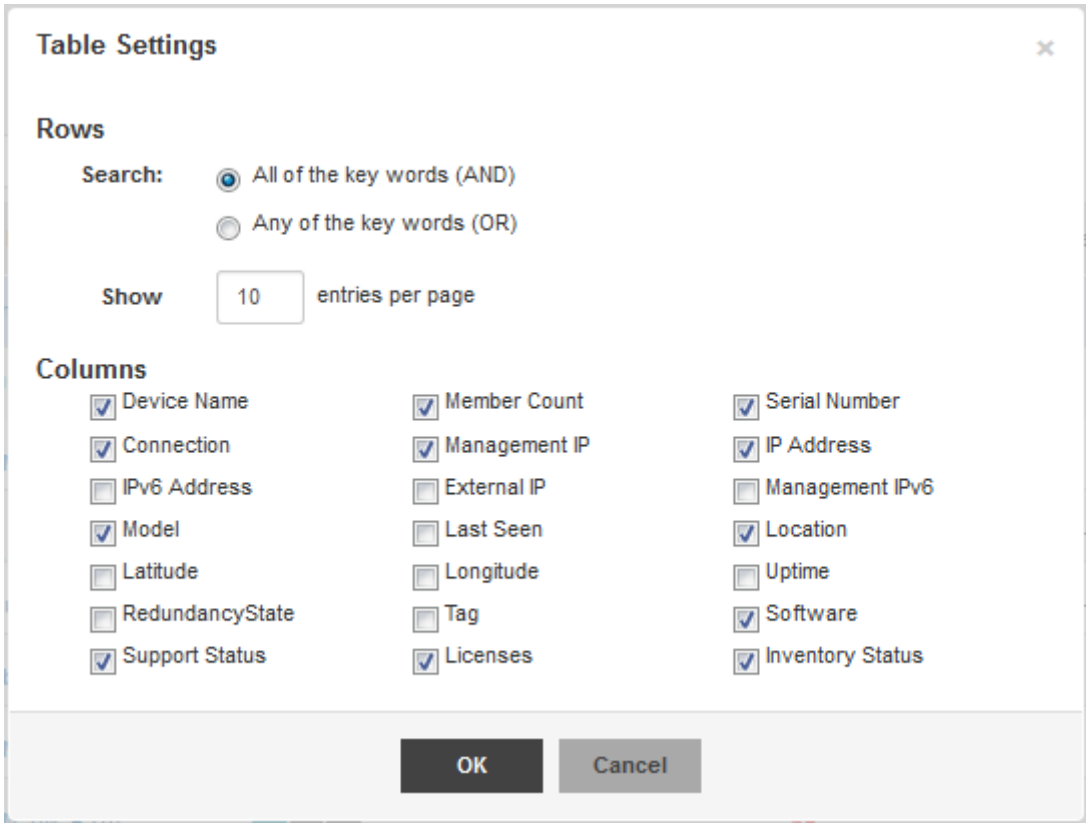
Field/Column	Description
Device Name	Displays the name of the device - it could be a ZD controller or an Unleashed network that software manages. Clicking the device name hyperlink opens the dashboard of the controller in a new page.

TABLE 6 Configuring Device Management (continued)

Field/Column	Description
Member Count	Display the number of Connected, Disconnected or Pending APs which are managed by the ZoneDirector controller or the Unleashed network.
Serial Number	Displays the serial number of the device.
Connection	Indicates whether the device is currently online ( ) or offline ( ).
SSH Connection	Indicates the status of the SSH tunnel between Unleashed Multi-Site Manager and ZoneDirector or Unleashed devices.
Management IP	Display the Management IP address of ZoneDirector and Unleashed devices.
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 200.5 Unleashed devices 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.
Last Seen	Displays the time stamp of the device when it was last online.
Uptime	Displays how long since the device was last rebooted.
Redundancy State	Indicates the status of the ZoneDirector's smart redundancy.
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 the Device Configuration

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

After you log in to the Web interface, select **Devices** from the menu in the left.

The **Devices** 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

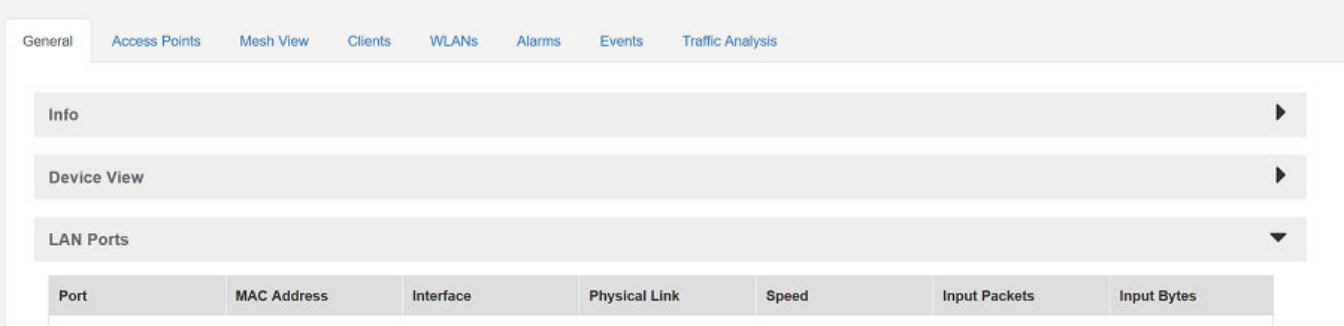


TABLE 7 Device Configuration Details

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.
Access Points	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 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 type of alarm that was triggered, the time and date when the alarm was generated, severity and activity associate with the alarm.
Events	Displays a table that lists information about the type of event that was triggered, the time, event type, severity and activity associate with the event.
Traffic Analysis	Displays traffic trends as graphs. The following trends are available: • Top 10 AP's Traffic • Top 10 AP's Client • Top 10 Client's Traffic

TABLE 7 Device Configuration Details (continued)

Configuration Tabs	Description
	• Client OS Traffic • Model Traffic • Client Count vs AP Counts by Model • AP Status • Vendor vs AP

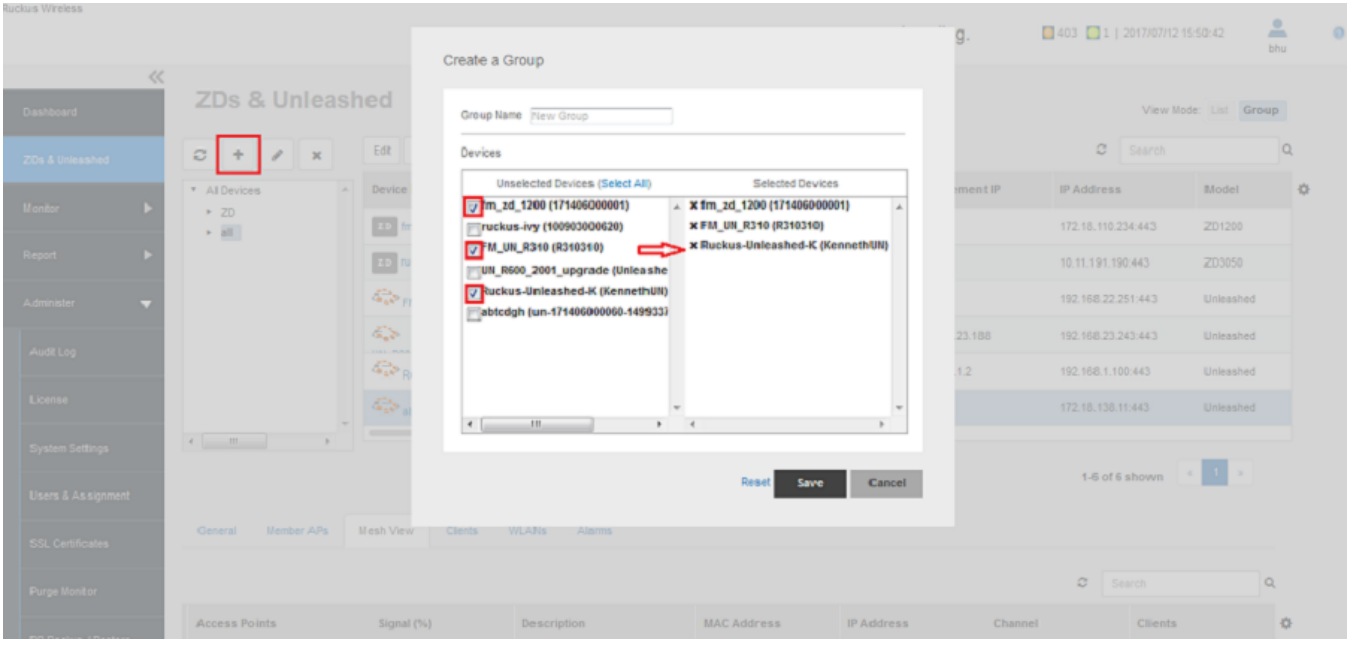
Click the icon to refresh the contents of the tables within these tabs. You can also customize the tables by clicking the icon. You can also make use of the **Search** box to look for specific information within the tables.

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 log in to the Web interface, select **Devices** from the menu in the left.
   The **Devices** 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.

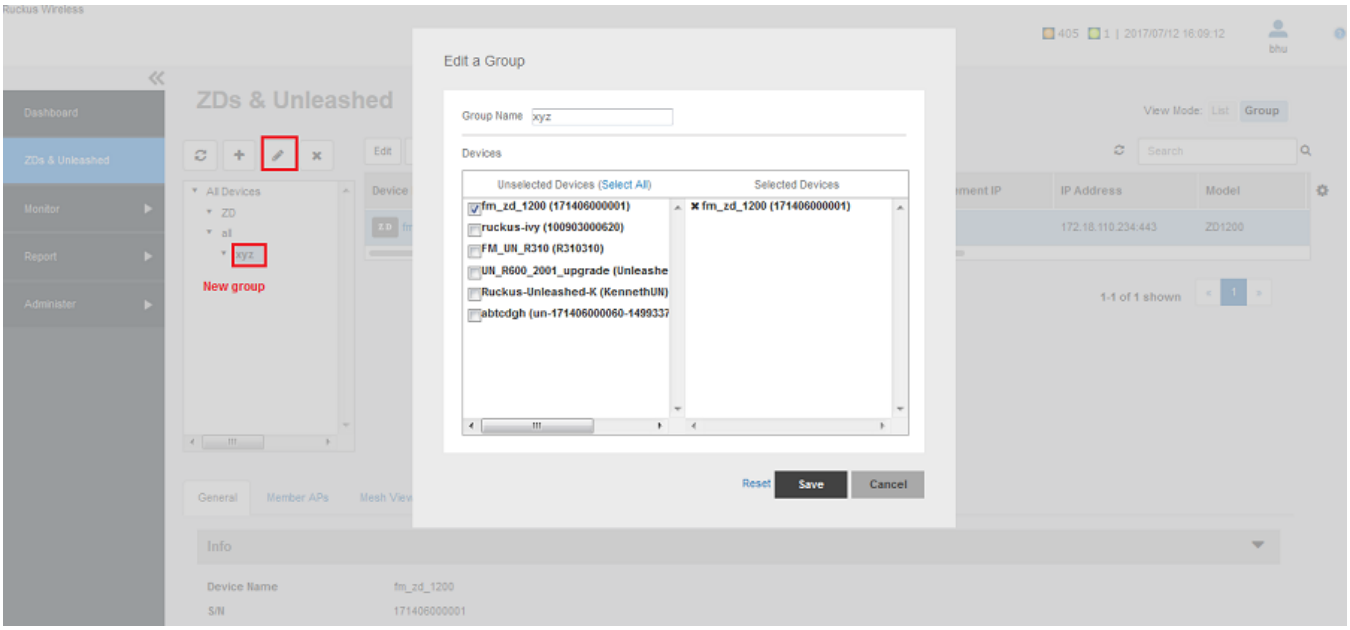
4. In **Devices**, under the *Unselected Devices* section, select the devices that you want to group by checking the box against the device. Those selected are populated under the *Selected Devices* section.
5. Click **Save** to confirm the grouping.

   A success message is displayed after the group is created.
6. Click **OK**.

   The newly created group is listed under the device hierarchy.
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.

Viewing Group Details

When you select a group, you can view details about the APs associated with the group, alarms and events.

1. After you to log in to the Web interface, select **Devices** from the menu in the left.

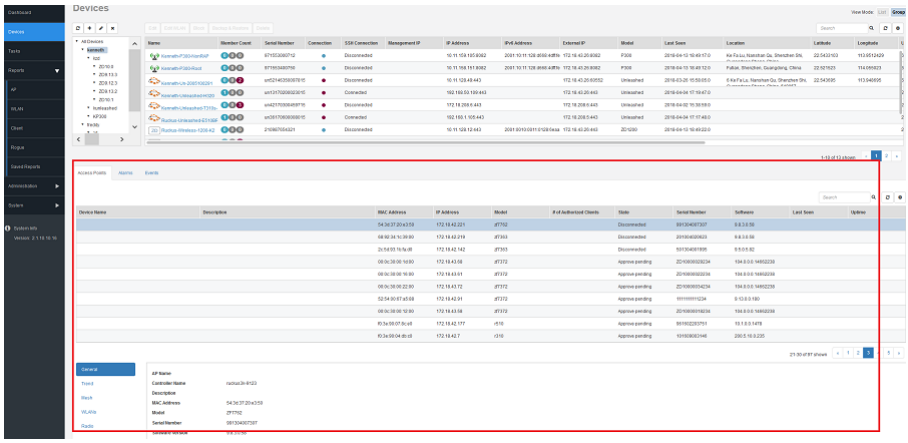
   The **Devices** page appears listing all the devices managed by the software.
2. From **View Mode**, select **Group** to view the groups of devices.

3. From the tree hierarchy, select a group that you created.

   The following information is displayed:

   - Access Points: displays information about the APs in the group such as the device name, model, IP address, state, software version etc. Additionally, you can also view the following:
     - General: displays general information about the AP such as controller name, IP address, location and so on.
     - Trend: displays graphical trends pertaining to the associated clients, traffic and state of the AP.
     - Mesh: displays details about the AP mesh type, up link and down link.
     - WLANs: displays information about the WLANs associated with the AP such as ESSID, BSSID and radio.
     - Radio: display details about the radio information of the AP.
   - Alarms: displays alarms that are **Active** and those that were generated earlier (under the **History** tab). You can select an alarm from this list and click **Acknowledge** to accept the alarm. A success message is displayed when it is accepted.
   - Events: displays the events generated.

FIGURE 18 Group Details



Editing the Device Properties

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

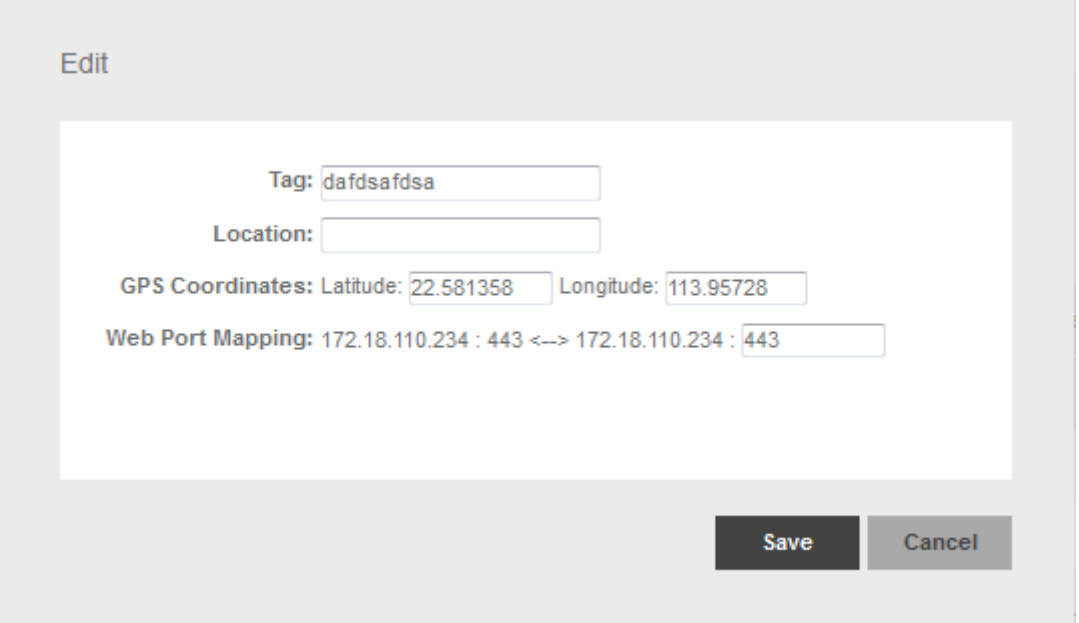
1. After you to log in to the Web interface, select **Devices** from the menu in the left.

   The **Devices** 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 19 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.

     NOTE
     200.6 Unleashed networks setup SSH tunnels between Unleashed Multi-Site Manager and it self, so you do not have to configure the Web Port Mapping.

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.

Editing WLAN SSID

You can configure the SSID of the WLAN associated with an Unleashed network to synchronize configuration between network devices.

NOTE
This is only support on 200.6 Unleashed network and ZoneDirector devices. 200.5 Unleashed networks are not supported.

NOTE
The supported Usage Type is Standard, the supported and Authentication Method is Open Wlan.

1. After you to log in to the Web interface, select **Devices** from the menu in the left.
   The **Devices** page appears listing all the devices managed by the software.
2. From the list of devices, select the Unleashed network for which you want to edit the WLAN SSID, then click **Edit WLAN**.
   The **Update WLAN** dialog box appears.
3. Select the ESSID from the drop-down list. The name, IP address and Sernial number of the unleashed network is displayed.
4. In **NewESSID/Name**, enter the name of the ID
5. In **NewP assphrase**, provide the password to login.
6. Click **Save**.

Blocking Devices from the Software

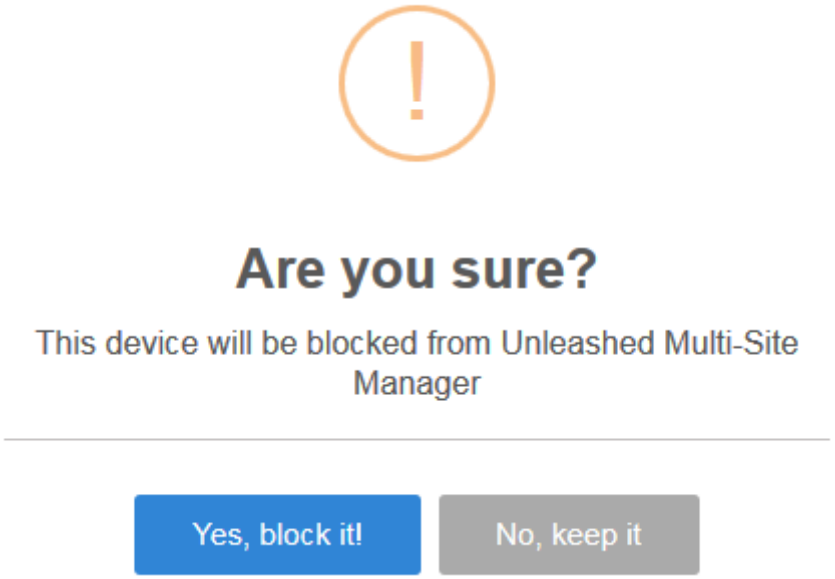
If devices within the network seem unauthorized or are a threat to security, you can use the software Web interface to block the device. You can block one or more devices at a time.

1. After you to log in to the Web interface, select **Devices** from the menu in the left.
   The **Devices** 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 20 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.
You can modify this number from **System** > **System Setting** > **Device Backup**.

1. After you to log in to the Web interface, select **Devices** from the menu in the left.

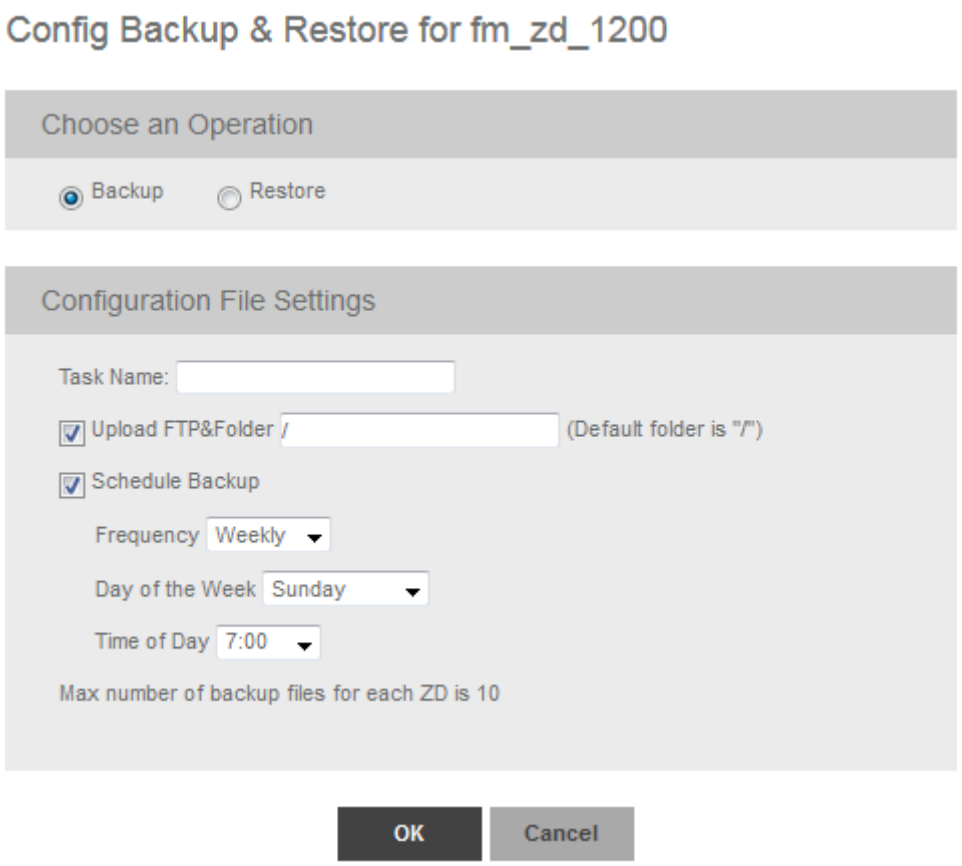
   The **Devices** page appears listing all the devices managed by the software.

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 21 Backing Up the 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 back up the device configuration is created.

Restoring the 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.
You can modify this number from **System** > **System Setting** > **Device Backup**.

NOTE
For ZD and 200.5 Unleashed devices, port 80 is used to download the configuration file from Unleashed Multi-Site Manager. Therefore, ensure port 80 is open in the firewall, otherwise, the restore task will continue to displays the status as Applying.

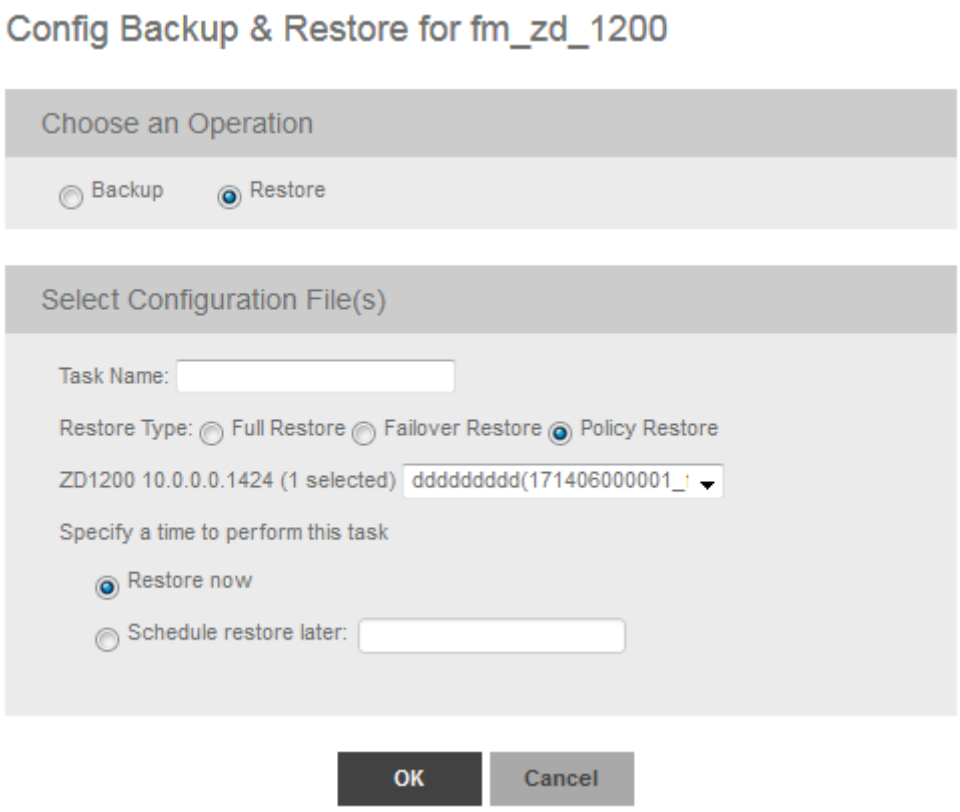
1. After you to log in to the Web interface, select **Devices** from the menu in the left.

   The **Devices** 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 22 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.

       The unleashed ID will be overwritten during Full Restore.
     - *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.

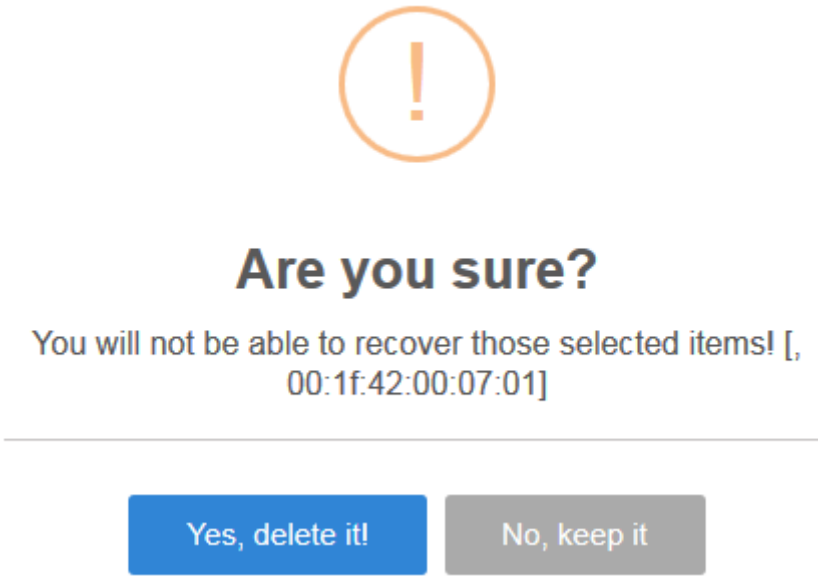
1. After you to log in to the Web interface, select **Devices** from the menu in the left.

   The **Devices** 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 23 Delete Screen



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

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

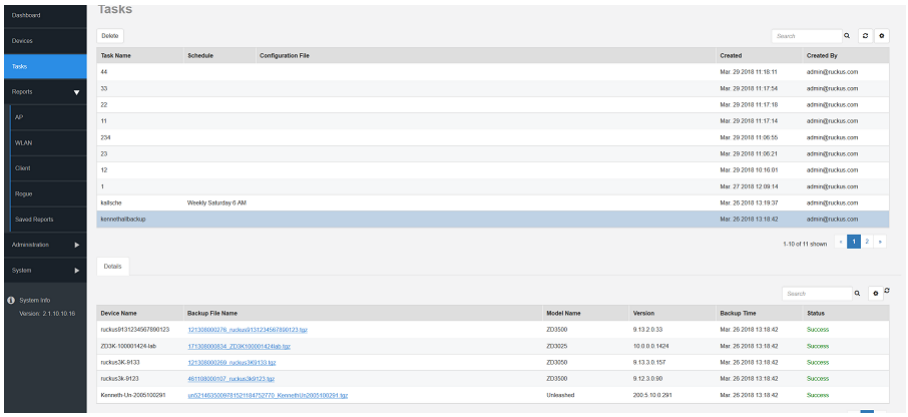
Managing Tasks

You can view, create and manage tasks assigned to a user.

After you to log in to the Web interface, select **Tasks** from the menu in the left.

The **Tasks** page appears listing all the tasks created so far.

FIGURE 24 Viewing Tasks



The following information about the task is displayed.

- Task Name: displays the name of the task.
- Schedule: displays the time and date for when the task is scheduled.
- Configuration File: displays the name of the configuration file used.
- Created: Displays the time and date when the task was created.
- Created By: display the User ID of the person who created the task.

Clicking the task displays more information about the device name, backup file, model name, version, backup time and status of the task.

To delete a task, select it and click **Delete**.

Working with Reports

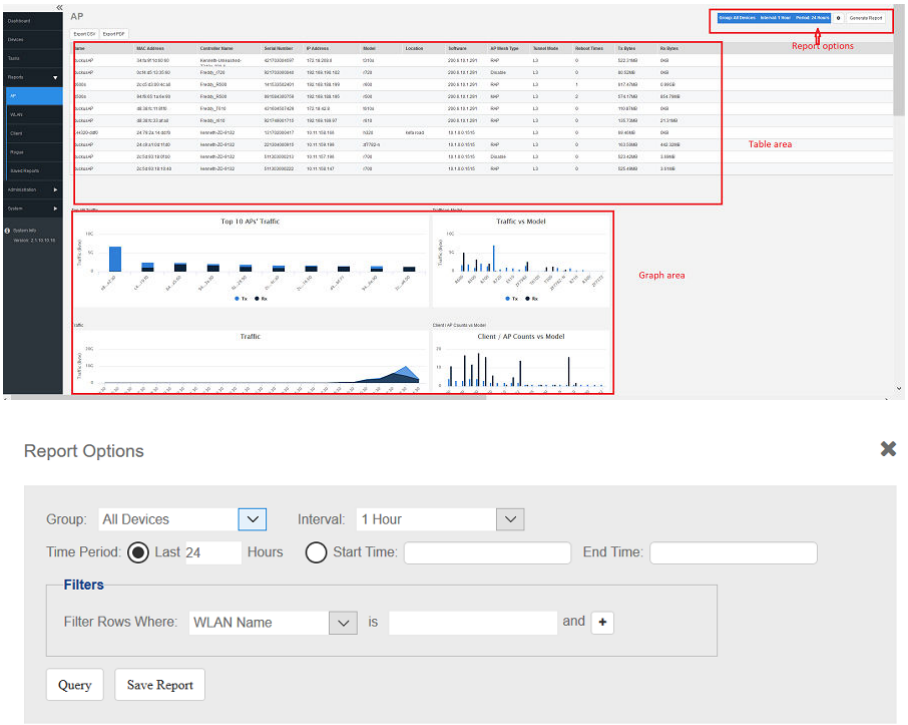
- Available Report Types..... 53
- Generating an AP Report..... 56
- Generating a WLAN Report..... 57
- Generating a Client Report..... 58
- Generating Reports for Rogue Devices..... 59
- Viewing Saved Reports..... 60

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.

Typically, every report page contains a **Report Options** area where you can set the configuration values for the report by clicking **Generate Report**, a **Table area** where the details are listed and a **Graph area** where the report can be interpreted as a graph.

FIGURE 25 Report Page



You can click **Export CSV** or **Export PDF** to generate reports as CSV files or PDF files, respectively.

TABLE 8 Reports in Software

Report Name	Description
AP	View current status and detailed information about APs.

TABLE 8 Reports in Software (continued)

Report Name	Description
WLAN	View the detail information about WLANs.
Client	View the detail information about Clients.
Rogue	View the detail information about Rogue APs.
Saved Reports	Displays information about the reports that are saved by the user.

Configuring Report Options

You can customize a report based on the device you wan to group based on the time interval and also provide the time-range between when you want the report to be generated for a device.

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

   The following sub-menu items appear:

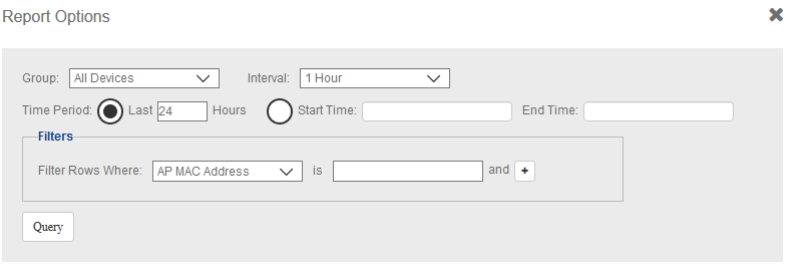
   - AP
   - WLAN
   - Client
   - Rogue
   - Saved Reports
2. Click on any of the sub-menu options.

   The corresponding reports page is displayed with a Report Option area, Table area and a Graph area.

   The Reports Option area displays the Group, Interval and Period.
3. Click one of the options (Group, Interval or Period).

   The **Reports Option** page appears.

   FIGURE 26 Report Options



4. In Group, select the list of devices or groups for which you want to generate the report.
5. In Interval, select the time interval within which the report must be generated periodically. Options include 15 minutes, 1 hour and 1 day.
6. In Time Period, select the time duration for which you want to generate the report. For example, you can set the report to be generate for APs in the last 48 hours.
7. In Start Time and End Time, provide the time-range within which you want to generate a report for the device.
8. In Filters, you can use this setting to filter reports based on one or more criteria. For example, you can generate reports where the AP firmware version is lesser than 2.0 and AP Model is R700.

9. Click **Query**. A report is generate based on the options configured.

   You can also save the report periodically. For more information see, Saving Reports on page 55

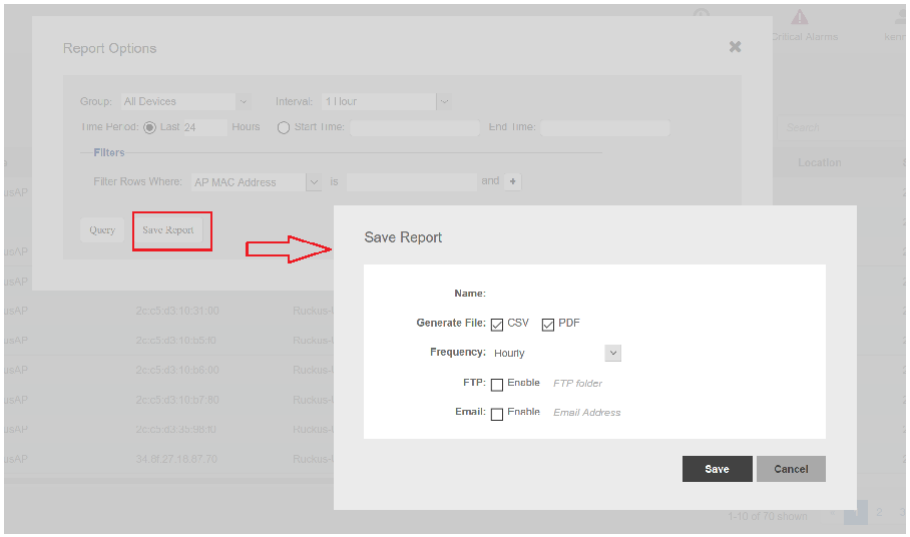
Saving Reports

You can periodically save the reports that you generate.

1. From the Reports Option page, click **Save Report**.

   The **Save Report** page appears.

   FIGURE 27 Saving a Report



2. In Name, provide the name of the report.
3. In Generate File, select the format in which you want to generate the report. Options include PDF and CSV.
4. In Frequency, select how often you want the report to be generated. Options include Hourly, Daily, Weekly and Monthly.
5. Enable the **FTP** and **Email Address** check boxes based on where you want to save the generated report.
6. Click **Save**.

   A message is displayed confirming the report is saved. The report is listed in the **Saved Report** sub-men now.

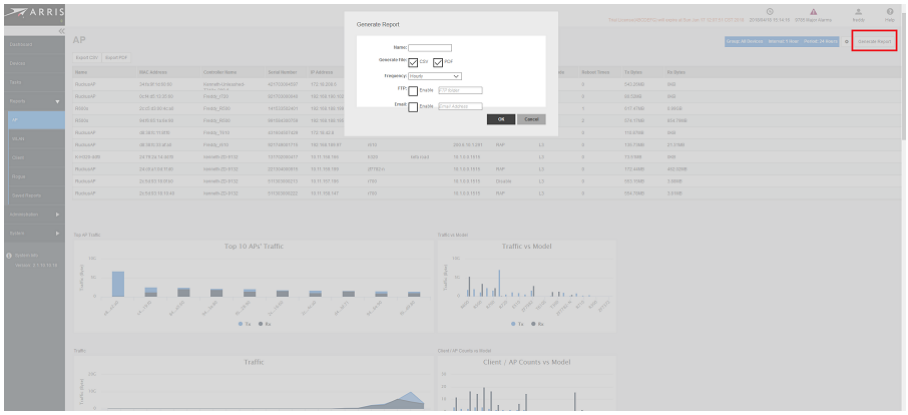
Generating Reports

You can generate reports and also predefine the report schedule and location or contact that it needs to be sent to.

1. From the report page, click **Generate Report**.

   The **Generate Report** page appears.

   FIGURE 28 Generating Reports



2. In Name, enter the name of the report.
3. In Generate File, select the file format that you want the report to be generated in Options include CSV and PDF.
4. In Frequency, select the how often the report should be generated. Options include Hourly, Daily, Weekly and Monthly.
5. In FTP, enable to checkbox and provide the FTP folder location to where the report must be saved.
6. In Email address, enable the checkbox and provide the email address to where the report must be sent.
7. Click **OK**.

   The repot is created.

Generating an AP Report

You can generate reports for APs to analyze their health and performance.

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

   The following sub-menu items appear:

   - AP
   - WLAN
   - Client
   - Rogue
   - Saved Reports

2. Click **AP** in the sub-menu.

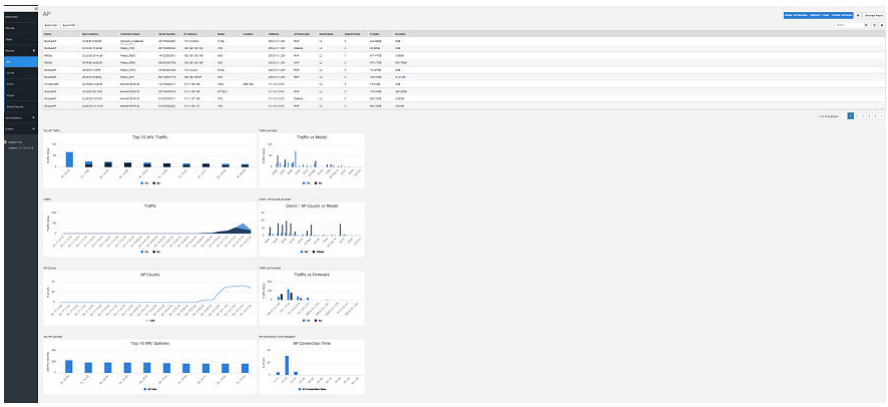
   The **AP** reports page is displayed with a Report Option area, Table area and a Graph area.

   The Reports Option area displays the Group, Interval and Period.

   The Table area displays additional information about the APs such as their name, IP address, controller name, serial ID, mesh type, tunnel mode and so on.

   You can also click on **Export CVS** and **Export PDF** to have the reports saved as a CSV or PDF file, respectively.

   FIGURE 29 AP Report Page



3. Configure the report settings as described in Configuring Report Options on page 54.

   The table area displays information about the APs such as the name, IP address, Model, Mesh type, Controller and so on. The Graph area displays trends pertaining to the APs performance such as top 10 APs by traffic, traffic analysis of APs based on their model, clients, firmware, AP count and so on.

4. Generate the report as described in Generating Reports on page 56.

Generating a WLAN Report

An WLAN 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. After you to login to the Web interface, select **Reports** from the menu in the left.

   The following sub-menu items appear:

   - AP
   - WLAN
   - Client
   - Rogue
   - Saved Reports

2. Click **WLAN** in the sub-menu.

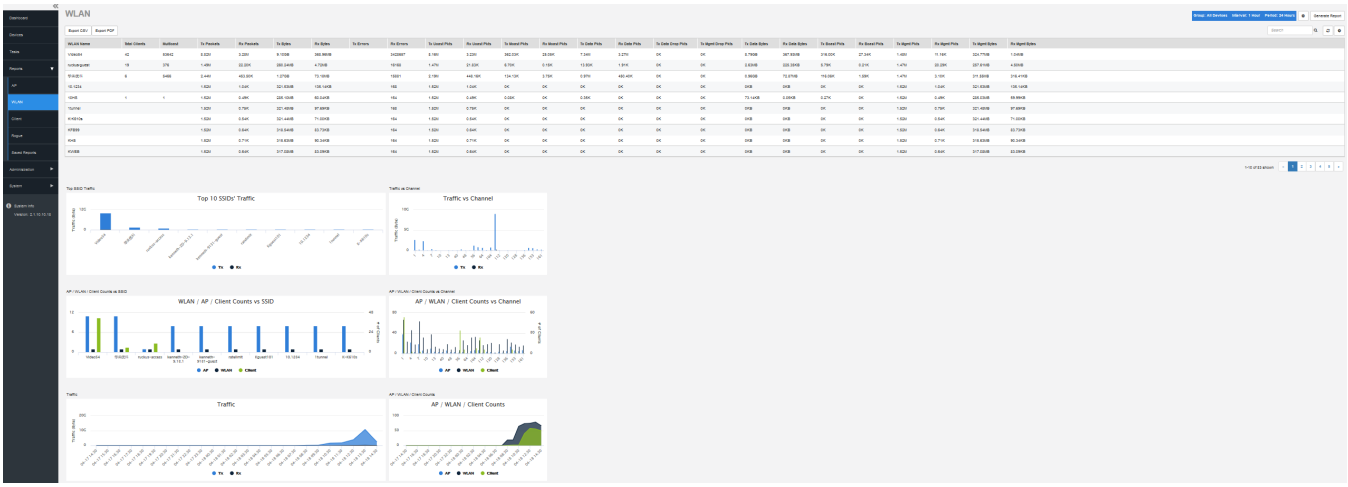
   The **WLAN** reports page is displayed with a Report Option area, Table area and a Graph area.

   The Reports Option area displays the Group, Interval and Period.

   The Table area displays additional information about the WLANs such as their name, IP address, total clients, multicast information, Tx/Rx packet information and so on.

   You can also click on **Export CVS** and **Export PDF** to have the reports saved as a CSV or PDF file, respectively.

   FIGURE 30 WLAN Report Page



3. Configure the report settings as described in Configuring Report Options on page 54.

   The table area displays information about the WLANs such as the name, TX/Rx packets, clients, Tx/Rx unicast packets, Tx/Rx errors, Tx/Rx data packets and so on. The Graph area displays trends such as top 10 SSID by traffic, traffic analysis of WLAN based on their client count, channel, 15 min intervals and so on.

4. Generate the report as described in Generating Reports on page 56.

Generating a Client Report

You can generate reports for clients to analyze their health and performance.

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

   The following sub-menu items appear:

   - AP
   - WLAN
   - Client
   - Rogue
   - Saved Reports

2. Click **Client** in the sub-menu.

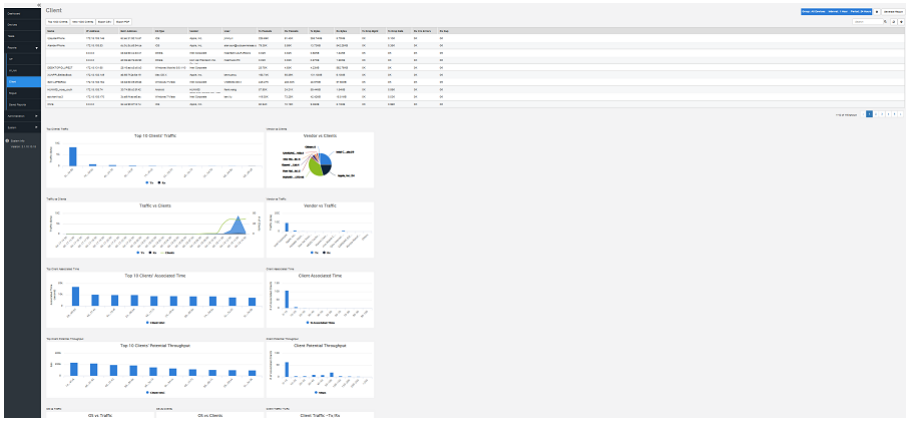
   The **Client** reports page is displayed with a Report Option area, Table area and a Graph area.

   The Reports Option area displays the Group, Interval and Period.

   The Table area displays additional information about the clients such as their name, IP address, OS type, Tx/Rx packets and so on. You can also view the list of clients by the top 1000 clients and next thousand client. You can click on **Top 1000 Clients** and **Next 1000 Clients** to view the same.

   You can also click on **Export CVS** and **Export PDF** to have the reports saved as a CSV or PDF file, respectively.

   FIGURE 31 Client Report Page



3. Configure the report settings as described in Configuring Report Options on page 54.

   The table area displays information about the client such as the name, IP address, OS type, vendor, Tx/Rx packets and so on. The Graph area displays trends pertaining to the clients performance such as top 10 clients by traffic, traffic analysis of clients based on their vendor, associated time, potential throughput, OS, Tx/Rx and so on.

4. Generate the report as described in Generating Reports on page 56.

Generating Reports for Rogue Devices

You can generate a Rogue report showing all current and past detected Rogue devices over the report period.

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

   The following sub-menu items appear:

   - AP
   - WLAN
   - Client
   - Rogue
   - Saved Reports

2. Click **Rogue** in the sub-menu.

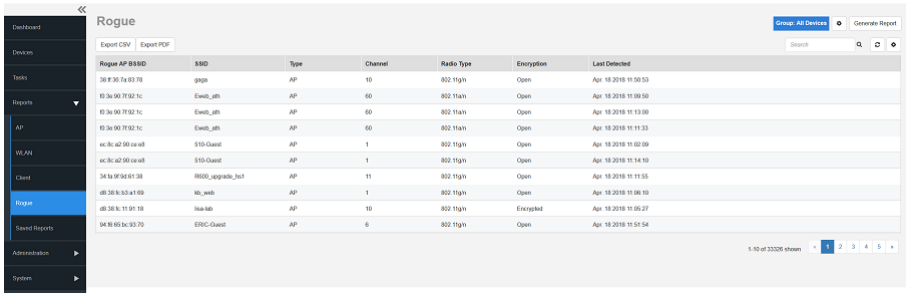
   The **Rogue** reports page is displayed with a Report Option area, Table area and a Graph area.

   The Reports Option area displays the Group, Interval and Period.

   The Table area displays additional information about the rogue devices such as their BSSID, SSID, type, channel, radio, encryption and so on.

   You can also click on **Export CVS** and **Export PDF** to have the reports saved as a CSV or PDF file, respectively.

   FIGURE 32 Rogue Report Page



3. Configure the report settings as described in Configuring Report Options on page 54.

   The table area displays information about the rogue devices such as the BSSID, type, channel, radio, encryption and so on.

Viewing Saved Reports

The Saved Reports page displays reports that you have previously configured and saved.

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

   The following sub-menu items appear:

   - AP
   - WLAN
   - Client
   - Rogue
   - Saved Reports

2. Click **Saved Reports** in the sub-menu.
   The **Saved Reports** reports page is displayed.

   FIGURE 33 Saved Report Page



   The first table lists all the reports generated and saved. Its displays the following information about the saved reports.

   - Report Name: displays the name of the report.
   - Category: displays whether the report is generated for an AP, WLAN, Client or Rogue device.
   - Frequency: displays how periodically the report was configured to generate.
   - Generate PDF: displays *Yes* if the report was saved as a PDF.
   - Generate CSV: displays *Yes* if the report was saved as a CSV.
   - Email: displays the email address provided while saving the report.
   - FTP: displays the FTP location where the report is saved.
   - Created Time: displays the time when the report was saved.

   The second table display the following:

   - File Name: displays the name of the report file name
   - PDF File: displays the size of the generated PDF. You can download the PDF by clicking the file.
   - CSV File: displays the size of the generated CSV. You can download the CSV by clicking the file.
   - Created Time: displays the time when the report was generated.

3. Configure the report settings as described in Configuring Report Options on page 54.

Performing Administrative Tasks

- The Administer Tab 63
- Viewing Audit Logs 63
- Managing Software Licenses 65
- Managing User Accounts 67
- Managing SSL Certificates 71
- Upgrading the Software 81
- Backing Up and Restoring the Database from the Web Interface 83
- Generating Support Information 86
- Manually Transferring Files 88

The Administer Tab

The **Administer** tab provides options for viewing audit logs, updating the software license file, performing user management, 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 Audit Log page displays the following:

- Audit Type: describes the user action that was performed such as a user logging off and so on.
- Severity: describes the severity of the event as High, Low and Normal.
- Time: displays the time when the event took place.
- User: displays the email ID or name of the user who initiated the event.
- Message: displays user notes included while initiating the event.

The following table lists the entries that can appear in the audit logs.

TABLE 9 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.

TABLE 9 Audit Log Entries (continued)

Audit Type	Description
User account deleted	Administrator deleted a user account.
Device log file retrieved	User retrieved an AP's log file from the Device View.
Device log file emailed	User sent out an AP's log file via email.
Device ping test performed	User performed a PING test from the Device View.
VLAN settings updated	User updated the AP's VLAN settings from the Device View.
Audit log emailed	User sent out 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, contact your 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.

TABLE 9 Audit Log Entries (continued)

Audit Type	Description
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.

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.

There are 2 kinds of software licenses file, one is for ZD and the other one is for unleashed. 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.

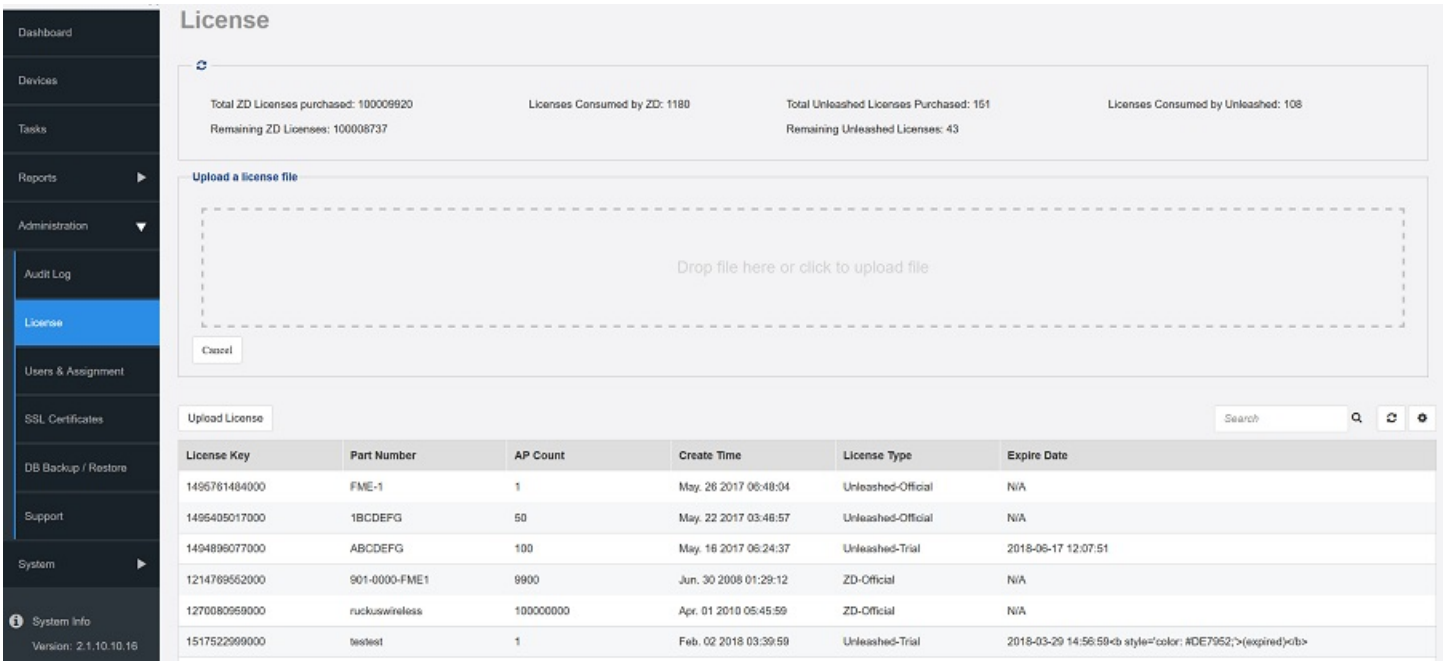
Unleashed license consumes software license according to its connected AP number. The unleashed license is updated whenever the software receives the information message from unleashed but the unleashed AP connect status is updated every 15 mins. So, there is a gap between the software update the Unleashed 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 34 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 until your license situation is resolved.

Uploading a License File

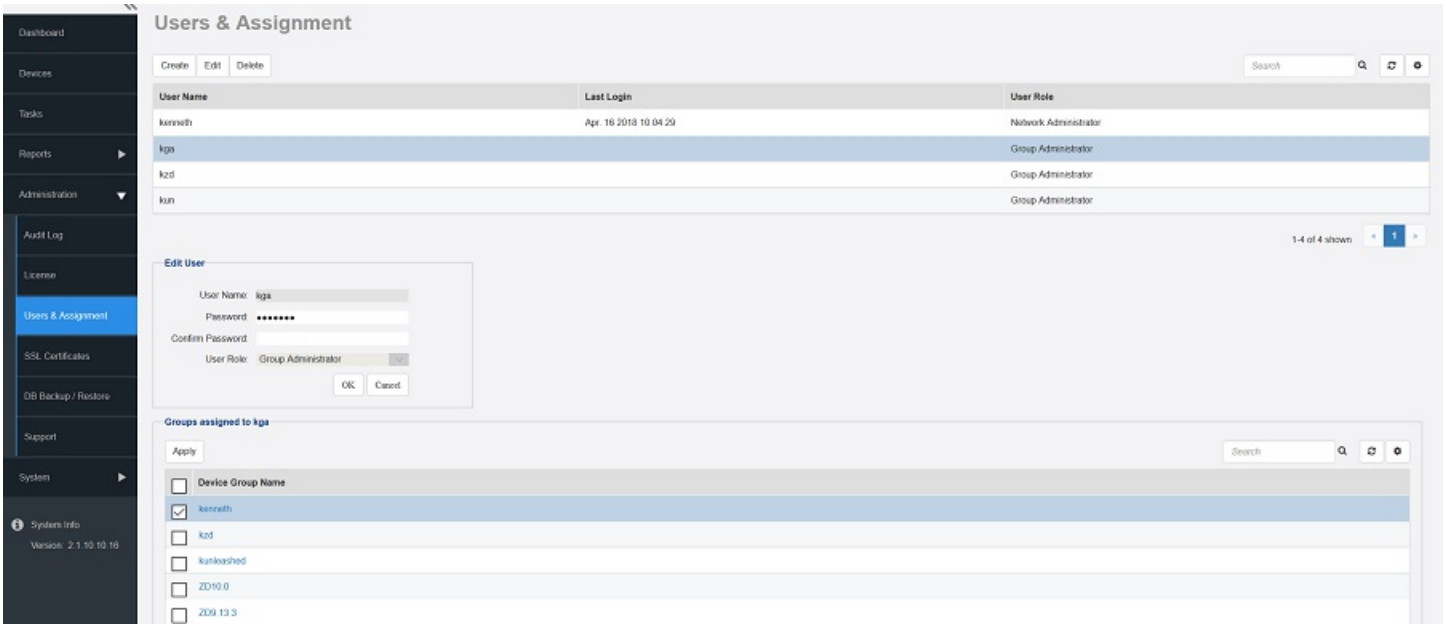
You can update your current software license by uploading additional license files using the Web interface.

1. Once you obtain a new license file from Ruckus, log in to the Unleashed Multi-Site Manager Web interface.
2. Go to **Administration** > **License**.
3. Click **Upload License**. The **Upload a license file** appears.
4. Click the **Drop file here or click to upload file** link.
5. Select the license file, and then click **Open**.
6. Click **OK** to upload the license file to Unleashed Multi-Site Manager.

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 35 Users & Assignment Page



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

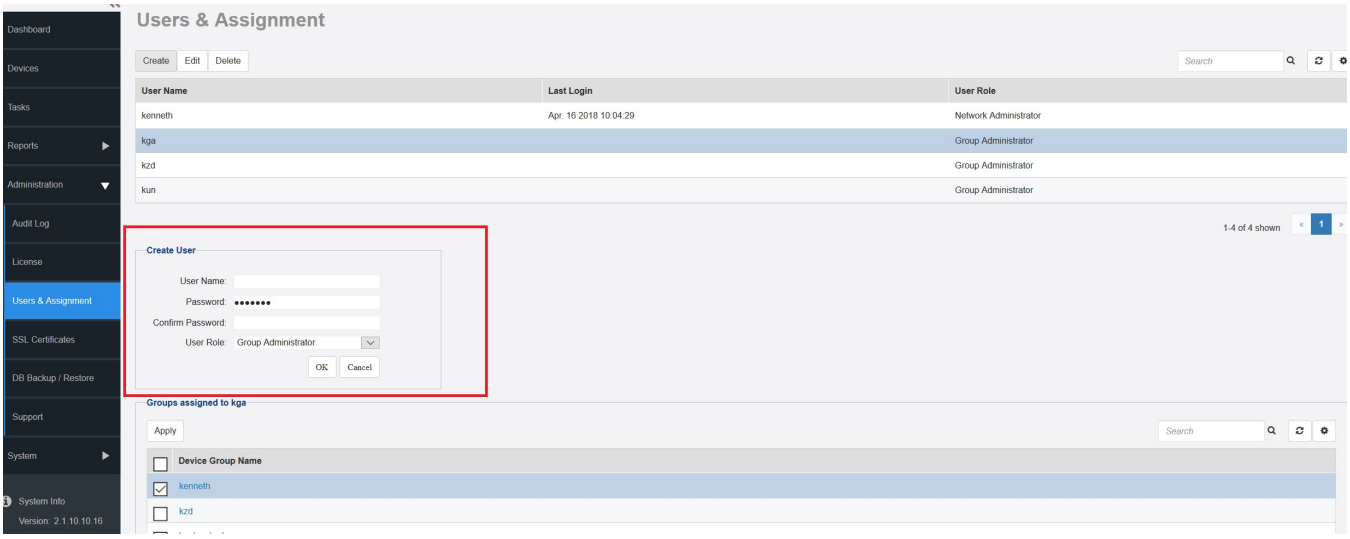
Creating a New User Account

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 **Administration** > **Users & Assignment**.
2. Click **Create**.

   The **Create User** page appears.

FIGURE 36 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 50 alphanumeric characters and spaces.
4. In **Password**, type a password for the account. The password is case-sensitive and can contain up to 50 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 role appear on the menu: **Group Administrator**.

   For more information on user roles, refer to User Roles and Privileges on page 67.
7. Click **OK** to create the account.

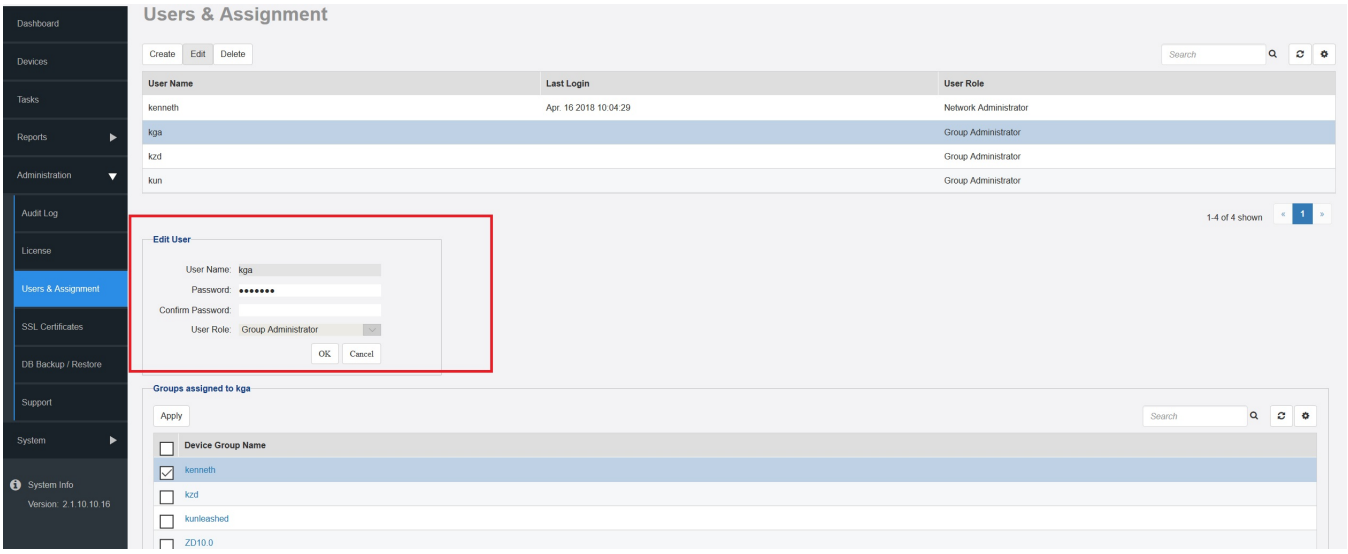
The page refreshes, and then the user account you have created appears in the **Users** list.

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 **Administration** > **Users & Assignment**.
2. Find the row in the **Users** table for the desired user account to edit, and then click **Edit**.

FIGURE 37 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 **Administration** > **Users & Assignment**.
2. Find the row in the **Users** table for the desired user account to delete, and then click **Delete**.

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

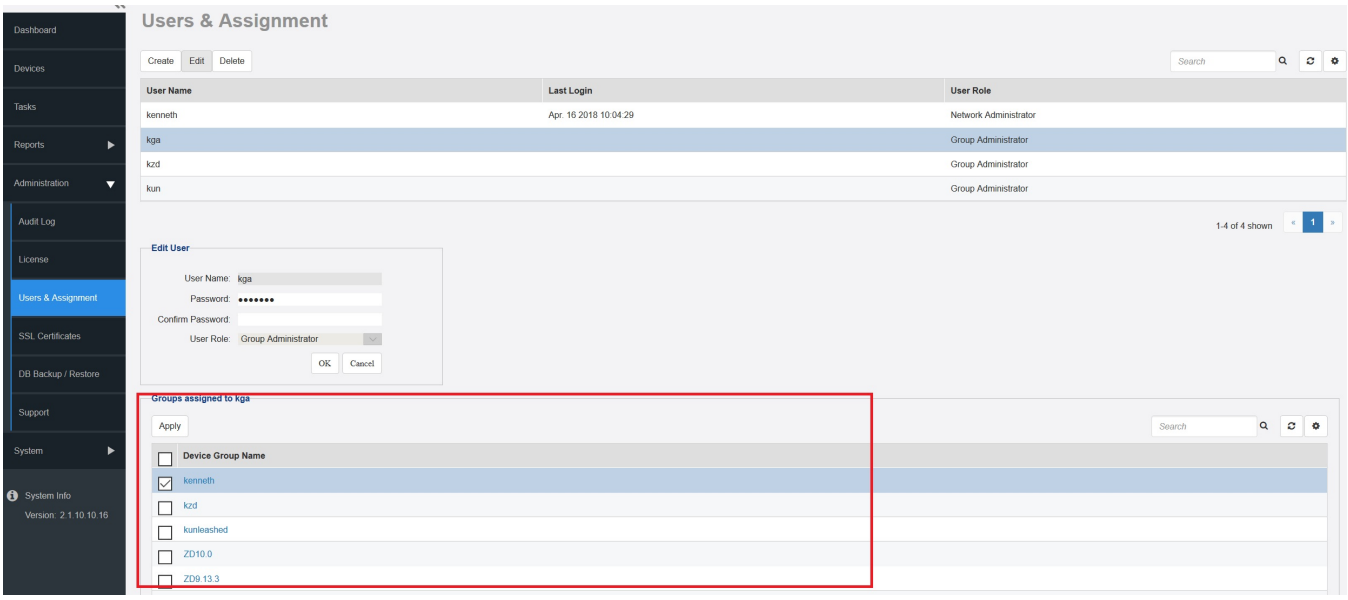
Assigning Users to Manage Device Groups

1. Create a User account as described in Creating a New User Account on page 68.

   NOTE
   The User account must have **Group Administrator** privileges to manage a Device Group, as described in User Roles and Privileges on page 67.

2. Create a Device Group as described in the **Creating and Managing Groups** section Creating and Managing Groups on page 40.
3. Go to **Administration** > **Users & Assignment**.
4. Find the entry for the user account that you want to assign as group owner.
5. In Groups assigned to <user name>, select the device group names that you want to assign to the user by selecting the check boxes.

   FIGURE 38 Assigning a User to Manage the Group



6. Click **Apply** to save your changes.

When the group owner logs in to 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.

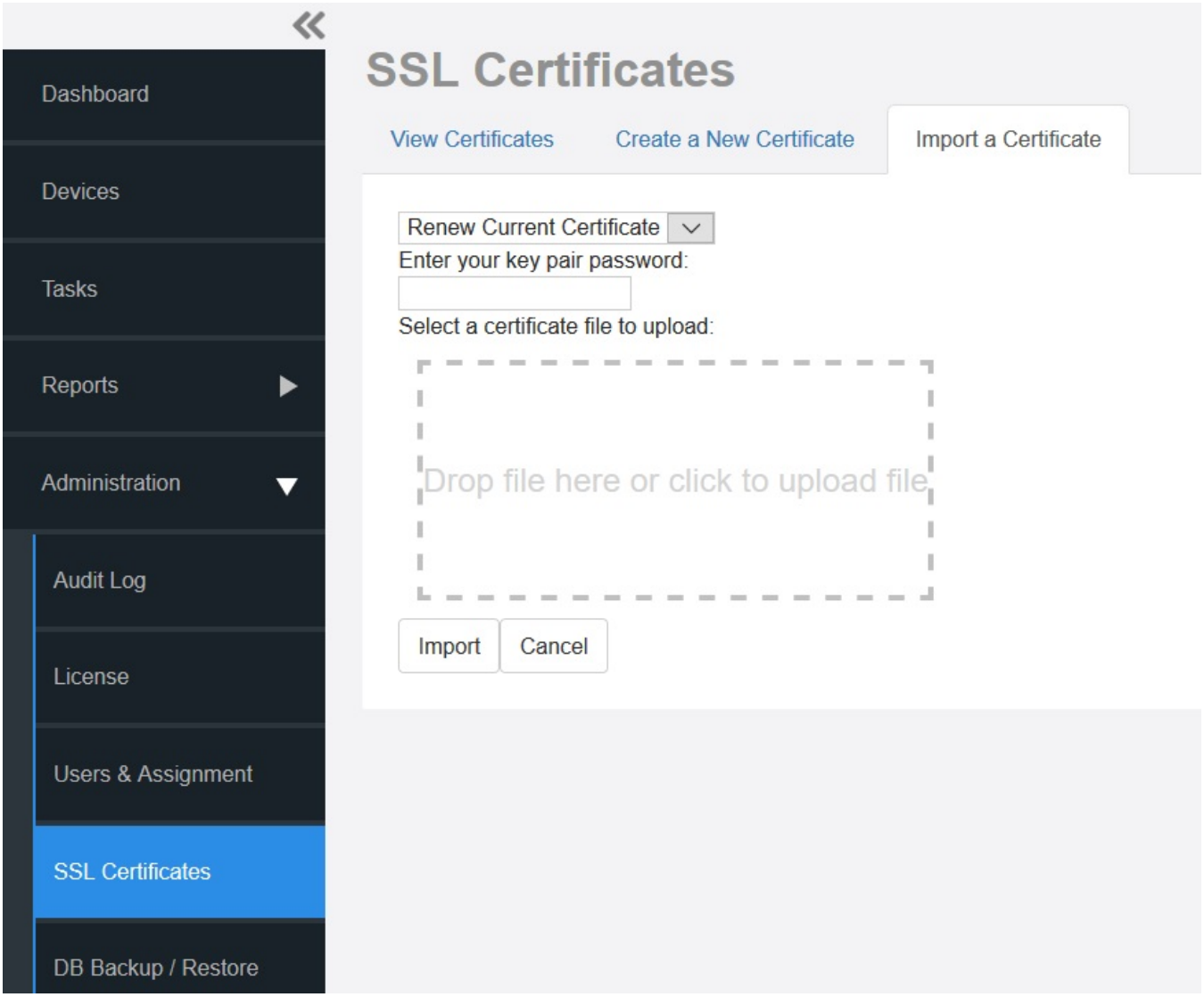
Importing an SSL Certificate

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 **Administration** > **SSL Certificates**.

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

FIGURE 39 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 **Drop file here or click to upload**, 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 79.

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 40 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.

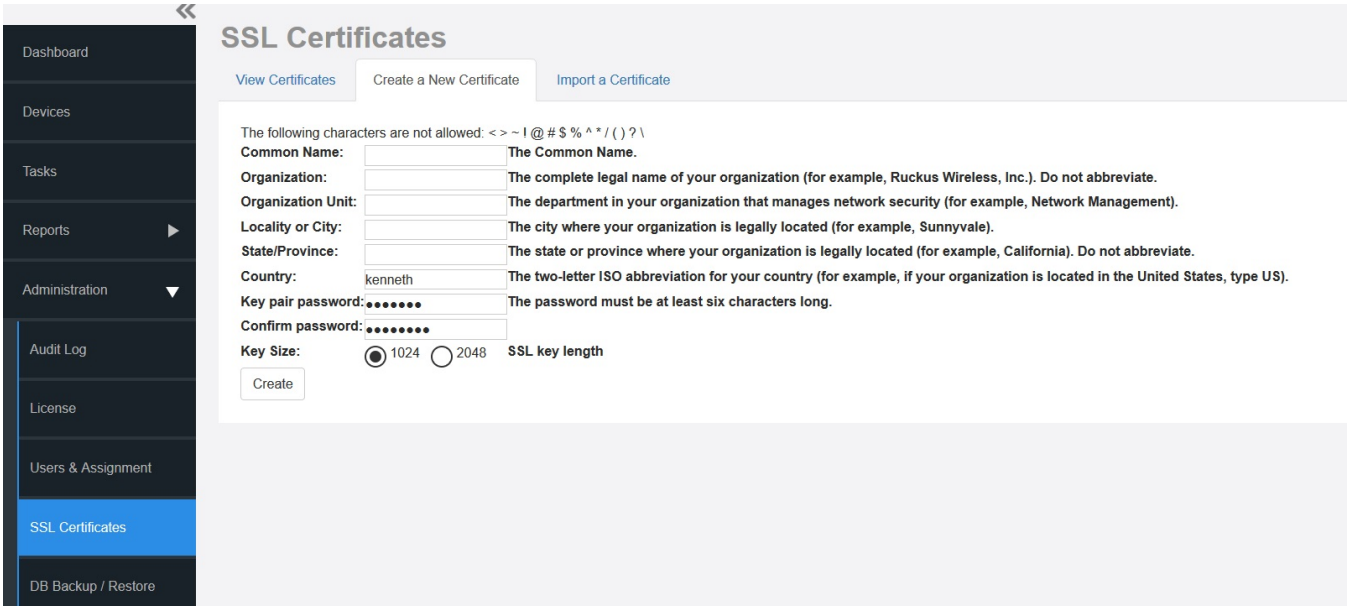
Try connecting to the software Web interface using HTTPS. The security alert should no longer appear.

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 41 Creating 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.

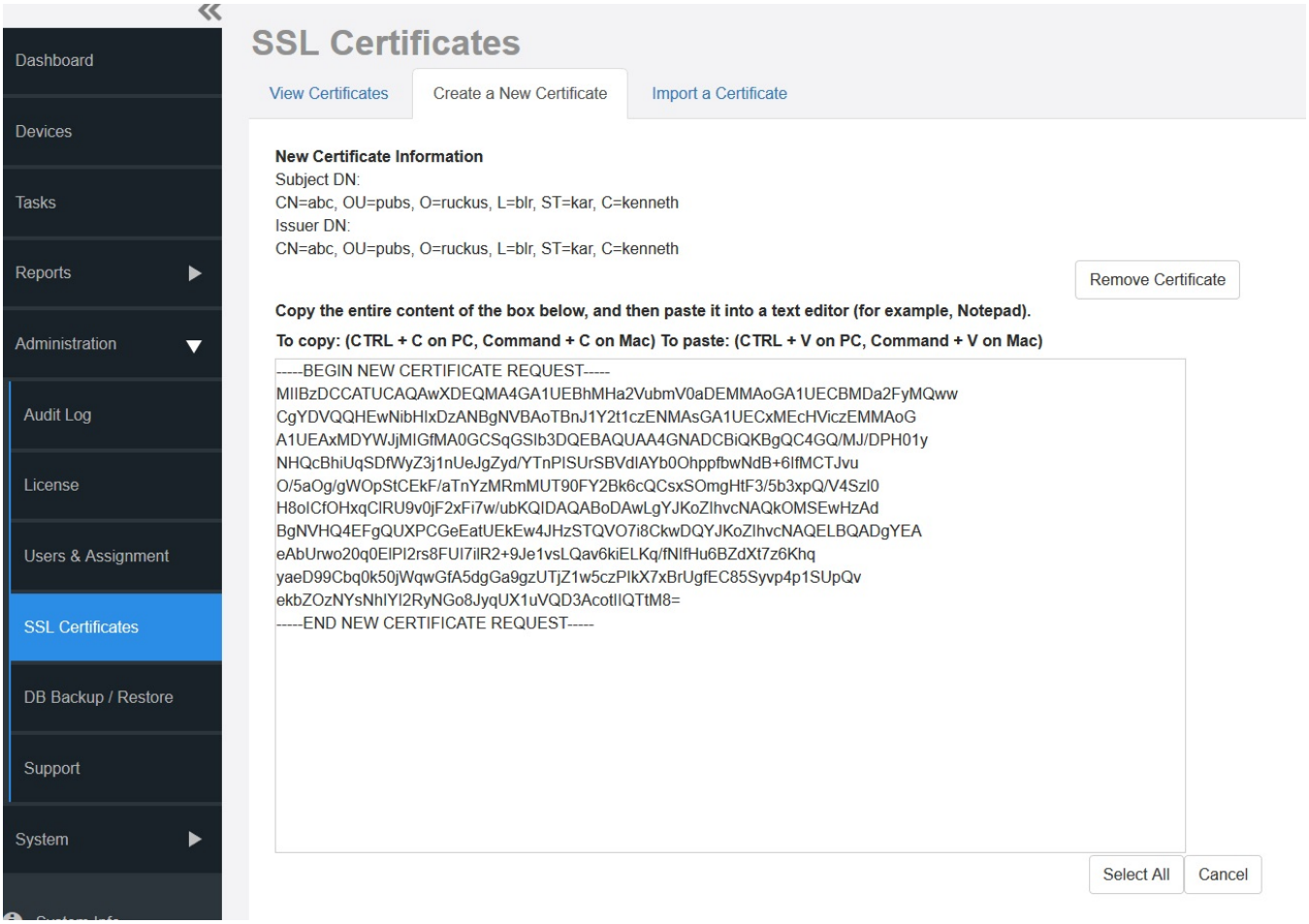
      ATTENTION
      Remember the key pair password that you set in this procedure. You need to enter this password when you import the SSL certificate that VeriSign sends you into Unleashed Multi-Site Manager.

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 42 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 website 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 website 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-----
```

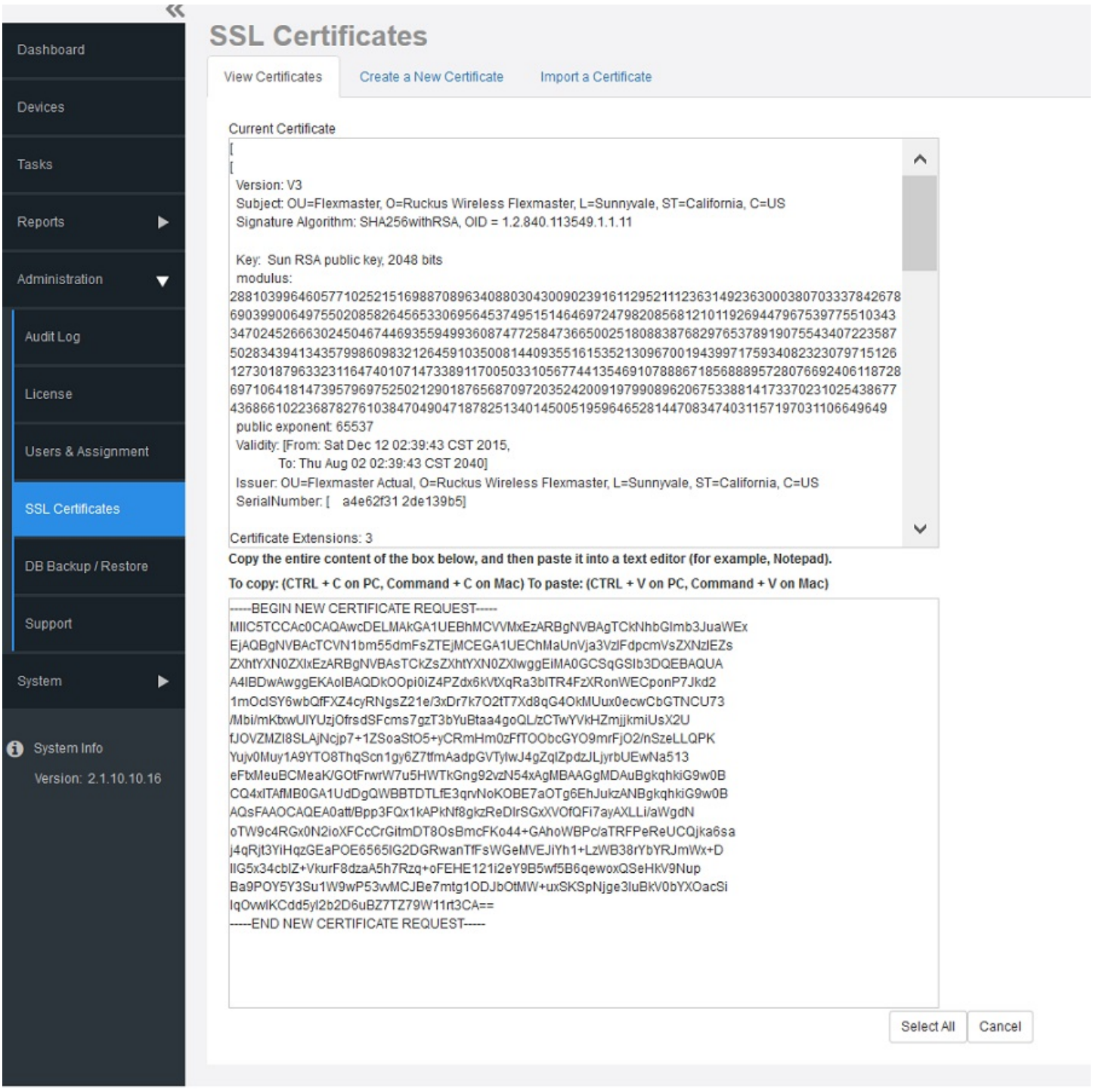
8. Copy the content of the signed certificate, and then paste it into a text file. Save the file.

You can now import the signed certificate from VeriSign into your the software server. For instructions, refer to Importing an SSL Certificate on page 71.

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 43 Viewing Current Certificates



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 website 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.

1. Log in to the host server as root.
2. Insert the Unleashed Multi-Site Manager upgrade CD into the CD-ROM drive.

   If the software server does not automatically mount the software CD-ROM, then continue with Step 3. If the server automatically mounts the CD-ROM, then continue with Step 5.
3. Type the following command to create a mount point (or directory where you want to mount the CD-ROM):

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

   ```
   # mount /dev/cdrom /mnt/cdrom
   ```
5. Upload the patch file (for example, `9.12.0.0.11.patch.tar`) to the software server.
6. Copy the patch file to the Unleashed Multi-Site Manager folder `/opt/UMM/`:

   ```
   # cp 9.12.0.0.11.patch.tar /opt/UMM/
   ```
7. Untar the patch file with following command:

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

   ```
   # ./upgrade.sh 9.12.0.0.11
   ```
10. 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 83 or Backing Up the Database from the Command Line Interface on page 22 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
   ```

   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 18.

Step 3: 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.

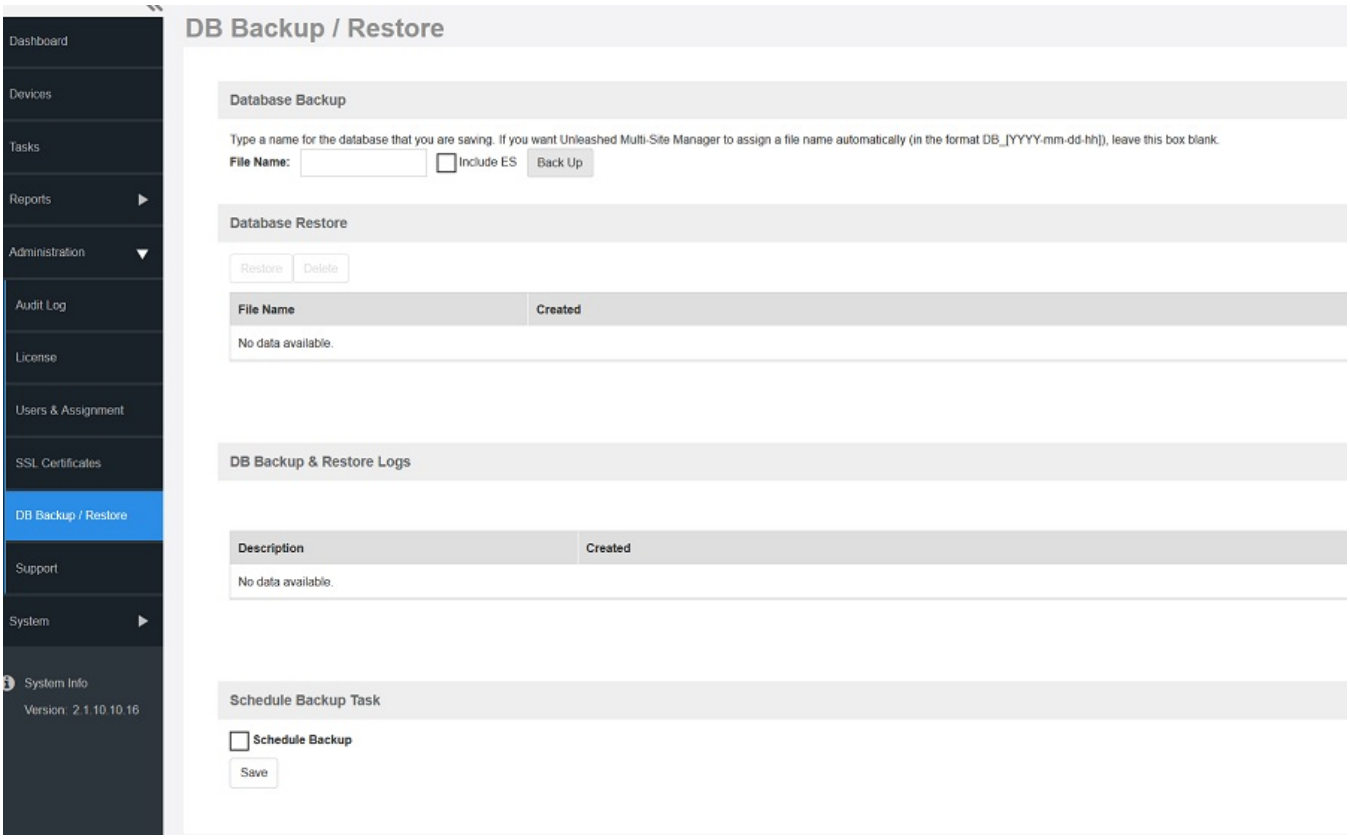
1. Go to **Administer** > **Support** and record the software version number (such as 9.12.0.0.11).
2. Go to **Administer** > **DB Backup/Restore**.
3. Look for the **Database Backup** section.
4. In **File Name**, type a name that you want to assign to the backup file, using the format `DB_[Unleashed 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 44 Backup Status Area Window



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 **Administration** > **DB Backup/Restore**.
2. Look for the **Schedule Backup Task** section.
3. Select the **Schedule Backup** checkbox.
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

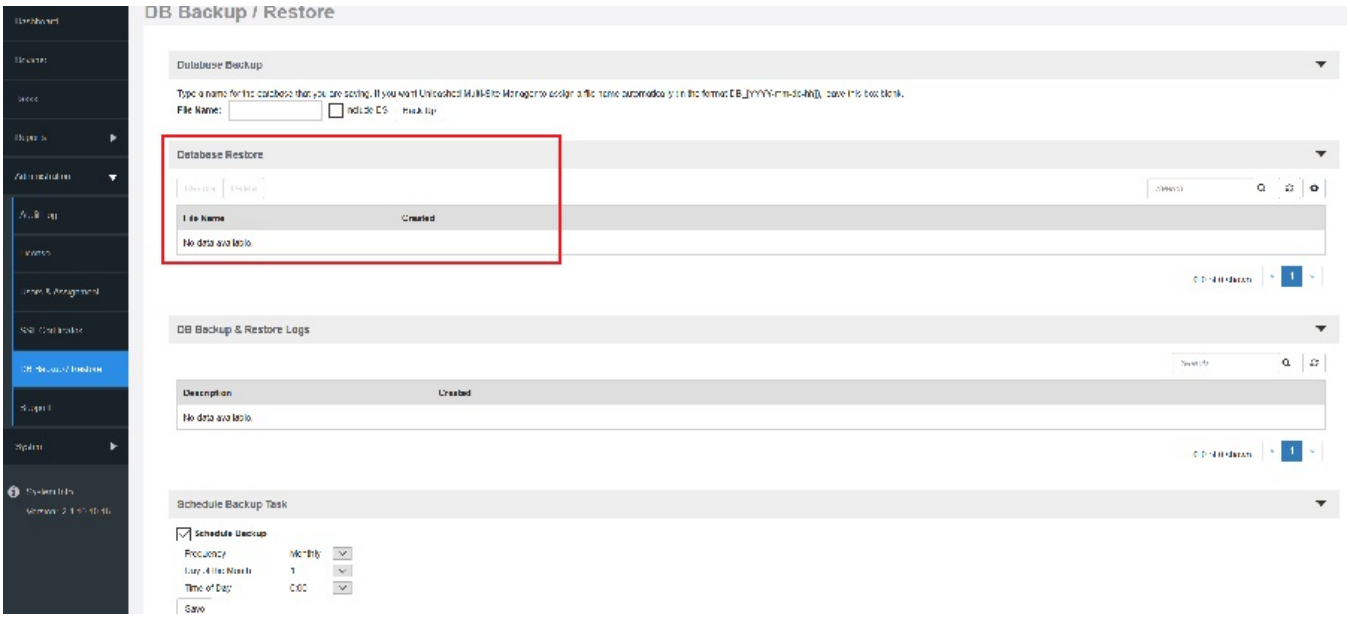
1. Go to **Administration** > **DB Backup/Restore**.
2. Look for the **DB Backup and Restore Logs** section.

   A table appears, displaying the file names of the database backup files and the dates when they were created.
3. 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 **Administration** > **DB Backup/Restore**.
2. In the **Database Restore** section, A table appears and displays the file names of the database backup files and the dates when they were created.
3. Select the database file name that you want to restore and click **Restore**.

FIGURE 45 Database Restore Screen



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

4. 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
```

5. Wait for the software login page to appear.

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

Generating Support Information

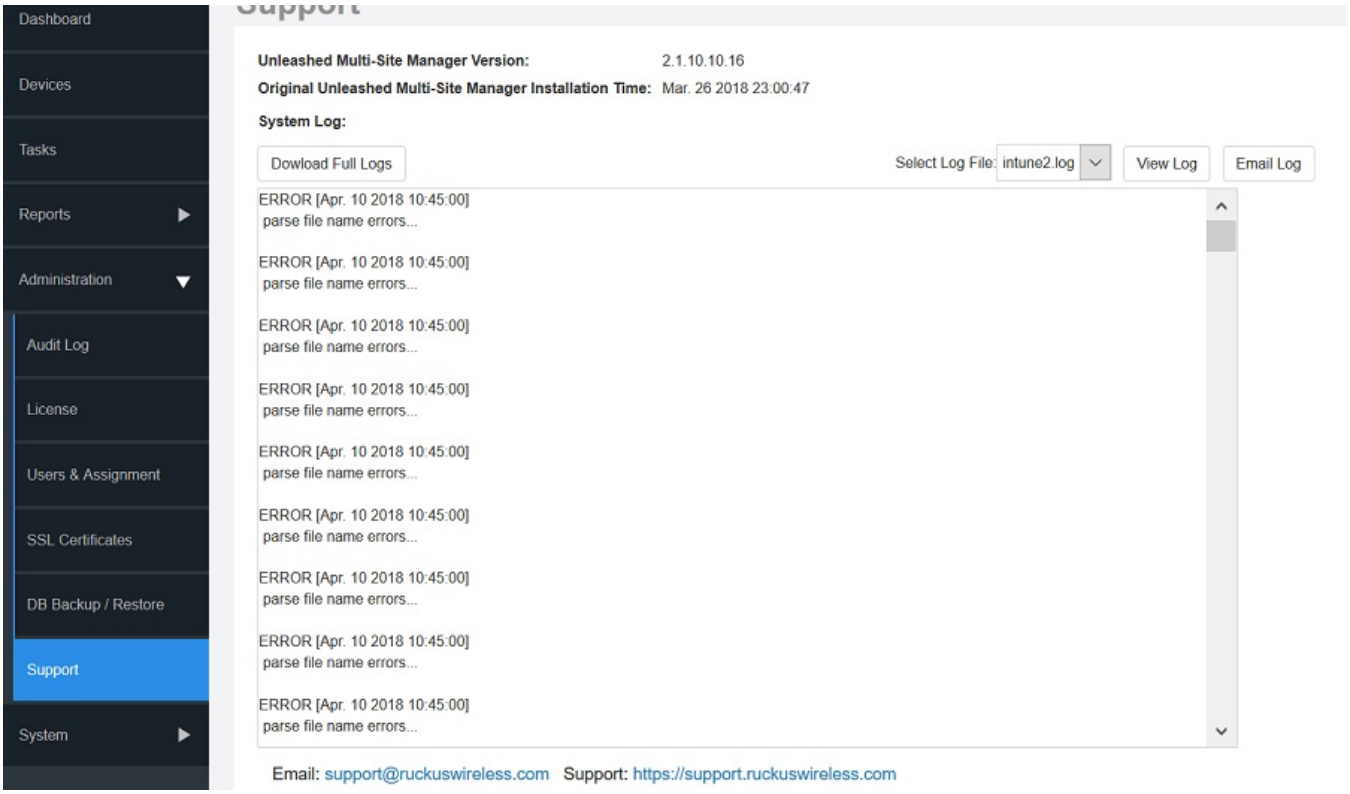
When you request technical support from Ruckus, you may be asked to collect information about Unleashed Multi-Site Manager that may help Ruckus troubleshoot the issue. You need to generate system logs.

Viewing System Logs

The system log captures information according to the file size. Unleashed Multi-Site Manager generates a new log file when the original log file size is bigger than the threshold.

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 46 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.

Emailing a Copy of the System Log File

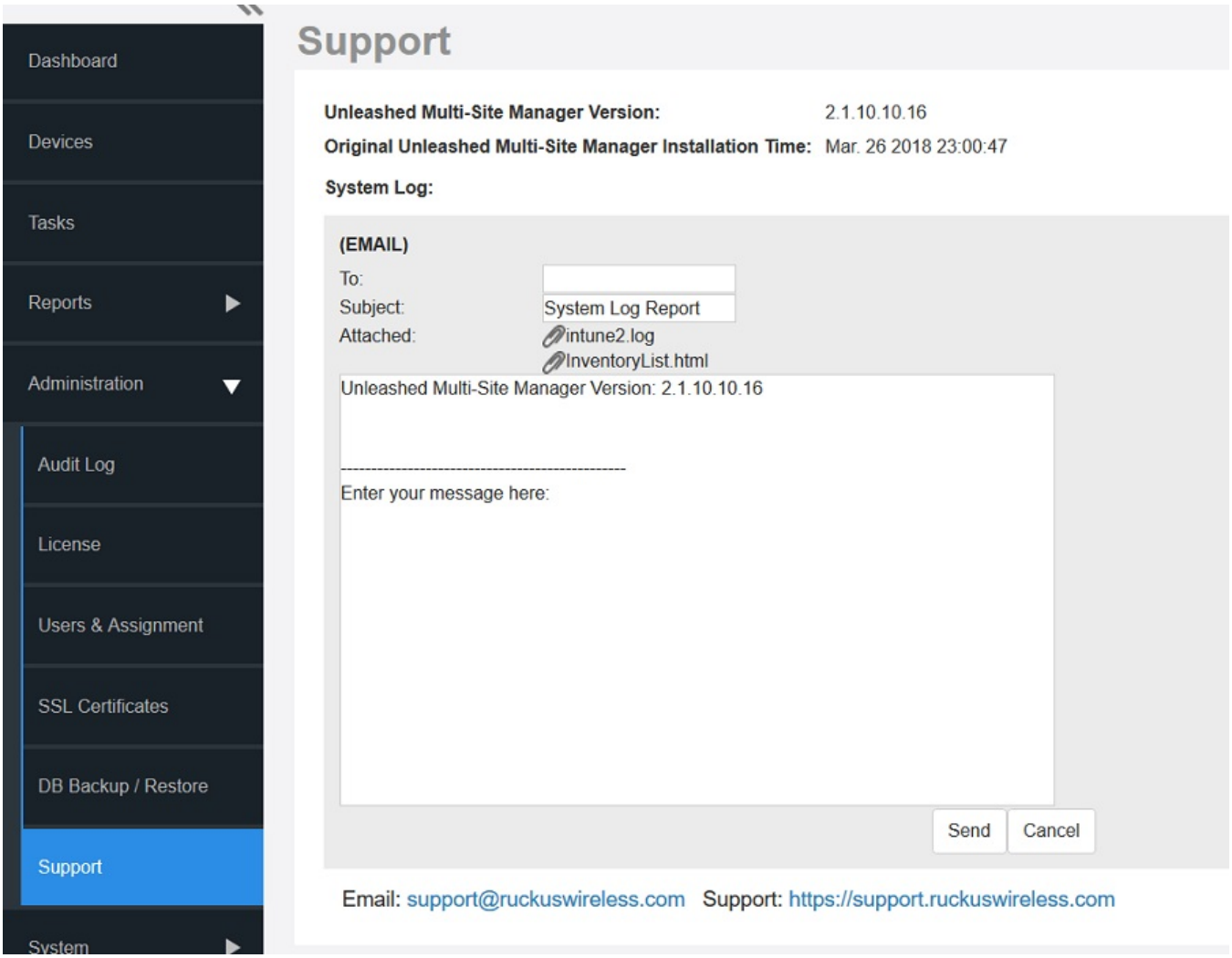
1. Go to **Administer** > **Support**.
2. Click the **Email Log** button. The **System Log** form appears.

   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. Refer to Configuring System Settings on page 91.
3. Type any information you want to highlight in the message box.

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

FIGURE 47 Sending the System Log in Email



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 files, you can use them as directed by Ruckus Support.

System

- Configuring System Settings..... 91
- Alarm Settings..... 103
- Monitoring Events..... 106

Configuring System Settings

The System Settings option allows you to specify an SMTP server.

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 48 System Settings Page (part 1 of 4)

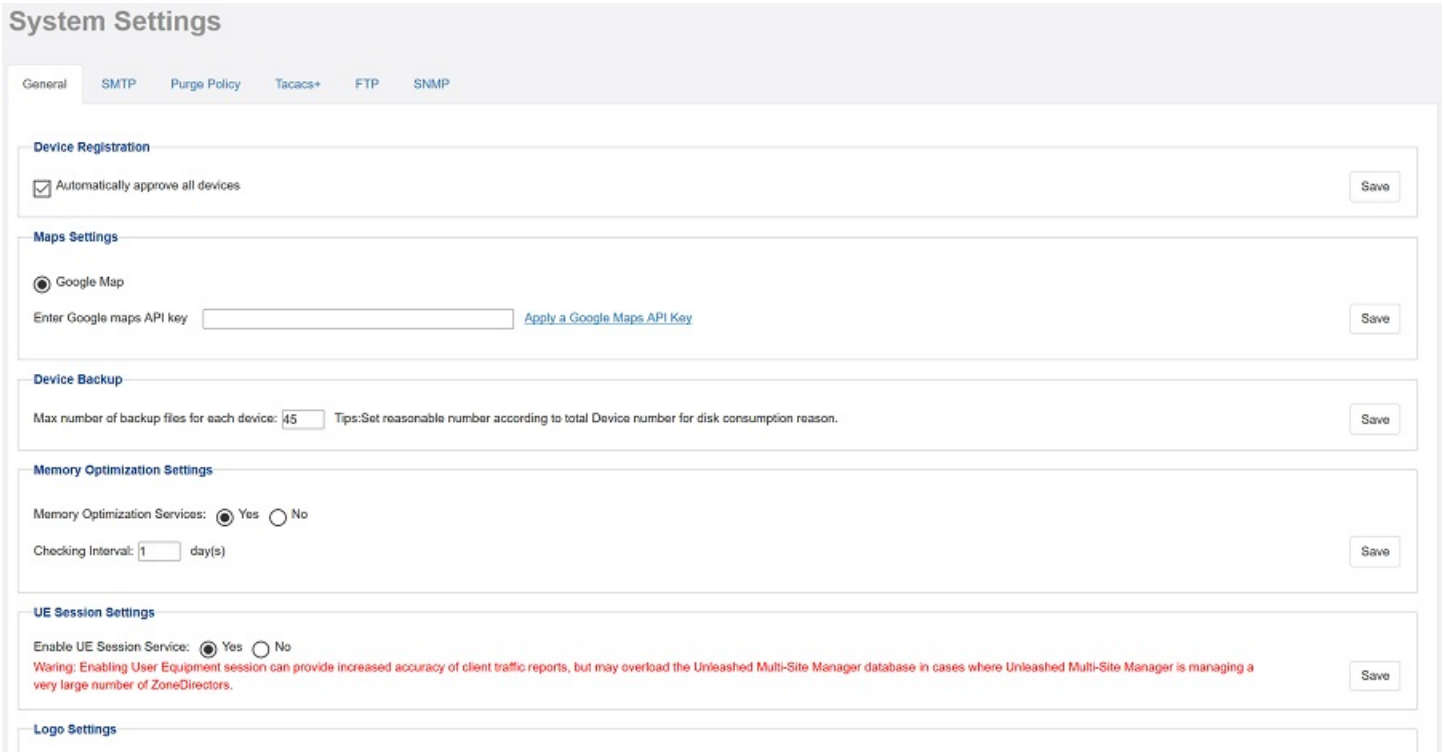


FIGURE 49 System Settings Page (part 2 of 4)

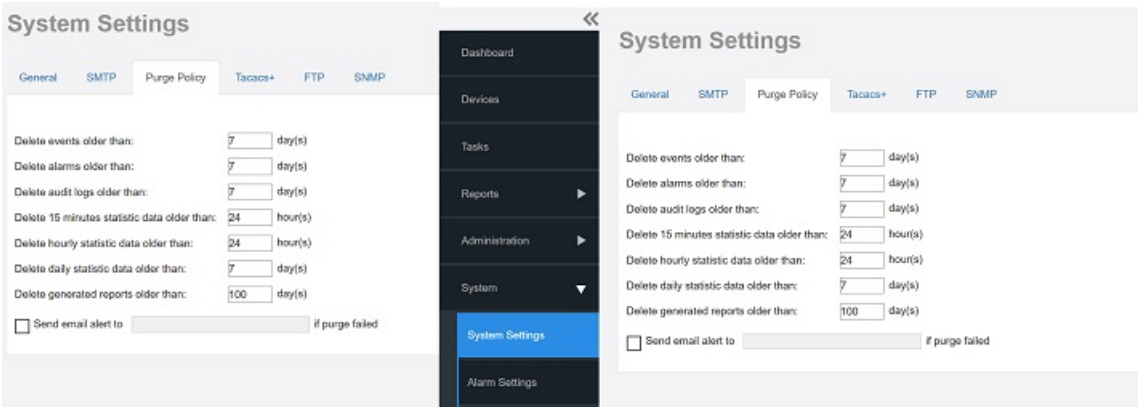


FIGURE 50 System Settings Page (part 3 of 4)

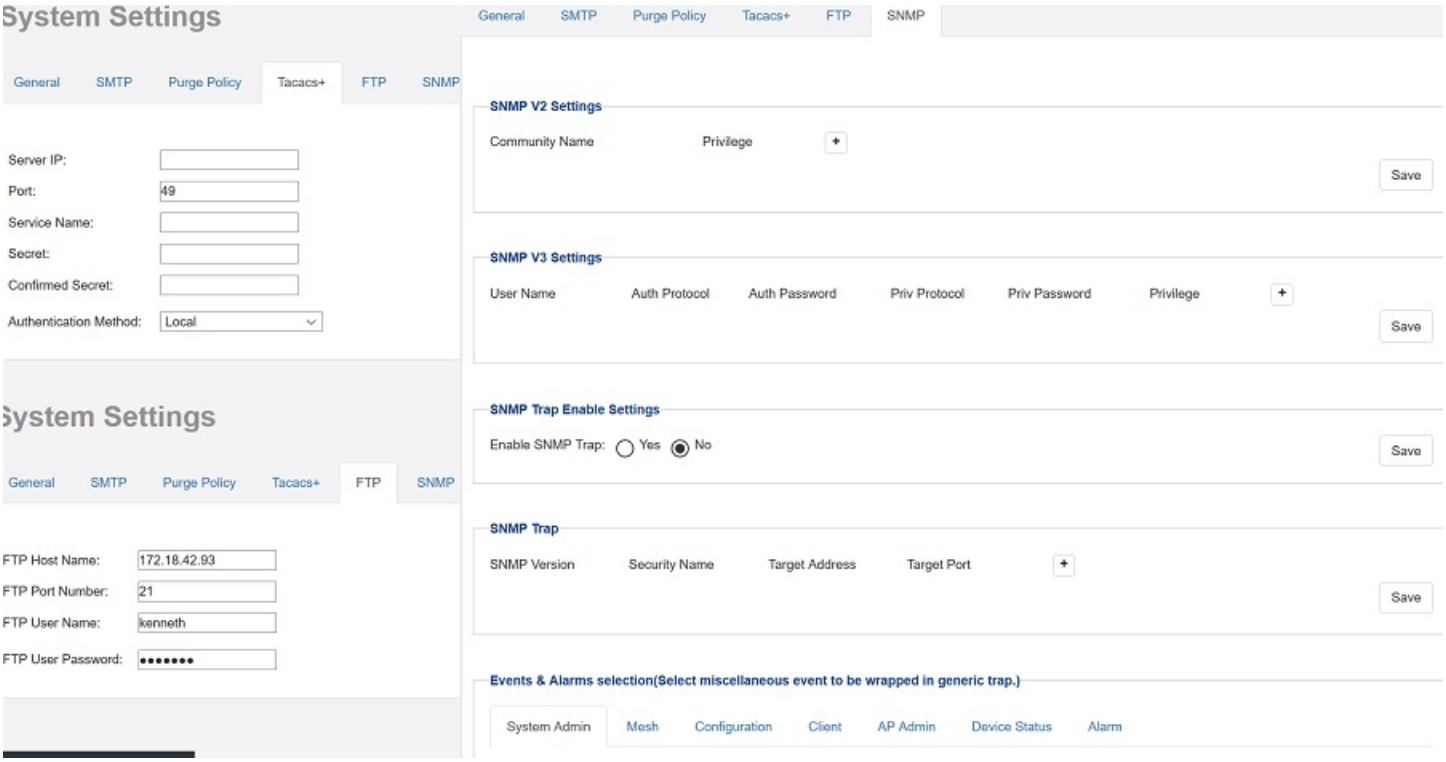


FIGURE 51 System Settings Page (part 4 of 4)



General Settings

You can configure some general settings such as device registration, map settings, ZD backup, memory optimization and so on.

Device Registration

This setting 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 (UE) 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.

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 50 KB, with a recommended size of 138 by 40 pixels.

1. Prepare a 138 by 40 pixels 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.

SMTP Settings

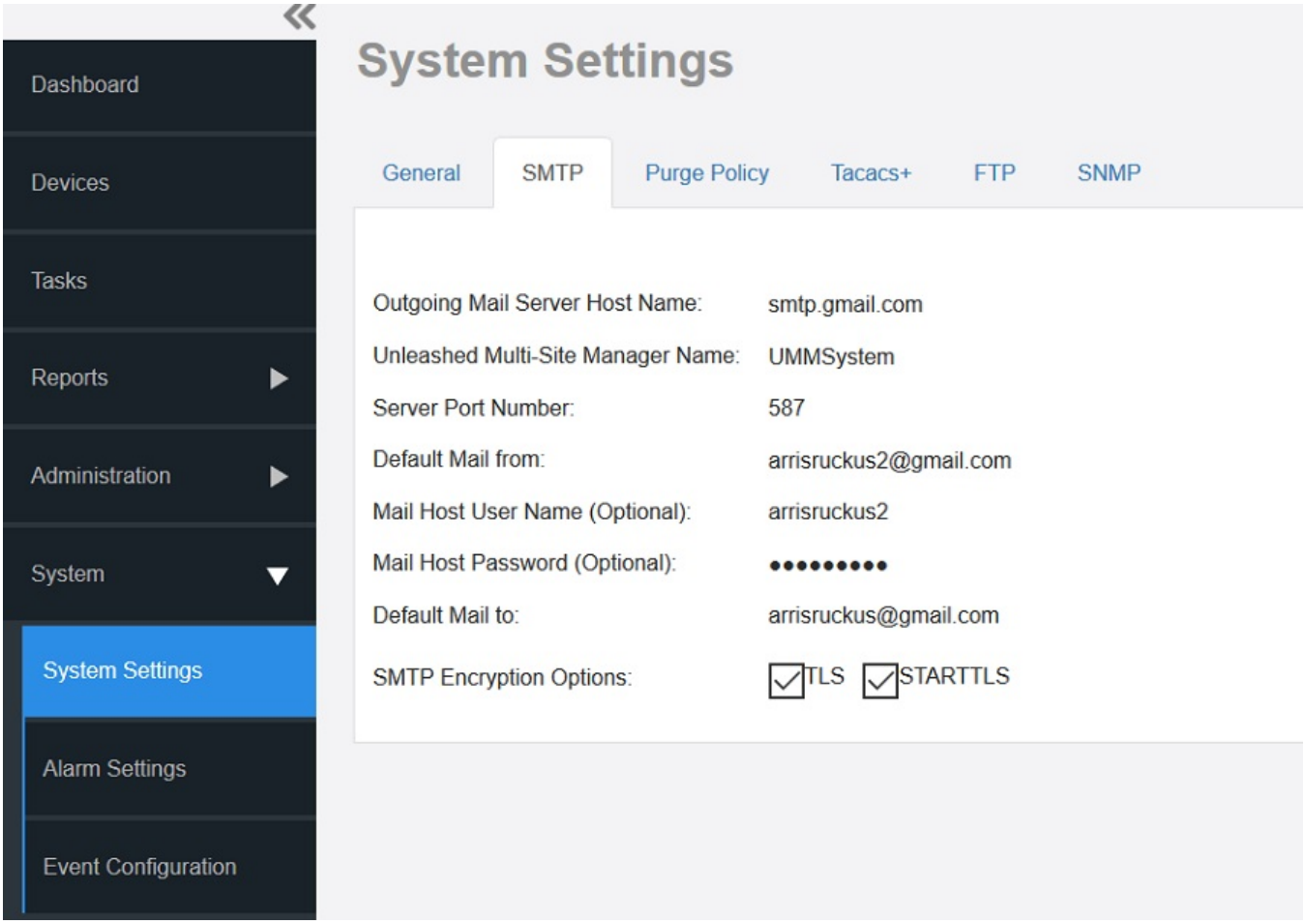
You must configure the software's host server to enable it to send email notifications. For example, the Audit Log and System Log menu items offer email options. When sending logs via email, the entire contents of these log files are sent to the preconfigured recipient (**Default Mail To**) specified on the **SMTP Settings** page.

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

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

2. Click **SMTP**.

FIGURE 52 SMTP Settings



3. In **Outgoing Mail Server Host Name**, type the host name of the outgoing SMTP server.
4. (Optional) In **UMM Name**, enter a new name for the software server.
5. In **Server Port Number**, type the SMTP server's listening port number.
   The default SMTP port number is 25.

   NOTE
   . If you select TLS or STARTTLS SMTP Encryption Options, You must check the SMTP host name and port number with the SMTP service provider, and configure Unleashed Multi-Site Manager accordingly. For example, the Gmail server uses 587 as its STARTTLS port and 465 as the TLS port, and the QQ server uses 25 as its non-SSL port and 465 as its TLS port.
   If your port number setting and protocol setting do not match, emails cannot be sent successfully. For example, if you select port 25 and select STARTTLS for a QQ server, testing will fail. Emails do not automatically revert to the non-TLS protocol.

6. In **Default Mail from**, type the email address that appears as the sender of the email.

7. In **Mail Host User Name (Optional)**, type the SMTP user name for the email account that you are using to send email notifications.
8. In **Mail Host Password (Optional)**, type the SMTP password for the email account.
9. In **Default Mail to**, type the email address of the user to whom you want to send email notifications.
10. In **SMTP Encryption Options**:
    - Check the **TLS** box if you want 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.
11. 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.
12. Click the **Save** button that is in the same section.

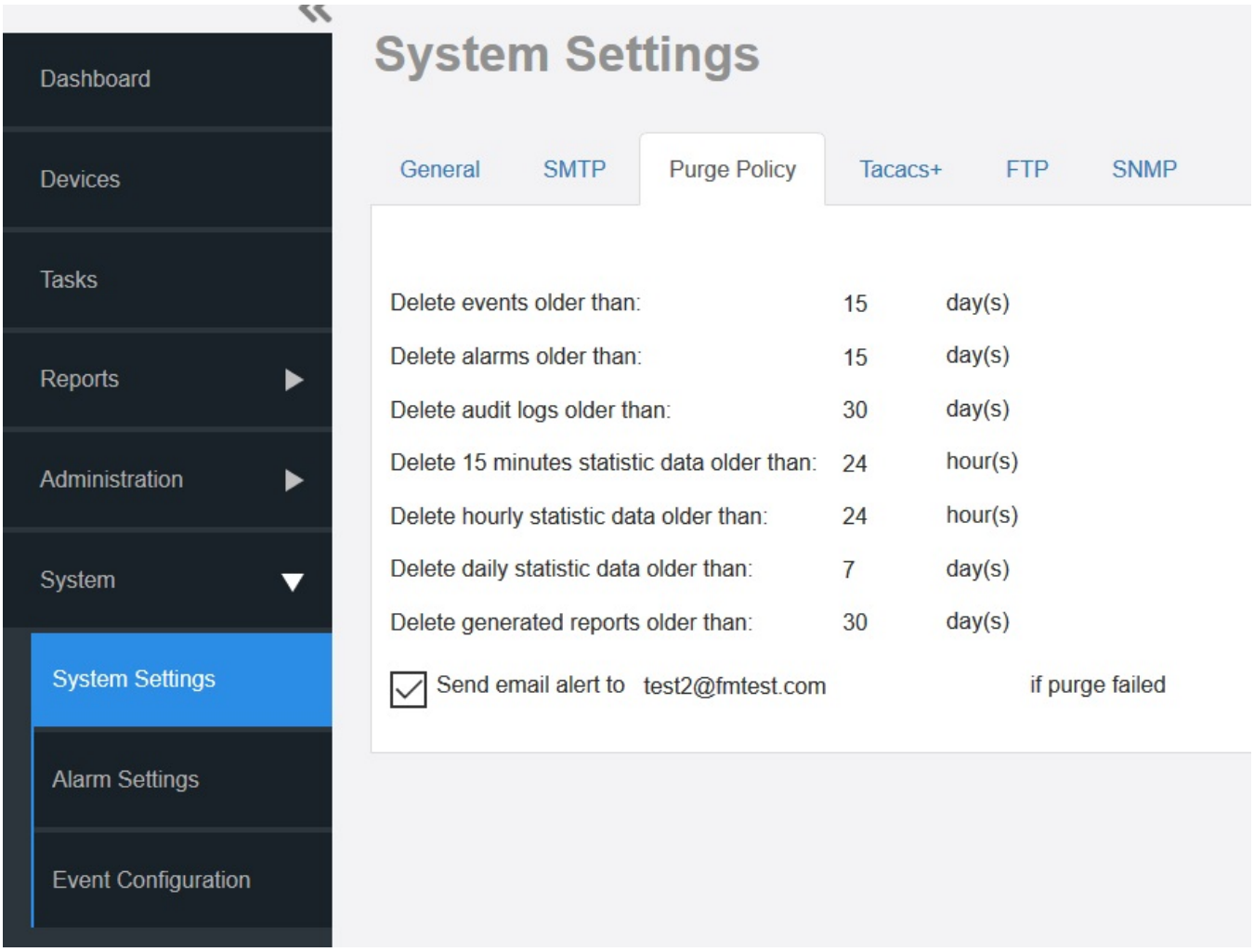
Purge Policy

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.

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

2. Click **Purge Policy**.

FIGURE 53 Purge Policy Settings



3. Type a numerical value (all values are number of days) for one or more of the following:
   - Delete events older than
   - Delete alarms older than
   - Delete audit logs older than
   - Delete 15 minutes statistic data older than
   - Delete hourly statistic data older than
   - Delete daily statistic data older than
   - Delete generated reports older than
4. Click **Save**.

   If purge fails, an email notification is sent to the email address provided.

TACACS+

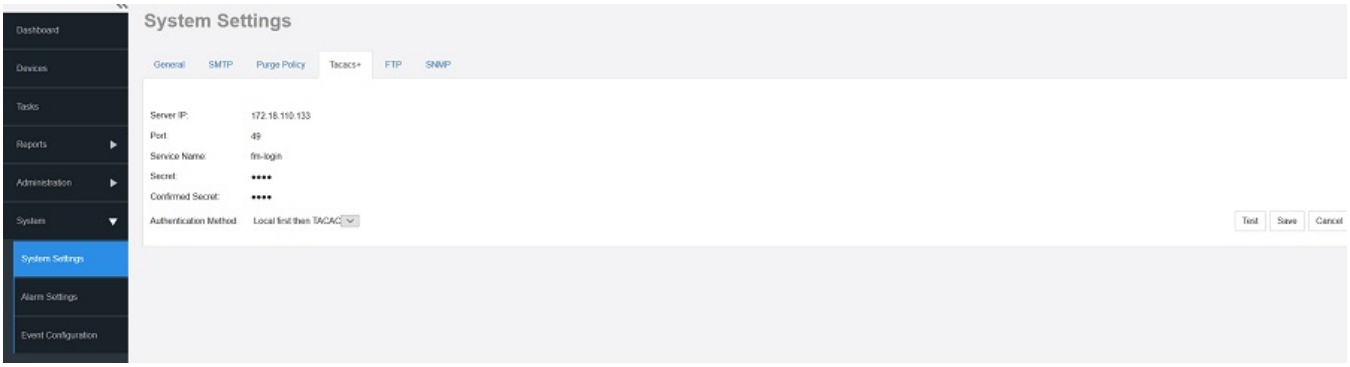
TACACS+ is an access control network protocol that provides separate authentication, authorization and accounting services.

NOTE
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 (Unleashed Multi-Site Manager will authenticate the user against the local database first and then against the TACACS server.)
- First TACACS then local (Unleashed Multi-Site Manager will authenticate the user against the TACACS server first and then against the local database.) The **Authentication Mode** affects the user login process.

1. Go to **Administration** > **System Settings**.
2. Click**Tacacs+** section.

FIGURE 54 TACACS+ Settings



3. Enter the TACACS+ parameters:
   - *Server* - IP or the host name of the TACACS server.
   - *Port* - The port number of the TACACS service, the default value is 49.
   - *Service Name*.
   - *Secret*.
   - *Confirmed Secret*.
4. 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.
5. Click **Save**.

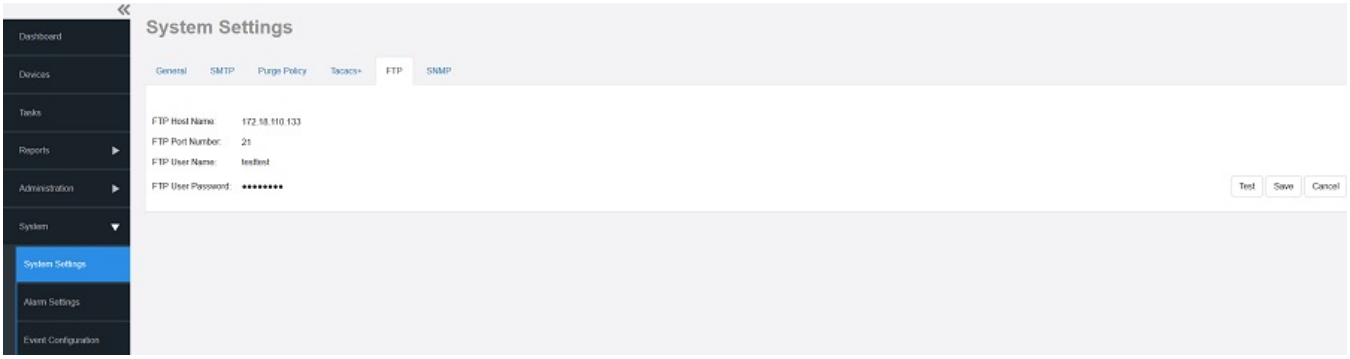
FTP Server Settings

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

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

2. Click **FTP** section.

FIGURE 55 Editing FTP Server Settings



3. Enter the FTP parameters:
   - *FTP Host Name* - IP or the host name of the FTP server.
   - *FTP Port Number* - The port number of the FTP service. The default value is 21.
   - *FTP User Name* - Login.
   - *FTP User Password* - Server password.
4. 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.
5. 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.

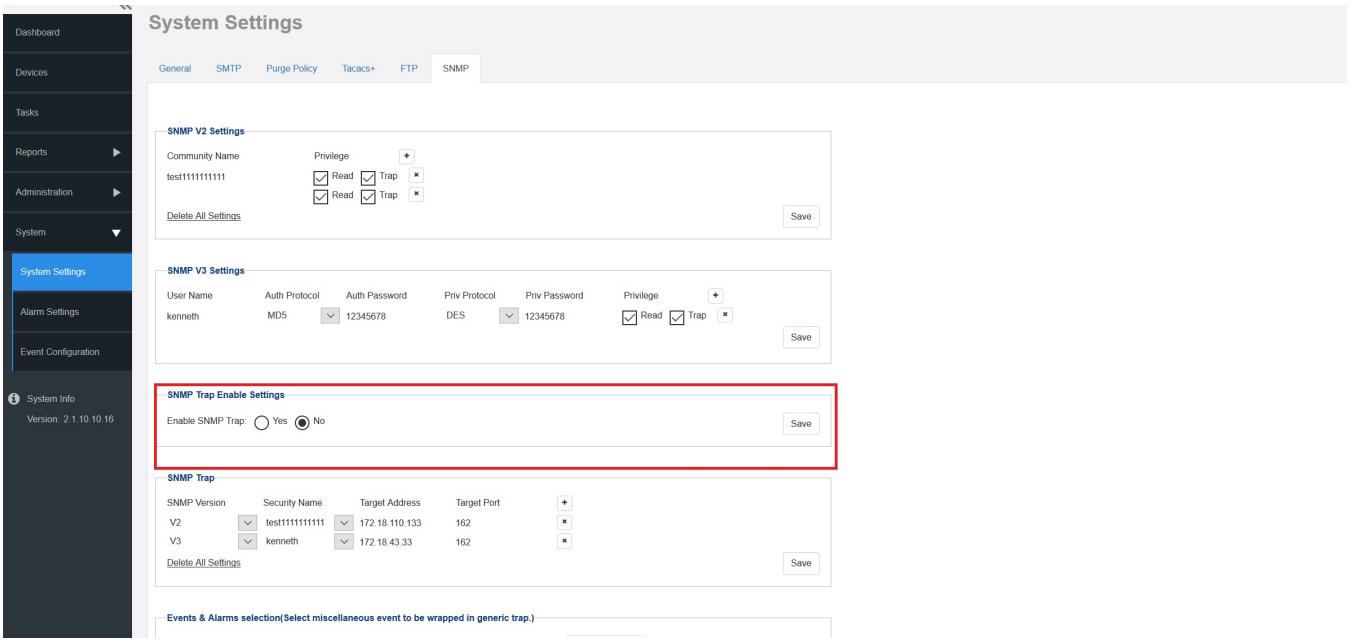
Enabling SNMP Traps

Before you can send SNMP trap notifications, you must enable SNMP trap notifications.

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

2. Click **SNMP Settings**.

FIGURE 56 SNMP Configuring Settings



3. In **Enable SNMP Trap**, click **Yes** or **No**.
4. Click **save**.
5. 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 SNMPv2

1. Click the **System Settings** > **SNMP** tab.
2. Under **SNMPv2 Settings**, configure the following settings:
   a) *Community:* Enter the SNMPv2 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 SNMPv2 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 **System Settings** > **SNMP** 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** section, scroll down to the **Events & Alarms selection** section.
2. 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.
3. Repeat as required.
4. Click **Save** to save your changes.

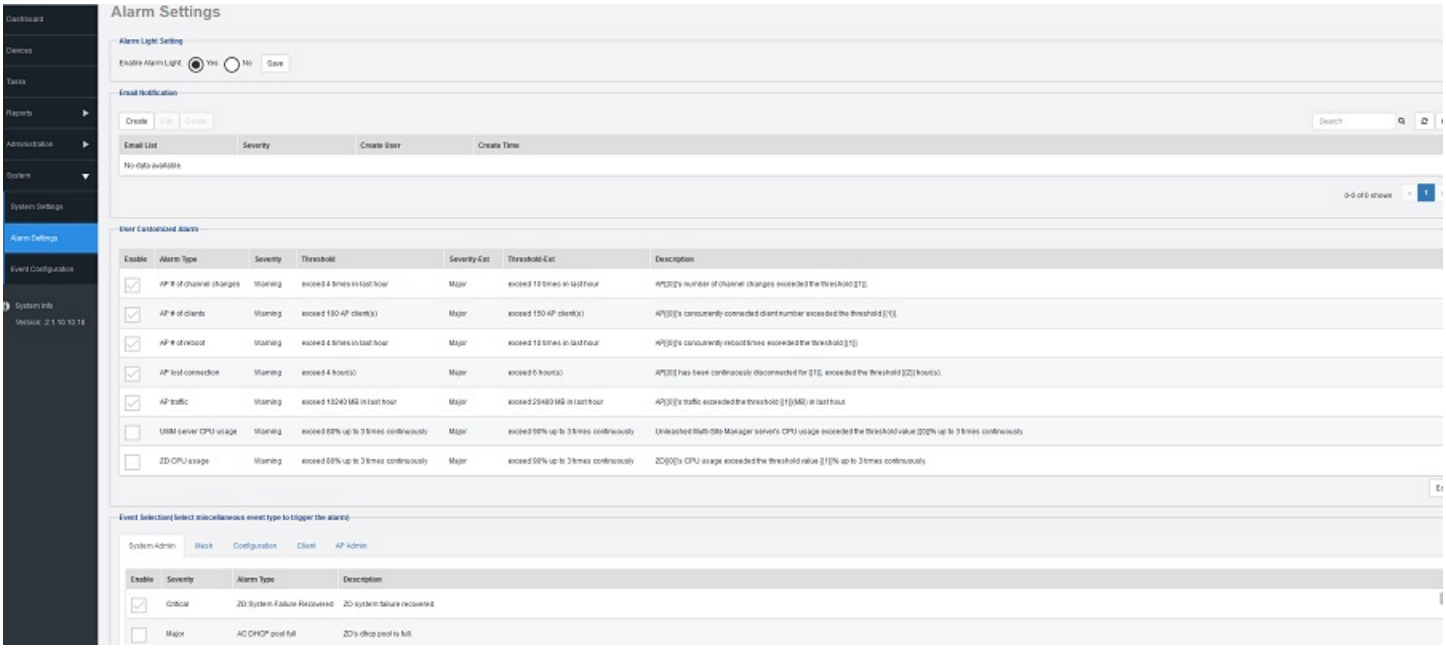
Setting User Customized Alarms

Refer to User-Customized Alarms on page 105 and Configuring Alarm Settings on page 103 for information about user-customized threshold-crossing alarms.

Alarm Settings

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

FIGURE 57 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 **System** > **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** 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 WLAN Controller** 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. In the **User Customized Alarm** section configure the alarm types 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
8. Select each tab under the **Event Selection** 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. Click the **Save** button in the **Event Selection** section.

You have completed configuring the alarm settings.

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 103 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 103 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).

NOTE
Unleashed networks do not support the ZD CPU Usage alarm.

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

Monitoring Events

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

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

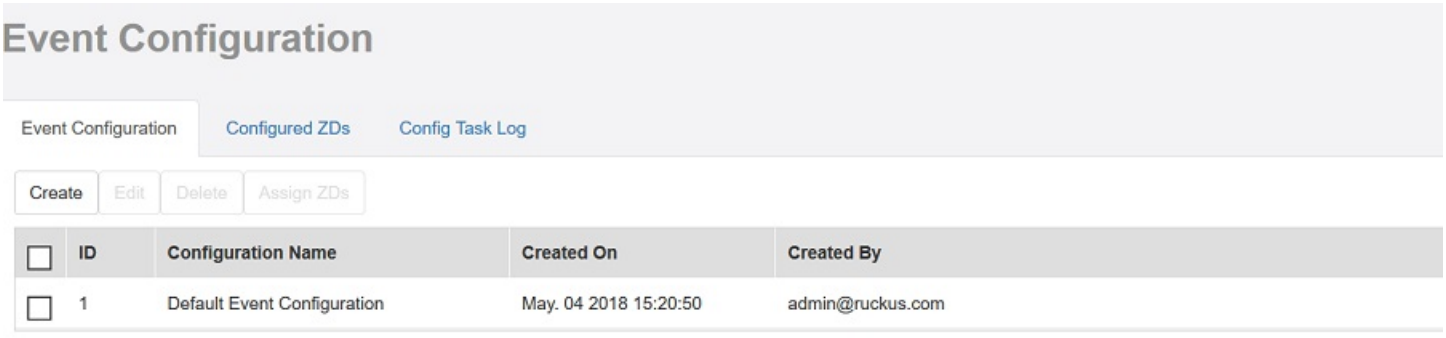
- **Date/Time**: When the event occurred.
- **Event Type**: Ruckus designated event title.
- **Sev**: Severity of the event.
- **Device Name**: Name of the device.
- **Activity**: A description of the event.

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.

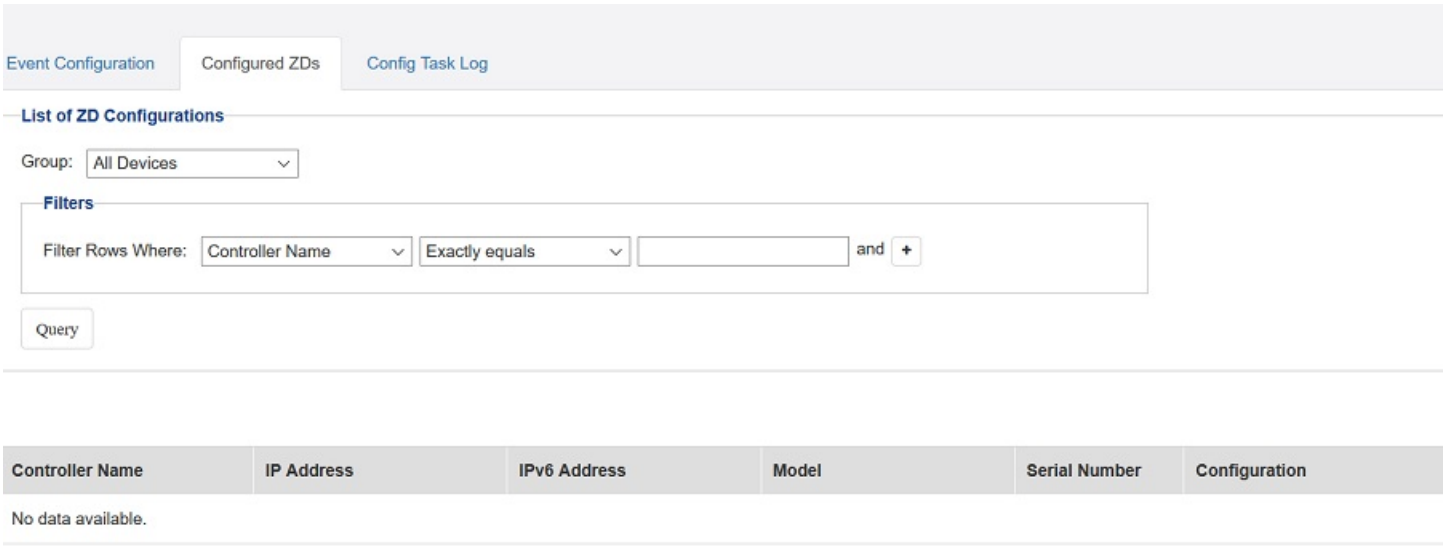
FIGURE 58 Event Configuration



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.

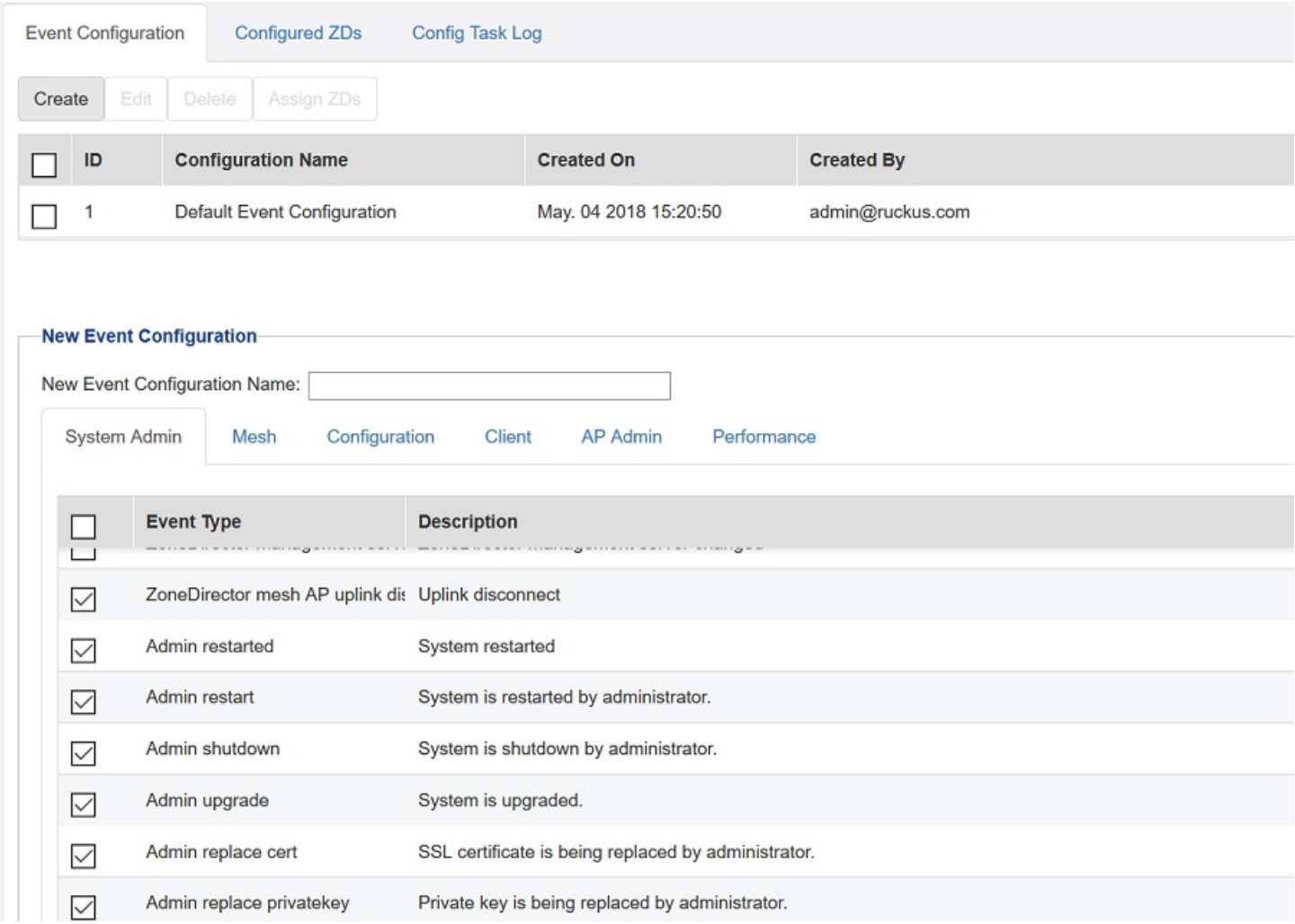
Multiple filter queries can be clubbed by clicking the "+" sign against each query row. Once all your filter queries are entered, click te **Query** button on the bottem right corner of the page to run the query and fetch the result. The result is displayed in the **List of ZDs** section.

FIGURE 59 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.

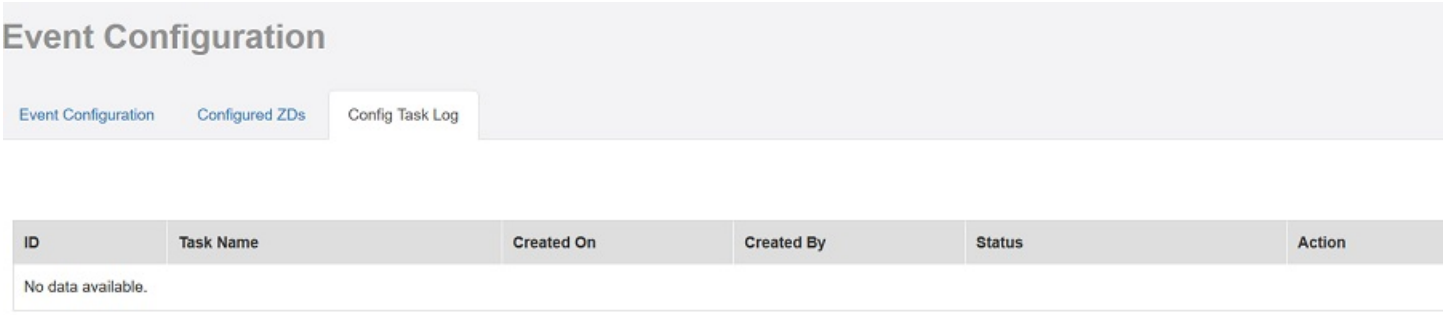
FIGURE 60 New Event Configuration



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 61 Task Logs



Appendix

- Configuring Unleashed Multi-Site Manager Behind the NAT Server..... 111
- Configuring Unleashed Multi-Site Manager In Front of NAT Server..... 112
- Configuring the 200.6 Unleashed Setup 113
- Configuring ZoneDirector & 200.5 Unleashed Behind NAT Server..... 115
- Configuring ZoneDirector & 200.5 Unleashed In Front of the NAT Server.....120
- Setting Up Unleashed Multi-Site Manager as a Virtual Machine.....122

Configuring Unleashed Multi-Site Manager Behind the NAT Server

You can configuring Unleashed Multi-Site Manager behind the NAT Server

Ensure that the following software requirements are met before installing the software.

- 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)

Before installing this version of the software install jemalloc. Follow these steps to install jemalloc:

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

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

Before installing this version of Unleashed Multi-Site Manager, you must upgrade Openssl and its library to the right Linux version as specified:

- RedHat or CentOS 6.x: Openssl 1.0.1 or later
- RedHat or CentOS 7.x: Openssl 1.0.2 or later

For example, you can issue this command to upgrade Openssl version with Linux:

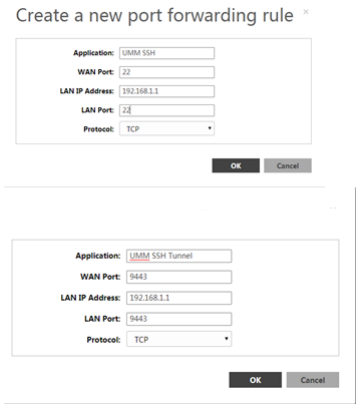
```
yum upgrade openssl 1.0.2
```

1. Install Unleashed Multi-Site Manager. See the *Installing and Upgrading Unleashed Multi-Site Manager*Unleashed Multi-Site Manager section of the *Unleashed Multi-Site Manager User Guide*
2. Login to the NAT server.

   By default, Unleashed Multi-Site Manager uses port 9443 and 22 to bring up the SSH tunnel. Ensure you allow these ports on your firewall and map them to the Unleashed Multi-Site Manager server on your NAT server.

3. Create port forwarding rules: TCP: UMM IP: 9443 and TCP: UMM IP: 22

FIGURE 62 Sample Port Forwarding Rule for Ports 22 and 9443



Configuring Unleashed Multi-Site Manager In Front of NAT Server

You can configure Unleashed Multi-Site Manager in front of the NAT Server

Ensure that the following software requirements are met before installing the software.

- 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)

Before installing this version of the software install jemalloc. Follow these steps to install jemalloc:

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

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

Before installing this version of Unleashed Multi-Site Manager, you must upgrade Openssl and its library to the right Linux version as specified:

- RedHat or CentOS 6.x: Openssl 1.0.1 or later
- RedHat or CentOS 7.x: Openssl 1.0.2 or later

For example, you can issue this command to upgrade Openssl version with Linux:

```
yum upgrade openssl 1.0.2
```

1. Install Unleashed Multi-Site Manager. See the Installing and Upgrading Unleashed Multi-Site Manager section of the *Unleashed Multi-Site Manager User Guide*

2. Login to the NAT server.

   By default, Unleashed Multi-Site Manager uses port 9443 and 22 to bring up the SSH tunnel. Ensure you allow these ports on your firewall.

Configuring the 200.6 Unleashed Setup

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 66.

   There are two types of Unleashed Multi-Site Manager licenses files; one for ZoneDirector and the other for Unleashed. Ensure you select the correct file.

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 63 Generating Unleashed ID

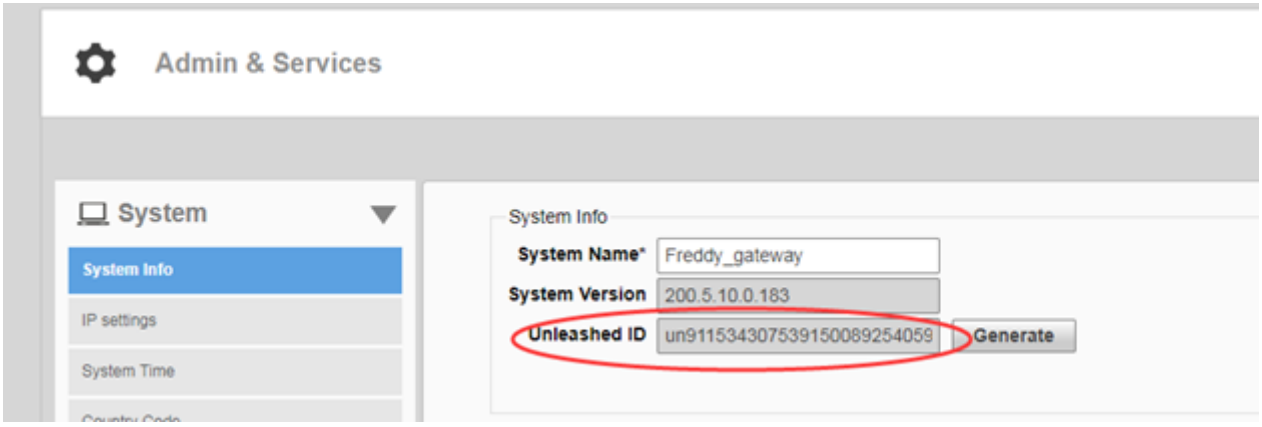
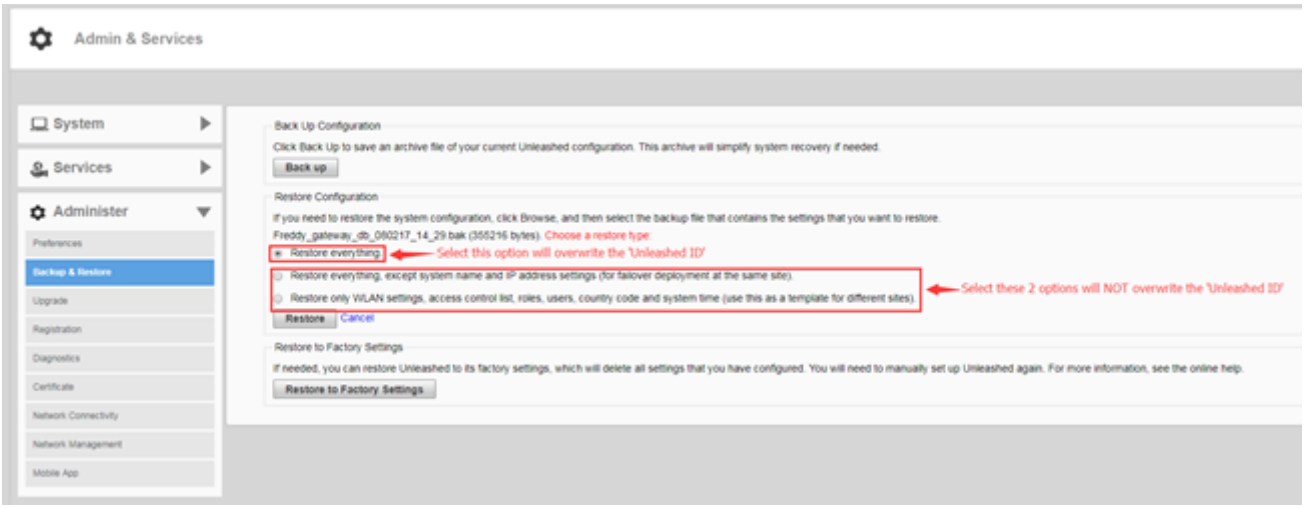


FIGURE 64 Unleashed - Restore Configuration

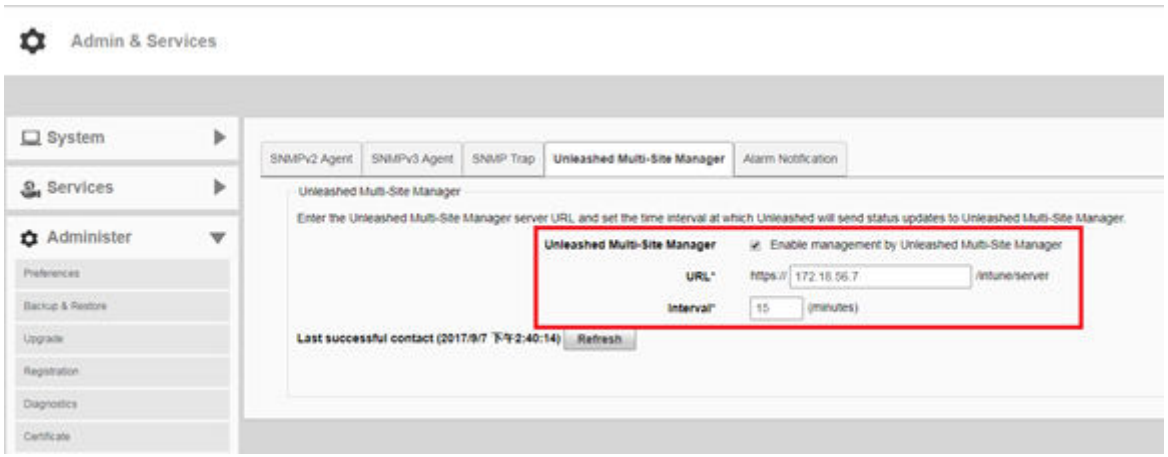


3. Enable software management from Unleashed web interface:
   a) Go to **Admin & Services** > **Administer** > **Network Management** > **Unleashed Multi-Site Manager Management**.
   b) Select the **Enable management by Unleashed Multi-Site Manager** check-box.

      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 65 Enabling Unleashed Multi-Site Manager Management



4. Log in to the Unleashed Multi-Site Manager web interface and go to **Devices**. The Unleashed device will be registered and displayed.
5. Login to the Unleashed Multi-Site Manager web interface, and go to **Devices**.

   You will see the unleashed devices.

You have successfully set up 200.6 Unleashed devices and registered the Unleashed device for Unleashed Multi-Site Manager to monitor.

Configuring ZoneDirector & 200.5 Unleashed Behind NAT Server

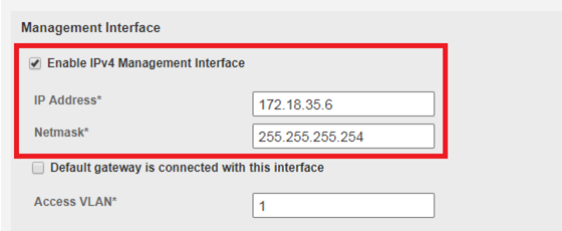
ZoneDirector and 200.5 Unleashed do not support SSH tunnels. Therefore for these devices behind the NAT server, it is recommend to enable the Management Interface, add one 443 port mapping on the NAT server and then configure the external port to the Unleashed Multi-Site Manager.

1. Upload the Unleashed license as described in Uploading a License File on page 66.

   There are two types of Unleashed Multi-Site Manager licenses files; one for ZoneDirector and the other for Unleashed. Ensure you select the correct file.

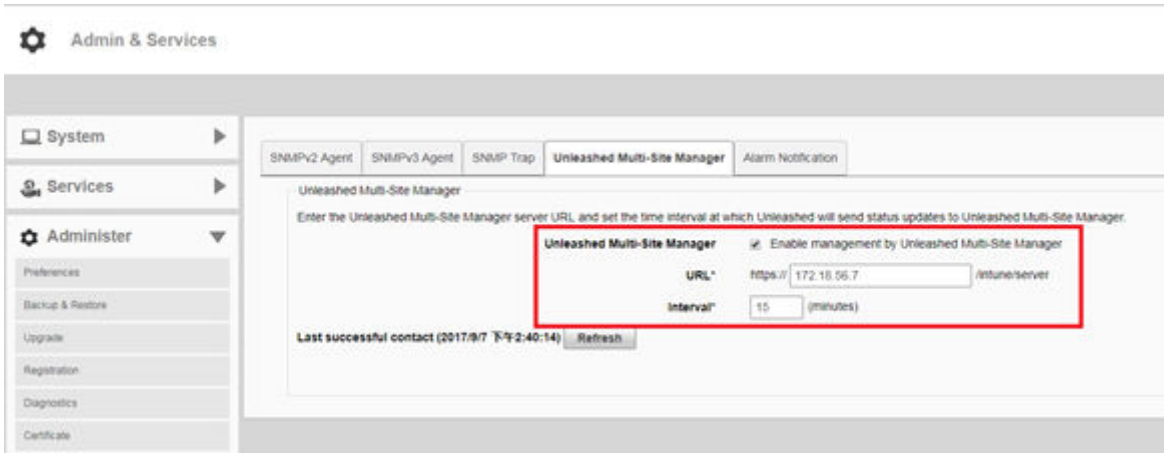
2. Enable and configure the management interface according to your network from ZoneDirector web interface:
   a) Go to **Configure** > **System** > **Network Management**.
   b) In **FlexMaster Management**, select the **Enable IPv4 Management Interface** check-box.
   Configure the following:
   - IP Address: enter IP address of the software server.
   - NetMask: enter the netmask IP address.

FIGURE 66 Enabling and Configuring the Management Interface on ZD



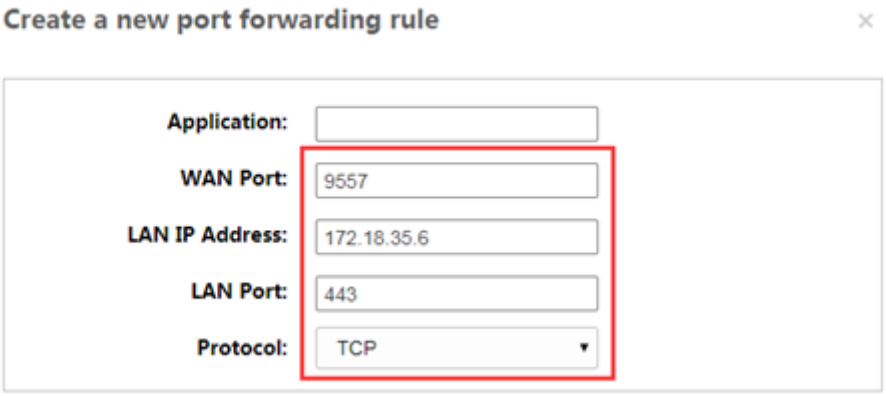
3. Enable and configure the management interface according to your network from 200.5 Unleashed web interface:
   a) Go to **Admin & Services** > **System** > **IP Setting** > **Management Interface**.
   b) Select the **Enable management by Unleashed Multi-Site Manager** check-box.
   Configure the 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 67 Enabling Unleashed Multi-Site Manager Management



4. Log in to the NAT server and map the LAN port to 443. Create a port forwarding rule: TCP: management IP: 443

FIGURE 68 Sample Port Mapping



5. 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 69 Generating Unleashed ID

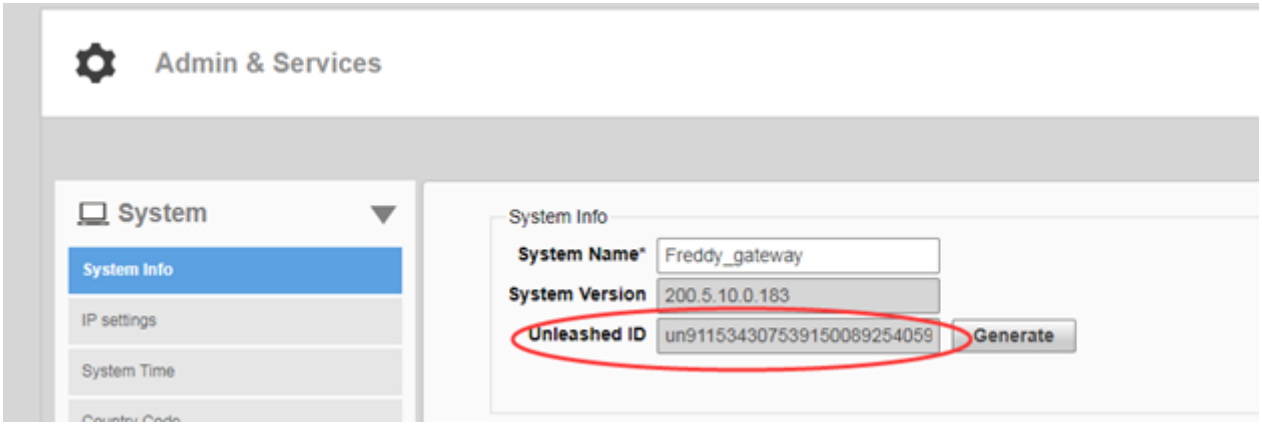
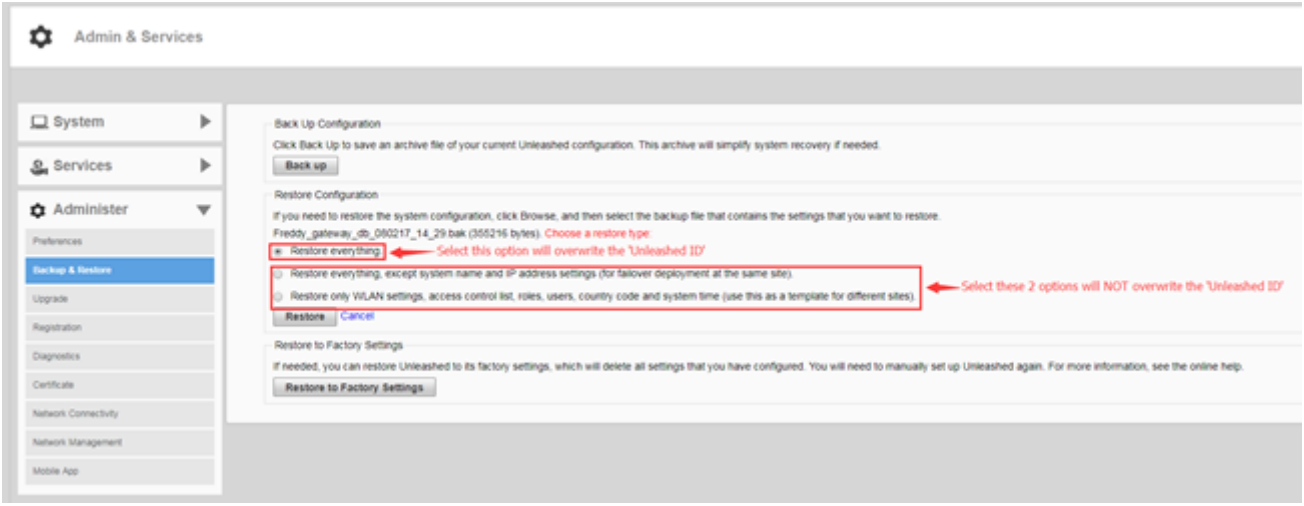


FIGURE 70 Unleashed - Restore Configuration

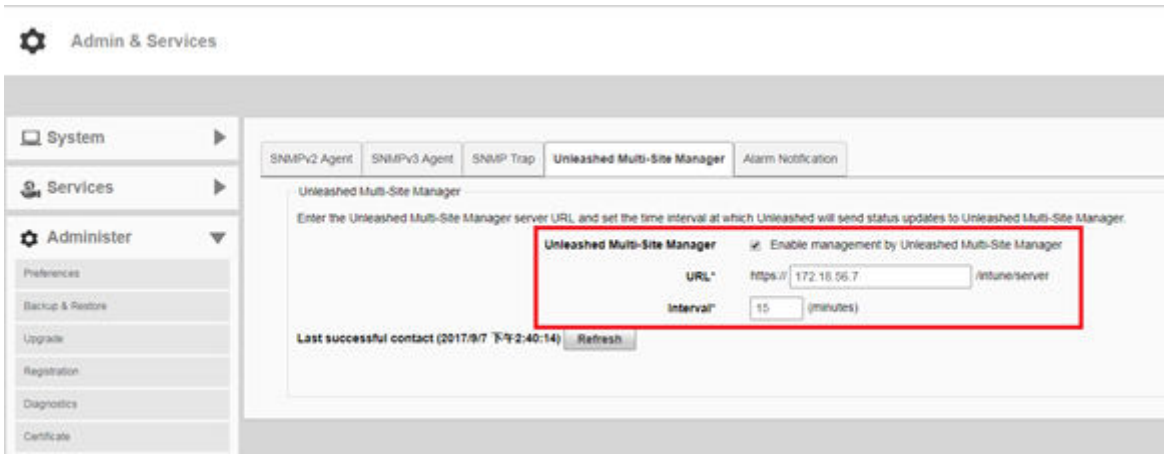


6. Enable Unleashed Multi-Site Manager management from Unleashed web interface:
   a) Go to **Admin & Services** > **Administer** > **Network Management** > **Unleashed Multi-Site Manager Management**.
   b) Select the **Enable management by Unleashed Multi-Site Manager** check-box.

      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 71 Enabling Unleashed Multi-Site Manager Management



7. 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 72 Enabling Unleashed Multi-Site Manager Management on ZD



Login to the Unleashed Multi-Site Manager web interface and go to **Devices**. You will see the ZD and Unleashed devices.

8. In the Unleashed Multi-Site Manager web interface, go to **Devices**. Select the device which is behind the NAT server, and click **Edit**. Configure the values.

FIGURE 73 Configuring External Ports



9. Click **Save**. The external port which you configured in step 3 is submitted.

Configuring ZoneDirector & 200.5 Unleashed In Front of the NAT Server

You can configure ZoneDirector & 200.5 Unleashed in front of the NAT Server.

1. Upload the Unleashed license as described in Uploading a License File on page 66.

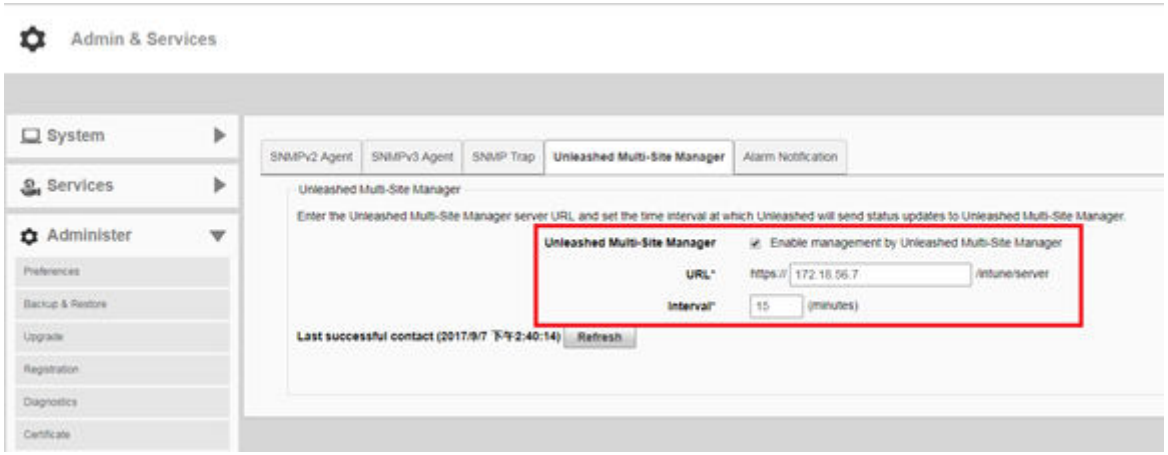
   There are two types of Unleashed Multi-Site Manager licenses files; one for ZoneDirector and the other for Unleashed. Ensure you select the correct file.

2. Enable and configure the management interface according to your network from 200.5 Unleashed web interface:
   a) Go to **Admin & Services** > **Adminster** > **Netwrok 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

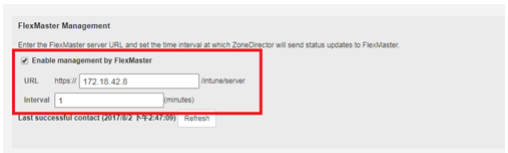


3. Enable and configure the management interface according to your network from ZoneDirector web interface:
   a) Go to **Configure** > **System** > **Network Management**.
   b) In **FlexMaster Management**, select the **Enable Management by FlexMaster** check-box.

      Configure the following:

      - URL: The IP address or URL of the software server.
      - Interval: the time interval (in minutes) within which the 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 75 Enabling Unleashed Multi-Site Manager Management on ZD



4. Login to the Unleashed Multi-Site Manager web interface and go to **Devices**. The ZD and 200.5 Unleashed devices will be listed.

Setting Up Unleashed Multi-Site Manager as a Virtual Machine

You can setup Unleashed Multi-Site Manager as a virtual machine, where, the VM image is a VMWare EXSI image that integrates the software with CentOS 6.5.

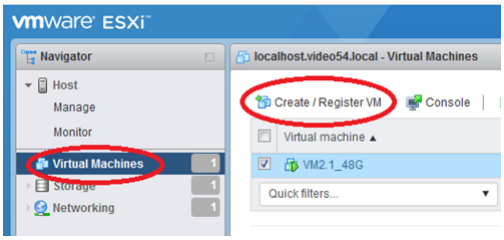
Minimum hardware requirements:

- 8 GB memory
- 4*1 processors
- 50 GB hard disk

You can only use VMWare EXSI images to create a VM, and it is recommend to use EXSI version 6.5.

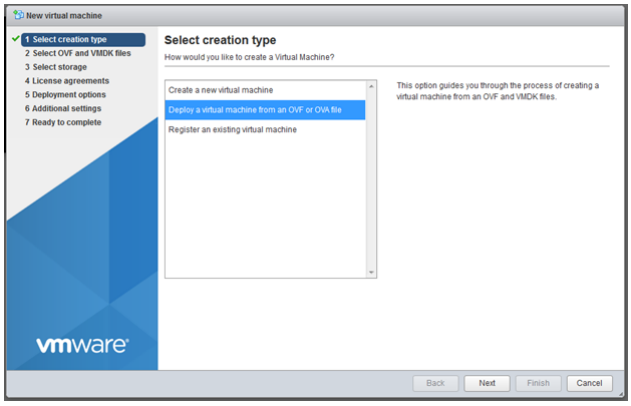
1. From the zip file, VM_UMM_ 2.1.0.0.27_Demo.7z extract the files.
   The files VM_UMM_2.1.0.0.27.ova, license-24-UMM.cert and VM_UMM_2.1 Release Note.docx are displayed.
2. Login to the VMware ESXI interface and go to **Virtual Machines**.

   FIGURE 76 Registering the VM



3. Click **Create/Register VM**.
   The **New virtual machine** page appears.

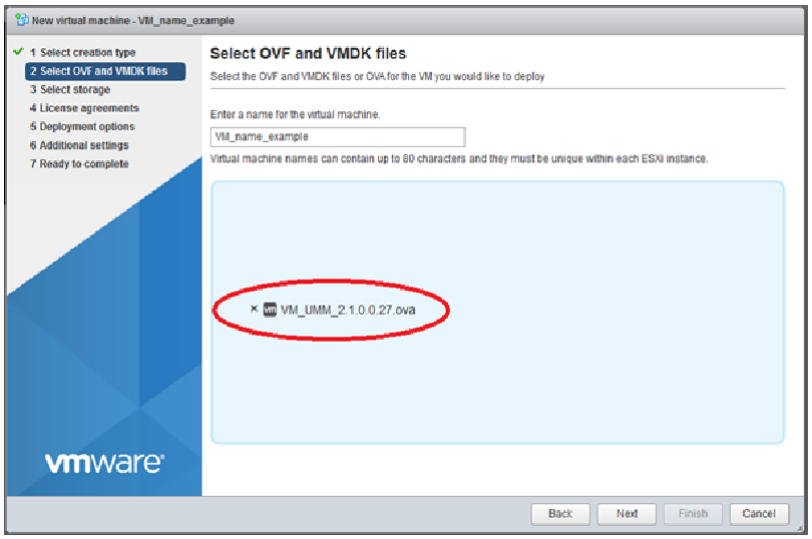
   FIGURE 77 Creating a VM



4. Select **Deploy virtual machine from an OVF or OVA file** and click **Next**.

5. Type the name virtual machine and select the VM_UMM_2.1.0.0.27.ova file.

FIGURE 78 Selecting the OVA File

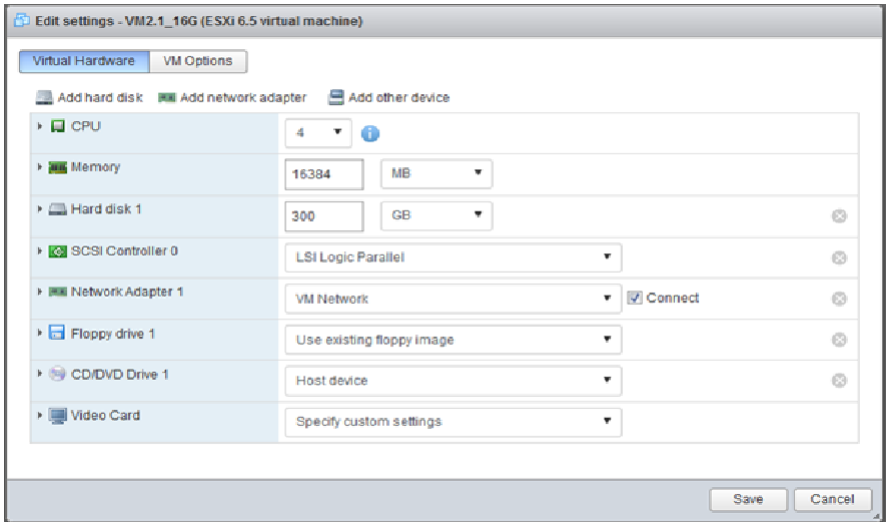


6. Click **Next**.

   Continue to click **Next** for the consequent screens, and click **Finish** to complete the VM creation.

   After you power off the device, you can edit the VM settings. You can change settings for the CPU, memory and hard disk according to your lab requirement.

FIGURE 79 Editing VM Settings



7. Power on the VM and wait several minutes to login to Unleashed Multi-Site Manager.

   After you login, you can do the following:

   - Change the root password for your Linux account. See Changing the Linux Password on page 133 for more information.
   - Change the login credential for Unleashed Multi-Site Manager. See Changing the Login Information for the Virtual Machine on page 133 for more information.
   - Change the login credentials for the database. See Changing the Login Credentials to Access the Database on page 134 for more information.

8. Using SSH, establish a connection with Unleashed Multi-Site Manager to change the time zone and date. See the following example.

[root@localhost ~]# date

```
Fri Jun 29 04:14:46 EDT 2018
```

[root@localhost ~]# tzselect

```
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
```

#? 5

```
Please select a country.
1) Afghanistan 18) Israel 35) Palestine
2) Armenia 19) Japan 36) Philippines
3) Azerbaijan 20) Jordan 37) Qatar
4) Bahrain 21) Kazakhstan 38) Russia
5) Bangladesh 22) Korea (North) 39) Saudi Arabia
6) Bhutan 23) Korea (South) 40) Singapore
7) Brunei 24) Kuwait 41) Sri Lanka
8) Cambodia 25) Kyrgyzstan 42) Syria
9) China 26) Laos 43) Taiwan
10) Cyprus 27) Lebanon 44) Tajikistan
11) East Timor 28) Macau 45) Thailand
12) Georgia 29) Malaysia 46) Turkmenistan
13) Hong Kong 30) Mongolia 47) United Arab Emirates
14) India 31) Myanmar (Burma) 48) Uzbekistan
15) Indonesia 32) Nepal 49) Vietnam
16) Iran 33) Oman 50) Yemen
17) Iraq 34) Pakistan
```

#? 9

```
Please select one of the following time zone regions.
1) Beijing Time
2) Xinjiang Time
```

#? 1

```
The following information has been given:
China
Beijing Time
```

Therefore TZ='Asia/Shanghai' will be used.

```
Local time is now: Fri Jun 29 16:14:59 CST 2018.
Universal Time is now: Fri Jun 29 08:14:59 UTC 2018.
Is the above information OK?
1) Yes
2) No
```

#? 1

You can make this change permanent for yourself by appending the line TZ='Asia/Shanghai'; export TZ to the file '.profile' in your home directory; then log out and log in again.

Here is that TZ value again, this time on standard output so that you can use the **/usr/bin/tzselect** command in shell scripts: Asia/Shanghai

[root@localhost ~]# vi /etc/sysconfig/clock //change to ZONE="Asia/Shanghai"

[root@localhost ~]# rm -rf /etc/localtime

[root@localhost ~]# ln -s /usr/share/zoneinfo/Asia/Shanghai /etc/localtime

[root@localhost ~]# cat /etc/sysconfig/clock

```
ZONE="Asia/Shanghai"
```

[root@localhost ~]# date -s 7/12/2018

```
Thu Jul 12 00:00:00 CST 2018
```

[root@localhost ~]# date -s 11:34:30

```
Thu Jul 12 11:34:30 CST 2018
```

[root@localhost ~]# date

```
Thu Jul 12 11:34:32 CST 2018
```

9. If you have modified the VM settings (refer Step 6), then you can change the size of the linux hard disk as well. See the following example.

[root@localhost ~]# df -h

```
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/VolGroup-lv_root 44G 7.5G 35G 19% /
tmpfs 7.8G 0 7.8G 0% /dev/shm
/dev/sda1 485M 32M 428M 7% /boot
```

[root@localhost ~]# fdisk -l

```
Disk /dev/sda: 322.1 GB, 322122547200 bytes
255 heads, 63 sectors/track, 39162 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00057088
Device Boot Start End Blocks Id System
/dev/sda1 * 1 64 512000 83 Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2 64 6528 51915776 8e Linux LVM
Disk /dev/mapper/VolGroup-lv_root: 47.8 GB, 47789899776 bytes
255 heads, 63 sectors/track, 5810 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
Disk /dev/mapper/VolGroup-lv_swap: 5368 MB, 5368709120 bytes
255 heads, 63 sectors/track, 652 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

[root@localhost ~]# fdisk /dev/sda

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to switch off the mode (command 'c') and change display units to sectors (command 'u').

Command (m for help): n

```
Command action
e extended
p primary partition (1-4)
```

p

Partition number (1-4): 3

```
First cylinder (6528-39162, default 6528):
Using default value 6528
Last cylinder, +cylinders or +size{K,M,G} (6528-39162, default 39162):
Using default value 39162
```

Command (m for help): t

Partition number (1-4): 3

Hex code (type L to list codes): 8e

Changed system type of partition 3 to 8e (Linux LVM)

Command (m for help): wq

The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource busy.

The kernel still uses the old table. The new table will be used at the next reboot or after you run partprobe(8) or kpartx(8)

Syncing disks.

[root@localhost ~]# fdisk -l

```
Disk /dev/sda: 322.1 GB, 322122547200 bytes
255 heads, 63 sectors/track, 39162 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00057088
Device Boot Start End Blocks Id System
/dev/sda1 * 1 64 512000 83 Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2 64 6528 51915776 8e Linux LVM
/dev/sda3 6528 39162 262139965 8e Linux LVM
Disk /dev/mapper/VolGroup-lv_root: 47.8 GB, 47789899776 bytes
255 heads, 63 sectors/track, 5810 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

```
Disk /dev/mapper/VolGroup-lv_swap: 5368 MB, 5368709120 bytes
255 heads, 63 sectors/track, 652 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

[root@localhost ~]# reboot

```
Broadcast message from root@localhost.localdomain
(/dev/pts/0) at 16:22 ...
```

The system is going down for reboot NOW!

```
[root@localhost ~]#
```

login as: root

root@172.18.42.209's password:

```
Last login: Fri Jun 29 16:19:13 2018 from 172.18.169.4
```

[root@localhost ~]# partprobe

Warning: the kernel failed to re-read the partition table on /dev/sda (Device or resource busy). As a result, it may not reflect all of your changes until after reboot.

[root@localhost ~]# partprobe /dev/sda3

[root@localhost ~]# pvcreate /dev/sda3

Physical volume "/dev/sda3" successfully created

[root@localhost ~]# df -h

```
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/VolGroup-lv_root 44G 7.5G 35G 19% /
tmpfs 7.8G 0 7.8G 0% /dev/shm
/dev/sda1 485M 32M 428M 7% /boot
```

[root@localhost ~]# vgextend VolGroup /dev/sda3

Volume group "VolGroup" successfully extended

[root@localhost ~]# vgdisplay

--- Volume group —

```
VG Name VolGroup
System ID
Format lvm2
Metadata Areas 2
Metadata Sequence No 4
VG Access read/write
```

```
VG Status resizable
MAX LV 0
Cur LV 2
Open LV 2
Max PV 0
Cur PV 2
Act PV 2
VG Size 299.50 GiB
PE Size 4.00 MiB
Total PE 76672
Alloc PE / Size 12674 / 49.51 GiB
Free PE / Size 63998 / 249.99 GiB
VG UUID 5YlcZA-1N5n-M1kd-cK2c-8UNP-Losa-DPKyst
```

[root@localhost ~]# lvresize -L +249.99G /dev/VolGroup/lv_root

```
Rounding size to boundary between physical extents: 249.99 GiB
Extending logical volume lv_root to 294.50 GiB
Logical volume lv_root successfully resized
```

[root@localhost ~]# resize2fs /dev/VolGroup/lv_root

```
resize2fs 1.41.12 (17-May-2010)
Filesystem at /dev/VolGroup/lv_root is mounted on /; on-line resizing required
old desc_blocks = 3, new_desc_blocks = 19
Performing an on-line resize of /dev/VolGroup/lv_root to 77201408 (4k) blocks.
The filesystem on /dev/VolGroup/lv_root is now 77201408 blocks long.
```

[root@localhost ~]# df -h

```
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/VolGroup-lv_root 290G 7.6G 268G 3% /
tmpfs 7.8G 0 7.8G 0% /dev/shm
/dev/sda1 485M 32M 428M 7% /boot
```

10. Restart Unleashed Multi-Site Manager. Issue the commands as shown in the following example.

    [root@localhost ~]# cd /opt/UMM/

    [root@localhost UMM]# ./restart.sh

    Restarting UMM...

    After a few minutes, you will be able to login to the Unleashed Multi-Site Manager interface.

Hardware Requirements and Specifications

The amount of memory and CPU power required on the Unleashed Multi-Site Manager server depends on the number of ZoneDirector devices and APs that software is to manage, and on the system configuration.

Refer to the following table as the examples of the minimum recommended RAM and CPU for the hosting computer.

TABLE 10 Recommended hardware specifications

Managed Devices	RAM	CPU	Hard Disk Space	Purge Policy
80 Unleashed or ZoneDirector networks with a total of 2000 APs 300 Unleashed networks with a total of 600 APs	16 GB	4 core processor such as 3.30 GHz Intel® Core i5-3550 or equivalent	300 GB	7 days
400 Unleashed or ZoneDirector networks with a total of 10,000 APs 1000 Unleashed networks with a total 1000 APs	48 GB	32 core processor such as 2 GHz Dell R710 platform with Xeon® E5-2650 or equivalent	1 TB	7 days

Changing the Login Information for the Virtual Machine

You can change the login credentials that you use to login to Unleashed Multi-Site Manager.

1. Using SSH, establish a connection with Unleashed Multi-Site Manager.
2. Go to `/opt/UMM/support_files`.
3. Execute the command **/upgradeUser.sh /opt/UMM**.
4. Enter the old username and password.
5. Enter the new username and password.

NOTE

The default Unleashed Multi-Site Manager login credentials are as follows:

1. username: admin@ruckus.com
2. password: admin

The default Unleashed Multi-Site Manager installation folder is `/opt/UMM`.

Changing the Linux Password

You can change the root password for your Linux account.

Follow these steps:

1. Using SSH, establish a connection with Unleashed Multi-Site Manager.
2. Execute the command **passwd root**.
3. Enter the old password.

4. Enter the new password.

   NOTE
   The default Linux login credentials are as follows:
   1. username: root
   2. password: ruckus

Changing the Login Credentials to Access the Database

You can change the username and password for the Unleashed Multi-Site Manager database.

Follow these steps:

1. Using SSH, establish a connection with Unleashed Multi-Site Manager.
2. Go to `/opt/UMM/support_files`.
3. Execute the command **./setDBPassword.sh**.
4. Enter the old username and password.
5. Enter the new username and password.

   The default MariaDB password in *admin*.



© 2018 ARRIS Enterprises LLC. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com