Extreme NSight™ User Guide

9035561-01

Published December 2018

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks

Software Licensing

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at:
www.extremenetworks.com/support/policies/software-licensing

Support

For product support, phone the Global Technical Assistance Center (GTAC) at 1-800-998-2408 (toll-free in U.S. and Canada) or +1-408-579-2826. For the support phone number in other countries, visit: http://www.extremenetworks.com/support/contact/

For product documentation online, visit: https://www.extremenetworks.com/documentation/

Table of Contents

Preface

This guide is intended for users of NSight version 5.9.3

Conventions

This section discusses the conventions used in this guide.

Text Conventions

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

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
	General Notice	Helpful tips and notices for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
New!	New Content	Displayed next to new content. This is searchable text within the PDF.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
The words **enter** and **type**	When you see the word "enter" in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
[Key] names	Key names are written with brackets, such as **[Return]** or **[Esc]**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **[Ctrl]**+**[Alt]**+**[Del]**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Terminology

When features, functionality, or operation is specific to a switch family, such as ExtremeSecurity or Summit®, the family name is used. Explanations about features and operations that are the same across all product families simply refer to the product as the switch.

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal	Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
The Hub	A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
Call GTAC	For immediate support: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)

- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribing to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1 Go to www.extremenetworks.com/support/service-notification-form.
2 Complete the form with your information (all fields are required).
3 Select the products for which you would like to receive notifications.

> **Note**
> You can modify your product selections or unsubscribe at any time.

4 Click **Submit**.

1 Extreme NSight Overview

Extreme NSight is an advanced network visibility, service assurance and analytics platform that is exceptionally responsive and easy to use. It is designed for day-to-day network monitoring and troubleshooting with the capability of providing essential macro trending analytics for network planning, usage modeling and SLA management. Extreme NSight provides real-time monitoring, historical trend analytics and troubleshooting capabilities for WLAN deployment management. Starting with the 5.9.3 release, Extreme NSight can be deployed as a stand-alone virtual machine that provides a single-pane-of-glass interface to monitor and manage multi-cluster controller deployments.

Extreme NSight is designed for day-to-day network monitoring and troubleshooting and provides macro trending analytics for network planning, usage modeling and SLA management. Extreme NSight provides administrators sophisticated network visualizations, graphically displaying the information they require with minimal keystrokes. Extreme NSight's user interface can display network visualizations at every level. Aggregate site-level information is used to assess connected user the application utilization and throughput or specific Access Point or client device RF parameters and statistics in real-time. With flexible deployment options, Extreme NSight can now scale to support 40,000 Access Points.

Using Extreme NSight, administrators can construct customized, role-based dashboards for every IT role in their organization (help desk, network administrator, CIO etc.). Dashboards abstract and simplify the presentation of critical data to facilitate rapid responses to potential network problems. Several default dashboards are provided along with the tools to create new dashboards to fit specific organizational requirements. Once created and shared, all users working on a specific issue share the same view.

Extreme NSight contains a built-in set of troubleshooting tools and an event log browser. When troubleshooting connectivity issues, an administrator has access to basic network debugging tools through the same Extreme NSight interface to further clarify the problems. Troubleshooting tools include:

- Packet capture
- Wireless Debug log access
- TCP/IP Ping & Traceroute
- Access Point Testing
- Spectrum Analysis

When reviewing Access Point details or a client details page, an administrator can review a summary of each event related to the device by launching the event log browser with appropriate filters applied for the device and, if desired, launch the packet capture tool and save the capture information to a local file and share it with relevant IT and Support teams. This troubleshooting can be done remotely without making site visits.

Central to Extreme NSight functionality is the map view . Map view is an interactive tool allowing an administrator to embed any network or RF specific attributes of an Access Point or client. For example, an administrator would typically want to obtain a quick overview of SmartRF™ channel planning to verify if device operating channels are evenly distributed and identify potential trouble spots. Extreme NSight floor maps optimally display specific network including RF channel assignments, SNR, Retries, Power, throughput, client count and other relevant data.

Displaying the RF quality index of managed Access Point radios allows an administrator to quickly identify Access Points with poor RF quality. Extreme NSight quality index labels are color coded to indicate the overall RF quality of the Access Point based on the signal strength of their connected clients connect and their retry rates. Using the associated sliders, an administrator can filter the list of Access Points with poor RF quality, then display additional RF parameters on the like retry rates, throughput and number of clients connected to assist with troubleshooting.

Extreme NSight User Interface

The Extreme NSight user interface is navigated using two primary menus, the Left Nav and the Top Nav.

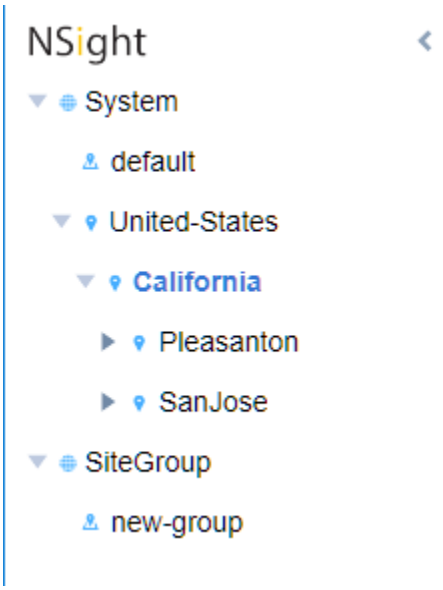


Figure 1: Extreme NSight Left Navigation Menu

The Left Nav displays a hierarchical view of locations and sites in the network. Selecting a site from the Left Nav updates the data in the main window.

Deployments can be organized in a tree hierarchy to reflect your actual network topology. The tree makes it convenient to browse the wireless network when organized hierarchically compared to looking for individual RF Domains. When selecting a higher level object in the tree hierarchy, the user can review consolidated information from all the RF Domains within that location's hierarchy.

The tree can be organized into multiple network levels (Country, Region, City or Campus). Create a tree hierarchy consistent with your wireless deployment. Once created, the tree hierarchy is available throughout the Extreme NSight UI.

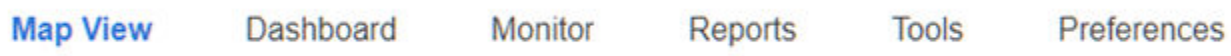


Figure 2: Extreme NSight Top Navigation

The Top Nav is used to select which Extreme NSight function is displayed for the selected site. The Top Nav is divided into *Map View, Dashboard, Monitor, Reports, Tools* and *Preferences*. Selecting one of these items updates the main window with corresponding data and tools.

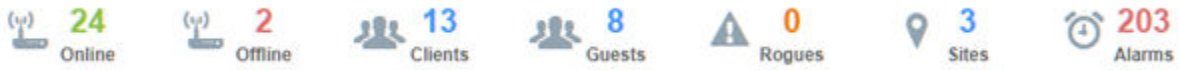


Figure 3: Extreme NSight Key Metrics

Each map view and monitor screen contains key information in the Key Metrics Strip. *Key Metrics Strip* (KMS) is available on a bar at the top of the screen. KMS displays the most recent available data. KMS includes online and offline APs, number of clients, number of unauthorized devices and number of sites.

When System is selected from the navigation tree on the left-hand side of the screen, KMS displays information supporting each RF Domain comprising your network's system wide deployment. Once the user navigates to a specific RF Domain from the left navigation tree, KMS information gets updated to display only the selected RF Domain. KMS also displays 2.4GHz and 5GHz frequency bands for specific RF Domains. Clicking on a specific RF Domain displays additional details.

Extreme NSight Licensing

Extreme NSight is a licensable feature which follows a subscription model. The license key comprises of two key parameters, Device Count & Expiry Date.

- Device Count: The count should be equal to or greater than the number of managed devices in the network, and is a sum of the total number of access points and controllers.
- Expiry Date: The licenses are valid until the expiry date specified on the licenses. Licenses are available for a period of 1 to 3 years.

Note
WiNG VX9000 NSight licenses are valid on Extreme NSight installations.

If the license count is insufficient or the licenses have expired, a warning message is displayed on the Extreme NSight UI for a period of 60 days. After 60 days, the user interface is shut down. After the UI is shut down, the server will continue to collect statistics and write information to the database. When a valid license is installed, the UI will resume normal operation.

2 Extreme NSight Installation and Migration

Installing Extreme NSight on a Hypervisor

1. Use the following link to go to the Extreme Networks Portal download page: Extreme Networks Portal Download Page.
2. If you do not have an Extreme Portal account, register here: https://extremeportal.force.com/ExtrAccountRegistration.
3. Select the ExtremeWireless product family.
4. Select the Firmware tab.
5. The Firmware page displays the resources that you are entitled to. If you do not see the items that you need or think that you are entitled to, please contact GTAC http:// www.extremenetworks.com/support/contact/.
6. Download the Extreme NSight application. The application is downloaded as an .iso image.

Note
Ensure a virtual machine hypervisor is installed in your server environment or the downloaded .iso image will not run.

7. Install the .iso following your hypervisors instructions for installing a virtual machine.
8. Boot the Extreme NSight application for the first time.

During installation you will be prompted to enable LVM (Linux Virtual Machine) disk support. If you need LVM/Elastic Storage enter **Yes**.

9. Log into the command line interface using the default username **admin** and default password **admin123**. The system will prompt you to change your password.
10. Create an Extreme NSight policy:

```
nsight-policy <name>
```

11. Configure Extreme NSight as a server:

```
nsight-server standalone
```

12. Enable the Extreme NSight policy from the device context of Extreme NSight:

```
use nsight-policy <name>
```

13. Enter license details.

```
ExtremeNSight# self
ExtremeNSight# license (NSIGHT/NSIGHT-PER) <license-key>
```

```
ExtremeNSight# commit write
      memory
```

Note

The command `no nsight client-history` should be run on all WiNG WLANs which are used for guest access in your network. This will ensure that new clients connecting to the guest WLANs will be marked as guest clients in Extreme NSight.

Note

On the WiNG controller `no controller adoption` should be run on any controller that does not adopt another controller.

14 For more advanced deployment information see Extreme NSight Deployment on page 17 and follow the instructions for your deployment type.

Enabling Mongo Database Authentication

To optionally enable Mongo authentication on Extreme NSight's database, perform the following steps from the CLI:

1 `config terminal`
2 `database-policy default`
3 `self`
4 `use database-policy default`
5 `commit write memory`
6 `database keyfile generate`
7 `service database authentication create-user username <username> password <password>`
8 `config terminal`
9 `database-policy default, authentication, authentication username <username> password <password>`
10 `database-client-policy default, authentication username <username> password <password>`
11 `self`
12 `use database-client-policy default`
13 `commit write memory`

Migrating Extreme NSight from a VX9000 Installation

When migrating from a WiNG VX9000 installation of NSight, a patch must first be applied. Standalone and replica set installations have different migrations processes.

Select the migration process that matches your current WiNG NSight installation type:

- Migrating a WiNG VX9000 Standalone NSight Server on page 13
- Migrating a WiNG VX9000 3 Node Replica Set NSight Server on page 13

Migrating a WiNG VX9000 Standalone NSight Server

The following instructions explain how to migrate a standalone WiNG VX9000 NSight server to a standalone Extreme NSight installation.

Ensure your previous version of NSight is running in standalone mode on a VX9000 WiNG controller before attempting the migration process. If you are running NSight on a replica set, see Migrating a WiNG VX9000 3 Node Replica Set NSight Server on page 13.

Note

Create a backup of the database before migration using the `database backup` command.

1. Create a backup of the current VX9000 NSight server's running configuration using the `copy running-config <options>` command.
2. Create a Tech Support backup using the `service copy tech-support <options>` command.
3. Install the migration patch using the `upgrade UpgradeVX9000ToExtremeNSight.patch` command.
4. Check `show boot` to verify the patch has been installed.
5. Upgrade the VX9000 to the Extreme NSight 5.9.3 firmware using the `upgrade <ftp/tftp> ExtremeNSight-5.9.3.0-00XR.img`.
6. Before reloading, remove the NSight policy using the `no use nsight-policy` command.
7. Reload into the upgraded partition.
8. Verify that the database server is up and in Primary state after the reload.
9. Re-apply the NSight policy on the Extreme NSight server.

Migrating a WiNG VX9000 3 Node Replica Set NSight Server

The following instructions explain how to migrate a 3 Node Replica Set WiNG VX9000 NSight installation to a Extreme NSight 3 Node Replica Set installation.

Ensure your previous version of NSight is running in a 3 Node Replica Set mode before attempting the migration process. If you are running NSight in a standalone configuration, see Migrating a WiNG VX9000 Standalone NSight Server on page 13

1. Remove the NSight policy from the Primary and Secondary using the `no use nsight-policy` command.

Perform the following commands first on the Arbiter node, then the Secondary node followed by the Primary node.

2. Create a backup of the current VX9000 NSight server's running configuration using the `copy running-config <options>` command.
3. Create a Tech Support backup using the `service copy tech-support <options>` command.
4. Install the migration patch using the `upgrade UpgradeVX9000ToExtremeNSight.patch` command.
5. Check `show boot` to verify the patch has been installed.

6 Upgrade the VX9000 to the Extreme NSight 5.9.3 firmware using the `upgrade <ftp/tftp> ExtremeNSight-5.9.3.0-00XR.img`.
7 Before reloading, remove the NSight policy using the `no use nsight-policy`.
8 Reload the Arbiter node first, and confirm the database status post reload.
9 Reload the Primary node, and use the `show database status` command to confirm the Primary node displays as Primary.
10 Reload the Secondary node.

Once the above commands have been run on all three nodes, proceed to the next step.

11 Confirm that the database servers are in their correct state (Primary/Secondary/Arbiter) after all three nodes have reloaded.
12 Reapply the NSight policy on the Primary Extreme NSight server, then apply it to the Secondary server.

Exporting and Restoring the Mongo Database

To migrate the Mongo Database from an existing WiNG NX9500, NX9600 or VX9000 NSight server you must first export the existing database and restore it on the new Extreme NSight installation.

- Exporting the Mongo Database on page 14
- Importing the Mongo Database without Mongo Authentication on page 15
- Importing the Mongo Database with Mongo Authentication on page 14

Exporting the Mongo Database

To export the Mongo database from an existing NX9500, NX9600 orVX9000 NSight server:

Note
For installations without Mongo authentication, skip to Step 2.

1 `NX9600# database keyfile export ftp://user:pass@ipv4address/database-keyfile`
2 NX9600# database-backup database nsight ftp://user:pass@ipv4address/nsightdb-with-auth.tar.gz

Importing the Mongo Database with Mongo Authentication

To restore a Mongo Database that uses Mongo Authentication:

1 Confirm that the default database policy is configured. If the default database policy is configured, proceed to step 8.
2 To configure the default database policy, run the following commands from the CLI.
3 `config terminal`
4 `database-policy default`
5 `self`
6 `use database-policy default`
7 `commit write memory`
8 Confirm that the NSight policy is not configured.

9 `show database keyfile`
10 `database keyfile zeroize`
11 `database keyfile import ftp://user:pass@ipv4address/database-keyfile`
12 Follow Mongo Authentication Procedure to create database users.
13 `ExtremeNSight# database-restore database nsight ftp://user:pass@ipv4address/nsightdb-with-auth.tar.gz`
14 `show database restore-status`
15 `show database status`
16 `show database statistics`
17 `self`
18 `use nsight-policy <policy-name>`
19 `commit write memory`
20 `show nsight status`

Importing the Mongo Database without Mongo Authentication

To restore a Mongo Database that does not use Mongo Authentication:

1 Confirm that the default database policy is configured. If the default database policy is configured, proceed to step 8.
2 To configure the default database policy, run the following commands from the CLI.
3 `config terminal`
4 `database-policy default`
5 `self`
6 `use database-policy default`
7 `commit write memory`
8 Confirm that the NSight policy is not configured.
9 `ExtremeNSight# database-restore database nsight ftp://user:pass@ipv4address/nsightdb-with-auth.tar.gz`
10 `show database restore-status`
11 `show database status`
12 `show database statistics`
13 `self`
14 `use nsight-policy <policy-name>`
15 `commit write memory`
16 `show nsight status`

Migrating WiNG to a New Controller on Combined WiNG and NSight VX9000 Installations

In installations where WiNG and NSight are running on the same VX9000, follow this procedure to migrate WiNG to a new controller and use the existing VX9000 as ExtremeNSight.

1 Host a new VX9000-02 (5.9.3.0-018R) and install WiNG adoption licenses.
2 Migrate configurations from existing VX9000 installation to VX9000-02. Update the IP address if needed..

3. Configure an auto-provisioning policy on the original VX9000 with redirect elements for adopting devices. Enable `evaluate-always`.
4. Delete adopted device context from the original VX9000 WiNG controller.
5. Let the adopted devices migrate to the new VX9000-02 WiNG controller.
6. Verify that the adopted devices get the new controller IP address.
7. Verify that all APs have migrated and adopted to the new VX9000-02 WiNG controller.
8. Upgrade the original VX9000 installation using the migration script: `UpgradeVX9000ToExtremeNSight.patch`.
9. Upgrade the original VX9000 with the Extreme NSight 5.9.3 image.

3 Extreme NSight Deployment

Standalone Deployment
3 Node Replica Set
Split VX Deployment

Database replica sets can be deployed when redundancy and high availability is required. To provide data redundancy and application high-availability, a replica set configuration is required. A replica set requires 3 members, ideally 1 in each in a data center, assuming more than 2 data centers exist. If no third data center is available, it is preferable that the third member is located in some external location to prevent a single point of failure by having 2 members in the same data center. If a third location is not possible, it is preferred that the third member be placed in the primary data center. TCP port 27017 is required to be open for inter-database communication between all replica set members. This guide will cover both standalone database and replica set deployments.

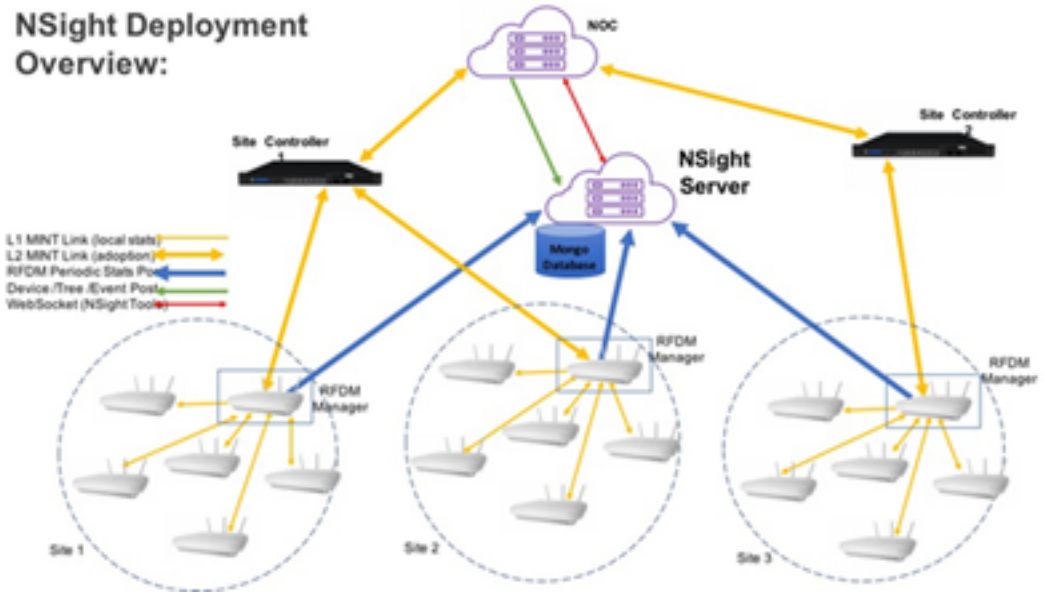


Figure 4: Extreme NSight Deployment Diagram

- Standalone Deployment
- 3 Node Replica Set
- Split VX Deployment

Standalone Deployment

Enabling Extreme NSight server on a VX appliance will automatically start the database server in a standalone mode. No data redundancy is provided in standalone mode. Extreme NSight and captive portal can be used in standalone mode without any further database specific configuration.

3 Node Replica Set

A 3 node replica set is the recommended high availability model for Extreme NSight deployments. A replica set is a group of database processes that maintains the same data set. Replica sets provide redundancy and high availability and are the basis for all production deployments. In a 3 node replica set, each member has a full copy of the database which is kept in sync with the other replica nodes.

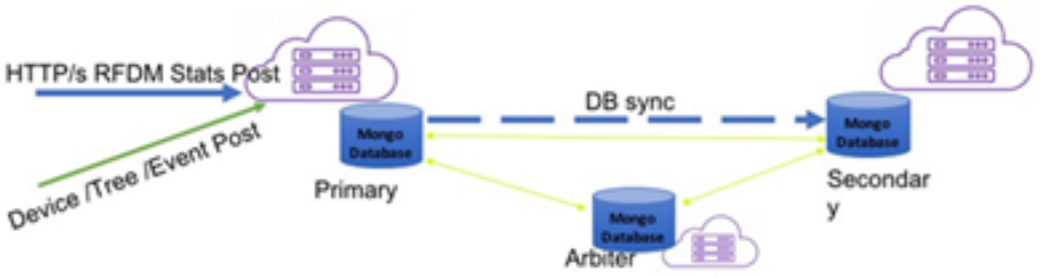


Figure 5: Extreme NSight 3 Node Replica Set Deployment Diagram

Note

TCP port 27017 is required to be open for inter-database communication between all replica set members.

To configure a 3 Node Replica Set:

1 Identify the tree devices to be used to form the replica set.

2 Identify the primary device, all other devices will be secondary. Total number of devices must be an odd number.

3 Create a database policy on each device. Statically set the priorities for primary and secondary devices. The default priority is 1, the higher the number, the higher the priority.

```
PRIMARY#conf t
Enter configuration commands, one per line.    End with CNTL/Z.
PRIMARY(config)#database-policy replica-set
PRIMARY(config-database-policy-replica-set)#replica-set member primary.domain.com
priority 200
PRIMARY(config-database-policy-replica-set)#replica-set member secondary.domain.com
priority 15
PRIMARY(config-database-policy-replica-set)#replica-set member tertiary.domain.com
priority 5
PRIMARY(config-database-policy-replica-set)#end PRIMARY#commit write
```

4 Apply the database policy to each device. The order that policies are applied does not matter.

```
PRIMARY#self
Enter configuration commands, one per line.    End with CNTL/Z.
PRIMARY(config-device-08-00-27-11-C2-DD)#use database-policy replica-set
PRIMARY(config-device-08-00-27-11-C2-DD)#end
PRIMARY#commit write
```

5 Check database status.

```
PRIMARY#show database status
--------------------------------------------------------------------------------
MEMBER    STATE    ONLINE TIME
--------------------------------------------------------------------------------
172.31.0.49*    PRIMARY    8 hours 9 min 12 sec
172.31.2.248    SECONDARY    8 hours 9 min 4 sec
172.31.5.121    SECONDARY    8 hours 9 min 8 sec
--------------------------------------------------------------------------------
[*] indicates this device.
```

Split VX Deployment

A split VX deployment consist of a primary, one or more secondary servers and an arbiter. An arbiter is a lightweight database server process which stores no data. The arbiter participates in replica set heart beats and primary elections only. Arbiters are good candidates for location outside of a data center as their data requirements are light, and the external location prevents a single point of failure scenario.

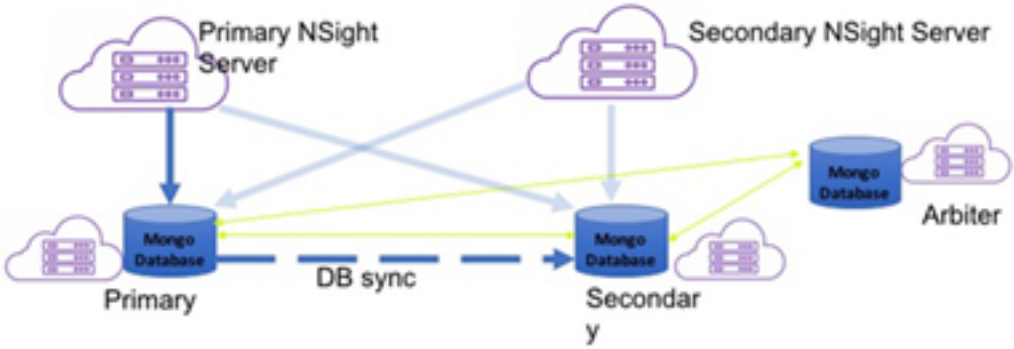


Figure 6: Extreme NSight Split VX Deployment Diagram

Note
TCP port 27017 is required to be open for inter-database communication between all replica set members.

The primary and secondary devices must be of the same device type: NX9600-NX9600 or VX9000-VX9000. Arbiters may be any device type that supports the arbiter role: NX9600, VX9000, NX7500, NX5500.

To configure a split VX deployment:

1 Identify the tree devices which will be used to form the replica set.
2 Identify the primary and secondary devices. If using a single secondary, the third device will be an arbiter.
3 Create a database policy on each device. Statically set the primary and secondary devices. Default priority is 1, the higher the number, the higher the priority.

```
PRIMARY#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PRIMARY(config)#database-policy replica-set
PRIMARY(config-database-policy-replica-set)#replica-set member primary.domain.com
priority 200
PRIMARY(config-database-policy-replica-set)#replica-set member secondary.domain.com
PRIMARY(config-database-policy-replica-set)#replica-set member arbiter.domain.com
arbiter
PRIMARY(config-database-policy-replica-set)#end
PRIMARY#commit write
```

4 Apply the database policy to each device. The order that policies are applied does not matter.

```
PRIMARY#self
Enter configuration commands, one per line.  End with CNTL/Z.
PRIMARY(config-device-08-00-27-11-C2-DD)#use database-policy replica-set
```

```
PRIMARY(config-device-08-00-27-11-C2-DD)#end
PRIMARY#commit write
```

5 Check the database status.

```
PRIMARY#show database status
--------------------------------------------------------------------------------
        MEMBER                 STATE                     ONLINE TIME
--------------------------------------------------------------------------------
172.31.0.49*            PRIMARY               8 hours 9 min 12 sec
172.31.2.248            SECONDARY            8 hours 9 min 4 sec
172.31.5.121            ARBITER               8 hours 9 min 8 sec
--------------------------------------------------------------------------------
 [*] indicates this device.
```

When the **show database** status output shows results like the example in step 5, a replica set has been configured, applied and formed. The asterisk [*] in the output indicates the device on which **show database status** was executed.

4 Map View

In a multi-site environment a top level view is available with each provisioned site. The high level view provides a quick snapshot of device and alarm status and client count at each site.

At the system level, the Map View displays each site with site locations displayed geographically for immediate visualization of the entire network. The Map View also displays the status of Access Points, connected clients and site status.

At its lowest level, a site view displays associated facility floor map(s). The floor map is an interactive tool displays the Access Points in their locations with configurable device or alarm status. At the site level, specific network information can be optionally displayed that includes RF channel assignments, SNR, retries, power, throughput, client count and alarm data.

Map View (System)

To view geographical or site based network maps:

1 Select Map View from the upper menu bar.
2 In the Left Nav select System.

The system level network map displays.

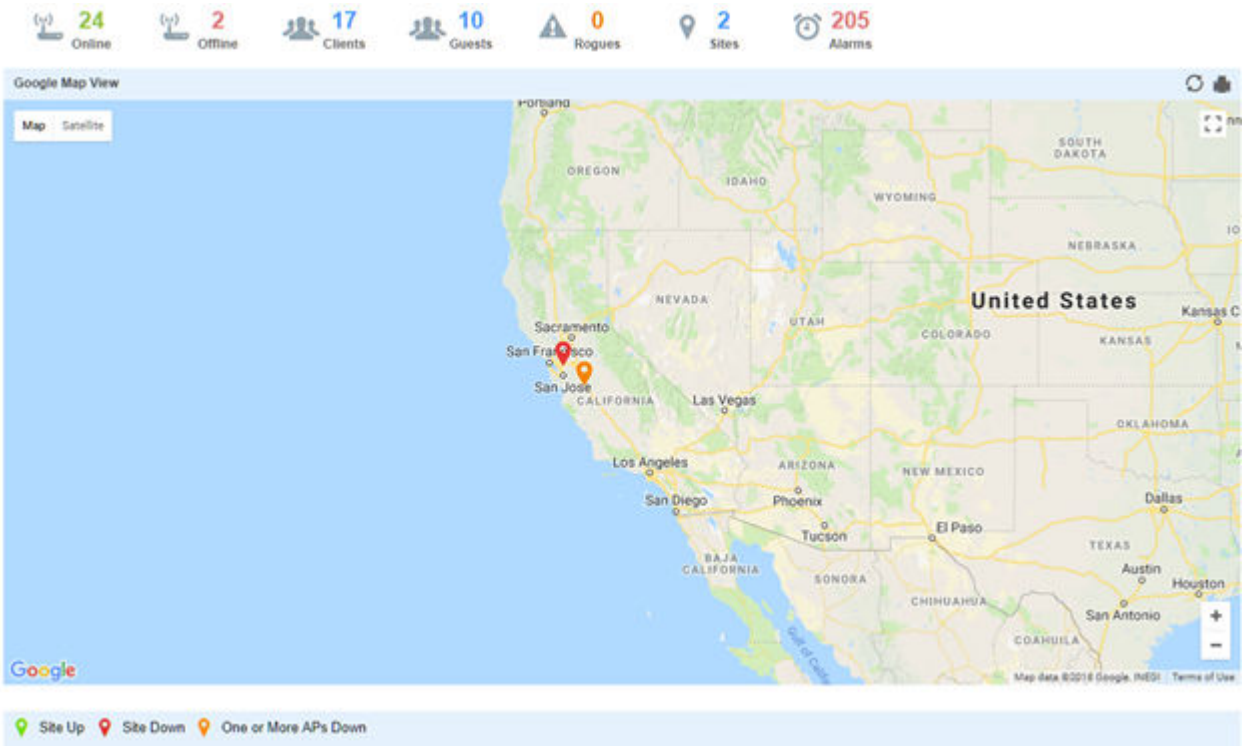


Figure 7: Extreme NSight > Map View > System

At the system level the Map View displays all the sites with site locations displayed geographically for immediate visualization of the entire network. The Map View also displays your connected site status. Hover the mouse on a site to see additional site details.

Map View (Site)

To view geographical or site based network maps:

1 Select Map View from the upper menu bar.
2 Select a site from the Left Nav.

The site level network map displays.

3 To view floor maps, expand the Left Nav menu until the list of sites is visible and select a site.

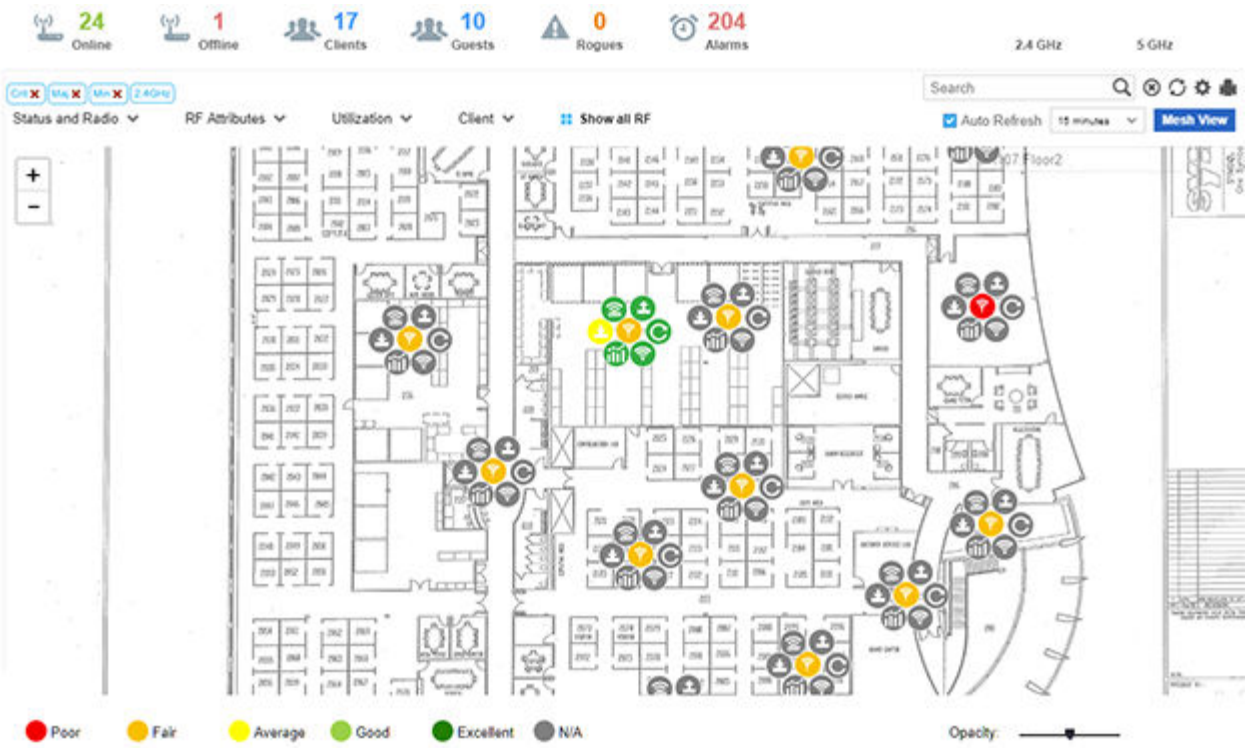


Figure 8: Extreme NSight > Map View > Site

At its lowest level, a site view displays associated facility floor map(s). The floor map is an interactive tool allowing an administrator to embed any network or RF specific attributes of an Access Point and its connected clients. At the site level, specific network information can be optionally displayed that includes RF channel assignments, SNR, retries, power, throughput, client count and other data.

A RF Quality Index allows administrators to quickly identify Access Points with poor RF quality. Quality index labels themselves are color coded to indicate overall Access Point RF quality based on the signal strength of connected clients and retry rates. Using the tool's sliders, an administrator can filter the list of Access Points with poor RF quality and show additional RF parameters likely retry rates, throughput and number of connected clients.

5 Dashboard

Dashboard

Use Dashboards to abstract and simplify the presentation of critical data to facilitate rapid responses to potential network problems. The Dashboard utilizes multiple tabs and customizable widgets and layouts within each tab. Several default Dashboards are provided, along with the tools to create new Dashboards to fit your organization's needs.

Dashboards can also be handy when troubleshooting network problems. Create a Dashboard in minutes and display aggregate level data or data tied to a specific network element. Once created and shared, all users working on a specific issue have the same view.

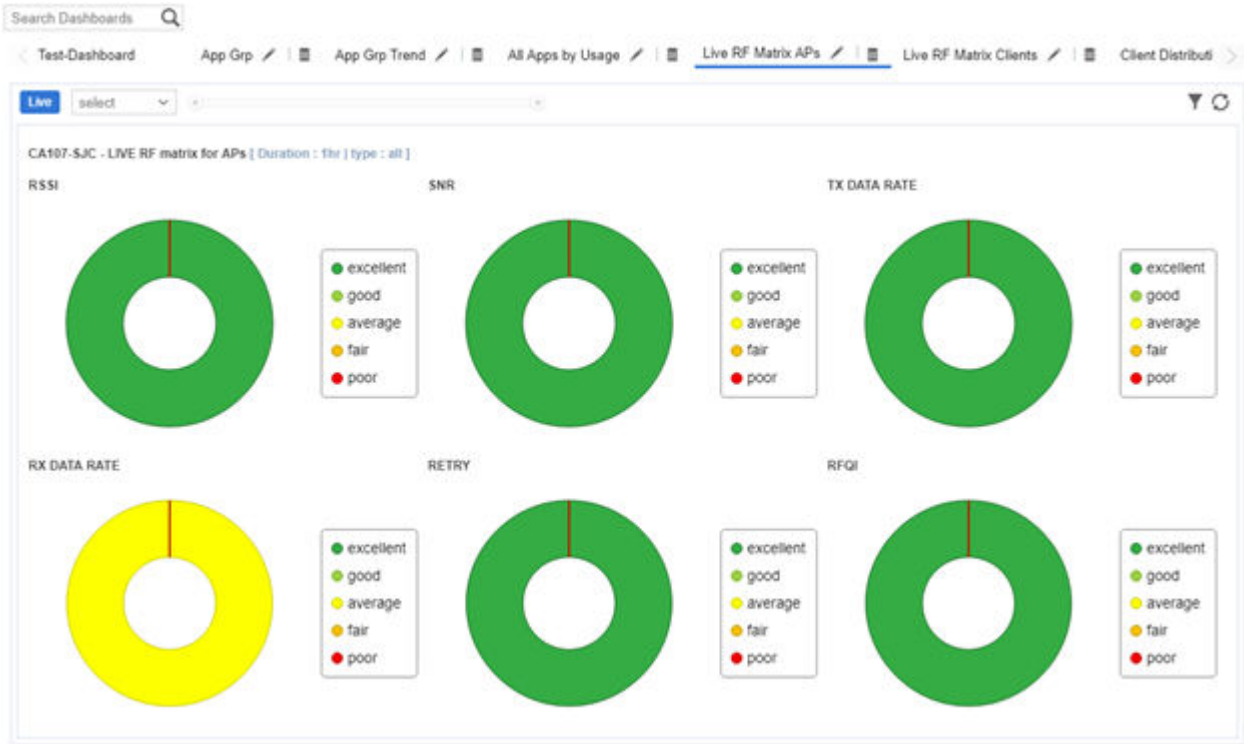
Dashboard

To view customizable network information on the Dashboard:

1 Select **Dashboard** from the upper menu bar.

2 Select **System**, a specific geographical location or site from the Left Nav.

Dashboard information specific to the selected item displays. If there are previously defined dashboards the display defaults to the first tab in the list. If there are no dashboards defined, an empty canvas displays.



3 Review the displayed network information, edit the existing tab layout or create a new tab to display customized network information. If reviewing an existing Dashboard, each widget can be expanded using the arrows in the upper right corner of each widget.

Create customized Extreme NSight Dashboards with specific theme and widget layouts. Themes enable an administrator define the number of data fields displayed in respect to the number of data items (widgets) trended.

Build an Extreme NSight Dashboard in three steps:

1 Select a Dashboard theme to define the number of panels and their order on the Dashboard
2 Drag and drop Dashboard widgets (from the Dashboard widget library) to define what data is displayed in each panel
3 Name the Dashboard and select **Save**

Dashboard Basics

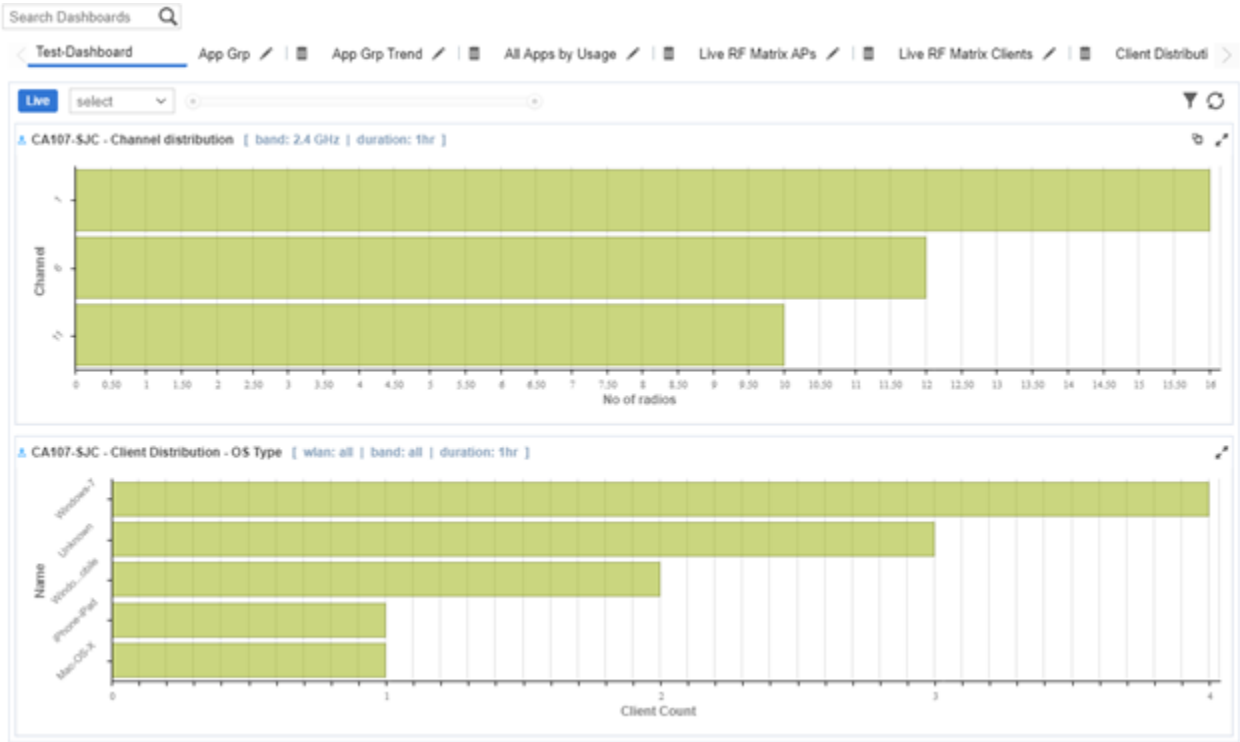


Figure 9: Extreme NSight Dashboard

Dashboards contain three main components: **Theme**, **Widgets**, and **Time**. The **Theme** controls the layout of a dashboard page and the number of widgets that can be displayed. The **Widgets** control the type of information that is displayed in the dashboard. The **Time** setting controls the period of time that data is displayed for in the widgets.

When accessing a user created dashboard the results can be further filtered by **Network** or by **Time**. To change the **Network** filter select a WLAN from the pull-down menu and the dashboard updates to show only data from that WLAN. To change the **Time** setting, use the pull-down menu to specify a time

period of **1 Hour**, **8 Hours**, **1 Day**, **1 Week**, **1 Month**, **3 Months**, **6 Months** or **1 Year**. Changes to the **Network** or **Time** are retained when accessing this dashboard.

Creating a New Dashboard

Describes the steps to create a customized Extreme NSight dashboard.

Create customized Extreme NSight dashboards with specific theme and widget layouts. Themes enable an administrator define the number of data fields displayed in respect to the number of data items (widgets) trended. Extreme NSight features a flexible dashboard design where the dashboard widgets can be added individually and freely resized once added to the dashboard.

To create a new dashboard:

1 Select **Dashboard** from the menu. Then select **Create New**.

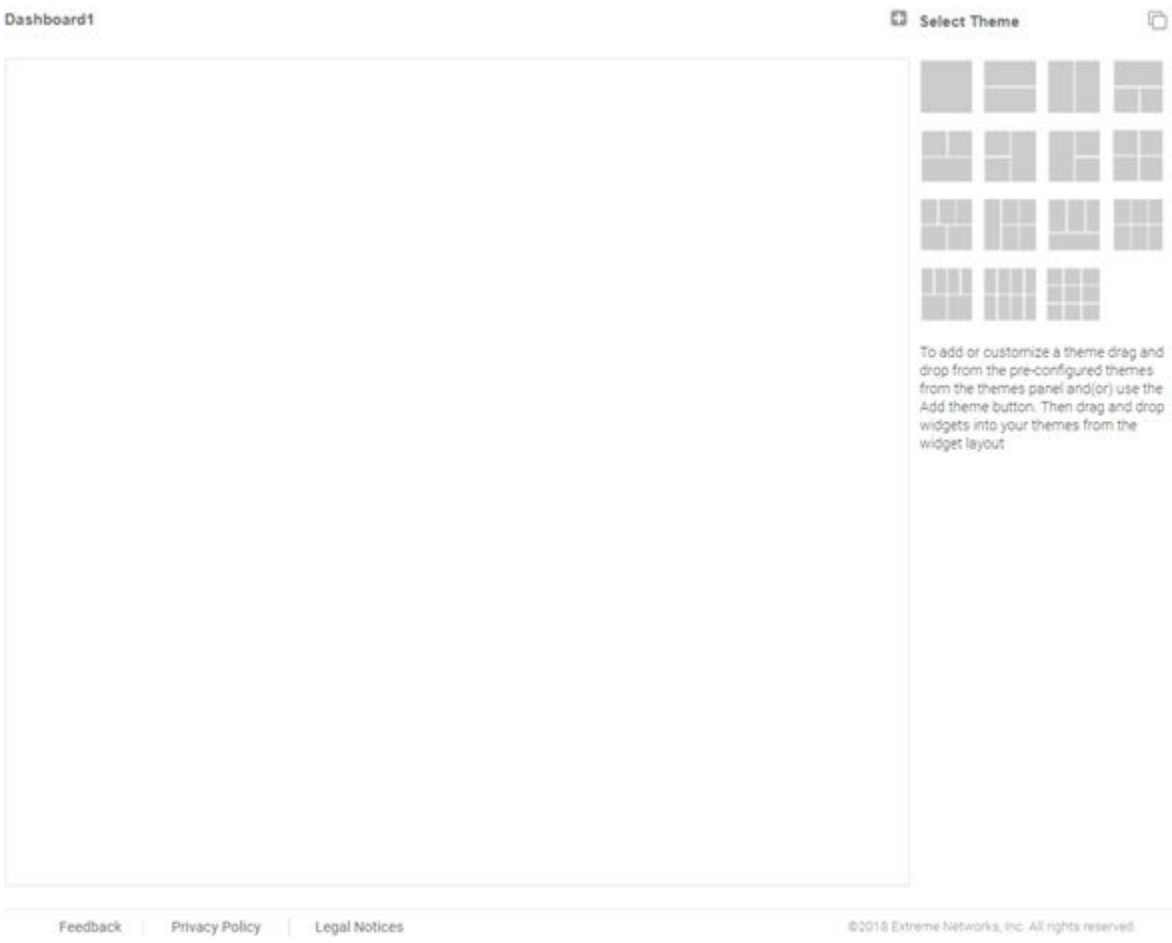


Figure 10: Extreme NSight New Dashboard

The new dashboard screen displays with no themes or widgets selected.

2 Select a theme from the **Select Theme** menu by dragging the layout to the main window. To change the layout, drag another theme in place of the current one.

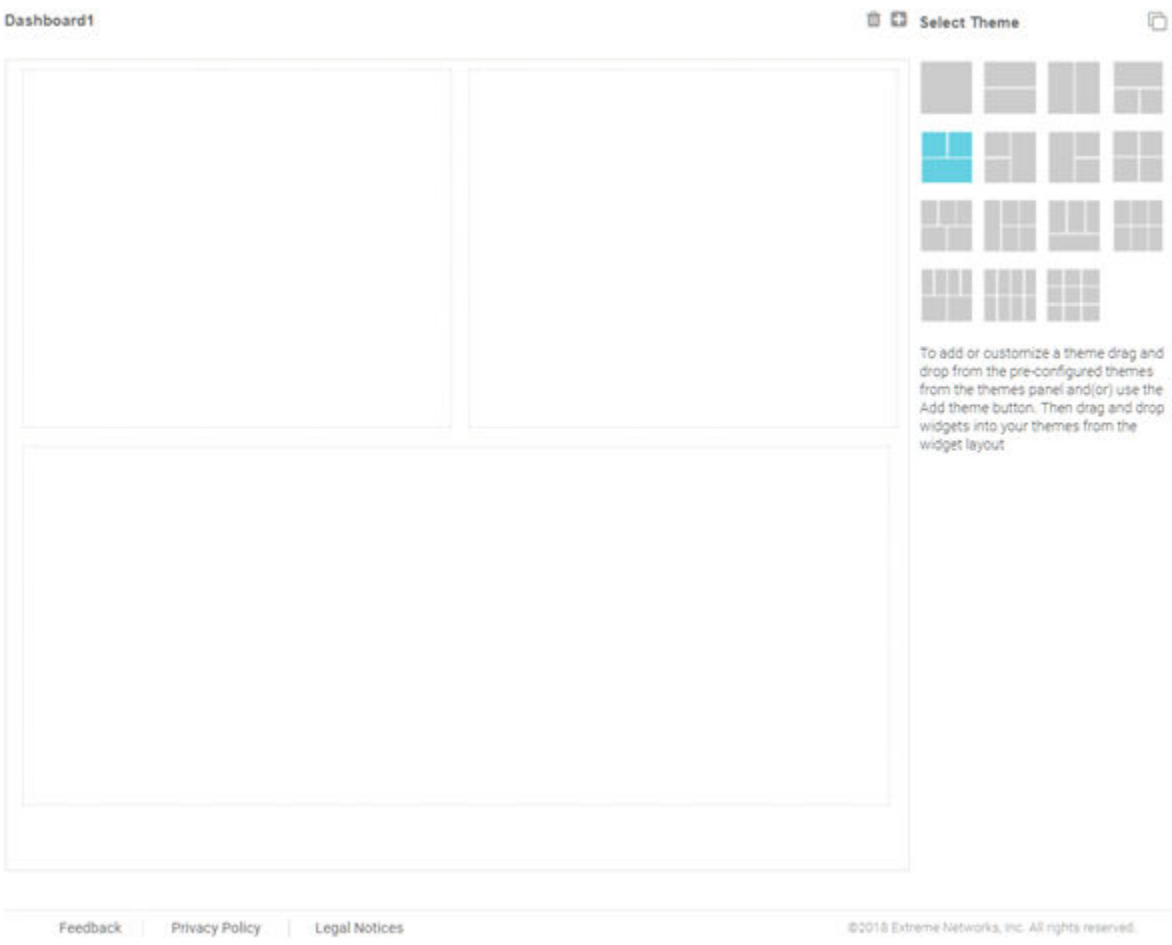


Figure 11: Selecting a Dashboard Theme

When a theme has been selected, an outline of the dashboard layout displays.

3 Change to the **Select Widget** view, by clicking on the icon next to **Select Themes**.

4 Drag widgets into empty windows to populate the dashboard.

Figure 12: Selecting Dashboard Widgets

Once a widget is placed it displays the data associated with that widget.

5 Select **Save** to commit the dashboard layout or select **Cancel** to cancel dashboard creation.

When saving a new dashboard provide the following information:

Name	The dashboard **Name** is used to identify the customized dashboard. This name displays in the menu when selecting **Dashboard** > **Dashboard Name**This value is mandatory.
Description	Provide a brief description of the newly created dashboard. This value is optional.
Public	Select this option to make the dashboard available to all users of the Extreme NSight management interface.

6 Select **OK** to finish saving the dashboard.

6 Monitor

Refer to the Monitor tools to assess Access Point and client performance and evaluate the risk to the network from unsanctioned (rogue) devices.

Summary (System)

Periodically review network Summary information of Access Point and client device utilization within the Extreme NSight network.

To view a summary of all monitored devices:

1 Select **Monitor** from the upper menu bar.
2 In the Left Nav select **Summary**.

The summary screen displays.

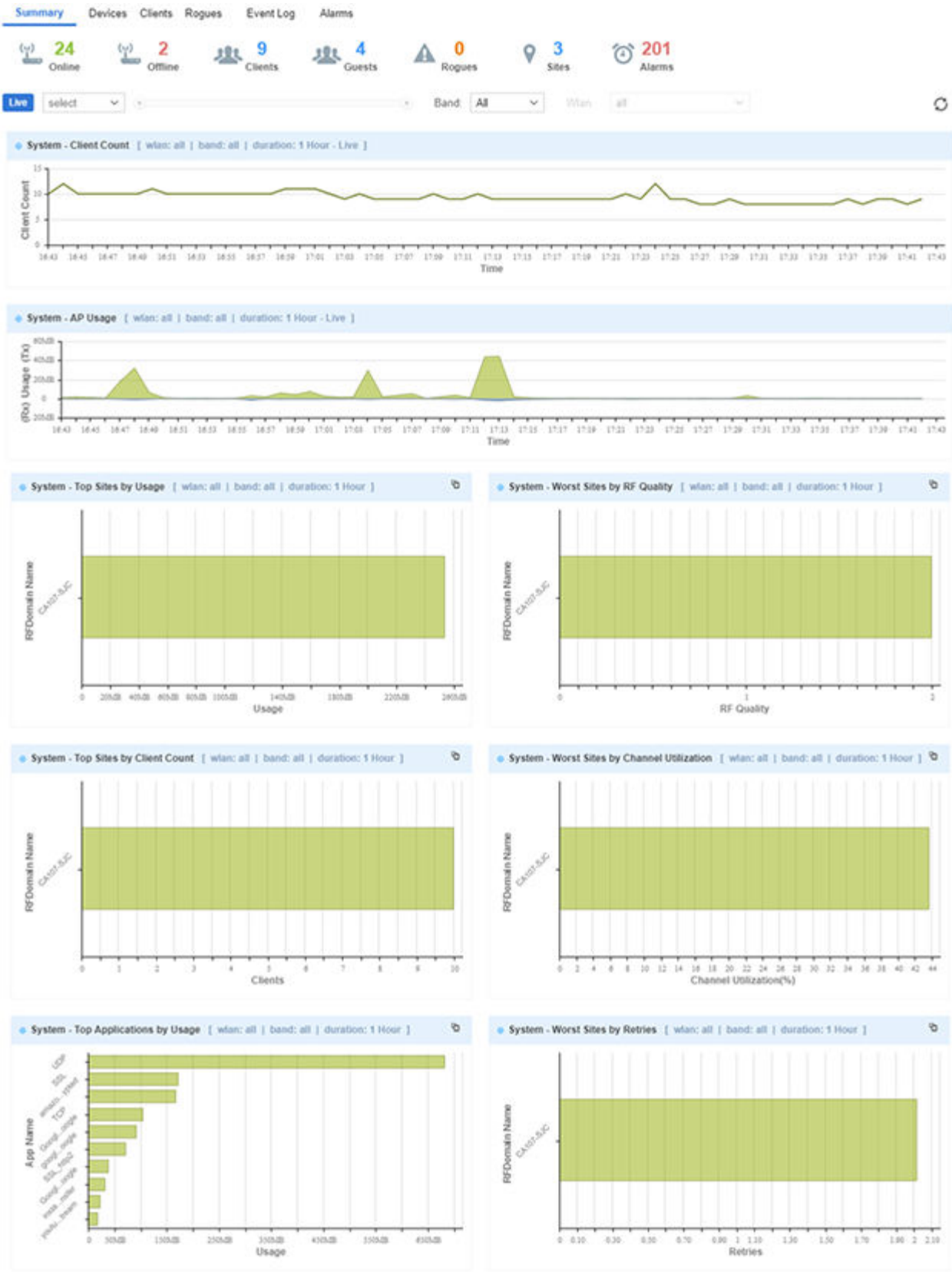


Figure 13: Extreme NSight > Monitor > Summary (System Level)

Summary (Site)

Periodically review network Summary information of Access Point and client device utilization within the Extreme NSight network to determine whether client load is evenly distributed amongst deployed Access Points.

To view a summary of all monitored devices:

1 Select **Monitor** from the upper menu bar.
2 Select **Summary** from the Left Nav.

The summary screen displays.

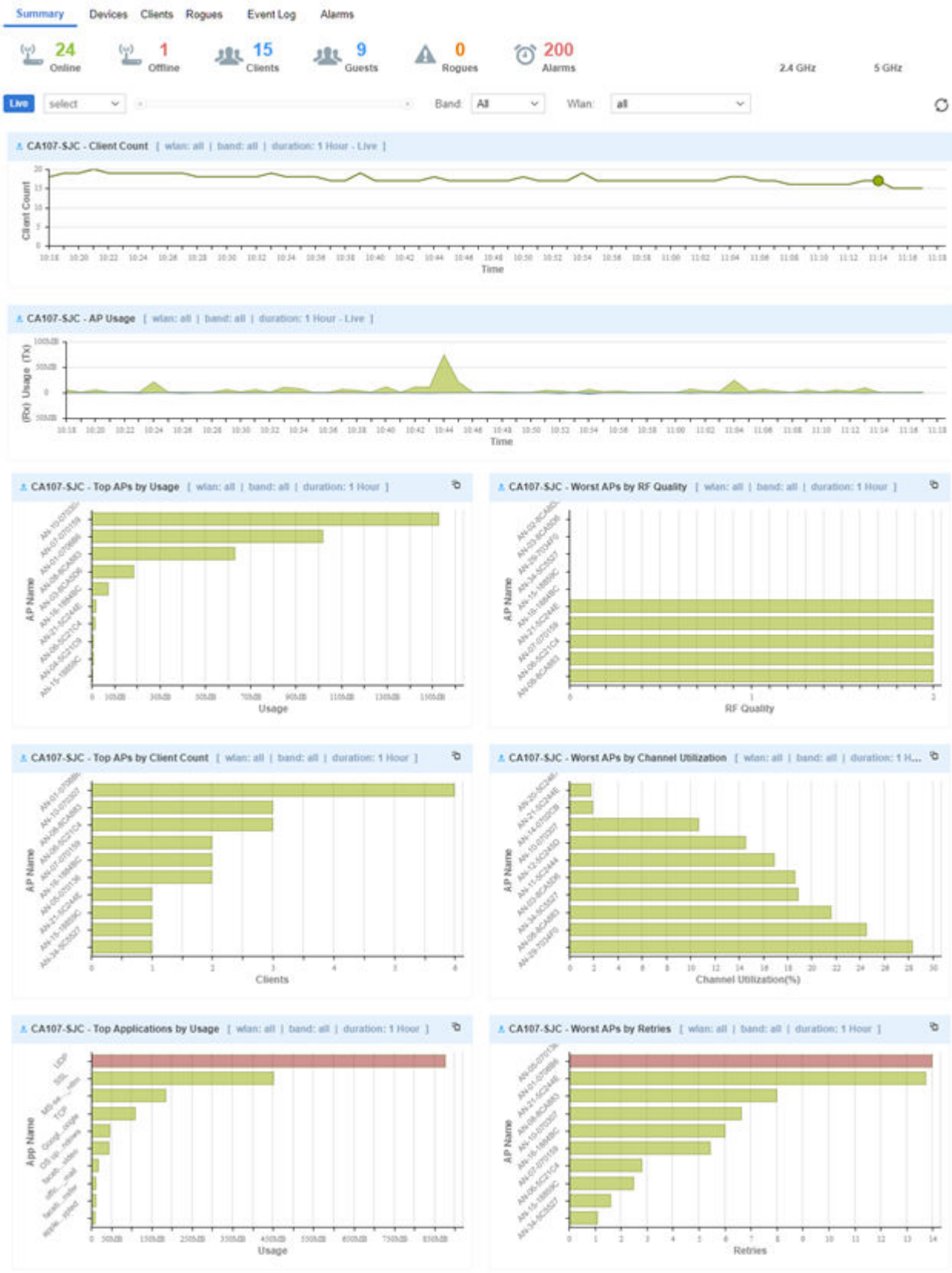


Figure 14: Extreme NSight > Monitor > Summary (Site Level)

Devices

To view a summary of all APs and devices:

1 Select **Monitor** from the upper menu bar.
2 In the menu bar select **Devices**.

The Devices screen displays.

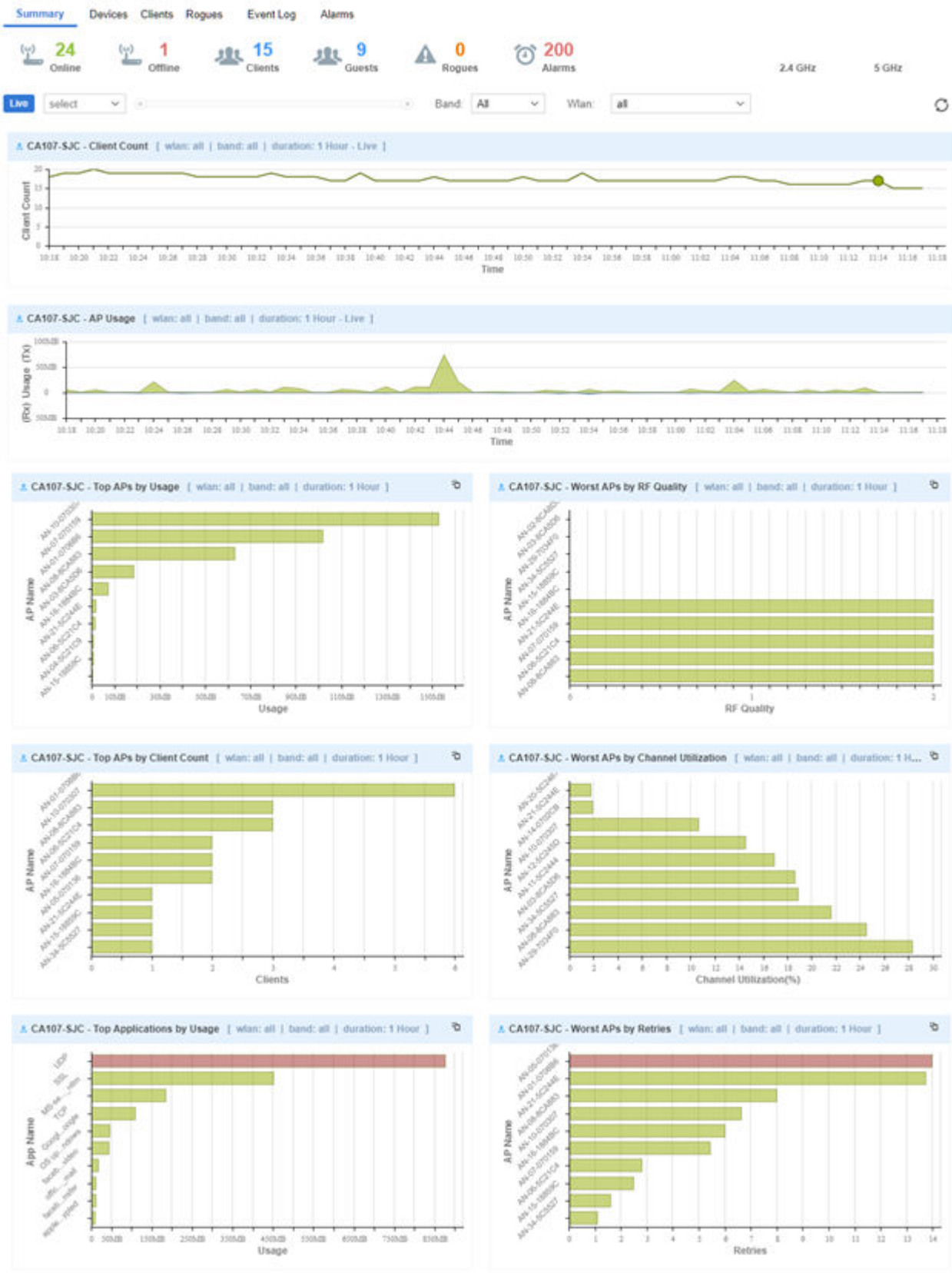


Figure 15: Extreme NSight > Monitor > Devices Screen

Device Details

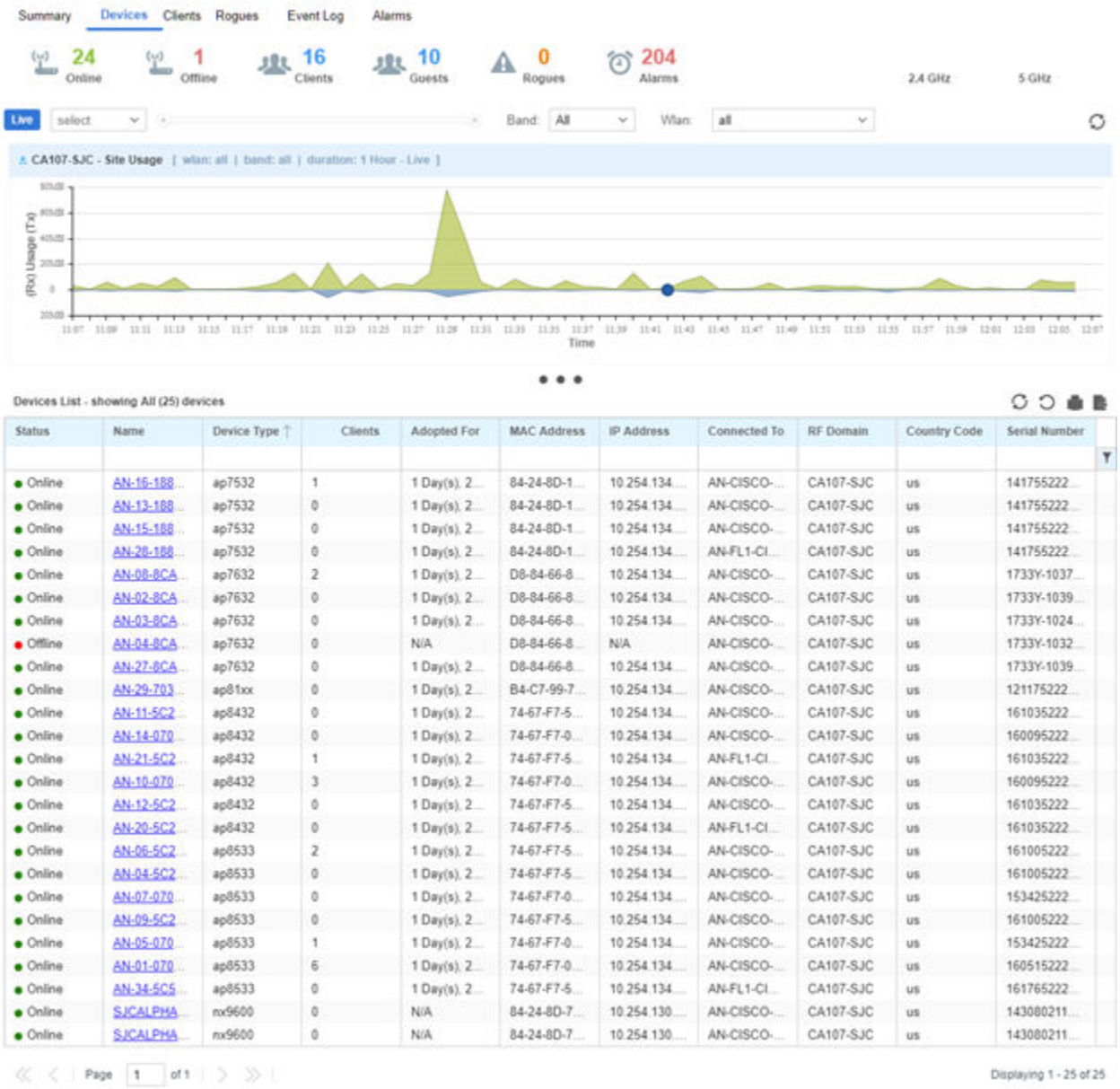


Figure 16: Extreme NSight > Monitor > Device Details Screen

To view details of a specific Extreme NSight managed device:

1 Select **Monitor** from the upper menu bar.

2 In the menu bar select **Devices**.

3 Select the **Name** of a specific device from the **Devices Summary** table to view device details.

4 Select **Live** to view the current device details in real time. Use the pull-down menu or the sliders to specify a time period to display device data from.

5 After selecting a time period use the **Band** pull-down menu to select the RF band(s) to display device details for. Details can be displayed for **All**, **2.4GHz** or **5GHz**.
6 After selecting a time period and band use the **WLAN** pull-down menu to select the wireless LAN to display device details for. Details can be displayed for All WLANs or a specific WLAN.
7 The **Total Usage** graph at the top of the screen displays total device usage over the specified time period with transmitted data, Tx, in blue and received data, Rx, in green
8 The **Details** section displays information known about the device as well as a site map, if available, showing which Access Point the device is communicating with.

Clients

To view a summary of all client devices:

1 Select **Monitor** from the upper menu bar.
2 In the Left Nav select **Clients**.

The **Clients** screen displays.

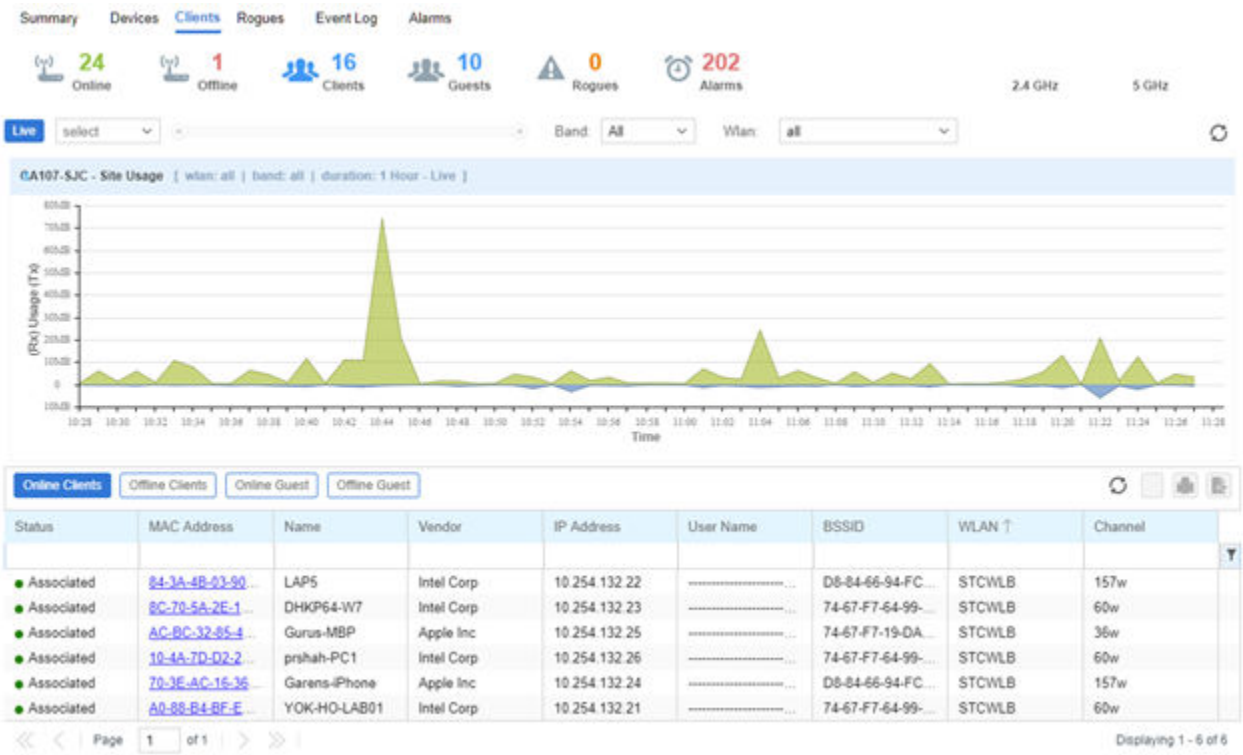


Figure 17: Extreme NSight > Monitor > Clients Screen

Client Details

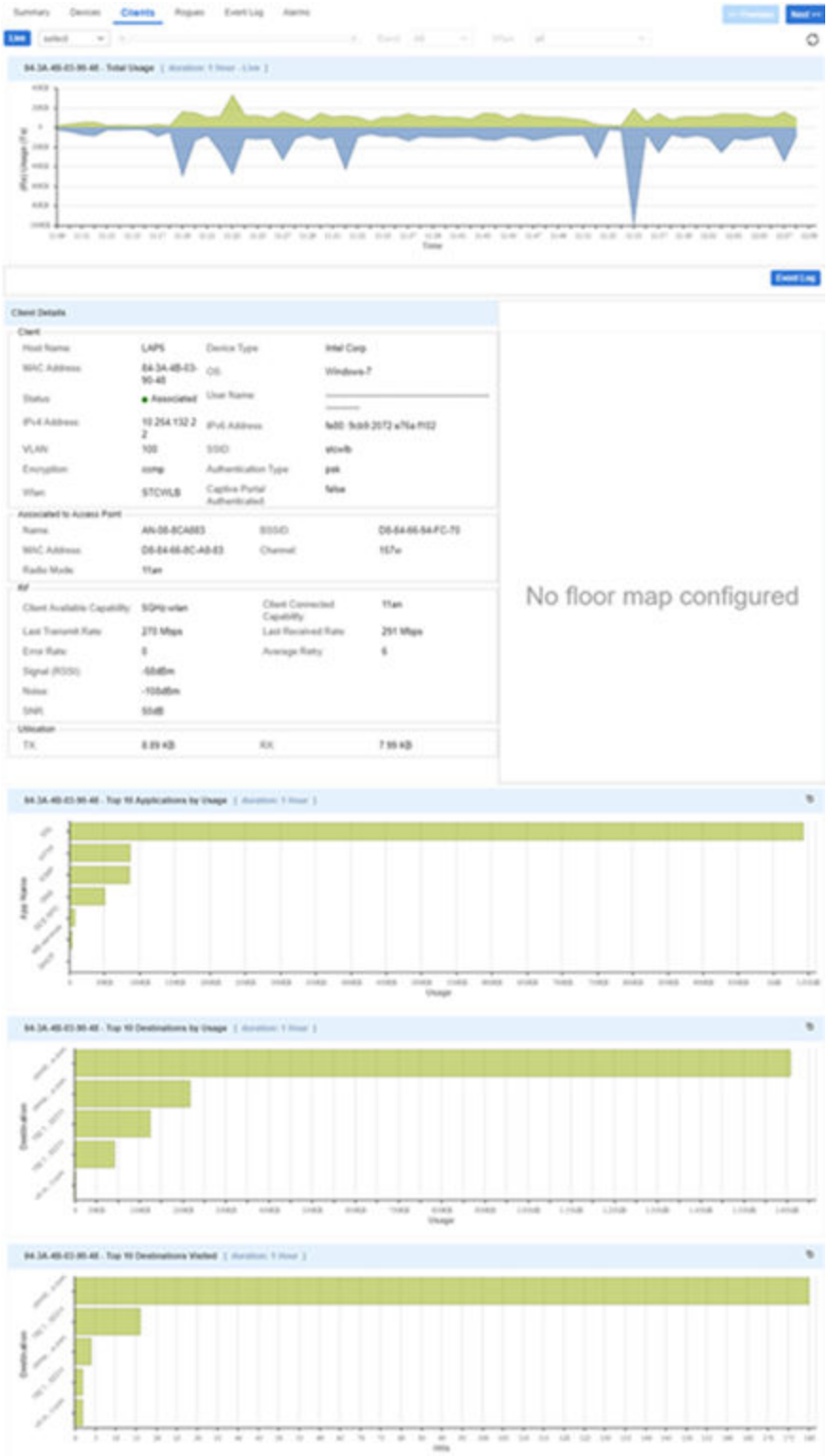


Figure 18: Extreme NSight > Monitor > Client Details Screen

To view details of a NSight managed client:

1 Select **Monitor** from the upper menu bar.
2 In the Left Nav select **Clients**.

   The clients screen displays.
3 From the list of clients select the **MAC Address** of a client to load its client details.
4 Select **Live** to view the current client details in real time. Use the pull-down menu or the sliders to specify a time period to client data from.
5 After selecting a time period use the **Band** pull-down menu to select the RF band(s) to display client details for. Details can be displayed for **All**, **2.4GHz** or **5GHz**.
6 The **Total Usage** graph at the top of the screen displays total client usage over the specified time period with transmitted data, Tx, in blue and received data, Rx, in green.
7 The **Client Details** section displays information known about the client as well as a site map, if available, showing which Access Point the client is communicating with.

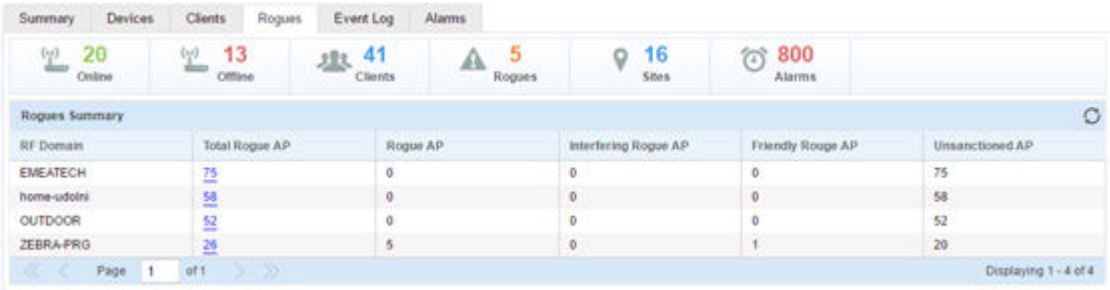
Rogues

Rogue devices are those devices detected in a sanctioned radio coverage area but have not been deployed by the Extreme NSight administrator as a known device.

To view a summary of all rogue APs:

1 Select **Monitor** from the upper menu bar.
2 In the Left Nav select **Rogues**.

   The Rogue APs screen displays.



3 Review the following rogue device information as detected within the Extreme NSight managed network:

Status	Displays the online status of each client. If a device is online, it displays a green checkmark. If the device is offline, it displays a red "X".
BSSID	Displays the *Broadcast Service Set ID (BSSID)* used for matching and filtering.
Vendor	Lists the manufacturer of the detected Access Point as an additional means of assessing its potential threat to the members of this RF Domain.
SSID	Displays the *Service Set ID* (SSID) of the network to which the detected Access Point belongs.
Signal Strength	Displays the signal strength of the detected Access Point. Use this variable to help determine whether a device connection would improve network coverage or add noise.
First Seen	Provides a timestamp when the detected Access Point was first detected by a RF Domain member device.

Top Reporter	Lists the administrator assigned hostname of the top performing RF Domain member detecting the listed Access Point MAC address. Consider this top performer the best resource for information on the detected Access Point and its potential threat.
RF Domain	Displays the RF Domain which the rogue device is associated to.
Reason	Displays the system assigned reason the Access Point is marked as rogue.

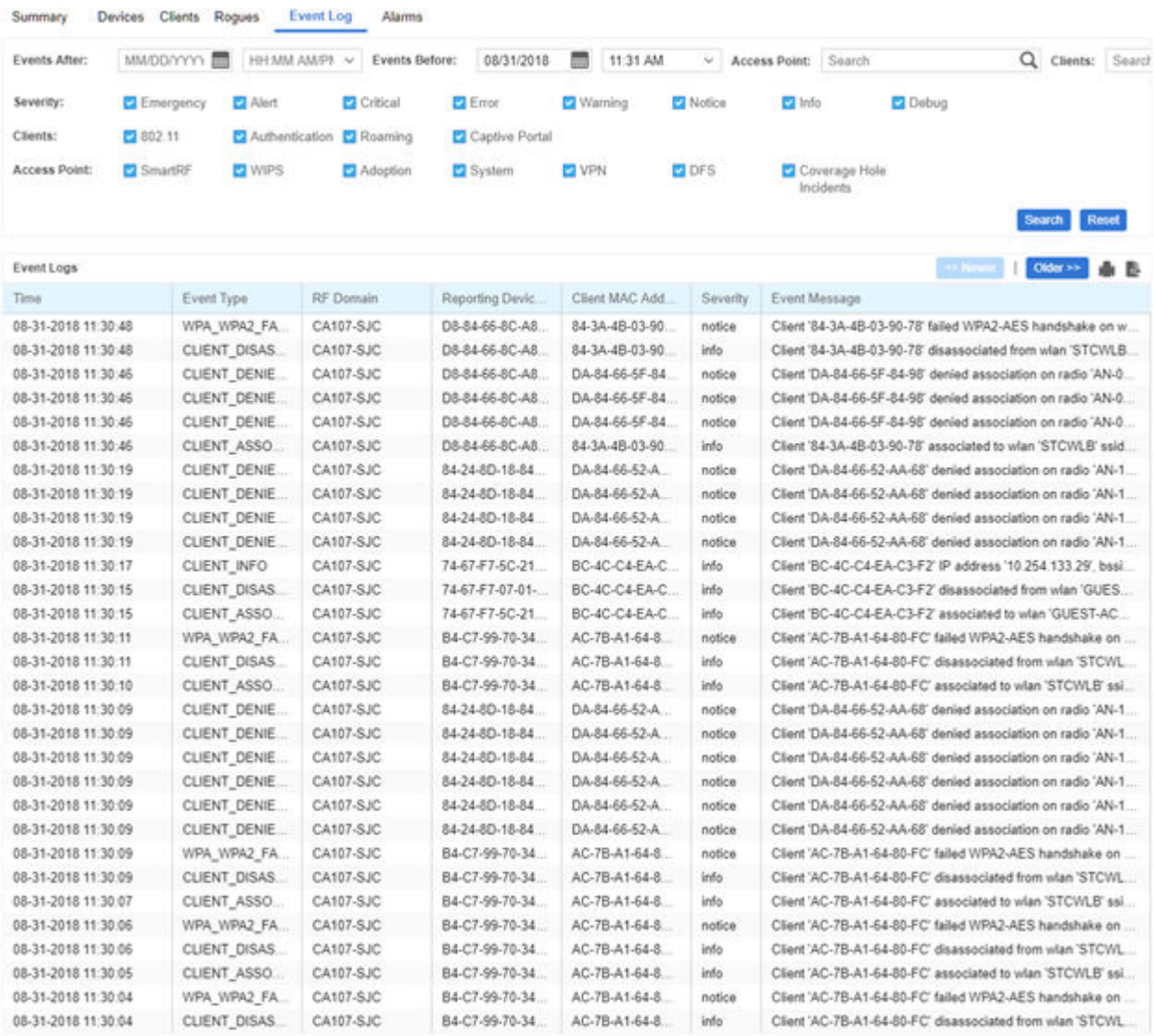
Event Log

The Event Log provides customizable access to network statistics and log information which can be used by network administrators to troubleshoot connectivity or other network issues. The Event Log screen filters information by time, Access Points or clients and allows searching for specific Access Points or Clients to see log information specific to those devices.

To view customizable log information:

1 Select **Monitor** from the upper menu bar.
2 In the Left Nav select **Event Log** from the menu

Event Log information specific to the selected item displays.



Events After: MM/DD/YYYY HH:MM AM/PM Events Before: 08/31/2018 11:31 AM Access Point: Search Clients: Search

Severity: ☑ Emergency ☑ Alert ☑ Critical ☑ Error ☑ Warning ☑ Notice ☑ Info ☑ Debug

Clients: ☑ 802.11 ☑ Authentication ☑ Roaming ☑ Captive Portal

Access Point: ☑ SmartRF ☑ WIPS ☑ Adoption ☑ System ☑ VPN ☑ DFS ☑ Coverage Hole Incidents

Event Logs

Time	Event Type	RF Domain	Reporting Devic...	Client MAC Add...	Severity	Event Message
08-31-2018 11:30:48	WPA_WPA2_FA...	CA107-SJC	D8-84-66-8C-A8...	84-3A-4B-03-90...	notice	Client '84-3A-4B-03-90-78' failed WPA2-AES handshake on w...
08-31-2018 11:30:48	CLIENT_DISAS...	CA107-SJC	D8-84-66-8C-A8...	84-3A-4B-03-90...	info	Client '84-3A-4B-03-90-78' disassociated from wlan 'STCWLB...
08-31-2018 11:30:46	CLIENT_DENIE...	CA107-SJC	D8-84-66-8C-A8...	DA-84-66-5F-84...	notice	Client 'DA-84-66-5F-84-98' denied association on radio 'AN-0...
08-31-2018 11:30:46	CLIENT_DENIE...	CA107-SJC	D8-84-66-8C-A8...	DA-84-66-5F-84...	notice	Client 'DA-84-66-5F-84-98' denied association on radio 'AN-0...
08-31-2018 11:30:46	CLIENT_DENIE...	CA107-SJC	D8-84-66-8C-A8...	DA-84-66-5F-84...	notice	Client 'DA-84-66-5F-84-98' denied association on radio 'AN-0...
08-31-2018 11:30:46	CLIENT_ASSO...	CA107-SJC	D8-84-66-8C-A8...	84-3A-4B-03-90...	info	Client '84-3A-4B-03-90-78' associated to wlan 'STCWLB' ssid...
08-31-2018 11:30:19	CLIENT_DENIE...	CA107-SJC	84-24-8D-18-84...	DA-84-66-52-A...	notice	Client 'DA-84-66-52-AA-68' denied association on radio 'AN-1...
08-31-2018 11:30:19	CLIENT_DENIE...	CA107-SJC	84-24-8D-18-84...	DA-84-66-52-A...	notice	Client 'DA-84-66-52-AA-68' denied association on radio 'AN-1...
08-31-2018 11:30:19	CLIENT_DENIE...	CA107-SJC	84-24-8D-18-84...	DA-84-66-52-A...	notice	Client 'DA-84-66-52-AA-68' denied association on radio 'AN-1...
08-31-2018 11:30:19	CLIENT_DENIE...	CA107-SJC	84-24-8D-18-84...	DA-84-66-52-A...	notice	Client 'DA-84-66-52-AA-68' denied association on radio 'AN-1...
08-31-2018 11:30:17	CLIENT_INFO	CA107-SJC	74-67-F7-5C-21...	BC-4C-C4-EA-C...	info	Client 'BC-4C-C4-EA-C3-F2' IP address '10.254.133.29', bssi...
08-31-2018 11:30:15	CLIENT_DISAS...	CA107-SJC	74-67-F7-07-01-...	BC-4C-C4-EA-C...	info	Client 'BC-4C-C4-EA-C3-F2' disassociated from wlan 'GUES...
08-31-2018 11:30:15	CLIENT_ASSO...	CA107-SJC	74-67-F7-5C-21...	BC-4C-C4-EA-C...	info	Client 'BC-4C-C4-EA-C3-F2' associated to wlan 'GUEST-AC...
08-31-2018 11:30:11	WPA_WPA2_FA...	CA107-SJC	B4-C7-99-70-34...	AC-7B-A1-64-8...	notice	Client 'AC-7B-A1-64-80-FC' failed WPA2-AES handshake on ...
08-31-2018 11:30:11	CLIENT_DISAS...	CA107-SJC	B4-C7-99-70-34...	AC-7B-A1-64-8...	info	Client 'AC-7B-A1-64-80-FC' disassociated from wlan 'STCWL...
08-31-2018 11:30:10	CLIENT_ASSO...	CA107-SJC	B4-C7-99-70-34...	AC-7B-A1-64-8...	info	Client 'AC-7B-A1-64-80-FC' associated to wlan 'STCWLB' ssi...
08-31-2018 11:30:09	CLIENT_DENIE...	CA107-SJC	84-24-8D-18-84...	DA-84-66-52-A...	notice	Client 'DA-84-66-52-AA-68' denied association on radio 'AN-1...
08-31-2018 11:30:09	CLIENT_DENIE...	CA107-SJC	84-24-8D-18-84...	DA-84-66-52-A...	notice	Client 'DA-84-66-52-AA-68' denied association on radio 'AN-1...
08-31-2018 11:30:09	CLIENT_DENIE...	CA107-SJC	84-24-8D-18-84...	DA-84-66-52-A...	notice	Client 'DA-84-66-52-AA-68' denied association on radio 'AN-1...
08-31-2018 11:30:09	CLIENT_DENIE...	CA107-SJC	84-24-8D-18-84...	DA-84-66-52-A...	notice	Client 'DA-84-66-52-AA-68' denied association on radio 'AN-1...
08-31-2018 11:30:09	CLIENT_DENIE...	CA107-SJC	84-24-8D-18-84...	DA-84-66-52-A...	notice	Client 'DA-84-66-52-AA-68' denied association on radio 'AN-1...
08-31-2018 11:30:09	CLIENT_DENIE...	CA107-SJC	84-24-8D-18-84...	DA-84-66-52-A...	notice	Client 'DA-84-66-52-AA-68' denied association on radio 'AN-1...
08-31-2018 11:30:09	WPA_WPA2_FA...	CA107-SJC	B4-C7-99-70-34...	AC-7B-A1-64-8...	notice	Client 'AC-7B-A1-64-80-FC' failed WPA2-AES handshake on ...
08-31-2018 11:30:09	CLIENT_DISAS...	CA107-SJC	B4-C7-99-70-34...	AC-7B-A1-64-8...	info	Client 'AC-7B-A1-64-80-FC' disassociated from wlan 'STCWL...
08-31-2018 11:30:07	CLIENT_ASSO...	CA107-SJC	B4-C7-99-70-34...	AC-7B-A1-64-8...	info	Client 'AC-7B-A1-64-80-FC' associated to wlan 'STCWLB' ssi...
08-31-2018 11:30:06	WPA_WPA2_FA...	CA107-SJC	B4-C7-99-70-34...	AC-7B-A1-64-8...	notice	Client 'AC-7B-A1-64-80-FC' failed WPA2-AES handshake on ...
08-31-2018 11:30:06	CLIENT_DISAS...	CA107-SJC	B4-C7-99-70-34...	AC-7B-A1-64-8...	info	Client 'AC-7B-A1-64-80-FC' disassociated from wlan 'STCWL...
08-31-2018 11:30:05	CLIENT_ASSO...	CA107-SJC	B4-C7-99-70-34...	AC-7B-A1-64-8...	info	Client 'AC-7B-A1-64-80-FC' associated to wlan 'STCWLB' ssi...
08-31-2018 11:30:04	WPA_WPA2_FA...	CA107-SJC	B4-C7-99-70-34...	AC-7B-A1-64-8...	notice	Client 'AC-7B-A1-64-80-FC' failed WPA2-AES handshake on ...
08-31-2018 11:30:04	CLIENT_DISAS...	CA107-SJC	B4-C7-99-70-34...	AC-7B-A1-64-8...	info	Client 'AC-7B-A1-64-80-FC' disassociated from wlan 'STCWL...

Figure 19: Extreme NSight > Monitor > Event Log Screen

The **Event Log** screen is divided into a filters section, at the top of the page, and a log section on the lower half of the screen.

3 Select the desired filters from the following to customize the **Event Log** information displayed:

Events Before	Use the date field and the time pull-down menu to specify a date and time data collection interval for event data collection.
Access Point (Search)	Enter a search string to limit the data displayed in the event logs to Access Points whose event log entries match the search string.
Clients (Search)	Enter a search string to limit the data displayed in the event logs to clients whose event log entries match the search string.
Clients: 802.11	Select to include client 802.11 entries in the log entries displayed.
Clients: Authentication	Select to include client authentication entries in the log entries displayed.

Clients: Roaming	Select to include client roaming entries in the log entries displayed.
Access Points: Smart RF	Select to include Access Point Smart RF entries in the log entries displayed. Smart RF events are those Access Point radio and channel compensations made for failed or poorly performing peer Access Points in the same radio coverage area.
Access Points: WIPS	Select to include Access Point *Wireless Intrusion Protection System* (WIPS) entries in the log entries displayed
Access Points: Adoption	Select to include Access Point adoption entries in the log entries displayed.
Access Points: System	Select to include Access Point System entries in the log entries displayed.
Access Points: VPN	Select to include Access Point *Virtual Private Networking* (VPN) entries in the log entries displayed.
Access Points: DFS	Select to include Access Point DFS entries in the log entries displayed.

4 When the desired filters and devices are selected, select **Search** to populate the **Event Logs**.

5 The **Event Logs** table displays the following log information:

Time	Displays the timestamp (in the browser's timezone) when each log entry was created.
Event Type	Displays the message type displayed in the event log table.
RF Domain	Displays the log originator's RF Domain membership.
AP MAC	Displays the hardware encoded MAC address of the Access Point associated with each event message.
Client MAC	Displays the hardware encoded MAC address of the client associated with each event message.
Severity	Lists the severity for each analytic event. Severity levels include 0 - *Emergency*, 1 - *Alert*, 2 - *Critical,* 3 - *Errors*, 4 - *Warning*, 5 - *Notice*, 6 - *Info* and 7 - *Debug*.
Event Message	Displays error or status messages for each event listed. Use the message text as an additional means of assessing an event's potential impact to the system.

6 To scroll through multiple pages of log information, select **<< Newer** or **Older >>** from the upper right corner of the table.

Alarms

Alarms are part of the Extreme NSight fault management subsystem. Alarms are for monitoring, detecting, isolating, notifying and correcting faults encountered in the network.

Note
With alarms, thresholds are set to trigger the alarm condition. This is different then events, which are enabled/disabled and raised without a defined threshold being exceeded and a rate limit logic.

A consolidated summary of alarms (in the form of graphs and charts) is available in the Dashboard. Users can drill down into the graphs and charts to review granular alarm details and their history.

The Alarms screen displays a list of all triggered alarms with the newest alarms displaying at the top by default.

To view alarm information:

1 Select **Monitor** from the upper menu bar.
2 In the Left Nav select **Alarms**.

Figure 20: Extreme NSight > Monitor > Alarms Screen

The most recent 30 alarms display.

3 Refer to the following alarm information:

RFD Name	Displays the RF Domain name whose member devices the alarm is associated with.
Active Alarms	Displays the number of enabled alarms associated with each RF Domain.
Severity	Use the drop-down menu to specify a severity at which the alarm is triggered. Severity options and colors include: **Critical** - Immediate action needed (red) **Major** - Action needed as soon as possible (orange) **Minor** - Watch the situation carefully (yellow) **Clear** - Moves an alarm from an active (raised alarm state) to a cleared state.
Critical Alarm	Displays the number of critical level alarms associated with each RF Domain in red. Critical alarms require immediate action.
Major Alarm	Displays the number of major level alarms associated with each RF Domain in orange. Major alarms require action as soon as possible.
Minor Alarm	Displays the number of minor level alarms associated with each RF Domain in yellow. Minor alarms do not require immediate action, but should be watched closely.
Impacted Devices	Displays the number of devices in the associated RF Domain impacted by the **Critical Alarm**, **Major Alarm** and **Minor Alarm**.

4 Selecting a **Critical Alarm**, **Major Alarm** or **Minor Alarm** loads a details screen showing detailed information about the alarm, including the **Hostname**, **IP Address**,**MAC Address** and **Raised Time**. This screen also allows the user to acknowledge the alarm status.

Filtering Alarm Data

At the top of each alarm column is a text field. Entering a keyword or string into one of these fields filters the alarm data and only displays entries matching the keyword or string. For example, entering the Major in the **Severity** column displays only alarm entries that match the Major severity. Entering keywords or strings in multiple columns will further filter the data displayed.

7 Reports

The Reports screen provides report generation and viewing tools in six categories. Reports can be run manually or scheduled to run at a certain time or at a certain interval. Reports can be sent to the screen for viewing or sent via E-mail.

Generated Reports

The Generated Reports tab displays manually generated and scheduled report output.

To view report information:

1 Select **Reports** from the upper menu bar.
2 In the Left Nav select **System** or a specific geographical location or site.
3 Select the **Generated Reports** tab.

The Reports screen is separated into **Generated Reports, Manage Reports** and **Scheduled Reports**. **Generated Reports** displays reports created manually or already run according to schedule.

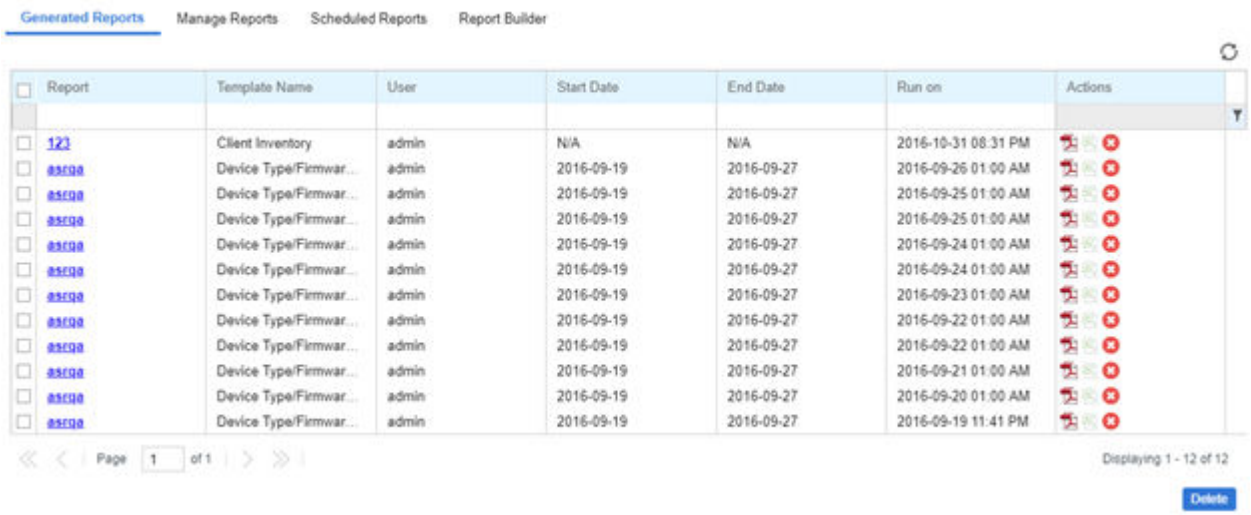


Figure 21: Extreme NSight > Reports > Generated Reports Screen

The **Generated Reports** table displays the following information about each generated report:

Report Displays the user configured report name for each scheduled report.

Category
Displays the report category for each generated report. The categories are:
- **Device Type / Firmware Summary**
- **Device Summary**
- **Client Inventory**
- **PCI (3.1) Report**
- **Network Usage**
- **RF Health**

User
Displays the name of the user that generated the report.

Start Date
Lists each report's compilation start time. Report information is gathered from this time through the listed end date.

End Date
Lists each report's compilation end time. Information is not longer trended and reported after this date, so ensure the trending period is long enough to apply significance to the report data.

Actions
Select the report output best suited to your reporting needs. Options include:
- **PDF**: Generates a PDF containing the select alarm details.
- **CSV**: Generates a *Comma Separated Values* (CSV) file containing the selected alarm details.
- **Delete**: Selecting "X" will delete the selected alarm from the generated report.

Manage Reports

Use the **Manage Reports** tab to manually generate and schedule reports. Existing scheduled reports can be edited within this tab.

To view report information:

1 Select **Reports** from the upper menu bar.
2 In the Left Nav select **System** or a specific geographical location or site.
3 Select the **Manage Reports** tab.

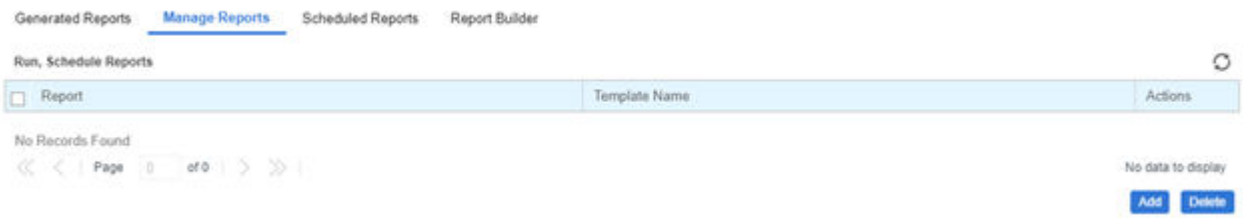


Figure 22: Extreme NSight > Reports > Manage Reports Screen

4 The **Manage Reports** table displays the following information about each generated report:

Report
Displays the user configured report name for each managed report.

Category
Displays the report category for each managed report. The categories are:
- **Device Type / Firmware Summary**
- **Device Summary**
- **Client Inventory**

- **PCI Report**
- **Network Usage**
- **RF Health**

Selecting the **Category** column allows sorting reports by category and customizing the **Columns** available.

Options Displays the report options selected and utilized for each listed report.

5 To add a **Managed Report** select **Add** and configure the following:

Title Enter a descriptive title for the report. This is the report name that displays in the **Manage Reports** and **Generated Reports** screen.

Type Select a report type from the pull-down menu. Available report types are:

- **Device Type / Firmware Summary**
- **Device Summary**
- **Client Inventory**
- **PCI Report**
- **Network Usage**
- **RF Health**

Scope Type Select **System** or **Site Group** to specify where the report will be run. This is used in conjunction with **Scope** to customize report information.

Scope If **System** is selected, optionally use the pull-down menu to specify an RF Domain for the report to be run on. Leaving System selected will run the report on the entire system. If **Site Group** is selected use the pull-down menu to specify a site group for the report to run on.

Period Select a time period for report data from the pull-down menu. Available time period options are:

- **Last Hour**
- **Last Week**
- **Last Month**
- **Custom**

When **Custom** is selected specify a **Start Date** and **Time** and an **End Date** and **Time** for the report range.

Schedule Select **Schedule** to enable the report to be run at specific intervals. When **Schedule** is enabled, specify a **Start Date** and **End Date** and specify the frequency in the **Recurrence** field.

Recurrence When **Schedule** is enabled specify the interval the report should be run. Reports can be run Daily, Weekly or Monthly. When using Weekly or Monthly specify the day of the week or day of the month the report will run. Specify th time of day that the report should run.

Format Select one or more report output formats. Reports can be output in PDF format or *Comma Seperated Values* (CSV) format. Both formats may be selected simultaneously.

Destination Specify where the report will be stored. The report can be stored on the server, or stored on the server and e-mailed to a specific address. When using e-mail, specify the e-mail address for the recipient.

Scheduled Reports

To view report information:

1 Select **Reports** from the upper menu bar.

2 In the Left Nav select **System** or a specific geographical location or site.

3 Select the **Scheduled Reports** tab.

Scheduled Reports have been configured to run at a scheduled date and time.

Figure 23: Extreme NSight > Reports > Scheduled Reports Screen

The **Scheduled Reports** table displays the following information about each generated report:

Report	Displays the user configured report name for each generated report.
Type	Displays the report category for each scheduled report. The categories are: • **Device Type / Firmware Summary** • **Device Summary** • **Client Inventory** • **PCI Report** • **Network Usage** • **RF Health**
Subject	Displays the user configured subject line for scheduled E-mail reports.
User	Displays the name of the administrator generating the report.
Start Date	Lists each report's compilation start time. Report information is gathered from this time through the listed end date.
End Date	Lists each report's compilation end time. Information is no longer trended and reported after this date, so ensure the trending period is long enough to apply significance to the report data.
Frequency	Displays the frequency in days, hours and minutes each report is scheduled to run.
Actions	Selecting "X" will delete the selected alarm from the generated reports.

Report Builder

To view report information:

1 Select **Reports** from the upper menu bar.
2 In the Left Nav select **System** or a specific geographical location or site.
3 Select the **Report Builder** tab.

The **Report Builder** tab displays a list of **Report Templates**

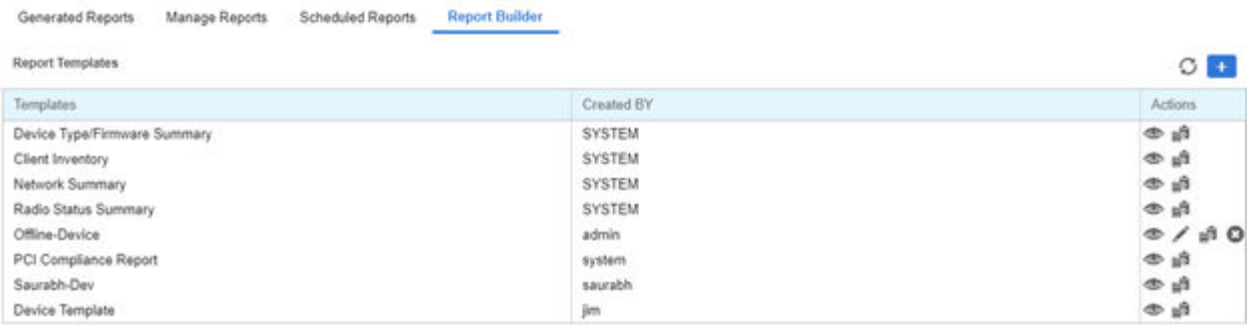


Figure 24: Extreme NSight > Reports > Report Builder Screen

.

The Report Builder table displays the following information :

Templates	Displays the name of each configured report template. To edit the title of of a template select the Edit Reports Template button associated with that report.
Created By	Displays the user that created each report template. Templates created by the system can be viewed and copied, but man not be edited or deleted.
Actions	Displays a series of buttons to view, edit, copy or delete each report template. Templates created by the system can be viewed and copied, but man not be edited or deleted.

4 Select the **View Report Template** button to open a read only view of the associated report template.

The report template screen displays the type of data displayed, the report name and all associated **Report Object Types**. To make changes to a report template select **Edit Report Template**.

5 Select the **Edit Report Template** button to modify the associated report template.

The following values may be modified on the report template screen:

Public	Select **Public** to make the report template available to all users on the system.
Report Name	Specify a unique Report Name used to identify each report template.
Report Object Types	Drag and drop each object you wish to include in the report template. The data associated with the that object will appear in the report in the order that they are listed. Report objects are separated into the following categories: Device, RF, Network, Utilization, Client and Application Visibility.

6 To create a new report template based on an existing template select the **Copy Report Template** button next to the report template you wish to copy. A report template window opens with the same values of the report template it was copied from. Modify any values you wish to edit, create a new **Report Name** and select **Save**.

7 To create a report template from scratch select the **+** in the upper right of the **Report Templates** section.

8 Tools

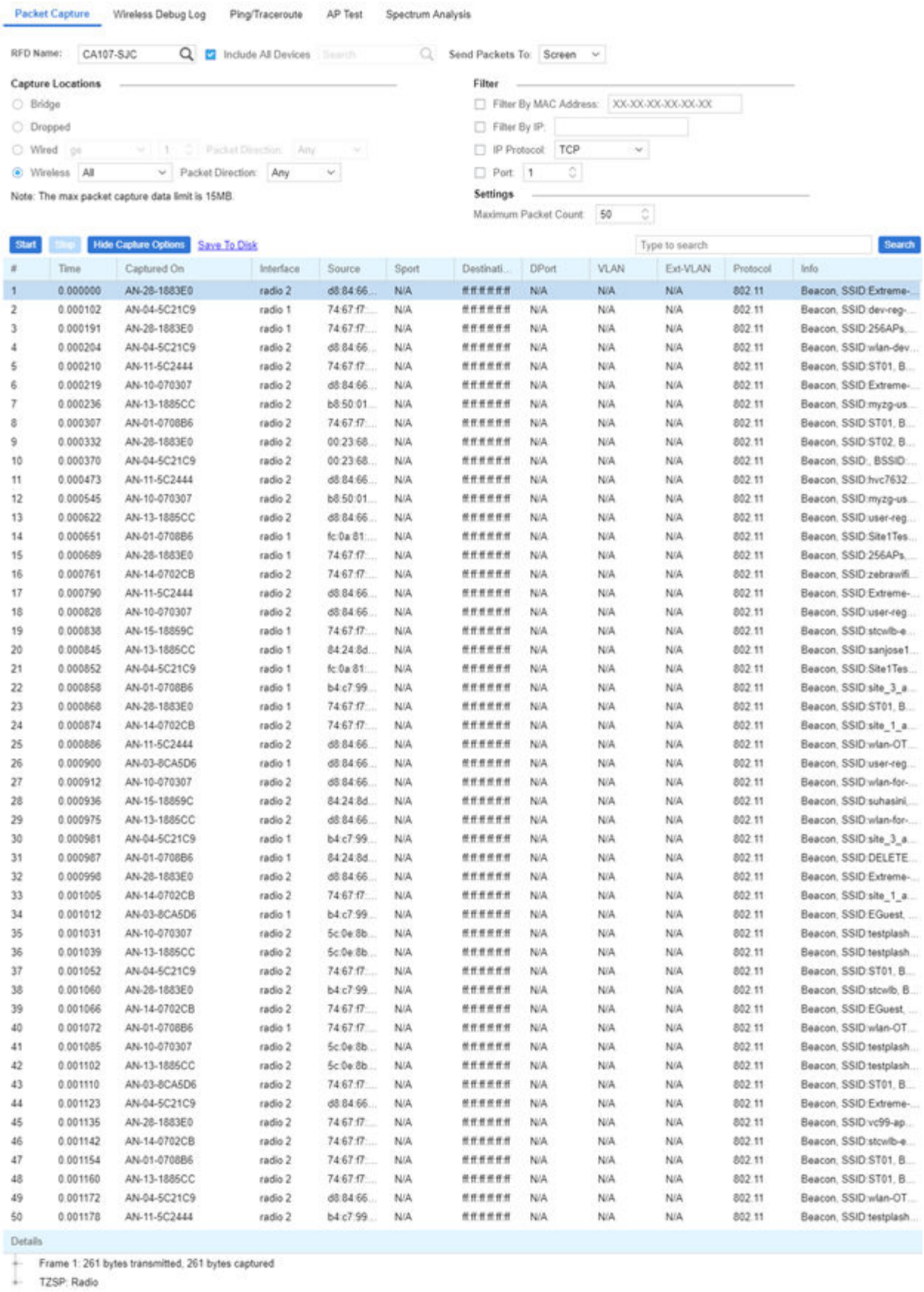
The Tools screen provides network troubleshooting tools to help diagnose connectivity and quality issues on the managed network. The Tools screen provides tools for packet capture, wireless debugging, ping and traceroute.

Packet Capture

Periodically launch the packet capture tool to save capture information on a local file to share with the those interested parties looking into a specific issue.

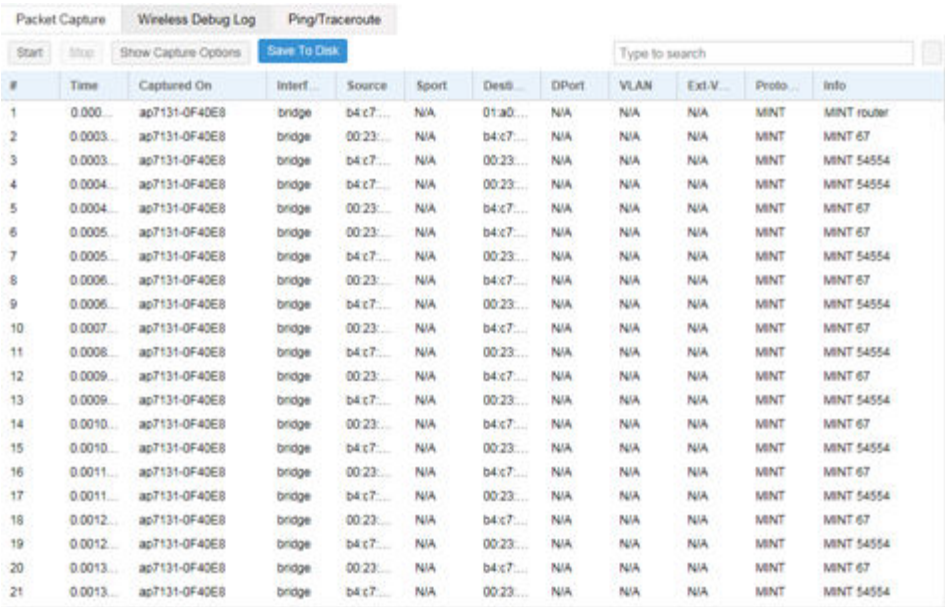
To access Packet Capture:

1 Select Tools from the upper menu bar.
2 Select the Packet Capture tab.


Packet Capture
Wireless Debug Log
Ping/Traceroute
AP Test
Spectrum Analysis
RFD Name: CA107-SJC
Include All Devices
Search
Send Packets To: Screen
Capture Locations
Bridge
Dropped
Wired
Packet Direction: Any
Wireless All
Packet Direction: Any
Note: The max packet capture data limit is 15MB.
Filter
Filter By MAC Address: XX-XX-XX-XX-XX-XX
Filter By IP:
IP Protocol: TCP
Port: 1
Settings
Maximum Packet Count: 50
Start
Stop
Hide Capture Options
Save To Disk
Type to search
Search
Time Captured On Interface Source Sport Destinati... DPort VLAN Ext-VLAN Protocol Info
1 0.000000 AN-28-1883E0 radio 2 d8:84:66... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:Extreme-...
2 0.000102 AN-04-5C21C9 radio 1 74:67:f7:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:dev-reg-...
3 0.000191 AN-28-1883E0 radio 1 74:67:f7:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:256APs,...
4 0.000204 AN-04-5C21C9 radio 2 d8:84:66... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:wlan-dev...
5 0.000210 AN-11-5C2444 radio 2 74:67:f7:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:ST01, B...
6 0.000219 AN-10-070307 radio 2 d8:84:66... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:Extreme-...
7 0.000236 AN-13-1885CC radio 2 b8:50:01... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:myzg-us...
8 0.000307 AN-01-0708B6 radio 2 74:67:f7:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:ST01, B...
9 0.000332 AN-28-1883E0 radio 2 00:23:68... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:ST02, B...
10 0.000370 AN-04-5C21C9 radio 2 00:23:68... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:, BSSID:...
11 0.000473 AN-11-5C2444 radio 2 d8:84:66... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:hvc7632...
12 0.000545 AN-10-070307 radio 2 b8:50:01... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:myzg-us...
13 0.000622 AN-13-1885CC radio 2 d8:84:66... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:user-reg...
14 0.000651 AN-01-0708B6 radio 1 fc:0a:81:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:Site1Tes...
15 0.000689 AN-28-1883E0 radio 1 74:67:f7:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:256APs,...
16 0.000761 AN-14-0702CB radio 2 74:67:f7:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:zebrawifi...
17 0.000790 AN-11-5C2444 radio 2 d8:84:66... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:Extreme-...
18 0.000828 AN-10-070307 radio 2 d8:84:66... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:user-reg...
19 0.000838 AN-15-18859C radio 1 74:67:f7:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:stcwlb-e...
20 0.000845 AN-13-1885CC radio 1 84:24:8d... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:sanjose1...
21 0.000852 AN-04-5C21C9 radio 1 fc:0a:81:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:Site1Tes...
22 0.000858 AN-01-0708B6 radio 1 b4:c7:99... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:site_3_a...
23 0.000868 AN-28-1883E0 radio 1 74:67:f7:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:ST01, B...
24 0.000874 AN-14-0702CB radio 2 74:67:f7:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:site_1_a...
25 0.000886 AN-11-5C2444 radio 2 d8:84:66... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:wlan-OT...
26 0.000900 AN-03-8CA5D6 radio 1 d8:84:66... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:user-reg...
27 0.000912 AN-10-070307 radio 2 d8:84:66... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:wlan-for-...
28 0.000936 AN-15-18859C radio 2 84:24:8d... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:suhasini,...
29 0.000975 AN-13-1885CC radio 2 d8:84:66... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:wlan-for-...
30 0.000981 AN-04-5C21C9 radio 1 b4:c7:99... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:site_3_a...
31 0.000987 AN-01-0708B6 radio 1 84:24:8d... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:DELETE...
32 0.000998 AN-28-1883E0 radio 2 d8:84:66... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:Extreme-...
33 0.001005 AN-14-0702CB radio 2 74:67:f7:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:site_1_a...
34 0.001012 AN-03-8CA5D6 radio 1 b4:c7:99... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:EGuest, ...
35 0.001031 AN-10-070307 radio 2 5c:0e:8b... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:testplash...
36 0.001039 AN-13-1885CC radio 2 5c:0e:8b... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:testplash...
37 0.001052 AN-04-5C21C9 radio 2 74:67:f7:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:ST01, B...
38 0.001060 AN-28-1883E0 radio 2 b4:c7:99... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:stcwlb, B...
39 0.001066 AN-14-0702CB radio 2 74:67:f7:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:EGuest, ...
40 0.001072 AN-01-0708B6 radio 1 74:67:f7:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:wlan-OT...
41 0.001085 AN-10-070307 radio 2 5c:0e:8b... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:testplash...
42 0.001102 AN-13-1885CC radio 2 5c:0e:8b... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:testplash...
43 0.001110 AN-03-8CA5D6 radio 2 74:67:f7:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:ST01, B...
44 0.001123 AN-04-5C21C9 radio 2 d8:84:66... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:Extreme-...
45 0.001135 AN-28-1883E0 radio 2 74:67:f7:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:vc99-ap...
46 0.001142 AN-14-0702CB radio 2 74:67:f7:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:stcwlb-e...
47 0.001154 AN-01-0708B6 radio 2 74:67:f7:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:ST01, B...
48 0.001160 AN-13-1885CC radio 2 74:67:f7:... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:ST01, B...
49 0.001172 AN-04-5C21C9 radio 2 d8:84:66... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:wlan-OT...
50 0.001178 AN-11-5C2444 radio 2 b4:c7:99... N/A ###### N/A N/A N/A 802.11 Beacon, SSID:testplash...
Details
Frame 1: 261 bytes transmitted, 261 bytes captured
TZSP: Radio

RFD Name	Lists the name of the RF Domain whose member devices are subject to the packet capture. RF Domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area, such as in a floor, building or site.
Include All Devices	Select this option to include all device types from the specified RF Domain.
Send Data To	Use the **Send Data To** drop-down menu to select where packet capture messages are archived. If Screen is selected, packet capture information is sent to the section at the bottom of the dialog window. If File is selected, the file location must be specified in the File Location section of the window.
Dropped	Select **Dropped** to create an event entry each time a packet is dropped from a client connected to a RF Domain member device. Use this information to assess whether a particular RF Domain is experiencing high levels of dropped packets that may require administration to distribute client connections more evenly.
Capture Location	Specify a **Capture Location** on a specific interface on the current RF Domain. Select **All Wired Interfaces** to capture packets from all wired interfaces. Selecting **Dropped** will only capture dropped packets. If **Wired** or **Wireless** is selected, specify the interface name and number and specify a **Packet Direction.**
Filter (MAC, IP, Protocol, Port)	Filter packet captures based on specific criteria. Select one or more of the following and specify the relevant information: • **Filter by MAC** • **Filter By IP** • **IP Protocol** • **Port**
Maximum Packet Count	Set the **Maximum Packet Count** to limit the number of packets captured for trending. Set this value between 1 - 4000 packets, with a default value of 200.

3 Select Start to begin the packet capture. Information sent to the screen displays in the lower portion of the window. If the data is being sent to a file, that file populates with the packet capture information. If you have set a long message capture duration and wish to end the capture early, select Stop.



#	Time	Captured On	Interf...	Source	Sport	Desti...	DPort	VLAN	Ext-V...	Proto...	Info
1	0.000...	ap7131-0F40E8	bridge	b4:c7:...	N/A	01:a0:...	N/A	N/A	N/A	MINT	MINT router
2	0.0003...	ap7131-0F40E8	bridge	00:23:...	N/A	b4:c7:...	N/A	N/A	N/A	MINT	MINT 67
3	0.0003...	ap7131-0F40E8	bridge	b4:c7:...	N/A	00:23:...	N/A	N/A	N/A	MINT	MINT 54554
4	0.0004...	ap7131-0F40E8	bridge	b4:c7:...	N/A	00:23:...	N/A	N/A	N/A	MINT	MINT 54554
5	0.0004...	ap7131-0F40E8	bridge	00:23:...	N/A	b4:c7:...	N/A	N/A	N/A	MINT	MINT 67
6	0.0005...	ap7131-0F40E8	bridge	00:23:...	N/A	b4:c7:...	N/A	N/A	N/A	MINT	MINT 67
7	0.0005...	ap7131-0F40E8	bridge	b4:c7:...	N/A	00:23:...	N/A	N/A	N/A	MINT	MINT 54554
8	0.0006...	ap7131-0F40E8	bridge	00:23:...	N/A	b4:c7:...	N/A	N/A	N/A	MINT	MINT 67
9	0.0006...	ap7131-0F40E8	bridge	b4:c7:...	N/A	00:23:...	N/A	N/A	N/A	MINT	MINT 54554
10	0.0007...	ap7131-0F40E8	bridge	00:23:...	N/A	b4:c7:...	N/A	N/A	N/A	MINT	MINT 67
11	0.0008...	ap7131-0F40E8	bridge	b4:c7:...	N/A	00:23:...	N/A	N/A	N/A	MINT	MINT 54554
12	0.0009...	ap7131-0F40E8	bridge	00:23:...	N/A	b4:c7:...	N/A	N/A	N/A	MINT	MINT 67
13	0.0009...	ap7131-0F40E8	bridge	b4:c7:...	N/A	00:23:...	N/A	N/A	N/A	MINT	MINT 54554
14	0.0010...	ap7131-0F40E8	bridge	00:23:...	N/A	b4:c7:...	N/A	N/A	N/A	MINT	MINT 67
15	0.0010...	ap7131-0F40E8	bridge	b4:c7:...	N/A	00:23:...	N/A	N/A	N/A	MINT	MINT 54554
16	0.0011...	ap7131-0F40E8	bridge	00:23:...	N/A	b4:c7:...	N/A	N/A	N/A	MINT	MINT 67
17	0.0011...	ap7131-0F40E8	bridge	b4:c7:...	N/A	00:23:...	N/A	N/A	N/A	MINT	MINT 54554
18	0.0012...	ap7131-0F40E8	bridge	00:23:...	N/A	b4:c7:...	N/A	N/A	N/A	MINT	MINT 67
19	0.0012...	ap7131-0F40E8	bridge	b4:c7:...	N/A	00:23:...	N/A	N/A	N/A	MINT	MINT 54554
20	0.0013...	ap7131-0F40E8	bridge	00:23:...	N/A	b4:c7:...	N/A	N/A	N/A	MINT	MINT 67
21	0.0013...	ap7131-0F40E8	bridge	b4:c7:...	N/A	00:23:...	N/A	N/A	N/A	MINT	MINT 54554

Figure 26: Capture Details

Wireless Debug Log

Detailed wireless device information can be obtained through debug logs retained by each Access Point. This information can disclose 802.11 protocol level errors that may be occurring yet not reported at other levels in a debug log.

To access Wireless Debug Logs:

1 Select Tools from the upper menu bar.
2 Select the Wireless Debug Log tab.

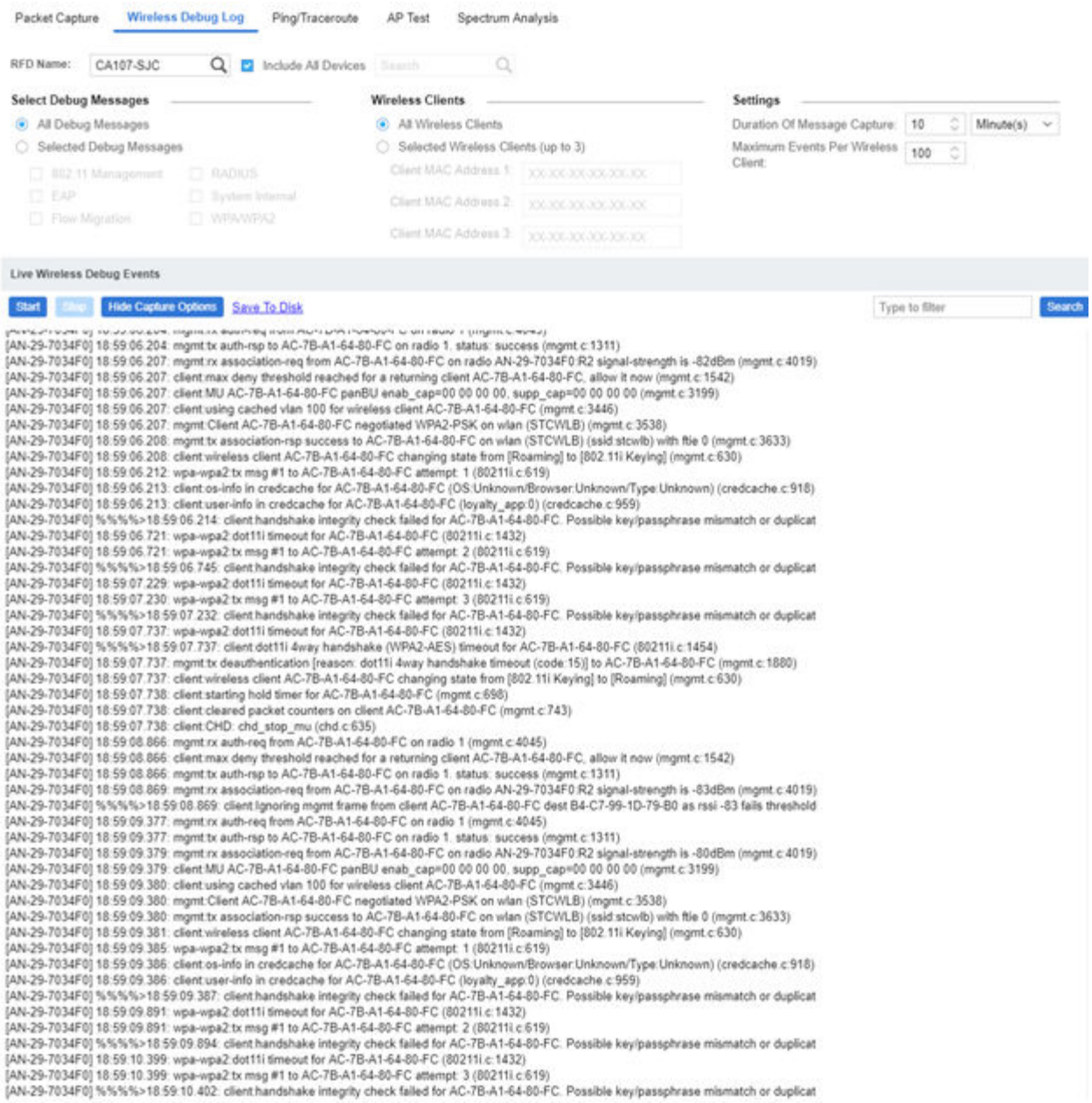


Figure 27: Extreme NSight > Tools > Wireless Debug Log Screen

3 The Wireless Debug Log tab displays with the following options and information:

RFD Name	Displays the administrator assigned name of the selected RF Domain used for wireless client debugging. RF Domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area, such as in a floor, building or site.
Include All Devices	Use the **Include All Devices** option to include debug messages from all clients, their connected Access Points and managing controllers or service platforms in the selected RF Domain.
Select Debug Messages	Select **All Debug Messages**, to display all wireless client debug information for selected RF Domain member clients. Select **Selected Debug Messages** to specify which wireless client debug messages to display. If Selected Debug Messages is selected, displays information for any combination of the following:

- **802.11 Management**
- **EAP**
- **Flow Migration**
- **RADIUS**
- **System Internal**
- **WPA/WPA2**

Wireless Clients	Select **All Wireless Clients** to display debug information for each client connected to a RF Domain member Access Point radio. Choose **Selected Wireless Clients** to display information only for specific wireless clients (between 1 and 3). If Selected Wireless Clients is selected, enter the MAC address for up to three wireless clients. The information displayed or logged will only be from the specified wireless clients.
Duration of Message Capture	Use the spinner controls to select how long to capture wireless client debug information. This can range between 1 second and 24 hours, with the default value of 1 minute.
Maximum Events Per Wireless Client	Use the spinner controls to select the maximum number of debug messages displayed per wireless client. Set the number of messages from 1 - 9999 events, with the default of 100 events.
File Location	When the **Send Data To** field is set to **File**, the **File Location** configuration displays below the configuration section. If **Basic** is selected, enter the URL in the following format: URL Syntax: • *tftp://<hostname|IP>[:port]/path/file* • *ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file* IPv6 URL Syntax: • *tftp://<hostname|[IPv6]>[:port]/path/file* • *ftp://<user>:<passwd>@<hostname|[IPv6]>[:port]/path/file* If **Advanced** is selected, configure the Target, Port, Host/IP, User, Password and optionally the path for the wireless client debug log file you wish to create.
Live Wireless Debug Events	When the **Send Data To** field is set to **Screen**, this area displays live debug information for connected wireless clients in the selected RF Domain.

4 When all configuration fields are complete, select **Start** to start the wireless client debug capture. If information is sent to the screen, it displays in the Live Wireless Debug Events section. If the data is sent to a file, that file populates with remote debug information. If you have set a long message capture duration and wish to end the capture early, select **Stop**.

Ping and Traceroute

Use a ping to test the reachability of a host on an IP network and measure the round trip time from originating host to destination and back again.

A traceroute is a diagnostic tool for displaying a route (path), and measuring transit delays of data packets across a network. The history of the route is recorded as the round-trip times of the packets received from each successive host in the route. The sum of the mean times in each hop is the total time required to establish the connection.

To access **Ping** and **Traceroute** tools:

1 Select **Tools** from the upper menu bar.
2 Select the **Ping/Traceroute** tab.

Figure 28: Extreme NSight > Tools > Ping Screen

3 Enter the hostname for the device to ping or trace in the **Device** field.
4 Enter the IP address for the device to ping or trace in the**IP Address** field.
5 Once the **Device** or **IP Address** field is populated, select **Ping** to test the reachability of a specified host. Select **Trace Route** to assess round-trip times for potential latency troubleshooting.

AP Test

AP Test is a troubleshooting tool to test if a WLAN is performing as expected in a live deployment. The AP Test simulates a wireless client and connects to WLAN tested with another WiNG AP in the vicinity. In addition to checking connectivity, AP Test can check DHCP, DNS, Ping, Throughput and Traceroute.

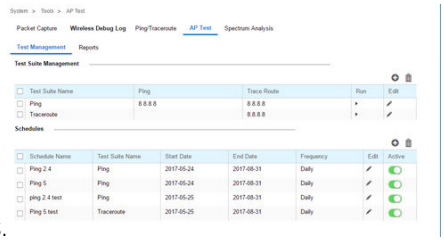
Note
The following APs are supported for AP Test as a sensor: AP7522, AP7532, AP7562, AP8432 and AP8533.

To access **AP Test** tools:

1 Select **Tools** from the upper menu bar.

2 Select the **AP Test** tab.

3 The **AP Test** tab displays.



Test Management contains a list of configured AP Test suites along with details of Ping and Traceroute tests. To create a new Test Suite, select **+** and configure the test parameters. To edit an existing Test Suite, select the pencil icon located to the right of the desired Test Suite and change test details. To remove Test Suites, select the test or tests to delete and select the trash can icon.

Test Suite Name	Displays the user generated name for each Test Suite.
Ping	Displays the IP address or hostname tested in the ping test if a Ping test is selected as part of the test suite.
Traceroute	Displays the IP address or hostname tested in the Traceroute if a Traceroute is selected as part of the test suite.
Run	Select the **Run** button to the right of the desired test. This will run this test on-demand and the results will be available in the Test Results section below.

4 To create a new Test Suite, select **+** or edit an existing Test Suite and configure the following test parameters:

Test Suite Name	Enter a descriptive name for the new test suite. This name cannot be changed once the Test Suite has been created.
New/Clone	Select **New** to create a new Test Suite. Select **Clone** to populate the new Test Suite with the tests and values used in another Test Suite. If Clone is selected, the auto-populated tests can then be edited.
Ping Test	Select to test the reachability of a host on an IP network and measure the round trip time from originating host to destination and back again.
Traceroute Test	Select to enable a network test that will show the intermediary IPs between the test site and the specified Hostname or Target IP address.
Throughput Test	Select to enable a test of throughput bandwidth by downloading or uploading a specified file from a specified FTP server. Specify if the test is Download or Upload. Then specify the FTP Server Address, Path to the test file, Port number, User and Password. Additionally specify a Maximum Transfer size in either MegaBytes or KiloBytes and a Minimum acceptable bandwidth throughput in either bps or kbps
Wireless Client	When running a test, a wireless client is simulated. Specify if the simulated wireless client uses a Random Address or a specific MAC Address. If a specific MAC Address is required, enter it in the field. Additionally specify if the simulated wireless client gets its IP information from a DHCP server, or uses a Static IP Address. When using a Static IP Address specify the IP Address, Subnet Mask and Default Gateway. Select Obtain DNS server address automatically to get DNS server information from a DHCP server, otherwise specify Primary DNS, Secondary DNS and Domain Name.

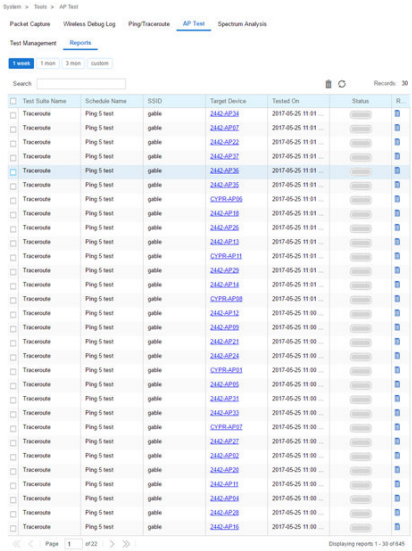
5 Schedules contains a list of scheduled AP Test suites with the Test Suite Name, Start Date, End Date and Frequency which the test is run. To create a new schedule, select +. To edit an existing schedule,

select the pencil icon located to the right of the desired schedule and change schedule details. To remove schedules, select the schedule(s) to delete and the trash can icon.

Schedule Name	Displays the user generated name given to the schedule at its creation.
Test Suite Name	Displays the user generated name for each Test Suite created.
Start Date	Displays the starting date for the scheduled tests in a Year-Month-Date format.
End Date	Displays the ending date that the scheduled tests no longer run in a Year-Month-Date format.
Frequency	Displays the interval the tests are repeated. Tests can be configured to run Daily, Weekly or Monthly.
Active	Select to activate or deactivate a specific schedule.

6 To create a new schedule, select **+**, or edit an existing schedule and configure the following:

Schedule Name	Enter a descriptive name for the new schedule. This name cannot be changed once the schedule has been created.
Test Suite List	Use the pull-down menu to select a test suite to associate with the new test schedule.
WLAN	Use the pull-down menu to select a wireless LAN to associate with the new test schedule.
Band	Use the radio buttons to select either the 2.4 GHz or 5 GHz band for the new test schedule.
Target Device	
Start Date	Use the calendar icon to select a starting date to run the scheduled test.
End Date	Use the calendar icon to select an ending date to run the scheduled test.
Recurrence	Select the frequency to run the scheduled test as either **Daily**, **Weekly**, or **Monthly**.
Time	Use the pull-down menu to select a time for the scheduled test to run. Times are available in 15 minute increments.

7 

Reports lists executed tests run on schedule or on demand. Tests results will contain DNS, DHCP, ARP, ping, traceroute and throughput information. The Search field displays results matching the search string provided. Selecting the Report icon next to a result displays that report in a new window.

Schedule Name	Displays the user generated name assigned to the schedule at its creation.

SSID	Displays the name of the WLAN tested for each report.
Target Device	Displays the MAC Address of the target device(s) tested in each report.
Tested On	Displays the date and time each test was executed.
Status	Displays the status of the test if incomplete.
Report	Select the Report icon, next to a test result, to display report details in a new window. Tests results will contain DNS, DHCP, ARP, ping, traceroute and throughput information.

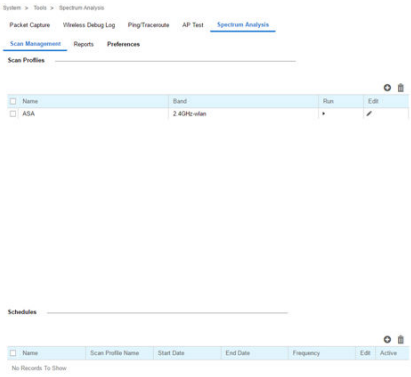
Spectrum Analysis

802.11 devices operate in unlicensed 2.4GHz and 5GHz bands and as a result, 802.11 devices experience noise and interference from both neighboring 802.11 networks operating in the same channel and non-802.11 wireless devices such as cordless telephones, wireless cameras, Bluetooth, weather radars, microwave ovens, etc.which operate in same frequency band. The presence of any of these application devices in the vicinity of 802.11 networks will have a profound impact on the reliability and throughput performance of these networks.

Organizations need IT staff with special RF skills and tools to detect interference and manage RF spectrum in which WLANs operate. Spectrum Analysis is the tool that those IT staff use to investigate the RF band for potential noise and interference sources and for troubleshooting physical layer network issues and is a valuable tool in troubleshooting and resolving performance issues which are prevalent in WLAN networks. Note that, 802.11 sniffers helps to analyze layer-2 data whereas Spectrum Analysis helps to analyze layer-1 issues.

Note
The following APs are supported for spectrum analysis as a sensor: AP7522, AP7532, AP7562, AP7612, AP7632, AP7662, AP8432, and AP8533.

To access **Spectrum Analysis** tools:

1 Select **Tools** from the upper menu bar.
2 Select the **Spectrum Analysis** tab.
3 

The **Scan Management** tab displays by default and is divided into **Scan Profiles** and **Schedules**.
4 The Scan Profiles table contains the following details and options:

Name	Displays the user generated name for each scan profile.

Band	Displays the RF band that the spectrum analysis will be performed on. The band may be 2.4GHz, 5GHz or both.
Run	Select the **Run** button to the right of the desired scan profile. This will run a spectrum analysis on the specified band(s) using the settings configured in the scan profile.
Edit	To modify a scan profile select the edit button next to the profile you wish to change.
Add	To create a new scan profile, select the + button in the upper right of the scan profiles table.
Delete	To remove scan profiles, select the box next to each profile you wish to delete and select the trashcan button in the upper right of the scan profiles table.

5 To create a new Scan Profile select the + button in the upper right of the Scan Profiles table and configure the following:

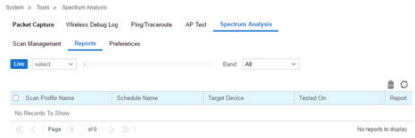
Name	Create a unique name for each Scan Profile. This name will be used to identify each profile.
New/Clone	Select **New** to create a scan profile from scratch. Select **Clone** to populate all of the values of the scan profile using the values from another scan profile.
Dwell Time	Specify an amount of time in milliseconds for the scanning radio to stay on each channel during a scan.
Duration	Specify the total amount of time a scan should run for in minutes.
Band	Select the RF band that the spectrum analysis will be performed on. The band may be 2.4GHz, 5GHz or Both.
Signal Threshold	Specify a signal power cutoff value, in dbm. The 2.4GHz and 5GHz bands can have different threshold values.
Duty Cycle Threshold	Specify a duty cycle cutoff value, in dbm. Duty cycle represents how busy a specific frequency is. The 2.4GHz and 5GHz bands can have different threshold values.
Channel Range	Use the sliders to specify a starting and ending channel range for the 2.4GHz and 5GHz spectrum used in the scan.
Chart Group Selection	The Chart Group determines which chart types will be included in the report that is generated during the scan. There are four pre-configured chart group types to show Utilization, Physical Layer, Interference, and Spectrum Details. In addition to the pre-configured chart types, Custom may be selected and any combination of Spectrogram, Spectral Density, FFT, Duty Cycle or Interference may be added to the scan report.

6 The Schedules table displays a list of scheduled scans with the following information:

Name	Displays the user generated name assigned to the schedule at its creation.
Scan Profile Name	Displays the name of the scan profile that is in use for each scheduled scan.
Start Date	Displays the starting date and time that each scan is scheduled to begin.
End Date	Displays the ending date and time that each scan is scheduled to complete.
Frequency	Displays the interval that the scan is scheduled to repeat. Scans may be scheduled to run Daily, Weekly or Monthly.
Edit	Select the edit icon to modify the associated scan schedule.
Active	Displays whether or not a scheduled scan is active or disabled.
Add	To create a new scan schedule, select the + button in the upper right of the Schedules table.
Delete	To remove scan schedules, select the box next to each scan you wish to delete and select the trashcan button in the upper right of the Schedules table.

7 To create a new scan **Schedule**, select the **+** button in the upper right of the **Schedules** table and configure the following:

Schedule Name	Enter a unique identifier for the new schedule. This name displays on the Schedule table of the Scan Management tab.
Profiles List	Use the pull-down menu to select a scan profile to associate with this scan schedule. To create a new scan profile, return to the Scan Management tab and create one in the Scan Profiles section.
Start Date	Use the calendar to select the starting date a scan is scheduled to begin.
End Date	Use the calendar to select the ending date a scan is scheduled to complete.
Recurrence	Use the pull-down menu to select the interval for the scan is scheduled to repeat. Scans may be scheduled to run Daily, Weekly or Monthly.
Time	Use the pull-down menu to select a time of day, in fifteen minute intervals, for the scan to begin.
Reset	Select Reset to clear all values from the new schedule. All information configured on this screen will be lost.
Cancel	Select Cancel to discard any configuration on a new schedule and return to the Scan Management tab.
Schedule	Once all schedule data is configured the Schedule button will be available. Select this button to save and activate the new scan schedule.

8 

Select the **Reports** tab to view the results of previously run scans.

9 Select **Live** to view reports from currently running scans. Use the pull-down menu or the sliders to specify a time period to display reports from.

10 After selecting a time period use the **Band** pull-down menu to select a RF band to display reports for. Reports can be displayed for **All**, **2.4GHz** or **5GHz**.

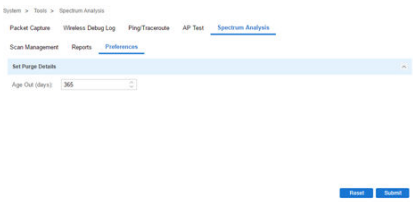
11 The reports table displays scan reports that match to the selected time period and band:

Scan Profile Name	Displays the name of the scan profile used during the scan.
Schedule Name	Displays the name of the scan schedule that ran the spectrum analysis. For reports that were run manually this displays as On Demand.
Target Device	Displays the name of the device that spectrum analysis was performed on.
Tested On	Displays the day of week, date and time that each report was completed.
Report	Select the Report icon to view the Test Report. Test reports are explained in detail below.
Delete	To remove any scan report, select the corresponding box and click the trashcan icon in the upper right of the reports table.
Refresh	To update the information displayed in the reports table select the refresh icon in the upper right of the reports table.

12 The **Test Report** page displays the following data from the spectrum analysis scan:

Spectogram	Spectrogram is a time sweep plot of the spectrum that shows how the RF power of the selected channels varies over time. This graph displays spectral power observed across 2.4 and 5GHz channels for which spectrum analysis is enabled. It indicates whether the spectrum is busy or not based on the transmit power seen from both 802.11 and non-802.11 sources using a color coded chart.

Spectral Density	The Spectral Density graph plots the snapshot of the density of power observed on each channel during the Spectrum Analysis scan. The intensity of the color indicates the power density for the frequencies. The amplitude of the curve indicates a measure of the density of the observed energy during the scan. The higher the amplitude of the curve, the busier is the spectrum. Unlike the Spectrogram which provides a historic view of the spectral power, this graph represents instantaneous power, and it provides a quick measure of which channels are busy and which are relatively quieter.A separate graph is displayed for the 2.4GHz and 5GHz band if the scan was run on both.
FFT (Fast Fourier Transformation)	The real-time Fast Fourier Transformation (FFT) graph shows the power spectrum for the current FFT sample in terms of the average, minimum and maximum power values. In addition, it shows the minimum and maximum power values out of all FFT samples since Spectrum Analysis has started.
Duty Cycle	The duty cycle graph displays how busy a particular frequency is. A 100% duty cycle for a frequency indicates it is continuously occupied and 0% indicates that the frequency is quiet. The graph contains two plots: **Current duty cycle**: Duty cycle % of latest scanning of that frequency **Average duty cycle**: Average duty cycle % of that frequency from when this scan was started.
Interference	The Interference section displays any of the following non-802.11 wireless devices that are interfering with the sensor: • CW • microwave oven • bluetooth short • bluetooth long • cordless phone • cck (802.11b) • ofdm (802.11a/g) • jammer/wideband CW • constant transmitter/narrowband CW • Proximity Detector Each of these interference types have different RF signatures. Once an interference type is detected, it will be added to the Interference section for the 2.4GHz or 5GHz band. In addition to the interference type, the frequency in which it was detected, the power and the time when it was detected are all displayed.

13 

Select the **Preferences** tab to select the purge details for old reports.

14 Configure an **Age Out** value, in days, to specify how long scan reports will be kept before being deleted from the system.

9 Preferences

You can configure preferences for alarms, for alarm notifications, and for grouping multiple RF Domains for easier managing.

Alarm Configuration

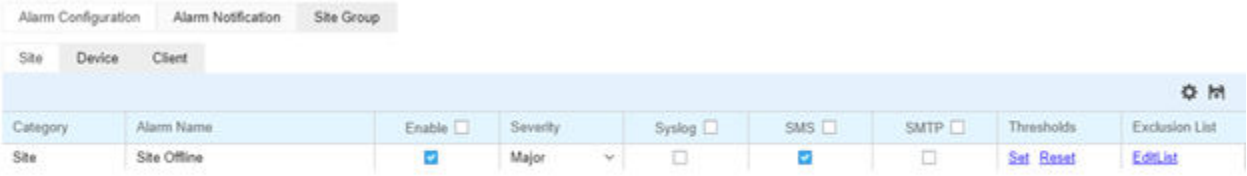


Figure 29: Extreme NSight > Preferences> Alarm Configuration > Site Screen

Alarms are part of NSight's fault management subsystem. NSight alarm management is for detecting, isolating, notifying and correcting network faults.

Alarms types include:

DHCP Failure - When any device(including wireless client) fails to get IP address. This is VLAN specific.

DNS Failure - When any device(including wireless client) fails get DNS resolution. This is VLAN specific.

Low SNR - When a radio on an AP has persistent low snr, low SNR alarm will be triggered for that AP radio.

Low RSSI - When a radio on an AP has persistent low rssi, Low RSSI alarm will be triggered for that AP radio.

High Retries - When a radio on an AP reports persistently high retries, High retry alarm will be triggered for that AP radio.

High Channel Utilization - When a radio on an AP reports persistently high channel utilization, High channel utilization alarm will be triggered for that AP radio.

802.11 EAP Authentication Failure - When a wireless client tries to authenticate with wrong password.

802.11 EAP Server Timeout - When a wireless client tries to authenticate with Radius server, but it times out from radius server.

802.11 EAP Client Timeout - When a wireless client tries to authenticate with Radius server, but it times out from wireless client.

High DNS RTT - When DNS round trip time takes longer than normal values.

Site Offline - When a reportable percentage of devices are offline.

Alarm Notification

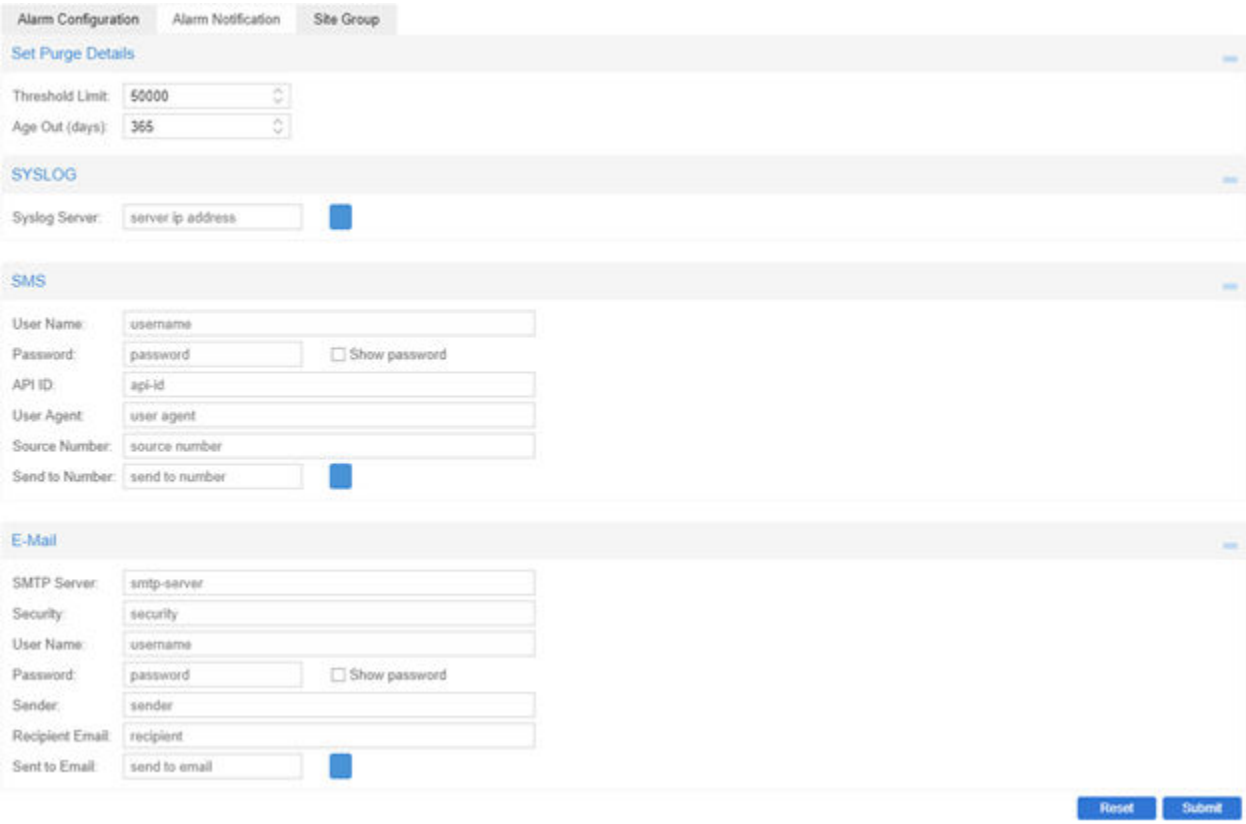


Figure 30: Extreme NSight > Preferences > Alarm Notification Screen

Alarm Notification enables administrators to globally configure how alarm notifications are sent via Syslog, SMS, and E-mail. The frequency alarms are purged can also be configured here.

Site Group

Use Site Groups to group multiple RF Domains into a single entity and manage them collectively. Site Groups can be dynamically created, modified or deleted without affecting their constituent RF Domains. Once a group is created, it displays in the left hand navigation bar below the list of RF Domains. Dashboard widgets and reports can be run on Site Groups.

To create or manage a Site Group:

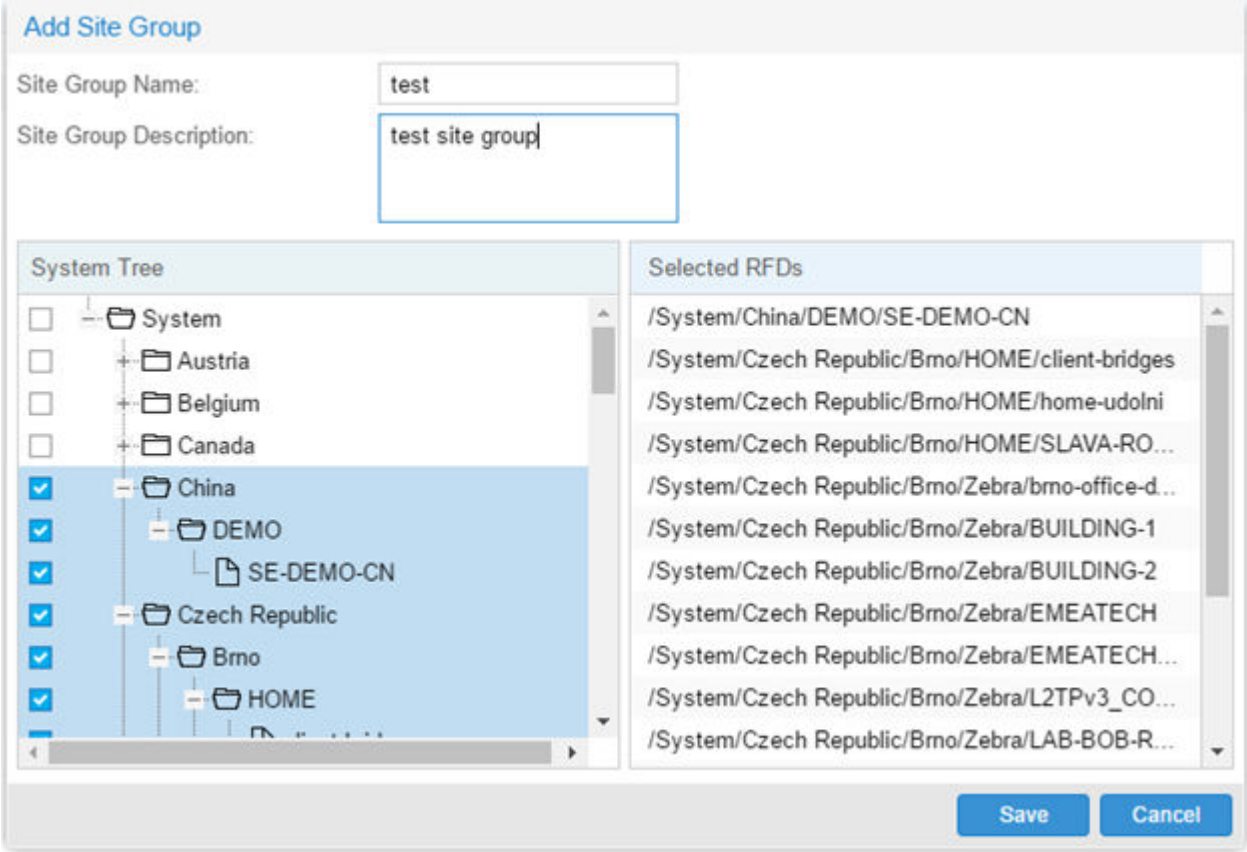
1 Select **Preferences** from the upper menu bar.
2 Select the **Site Group** tab.

The **Site Group** management tab displays.

Figure 31: Extreme NSight > Preferences > Site Group Screen

3 The following displays for the **Site Group**:

Site Group	Displays the site group name assigned by the administrator when the group was created.
Description	Displays the user generated description for the site group when the group was originally created.
Site/RFD List	Select the Site List for a specific group. A window displays a list of the member RF Domains for that group.
Actions	The Actions column allows administrators to edit or delete a specific Site Group. To edit a site group, select the pencil icon in the **Actions** column. To remove a specific site group, select the trash can icon next to it. A confirmation is displayed before deleting the group.



4 To create a new **Site Group**, select **+** and configure the **Site Group Name**, **Description** and members. To add members to a site group, select the RF Domain(s) from the **System Tree**. Selected RF

Domains appear in the **Selected RFDs** column on the right. When all members have been added, select **Save**.

5 To delete one or more **Site Groups**, select the groups to remove and select the trash can icon in the upper right.

10 Extreme NSight Troubleshooting

Debug Commands for Logging
Extreme NSight Troubleshooting FAQ

Debug Commands for Logging

Logging Commands for Extreme NSight Server

Command	Function
`debug nsight all level debug4`	Checks Extreme NSight server stats reception from the site or WiNG controller websocket ui api server posts.
`debug nsightd`	Reports KMS related logging.
`debug alarmd`	Reports alarm mining related logging.
`debug cfgd (config / nsight)`	Pushes nsight server cfgd to self.
`debug httpd`	Reports logging of lighttpd for HTTP/s.

Logging Commands on RFMD (Site) Manager

Command	Function
`debug ssm nsight level debug`	Performs periodic "POST is OK" checks on the Extreme NSight server.

Logging Commands on NOC (WiNG Controller)

Command	Function
`debug cfgd nsight / uiapi`	Checks Extreme NSight tools and pushes config to the Extreme NSight server.

WiNG CLI Commands to Check Extreme NSight and Database Status

- `show database status`
- `show nsight status`
- `show license`
- `show database statistics`
- `show version`
- `service show memory`
- `service show database collection statistics`
- `show database users`
- `show database keyfile`

- `show database restore-status`
- `show database backup-status`

Extreme NSight Troubleshooting FAQ

Not able to login to the Extreme NSight GUI

- Check if `use nsight-policy` is configured for Extreme NSight.
- Check `show nsight status` and `show database status`

Grace period license has expired.

- Check `show license` and verify that the license for Extreme NSight has been installed.

Extreme NSight does not populate sites on the left navigation tree.

- `no controller adoption` should be configured on the WiNG controller.

Extreme NSight does not show correct online devices count.

- `use nsight-policy` should be configured on all the RF Domain / Sites and should point to the Extreme NSight server IP address.
- Check if the management-policy if HTTPS/HTTP is enabled.
- If the issue persists, issue the following commands on Extreme NSight:`no use nsight`, `commit`, `use nsight-policy`

RF Domain does not show all the access points that are online. WiNG adoption status shows all access points as adopted.

- Issues the following commands for the RF Domain: `no use nsight`, `commit`, `use nsight-policy`

Dashboard widgets are not populated.

- Issues the following commands for the Extreme NSight server.: `no use nsight`, `commit`, `use nsight-policy`

Need to configure or mark guest clients on guest WLANS.

- For each guest WLAN configure `no nsight client-history` on the WiNG controller. This will ensure that new clients connecting to guest WLANs are marked as guest clients for Extreme NSight.

Dashboard widget does not show data for a given site or at the system level.

- Some dashboard widgets are dependent on the left tree navigation. Additionally, a few widgets are not applicable to system level.

Floor maps do not show the site floor map and access point placement.

- Ensure the floor map is configured correctly and that access points have been placed on the floor map using the Extreme NSight GUI.

3 Node Replica Set: Secondary node is stuck in recovering state.

- Check the flash:/log/mongod.log for any errors.
- Stop the NSight policy on Primary and Secondary nodes using `no use nsight-policy`
- Stope the database server on only the Secondary node using `service database server stop`
- Erase the database on the Secondary node using `service database remove-all-files`
- The Secondary node will automatically reload after erasing the database. After the node has reloaded check that the database is in sync and moved to a secondary state.

No email received for Extreme NSight alarm notifications.

- Run `debug alarmd` on Extreme NSight
- Check the security configuration and ensure that it is set to either **open**, **ssl**, or **starttls**.

Need to delete a RF Domain / Site from Extreme NSight.

- On the WiNG controller run `no rf-domain <site name>` and the WiNG controller will update the Extreme NSight GUI.

Access Points not showing on the NSight floor map.

- On the WiNG controller ensure that the access points are marked with the correct area and floor name.
- On the Extreme NSight floor maps section, place the access points on the map as configured.
- If you need to change the floor name or area for an access point, undo the changes on Extreme NSight first by unmapping the access point from the Extreme NSight floor map. Then modify the area or floor name for the access point on the WiNG controller. The WiNG controller will update the Extreme NSight GUI.

Events are not shown in the Extreme NSight GUI for previous days / months.

- Check if the events are visible on the WiNG Controller using `show event-history`

- Configure `event-history-size <low/medium/high>` in the nsight-policy for the Extreme NSight server based on the number of events generated across the system and the size of available data storage.

Reset the database on a 3 Node Replica Set.

Note

Before starting this process run `show database backup-status` to ensure the database export has completed.

1. Run `no use nsight-policy` in the device context of both the primary and secondary nodes.
2. Run `service database server stop` on the primary and secondary nodes.
3. Run `service database remove-all-files` on the primary and secondary nodes.
4. Reboot the primary and secondary nodes.
5. After rebooting, the primary and secondary nodes should display as **Primary** and **Secondary** when running `show database status`. No changes are needed on the arbiter.
6. If the primary and secondary nodes and arbiter are not showing the correct states, repeat steps 2 and 3 on both the primary and secondary nodes.
7. Once the state of the primary and secondary nodes are showing correctly, proceed to step 8.
8. On the primary node set only run `database-restore database nsight ftp://`***`user`***`:`***`pass`***`@`***`ipaddress`***`/nsightdb-primary.tar.gz`
9. Run `show database status` and `show database statistics`.
10. The secondary node will sync the database from the primary node automatically.
11. Run `use nsight-policy` on the primary node and confirm that it shows APs online.
12. Run `use nsight-policy` on the secondary node.

Recover Database when Secondary is in Recovering State

1. Stop the nsight service on the primary and secondary nodes by running `no use nsight policy` followed by `commit write mem` on both nodes.
2. Confirm that the nsight process has been stopped on the primary and secondary nodes by running `show nsight status` on both nodes.

No changes need to be made to the arbiter node.

3. On the secondary node, which is in a `Recovering` state, run `service database server stop`
4. On the primary node, run `show database status` and confirm it displays as `not running`.
5. On the secondary node, run `show database status` and confirm that it displays as `not reachable`.
6. On the secondary node run `service database remove-all-files`. Enter `y` when prompted for a confirmation.

When the database cleanup is complete, the secondary node will auto reload the database from the primary node.

7. Wait for the secondary node to reload and sync with the primary node's database. On larger databases this can take several hours.

Note

To view sync related logs for the secondary node run `more flash/log/mongod.log`

8. After sync is complete, the primary and secondary nodes should display as `Primary` and `Secondary` when running `show database status`.
9. On the primary node, run `use nsight policy` and verify using the GUI.
10. On the secondary server, run `use nsight policy`.