USER GUIDE



RUCKUS Unleashed Multi-Site Manager User Guide, 2.6

Supporting Unleashed Multi-Site Manager Release 2.6

Copyright, Trademark and Proprietary Rights Information

© 2022 CommScope, Inc. 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 CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope 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, COMMSCOPE 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. CommScope 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. CommScope 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 CommScope 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 COMMSCOPE, COMMSCOPE 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 COMMSCOPE 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, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

| Preface | 7 |
|---|----|
| Contacting RUCKUS Customer Services and Support | 7 |
| What Support Do I Need? | 7 |
| Open a Case | 7 |
| Self-Service Resources | 8 |
| Document Feedback | |
| RUCKUS Product Documentation Resources | 8 |
| Online Training Resources | |
| Document Conventions | |
| Notes, Cautions, and Safety Warnings | |
| Command Syntax Conventions | |
| About This Guide | 11 |
| Introduction to Unleashed Multi-Site Manager | |
| Related Documentation | 11 |
| Introducing RUCKUS Unleashed Multi-Site Manager | 13 |
| Unleashed Multi-Site Manager Overview | |
| Introducing Lite Mode | |
| Management Software and Server | 14 |
| Event Times | |
| Management Protocol | |
| Internet Accessibility | |
| Where Should You Place Unleashed Multi-Site Manager? | 14 |
| Key Terms | 15 |
| Installing and Upgrading Unleashed Multi-Site Manager | 17 |
| Firewall Ports that Must Be Open for Communications | |
| Administering a Linux Server | |
| Preparing the Server for Software Installation | |
| Editing the Server Hosts File | 19 |
| Installing the Software | 19 |
| Notable Files in the Software Root Directory | |
| Upgrading the Software | |
| Uninstalling the Software | |
| Backing Up the Database from the Command Line Interface | |
| Restoring the Database from the Command Line Interface | |
| After Installation | 26 |
| Getting Started with Unleashed Multi-Site Manager | 27 |
| Logging In to Unleashed Multi-Site Manager | |
| Features of the Web Interface | 29 |
| Getting to Know the Dashboard | |
| Getting Started Tasks | |
| Changing the Default Administrative Password | |
| Pointing ZoneDirector, an Unleashed Network, and ICX Switches to Unleashed Multi-Site Manager | |
| Checking Your Software License | |
| Working with ZoneDirector Controllers, Unleashed APs, and ICX Switches | |

| Viewing Devices Managed by UMM | |
|--|--|
| Viewing the Device Configuration | |
| Creating and Managing Groups | |
| Viewing Group Details | |
| Editing the Device Properties | |
| Editing AP Details | |
| Using QR Code for Network Access | |
| Editing WLAN SSID | |
| Resetting the Password | |
| Blocking Devices from the Software | |
| Connect to Unleashed CLI | |
| Backing Up Device Configuration Files | |
| Restoring the Device Configuration | |
| Upgrading Device Firmware | |
| Deleting Devices Managed by the Software | |
| Downloading AP log | |
| Managing Tasks | |
| Zero Touch Deployment | |
| Zero Touch Deployment Workflow | |
| Creating a New Rule | |
| Registering Unleashed to UMM | |
| | |
| Working with Reports | |
| Available Report Types | |
| Configuring Report Options | |
| Saving Reports and Generating Reports | |
| Generating an AP Report | |
| Generating a WLAN Report | |
| Generating a Client Report | |
| Generating Reports for Rogue Devices | |
| Viewing Saved Reports | 72 |
| Performing Administrative Tasks | |
| The Administer Tab | |
| Viewing Audit Logs | |
| Managing Software Licenses | |
| Uploading a License File | |
| Deleting the Expired Temporary License | |
| Managing User Accounts | |
| User Roles and Privileges | |
| Creating a New User Account | |
| Editing a User Account | |
| Deleting a User Account | |
| Upgrading Switch Firmware | |
| Managing SSL Certificates | |
| Importing an SSL Certificate | |
| Creating a Certificate Signing Request File | |
| Viewing Current Certificates | |
| Upgrading the Software | |
| Recovering Unleashed Multi-Site Manager from an Unsuccessful Software Update | |
| Backing Up and Restoring the Database from the Web Interface | |
| | ······································ |

| Backing Up the Database from the Web Interface | |
|---|-----|
| Scheduling Database Backup | |
| Viewing and Deleting Database Backup Files | |
| Restoring a Backup Copy of the Database | 95 |
| Generating Support Information | |
| Viewing System Logs | |
| Downloading System Logs | 97 |
| Emailing a Copy of the System Log File | |
| Manually Transferring Files | |
| System | |
| Configuring System Settings | |
| General Settings | 104 |
| SMTP Settings | |
| Purge Policy | |
| TACACS+ | |
| FTP Server Settings | |
| SNMP Server Settings | |
| SMS Setting | |
| Alarm Settings | |
| Configuring Alarm Settings | |
| User-Customized Alarms | |
| Monitoring Events | |
| Event Configuration | |
| Appendix | |
| Configuring Unleashed Multi-Site Manager Behind the NAT Server | |
| Configuring Unleashed Multi-Site Manager In Front of NAT Server | |
| Configuring the 200.6 Unleashed Setup | 123 |
| Configuring ZoneDirector & 200.5 Unleashed Behind NAT Server | |
| Configuring ZoneDirector & 200.5 Unleashed In Front of the NAT Server | |
| Zero Touch Deployment Setup Example | |
| Setting Up Unleashed Multi-Site Manager as a Virtual Machine | |
| Hardware Requirements and Specifications | |
| Changing the Login Information for the Virtual Machine | |
| Changing the Linux Password | |
| Changing the Login Credentials to Access the Database | |
| Configuring ICX Switches | |
| | |

Preface

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

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 products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using https://support.ruckuswireless.com, or go to https://www.commscope.com/ruckus 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. Requests 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, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at https://support.ruckuswireless.com 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/
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes-https://support.ruckuswireless.com/#products_grid
- 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.

Document Feedback

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

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

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

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

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 the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

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

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. You create a CommScope account and then register for, and request access for, CommScope University.

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

| Convention | Description | Example |
|------------|--|--|
| monospace | Identifies command syntax examples | <pre>device(config)# interface ethernet 1/1/6</pre> |
| 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 Safety 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.

ATTENTION

An ATTENTION statement indicates some information that you must read before continuing with the current action or task.



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]. |
| ١ | 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. |

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 a 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 Unleashed Multi-Site Manager interface. The online help is accessible from the 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 |
|---|--|------|
| | Introducing Lite Mode | |
| | Management Software and Server | |
| • | Where Should You Place Unleashed Multi-Site Manager? | . 14 |
| • | Key Terms | 15 |

Unleashed Multi-Site Manager Overview

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

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

NOTE

Unleashed Multi-Site Manager does not support solo APs, except for RUCKUS P300.

ATTENTION

By downloading Unleashed Multi-Site Manager, be advised that:

• This information may be transferred and stored outside of your country of residence where data protection standards may be different.

Introducing Lite Mode

Unleashed Multi-Site Manager 2.4 introduces 'Lite' mode along with the existing standard mode.

Lite mode can manage more devices with lesser functionalities compared to standard mode. UMM 2.4 and later release allows the customer to choose between standard and lite mode during the initial installation process. Refer to the Installing from an FTP Download on page 20 for more information.

TABLE 2 Difference between Standard and Lite mode

| Functionality | Standard mode | Lite mode |
|--|---------------|---------------|
| Dashboard AP clients | Supported | Not supported |
| Dashboard AP client OS/Radio/Vendor | Supported | Not supported |
| Device AP and radio traffic statistics | Supported | Not supported |
| Device clients statistics | Supported | Not supported |
| Device clients events | Supported | Not supported |
| Rogues APs | Supported | Not supported |
| Device traffic analysis | Supported | Not supported |
| Reports | Supported | Not supported |
| Backup elasticsearch DB | Supported | Not supported |

Introducing RUCKUS Unleashed Multi-Site Manager

Management Software and Server

TABLE 2 Difference between Standard and Lite mode (continued)

| Functionality | Standard mode | Lite mode |
|---|---------------|---------------|
| Configurable statistic data purge policy | Supported | Not supported |
| Unleashed managed ICX port traffic statistics | Supported | Not supported |

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 19.

Event Times

Unleashed Multi-Site Manager 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 Unleashed Multi-Site Manager 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 (https://www.broadband-forum.org).

Internet Accessibility

Unleashed Multi-Site Manager requires an Internet-accessible interface to enable:

- 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.
- The Map View feature: Map View data is provided by Google Maps or Bing Maps, and thereforeUnleashed Multi-Site Manager must be able to connect to Google Maps or Bing Maps via the Internet to display the maps. When the software is unable to access Google Maps or Bing Maps, gray boxes appear on the web interface, instead of the map that Google Maps or Bing 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 IP address of the Unleashed Multi-Site Manager is reachable via HTTPS from outside of your internal network.

Key Terms

Before using the Unleashed Multi-Site Manager, RUCKUS recommends that you become familiar with the key terms that are used in this Guide and on the web interface. The following table lists terms that are key to full understanding and proper use of Unleashed Multi-Site Manager.

TABLE 3 Key Terms

| Term | Description |
|--------------------------|--|
| Device Registration | Enable software management on the Unleashed and ZoneDirector devices and then they will register to Unleashed Multi-Site Manager automatically. |
| Periodic Inform Interval | 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, controls, and reporting. |
| Default Mail to | Refers to the email address to which messages are sent 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 email address. Refer to SMTP Settings on page 106. |

Installing and Upgrading Unleashed Multi-Site Manager

| • | Firewall Ports that Must Be Open for Communications | . 17 |
|---|---|------|
| • | Administering a Linux Server | . 18 |
| • | After Installation | . 26 |

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 IPTables information under the "Firewalls" section).

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

TABLE 4 Firewall Ports That Must Be Open for Unleashed Multi-Site Manager Communications

| Communication | Ports |
|-------------------------------------|---------------------------|
| ZoneDirector and Unleashed (Device) | |
| HTTPS port for Device registration | TCP destination port 443 |
| HTTPS port for WebUI login | TCP destination port 8443 |
| НТТР | 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 the TCP 22, 80, 443, 8443 and 9443 ports to the Unleashed Multi-Site Manager server

NOTE

For ZoneDirector and Unleashed 200.5 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 display the status as Applying.

NOTE

Ensure port 443 is open in the firewall when Unleashed Multi-Site Manager manages ICX switches, because switches register to the application through port 443 and this port is not configurable on the switch. ICX switches use port 443 and port 22 to register to UMM server by default.

Administering a Linux Server

RUCKUS recommends that you use the following OS:

- CentOS release 6.5 (64 bit)
- CentOS release 7.2 (64 bit)
- Red Hat Enterprise Linux Server release 6.5 (64 bit)
- Red Hat Enterprise Linux Server release 7.2 (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. You must prepare the host server for Unleashed Multi-Site Manager installation and operation.

What You Will Be Doing

- Prepare a clean Linux server according to the minimum system requirements.
- Place the server on a subnet that is reachable by the RUCKUS devices to be managed.
- Customize your DHCP server.
- Before you install Unleashed Multi-Site Manager, ensure that you upgrade Openssl and its library 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 must 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, Unleashed APs, and ICX switches on the purge policy. Refer to the RUCKUS Unleashed Multi-Site Manager Release Notes for the hardware specifications.
- RUCKUS recommends that you use the following OS:
 - CentOS release 6.5 (64 bit)
 - CentOS Linux release 7.2 (64 bit)
 - Red Hat Enterprise Linux Server release 6.5 (64 bit)
 - Red Hat Enterprise Linux Server release 7.2 (64 bit)
- HDD: 30 GB dedicated to Unleashed Multi-Site Manager, minimum
- 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 Unleashed Multi-Site Manager services 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 to ensure a successful database backup.

Web Browser Requirements

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

Editing the Server Hosts File

Unleashed Multi-Site Manager 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 must edit your Linux server hosts file to include its DNS-related information.

NOTE

If you are planning to enable SMTP notification on the software, then you must add another line in the hosts file for your SMTP server's DNS information. For more details, refer to SMTP Settings on page 106.

NOTE

If you use a period (.) in the host name to separate the host name.from the domain name, then you are not allowed to use a digit-only domain name. For instance, UMM.ruckus and UMM.98ABC are allowed, and UMM.98 and Localhost.12345 are not allowed.

- 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 18.

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 81.

- 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)

| Your system time and timezo | me is:Fri, 24 Jul 2020 13:41:40 +0800. |
|--|--|
| yes?(Put yes to continue or choose yes | programm will be terminated!):yes |
| The total memory: (15GB) | |
| PERL checking result: Ok | |
| UNZIP checking result: Ok CURL checking result: Ok | |
| libaio checking result: Ok | |
| warning: 3rdparty/jemalloc- e, key ID 0608b895: NOKEY | 3.6.0-1.el6.x86_64.rpm: Header V3 RSA/SHA256 Signatur |
| Preparing | *************************************** |
| 1:jemalloc | \$ |
| Testing network connection Result: Ok | for 'localhost' |
| The hostname of this machin | e is 'dhep-10-223-73-70' |
| Testing network connection Result: Ok | for dhep-10-223-73-70 |
| Testing network connection Result: Ok | for '127.0.0.1' |
| REBUILT OF | |
| | where UNM should be installed. |
| Location[/home/UMM]: Script started, file is /ho | me/UNM/install.tmp |
| | |
| The installation process is | starting, please wait |
| Standard/Lite mode:1/2. or | press <enter key=""> to use standard mode:</enter> |
| Standard/Lite mode[1]: Standard mode. | |
| Please enter a domain name | for your UNM admin account. |
| domain name(eg. <your_doma< td=""><td>lin>.com): ruckus.com</td></your_doma<> | lin>.com): ruckus.com |
| Please enter a password for | your UMM admin account. |
| Password: admin | |
| Please confirm your passwor | d: admin |
| Please enter a password for | your DB root. |
| Password: admin | |
| Please confirm your passwor | d: admin |
| Please enter the HTTPs port | number for Device. |
| Https port[443]: | |
| D1 | |
| Please enter the HTTPs port Https port[8443]: | number for web Browser. |
| Please enter the following | information for SMTP settings. |
| You will have the option to | change this setting from the System> System Setti |
| ngs menu after installation SMTP host: | |
| SMTP port[25]: | |
| SMTP mail to: | |
| | port number, or press <enter key=""> to use the default</enter> |
| value: SSHTunnel port[9443]: | |
| Please enter the SSH port of | number, or press <enter key=""> to use the default value:</enter> |
| SSH port[22]: | |
| Starting nginx, syslog-ng in | atallation |



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[/home/UMM]:

9. Before the installation process begins to install the software, respond to the prompt message by entering the number associated to your choice of mode. Enter '1' or press the <Enter key> if you want to install the standard mode. Enter '2' to install the lite mode.

```
The installation process is starting, please wait...
Standard/Lite mode:1/2, or press <Enter Key> to use standard mode:
Standard/Lite mode[1]:
Standard mode.
```

10. 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

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

Password: **password** Please confirm your password: **password**

12. Enter a password for the MariaDB root account.

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

13. Enter the HTTPs port number for the device.

Https port[443]:

14. Enter the HTTPs port number for the Web Browser.

Https port[8443]:

Installing and Upgrading Unleashed Multi-Site Manager

Administering a Linux Server

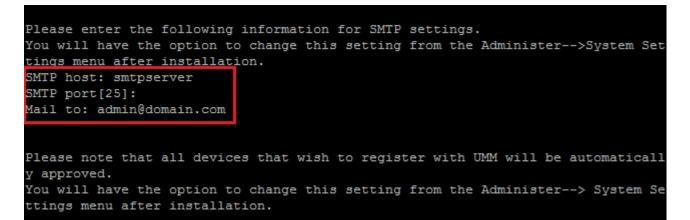
15. Enter your SMTP server host name and port number, as well as a default email address to which alerts for software system events are sent.

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

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

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

FIGURE 2 Configuring the SMTP Settings



16. Enter the SSH Tunnel port number and the SSH port number.

```
Please enter the SSH Tunnel port number, or press <Enter Key> to use the default value:
SSHTunnel port[9443]:
Please enter the SSH port number, or press <Enter Key> to use the default value:
SSH port[22]:
```

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 27.

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 (/home/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, 2.1 2.2 2.3–2.4.0.0.22.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 25 and Backing Up and Restoring the Database from the Web Interface on page 92.

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 25 and Backing Up and Restoring the Database from the Web Interface on page 92.

Uninstalling the Software

Execute the software uninstall script.

[root@umm UMM]# ./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 MariaDB and Elasticsearch 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 /home/UMM directory.

When the uninstall script completes deleting the /home/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.

Installing and Upgrading Unleashed Multi-Site Manager

After Installation

Follow these steps to back up the software database.

- 1. On the Linux server, go to the software root directory (/home/UMM).
- 2. Execute the database backup script.
 - To back up the software database to a specific file path and file name, enter the following command:

./backup.sh

Press Enter. You can enter the file name and then Unleashed Multi-Site Manager starts database backup.

Type a name for the database that you are saving. If you want Unleashed Multi-Site Manager to assign a file name automatically (in the format DB_[YYYY-mm-dd-hh]), leave this blank.

Input the file name.

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 93

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 (/home/UMM).
- 2. Execute the database restore script by entering the following command:

./restore.sh

Press Enter and provide the filename. Unleashed Multi-Site Manager will restore the database.

For example,

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

Enter the path of your backup file.

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 | 27 |
|---|--|----|
| • | Features of the Web Interface | |
| • | Getting to Know the Dashboard | 30 |
| • | Getting Started Tasks | 33 |

Logging In to Unleashed Multi-Site Manager

Use one of the Web browsers described in Web Browser Requirements on page 19 to access the software Web interface:

NOTE

The default Unleashed Multi-Site Manager OVA login credentials are as follows: a. username: admin@ruckus.com b. password: admin The default Linux login credentials are as follows: a. username: root b. password: ruckus

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>:8443

--OR--

https://umm:8443

Logging In to Unleashed Multi-Site Manager

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 85.

The RUCKUS Admin login page appears.

FIGURE 3 RUCKUS Admin Login Page

| Contraction of the second seco |
|--|
| þsemama - |
| Password |
| |
| Login |
| |

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 19). 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 109.

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 30.

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

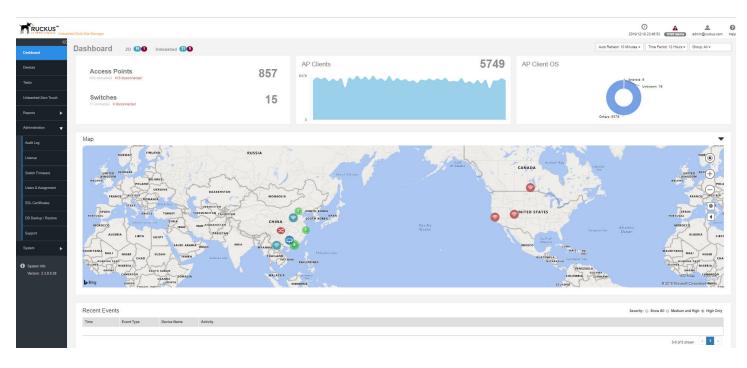


TABLE 5 Web Interface Elements

| No. | Interface Element | Interface Element Description |
|-----|--------------------------|--|
| 1 | Main Menu | Seven tabs group related tasks that you can perform in Unleashed Multi-Site Manager . These tabs include: Dashboard Devices Tasks Unleashed-Zero Touch 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. 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 <i>trial</i> license file, then a notice appears that the software is using the trial license file and when the trial license file expires. Unleashed Multi-Site Manager will not delete the device when license expires. It just changes the status of the device which does not have enough licenses to <i>license exceed</i> and stops to monitor and manage them. |
| 4 | APs and Switch panel | Displays the number of APs and switches that are connected and disconnected for a period of time. |

Getting Started with Unleashed Multi-Site Manager

Getting to Know the Dashboard

TABLE 5 Web Interface Elements (continued)

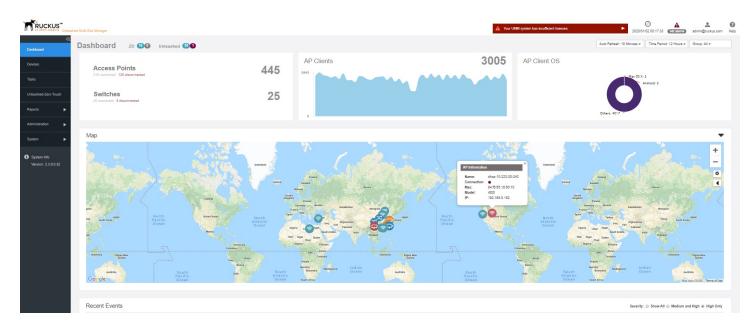
| No. | Interface Element | Interface Element Description | | | | |
|-----|----------------------------------|---|--|--|--|--|
| 5 | Clients panel | Displays the number of clients that are connected for a period of time. | | | | |
| 6 | Clients OS/Radio/Vendor panel | Displays the OS/Radio/Vendor utilization 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 | Мар | Displays information about the APs deployed in the Goggle map. | | | | |
| 8 | Recent Events/Alarm | Displays the events/Alarm that were recently triggered for the device (ZoneDirector, Unleashed APs or ICX switches). You can also sort the events to view them by severity type. | | | | |

Getting to Know the Dashboard

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

The **Auto Refresh** menu allows you to select the time interval for the page to refresh automatically and display the latest information. The **Time Period** menu allows you to select the period of time for which data must be displayed in the Dashboard. You have the option to select 12 hours, 24 hours, 7 days, or 3 months. The **Group All** menu allows you to select the data you want to display on the Dashboard. You can select **All** or select another group based on the user.

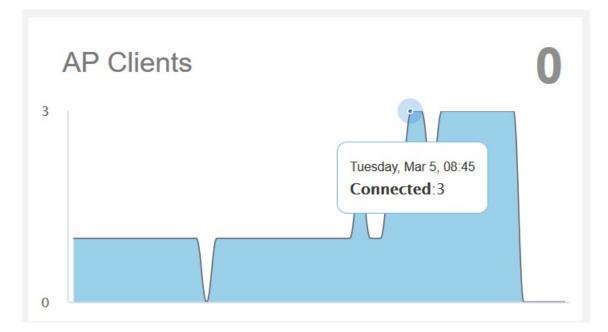
FIGURE 5 The Dashboard



The Dashboard displays at-a-glance information about the following managed devices:

- The number of connected and disconnected ZoneDirector and Unleashed devices.
- The number of connected and disconnected switches.
- 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 AP Clients Graph



The number of AP clients that are associated with the currently connected APs are displayed. Pause the pointer along the graph to display the connected clients at any time within the selected time range. The graph displays the number of connected AP clients 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.

• The AP Client OS panel displays a donut chart of wireless clients based on the operating systems (Windows, Vista, Android, iOS, and others) that they are running.

FIGURE 7 AP Client OS Chart

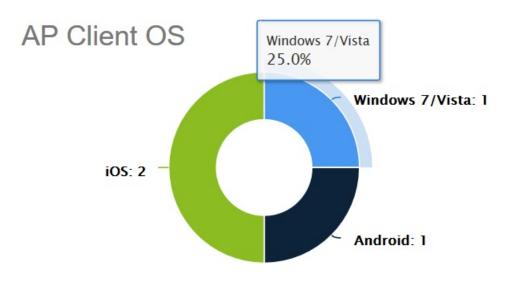
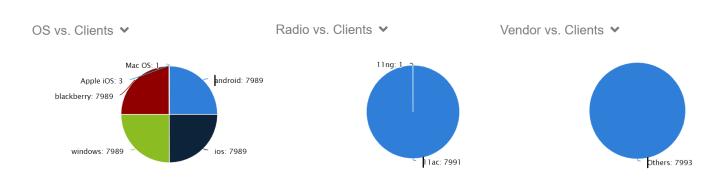


FIGURE 8 Client Charts

Pause the pointer on the chart to see the percentage share of OS used by client devices. For example, 56% for Windows means, out of the total client devices accessing the server, 56 percent of those devices are using the Windows operating system. The percentage of various versions of each OS accessing the server is displayed also.

• The Client charts display a donut chart of wireless clients based on the operating system, radio frequency and vendors. Pause the pointer over the chart for more information. For example, if you pause the pointer over the OS vs. Clients chart, is displays that 25% of the clients are iOS OS users.



• A map which displays the AP and device information across the globe. Pause the pointer on the AP, switch, 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, Unleashed devices, ICX switches and on clients.

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

TABLE 6 Columns on the Recent Events Panel

| Column Name | Description |
|-------------|--------------------------------|
| Time | Displays the event time stamp. |

TABLE 6 Columns on the Recent Events Panel (continued)

| Column Name | Description |
|-------------|--|
| 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 top-right corner of the panel.

• The **Recent Alarms** panel displays information about alarms that have occurred on Unleashed Multi-Site Manager, on managed ZoneDirector, Unleashed devices, ICX switches and on clients.

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

| Column Name | Description | | | |
|-------------|--|--|--|--|
| Time | Displays the alarm time stamp. | | | |
| Severity | Displays the severity of the alarm such as Warning, Minor, Major, and Critical. | | | |
| Device Name | Name of device reporting the alarm. Click this link to go to the devices reporting the specific alarm. | | | |
| Alarm Type | Displays the type of alarm such as AP traffic, number of channel changes and so on | | | |
| Activity | Events description. | | | |

The information in the **Recent Alarms** can be displayed based on the severity (**Show All**, **Warning**, **Major**, **Minor** and **Critical**), which you can select from the top-right corner of the panel.

Getting Started Tasks

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

• Changing the default administrative password

TABLE 7 Columns on the Recent Alarms Panel

- Pointing ZoneDirector, Unleashed devices, and ICX switches 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 web interface and modifying the settings you have configured.

1. After logging in to the web interface, click the Logout icon and then select Change Password.

FIGURE 10 Editing the User Password

| | ed Multi-Site Manager | | | | 2019/12/19 23:50:1 | 5 19229 alarms admin@ruckus.com Help |
|----------------------|---|----------|------------|------|-----------------------------------|--------------------------------------|
| Cashboard | Dashboard ZD 10 Unleas | shed 218 | | | Auto Refresh: 10 Minutes 🕶 Time F | Period: 12 Hours - Group: 8 - |
| Devices | Access Points | 857 | AP Clients | 6042 | AP Client OS | Logout icon |
| Tasks | 440 connected 417 disconnected | 001 | 04/8 | | | Android: 6 Unknown: 16 |
| Unleashed-Zero Touch | Switches 19 connected 4 disconnected | 23 | | | | |
| Reports > | | | 0 | | Others: 6578 | |
| Administration 🗸 | | | | | | |

- 2. In the Update Password dialog box, enter the current password in the Current Password field
- 3. Enter a new password in the Password field.
 - Passwords must be from 6 through 32 characters long, and must be comprised of letters and numbers only.
 - Passwords are case-sensitive.
 - Spaces cannot be used in passwords.

NOTE

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

- 4. Enter the new password in the Confirm Password field.
- 5. Click OK.

Pointing ZoneDirector, an Unleashed Network, and ICX Switches to Unleashed Multi-Site Manager

If you want to use Unleashed Multi-Site Manager to monitor and administer ZoneDirector, an Unleashed network, or ICX switches, follow the procedures listed in the Enabling Management via UMM section in the *ZoneDirector User Guide*. For more information, see Appendix on page 121

NOTE

Make sure that the required communication ports are open between the ZoneDirector, the Unleashed network, the ICX switches, and Unleashed Multi-Site Manager as described in Firewall Ports that Must Be Open for Communications on page 17.

Checking Your Software License

A new Unleashed Multi-Site Manager installation provides only one Unleashed license by default. When you upgrade 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 additional licenses and upload them.. Unleashed networks consume license numbers by the "active AP number" under it.

Beginning with UMM 2.3, Unleashed Multi-Site Manager supports monitoring and managing ICX switches. The number of licenses required by the switch depends on the unit number of the switch.

When you are managing ZoneDirector using Unleashed Multi-Site Manager, the number of license seats that ZoneDirector requires 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.

When the 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.

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

Unleashed Multi-Site Manager does not delete a device when the license expires. The status of the device changes to *license exceed* if it is not having enough license and Unleashed Multi-Site Manager stops monitoring and managing the device.

Before using Unleashed Multi-Site Manager to manage RUCKUS devices, RUCKUS recommends that you check how many ZoneDirector devices, Unleashed APs and ICX switches can be supported by your current license. Select**Administer** > **License** and review the total number of devices supported by your license and the number of seats used by ZoneDirector devices, Unleashed APs, and ICX switches.

FIGURE 11 License Details

| RUCKUS" | a meditação dato dicas agui | | | | | | | © A 2013/13/20 14 46 12 | e admin@xx/xx.com 1 |
|-------------------|--|-------------------|----------|-----------------------|--------------------|---|--|----------------------------|---------------------|
| Cashboard | License | | | | | | | | |
| | | | | | | | | | |
| | Tanal 2016/soca AP Listenses guistinasora. 1149 Tatali Utersaaned Listenses Paratases 1. 1001 | | | | | Unders ein Domsumed by 20-Bridge AP. 5 Listens eis Domsumed by Unieaster 3 | Remaining Utile addresses in 2000 Remaining Utile addresses in 2000 | | |
| Ren F | Total Switch Licero | es Parchised (30) | | | | Licens as Consumed by Switch 1 | Remaining Switch Learna as: 20 | | |
| Administrative 💌 | OperadLowise | | | | | | | dearth | 9 Z |
| A400.00 | License Rey | Part Number | AP Count | Create Terra | License Type | Expire Date | | | |
| | 128570148.000 | FME 4 | 1 | May 26/2017 06:48:04 | Unleashed-Official | tun, | | | |
| LOUIS | 1503227220000 | Diversi | 100 | Heg 13 2013 00 45 20 | Switch-Official | 16% | | | |
| Switch Formula | 1515349651068 | UNKA | 1008 | 11 FX (C (115 70 ret. | Unieashed-Official | 164 | | | |
| alandi tuttadi k | 15-15357317000 | 20 | 1000 | Jan 00-2010 04:58:57 | 20-0### | NK. | | | |
| Uses & Assignment | | | | | | | | , | 4 st 4 st au |
| SR ORIGAN | | | | | | | | | |

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, Unleashed APs, and ICX Switches

| • | Viewing Devices Managed by UMM | 37 |
|---|---|----|
| • | Viewing Devices Managed by UMM Viewing the Device Configuration | 40 |
| • | Creating and Managing Groups | 43 |
| • | Editing the Device Properties | 47 |
| • | Editing AP Details | 48 |
| • | Using QR Code for Network Access Editing WLAN SSID Resetting the Password | 49 |
| • | Editing WLAN SSID | 49 |
| • | Resetting the Password | 50 |
| • | Blocking Devices from the Software | 51 |
| • | Connect to Unleashed CLI | 52 |
| • | Backing Up Device Configuration Files | 52 |
| • | Restoring the Device Configuration | 54 |
| • | Upgrading Device Firmware | |
| • | Deleting Devices Managed by the Software | |
| • | Downloading AP log | 57 |
| • | Downloading AP log Managing Tasks | 58 |
| • | Zero Touch Deployment | |

Viewing Devices Managed by UMM

The **Devices** page of the Web interface displays information about devices managed by Unleashed Multi-Site Manager software. These devices include ZoneDirector controllers, ICX switches, Unleashed APs and Clients.

After you to log in to the web interface, select **Devices** from in the navigation bar.

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

• List: Displays the list of all devices irrespective of the group to which they belong.

Viewing Devices Managed by UMM

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

FIGURE 12 Devices Managed by Unleashed Multi-Site Manager: List View

| | ashed Mulli-Site Manager | | | | | | | | Q 2021/08/19 16:01:18 | | L. admin@ruckus. | com Hel |
|---------|--------------------------|-----------------|------------------|----------------|------------|----------------|---------------|-------------------|--------------------------|-------------|---------------------|-----------|
| | Devices | | | | | | | | | | Lis | t Group |
| Devices | Edit Edit WLAN Edit | AP Show QR Code | Backup & Restore | Upgrade More - | | | | | 5 | erch. | ٩ | ø 🔹 |
| Tasks | Name | Location | | Member Count | Connection | SSH Connection | Management IP | MAC Address | Software | IP Address | | Serial No |
| | Ruckus-Unleashed | | | 000 | • | • | | c8:08:73:3c:64:10 | 200.11.10.5.59 | 10.223.34.9 | 5:443 | un47183 |
| | Colon un | | | 000 | | • | | 94:15:65:14:c8:50 | 200.12.10.5.88 | 10.223.82.1 | 33:443 | un11158: |

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

| COMMSCOPE" RUCKUS" | athed Multi-Ste Manager | | | | | | | 9 15:59:02 (177 Starms) | admin@ruckus.co | om Help |
|-----------------------|-------------------------|---------------------------|------------------------------|----------------|------------|----------------|---------------|-------------------------|-----------------|---------|
| Dashboard | Devices | | | | | | | | List | Group |
| Devices | 2 + / × 🗢 🗛 | Edit Edit WLAN Edit AP St | how GR Code Backup & Restore | Upgrade More - | | | | Search | ٩ | Ø 0 |
| Taska | - Wireless Networks | Name | Location | Member Count | Connection | SSH Connection | Management IP | MAC Address | Software | |
| | real | Ruckus-Unleashed | | 000 | | | | c8.08.73.3c:64:10 | 200.11.10.5 | 5.59 |
| | | € pint_un | | 000 | • | • | | 94:18:65:14:08:50 | 200.12.10 | 5.88 |

Click the Refresh icon ($\stackrel{\frown}{\sim}$) to refresh the contents of the table.

Click the Edit WLAN icon ()) to edit the selected WLAN to the Unleashed which belong to this group.

Click the Upgrade icon (

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

TABLE 8 Configuring Device Management

| Field/Column | Description | | | |
|---|--|--|--|--|
| Name | Displays the name of the device (may be a ZoneDirector controller or an Unleashed network that UMM manages). Clicking the device name hyperlink opens the dashboard of the controller in a new page. | | | |
| Member CountDisplays the number of connected, disconnected or pending APs that are managed by the ZoneDirector controller Unleashed network. | | | | |
| ICX Switches Count | Displays the number of connected, disconnected or pending ICX switches. | | | |
| Port Status | Displays the port status of the switch | | | |
| Serial Number | Displays the serial number of the device. | | | |
| Connection | Indicates whether the device is currently online (blue) or offline (red). | | | |
| SSH Connection | Indicates the status of the SSH tunnel between Unleashed Multi-Site Manager and ZoneDirector or Unleashed devices. | | | |
| Management IP | Displays the Management IP address of ZoneDirector and Unleashed devices. | | | |
| MAC Address | Displays the MAC address of ZoneDirector and master AP's MAC address for 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 that are behind NAT, include port 443 for port forwarding. | | | |
| Тад | 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 a main office, you can assign the tag "Main" to it. | | | |

| TABLE 8 Configuring Device | Management (continued) |
|----------------------------|------------------------|
|----------------------------|------------------------|

| Field/Column | Description | | | | | | | |
|-------------------|---|--|--|--|--|--|--|--|
| 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 web interface of the | | | | | | | |
| | device. If :443 is displayed after the port number, you can access the device Web interface using: | | | | | | | |
| | https://{device-IP-address}. | | | | | | | |
| IPv6 Address | Displays the IPv6 address of the device. | | | | | | | |
| Model | Displays the model number 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 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 Consumed | 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 Configure table icon (²⁴), 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

| Table Settings | i | | | × |
|----------------|--|--------------------------------|----------------------------|----|
| | | | | |
| Rows | | | | |
| Search | All of the ke Any of the ke | y words (AND) ey words (OR) | | |
| Show | 10 entri | es per page | | |
| Columns | | | | |
| 🗹 Name | | Location | Member Count | |
| Conne | ction | SSH Connection | 🗌 Tag | |
| 🗸 Manag | ement IP | MAC Address | Uptime | |
| 🗹 Softwa | re | IP Address | External IP | |
| C ICX Sv | vitches Count | Serial Number | IPv6 Address | |
| 🗌 Manag | ement IPv6 | Model | Last Seen | |
| 🗌 Latitud | e | Longitude | Redundancy State | |
| 🔽 Suppor | rt Status | License Consumed(| 🖌 Inventory Status | |
| | | | OK Cance | 3Î |

To search for information in the table, enter word or phrase in the Search field. The page refreshes 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 customizable. When your search generates more results than the number of rows set, use the left arrow and right arrow buttons 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 navigation bar.

The Devices page of the Web interface displays information about devices that the Unleashed Multi-Site Manager software.

FIGURE 15 Viewing Device Configuration Details for Wireless Devices

| General | Access Points | ICX Switches | Mesh View | Clients | WLANs | Alarms | Events | Rogues | Traffic Analysis | | |
|---------|---------------|--------------|-----------------------------|---------|-------|--------|--------|--------|------------------|--|--|
| Info | | | | | | | | | | | |
| Device | e Name | Kenneth- | Unleashed-T310 | s-2008 | | | | | | | |
| Unleas | shed ID | un42170 | un4217030045971565061650672 | | | | | | | | |

TABLE 9 Device Configuration Details

| Tab | Description |
|---------------|--|
| General | Displays the following information: Info: Provides basic device information including the number of data bytes and packets transmitted and received by the device. Click Save Unleashed System Log to save the unleashed system log. 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, the speed of data transfer and 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 authorized clients associated with the AP, software version, model number, uptime, IP address, and current status of the AP. For Unleashed Device, the AP Role is also displayed - there are two roles - master and member. Every Unleashed network has one master AP and several member APs that are managed by the master AP. The APs are displayed in a tree structure. |
| | In addition, the following information is displayed: General: displays general properties of the AP Trend: displays a graphical representation of the associated clients, traffic trends and AP status. Mesh: displays the mesh type, uplink and downlink APs WLANs: displays the BSSID and ESSID of associated WLANs Dedies displays the guarant radia channel menorities that the AD is unice. |
| ICX Switches | Radio: displays the current radio channel properties that the AP is using Displays a table detailing information about the ICX switch such as Name, Controller Name, MAC Address, Port Status, Serial Number, Connection, Management IP, Model, Last Seen, Uptime, and Software. Beginning with UMM 2.4, the backup or restore and the upgrade options are supported in the ICX switches tab. |
| 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 authorized 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, and the 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, the severity and activity associated 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. |
| Rogues | Displays rogue (or unauthorized) APs that pose problems for a wireless network in terms of airtime contention, as well as security. Information such as the rogue AP SSID, type, channel, and so on is displayed. This tab is only applicable for ZoneDirector devices and Unleashed networks |

Working with ZoneDirector Controllers, Unleashed APs, and ICX Switches

Viewing the Device Configuration

TABLE 9 Device Configuration Details (continued)

| Tab | Description |
|------------------|--|
| Traffic Analysis | Displays traffic trends as graphs. The following trends are available: |
| | • Top 10 APs Traffic |
| | • Top 10 APs Client |
| | Top 10 Clients Traffic |
| | Client OS Traffic |
| | Model Traffic |
| | Client Count versus AP Counts by Model |
| | AP Status |
| | Vendor versus AP |

NOTE

Lite mode does not support clients, rogues and traffic analysis in UMM 2.4 release.

FIGURE 16 Viewing Device Configuration Details for Switches

| | = freddy | | | | | | | | | | | |
|---------------------|----------------------|-----------------------|--------------|-------------|---|---|---------------|-------------|--------------------|----------|----------------|-------|
| Reports 🕨 | - 1720 | CX7450-48P-Router | 2063 | CYR3318P0DH | • | • | 10.223.10.228 | ICX7450-48P | 3 days, 5:41:06:00 | SPR08090 | 1 | P |
| Administration | - Switches (A) | | | | | | | | | | | |
| Maninistration P | freddyicx | | | | | | | | | | | |
| System 🕨 | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| System Info | | | | | | | | | | | | |
| Version: 2.2.0.0.35 | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | 1-2 of 2 shown | < 1 > |
| | General Ports Health | Traffic Alarms Events | | | | | | | | | | 2 |
| | General Ports Health | manic Alamis Evens | CLUP Neglous | | | | | | | | | |
| | | | | | | | | | | | | - |
| | Info | | | | | | | | | | | • |
| | Switch Name | ICX7450-48P-Router | | | | | | | | | | |
| | MAC Address | 64 c1 9a 06 a6 80 | | | | | | | | | | |
| | Serial Number | CYR3318P00H | | | | | | | | | | |
| | IP Address | 10 223 10 228 | | | | | | | | | | |

TABLE 10 Switch Configuration Details

| Tab | Description | | | | |
|----------------|---|--|--|--|--|
| General | Displays the following information: | | | | |
| | • Info: Provides basic device information about the switch, such as the switch name, IP address, model, stack information, and firmware version. | | | | |
| | • Stack Members: Provides detailed information about the switches in the stack. | | | | |
| | • Status Summary: Provides information about the switch status, registration state, and uptime. | | | | |
| Ports | Displays the port details, such as a brief summary of the ports, a view of ports that are engaged with the switc and details such as speed, PoE usage, VLANs, bandwidth, and so on. | | | | |
| Health | Displays a CPU and memory utilization, and also displays the status of the slots based on the power supply, temperature, and fan. | | | | |
| Traffic | Displays a traffic trends of the switch including the top ports by traffic. | | | | |
| Alarms | Displays a table that lists information about the type of alarm that was triggered, the time and date when the alarm was generated, the severity and activity associated with the alarm. The alarm history is displayed also. | | | | |
| Events | Displays a table that lists information about the type of event that was triggered, the time, event type, the severity and activity associated with the event. | | | | |
| LLDP Neighbors | Displays neighbor information, such as the device name, IP address, remote port information, and so on. | | | | |

NOTE

For a switch stack, the health of the master unit is displayed.

Click the Refresh icon 🗳 to refresh the contents of the tables within the tabs. You can also customize the tables by clicking the Configure table icon

You can also use the Search field 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. You can also create an empty group. 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.

There are two types of groups-one is for ZoneDirector and Unleashed, and the other for ICX switches. Devices can not be moved between these groups. The default group *Wireless Network* lists all the ZoneDirector and Unleashed devices, and the default group *Switches* lists all the ICX switches.

- 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.
- 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.

RUCKUS . 0 A Create a Group Group Name New Group All Devices (Select All) Selected Devices 2008-upgrade (un9616024037881566: 720720 (un421606000024157544513⁻ ANWC (171838001000) ANWC-Back (401608000001) Access-Network-Test (131508000013) FreddyZD_103_3 (171406000196) Freddy_103 (411738000593) Freddy_103_2 (961838000778) Freddy 2005 (un52148460657014406 • Cancel

FIGURE 17 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 18 Editing a Group

| | | Edit a Group | | 2019/12/05 15:4 | A 3:31 24396 alarms | admin@ruckus.com |
|---------------------------------|-----------------------------|--|--|-----------------|--------------------------------------|-------------------|
| Cashboard | Devices | Group Name Kenneth | | | | List Group |
| Devices | 2 + 🖋 x 😤 🗅 | Devices | | | | ۵ ۵ ۵ |
| | _ System | All Devices (Select All) | Selected Devices | Connection | Management IP | IP Address |
| Tasks | - Wireless Networks 🔺 24394 | Search | | • | | 10.223.5.201:443 |
| Unleashed-Zero Touch | | 2008-upgrade (un9616024037881566: 720720 (un421606000024157544513⁻ | Kenneth-M510 (un9418020012491548 Kenneth-Unleashed-T310s-2008 (un4) | • | | 10.223.87.99:443 |
| Reports ► | KUN | ANWC (171838001000) | Ruckus-Unleashed-Kenneth (un52146 | • | | 10.11.158.47:443 |
| | | ANWC-Back (401608000001) Access-Network-Test (131508000013) | Ruckus-Wireless-1200-K2 (210987654 kenneth-ZD3K-9132 (211208000191) | • | | 10.11.128.12:443 |
| Administration | | FreddyZD_103_3 (171406000196) | X ruckus-K-1200 (201601210008) | • | | 10.11.157.188:443 |
| System 🕨 | | Freddy_103 (411738000593) Freddy_103_2 (961838000778) | | • | | 10.223.4.238:443 |
| | | □ Freddy_2005 (un52148460657014406 ▼ | ▼ | | | |
| System Info | | | | | | |
| Version: 2.3.0.0.27 | KICX | | Reset OK Cancel | | | |
| | | | | | | |

8. Make the necessary changes and click Save.You have successfully edited the group.

To delete a group, select it and click the \times 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. You can also view the switches in a switch group and their associated ports, alarms, events, traffic trends and LLDP neighbors.

- 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 for APs:

- 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.
- ICX Switches: displays the details of the switches. The backup or restore and the upgrade options are supported in the ICX switches tab.
- 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 19 Group Details

| K Dashboard | Devices | | | | | | |
|---------------------------------------|----------------------------|--------------------|-------------------|-------------|-----------------|---------------------|---------------|
| Devices | 2 + / × 🗢 🗅 | | | | | | |
| Tasks | - Wireless Networks (A1) | Name | Location | Member (| Count Connectio | on \$\$H Connection | Management IP |
| | r | T20gate | | 100 | • | • | |
| Unleashed-Zero Touch | | SUGLEI | | 200 | • | ٠ | 1.1.1.1 |
| Reports 🗸 | | SUGLEI | | 200 | • | ٠ | 1.1.1.1 |
| | | 🦚 john | | 100 | • | • | 10.223.82.139 |
| АР | | SUGLEI | | 200 | • | ٠ | 1.1.1.1 |
| WLAN | | Contraction BUGLEI | | 200 | • | ٠ | 1.1.1.1 |
| WLAN | | SUGLEI | | 200 | • | ٠ | 1.1.1.1 |
| Client | | SUGLEI | | 200 | • | • | 1.1.1.1 |
| | | SUGLEI | | 200 | • | ٠ | 1.1.1.1 |
| Rogue | | Contraction BUGLEI | | 200 | • | • | 1.1.1.1 |
| Administration | | | | | | | |
| | | | | | | | |
| System 🕨 | Access Points ICX Switches | Alarms () Events | | | | | |
| System Info | Backup & Restore Upgrade | | | | | | |
| Version: 2.4.0.0.20 Mode: Standard | Name | Controller Name | MAC Address | Port Status | Serial Number | Connection | Management IP |
| | ab-sw1fl5-a.chnshe3 | john | d4:c1:9e:1a:04:95 | 000 | | Approval pending | 10.74.46.253 |

The following information is displayed for switch groups and individual switches:

- Switches & Ports: displays information about the switches such as the top switches by model, firmware, ports summary details, and ports details such as the following:
 - Switch Name: displays the name of the switch
 - Serial Number: displays the serial number of the switch
 - Port Name: displays the port name
 - Port Number: displays the port number

Creating and Managing Groups

- Status: displays whether the port is operationally Up or Down
- Admin Status: displays whether the port has been set to Up or Down by the network administrator
- Speed: displays the speed of the port
- PoE Usage (used/total watts): displays the PoE power usage compared to the allocated power
- VLANs: displays the VLAN(s) to which the port is connected
- Bandwidth IN (%): displays the bandwidth utilization for incoming traffic
- Bandwidth OUT (%): displays the bandwidth utilization of the port for outgoing traffic
- LAG Name: displays the name of the Link Aggregation Group (LAG)
- Optics: displays the type of optic
- Neighbor Name: When LLDP is enabled, the name of the neighboring device, such as an AP or another switch or router
- Ports (tab appears only for individual switches): displays the **Ports Summary** page provides information on the ports for the selected switch, including the total number of ports connected to the switch or stack, the number of ports active at various speeds, operational status of the ports (Up or Down), warnings associated with ports when alarms or events are triggered, and the number of ports managed by an administrator.

The **Ports View** page provides information on the state of all ports in each switch module, for example port Up, Down, or Administratively Down.

• Health (tab appears only for individual switches): displays the switch health for the duration selected from the drop-down menu.

NOTE

For switch stack, the health of the master unit is displayed.

The following information is displayed based on the duration selected:

- CPU (%): The CPU usage of the switch, including the minimum, maximum, average, and current CPU usage trends of the switch.
- Memory (%): The memory usage of the switch, including the minimum, maximum, average, and current memory usage trends of the switch.
- Status: The health status of the power supply, temperature, and the fans for up to four switch modules are displayed. OK indicates the parameter and components are in good health.
- Traffic: provides a graphical representation of the total traffic trend at the switch-level and also shows the top switches based on the traffic handled by the device.
- 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.
- LLDP Neighbors: Link layer discovery protocol or LLDP is used to discover and identify the clients. You can view information about the LLDP neighbors such as printers, VOIP devices, or other user equipment connected to the switch.

FIGURE 20 Switch Group Details

| | Name | Por | rt Status | Serial Number | Connection | SSH Connection | Management IP | Model | Uptime | Software | License Cor | nsumed |
|--------------------------|------------------------|-----------------------|--------------|-------------------------------------|------------|-------------------------|---------------------------------|------------------|----------------------|--|------------------------|------------------------|
| + Wireless Networks | 23 ICX71 | 50-C12 Switch_Ken 3 | 01 | FEK3224P044 | • | • | 172.18.208.33 | ICX7150-C12-POE | 13 days, 0:19:45:00 | SP508080ca | 1 | |
| = Switches KICX | jim_71 | 50_c12_1728888 6 | 010 | FEK3222P0KT | • | • | 172.18.131.37 | ICX7150-C12-POE | 6 days, 21:11:32:00 | SPS08080ca | 1 | |
| freddyicx | vendy | icx1 📀 | 00 | FEK3224P046 | • | • | 192.168.10.241 | ICX7150-C12-POE | 27 days, 8 36 22 00 | SPS08090_Q17 | 1 | |
| - jim_icx | im_71 | 50_12_192_newCh (1 | 01 | FEK3222P04W | • | • | 192.168.24.251 | ICX7150-C12-POE | 6 days, 21:32:08.00 | SPR08090_Q17 | 1 | |
| jim_icx2 wondyicxgupr | cat Freddy | r c12 before restore | 00 | FEK3224P043 | • | • | 172.18.169.2 | ICX7150-C12-POE | 3 days, 3 02 51.00 | SPR08080b | 1 | |
| wonoyczgola | Jim_2 | stack stack 6 | 0 107 | FJN3228P01C | • | • | 192.168.23.247 | ICX7150-48Z-HPOE | 68 days, 22.23.05.00 | SPS08080b | 2 | |
| | 20 ICX71 | 50-482P Switch_Ke 0 | 00 | FJN3842N005 | | • | 10.11.158.66 | ICX7150-48Z-HPOE | 15 days, 0.50.17.00 | SPS08080d | 1 | |
| | 34 ICX72 | 50-24P Switch_Ken 1 | 031 | DUI3820P0A7 | • | • | 172.18.42.58 | ICX7250-24-HPOE | 12 days, 20:49:08.00 | 9 SPR08080d | 4 | |
| | 24 Freddy | riCX7450-48PSwitch 1 | 069 | CYR3318P0DH | • | | 172.18.57.53 | ICX7450-48-HPOE | 25 days, 20:11:07:00 | SPS08080d | - 1 | |
| | oc freddy | changename stack 📀 | 00 | FEC3221P05W | • | • | | ICX7150-48-POE | 3 days, 19:28:04:00 | SPR08080 | 2 | |
| | | | | | | | | | | 1-10 of 1 | 5 shown | 1 2 |
| witches & Ports Traff | ffic Alarms Even | nts LLDP Neighbors | | | | | | | | 1-10 of 1 Search | 5 shown * | 1 2 C |
| vitches & Ports Trait | ffic Alarms Ever | tts LLDP Neighbors | | Local Port | Loc | al MAC | Remote Port | Remote I | мас | | | |
| witch Name | | | | Local Port 2.5GgabtEthernet1/1/3 | | al MAC 1:9e-4b:13:bc | Remote Port GigabilEthernet0 | Sector 1 | 1952 | Search | ٩ | 0 |
| witch Name n_2_stack | Device Name | Device Type | | | d4:c | | | Sector 1 | 36:48:10 | Search Remote Device Description | Q, Versatile Routin | g Platform |
| | Device Name Quidwäy | Device Type Bridge | oint, Router | 2.5GigabitEthernet1/1/3 | d4:c | 1.9e:4b:13.bc | GigabitEthemet0 | 0/6 64:3e:8c | 36 48 10 36 79 a0 | Search Remote Device Description \$5700.24TP-PWR-SI Huswei | Q. Versatile Routin | g Platform P/SW Ver |

Editing the Device Properties

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

Edit Sim1125

- 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.
- 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 21 Edit Dialog Box

| Device Name: | Sim1125 | | |
|------------------|----------------------|----|--------|
| Tag: | | | |
| Location: | | | |
| GPS Coordinates: | Latitude: Longitude: | | |
| | | | |
| | | | |
| | | ок | Cancel |

- 3. Modify the following configuration settings:
 - Device Name: Assign a name to the device.
 - 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 and later Unleashed networks versions setup 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 AP Details

You can edit the AP details as necessary.

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 view the QR code, then click Edit AP.

FIGURE 22 Editing AP

| Edit AP | | | × |
|---------------|---------------------------------|----|--------|
| | | | |
| * Select AP | dhcp-10-223-34-166(c8:08:73:: V | | |
| * Device Name | dhcp-10-223-34-166 | | |
| Description | testing new set of APs | | |
| Location | Qingdao, China | | |
| | | | |
| | | | |
| | | ок | Cancel |
| | | | |

NOTE

Editing AP details is only supported for Unleashed AP version 200.11 or later.

Using QR Code for Network Access

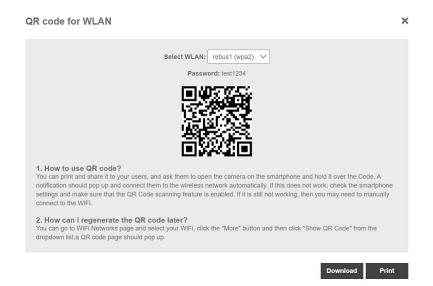
You can now quickly connect to the Wi-Fi network by using the QR code for the network instead of using the username and password. You can also print or download the code for easy access.

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 view the QR code, then click Show QR Code.

FIGURE 23 QR code Generation to Access the Network



NOTE

Generating QR code is only supported for Unleashed AP version 200.11 or later.

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 or later unleashed network. ZoneDirector devices and 200.5 Unleashed networks are not supported.

NOTE

You can apply the new SSID and passphrase to all WLANs, but the new passphrase will only take effect when the WLAN's Encryption Method is WPA2 or WPA3.

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.

Working with ZoneDirector Controllers, Unleashed APs, and ICX Switches Resetting the Password

2. From the list of devices, select the Unleashed network for which you want to edit the WLAN SSID, then click **Edit WLAN**. The **Edit WLAN** dialog box appears.

| Existing WLAN Na | me: johnGuest (wpa2) 🗸 | |
|-------------------------|------------------------|----------------------|
| Enable/Disable WL | AN: Enable Disable | |
| New WLAN Na | me: johnGuest | |
| Access VL | AN: | |
| New WPA2 Passphra | ise: | |
| Total 1 Unleashed netwo | rks will be affected: | |
| Name | Serial Number | IP Address |
| | un111583407426 | 158 10.223.82.133 |
| try | | |
| try | 1 | 1-1 of 1 shown 🔍 1 🔉 |

FIGURE 24 Edit WLAN

- 3. Select the ESSID from the drop-down list. The name, IP address and Serial number of the unleashed network is displayed.
- 4. In Enable/Disable WLAN, select the desired radio button.
- 5. In New WLAN Name, enter the name of the WLAN.
- 6. Click the Access VLAN, to edit the WLAN VLAN.
- 7. Click the New WPA2 Passphrase, provide the password of the WLAN.
- 8. Click OK.

Resetting the Password

You can reset the Web UI login user name and password for devices within the network from the web interface.

 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. From the list of devices, select the device you want to block and then click More > Reset Password. The Reset Password page is displayed.

| FIGURE 25 Resetting the Password |
|----------------------------------|
|----------------------------------|

| User Name | admin | | |
|-------------------------------|-------|--|--|
| New Password | | | |
| * Confirm Password | | | |
| Commin Password | | | |

Configure the following:

- User Name: type a user name
- New Password: type the new password that you want to set to
- Confirm Password: type the new password again to confirm

Blocking Devices from the Software

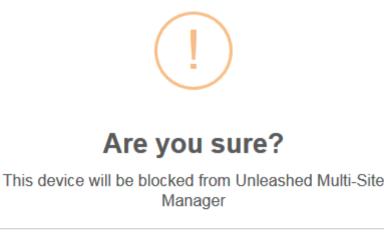
If devices within the network seem unauthorized or are a threat to security, you can use the software Web interface to block the device. You can block one devices at a time.

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.

From the list of devices, select the device you want to block and then click More > Block.
 A confirmation message appears asking if you want to block the devices from the software.

FIGURE 26 Block Screen



Yes, block it!

No, keep it

3. Click Yes, block it!.

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

Connect to Unleashed CLI

You can connect to Unleashed devices CLI from the web interface through tunnel connection.

- 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.
- From the list of devices, select the Unleashed device you want to connect CLI and click More.
 The connection to CLI is supported only on Unleashed 200.12 and above version.

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, Unleashed devices and ICX switches, to make sure that you can easily recover the configuration settings if they ever become corrupted.

NOTE

The number of ZoneDirector (ZD), Unleashed and switch configuration backups to retain in the software database for each device 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.

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

Config Backup & Restore for fm zd 1200

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

FIGURE 27 Backing Up the Configuration

| Choose an Operation |
|--|
| Backup |
| |
| Configuration File Settings |
| Task Name: |
| Upload FTP&Folder / (Default folder is "/") |
| Schedule Backup |
| Frequency Weekly - |
| Day of the Week Sunday - |
| Time of Day 7:00 - |
| Max number of backup files for each ZD is 10 |
| |
| OK Cancel |

In Choose and Operation, select Backup.

3.

- 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 ICX backup file can only be restored to itself and can not be restored to another ICX switch.

NOTE

The restore type (full restore, failover restore, policy restore) is only valid for ZoneDirector and Unleashed devices. You cannot select the restore type for switches.

NOTE

The number of ZoneDirector (ZD), Unleashed and switch 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.

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.

Config Backup & Restore for fm_zd_1200

FIGURE 28 Restoring the Configuration

| Choose an Operation |
|--|
| |
| |
| Select Configuration File(s) |
| Task Name: |
| Restore Type: 🔘 Full Restore 🔘 Failover Restore 💿 Policy Restore |
| ZD1200 10.0.0.1424 (1 selected) ddddddddd(171406000001_1 - |
| Specify a time to perform this task |
| Restore now |
| Schedule restore later: |
| |
| OK Cancel |

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: 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.

Upgrading Device Firmware

You can initiate the upgrade of unleased networks and switches from the Unleashed Multi-Site Manager web interface.

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 upgrade the firmware and then click Upgrade.

A confirmation message appears.

NOTE

To upgrade the switch, go to **Administration** > **Switch Firmware** and upload the ICX image to Unleashed Multi-Site Manager first. You can then select the uploaded ICX image. For Unleashed networks, only online upgrade is supported.

3. Click **Yes** to upgrade the device firmware.

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.

- 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 **Delete**.

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

FIGURE 29 Delete Screen

(!)

Are you sure?

You will not be able to recover those selected items! [, 00:1f:42:00:07:01]

Yes, delete it!

o, keep it

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

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

Downloading AP log

For debugging purpose, you can download Unleashed System Log through UMM directly. It is not local in UMM but a request to Unleashed. Both Unleashed connection and SSH connection should be online.

1. In the left pane, click **Devices**.

2. In the **Devices**table, click Unleashed network.

| RUCKUS | red Mati-Ste Votager | | | | | A Your | WM system has insufficien | ticenses. | • | 2019/12/03 13:10 | • | admin@rudus. | orn Hel |
|-----------------------|----------------------|------------------------------------|------------------|---------------|------------|-----------------|---------------------------|---------------------|-----------|------------------|--------|--------------|----------|
| Dathboard | Devices | | | | | | | | | | | Let | Group |
| Devices | 0 + / = 7 A | Ect. Ect WLAN Block Boc | kup & Restore Up | grade Delete | | | | | | | Storph | Q | |
| Taos | - System | Nave | Member Count | Serial Number | Connection | 5.5H Connection | Management IP | IP Address | Model | Locat | ion | | Software |
| 1777 | - Waxies Networks | 20 Servets-203K-9132 | 000 | 211208000181 | | | | 10 11.157.158.443 | 201500 | | | | 10.2 8 0 |
| Unleasived-Zero Youch | - Kennath KZD | Construction Construction - T310-2 | 000 | un42170000458 | • | | 10.223.87.12 | 18 223 87.99 443 | Unieshed | | | | 200.8.10 |
| Resta | RUN | 20 Freddy_101_2 | 000 | \$61030003770 | | | | 18 223 5 208 443 | 201290 | | | | 10.3 8 0 |
| nipora 🕨 | Kin | RTSS-Universited-galescey-ba | 000 | un20190200002 | | | | 12 (3 150,255-443 | Unleathed | | | | 200.0 % |
| Administration 👻 | treddy | 20 0000000-000001 | 000 | 051608081840 | | | 10.223.21.1 | 18 223 20 1 443 | 201200 | | | | 10.3.0.0 |
| | jin_un jin_zd | 20 m. edi20000000 | 000 | 171838001080 | | | | 18.223.21.48.443 | ZD1299 | | | | 10380 |
| Autt Log | | 20 Fredex20_103_3 | 000 | 171806080196 | | | | 10 223 5 57 643 | ZD1200 | | | | 10.4 8 0 |
| Lorse | NICX. | | 000 | un93194900000 | | | | 182 159 12 57 443 | Uniesched | | | | 200.8.90 |
| | | Contraction Unleasthed | 000 | un60160200685 | | | | 28 20 0 42 443 | Uniegoned | | | | 200.8.10 |
| Switch Firmware | | A 2008-upgrade | 000 | u#95160240378 | | ٠ | 192.168.224.190 | 182 150 225 136 443 | Unleashed | | | | 200.8.10 |
| Users & Assignment | | 1 | | | | | | | _ | | | | _ |

3. In the General tab, click Save Unleashed System Log to download the unleashed system log.

| License | | Geo UMM_AUTO_R610 | 000 | 01192194900090 |
|--|---------------------------|------------------------------|--------------|-----------------|
| | | Ruckus-Unleashed | 000 | un50160200885 |
| Switch Firmware | | 2008-upgrade | 806 | un96160240378 |
| Users & Assignment | | | | |
| SSL Certificates | General Access Points II | CX Switches Mesh View C | lients WLANs | Alarms 🛜 Events |
| DB Backup / Restore | | | | |
| a sura | Info | | | |
| Support | Device Name | R750-Unleashed-gateway-built | 1195 | |
| System 🕨 | Unleashed ID | un20190200002115723364687 | 62 | |
| and the second sec | Model | Unleashed | | |
| | MAC Address | 1c:3a:60:3b:de:a0 | | |
| System Into Version: 2.3.0.0.27 | IP Address | 10.13.150.255 | | |
| Version. 2.3.0.0.27 | IPv6 Address | | | |
| | SSH Connection | Connected | | |
| | Management IP | | | |
| | Last Seen | 2019-12-03 15:43:55.0 | | |
| | Up Time | 4d 22h 16m | | |
| | Software | 200.8.10.3.199 | | |
| | Location | | | |
| | GPS | | | |
| | Total Transmitted | 356.68GB | | |
| | Total Received | 859.20MB | | |
| | Total Transmitted Packets | 437.20M | | |
| | Total Received Packets | 10.35M | | |
| | Received Bytes | 4.00MB | | |
| | Transmitted Bytes | 114.88MB | | |
| | Received Packets | 47.60K | | |
| | Transmitted Packets | 854.61K | | |

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 30 Viewing Tasks

| O & an ARBIG company Unlearsh | ed Multi Site Manager | | | | 2019/03/05 | 10:48:38 | (8 elerine) adr | rin@rucki | is.com |
|------------------------------------|-----------------------|---------------|------------------------|---------------------------------|--------------------|----------|-----------------|-----------|--------|
| | Tasks | | | | | | | | |
| Devices | 🗊 Delete 🥒 Edit | | | | | Search | d | ø | ٠ |
| | Task Name | Task Type | Schedule | Status | Configuration File | | Created | | |
| Tasks | backup20190227163929 | Backup | | Success on Feb 27 2019 16:40:10 | | | Feb. 27 201 | 14:09:43 | |
| Reports | Detais | | | | | | 1-1 of 1 shown | x 1 | R |
| System 🕨 | | | | | | Search | | ۹ [۵ | 0 |
| System Info Version: 2.2.0.0.28 | Device Name | Backup File M | lame | Model Name | Version | | Backup Time | | |
| Version ^e 2.2 fr 0.28 | ICX7150-24P Switch | FFA3224P004 | hackup20190227183929_1 | 302270 ICX7150-24P | SPS08090_b289 | | Feb 27 2019 14 | 10-11 | |
| | | | | | | | _ | | |

The following information about the task is displayed.

- Task Name: displays the name of the task.
- Task Type: displays the type of task created for the user such as Backup, Restore and so on.
- 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**. You can also select a task in progress and click **Edit** to modify the settings, however you can only edit scheduled tasks.

Zero Touch Deployment

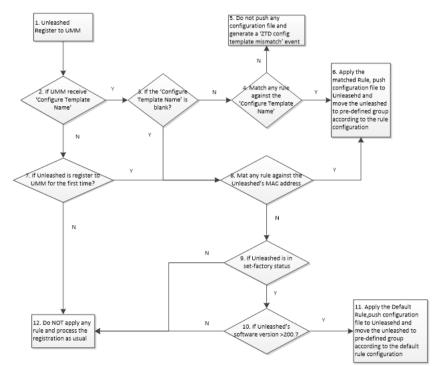
Unleashed Zero Touch Deployment feature simplifies the deployment for Unleashed. The deployment is ready with some simple configurations on Unleashed Multi-Site Manager and Unleashed side as the power is on.

The main purpose of this feature:

- Unleashed can be configured to designated version and configuration automatically after power on.
- Unleashed can be assigned to designated groups in joining Unleashed Multi-Site Manager automatically.
- It allows to pre-configure the 'Configure Template Name' and 'UMM IP' on the Unleashed by Unleashed Setup Wizard manually or by DHCP server.
- It also pre-configure a rule with the same 'Configure Template Name' on the UMM server and attach one Unleashed backup file to it.
- Whenever a set factory Unleashed boots up, it sends a message with 'Configure Template Name' to the UMM server according the IP inside the parameter 'UMM IP'. Once UMM server receives the message, it matches the rule with 'Configure Template Name' against its data base and push the configure file to the Unleashed.
- For the Unleashed 200.7 or previous release Unleashed which does not support the new parameter 'Configure Template Name' and 'UMM IP', can pre-configure a rule with Unleashed master AP's MAC address to UMM. When the Unleashed register to UMM for the first time, UMM matches the rule against the MAC address and push the configuration file to Unleashed.

Zero Touch Deployment Workflow

- 1. Unleashed register to UMM: For 200.8 Unleashed, you can provision the UMM IP to Unleashed during the setup wizard manually or you can provision by DHCP server option 43 automatically.
- 2. When UMM receive the registration message from Unleashed, it checks whether the parameter 'Configure Template Name' is inside the message. For 200.8 Unleashed, you can provision the 'Configure Template Name' during the setup of the wizard manually or provision by DHCP server option 43 automatically.
- 3. The 'Configure Template Name' is optional, Unleashed sends a blank 'Configure Template Name' to UMM if you do not provision this parameter.
- 4. UMM matches the Zero Touch Deployment rule against the 'Configure Template Name'.
- 5. If UMM cannot match any Zero Touch Deployment rule, it stops the deployment and generate a 'ZTD config template mismatch' event to remind you. The Unleashed retry the registration after timeout.
- 6. If UMM find any rule which contain the same 'Configure Template Name', it pushes configuration file to Unleashed and move the unleashed to pre-defined group according to the configuration of the Zero Touch Deployment rule.
- 7. UMM checks if the Unleashed is register to UMM for the first time.
- 8. UMM matches the Zero Touch Deployment rule against the Unleashed AP's MAC address. This only apply to the Unleashed which is register to UMM for the first time. For example, Unleashed already register to UMM, and then customer restart the Unleashed AP, after start up, the Unleashed will register to UMM again but UMM won't apply the Zero Touch Deployment to the Unleashed since it's not the first time registration.
- 9. UMM check if Unleashed is in set-factory status.
- 10. UMM check if Unleashed's software version is later than 200.7
- 11. UMM apply the Default Rule only to the 200.8 or later Unleashed which is NOT in set-factory status. This is to avoid unintentional deployment. For example, if Unleashed is not in set-factory status which means the Unleashed has the setup already, then in this case we do not deploy the default configuration file to the Unleashed to avoid any mistake.
- 12. UMM do not apply any Zero Touch Deployment rule and process the registration as usual.



Creating a New Rule

The Unleashed-Zero Touch Deployment page in the user interface allows the user to create, edit, import, and download an example rule.

- 1. After you log in to the Web interface, select Zero Touch Deployment from the menu in the left.
- 2. Click Create button, the Create New page appears.

| Deployment Rule Assign Unleashed to group and | example restore the selected configuratio | n file | |
|---|--|---------------|-----------------------------|
| * Assign To Group | freddym | · (+) | |
| Restore Configuration | - Wireless Networks | + × | |
| Unleashed networks match belo | – jim_un – jim_zd – Kim | pplied to thi | s rule |
| Config Template Name Mac Address List | - CorpZD - P300 | gment. For | For example file click here |
| | – Kenneth KUN KZD | | Import Mac Address |
| | - freddym | | |
| | 710720 | | |
| | 770 | • | |

- 3. In **Deployment Rule**, enter the rule name.
- 4. In **Assign To Group**, select the group name from the drop-down, when the device registers to UMM for the first time. UMM assigns the device to the predefined group automatically.
- 5. In Restore Configuration, if you click the Select backup file to restore checkbox then do the following:
 - a) Select the backup file from the drop-down.
 - b) Click () and Create New window pops-up. In the pop-up, click Choose file to select the backup file, enter the comment, and click OK.
- 6. In Mac Address List, enter the mac address or click Import Mac Address.

In Unleashed-Zero Touch Deployment, click Import Rule button to import a rule.

NOTE

The file formats are only in CSV or TXT format.

In Unleashed-Zero Touch Deployment, select the required rule and click Edit or Delete button to edit or delete the rule respectively.

Registering Unleashed to UMM

It is for the first time registration of Unleashed to the Unleashed Multi-Site Manager. After Unleashed passes the condition check, Unleashed Multi-Site Manager will apply the rule.

Use case for Unleashed registering to UMM at the first time

| Serial number | Unleashed Status | TAG | Unleashed Version | MAC | UMM Actions |
|---------------|---------------------|---|-------------------|-----------|---|
| 1 | Factory reset | Configured by DHCP Option or Unleashed Wizard. | 200.8 and above | not apply | TAG match: trigger rule for TAG TAG mismatch: Generate a fail event ZTD config template mismatch or ZTD backup file not found |
| 2 | Factory reset | TAG is not set in DHCP Option, Wizard, or TAG is an empty string. | 200.8 and above | apply | MAC match: trigger rule for MAC. MAC mismatch: trigger default rule |
| 3 | None factory status | Not apply even if the TAG is set in the DHCP Option. | All | apply | MAC match: trigger rule for MAC. MAC mismatch: do nothing |

Working with Reports

| • | Available Report Types | . 63 |
|---|--------------------------------------|------|
| | Generating an AP Report | |
| | Generating a WLAN Report | |
| | Generating a Client Report | |
| | Generating Reports for Rogue Devices | |
| | Viewing Saved Reports | |

Available Report Types

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

NOTE

Lite mode does not provide report page and client information.

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

Working with Reports

Available Report Types

FIGURE 31 Report Page

| RUCKUS" | hed Multi-Sile Menager | | | | | | | | | | | | | | | | |
|------------------------------------|------------------------|----------------------|---------------------------------------|--|------------------------------|---------------|--|---------------------|---|--|---------------|------------------|---|-------------|--------------|------------------|-----|
| Contract Contract | AP | | | | | | | | | | | | | | | | |
| Devices | • | | | | | | | | | | | | New Report | | | | |
| Taska | New Report | Overview | | | | | | | | | | | Top AP 1 | Traffic | | | |
| Unleashed-Zero Touch | 8aved Reports | | | | | | | | | | | | | | | | |
| Reporta 🗸 | Report Name | ~ | | | | | Rx 45.65 GB | | | | | | 15-20 | _ | | | - |
| 40 | ap all | | | | | 1 | h: 113.24 GB | | | | | | | | | | |
| | | | | | | | | | , in the second s | | | | 1979 - 1979 - 1979 - 1979 - 1979 - 1979 - 1979 - 1979 - 1979 - 1979 - 1979 - 1979 - 1979 - 1979 - 1979 - 1979 - 1979 - 1979 | | | | |
| WLAN | | 158.89 | | | | | | | | | | TERM AT'S 193 | 6-90 6-70 9-70 | | | | |
| Client | | 100.05 | aa | | | | | | | | | 193 | 2 | o 50 | 100 | 150 | 200 |
| Нодан | | | | | | | | | | | | | | | | | |
| Administration | | | | | | | | | | | | | | | | | |
| System 🕨 | | Name | MAC Address | Controller Name | Sensi Number | II' Address | II'v6 Address | External II* | Model | Last Seen | Location | Software | Al" Mesh Type | Tunnel Mode | Heboot I mee | Iz Bytwa 🕶 | |
| | | H510-maxter | 94.f8.65.2a;2x;a0 | HS10-Universited-build180 | 211806000047 | 10.12.150.251 | | 10.12.150.251:12225 | 8610 | Nov. 20 2019 00:38:14 | | 200.8.10.3.190 | Disable | 13 | 0 | 52.84GB | |
| System Info Version: 2.3.0.0.25 | | T310x R510-K-8CE0 | 34.8127:18.78.80 10:3e:50.07:8::e0 | kenneth-203K-0132 Ruckus-Witeless-1200-K2 | 331708000024 961602203/51 | 10.11.158.235 | 2001:10:11:128:3881:2785w1 2001:10:11:128:825w:9085w0 | | 1310a r510 | Nov. 20 2019 00:32:02 Nov. 20 2019 00:31:30 | | 10.2.0.0.142 | RAP Disable | 13 | 0 | 2.47G8 2.4308 | |
| Validite 2.300.025 | | TSTON | 34.fac9f.25:91.b0 | Universitied_Jim_R510 | 481703000025 | 192.168.23.49 | 2001:10.11.120.234.501046 | 192.168.23.49.12225 | 1310n | Nov. 20 2019 00:31:30 | xIIC abenzhen | 200.8.10.3.173 | RAP | 6 | 0 | 2.0108 | |
| | | dhop-10-223-6-221 | 44:14:38:21:48:71 | Kennedh-N/510 | 941802001249 | 11.12.0.1 | | 11.12.0.1:12225 | m510 | Nov. 20 2019 00:35:57 | | 200.8.10.3.190 | Disable | 13 | 0 | 1.9168 | |
| | | H800-K-2850 | 10:50:52:29:28:90 | Ruckus-Witeless-1200-K2 | 521493802981 | 10.11.158.69 | 2001:10:11:128:1260:528.542 | 10.11.158.69.12223 | 1600 | Nov. 20 2019 00:31:30 | | 10.4.0.0.23 | RAP | 13 | 0 | 1.47GB | |
| | | dhcp-10-223-4-175 | 2::54.93:18:07:80 | kenneth-203K-0132 | 511303000213 | 10.11.157.198 | 2001:10:11:128:2x5d:50%/w | | r700 | Nov. 20 2019 00:32:13 | | 10.2.0.0.142 | RAP | 13 | 0 | 1.45G8 | |
| | | dhop-10-223-4-223 | 21:54.93:18:10:40 54:ec:2105:e3:e0 | kenneth-203K-9132 UMM_AUTO_R610 | 511303000222 | 10.11.158.147 | 2001:10:11:128:2x5d:5317.fw | 10.11.158.147:12223 | #700 #320 | Nov. 20 2019 00:32:25 Nov. 20 2019 00:43:40 | shenchai | 10.2.0.0.142 | RAP Not Supported | 13 | 0 | 1.44G8 | |
| | | RuckuaAP | 54 ac 2108 p4 w0 | UNM_AUTO_R610 | 27120208038 | 192.168.12.50 | | 192.168.12.50.12225 | r320 | Nov. 20 2019 00:43:40 | 24.04 | 200.8.10.3.190 | Not Supported | 13 | 0 | 1.3868 | |
| | | | | | | | | | | | | | | | | | - |
| | | | | | | | | | | | | | | | | | |
| | | Traffic vs Model | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | Tr | affic vs Mode | 1 | | | |
| | | | | | | | | | | | | | | | | | |
| | | Rep | ort Options | | | | | | | | | × | : | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | G | roup: All Device | es 🔻 | Interv | al: 1 Hour | ▼ | | | | | | | | | | |
| | | ті | ime Period: 💿 La | ast Hou | ır 🔘 Sta | rt Time: | | End Tir | ne: | | | | | | | | |
| | | | _ | | | | | | | | | | | | | | |
| | | | Filters | | | | | | | | | | | | | | |
| | | | Filter Rows Whe | ere: MAC Addre | SS | ▼ is | | and 4 | - | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | Oł | ٢ | Cancel | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |

You can click Export and select CSV or PDF to generate reports as CSV files or PDF files respectively.

TABLE 11 Reports in Software

| Report Name | Description |
|-------------|---|
| AP | View current status and detailed information about APs. |
| WLAN | View the detail information about WLANs. |
| Client | View the detail information about Clients. |
| Rogue | View the detail information about Rogue APs. |

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
- 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 32 Report Options

| Report Options | × |
|--|---|
| Group: All Devices Interval: 1 Hour Interval: End Time: Time Period: | |
| Filters Filter Rows Where: AP MAC Address is and + | |
| Query | |

- 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, 1 day, and 1 week.
- 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 24 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 OK. A report is generate based on the options configured.
 You can also save the report periodically. For more information see, Saving Reports and Generating Reports on page 66

Saving Reports and Generating Reports

You can periodically save the reports that you generate.

1. From the Reports Option area, click Save.

The Generate Report page appears.

FIGURE 33 Saving and Generating a Report

| | | | | | | C 2019/11/20 14:01:20 | A 375 alarms | admin@ruckus.com | (2) Help |
|----------------------|--------------------|----------|------------------------------|-------------|---------------|-----------------------------|-----------------|------------------|-------------|
| * | AP | | Generate Report | × | All Caujoos | | vt 19 Linuire | | Save |
| Dashboard | | | Name: | | | | | _ | |
| Tasks | New Report | | Generate File: 🖉 CSV 🛛 Ø PDF | | | | | | |
| Unleashed-Zero Touch | Saved Reports Area | Overview | Frequency: Hourly | | affic To | op 10 APs' Traffic | | | |
| Reports 🗸 | Report Name | 110 | FTP: Enable FTP folder | | | | | | |
| AP | abcd ap all | | Email: Enable Email Address | Θ | | | | | |
| WLAN | 1-2 of 2 shown | То | | OK Cancel | | | | | |
| Client | | 160 | 7.00 as | \$ 0 | 0 10G 20G 30G | 40G 50G 6 Traffic (Byte) | | | |

- 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 OK.

A message is displayed confirming the report is saved. The report is listed in the Saved Report area now.

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

2. Click AP in the sub-menu.

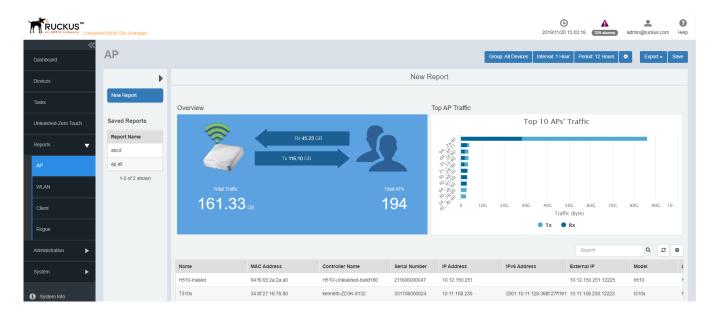
The **AP** reports page is displayed with a Set Report Option (

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 and select CSV or PDF to have the reports saved as a CSV or PDF file respectively.

FIGURE 34 AP Report Page



3. Configure the report settings as described in Configuring Report Options on page 65.

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 Saving Reports and Generating Reports on page 66.

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

2. Click WLAN in the sub-menu.

The WLAN reports page is displayed with a Set Report Option (

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 and select CSV or PDF to have the reports saved as a CSV or PDF file respectively.

FIGURE 35 WLAN Report Page

| RUCKUS" | | | | | | | | | | | | | | | | | | | | | | | | | | 2010/11/20 1 | | ± O |
|----------------------|-----------------------------|-------------------------------------|----------------|-------------------|-------------|----------------------|----------|----------------------|------------|--------------------|--------------------------|-------------------|----------------|----------------|---------------|---------------|-----------------|--------------------|-------------------|-------------------------|-------------------|-----------------|---------------|-----------------|----------------|---------------------|--------------------|--|
| Daubteard | WLAN | | | | | | | | | | | | | | | | | | | | | | | | Group A | Devices Device: 114 | r Period 12 Hans 0 | Equi- See |
| Devices | • | | | | | | | | | | | | | | New Rep | ort | | | | | | | | | | | | |
| Inte | New Report | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Jeved Reports | Overview | | | | | | | | | | | | | Top | SSID Traffic | | | | | | Top 10 SSIDs' | Traffic | | | | | _ |
| Colorado Carlo Kouch | Report Name | ~ | | | | | | ** 2.11 (| a | | | | | | | | | | | _ | | 100 10 33103 | - Talling | | | | | _ |
| Papata 👻 | when all 1-1 of 1 aboves | | | | | | | 1.20.10 (3) | | | ⇒ | | | 2 | | | | | | | | | | | | | | |
| | | 22.27 | | | | | | | | | | | | | 8 | 19. | 1904 9004 | 750M 1,000M | 1,8504 1,5004 | 1,790M 8,000M | 4,250M 4,500M | 2,790M 2,000M | 4,2104 4,000 | 4 0,750M 4,000 | 4,2904 4,900 | W 4,750W 5,000W | LENN LOOM C | TON 8,0004 8,2- |
| | | | | | | | | | | | | | | | ~ | | | | | | | • Ta • | fic (Ryte) | | | | | |
| Paga | | | | | | | | | | | | | | | | | | | | | | | - | | | | | _ |
| Accumation 🕨 | | | | | | | | | | | | | | | | | | | | | | | | | | | Dearch | 9 Ø Ø |
| System (| | WLAN Name | Istal Cianta + | Bultural 5.725 | La Pauloate | He Pashata 05.325 | In Hyber | A 2200 | In letters | He krouty | En Dowel Phile | It's Depart Phile | In Board Phile | Ro Based Phile | La Data Phile | He Date Phile | To Date Drop 1% | a In Hypel Deep 79 | for To Data Hytes | Ha Data Kyles 4.2205 | La Reput Pitte | He Report Phile | To Mgrei Phia | 10. Mgred Palar | La Mgeri Mylea | Ha Mgert Myles | | |
| O System bein | | Mh11pak | 440 | 421K | 287.746 | 16.314 | 18.7946 | 17946 | on. | 0X | 20.866 | 12.70K | 38.396 | 4.216 | 250.30K | 7.336 | DK. | DK DK | 16.71M8 | 774.7968 | 208.75K | 0K | 17.446 | 0.81K | 2.0998 | 0.35545 | | |
| Ventore 23.8.025 | | 10 Yeak | 21 | 21.294 | 3.53M | 1.569 | 3.68G8 | 1.8108 | 06 | 04 | 3.1491 | 1.54M | 15.536 | 0.20% | 3.18M | 1.400 | 04. | IK. | 3.8108 | 1.1958 | 371.98K | 20.194 | 351,214 | 181.47K | 70.1346 | 33.38648 | | |
| | | Freddy, 30720 | 4 | 0.095 | 1.836 | 0.885 | 340.5393 | 105.979.8 | 06 | 05. | 1.25K | 0.836 | 0.354 | 0.095 | 0.55% | 0.355 | 06. | 0K | 121.098 | 34.7843 | 0.15K | 06 | 0.5/K | 0.316 | 221.5248 | 75.19KB | | |
| | | ruchua-accaso | | 2.325 | 845.141 | 105.06K | 316.85WD | 12.74555 | 05 | 306.38% | 773.696 | 181.995 | 42.161 | 0.155 | 242.40% | 155.124 | 06. | 05 | 170.90MB | 14.819/0 | 32.096 | 2.924 | 605.714 | 29.95% | 148.05440 | 4.5453 | | |
| | | Kerneth-Utileashed-1212a- 3036.1 | | 0.31K | 45.555 | 20.746 | 54.38MB | 3.94MD | 05 | 01. | 20.814 | 31.435 | 2.944 | 0.22% | 37.48K | 26.504 | 06. | 01 | 22.17MB | 2.949/0 | 4.305 | 0.094 | 9.176 | 4,245 | 2.1990 | 1.00M3 | | |
| | | 11ao-1850-16-50-Tunnel-2 | | 0K | 2.25M | 1.389 | 2.5068 | 131.79MD | OK. | DK. | 2.294 | 1.384 | DK. | 0.85K | 2.194 | 1.3894 | OK. | DL | 2.5360 | 101.7940 | 04. | 1.284 | 28.85K | DK | 042 | 042 | | |
| | | Jan, Litheoded, 9020, W1 | | 0.12K | 22.40K | 11426 | 0.0450 | 2.3550 | 05 | 04. | 10.424 | 13.30K | 1.885 | 0.12% | 8.87% | 3.425 | 04. | 04 | 6.15402 | 1.419/2 | 0.316 | 0K | 11.61K | 3396 | 2,759/2 | 981.5142 | | |
| | | mapor. | | 05 | 221.00K | 05 | 43.6763 | 09 | 05 | 8 | 201.005 | OK. | 8 | 05 | 05 | 05 | | 05 | 09 | 0.0 | 05 | 05 | 201.005 | 05 | 49.419.9 | 053 | | |
| | | Traffic va Channel | | | | | | | | | | | | | | | | | | | | | | | | 14 | of 150 above 4 | 23455 |
| | | 20 | | | | | | | | | | | | | Traffic vs Cl | sannel | | | | | | | | | | | | _ |
| | | | | | | | | | | | | | | | | | | | | | | 1.1 | | | | | | |
| | | · . | | | 3 | . , | | | 10 | - | 14 14 | | 40 | | 4 • 14 | 20 00 | | 100 | 104 | 110 | | 189 | 124 | 122 7 | 140 | 140 | 124 127 | |
| | | AP / WLAN / Client Co | ounts vs SSID | | | | | | | | | | | | • | - | | | | AP / WLAT | I / Client Counts | vs Channel | | | | | | |
| | | 100 | - | | | | | | W | LAN / AP / Clie | nt Counts vs S | SID | | | | | | | p. | 200 | | | AP / 1 | WLAN / Client | Counts vs Ch | annel | | - 4200 |
| | | 8 | ryak | 114-000-0-00-% | eral-1 | 9184 | Dates | - Window Harrado - 1 | laval | -20-3.12.1 • AP | larvafi-2121- • Chest | E-mil | trolate | , - | Kguani (2) | 10 | 17224 | There | | **/Gas | ų, į | ųų | | •••• | | | | ₩ ² ¹⁰⁰ ⁶ |

3. Configure the report settings as described in Configuring Report Options on page 65.

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 Saving Reports and Generating Reports on page 66.

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

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, Controller Name 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 and select CSV or PDF to have the reports saved as a CSV or PDF file, respectively.

FIGURE 36 Client Report Page

| CKUS" | | | | | | | | | | | | | | | | | | | 2019/ | | <u>e</u> atrojuta.co |
|------------------|--|--|-----------------------------|----------------------------------|------------------|--|---|--|-------------------|--------------------------|-------------------------|--------------------------------|-----------------------|---------------------------|--|--|---|--|------------------------------------|--|-------------------------|
| Client | | | | | | | | | | | | | | | | | | Gene | pr Al Devices Minro | al 1 Har Partial 12 Hours | • Equat • Sec |
| • | | | | | | | | | | | New Report | | | | | | | | | | |
| New Report | | | | | | | | | | | | | | | | | | | | | |
| Deved Reports | Overview | | | | | | | | | | Top Clients' Traffic | | | | | Top 10 Clients' Traffi | | | | | |
| Report Name | ~ | | | / | | Pa 8.52 G8 | | | | | | | | | | Top To Clients Train | | | | | _ |
| thei standard 30 | | | | | | | | | | | 1 8 E | | | | | | | | | | |
| thei al | | | | | | - 31.42 (1) | | | | | | | | | | | | | | | |
| 1.2 of 2 shows | San Sufe | | | | | | | | | | | | | | | | | | | | |
| | 31.14∝ | | | | | | | | | 1000 | 197 - T | 10 20 4 | e0 40 50 | 80 | 70 80 80 | 100 110 | 120 140 14 | 0 150 | 100 170 | 180 190 | 200 210 220 |
| | | | | | | | | | | | | | | | • • | Traffic (kyss) allia(Daurchai) 🔹 Traffic) | وشطي | | | | |
| | | | | | | | | | | | | | | | | | | | | | |
| | Top 1000 Chards Navi 100 | | | | | | Total International Internationa International International Internation | | | | | | Departure Department | | | | | | | 2ams) | a 8 • |
| | Name VWC.0001 Mail: 00040102 | Cantrolar Name | 8184899999 10.12.160.183 | MAC Address 00 05:01:02 00:01 | CE Hype | Vanalar Ciaco Systema, Inc | | | Zearrinth Pashata | Upleth Paultalu 7.37M | Indha(Desminik) Hyber + | Bratha (Dplot) Byles 8.2208 | Dearstock Drag Hyrrit | Description Drug | Date Dplink Drul | amana Biplinik Dagi DK | | | | | |
| | ter-fad | Reckus Winkess 1200-82 | 16.11.158.181 | 14.20.5x81.75.54 | Appin IOS | Appin, Ire. | | | L TRM | 1.404 | 2.8008 | 132.2/148 | DK. | DK . | DK . | 0K | | | | | |
| 230.028 | VWC-0005-MAC-00050102 | PS10-Universited-build 180 | 10.12.150.179 | 00.05.01.02.00.05 | Others | Ciaco Systema, inc | | | 961.58K | 5.20K | 476.554/6 | 1.1616 | 04 | 05 | 06 | 06 | | | | | |
| | | PS10-Universited-build150 | 10.12.150.178 | 00.05.01.02.00.08 | Others | Checo Sysilema, inc | | | 961.58K | 5.196 | 475.5540 | 1.16965 | 04. | 05 | 06 | 06 | | | | | |
| | VWC-0011-MAC-00090182 | PS10-Uniexeteoroute150 | 10.12.150.175 | 00.05.01.02.00.06 | Others Others | Cisco Systems, Inc. Cisco Systems, Inc. | | | 161.58K | 5.204 | 4/6.5540 | LIEND | DK. | DK. | 05 | 0K | | | | | |
| | VWC-0004-MAC-00050102 | | 10.12.150.180 | 08.05.07.02.00.04 | Others | Claco Systema, Inc. | | | 901.5/W | 5.214 | 476,5450 | 11640 | 04 | 04 | | | | | | | |
| | VWC-0013-MMC-00030702 | PS10-Universited-Guild 190 | 10.12.150.171 | 08.05.01.02.00.54 | Otwo | Claco Systema, Inc. | | | 01.57% | 5.158 | 478.5450 | 1.16142 | 04. | DI. | 05 | 05 | | | | | |
| | | PS10-Orientechuld180 PS10-Orientechuld180 | 10.12.150.170 | 00.05.01.02.00.04 | Otwo | Claco Systema, Inc. | | | 81.5/K | 5216 | 401.5400 | 11810 | 05 | DK. | 0K 0K | OK (W | | | | | |
| | | | | | | | | | | | | | | | | | | | | 1-10 of 1000 shows | 12345 |
| | | | | | | | | | | | | | | | | | | | | | |
| | Vendor vs Clients | | | | | | Vendor vs Cli | ents | | | | | | × | endor vs Traffic | | Vend | or vs Traffic | | | |
| | Vendor vs Clients | | | | | | | ents | | | | | | | endor vs Traffic 400 | | Vend | or vs Traffic | | | |
| | Vendor vs Clients | | | | | | | | | | | | | v | 400 781 410 | | Vend | or vs Traffic | | | |
| | Vendor vs. Clients | | | | | | | | | | | | | | *** | νς, 114 Αφρία, 114 | Intel Carpor | | CM | martsan Tedrology Co., Lod. | Ollers |
| | Vendor vs Clients | | | | | | | | | | | | | | +00 20 20 20 | | Intel Carpor | ela Xaseri Ga | CM | nartuar Technology Co., Lol. | Olive |
| | | | | | | | | s C.ine80 | | | | | | | 400 7 400 8 400 0 Check System | | tal Cryse Talldoad | ela Xaseri Ga | - cul | nartan Telivulay Co., Lui | Dilws |
| | Traffic ye Clanete | | | | | | Ober 207 | s C.ine80 | | | | | | | 400 7 400 8 400 0 Check System | | tal Cryse Talldoad | n Xaari Ga bal) & Taalhajaga | - cul | nahtan mahudugi Ca, Lat | Ofers |
| | Traffic vs Ciente | | | | | | Ober 207 | s C.ine80 | | | | | | c | 400 7 400 8 400 0 Check System | | inii Ciyo O Tallidaad | n Xaari Ga bal) & Taalhajaga | - cul | nattan "tabulag Ca, Lat | Offers |
| | Traffic ye Clanete | 440 11,02 20 | 19 11.484 | 0840 11,010 | (720 11,42) | | otensit? | 11.021102 | 11,40 1240 | 11.021440 | 11.21.422 | 11,0215.00 | 11,421685 | 0 8400 | 400 200 200 Court System Event Traditic - Downsinkly Event Traditic - Downsinkly Event Traditic - Downsinkly | | Ind Case Tublicand Client Traffic 20:300 39: | n Xaari Ga bal) & Taalhajaga | ual bab) blink | nartsan tudinulagr Sa, Lat 300-1000M 1000- | |
| | Traffic as Clients | | 0 11,40 | 0840 11/20 ¹⁰ | 94 1.44 | | Counted State | 11.021102 | 1.at load | 1.421442 | 11.22 1448 | 1.010.0 | 1,421448 | 2400 1200 **C bas 0 | Hand Jack Converting of the second se | plink | Ind Case Tublicand Client Traffic 20:300 39: | na Sauri Gu hili Tudhégel -Downlink/Up | ual bab) blink | u | |
| | Traffic ve Clienta 90 40 40 40 40 | | 2 11.404 | 3949 11.819 | 11.92 | • | Counted State | но констранции и констранции | 1.01120 | 1.0148 | L.E.H.G | 1.6118 | 1,21948 | 2400 1200 **C bas 0 | | plink | enti Case • Turkiçanı Client Traffic • Second • Reak to the | na Sauri Gu hili Tudhégel -Downlink/Up | uai biaŭ slink M 400-500M | u | |

3. Configure the report settings as described in Configuring Report Options on page 65.

The table area displays information about the client such as the name, IP address, OS type, vendor, Controller Name 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, and so on.

4. Generate the report as described in Saving Reports and Generating Reports on page 66.

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

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 and Filters. Refer the illustration below.

FIGURE 37 Rogue Report Options

| Report Options | | × |
|---|----|--------|
| Group: All Devices Filters Filter Rows Where: Rogue AP BSSID is and | | |
| | ок | Cancel |

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** and select CSV or PDF to have the reports saved as a CSV or PDF file respectively.

The options **Top 1000 Rogues** and **Next 1000 Rogues** displays the list of top 1000 and next 1000 rouges devices detected thus far respectively.

The page typically displays following information about the rouge device that's detected:

- Detecting Network Name
- Detecting AP Name
- Rouge AP BSSID
- SSID
- Туре
- Channel
- Radio Type
- Encryption
- Last Detected

FIGURE 38 Rogue Report Page

| | ed Multi-Site Manager | | | | | | | | | | © 2019/11/20 17:55:54 @ | A adming | A Parton Balantian |
|----------------------|-----------------------|--------------------------|-------------------|-------------------|-----------------------------|------|---------|------------|------------|-----------------------|----------------------------|-----------|--------------------|
| Cashboard | Rogue | | | | | | | | | | Group: All | Devices o | Export • Save |
| Devices | • | | | | | | | New Repor | t | | | | |
| Tasks | New Report | Top 1000 Rogues Next 1 | 000 Rogues | | | | | | | | Search | | Q 0 0 |
| | | Detecting Network Name | Detecting AP Name | Rogue AP BSSID | SSID | Туре | Channel | Radio Type | Encryption | Last Detected | | | |
| Unleashed-Zero Touch | Saved Reports | Jim_R600_2005 | RuckusAP | d8:38.fc:2a:72:ao | Hotspot/WPA2BydGPWLAN | AP | 40 | 802.11a/n | Encrypted | Nov. 18 2019 22:18:02 | | | |
| Reports 🗸 | Report Name | Jim_R600_2005 | RuckusAP | 58:b6:33:3b:fb:bo | Hotspot/WPA2BydGPWLAN | AP | 163 | 802.11a/n | Encrypted | Nov. 18 2019 22:18:42 | | | |
| Reports V | rogue | Jim_R600_2005 | RuckusAP | 94:bf:c4:14:f1:fc | Hotspot/WPA2BydGPWLAN | AP | 38 | 802.11ain | Encrypted | Nov. 18 2019 22:17:42 | | | |
| AP | 1-1 of 1 shown | H510-Unleashed-build180 | | 18:4b:0d:1e:13:99 | UMMAutoTL1_R500_hotspot_cha | AP | 11 | 802.11g/n | Open | Nov. 18 2019 22:27:44 | | | |
| WLAN | | H510-Unleashed-build180 | RuckusAP | 0c:f4:d5:13:34:fc | iot-802.1x | AP | 38 | 802.11a/n | Encrypted | Nov. 18 2019 22:29:24 | | | |
| WLAN | | H510-Unleashed-build180 | | 54:ec:2188:c4:ec | UMMAutoTL1_R500_802_cha | AP | 153 | 802.11ain | Encrypted | Nov. 18 2019 22:28:30 | | | |
| Client | | H510-Unleashed-build180 | | 94:bf:c4:54:10:b7 | Recover.Me-14F0B0 | AP | 38 | 802.11a/n | Encrypted | Nov. 18 2019 22:24:08 | | | |
| | | Ruckus-Unleashed-Kenneth | RuckusAP | 58:68:33:36:fb:6c | sysbasic-open-none | AP | 153 | 802.11ain | Open | Nov. 18 2019 22:23:51 | | | |
| Rogue | | Ruckus-Unleashed-Kenneth | RuckusAP | 58:b8:33:3b fb bo | sysbasic-open-none | AP | 153 | 802.11a/n | Open | Nov. 18 2019 22:22:27 | | | |

3. Configure the report settings as described in Configuring Report Options on page 65.

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

2. Click any of the sub menu.

The Saved Reports reports is appeared in the middle pane.

FIGURE 39 Saved Report Page

| | ed Multi-Site Manager | | | | | | 2019/11/20 20:14:26 344 alarms | admin@ruckus.com |
|----------------------|-----------------------|-------------------|-------------------------------------|--------------------------|-------------------|-------------------|--------------------------------|------------------|
| K Dashboard | Rogue | | | | | | Group: All Devices | Export - Edit |
| Devices | | | 4 | | | rogue | ł | |
| Tasks | New Report | | | Top 1000 Rogues Next 10 | 000 Rogues | | Search | Q C 0 |
| | _ | | | Detecting Network Name | Detecting AP Name | Rogue AP BSSID | SSID | Туре |
| Unleashed-Zero Touch | Saved Reports | | | Jim_R600_2005 | RuckusAP | d8:38:fc:2a:72:ac | HotspotWPA2BydGPWLAN | AP |
| Reports 🗸 | Edit Delete | Search | Q 2 🕈 | Jim_R600_2005 | RuckusAP | 58:b6:33:3b:fb:bc | HotspotWPA2BydGPWLAN | AP |
| | e CSV FTP | Email | Created Time | Jim_R600_2005 | RuckusAP | 94:bf:c4:14:f1:fc | HotspotWPA2BydGPWLAN | AP |
| АР | 1 | freddy@freddy.com | Jul. 26 2019 07 <mark>:56:01</mark> | H510-Unleashed-build180 | | 18:4b:0d:1e:13:99 | UMMAutoTL1_R500_hotspot_cha | AP |
| | | | | H510-Unleashed-build180 | RuckusAP | 0c:f4:d5:13:34:fc | iot-802.1x | AP |
| WLAN | | | 1-1 of 1 shown 4 1 2 | H510-Unleashed-build180 | | 54:ec:2f:88:c4:ec | UMMAutoTL1_R500_802_cha | AP |
| Client | Generated Reports | Search | Q 2 0 | H510-Unleashed-build180 | | 94:bf:c4:54:f0:b7 | Recover.Me-14F0B0 | AP |
| | | | | Ruckus-Unleashed-Kenneth | RuckusAP | 58:b6:33:3b:fb:bc | sysbasic-open-none | AP |
| Rogue | File Name | PDF File | CSV File | Ruckus-Unleashed-Kenneth | RuckusAP | 58:b6:33:3b:fb:bc | sysbasic-open-none | AP |
| Administration | rogue-2019112022 | | 769.22KB | Jim_Unleashed_R510_ICX | R510 | 94:bf:c4:14:f1:fc | wl_default_0920 | AP |
| | rogue-2019112021 | | 766.23KB |] | | | | |
| System 🕨 | rogue-2019112020 | | 763.46KB | | | | 1-10 of 1000 shown | 1 2 3 4 5 » |
| | rogue-2019112019 | | 756.48KB | | | | | |

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.
- 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 65.

Performing Administrative Tasks

| • | The Administer Tab | 75 |
|---|--|------|
| | Viewing Audit Logs | |
| | Managing Software Licenses | |
| | Managing User Accounts | |
| | Managing SSL Certificates | |
| • | Upgrading the Software | . 90 |
| • | Backing Up and Restoring the Database from the Web Interface | . 92 |
| • | Generating Support Information | . 96 |
| • | Manually Transferring Files | . 98 |

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 log is shown as per time sequence.

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 12 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 failed to log in | User failed to 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. |

Viewing Audit Logs

TABLE 12 Audit Log Entries (continued)

| ser account updatedAdministrator updated a user account.ser account deletedAdministrator deleted a user account.evice log file retrievedUser retrieved an AP's log file from the Device View.evice log file emailedUser sent out an AP's log file via email.evice ping test performedUser performed a PING test from the Device View.LAN settings updatedUser updated the AP's VLAN settings from the Device View.udit log emailedUser sent out software's audit log via email.cense file verificationThe 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.evice registeredA device registered with the software.wentory file importedUser uploaded new firmware image files.onfiguration template created or updatedUser created or updated the device group.evice group created or updatedUser created or updated the device group.evice tag created or updatedUser created or updated he device group.evice tag created or updatedUser created or updated a tag name.ask canceledA user-created task has been canceled. |
|--|
| evice log file retrievedUser retrieved an AP's log file from the Device View.evice log file emailedUser sent out an AP's log file via email.evice ping test performedUser performed a PING test from the Device View.LAN settings updatedUser updated the AP's VLAN settings from the Device View.udit log emailedUser sent out software's audit log via email.cense file verificationThe 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.evice registeredA device registered with the software.ventory file importedUser uploaded new license file.onfiguration template created or updatedUser created or updated the configuration template.evice group created or updatedUser created or updated the device group.user created or updatedUser created or updated a tag name. |
| unitUser sent out an AP's log file via email.evice ping test performedUser performed a PING test from the Device View.LAN settings updatedUser updated the AP's VLAN settings from the Device View.udit log emailedUser sent out software's audit log via email.cense file verificationThe 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.cense file uploadedUser uploaded a new license file into the software.evice registeredA device registered with the software.wentory file importedUser uploaded new firmware image files.onfiguration template created or updatedUser created or updated the device group.evice group created or updatedUser created or updated the device group.evice tag created or updatedUser created or updated a tag name. |
| ProcessionUser performed a PING test from the Device View.LAN settings updatedUser updated the AP's VLAN settings from the Device View.udit log emailedUser sent out software's audit log via email.cense file verificationThe 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.cense file uploadedUser uploaded a new license file into the software.evice registeredA device registered with the software.wentory file importedUser uploaded new firmware image files.onfiguration template created or updatedUser created or updated the device group.evice tag created or updatedUser created or updated the device group. |
| LAN settings updatedUser updated the AP's VLAN settings from the Device View.udit log emailedUser sent out software's audit log via email.cense file verificationThe 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.cense file uploadedUser uploaded a new license file into the software.evice registeredA device registered with the software.eventory file importedUser imported an inventory file (XLS) into the software.onfiguration template created or updatedUser edited the configuration template.evice group created or updatedUser created or updated the device group.evice tag created or updatedUser created or updated a tag name. |
| udit log emailedUser sent out software's audit log via email.cense file verificationThe 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.cense file uploadedUser uploaded a new license file into the software.evice registeredA device registered with the software.eventory file importedUser imported an inventory file (XLS) into the software.rmware file importedUser uploaded new firmware image files.onfiguration template created or updatedUser created or updated the device group.evice tag created or updatedUser created or updated a tag name. |
| Cense file verificationThe 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.cense file uploadedUser uploaded a new license file into the software.evice registeredA device registered with the software.eventory file importedUser imported an inventory file (XLS) into the software.onfiguration template created or updatedUser edited the configuration template.evice group created or updatedUser created or updated the device group.evice tag created or updatedUser created or updated a tag name. |
| additional devices, contact your Ruckus Sales representative and obtain a license for additional devices.cense file uploadedUser uploaded a new license file into the software.evice registeredA device registered with the software.eventory file importedUser imported an inventory file (XLS) into the software.immware file importedUser uploaded new firmware image files.onfiguration template created or updatedUser edited the configuration template.evice group created or updatedUser created or updated the device group.evice tag created or updatedUser created or updated a tag name. |
| evice registeredA device registered with the software.evice registeredUser imported an inventory file (XLS) into the software.immware file importedUser uploaded new firmware image files.onfiguration template created or updatedUser edited the configuration template.evice group created or updatedUser created or updated the device group.evice tag created or updatedUser created or updated a tag name. |
| wentory file importedUser imported an inventory file (XLS) into the software.imware file importedUser uploaded new firmware image files.onfiguration template created or updatedUser edited the configuration template.evice group created or updatedUser created or updated the device group.evice tag created or updatedUser created or updated a tag name. |
| irmware file importedUser uploaded new firmware image files.onfiguration template created or updatedUser edited the configuration template.evice group created or updatedUser created or updated the device group.evice tag created or updatedUser created or updated a tag name. |
| onfiguration template created or updated User edited the configuration template. evice group created or updated User created or updated the device group. evice tag created or updated User created or updated a tag name. |
| evice group created or updated User created or updated the device group. evice tag created or updated User created or updated a tag name. |
| evice tag created or updated User created or updated a tag name. |
| |
| A user-created task has been canceled. |
| |
| pproval mode updated User updated the AP approval mode on the Inventory page |
| ew event occurred User created a new event. |
| uto configuration rule created User created a new auto-configuration rule. |
| ontroller configuration obtained User performed "obtain Controller configuration" from a controller device. |
| SL certificate uploaded User uploaded an SSL certificate to the software. |
| ventory status created User created an inventory status. |
| ventory status modified User updated an inventory status. |
| ventory status assigned User changed a n AP's inventory status. |
| ventory comment assigned User edited an AP's comment on the Inventory page. |
| ventory status deleted User deleted an inventory status. |
| ontroller configuration cloned User created a "Clone Controller" task. |
| evice authenticated UMM authenticates the device successfully. |
| Ianaged group created User created a group for delegated management. |
| Ianaged group updated User updated a group for delegated management. |
| Ianaged group deleted User deleted a group for delegated management. |
| Ianaged group device(s) addedUser assigned devices to a managed group. |
| Ianaged group device(s) removed User removed devices from a managed group. |
| ser group mapping updated User changed the "user account" and "managed group" mapping. |
| ser logged in via the Northbound interface A 3rd party system logged into the software via the Northbound interface. |
| ser logged out via the Northbound interface A 3rd party system logged out of the software via the Northbound interface. |
| orthbound interface operation invoked A 3rd party system invoked the Northbound interface. |
| pgrade script started User installed a patch on the software server. |
| pgrade successful User patched the software successfully. |
| pgrade failed User patch for the software failed. |
| oneDirector could not be reached The software could not reach a managed ZoneDirector. |

TABLE 12 Audit Log Entries (continued)

| Audit Type | Description |
|---------------------------------------|---|
| Task deleted | User deleted a task. |
| Task restarted | User restarted a failed task. |
| Automatic report created or updated | User created an automatic report. |
| Automatic report emailed success | Automatic report is emailed successfully. |
| Automatic report emailed failed | Automatic report email is failed. |
| System log emailed | System log is emailed. |
| Connectivity of devices emailed | Connectivity of devices is emailed. |
| Connect to Controller fail | The software not able to connect to controller. |
| A new Controller template created | User creates a new controller template. |
| A Controller template updated | User updates a controller template. |
| A Controller template deleted | User deletes a controller template. |
| Automatic report ftp uploaded success | Saved report is successfully uploaded to FTP server. |
| Automatic report ftp uploaded failed | Saved report fails to upload to the FTP server. |
| Automatic report local file saved | User saves Automatic report local file. |
| Alarm notification emailed | UMM has send out the alarm via email. |
| Backup database | Backup the database by the User. |
| Restore database | Restore the database by the User. |
| Purge job failed | Purge job is failed. |
| License delete | User can delete a license. |
| Group create | User can create a group. |
| Group modify | User can modify a group. |
| Group delete | User can delete a group. |
| Device settings modify | User can modify the device settings. |
| Device delete | User can delete a device. |
| Device edit WLAN | User can edit the controller's WLAN. |
| Device block | User can block the device. |
| Device unblock | User can unblock the device. |
| Device backup | User can backup the device. |
| Device restore | User can restore the device. |
| Device upgrade | User can upgrade the device. |
| Rule create | User can create a rule. |
| Rule update | User can update a rule. |
| Rule delete | User can delete a rule. |
| Rule import | User can import a rule. |
| Zero touch backup file upload | Zero Touch Deployment Unleashed configuration file is uploaded to UMM. |
| Zero touch backup file delete | Zero Touch Deployment Unleashed configuration file is deleted from UMM. |
| Report create | User can create a report. |
| Report update | User can update a report. |
| Report delete | User can delete a report. |
| Report generate | User can generate a report. |
| Cert update | User can update a certificate. |

Viewing Audit Logs

TABLE 12 Audit Log Entries (continued)

| Audit Type | Description |
|--|---|
| Cert import | User can import a report. |
| Cert Restore | User can restore a report. |
| Device Registration | User can register a device. |
| Maps Settings | Map setting is changed. |
| Device Backup | User can backup a device. |
| Memory Optimization Settings | Memory Optimization Settings is changed. |
| UE Session Settings | UE Session Settings is changed. |
| Security Code | Security code is reset. |
| Logo Settings | Logo Settings is changed. |
| SMTP Settings | SMTP Settings is changed. |
| Purge policy | Purge policy is changed. |
| Tacacs+ Settings | Tacacs+ Settings is changed. |
| FTP Settings | FTP Settings is changed. |
| SNMP V2 Settings | SNMP V2 Settings is changed. |
| SNMP V3 Settings | SNMP V3 Settings is changed. |
| SNMP Trap Enable Settings | SNMP Trap Enable Settings is changed. |
| SNMP Trap Settings | SNMP Trap Settings is changed. |
| Events & Alarms selection | Alarm Event selection settings is changed. |
| Flexera server setting | UMM licenses is changed via Flexera server. |
| Download system full logs | System full logs are downloaded. |
| Alarm Light Setting | Alarm Light Setting is changed. |
| Alarm Email Notification | Alarm Email Notification is changed. |
| User Customized Alarm | User Customized Alarm is changed. |
| Alarm Event Selection | Alarm Event Selection is changed. |
| Alarm Acknowledge | User acknowledges the alarm. |
| Event configuration create | User can create an event configuration. |
| Event configuration update | User can update an event configuration. |
| Event configuration delete | User can delete an event configuration. |
| Event configuration assign controllers | ZD is assigned to an Event configuration group. |
| Task create | User can create a task. |
| Task update | User can update a task. |
| Task delete | User can delete a task. |
| Download backup file | User can download a backup file. |
| Saved backup file | User can save a backup file. |
| Backup file ftp uploaded success | User successfully uploaded a backup file ftp into the software. |
| Backup file ftp uploaded failed | User failed to upload a backup file ftp into the software. |
| User create | User can be created. |
| User update | User can be updated. |
| User delete | User can be deleted. |
| Device redirect | User is redirected from UMM to devices. |
| Add indoor map | Indoor map is added. |

TABLE 12 Audit Log Entries (continued)

| Audit Type | Description |
|-----------------------------|--|
| Update indoor map | Indoor map is updated. |
| Delete indoor map | Indoor map is deleted. |
| Switch firmware upload | User can upload a switch firmware. |
| Switch firmware delete | User can delete a switch firmware. |
| Database backup file delete | User can delete a database backup file. |
| 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. |
| Notify third-party Settings | User Update Notify third-party Configuration |

Managing Software Licenses

The number of RUCKUS AP devices and ICX switches 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, the additional devices will be set to 'license exceed status' and Unleashed Multi-Site Manager will stop monitoring or managing them. Refer to the Administer > License page to see how many APs and switches 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 three types of software licenses file- one for ZD and P300, one for Unleashed, and one for ICX. 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.

Unleashed Multi-Site Manager will not delete the device when license expires. It just changes the status of the device which does not have enough license to *license exceed* and stops monitoring and managing them.

ICX licenses consume software license according to the number of switch units.

To enable Unleashed Multi-Site Manager to manage additional APs or switches, 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.

Performing Administrative Tasks

Managing Software Licenses

FIGURE 40 License Page

| | shed Multi-Site Manager | | | | A Your U | MM system has insufficient licenses. | 2019/12/03 17:5 | A 9:18 100 alarms | admin@ruckus.o | com Help |
|----------------------|--|--|--------------|-----------------------|---|--------------------------------------|--|------------------------------------|----------------|-----------|
| K Dashboard | License | | | | | | | | | |
| Devices | | | | | | | | | C Flexera | a License |
| Tasks | UMM ID: | | | | | | | | | v |
| Unleashed-Zero Touch | Total ZD/Bridge AP Licen Total Unleashed Licenses | ises purchased: 100000000 s Purchased: 100001 | | | umed by ZD/Bridge AP: 1720 umed by Unleashed: 58 | | Remaining ZD/Bridge AP Licenses: 99998280 Remaining Unleashed Licenses: 99943 | | | |
| Reports 🕨 | Total Switch Licenses Pu | rchased: 2033 | | Licenses Consi | umed by Switch: 15 | | Remaining Switch Licenses: 2018 | | | |
| Administration 🗸 | Upload License Delete | | | | | | | Search | ٩ | 2 ¢ |
| Audit Log | License Key | Part Number | AP/ICX Count | Create Time | License Type | Expire Date | | | | |
| License | 1495761484000 | FME-1 | 1 | May. 26 2017 06:48:04 | Unleashed-Official | N/A | | | | |
| License | 1270080959000 | ruckuswireless | 10000000 | Apr. 01 2010 05:45:59 | ZD-Official | N/A | | | | |
| Switch Firmware | 1560904102000 | unleashed10kofficial | 100000 | Jun. 19 2019 05:58:22 | Unleashed-Official | N/A | | | | |
| | 1536278079000 | ICX2kofficial | 2000 | Sep. 07 2018 05:24:39 | Switch-Official | N/A | | | | |
| Users & Assignment | 1575312492000 | 3ICX30days | 30 | Dec. 03 2019 00:18:12 | Switch-Trial | 2020-01-02 10:50:21 | | | | |
| SSL Certificates | 1575312619000 | UMM_3ICX30days | 3 | Dec. 03 2019 00:20:19 | Switch-Trial | 2020-01-02 10:52:11 | | | | |
| DB Backup / Restore | | | | | | | | 1-6 | 6 of 6 shown 4 | 1 > |

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

Click **Delete** to remove the expired temporary licenses.

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.

Deleting the Expired Temporary License

You can delete your expired temporary software license.

- 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. Select the license file, and then click **Delete**.

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 41 Users & Assignment Page

| RUCKUS" | hed Muti-Site Manager | | Your UMM system has insufficient licenses. | O ▲ ▲ Ø 202001/02 00:51:40 GTEXTITIES admin@ruckus.com Help |
|------------------------------------|-------------------------|-----------------------|--|--|
| C Dashboard | Users & Assignment | | | |
| Devices | Create Edit Delete | | | Search Q. 2 • |
| | User Name | Last Login | User Role | |
| Tasks | admin@ruckus.com | Jan. 02 2020 00:18:35 | Network Administrator | |
| Unleashed-Zero Touch | freddy | | Network Administrator | |
| | fga | Dec. 31 2019 09:12:07 | Group Administrator | |
| Reports 🕨 | fro | Dec. 31 2019 09:12:21 | Read Only | |
| Administration 🚽 | ro | Dec. 31 2019 14:38:17 | Read Only | |
| Audit Log | Groups assigned to fro- | | | 1-ő of ð shown 🤟 🕴 🕨 |
| License | | | | Search Q 2 0 |
| Switch Firmware | Device Group Name | | | |
| | freddt | | | |
| Users & Assignment | unleashed | | | |
| SSL Certificates | 1720 | | | |
| | 7460 | | | |
| DB Backup / Restore | jm_un | | | |
| Support | jim_2d 7160 | | | |
| | | | | |
| System 🕨 | fed 7710 | | | |
| System Info Version: 2.3.0.0.32 | 2 | | | 1-10 of 11 shown 🔍 🚺 2 🔹 |
| | | | | |

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
- Read Only

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).

Performing Administrative Tasks

Managing User Accounts

A Network Administrator can perform the following tasks:

- Manage all devices in the Inventory.
- Create user accounts for a Group Administrators and Read Only.
- Assign devices to device management groups. These device groups can be assigned to create user accounts for a Group Administrators and Read Only.

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

Read Only Role

The Read Only role only grants the privilege to view assigned devices.

Users with the Read Only privilege will have a limited view of the web interface features. In this release of the software, only the Dashboard, Device and Report menus are visible. Also, only device groups assigned to the user are visible under the **Devices** menu. There are no write privileges given in this role. Read Only users can use the hyperlinks to ZD and 200.7 MR Unleashed networks. For versions of Unleased prior to 200.7, the hyperlinks are disable for Read Only users.

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 42 Creating a User Account

| RUCKUS | | Create User | Your UMM system has insufficient licenses. | O A 2020/01/02 08:58:38 (222000) sdmin@ruckus.com Help |
|--|------------------------|---|--|--|
| Dashboard | | User Name: | | |
| Devices | Create Edit Delete | Password: | | Search Q D O |
| | User Name | Confirm Password: User Role: Group Administrator | User Role | |
| Tasks | admin@ruckus.com | | Network Administrator | |
| Unleashed-Zero Touch | | Assign Groups: Device Groups | Network Administrator | |
| | | 7150 | Group Administrator | |
| Reports ► | | i fed | | |
| Administration 🚽 | | 💌 🖂 fredst | Read Only | |
| Reports Administration Audit Log License Switch Pirmware | Groups assigned to fpa | unteached | | 1-8 of 8 shown 🔹 💶 - |
| License | | ijm ▼ ijm_un | | Search Q C O |
| Switch Elementer | Device Group Name | | | |
| Contract Contraction | | 3] jm_zd | | |
| Users & Assignment | | You should choose at least one group | | |
| SSL Certificates | | | | |
| SSL Certificates DB Backup / Restore | | OK Casel | | |
| DB Backup / Restore | | | | |
| Support | | | | |
| | | | | |
| System 🕨 | | | | |
| | | | | |
| System Info Version: 2.3.0.0.32 | | | | |
| 983 5001. 23.0.036 | | | | 1-10 of 12 shown < 1 2 > |
| | | | | |
| | | | | |

- 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 and Read Only**.

For more information on user roles, refer to User Roles and Privileges on page 81.

7. In Device Groups, select the desired device group to the user.

NOTE

The select device group is only available for Group Adminitrator and Read Only user roles.

8. 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 43 Editing a User Account |
|----------------------------------|
|----------------------------------|

| | | Edit User | | × | 2 019/12/30 15:03:55 | A 305 alarms | admin@ruck | | () Help |
|-------------------------|-------------------------------|--------------------------------|---|--------|-----------------------------|-----------------|------------|------------|------------|
| | Users & Assign | User Name: | ga | | | | | | |
| Devices | Create Edit Delete | Password: Confirm Password: | | | | | C | 2 2 | \$ |
| Tasks | User Name admin@ruckus.com | | Group Administrator | | r Role | | | | |
| Unleashed-Zero Touch | freddy | Assign Groups: | Device Groups | | vork Administrator | | | | |
| Reports 🕨 | | | ✓ freddy ✓ unleashed | | | | | | |
| Administration v | | | ✓ r710 ✓ r720 | | | 1-4 | of 4 shown | « 1 | * |
| Audit Log | Groups assigned to ga | | ▼ □ jim_un ▼ □ 1 | | | | Q | 0 0 | |
| License | Device Group Name | | ▼ □ 2 □ 3 | | | | | | |
| Switch Firmware | | | jim_zd | | | | | | |
| Users & Assignment | | | ок | Cancel | | | | | |
| CCI Cartificatos | | | | | | | | | |

- 3. Edit the following options as required:
 - User Name
 - Password
 - Confirm Password
 - Assign Groups
- 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.

Upgrading Switch Firmware

You can upload the switch configuration file to upgrade a switch version.

Go to Administration > Switch Firmware

The **Switch Firmware** page appears. You can drop the file within the grey box provided. After the upgrade is completed the details of the upgrade are displayed below such as the firmware version and models supported.

FIGURE 44 Upgrading the switch firmware version

| ~ | Switch Firmw | are | |
|--------------------|----------------------------|--|---|
| Dashboard | 0 11 10 11 11 11 11 | | |
| Devices | Upload the firmware(*.zip) | used for upgrading the Switch(es) | |
| Tasks | Drop fi | le here or click to upload file | |
| Reports 🕨 🕨 | | | |
| Administration 🗸 🗸 | | | |
| Audit Log | Firmware Version | Models Supported | |
| | F108080 | ICX7250, ICX7650, ICX7750, ICX7150, ICX7450 | |
| License | FI08090 | ICX7250, ICX7850, ICX7650, ICX7750, ICX7150, ICX7450 | D |
| | F108080ca | ICX7250, ICX7650, ICX7750, ICX7150, ICX7450 | |
| Switch Firmware | | | |
| Users & Assignment | | | |

Managing SSL Certificates

When you use HTTPS to connect to 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

When you upload a new certificate to Unleashed Multi-Site Manager, ensure that the root certificate is trusted by the ZD and Unleashed, else, it will break the connection between Unleashed Multi-Site Manager and ZD/Unleashed

This section describes how to generate a certificate request file to obtain an SSL certificate and how to import a SSL certificate into the software.

Importing an SSL Certificate

When you already have an SSL certificate, 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. Go to Administration > SSL Certificates.

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

FIGURE 45 Importing an SSL Certificate

| M Dashboard | SSL Certificates |
|--------------------|--|
| Devices | View Certificates Create a New Request Import a Certificate |
| Tasks | Warning: Incorrect certificate will cause connection error of ZD/Unleashed/Switch to UMM |
| Reports ► | Server Certificate: Drop file here or click to upload file |
| Administration V | |
| | ? Intermediate CA Certificate: |
| Audit Log | Drop file here or click to upload file |
| License | Driveta Karr |
| Switch Firmware | Private Key: Drop file here or click to upload file |
| Users & Assignment | Key Passphrase: |
| SSL Certificates | Import Restore |

- 3. In **Server Certificate**, drop the file to the box provided or click the box to upload the certificate file.
- 4. In Intermediate CA Certificate, drop the file to the box provided or click the box to upload the Intermediate CA certificate file.
- 5. In **Private Key**, drop the file to the box provided or click the box to upload the private key.
- 6. Click Import.

A message appears, informing you that the certificate has been imported successfully. If you want to restore to the default certificate and private key, click **Restore**.

7. Click the View Certificates tab.

For more information, refer to Viewing Current Certificates on page 90.

Try connecting to the software Web interface using HTTPS.

Creating a Certificate Signing Request File

When you do not have a certificate, you need to create a certificate signing request (CSR) file and send it to a SSL Certificate provider to purchase an SSL certificate. 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 Request tab.

FIGURE 46 Creating the Certificate Signing Request

| « | SSL Certific | anton | |
|--------------------|---------------------------------------|--------------------------|--|
| Dashboard | SSL Certific | Jales | |
| Devices | View Certificates | Create a New Request | Import a Certificate |
| Tasks | The following charact Common Name: | ers are not allowed: < > | ~!@#\$%^*/()?\ The Common Name. |
| | Organization: | | The complete legal name of your organization (for example, Ruckus Wireless, Inc.). Do not abbreviate. |
| Reports < | Organization Unit: | | The department in your organization that manages network security (for example, Network Management). |
| | Locality or City: | | The city where your organization is legally located (for example, Sunnyvale). |
| Administration 🗸 🗸 | State/Province: | | The state or province where your organization is legally located (for example, California). Do not abbreviate. |
| | Country: | admin@ruckus.com | The two-letter ISO abbreviation for your country (for example, if your organization is located in the United States, type US). |
| Audit Log | Key pair password: | | The password must be at least six characters long. |
| Audit Log | Confirm password: | | |
| License | Key Size: | | SSL key length |
| Switch Firmware | | | |
| Users & Assignment | | | |
| SSL Certificates | | | |

- 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 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 47 The Default SSL Certificate on the Software

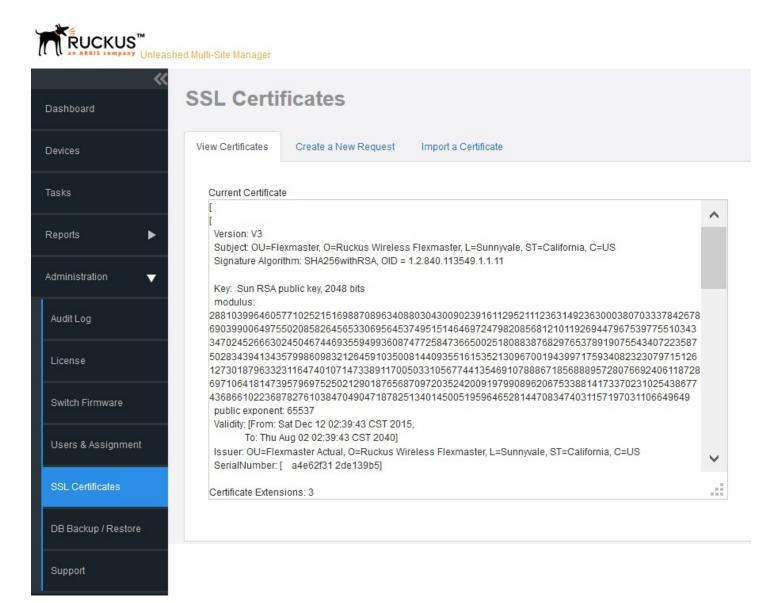
| vices | View Certificates | Create a New Request | Import a Certificate | | | |
|-------------------|----------------------------------|----------------------|---|---|------------|----------|
| sks | New Certificate I Subject DN: | Information | | | | |
| ports 🕨 | Issuer DN: | | 44 | [| Remove Cer | tificate |
| ninistration 🗸 | | | then paste it into a text editor (for example, l lac) To paste: (CTRL + V on PC, Command + V | | | |
| dit Log | | | | | | |
| ense | | | | | | |
| tch Firmware | | | | | | |
| rs & Assignment | | | | | | |
| . Certificates | | | | | | |
| Backup / Restore | | | | | | |
| oport | | | | | | |
| em 🕨 | | | | | | |
| stem Info | | | | | | |
| rsion: 2.2.0.0.36 | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | Select All | Cano |

- 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 SSL Certificate provider website and follow the instructions for purchasing an SSL certificate.

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.

FIGURE 48 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 /home/UMM/:

cp 9.12.0.0.11.patch.tar /home/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, /home/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 92 or Backing Up the Database from the Command Line Interface on page 25 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 /home/UMM directory.

When the uninstall script completes deleting the /home/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 19.

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 (/home/UMM), where the database restore script is located.
- 2. Execute the database restore script by entering the following command:
 - # ./restore.sh

Press Enter and submit the file name. and them application begins restoring the database .

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

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.

NOTE

There are two databases running on the Unleashed Multi-Site Manager server; MariaDB and ElasticSearch. By default, Unleashed Multi-Site Manager backs up the MariaDB. You must check the **Include ES** option to backup both MariaDB and ElasticSearch.

- 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.

NOTE

There are two databases running on the Unleashed Multi-Site Manager server; MariaDB and ElasticSearch. By default, the software backs up MariaDB only. Ensure you select the **Include ES** option to backup both MariaDB and ElasticSearch.

Backing Up and Restoring the Database from the Web Interface

5. Click Back Up. The Backup Status Area window appears and displays the progress of the backup process.

FIGURE 49 Backup Status Area Window

| Dashboard | Backup / Restore |
|--------------------------------------|--|
| | |
| Devices | Database Backup |
| Tasks | Type a name for the database that you are saving. If you want Unleashed Multi-Site Manager to assign a file name automatically (in the format DB_(YYYY-mm-dd-hh)), leave this box blank. File Name: Include ES Back Up |
| Reports > | Database Restore |
| Administration | |
| Audit Log | File Name Created |
| License | No data available. |
| Users & Assignment | |
| SSL Certificates | DB Backup & Restore Logs |
| DB Backup / Restore | |
| | Description Created |
| Support | No data available. |
| System 🕨 | |
| System Info Version: 2.1.10.10.16 | Schedule Backup Task |
| | Save |

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.

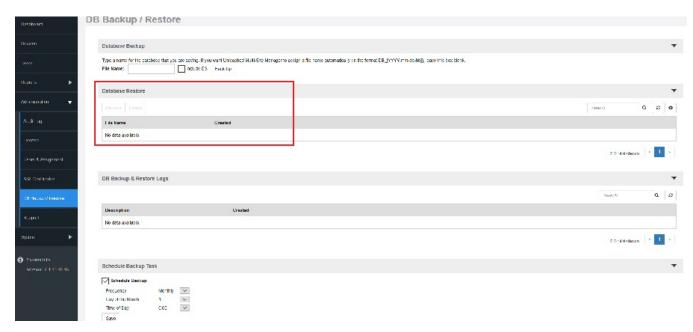
A table appears, displaying the file names of the database backup files and the dates when they were created.

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 50 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 51 Viewing a System Log File

| | Unleashed Multi-Site Manager Version: | 2.1.10.10.16 | |
|-----------------|--|----------------------------------|----------------|
| s | Original Unleashed Multi-Site Manager Installa | tion Time: Mar. 26 2018 23:00:47 | |
| | System Log: | | |
| | Dowload Full Logs | Select Log File: intune2.log 🗸 | View Log Email |
| | ERROR [Apr. 10 2018 10:45:00] | | ^ |
| s 🕨 | parse file name errors | | |
| | ERROR [Apr. 10 2018 10:45:00] | | |
| stration 🗸 🔻 | parse file name errors | | |
| | ERROR [Apr. 10 2018 10:45:00] | | |
| Log | parse file name errors | | |
| | ERROR [Apr. 10 2018 10:45:00] | | |
| se | parse file name errors | | |
| | ERROR [Apr. 10 2018 10:45:00] | | |
| & Assignment | parse file name errors | | |
| | ERROR [Apr. 10 2018 10:45:00] | | |
| Certificates | parse file name errors | | |
| | ERROR [Apr. 10 2018 10:45:00] | | |
| ackup / Restore | parse file name errors | | |
| | ERROR [Apr. 10 2018 10:45:00] | | |
| ort | parse file name errors | | |
| | ERROR [Apr. 10 2018 10:45:00] | | |
| 1 Þ | parse file name errors | | ~ |

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.
- 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 101.

3. Type any information you want to highlight in the message box.

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

FIGURE 52 Sending the System Log in Email

| Dashboard | Support |
|---------------------|---|
| Devices | Unleashed Multi-Site Manager Version:2.1.10.10.16Original Unleashed Multi-Site Manager Installation Time:Mar. 26 2018 23:00:47System Log: |
| Tasks | (EMAIL) |
| Reports > | To: Subject: System Log Report Attached: Dintune2.log InventoryList.html |
| Administration | Unleashed Multi-Site Manager Version: 2.1.10.10.16 |
| Audit Log | Enter your message here: |
| License | |
| Users & Assignment | |
| SSL Certificates | |
| DB Backup / Restore | Send Cancel |
| Support | |
| | Email: support@ruckuswireless.com Support: https://support.ruckuswireless.com |

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:

- /home/UMM/<version number>.patch.log
- the log files in folder /home/UMM/logs

After you have transferred the files, you can use them as directed by Ruckus Support.

System

| • | Configuring System Settings | 101 |
|---|-----------------------------|-----|
| • | Alarm Settings | 114 |
| • | Monitoring Events | 117 |

Configuring System Settings

Beginning with UMM 2.6 release, the read only user will get an option to edit the Unleashed WLAN name and password when they enable the RO User Permission Settings.

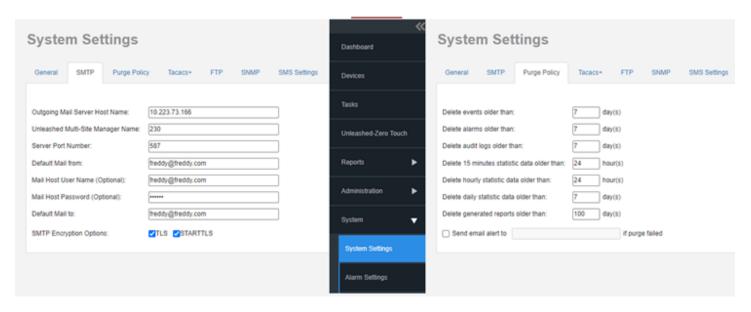
The System Settings option allows you to specify an SMTP server.

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 53 System Settings Page (part 1 of 5)

| System Settings | |
|--|-------------|
| General SMTP Purge Policy Tacacs+ FTP SNMP SMS Settings | |
| - Device Registration | |
| Z Automatically approve all devices | Save |
| Maps Settings | |
| Google Maps | |
| Enter Google Maps API key Accelute Acce | |
| Bing Maps Do Not Need Maps | Save |
| Device Backup | |
| Max number of backup files for each device: 10 Tips:Set reasonable number according to total Device number for disk consumption reason. | Save |
| UE Session Settings | |
| Enable UE Session Service: 👻 Yes 🔗 No Waring: Enabling User Equipment session can provide increased accuracy of client traffic reports, but may overload the Unleashed Mut5-Site Manager database in cases where Unleashed Mut5-Site Manager is managing a very large number of Devices. | Save |
| RO User Permission Settings | |
| Update WLAN password | |
| | Save |
| Logo Settings | |
| Uplead Lopo Choose File No file chosen | |
| Image should be smaller than 50KB. Suggested width/height is 150/70 | Save Cancel |

FIGURE 54 System Settings Page (part 2 of 5)



NOTE

Lite mode does not support configure purge policy for the statistic data.

FIGURE 55 System Settings Page (part 3 of 5)

| System Settings System | tem Settings |
|--|--|
| General SMTP Purge Policy Tacacs+ FTP SNMP SMS Settings General | ral SMTP PurgePolicy Tacacs+ FTP SNMP SMS Settings |
| Port: 49 Com Service Name: fm-login fmed Secret: **** gm gm Confirmed Secret: **** Date Authentication Method: Local first them TACACS v | V Read V Trap × |
| | MP V3 Settings er Name Auth Protocol Auth Password Priv Protocol Priv Password Privilege |
| | MP Trap Enable Settings- uole SNMP Trap: Yes No Save |
| FTP User Password: | MP Trap MP Version Security Name Target Address Target Port + t v) [heddy v) [10.223.73.166 [162] |
| | Save |
| Even | ents & Alarms selection(Select miscellaneous event to be wrapped in generic trap.) |

FIGURE 56 System Settings Page (part 4 of 5)

Beginning with UMM 2.6 release, the system settings option allows you to enable SMS server. There are three methods to enable SMS server: Twilio account information, Clickatell account information and Customized server.

| System Settings | |
|---|-------------------------------------|
| General SMTP Purge Policy Tacacs+ FTP SNMP | SMS Settings |
| Enable SMS Server Twilio account information | |
| Account SID | [Register a new Twilio account] |
| Auth Token | |
| From PhoneNumber | |
| Clickatell account information | |
| User Name | [Register a new Clickatell account] |
| Password | |
| APLID | |
| From PhoneNumber | |
| Customized Server | |
| Method | GET V |
| URL | |

FIGURE 57 System Settings Page (part 5 of 5)



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.

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

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.

RO User Permission Settings

The ReadOnly account users can edit the Unleashed WLAN name and password when they enable the RO User Permission Settings.

Security Code

Through Public APIs, third-party software can integrate with Unleashed Multi-Site Manager managed devices, and access all the data from these devices.

The security code is a token that you can use to communicate with the software application. This feature allows for enhanced security while attempting to access the software. The code is system generated and can be reset only by a super administrator as the Security Code is only visible to the supper user (admin@domianname).

Unleashed Multi-Site Manager provides APIs to:

- List customer created groups
- List Unleashed/ZD/P300 devices
- List detail of one device for Unleashed/ZD/P300
- List APs/clients/WLANs
- List events/alarms

- List ICX data
- Edit SSID/PSK for selected WLAN
- Enable/Disable for selected WLAN

In the **Security Code** area, you can configure the application to send a HTTPS Post message with the AP's model/MAC/Unleashed ID/ZD SN whenever a new AP join the UMM. The third-party URL must be provided in the URL field. Click **Test** to trigger a test message to the URL.

To view the security code or edit the code if you are a super admin, go to **System > System Settings > General tab** Click **Test** to trigger a test message to the URL.

FIGURE 58 Security Code

| System Settings |
|--|
| Seneral SMTP Purge Polo; Tacass+ FTP SHMP |
| Device Registration |
| Maps Solitings |
| Groupit Majas |
| Enter Coogle Mars All Key Agoly in Coogle Mars All Key |
| C Hind Maps |
| C Do Not Need Maps |
| Levce Bockup |
| Max number of hedsup flor, for each divide: 10 Tipe Set reasonable number according to total Device number for dick consumption reason |
| UL Session Settings |
| Linkle ULLEssion Service: (a) Yes () No () Yes () No () Yes () Ye |
| Security Code |
| Lisefs security code for public AFI1 |
| 7ab27d71130a4ed1a3f06056883d0eda 📳 |
| Click here to show the public API document |
| Wanno, It changed the security code, the clid security code will be lose efficacy |
| Notify Subparty system when new AP-joins UMM. |
| Retinction URL https:// |
| |
| Logo setungs |
| Urbad Lese: Concept Pill Nu Rie dance |
| Londota Fila) va B.o. dotom Imago shaku tek sender han Selik. Ruggotada ulatminolgiti iz 16070 |
| ency and a second s |

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 59 SMTP Settings

| M Dashboard | « System Settings | | | | | | |
|---------------------|---|--|--|--|--|--|--|
| Devices | General SMTP Purge Policy Tacacs+ FTP SNMP | | | | | | |
| Tasks | Outgoing Mail Server Host Name: smtp.gmail.com | | | | | | |
| Reports ► | Unleashed Multi-Site Manager Name: UMMSystem Server Port Number: 587 | | | | | | |
| Administration | Default Mail from: arrisruckus2@gmail.com Mail Host User Name (Optional): arrisruckus2 | | | | | | |
| System 🔻 | Mail Host Password (Optional): Default Mail to: arrisruckus@gmail.com | | | | | | |
| System Settings | SMTP Encryption Options: | | | | | | |
| Alarm Settings | | | | | | | |
| Event Configuration | | | | | | | |

- 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 60 Purge Policy Settings

| Dashboard | System Settings | | | | | | |
|---------------------|--|----------|---------------------------|------|--|--|--|
| Devices | General SMTP | Tacacs- | + FTP | SNMP | | | |
| Tasks | Delete events older than: | 15 | day(s) | | | | |
| Reports > | Delete alarms older than Delete audit logs older th | 15 30 | day(s) day(s) | | | | |
| Administration | Delete 15 minutes statist Delete hourly statistic dat | 24 24 | hour(s) hour(s) | | | | |
| System 🗸 | Delete daily statistic data | 7 | day(s) | | | | |
| System Settings | Delete generated reports | 30 | day(s) if purge failed | | | | |
| Alarm Settings | | | | | | | |
| Event Configuration | | | | | | | |

- 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. ClickTacacs+ section.

FIGURE 61 TACACS+ Settings

| Dastboard | System Se | ttings | | | | | | |
|---------------------|-----------------------------|------------------------|----------|--|--|--|-------------|--------|
| Devices | General SMTP | Purge Policy Tacacs+ | FTP SNWP | | | | | |
| Tasks | Server IP: | 172.18.110.133 | | | | | | |
| Reports 🕨 | Port. Service Name: | 49 fm-login | | | | | | |
| Administration 🕨 | Secret Confirmed Secret: | | | | | | | |
| System 🔻 | Authentication Method | Local first then TACAC | | | | | Test Save 0 | lancel |
| System Settings | | | | | | | | |
| Alarm Settings | | | | | | | | |
| Event Configuration | | | | | | | | |

- 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.

System Configuring System Settings

2. Click FTP section.

FIGURE 62 Editing FTP Server Settings

| Coshiboard | System Settings |
|---------------------|---|
| Devices | General SMTP Purge Policy Tacaca+ FTP SMMP |
| Taska | FTP Host Name: 172.58.110.133 |
| Reports 🕨 | FTP Port Number: 21 FTP User Name: Institut |
| Administration | Test Save Cancel |
| System 🔻 | |
| System Settings | |
| Alarm Settings | |
| Event Configuration | |

- 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 63 SNMP Configuring Settings

| ices | General SMTP Purge Policy Tacacs+ FTP SNMP | |
|-----------------------|--|------|
| ĸs | - SNMP V2 Settings | |
| orts 🕨 | Community Name Privilege + | |
| ninistration | tesittittittit | |
| tem 🔻 | Delete All Settings | Save |
| stem Settings | SNMP V3 Settings | |
| arm Settings | User Name Auth Protocol Auth Password Priv Protocol Priv Password Priv loge kenneth MD5 v 12345678 DES v 12345678 Trap × | |
| ent Configuration | | Save |
| System Info | SNMP Trap Enable Settings | |
| /ersion: 2.1.10.10.16 | Enable SNMP Trap. O Yes 💿 No | Save |
| | SNMP Trap | |
| | SNMF Hap | |
| | | |
| | | |
| | SNMP Version Security Name Target Address Target Port + | |
| | | Save |

- 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 116 and Configuring Alarm Settings on page 115 for information about user-customized thresholdcrossing alarms.

SMS Setting

Beginning with UMM 2.6 release, the system settings option allows you to enable SMS server. There are three methods to enable SMS server: Twilio account information, Clickatell account information and Customized server.

Alarm Settings

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

FIGURE 64 Alarm Settings

| | | | Create New No | tification Ema | il Group | × | | C A | e (|
|---|----------|----------------------|---------------------|----------------|-----------------------------------|----------------------------------|---|-----|---------------|
| Alarm Settings | | | Severity Criteria (| Critical Major | Minor Warning | | | | |
| Alarm Light Setting | | | Email Address: | | esses, please separate each addre | ess by a semicolon.) | | | |
| Enable Alarm Light: Yes No | Save | | Select Oroups | | ontroller Select ICX Switch | | | | |
| Email Notification | | | Select Wire | ess Group | | | | | |
| Create Edit Debits | | | ▼ □ Wrold | | | | | | Q (2) (0) |
| Email List 5 | ieverity | | 0 | 1 | | | | | |
| Create Tot Donne Phone Number List 5 | leverity | | | 2 | | | | | Q. <i>1</i> 0 |
| | | | | | | Save Cancel | | | |
| User Customized Alarm | | | | | | | | | |
| Enable Alarm Type | Severity | Threshold | | Severity-Ext | Threshold-Ext | Description | | | |
| AP # of channel changes | Warning | exceed 1 times in la | | Major | exceed 2 times in last hour | AP[[0]]'s number of channel ch | sanges exceeded the threshold $[[1]]_{\rm c}$ | | |
| AP # of clients | Warning | exceed 1 AP client() | | Major | exceed 2 AP client(s) | AP[[0]['s concurrently connect | ed client number exceeded the threshold [[1]]. | | |
| AP # of reboot | Warning | exceed 1 times in la | | Major | exceed 2 times in last hour | AP[[0]]'s concurrently reboot to | mes exceeded the threshold $\underline{\mathbb{N}}[1]]_{i}$ | | |

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 **SMS Notification** section send SMS to their respective phone numbers when alarms are generated. Go to **Administration** > **System Settings** and click **SMS settings** to enable SMS server. There are three methods to enable SMS server: Twilio account information, Clickatell account information and Customized server.

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 *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 *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 Groups** tab, select the wireless groups 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 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**.
- 6. From the **Select ICX Switch** 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**.
- 7. From the Select Alarm Type tab, select the alarm types which you want to generate for the selected devices and click Save.
- 8. In the SMS Notification section, enter the phone numbers to which alarm notifications are sent and alarm severities.
 - To create a new sms notification group, click **Create** under the **SMS Notification** section and then:
 - In **Severity Criteria**, select the check boxes for the alarm severity that you want to send notifications for: options include *Critical*, *Major*, *Minor* and *Warning*.
 - Enter the phone numbers to send notifications using a semi-colon (;) to separate multiple phone numbers.

NOTE

You should provide the complete phone number, including the country code.

- From the **Select Groups** tab, select the wireless groups to be monitored from the list so that sms notifications are sent for the alarms generated for these devices and click **Save**.
- From the Select WLAN Controller tab, select the device to be monitored from the list so that sms notifications are sent for the alarms generated for these devices and click Save.
- From the **Select ICX Switch** 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**.
- From the Select Alarm Type tab, select the alarm types which you want to generate for the selected devices and click Save.

System Alarm Settings

9. 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 lost connection alarm in minutes: Triggered when an AP lost heartbeat event and not recovered within the specified minutes.
- 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.

10. 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
- 11. 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.
- 12. 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 115 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 115 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 65 Event Configuration

| Event Cor | nfiguration | | |
|---------------------|-------------------------------|-----------------------|------------------|
| Event Configuration | Configured ZDs Config Task Lo | og | |
| Create Edit D | | | |
| | onfiguration Name | Created On | Created By |
| | efault Event Configuration | May. 04 2018 15:20:50 | admin@ruckus.com |

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 66 Filtering Configured ZDs

| Event Configuration | Configured ZDs Config | Fask Log | | | |
|--------------------------|-----------------------|------------------|-------|---------------|---------------|
| List of ZD Configuration | ~ | | | | |
| Filter Rows Where: | Controller Name v | Exactly equals ~ | and + | | |
| Controller Name | IP Address | IPv6 Address | Model | Serial Number | Configuration |

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 67 New Event Configuration

| Event | Configura | ation Configured ZDs | Config Task Log | 9 | |
|-------|-----------|---------------------------------|------------------|-----------------------------------|------------------|
| Creat | te Edit | Delete Assign ZDs | | | |
| | ID | Configuration Name | | Created On | Created By |
| | 1 | Default Event Configuration | | May. 04 2018 15:20:50 | admin@ruckus.com |
| New | / Event C | onfiguration | | | |
| New | Event Co | onfiguration Name: | | | |
| S | ystem Ad | Imin Mesh Configurat | ion Client | AP Admin Performance | ce |
| | | | | | |
| [| | Event Type | Description | | |
| [| _ | ZoneDirector mesh AP uplink di: | Uplink disconn | ect | |
| E | | Admin restarted | System restart | ed | |
| [| | Admin restart | System is resta | arted by administrator. | |
| [| | Admin shutdown | System is shut | down by administrator. | |
| E | | Admin upgrade | System is upgr | raded. | |
| [| | Admin replace cert | SSL certificate | is being replaced by administrate | or. |
| E | | Admin replace privatekey | Private key is t | being replaced by administrator. | |

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 68 Task Logs

| Event Con | figuration | |
|---------------------|----------------|-----------------|
| Event Configuration | Configured ZDs | Config Task Log |

| ID | Task Name | Created On | Created By | Status | Action |
|--------------------|-----------|------------|------------|--------|--------|
| No data available. | | | | | |

Appendix

| • | Configuring Unleashed Multi-Site Manager Behind the NAT Server | 121 |
|---|---|-----|
| • | Configuring Unleashed Multi-Site Manager In Front of NAT Server | 122 |
| • | Configuring the 200.6 Unleashed Setup | 123 |
| • | Configuring ZoneDirector & 200.5 Unleashed Behind NAT Server | |
| • | Configuring ZoneDirector & 200.5 Unleashed In Front of the NAT Server | 130 |
| • | Zero Touch Deployment Setup Example | 132 |
| • | Setting Up Unleashed Multi-Site Manager as a Virtual Machine | |
| • | | 147 |

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 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 ManagerUnleashed 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.

If Unleashed Multi-Site Manager is managing ICX switches, ports 443 and 22 are used to bring up the SSH Tunnel. These ports are not configurable on the switch, so ensure the ports are mapped to Unleashed Multi-Site Manager on the NAT server.

Appendix

Configuring Unleashed Multi-Site Manager In Front of NAT Server

3. Create port forwarding rules: TCP: UMM IP: 9443, TCP: UMM IP: 443 and TCP: UMM IP: 22

FIGURE 69 Sample Port Forwarding Rule for Ports 22 and 9443

| Application: | UMM SSH | | |
|-------------------------|------------------------|----|-----|
| WAN Port | 22 | | |
| LAN IP Address: | 192.168.1.1 | | |
| LAN Port | 22 | | |
| Protocol: | TCP | | |
| | | ок | Can |
| Application: | UMM SSH Tunnel | | |
| WAN Port | 9443 | | |
| AN IP Address: | 192.168.1.1 | | |
| LAN Port | 9443 | | |
| Protocol: | TCP | • | |
| | | ок | ¢ |
| Application WAN Port | E 443 | | |
| WAN Port | t 443 t 192.168.1.1 | | |
| WAN Port | t 443 t 192.168.1.1 | | |

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, 443 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. This procedure is applicable for Unleashed device versions 200.6 and later.

1. Upload the Unleashed license as described in Uploading a License File on page 80.

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 70 Generating Unleashed ID

| Admin & S | ervices | | | |
|-----------------|----------|----------------|-------------------------------------|--|
| 🖵 System | T | System Info | | |
| System Info | | System Name* | Freddy_gateway | |
| 1 0 - 11 | | System Version | 200.5.10.0.183 | |
| IP settings | | Unleashed ID | un911534307539150089254059 Generate | |
| System Time | | | | |
| Country Code | | | | |

FIGURE 71 Unleashed - Restore Configuration

| Admin & Services | |
|----------------------|---|
| | |
| 🛄 System 🔰 | Back Up Configuration |
| Services | Click Back Up to save an archive file of your current Unleashed configuration. This archive will simplify system recovery if needed. |
| | Restore Configuration |
| Administer V | If you need to restore the system configuration, click Browse, and then select the backup file that contains the settings that you want to restore. |
| Preferences | Freddy_gateway_db_000217_14_29 bak (355216 bytes). Choose a restore hpm Restore everything Restore everything Freddy_gateway_db_000217_14_29 bak (355216 bytes). Choose a restore hpm |
| Dackup & Restore | Restore even thing, except system name and IP address settings (for fallover deployment at the same site). |
| Upprade | Restore only WLAN settings, access control list, roles, users, country code and system time (use this as a template for different sites). Select these 2 options will NOT overwrite the "Unleashed ID" |
| Repistration | Restore Cancel |
| | Restore to Factory Settings |
| Diagnostics | If needed, you can restore Unleashed to its factory settings, which will delete all settings that you have configured. You will need to manually set up Unleashed again. For more information, see the online help. |
| Certificate | Restore to Factory Settings |
| Network Connectivity | |
| Network Management | |
| Mobile App | |

- 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 72 Enabling Unleashed Multi-Site Manager Management

| System | • | SNMPv2 Agent | SNMPv3 Agent | SNMP Trap | Unleashed Multi-Site Manager | Alarm Notifica | ation | |
|--|---|--------------|--------------------|-------------------|---|----------------|--|---|
| Services | • | Unleashed I | Mutt-Site Manager | - | | | | |
| Administer | v | Enter the Un | leashed Multi-Site | 1000 C 1000 C 100 | er URL and set the time interval at w Unleashed Multi-Site Manager | | and the second | des to Unleashed Multi-Site M ashed Multi-Site Manager |
| | | | | | URL | https:// 172 | 18.56.7 | Antune/server |
| helerences | | | | | | | | |
| | | | | | Interval" | 15 0 | minutes) | |
| Backup & Restore | | Last succes | ssful contact (201 | 7/9/7 17:42:40 | 1. STANDER | 15 0 | ninutes) | |
| Backup & Restore Upgrade | | Last succes | ssful contact (201 | 7/\$/7 17:42:40 | 1. STANDER | 15 0 | nihutes) | |
| Preferences Backup & Restore Upgrade Registration Diagnotics | | Last succes | ssful contact (201 | 7/9/7 17:42:40 | 1. STANDER | 15 9 | ninutes) | |

- 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 the Unleashed devices and registered the them 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 80.

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.

Appendix

Configuring ZoneDirector & 200.5 Unleashed Behind NAT Server

- 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 73 Enabling and Configuring the Management Interface on ZD

| Enable IPv4 Management I | nterface |
|--------------------------|-----------------|
| IP Address* | 172.18.35.6 |
| Netmask* | 255,255,255,254 |

- 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 74 Enabling Unleashed Multi-Site Manager Management

| 🎝 Admin & Se | rvices | | | | | | |
|------------------|--------|--------------|---------------------|---------------|--|----------------------|---|
| 🛄 System | Þ | SNMPv2 Agent | SNMPv3 Agent | SNMP Trap | Unleashed Multi-Site Manager | Alarm Notification | |
| Services | • | | Muti-Site Manager | | | | |
| Administer | v | Enter the Un | nleashed Multi-Site | 1000 TO 100 | er URL and set the time interval at wi Unleashed Multi-Site Manager | | updates to Unleashed Multi-Site M Unleashed Multi-Site Manager |
| Preferencies | | | | | URL | https:// 172.18.56.7 | /intune/server |
| Backup & Restore | | | | | Interval" | 15 (minutes) | |
| Upgrade | | Last succes | ssful contact (201 | 7/9/7 1-42:40 | 14) Refresh | | |
| Registration | | | | | | | |
| Dagrotics | | | | | | | |
| Cetificate | | | | | | | |

 \times

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

FIGURE 75 Sample Port Mapping

Create a new port forwarding rule

| Application: | |
|-----------------|-------------|
| WAN Port: | 9557 |
| LAN IP Address: | 172.18.35.6 |
| LAN Port: | 443 |
| Protocol: | TCP |

Configuring ZoneDirector & 200.5 Unleashed Behind NAT Server

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 76 Generating Unleashed ID

| Admin & S | ervices | | | |
|--------------|---------|----------------|-------------------------------------|--|
| C. Sustam | - | | | |
| 🛄 System | | System Info | | |
| System Info | | System Name* | Freddy_gateway | |
| | | System Version | 200.5.10.0.183 | |
| IP settings | | Unleashed ID | un911534307539150089254059 Generate | |
| System Time | | | | |
| | | | | |
| Country Codo | | | | |

FIGURE 77 Unleashed - Restore Configuration

| Admin & Ser | vices | |
|----------------------|-------|--|
| | | |
| D System | ► | Back Up Configuration |
| Services | Þ | Click Back Up to save an archive file of your current Unleashed configuration. This archive will simplify system recovery if needed. Back up |
| Administer | Ŧ | Restore Configuration If you need to restore the system configuration, click Browse, and then select the backup file that contains the settings that you want to restore. |
| Preferences | | Freddy_pateway_db_000217_14_29 bak (355216 byles). Choose a restore type: Restore everything Select this option will overwrite the 'Unleashed ID' |
| Dackup & Restore | | Restore everything, except system name and IP address settings (for fallover deployment at the same site). |
| Upgrade | | Restore only WLAN settings, access control list, roles, users, country code and system time (use this as a template for different sites). |
| Registration | | Restore |
| Diagnostics | | Restore to Factory Settings If needed, you can restore Unleashed to its factory settings, which will delete all settings that you have configured. You will need to manually set up Unleashed again. For more information, see the online help. |
| Certificate | | Restore to Factory Settings |
| Network Connectivity | | |
| Network Management | | |
| Mobile App | | |

- 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 78 Enabling Unleashed Multi-Site Manager Management

| 🎗 Admin & Se | rvices | | | | | | | |
|------------------|--------|--------------|--------------------|---------------|---|-----------------|---------|--|
| 🛄 System | Þ | SNMPv2 Agent | SNI//Pv3 Agent | SNMP Trap | Unleashed Multi-Site Manager | Alarm Notificat | | |
| Services | Þ | | Mutt-Site Manager | | Uniezsneo Molo-Sne Manager | August records | lon | |
| Administer | Ŧ | Enter the Un | leashed Multi-Site | Manager serv | er URL and set the time interval at w Unleashed Multi-Site Manager | | | dates to Unleashed Multi-Site Ma leashed Multi-Site Manager |
| Preferences | i | | | | URL | https:// 172. | 18.56.7 | Antune/server |
| Backup & Restore | | | | | Interval" | 15 Qm | inutes) | |
| Upgrade | | Last succes | ssful contact (201 | 7/9/7 1-42:40 | :14) Refresh | | | |
| Registration | | | | | | | | |
| Diagnostica | | | | | | | | |
| Certificate | | | | | | | | |

- 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 79 Enabling Unleashed Multi-Site Manager Management on ZD

| r the F | FlexMaster server URL and set | the time interval at which Zonel | Director will send status updates to Fier | Master. |
|---------|-------------------------------|----------------------------------|---|---------|
| Enabl | le management by FlexMaste | r | | |
| JRL | https:// 172.18.42.8 | /intune/server | | |
| | 1 | (minutes) | | |

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

Appendix

Configuring ZoneDirector & 200.5 Unleashed In Front of the NAT Server

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 80 Configuring External Ports

| ZDs & Unle | eashed | Eat |
|--|--------------|---|
| Al Devices ZO | ^ Name | GPS Coordinates: Lattude: Longtude: |
| kenneth KUN | Ereddy3k1 | Web Port Mapping: 172.18.35.6 : 443 ↔ 172.18.101 (1007) 3 |
| CorpZD freddy | E Freddy3k2 | 4 |
| • R710 | FreddyT600 | 40 |
| | Freddy_12002 | Save Cancel 24 |
| | Freddy_R710 | un32150330772215C 172.18.56.53.443 |
| | Freddy_R720 | uns2170300004015C 192.168.190.118.4 |
| < | Freddy_T710 | unil4160480556815C 172.18.34.242.445 |

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 80.

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 > 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 81 Enabling Unleashed Multi-Site Manager Management

| 🎗 Admin & Se | rvices | | | | | | | |
|------------------|--------|--------------|--------------------|---------------|--|------------------------|--|-------|
| 🔲 System | Þ | SNMPv2 Agent | SNMPv3 Agent | SNMP Trap | Unleashed Multi-Site Manager | Alarm Notification | | |
| Services | Þ | | Mutt-Site Manager | | Unieasneo Multi-Site Manager | Addition records anoth | | |
| Administer | v | Enter the Un | leashed Multi-Site | 1000 TO 100 | er URL and set the time interval at wi Unleashed Multi-Site Manager | | end status updates to Unleashed Multi-Site rement by Unleashed Multi-Site Manager | e Man |
| Preferences | | | | | URL | https:// 172.18.56 | .7 /ntune/server | Т |
| Backup & Restore | | | | | Interval" | 15 (minute | rs) | Т |
| Upgrade | | Last succes | ssful contact (201 | 7/9/7 1 42:40 | :14) Refresh | | | |
| Registration | | | | | | | | |
| Diagnostics | | | | | | | | |
| Certificate | | | | | | | | |

- 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 82 Enabling Unleashed Multi-Site Manager Management on ZD

| r the F | FlexMaster server URL and | set the time interval at which ZoneDi | rector will send status updates to FlexMaster. |
|---------|---------------------------|---------------------------------------|--|
| Enable | e management by FlexMa | ster | 1 |
| RL. | https:// 172.18.42.8 | /intune/server | |
| erval | 1 | (minutes) | |

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

Zero Touch Deployment Setup Example

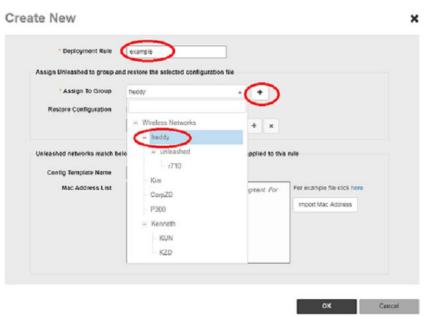
1. Backup the Unleashed configuration via Unleashed UI or you can register the Unleashed to UMM and backup the Unleashed configuration via UMM backup task and download it to your laptop.

- 2. Provision the Zero Touch Deployment rule on UMM server.
 - a) Login to UMM WebUI and go to the Unleashed-Zero Touch Deployment page.
 - Click the 'Create' Icon to create a new Zero Touch Deployment rule. b)

| TRUCKUS TM An ARRIS company Unleashed Multi-Site Manager | | | | | | |
|--|--|----------------------|-------------------|--|--|--|
| K Dashboard | Unleashed–Zer | o Touch Deployı | nent | | | |
| Devices | To download an example rule click here | | | | | |
| Tasks | + Create Create | Limport Rule | | | | |
| | Rule Name | Config Template Name | Group | | | |
| Unleashed-Zero Touch | Default Rule | | Wireless Networks | | | |
| Reports 🕨 | | | | | | |
| Administration | | | | | | |

Enter the Deployment Rule name and select the Device Group from the Assign To Group drop-down menu. c)

Whenever UMM apply this rule, it will move the Unleashed to the selected group automatically. And if your group is not in the list,



) icon to add the new group.

you can click (

÷

Appendix Zero Touch Deployment Setup Example

d) Enter the Deployment Rule name and select the Device Group from the Assign To Group drop-down menu.

| Create New | | | × |
|---|---|---|---|
| * Assign To Group | Ind restore the selected configuration file Wireless Networks | | |
| Restore Configuration 《 Unleashed networks match b Config Template Name | Select backup file to restore Select backup file to restore | s rule | - |
| Mac Address List | Mec addresses use ',' or spece or enter to segment. For example aa bb.cc.dd ee ff, 11.22, 11.11, 11.11 | For example file click here Import Mac Address | |
| | | | |

- f) Match the **Config Template Name** with the **Config Template Name** received from Unleashed and make sure to provision the same 'Config Template Name' on both UMM and Unleashed.
- g) Use the Mac Address List to match the rule against Unleashed Master AP and Click OK to save the rule..

| * Deployment Rule | and restore the selected configuration | -51a | | |
|--|---|-----------------------|---|--|
| * Assign To Group Restore Configuration | Wireless Networks | * + | | |
| Restore computation | | • + × | | |
| Unleashed networks match | below Template Name or Mac Address | will be applied to th | s rule | |
| Config Template Name Mac Address List | example 11:11:27:18:74:80 22:22:27:18:74:80 |] | For example file click here Import Mac Address | |

- 3. Initiation of Unleashed manually.
 - a) Power up the AP.
 - b) In the Setup Wizard, click UMM Install and enter the following parameters:
 - UMM Domain/IP: the IP of the UMM server.
 - Config Template Name: make sure that the name inside the UMM rule matches to the Zero Touch Deployment rule in the UMM server.
 - System Name: the name of your Unleashed.
 - c) Click Next to connect the Unleashed to the UMM server and the configuration file downloads automatically.
- 4. Initiate Unleashed AP by DHCP
 - a) Add the following options to the DHCP configured file (etc/dhcp/dhcpd.conf)

```
option space ruckus_info;
option ruckus_info.ummtag code 2 = text;
option ruckus_info.ummiplist code 1 = text;
vendor-option-space ruckus_info;
option ruckus_info.ummiplist "ummtest1.com, 10.223.5.230:9444"; //the UMM IP
option ruckus info.ummtag "noupgrade"; // the Config Template Name
```

b) Make sure the AP is in set factory status before powering on the AP.

AP receives the UMM IP and Config Template Name from the DHCP server and the Zero Touch Deployment is initiated.

- 5. Whenever there is an Unleashed match the Zero Touch Deployment rule, UMM creates a Zero Touch Deployment task in the Task page and displays the status of the deployment.
- 6. Check the status of Zero Touch Deployment in the task page.

Whenever there is an Unleashed match the Zero Touch Deployment rule, UMM creates a Zero Touch Deployment task in the Task page.

| ched Muth-Site Manager | | | | 2019/12/16 23 1 | 18:01 (53) et entres | admin@ruckus | com He |
|--------------------------------|---|---|--|---|--|---|---|
| Tasks | | | | | | | |
| Blands Fest | | | | | Search | ٩ | 0 O |
| Task Name | Task Type | Schedule | Status | Configuration File | | | Cre |
| | Zero Touch Deployment | | Success on Dec 16 2019 17 25:18 | Default Rule(backup2019121615 | 4023_un321503307 | 723157354709647 | Dec |
| | Backup | | Success on Dec 16 2019 16 55 10 | | | | Dec |
| freddymodify(58 b6 33 38 b7 40 | Zero Touch Deployment | | Success on Dec 16 2019 16 40 02 | freddymodify(backup201912161 | 45158_un321503307 | 723157354709647 | Dec |
| upgrade20191216163139 | Upgrade | 2019/12/30 21:30 | Not Started Yet | | | | Dec |
| backup20191216162828 | Backup | | Success on Dec 16 2019 16:30:04 | | | | Dec |
| upgrade20191216162815to8090 | Upgrade | | Success on Dec 16 2019 16 44:20 | | | | Dec |
| backup20191216154233 | Backup | | Success on Dec 16 2019 15 44 38 | | | | Dec |
| backup20191216154228 | Backup | | Success on Dec 16 2019 15:44:30 | | | | Dec |
| restore20191216154052 | Restore | 2019/12/16 13:40 | Success on Dec 16 2019 16:14:21 | backup20191216145156(backup | 20191216145156_u | 32150330772315 | Dec |
| backup20191216154023 | Backup | Daily 16:00 | Success on Dec 16 2019 16:00:00 | | | | Dec |
| | B Dobb # Fait Task Name Defait Defait Backup20191216185300 ReddymodryC88 b5 33.38 b7.40 Upgrads20191216183130 backup20191216182828 Upgrads2019121618283 Upgrads20191216162815 Upgrads20191216162815 backup20191216162815 Upgrads20191216162815 backup20191216162828 Upgrads20191216164283 | Tasks Task Name Task Type Delauti Zero Touch Depbyment backup20191216105300 Backup reddymodity(58 b6 33.38.67.40) Zero Touch Depbyment upgrads20191216105300 Backup backup20191216105300 Backup upgrads20191216105301 Upgrads backup20191216108155005 Upgrads | Tasks Task Name Task Type Schedule Delauti Zero Touch Deployment Indeds 93 98 87 400 Edeclup 20191216165300 Backup Indeds 93 08 87 400 Zero Touch Deployment Indeds 90 98 78 400 Indeds 93 08 87 400 Zero Touch Deployment Indeds 90 98 78 400 Indeds 93 08 87 400 Backup Indeds 90 98 74 400 Indeds 93 08 87 400 Backup 2019121610815640054 Upgrade Index 93 019121610815640054 Upgrade Index 90 91 9121610815640054 Index 93 019121610815640054 Upgrade Index 90 91 9121610815640054 | Task Name Task Type Schedule Babus Default Zero Toxch Deployment Success on Dec 16 2019 17 26 18 backup 201612101165000 Backup Success on Dec 16 2019 17 26 18 backup 201612101165000 Backup Success on Dec 16 2019 16 26 10 modymodat/08 b6 33.38 bF 24 Zero Toxch Deployment Success on Dec 16 2019 16 26 10 modymodat/08 b6 33.38 bF 24 Zero Toxch Deployment Success on Dec 16 2019 16 36 10 modymodat/08 b6 33.38 bF 24 Zero Toxch Deployment Success on Dec 16 2019 16 36 10 modymodat/08 b6 33.38 bF 24 Zero Toxch Deployment Success on Dec 16 2019 16 36 00 modymodat/08 b6 33.38 bF 24 Zero Toxch Deployment Success on Dec 16 2019 16 30.01 mysdak2019121616328 Backup Success on Dec 16 2019 16 30.01 mysdak2019121616328 Backup Success on Dec 16 2019 16 34.01 backup2019121616328 Backup Success on Dec 16 2019 15 34.01 backup2019121616328 Backup Success on Dec 16 2019 15 34.01 backup2019121616328 Backup Success on Dec 16 2019 15 34.01 | Task Ss Task Name Task Type Schedule Status Configuration File Default Zero Touch Deployment Success on Doc. 16 2019 17.25.18 Default Ruieblackup20191216165 backup20191216165300 Backup Success on Doc. 16 2019 17.25.18 Default Ruieblackup2019121616 modgmodstyl64.b6.33.38.b7.40 Zero Touch Deployment Success on Doc. 16 2019 17.25.18 Default Ruieblackup2019121616 modgmodstyl64.b6.33.38.b7.40 Zero Touch Deployment Success on Doc. 16 2019 16 4.00 modgmodfylbackup2019121616 upgrask20191216162828 Beckup Success on Doc. 10 2019 16 3.004 modgmodfylbackup2019121616 upgrask20191216162823 Beckup Success on Doc. 10 2019 16 3.004 modgmodfylbackup2019121616 upgrask20191216162823 Beckup Success on Doc. 10 2019 16 3.014 modgmodfylbackup2019121615 backup20191216162828 Beckup Success on Doc. 10 2019 16 4.420 modgmodfylbackup2019121615 backup20191216154233 Beckup Success on Doc. 10 2019 15 4.430 modgmodfylbackup2019121615 backup20191216154528 Beckup Success on Doc. 10 2019 15 4.430 modgmodfylbackup2019121615 | Task Same Schedule Status Configuration File Default Zero Toxch Deptoyment Stacoss on Dec 16 2019 17 25 18 Default Rivelbackup20191216154023_un321503307. backup20191216165300 Backup Stacoss on Dec 16 2019 17 25 18 Default Rivelbackup20191216154023_un321503307. backup20191216165300 Backup Stacoss on Dec 16 2019 17 25 18 Default Rivelbackup20191216154023_un321503307. backup20191216165300 Backup Stacoss on Dec 16 2019 16 25 10 modgmodty(bb 63 33 86 7 40. reddymodty(bb 63 33 86 7 40. Zero Toxch Deptoyment Stacoss on Dec 16 2019 16 40 02 modgmodty(bb 63 33 86 7 40. upgrask2019121616283 Backup Stacoss on Dec 16 2019 16 30 44 modgmodty(bb 63 2019 12 10 16 45 156_un321 500307. upgrask2019121616283 Backup Stacoss on Dec 16 2019 16 30 44 modgmodty(bb 63 2019 12 10 16 45 156_un321 500307. upgrask2019121616283 Backup Stacoss on Dec 16 2019 16 34 428 modgmodty(bb 63 2019 12 10 16 40 10. backup2019121616283 Backup Stacoss on Dec 16 2019 15 44 38 modgmodty 10 10.00 10. backup20191216154233 Backup Stacoss on Dec 16 2019 15 44 30 modgmodty 10.00 10.00 10.00 10.00 10.00 10.00 10.00 10.00 10.00 10.00 10 | Task Size Summbrief Summbrief <t< td=""></t<> |

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 6.10.

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. Login to the VMware ESXI interface and go to Virtual Machines.

FIGURE 83 Registering the VM

| vmware [®] Esxi [®] | | | |
|---|--|--|--|
| 📲 Navigator 🛛 | 🔁 localhost.video54.local - Virtual Machines | | |
| ✓ ☐ Host Manage Monitor | 🔁 Create / Register VM 🛛 💕 Console 📔 Virtual machine 🔺 | | |
| Virtual Machines 1 Storage 1 Q Networking 1 | VM2.1_48G | | |

2. Click Create/Register VM.

The **New virtual machine** page appears.

FIGURE 84 Creating a VM



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

4. Type the name virtual machine and select the VM_UMM_2.2.0.0.40.ova file.

FIGURE 85 Selecting the OVA File

| B New virtual machine - VIII_name_es | cample |
|---|---|
| 1 Select creation type 2 Select OVF and VMDK files 3 Select storage | Select OVF and VMDK files Select the OVF and VMDK files or OVA for the VM you would like to deploy |
| 4 License agreements 5 Deployment options 6 Additional settings 7 Ready to complete | Enter a name for the virtual machine. VM_name_example Virtual machine names can contain up to 80 characters and they must be unique within each ESN instance. |
| vm ware | × 📾 VM_UMM_2.1.0.0.27.ova |
| | Back Ned Finish Cancel |

5. 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 86 Editing VM Settings

| 🔁 Edit settings - VM2.1_16G (ESXi 6.5 vin | ual machine) | |
|---|---------------------------|-------------|
| Virtual Hardware VM Options | | |
| 🔜 Add hard disk 🛛 🛤 Add network ad | pter 🗧 Add other device | |
| POL | 4 • () | |
| Memory | 16384 MB • | |
| Hard disk 1 | 300 GB • | 0 |
| SCSI Controller 0 | LSI Logic Parallel | 0 |
| INNE Network Adapter 1 | VM Network 💌 📝 Co | nnect 🛞 |
| Floppy drive 1 | Use existing floppy image | 0 |
| CD/DVD Drive 1 | Host device 🔻 | 0 |
| Video Card | Specify custom settings | |
| | | |
| | | Save Cancel |

Setting Up Unleashed Multi-Site Manager as a Virtual Machine

6. 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 146 for more information.
- Change the login credential for Unleashed Multi-Site Manager. See Changing the Login Information for the Virtual Machine on page 146 for more information.
- Change the login credentials for the database. See Changing the Login Credentials to Access the Database on page 147 for more information.

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

Setting Up Unleashed Multi-Site Manager as a Virtual Machine

[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 ~]# In -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

Setting Up Unleashed Multi-Site Manager as a Virtual Machine

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/sdal 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: 0x0000000 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: 0x0000000

[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)

р

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: 0x0000000 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: 0x0000000

[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

Setting Up Unleashed Multi-Site Manager as a Virtual Machine

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

[root@localhost ~]# cd /home/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 13 Recommended hardware specifications

| Managed Devices | RAM | CPU | Hard Disk Space | Purge Policy |
|---|-------|---|-----------------|--------------|
| Up to 40 Unleashed/ZD network with total 2000 APs Up to 100 Unleashed network with 200 AP + 100 ICX switch | 16 GB | 4 core processor such as 3.30 GHz Intel [®] Core i5-3550 or equivalent | 300 GB | 7 days |
| Up to 200 Unleashed/ZD network with total 10000 APs Up to 1000 Unleashed network with total 2000 APs+ 1000 ICX switch | 64 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 /home/UMM/support files.
- 3. Execute the command /upgradeUser.sh /home/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:

- a. username: admin@ruckus.com
- b. password: admin

The default Unleashed Multi-Site Manager installation folder is /home/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:

- a. username: root
- b. 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 /home/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.

Configuring ICX Switches

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

1. Upload the Unleashed license as described in Uploading a License File on page 80.

There are three types of Unleashed Multi-Site Manager licenses files; one for ZoneDirector, one for switch and the other for Unleashed. Ensure you select the correct file. 2. Enable Unleashed Multi-Site Manager on the switch:

There are two ways to make an ICX switch aware of the Unleashed Multi-Site Manager's IP address - one is using DHCP option 43, and the other is using manual configuration through ICX commands.

• Manually configuring the Unleashed Multi-Site Manager IP Address on a switch includes issues the **sz active-list <IP address>**. Example:

```
SSH@Freddy-ICX7150-48PF-Router>enable
No password has been assigned yet...
SSH@Freddy-ICX7150-48PF-Router#configure terminal
SSH@Freddy-ICX7150-48PF-Router(config)#sz active-list 10.223.5.230
```

- Configuring DHCP to send Unleashed Multi-Site Manager IP addresses to ICX switches using DHCP Option 43, includes the following steps as shown in the example:
 - a. Configure DHCP Option 43 on the DHCP server using the RKUS.scg-address to identify the Unleashed Multi-Site Manager IP addresses.

Unleashed Multi-Site Manager IP addresses are sent with 6 as the sub-option value. The switch ignores all other data in DHCP Option 43 if Unleashed Multi-Site Manager IP addresses are present. Example:

```
subnet 192.168.12.0 netmask 255.255.255.0 {
range 192.168.12.100 192.168.12.199;
option routers 192.168.12.1;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.12.255;
option ntp-servers 192.168.11.22;
class "Ruckus AP" {
match if option vendor-class-identifier = "Ruckus CPE";
option vendor-class-identifier "Ruckus CPE";
default-lease-time 86400;
vendor-option-space RKUS;
option RKUS.scg-address "192.168.11.200";
}
```

3. You can view the status of the Unleashed Multi-Site Manager connection using the show sz status command.

Example:

```
SSH@Freddy-ICX7150-48PF-Router#show sz status
```

```
_____
                   SZ Agent State Info
                                                _____
Config Status: None Operation Status: Enabled
State: SZ SSH CONNECTED
                                Prev State: SZ SSH CONNECTING Event: NONE
Active List
                       : 10.223.5.230
DHCP Option 43 : No
DHCP Opt 43 List : None
Passive List
                      : None
                        : 10.223.5.230
Merged List
Merged Idx: 0 IP : 10.223.5.230
SZ IP Used
                        : 10.223.5.230
SZ Query Status
          Response Received
SSH Tunnel Status - :

        Tunnel Status
        : Established

        CLI IP/Port
        : 10.223.5.230/40005

        SNMP IP/Port
        : 10.223.5.230/30005

  Syslog IP/Port : 127.0.0.1/6514
Timer Status
                        : Not Running
```

You can use the sz-disconnect command to disconnect the ICX switch from the current connection with Unleashed Multi-Site Manager, and initiate a new connection based on the currently available list of Unleashed Multi-Site Manager IP addresses.
 Example:

ICX# sz disconnect SZ Disconnect initiated...

5. Login to the Unleashed Multi-Site Manager web interface and go to **Devices** and to see the ICX switch within the Switch group.



© 2022 CommScope, Inc. All rights reserved. 350 West Java Dr., Sunnyvale, CA 94089 USA https://www.commscope.com