



# NSight User Guide

*For Version 5.9*

Published: June 2017

Extreme Networks, Inc.  
Phone / +1 408.579.2800  
Toll-free / +1 888.257.3000

**[www.extremenetworks.com](http://www.extremenetworks.com)**

© 2017 Extreme Networks, Inc. All rights reserved.

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 are the property of their respective owners. All other registered trademarks, trademarks, and service marks are property of their respective owners. For additional information on Extreme Networks trademarks, see [www.extremenetworks.com/company/legal/trademarks](http://www.extremenetworks.com/company/legal/trademarks).

P/N 9035124-01

Copyright © 2017 Extreme Networks, Inc. All rights reserved.

## 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](http://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](http://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

---

<b>Overview .....</b>	<b>7</b>
NSight Overview .....	7
NSight User Interface.....	8
<b>Map View .....</b>	<b>10</b>
Map View Overview .....	10
Map View (System) .....	11
Map View (Site).....	12
<b>Dashboard.....</b>	<b>15</b>
Dashboard Overview .....	15
Dashboard.....	15
<b>Monitor.....</b>	<b>23</b>
Summary (System).....	23
Summary (Site).....	26
Devices.....	29
Device Details.....	30
Clients .....	31
Client Details.....	33
Rogues .....	34
Event Log.....	35
Alarms.....	37
Filtering Alarm Data.....	38
<b>Reports .....</b>	<b>39</b>
Reports Overview.....	39
Generated Reports.....	39
Manage Reports .....	41
Scheduled Reports.....	43
Report Builder.....	44
<b>Tools .....</b>	<b>49</b>
Tools Overview.....	49
Packet Capture.....	49
Wireless Debug Log .....	51
Ping and Traceroute.....	53

AP Test.....	54
Spectrum Analysis.....	58
<b>Preferences.....</b>	<b>65</b>
Alarm Configuration.....	65
Alarm Notification.....	67
Site Group.....	69

# Preface

---

## Providing Feedback to Us

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 about this document, please contact us using our short [online feedback form](#). You can also email us directly at [InternallInfoDev@extremenetworks.com](mailto:InternallInfoDev@extremenetworks.com).

## Getting Help

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

- **GTAC (Global Technical Assistance Center) for Immediate Support**
  - Phone: 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](http://www.extremenetworks.com/support/contact)
  - Email: [support@extremenetworks.com](mailto:support@extremenetworks.com). To expedite your message, enter the product name or model number in the subject line.
- **GTAC Knowledge** — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- **The Hub** — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- **Support Portal** — Manage cases, downloads, service contracts, product licensing, and training and certifications.

## Extreme Networks Publications

### General

Product documentation is available at: <http://documentation.extremenetworks.com>. Release notes are available at: [www.extremenetworks.com/support/release-notes](http://www.extremenetworks.com/support/release-notes)

### Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: [www.extremenetworks.com/support/policies/software-licensing](http://www.extremenetworks.com/support/policies/software-licensing)



# Overview

---

## NSight Overview

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. NSight provides real-time monitoring, historical trend analytics and troubleshooting capabilities for WLAN deployment management.

With the 5.8.2 version, NSight can be deployed in stand-alone mode on a dedicated NX95xx/NX96xx appliance or a virtual appliance that provides a single-pane-of-glass interface to monitor and manage multi-cluster controller deployments. As introduced in 5.8 NSight is continued to be supported on the NX (95xx & 96xx) & VX platforms as a launch-able application with WING. With flexible deployment options, NSight can now scale to support 40,000 Access Points.

NSight 5.8.2 provides the flexibility to deploy the application on the NX/VX controller adopting Access Points or as a standalone instance outside the controller.

NSight is designed for day-to-day network monitoring and troubleshooting and provides macro trending analytics for network planning, usage modeling and SLA management. NSight provides administrators sophisticated network visualizations, graphically displaying the information they require with minimal keystrokes. 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.

Using 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.

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 NSight interface to further clarify the problems. Troubleshooting tools include:

1. Packet capture
2. Wireless Debug log access
3. TCP/IP Ping & Traceroute

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.

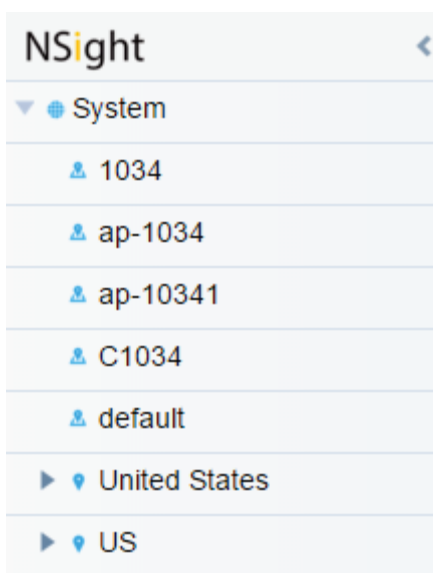
Central to NSight functionality is the map view . Map view is an interactive tool allowing an administrator to embed any network or RF specific attributes of an Access Point or client. For example, an administrator would

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. 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. 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.

## NSight User Interface

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



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 NSight UI.





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



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.

# Map View

---

## Map View Overview

In a multi-site environment a top level view is available with each provisioned site identified. The high level view provides a quick snapshot of Access Point status and client count at each site, with links to launch monitor screens or drill down to an interactive floor map.

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 allowing you 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 for RF channel assignments, SNR, retries, power, throughput, client count and other data.

### Note

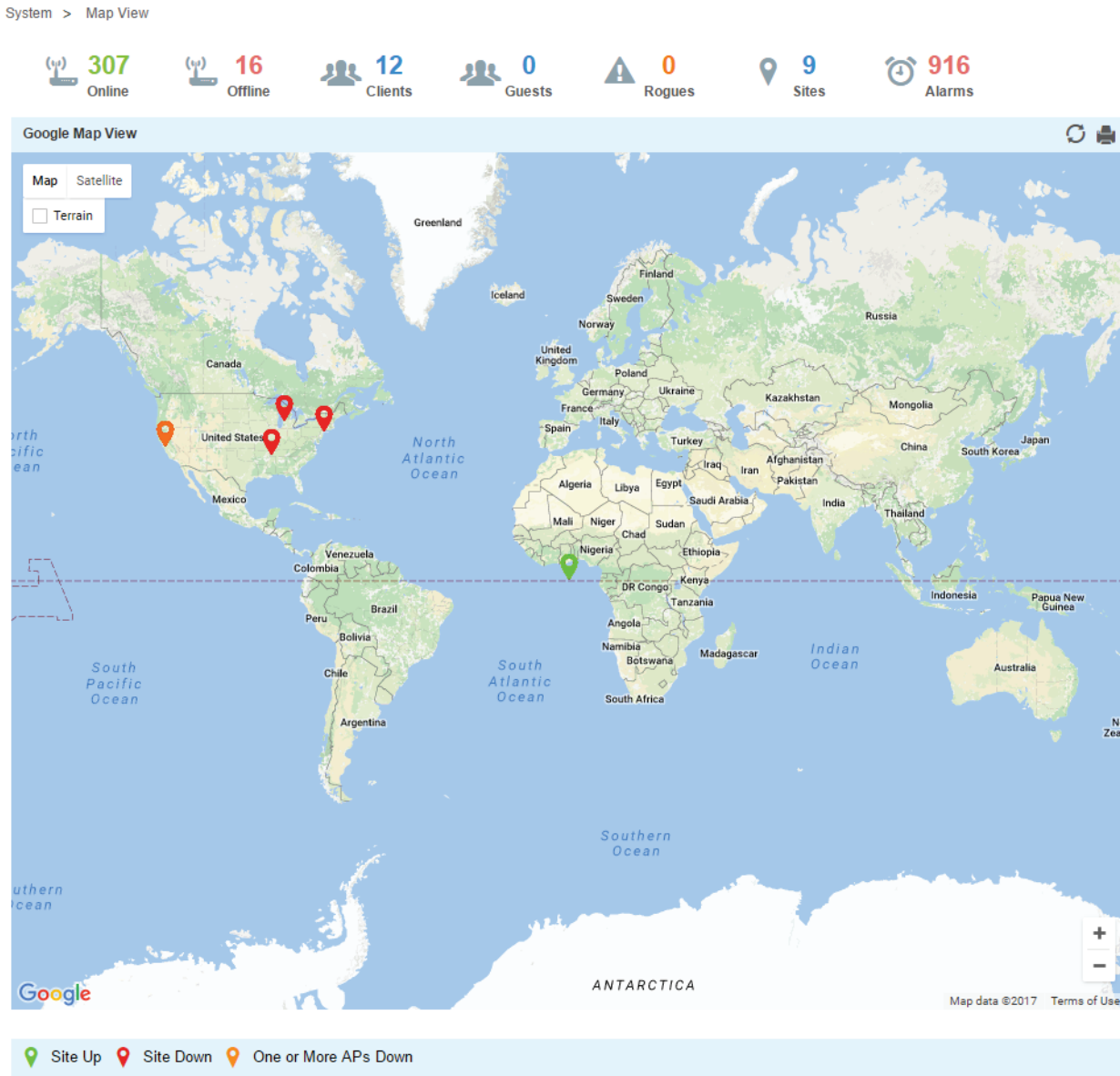
Sites are placed on the map using “location /long>” in the RF-Domain context in the Command Line Interface (CLI).

## Map View (System)

To view geographic or site based network maps:

4. Select **Map View** from the upper menu bar.
5. Select **System** from the Left Nav.

The system level network map displays.

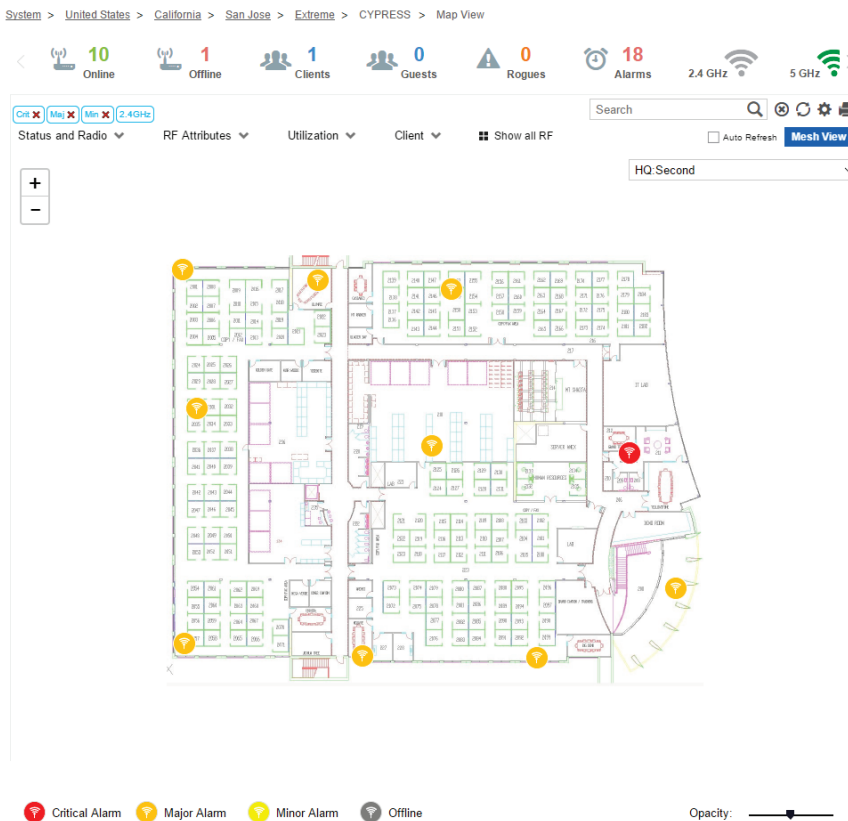


The system level Map View displays each site with site locations displayed geographically for immediate visualization of the entire network. The Map View also displays the status of your connected clients and site status.

## 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.



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 for 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 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.

Refer to the following to customize the site level map display:

<p><b>APs &amp; Radios: Online</b></p>	<p>Select this option to include all online APs and radios in the site map. Use this option with the APs &amp; Radios: Offline to assess whether specific sites are adequately supported by functional Access Point radios. Unselecting this option hides all online APs and radios.</p>
--	--

<b>APs &amp; Radios: Offline</b>	Select this option to include all offline APs and radios in the site map. This is a helpful option to identify potential areas of poor coverage in respect to unplanned offline devices. Unselecting this option hides all offline APs and radios.
<b>APs &amp; Radios: 2.4 GHz / 5.0 GHz</b>	Select either 2.4 GHz or 5.0 GHz to define which RF band to show on the floor map.
<b>RF Attributes: Channel</b>	Select this option to display RF channels on the floor map. This feature helps validate whether adjacent coverage areas are properly segregated by non-overlapping channels. Unselecting this option hides RF channel information.
<b>RF Attributes: Power</b>	Select this option to display power levels on the floor map. Unselecting this option hides power level information.
<b>RF Attributes: SNR</b>	Select this option to display signal to noise ratio information on the floor map. This value helps administrators assess the level of radio interference that can be tolerated within the network. Unselecting this option hides signal to noise ratio information.
<b>Utilization: Throughput</b>	Select this option to display data throughput speed on the floor map. This value helps administrators assess the level of radio interference tolerated within the network. Unselecting this option hides data throughput speed information.
<b>Utilization: Client Count</b>	Select this option to display adopted client count information on the floor map. This helps administrators assess whether client adoption counts are close, or are exceeding, the limits specified in their licenses. Unselecting this option hides adopted client count information.
<b>Utilization: Usage</b>	Select this option to display usage information on the floor map. Unselecting this option hides usage information from the floor map.
<b>Utilization: Retries</b>	Select this option to display client retry information on the floor map. Use this information to assess whether the retry count is excessive in respect to the number of clients currently utilizing an Access Point's radio resources and whether the noise ratio is currently high. Unselecting this option hides client retry information from the floor map.
<b>Show: Heat Map</b>	Select this option to generate and display RF heat map information in the floor map. The heat map is a graphical presentation of how RF coverage is anticipated within the site map (and floor plan) based on the barriers and transmission capabilities defined for the devices within. The heat map displays areas of heat (defined by the darker reddish color) where RF coverage is at its best. As the color changes to a lighter yellow the signal strength within the site becomes less optimal and is more subject to RF attenuation associated with building obstacles. Unselecting this option will hide heat map from the floor map.
<b>Show: Floor Map</b>	Select this option to display the Floor Map image. The floor map is an image showing a geographical map of the site. Unselecting this option will hide the floor map image.
<b>Show: Clients</b>	Select this option to display client details on the floor map. Clients are represented by blue dots on the floor map. This option is useful in assess areas where large groups of clients are dwelling and consuming a larger proportion of network resources. Unselecting this option hides client information from the floor map.
<b>Show: Table</b>	Select this option to display a table with RF attributes for each AP and radio in the site.

<p><b>Apply Filters: SNR</b></p>	<p>When <i>SNR</i> is selected in RF Attributes, use the slider to filter the information displayed to fit the signal to noise ratio selected. If SNR is not selected, this filter is disabled.</p>
<p><b>Apply Filters: Power</b></p>	<p>When <i>Power</i> is selected in RF Attributes, use the slider to filter the information based on selected power range.</p>
<p><b>Apply Filters: Throughput</b></p>	<p>When <i>Throughput</i> is enabled in <i>Utilization</i>, use the <i>Throughput</i> pull-down menu to filter information based on selected throughput range.</p>

# Dashboard

## Dashboard Overview

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 geographic 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 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 NSight Dashboard in 3 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 save

To create a new (blank) Dashboard that can be manually populated with customized data (widgets):

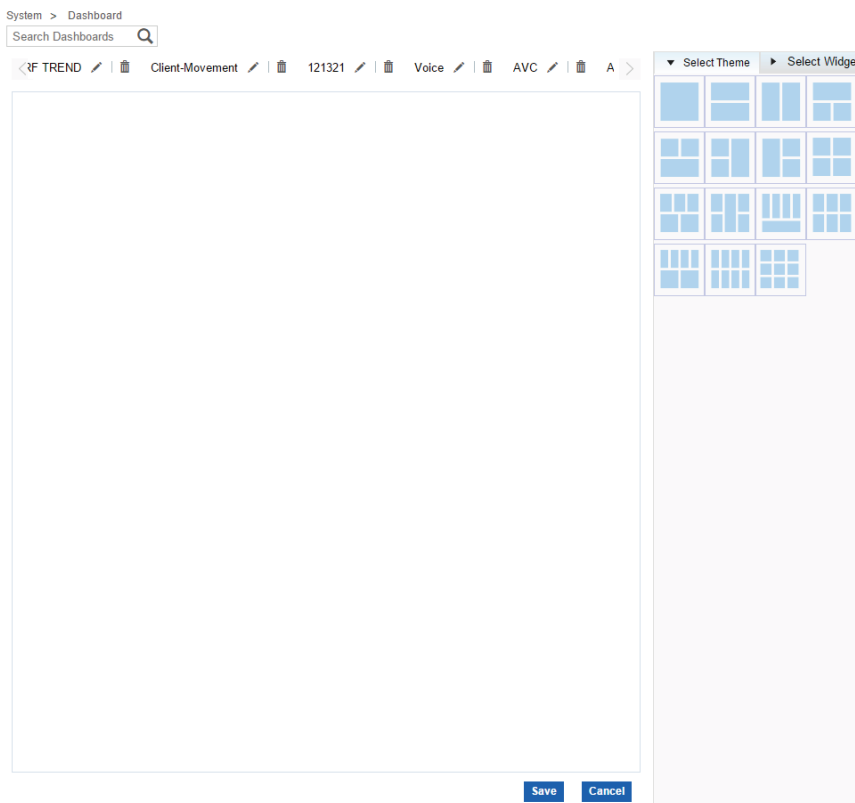
1. Select **Dashboard** from the upper menu bar.

**Note**

Selecting System, locations or sites from the Left Nav changes the network information displayed. However Dashboard tabs are system-wide and not associated with a specific site or location.

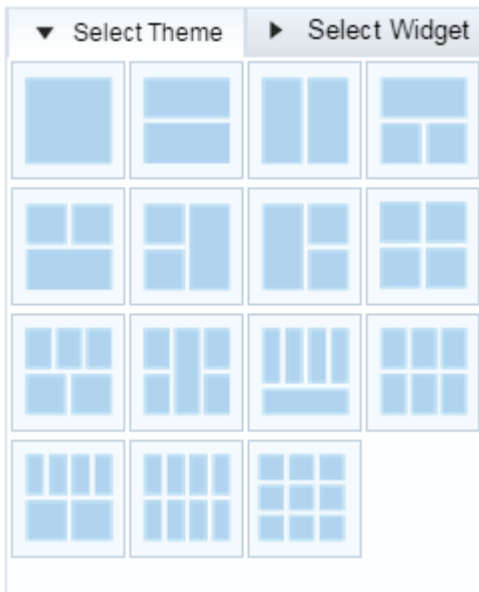
2. Select **+** at the top of the page next to any existing tab.

A blank **Dashboard** tab displays.

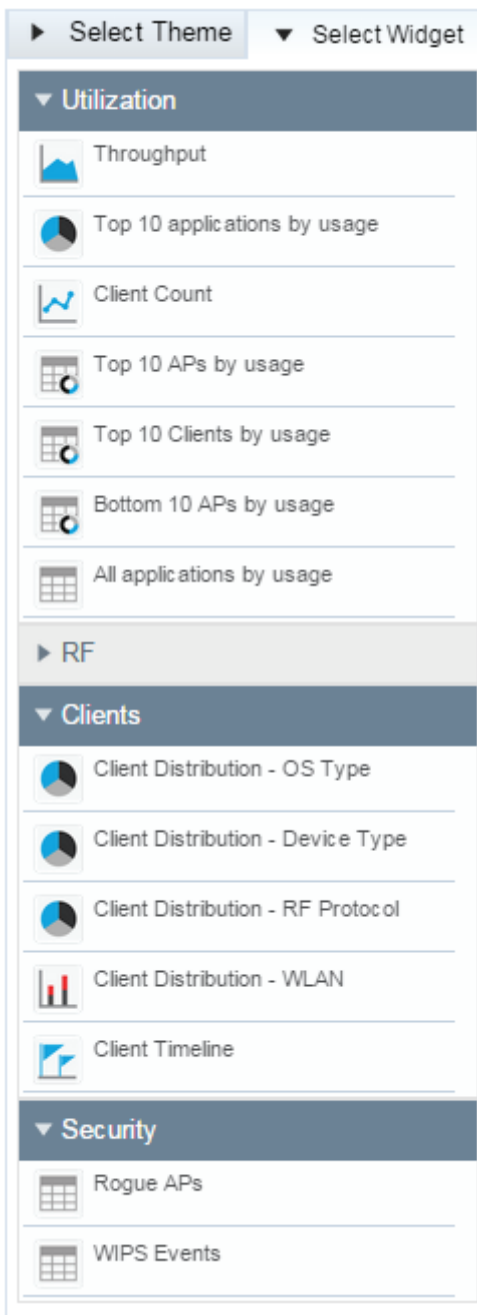




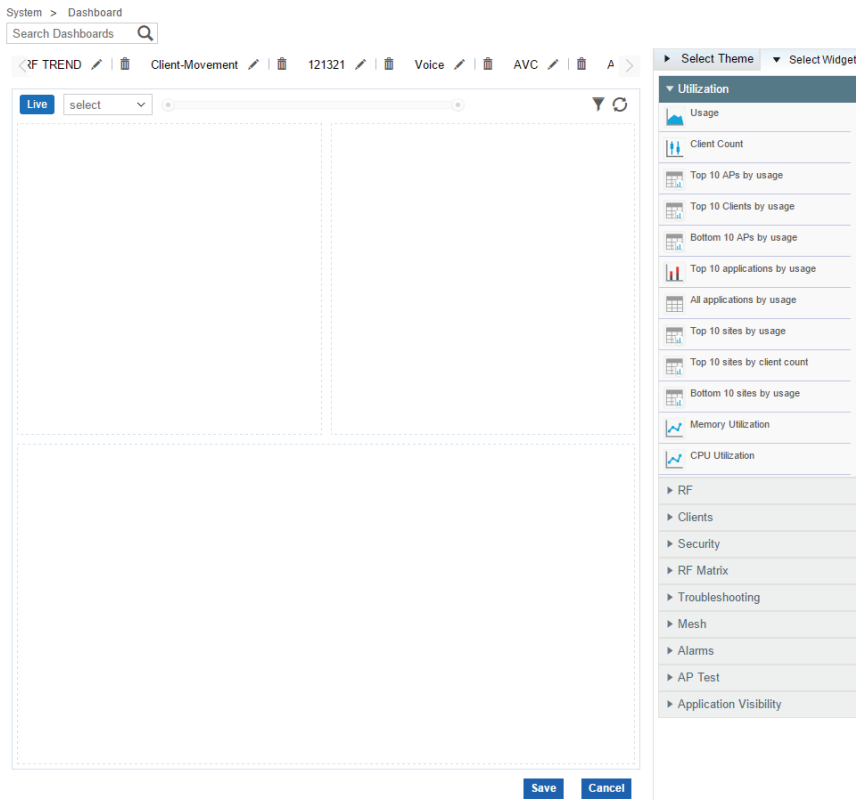
- From the **Select Theme** menu, choose a display theme (screen panel layout) and drag the theme into the blank Dashboard.



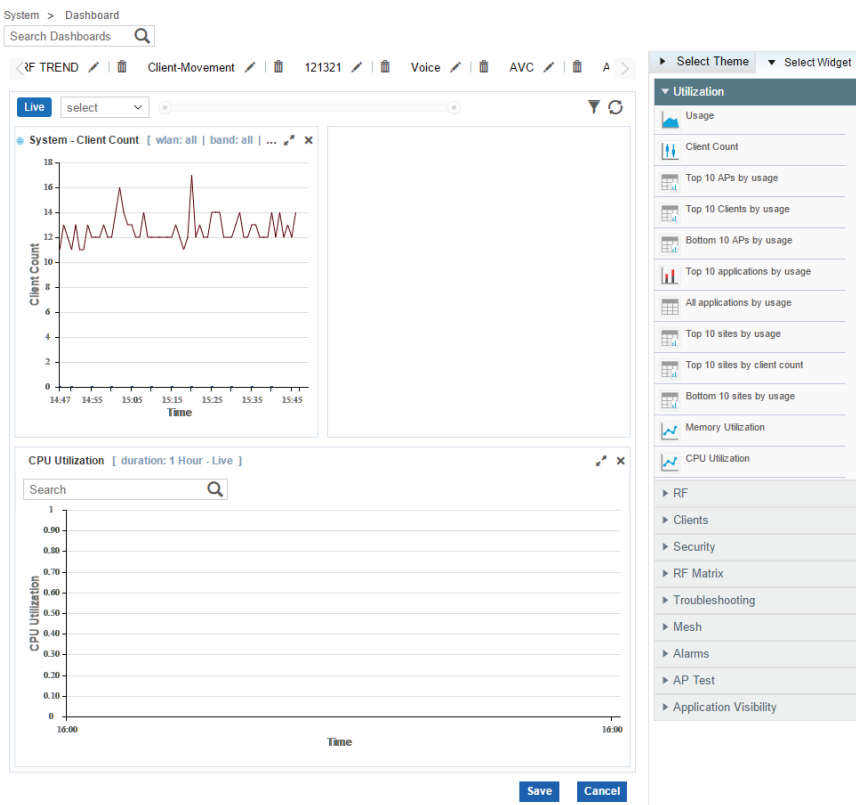
- From the **Select Widget** menu, select **Utilization**, **RF**, **Clients**, **Security**, **RF Matrix**, **Troubleshooting**, **Mesh**, **Alarms**, **AP Test**, or **Application Visibility** and use the arrow to expand the list.



5. For each grid in the new Dashboard, select a widget and drag it to the desired location until each panel is populated.



As widgets are added, they immediately populate with the selected data type based on the information for the System, locations or sites selected in the Left Nav.



Note

TCP-RTT metadata collection can be only enabled using the command line interface. For more information, see the WiNG CLI Reference Guide.

6. Select **Save** to commit the changes to the new Dashboard, or **Cancel** to revert to the last saved configuration.

Existing Dashboards can have their layout themes and widget configurations updated as their data presentation and analysis requirements dictate.

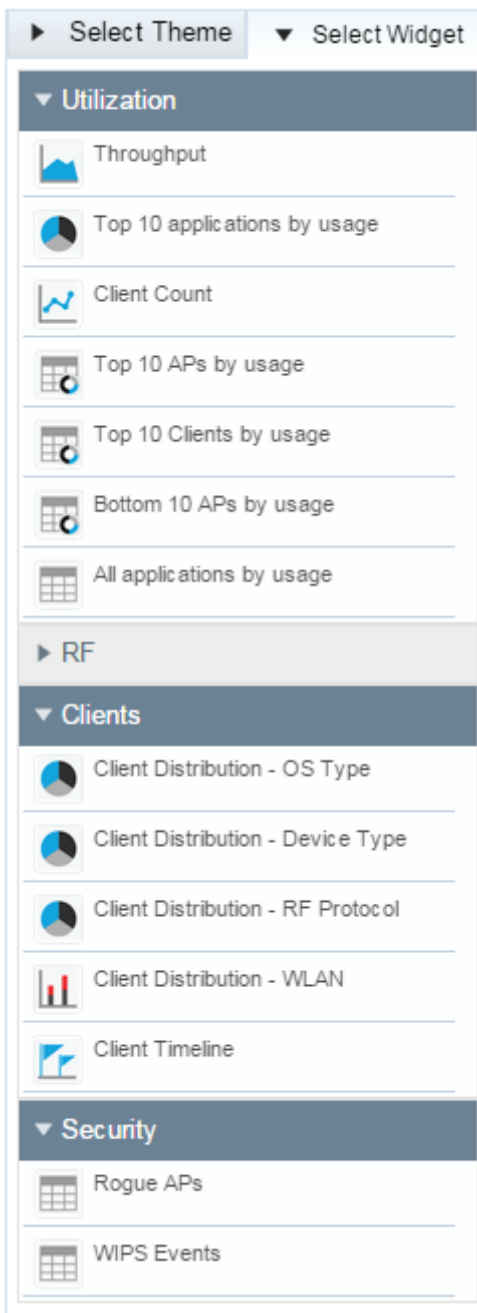
To modify the configuration of an existing Dashboard:

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

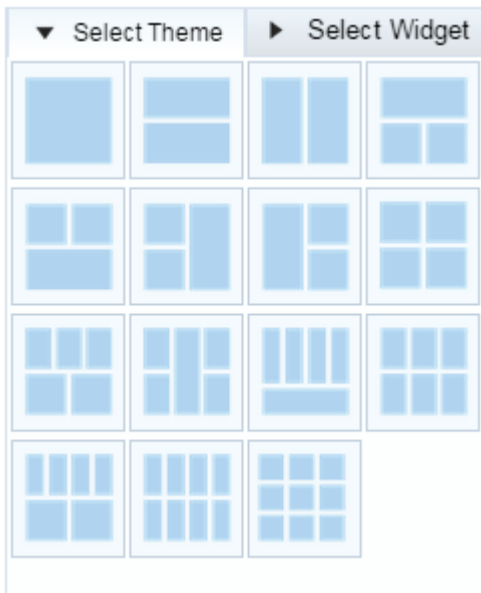
#### Note

Selecting System, locations or sites from the Left Nav changes the network information displayed. However, Dashboard tabs are system-wide and not associated with a specific site or location..

8. Select the pencil icon at the top of the page next to any existing tab to edit that tab's name.
9. To replace existing widgets, select **Utilization**, **RF**, **Clients**, **Security**, **RF Matrix**, **Troubleshooting**, **Mesh**, **Alarms**, **AP Test**, or **Application Visibility** from the **Select Widget** menu and use the arrow to expand the list.



10. For each widget replaced in the **Dashboard** tab, select a widget and drag it to the desired panel. The existing widget is replaced with the new widget.
11. As widgets are added they are immediately populated with the selected data type for the new widget, based on information for the **System**, locations or sites selected in the Left Nav.
12. To change the layout of an existing tab, choose a page layout from the **Select Theme** menu and drag that layout to the existing tab. The existing tab layout and widgets are replaced by the new layout.



13. Select **Save** to commit the changes to the **Dashboard** tab or **Cancel** to revert to the last saved configuration.

## 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 wide Access Point and client utilization summary information to assess the system-wide health of the NSight managed 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.



Note

Usage data displays in green and blue. Green represents upstream data and is shown on the upper half of the graph. Green upstream data is shown in the upper half of the graph and blue downstream data is shown on the lower half.

3. Set the following trending information for the data polled and reported:

<p><b>WLAN</b></p>	<p>Refine the client count or AP usage data displayed to either a single selected WLAN or all the WLANs in the Nsight network to better assess if client load is adequately distributed.</p>
--------------------	--



<b>Band</b>	Optionally filter client count or AP usage to either the 2.4 or 5 GHz radio band to assess whether clients are adequately supported by online Access Points with available bandwidth in both the 2.4 and 5 GHz radio bands.
<b>Trending Period</b>	Select whether summary information is trended and displayed for the previous 30 minutes (default setting), 2 hours, 1 day, 1 week, 1 month or 3 months.
<b>Refresh</b>	The refresh button updates summary data in the key metrics bar.

**Note**

The Refresh button does not update chart data. Chart data is refreshed automatically every 30 seconds.

4. Refer to the **Client Count** graph to periodically assess whether client counts are adequately supported by online Access Points over a specified trending period.
5. The **AP Usage** graph displays the total throughput for online Access Points, in Megabits, over the specified trending period. Assess whether additional Access Points are needed to support client bandwidth by filtering different WLANs and radio bands to specific periods of high and low throughput.
6. **Top APs by Usage** displays top 10 Access Points by data usage in MegaBytes, ordered from highest to lowest on the graph, with each top Access Point color coded for visual differentiation.
7. The following information displays for each listed Access Point:

<b>AP Name</b>	Lists the administrator assigned name of each top performing Access Point. The name displays as a link that can be selected to display this Access Point's information in greater detail.
<b>IP Address</b>	Lists the Access Point IP address used as its network identifier.
<b>RF Domain</b>	Displays each listed Access Point's RF Domain membership. 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. Each RF Domain contains policies that can determine a Smart RF or WIPS configuration. RF Domains enable administrators to override WLAN SSID name and VLAN assignments. This enables the deployment of a global WLAN across multiple sites and unique SSID name or VLAN assignments to groups of Access Points servicing the global WLAN.
<b>Channel</b>	Displays the channel setting for each listed Access Point radio. Country requirements restrict Access Point radio transmissions, so ensure each top performing Access Point is operating legally in respect to its deployed country.
<b>Usage</b>	Lists each top performing Access Point's throughput in megabytes. Assess this integer in respect to the number of connected clients and the throughput of lower performing Access Points and their client counts.
<b>Clients</b>	Lists each Access Point's number of connected clients. Assess whether an increased number of connected clients translates into a high level of reported usage (megabyte consumption).

8. **Top WLANs by Usage** displays a list of the top 10 WLANs by data usage, displayed in MegaBytes, from highest to lowest and displayed as a graph.

<b>WLAN Name</b>	Lists each top performing WLAN whose member Access Points and connected clients report the highest usage.
<b>Usage</b>	Lists each top performing WLAN's throughput in megabytes. Assess this integer in respect to the number of connected clients and WLAN member Access Point radios supporting them.
<b>Clients</b>	Lists each WLAN's number of connected clients. Assess whether an increased number of connected clients translates into a high level of reported utilization (megabyte consumption).

9. **Top Devices by Usage** displays a list of the top 10 client devices by data usage, in MegaBytes, from highest to lowest.

<b>Device Name</b>	Lists each top performing device's name (by manufacturer) whose connected clients report the highest network utilization (in Megabytes).
<b>Usage</b>	Lists each top performing device's network utilization in megabytes. Assess this integer in respect to the number of connected clients for consistency.
<b>Clients</b>	Lists each device's number of connected clients. Assess whether top reporting devices appear random, or if there's a trend in one a particular device type with the highest reported usage.

10. **Top Operating Systems by Usage** displays a list of the top 10 client operating systems by data usage, displayed in MegaBytes, ordered from highest to lowest.
11. **Top Applications by Usage** displays a list of the top 10 client applications by data usage, displayed in MegaBytes, ordered from highest to lowest. Use this information to assess if specific client applications are adversely impacting performance and warrant filtering.
12. **All Applications Details** displays a list of all client applications, their data usage, category, total number of clients and the client with the most data usage for each application. Use this information to assess if specific client applications are adversely impacting performance and warrant filtering.

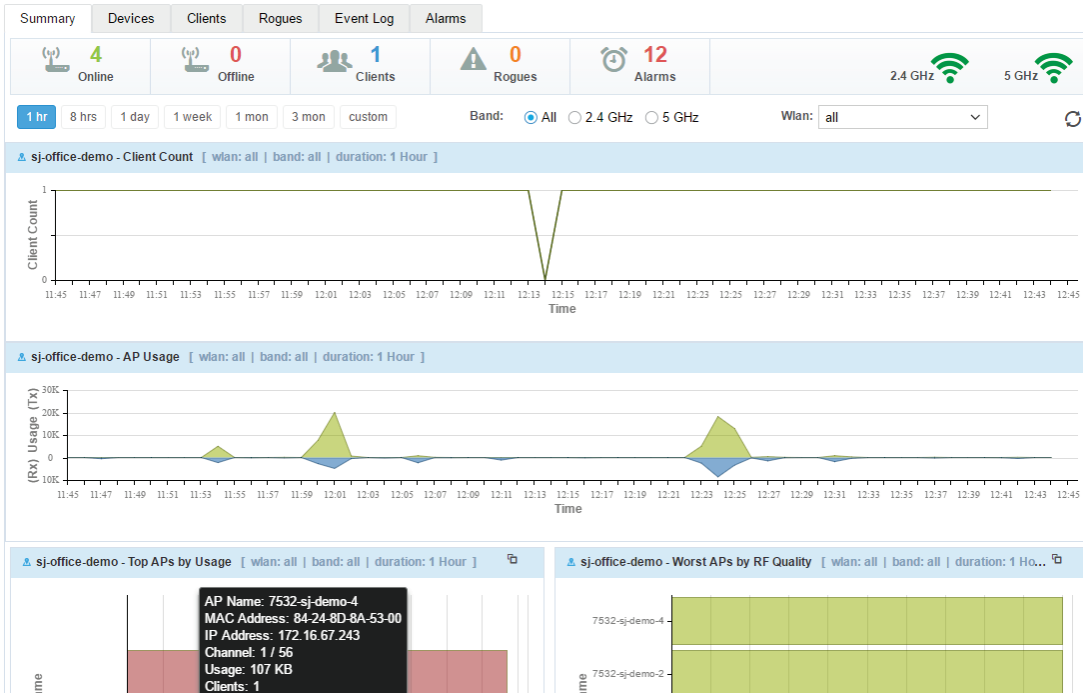
## Summary (Site)

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



**Note**

Usage data is displayed in green and blue. Green upstream data is shown in the upper half of the graph and blue downstream data is shown on the lower half.

3. Set the following trending information for the data polled and reported:

<b>WLAN</b>	Refine the client count or AP usage data displayed to either a single selected WLAN or all the WLANs in the Nsight network to better assess if client load is adequately distributed.
<b>Band</b>	Optionally filter client count or AP usage to the 2.4 or 5 GHz radio band to assess whether clients are adequately supported by online Access Points with available bandwidth.
<b>Trending Period</b>	Select whether summary information is trended and displayed for the previous 30 minutes (default setting), 2 hours, 1 day, 1 week, 1 month or 3 months.
<b>Refresh</b>	The refresh button updates summary data in the key metrics bar.

**Note**

The Refresh button does not update chart data. Chart data is refreshed automatically every 30 seconds.

4. The **Client Count** graph displays the number of clients detected within a selected WLAN. Periodically assess whether client counts are adequately supported by online Access Points across the radio bands utilized.

5. The **AP Usage** graph displays the total throughput for online Access Points, in Megabits, over the specified trending period. Assess whether additional Access Points are needed to support resource requesting clients by filtering different WLANs and radio bands to specific periods of high and low throughput.
6. **Top APs by Usage** displays top 10 Access Points by data usage in MegaBytes, ordered from highest to lowest, with each top Access Point color coded for visual differentiation.
7. The following information displays for each listed Access Point:

<b>AP Name</b>	Lists the administrator assigned name of each top performing Access Point. The name displays as a link that can be selected to display this Access Point's information in greater detail.
<b>IP Address</b>	Lists the Access Point IP address used as each Access Point's network identifier.
<b>RF Domain</b>	Displays each listed Access Point's RF Domain membership. 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. Each RF Domain contains policies that can determine a Smart RF or WIPS configuration. RF Domains enable administrators to override WLAN SSID name and VLAN assignments. This enables the deployment of a global WLAN across multiple sites and unique SSID name or VLAN assignments to groups of Access Points servicing the global WLAN.
<b>Channel</b>	Displays the channel setting for each listed Access Point radio. Country requirements restrict Access Point radio transmissions, so ensure each top performing Access Point is operating legally in respect to its deployed country.
<b>Usage</b>	Lists top performing Access Point throughput in megabytes. Assess this integer in respect to the number of connected clients.
<b>Clients</b>	Lists each Access Point's number of connected clients.

8. **Top WLANs by Usage** displays a list of the top 10 wireless LANs by data usage, displayed in MegaBytes, ordered from highest to lowest and displayed as a graph.

<b>WLAN Name</b>	Lists each top performing WLAN name whose member Access Points and connected clients report the highest usage.
<b>Usage</b>	Lists each top performing WLAN's throughput in megabytes. Assess this integer in respect to the number of connected clients and WLAN member Access Point radios supporting them.
<b>Clients</b>	Lists each WLAN's number of connected clients.

9. **Top Devices by Usage** displays a list of the top 10 client devices by data usage, displayed in MegaBytes, ordered from highest to lowest and displayed as a graph.

<b>Device Name</b>	Lists each top performing device name whose connected clients report the highest network utilization (in Megabytes).
<b>Usage</b>	Lists each top performing device's network utilization in megabytes. Assess this integer in respect to the number of connected clients for consistency.

<b>Clients</b>	Lists each device's number of connected clients. Assess whether top reporting devices appear random, or if there's a trend in one a particular device type with the highest reported usage.
----------------	---

- Top Operating Systems by Usage** displays the top 10 client operating systems by data usage, displayed in MegaBytes, ordered from highest to lowest.
- Top Applications by Usage** displays the top 10 client applications by data usage, displayed in MegaBytes, ordered from highest to lowest.

**Note**

If AVC is disabled, charts and grids related to application visibility, such as Top 10 Applications are not shown.

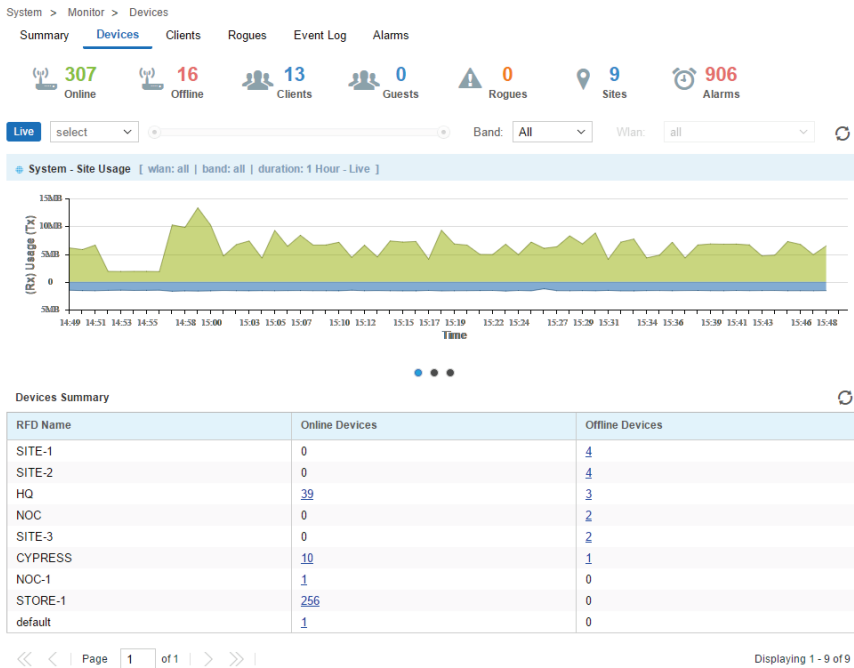
- All Applications Details** displays a list of client applications, their data usage, category, total number of clients and the client with the most data usage for each application.

## Devices

To view a summary of all APs and devices:

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

The Devices screen displays.



**Note**

Usage data is displayed in green and blue. Green upstream data is shown in the upper half of the graph and blue downstream data is shown on the lower half.

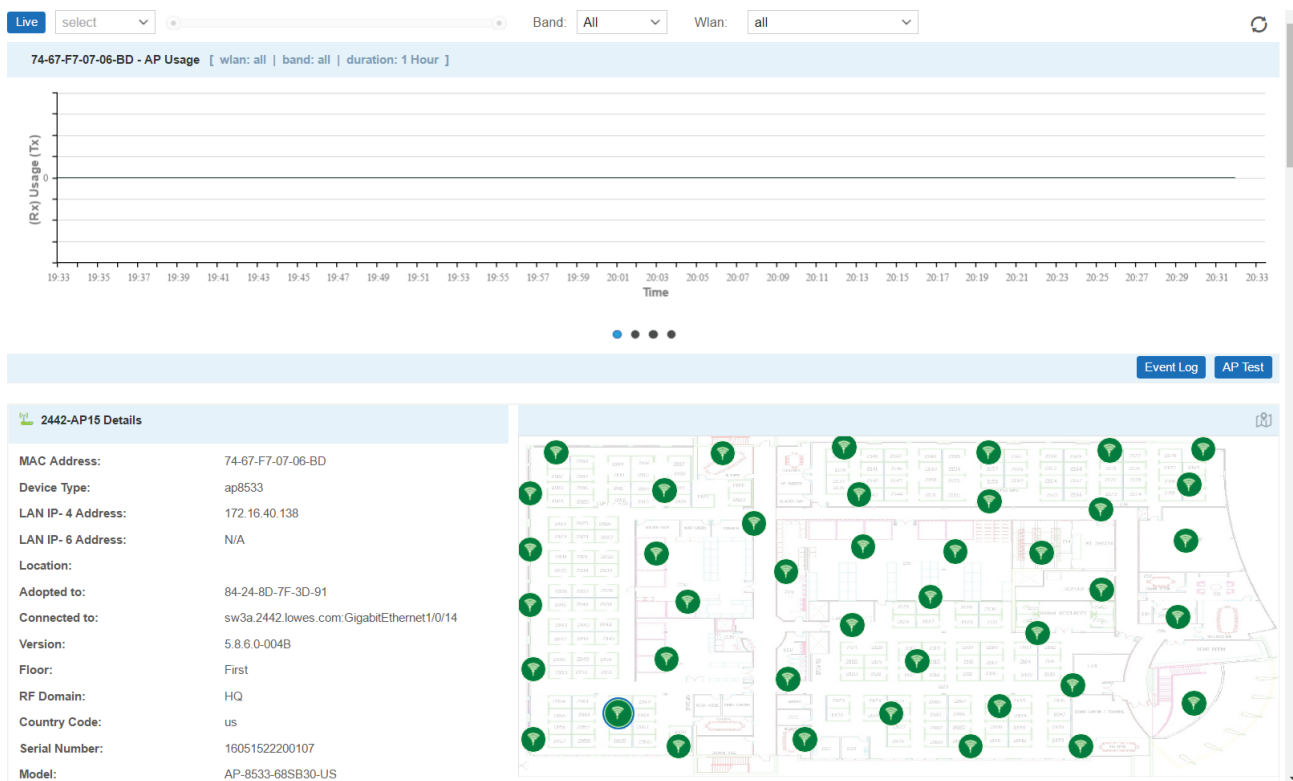
- Review the following information for Access Points and their connected clients:

<b>Status</b>	Displays the online status of each device. If a device is online, it displays a green checkmark. If the device is offline, it displays a red "X".
<b>Name</b>	Displays the Access Point's unique administrator assigned name provided upon initial configuration.
<b>Device Type</b>	Displays the model number for NSight managed devices to help assess the diversity of connected devices.
<b>Clients</b>	Displays the number of wireless clients connected to each NSight managed device.
<b>Adopted For</b>	Displays the time in days, hours and minutes the Access Point or client has been adopted.
<b>MAC Address</b>	Displays the <i>Media Access Control</i> (MAC) address factory assigned to each device as its unique hardware network identifier.
<b>IP Address</b>	Displays the current IP address the device is using as its network identifier.
<b>RF Domain</b>	Displays the name of the RF Domain associated with each NSight managed device.
<b>Serial Number</b>	Displays the unique hardware serial number assigned to each device.

## Device Details

To view details of a specific 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.

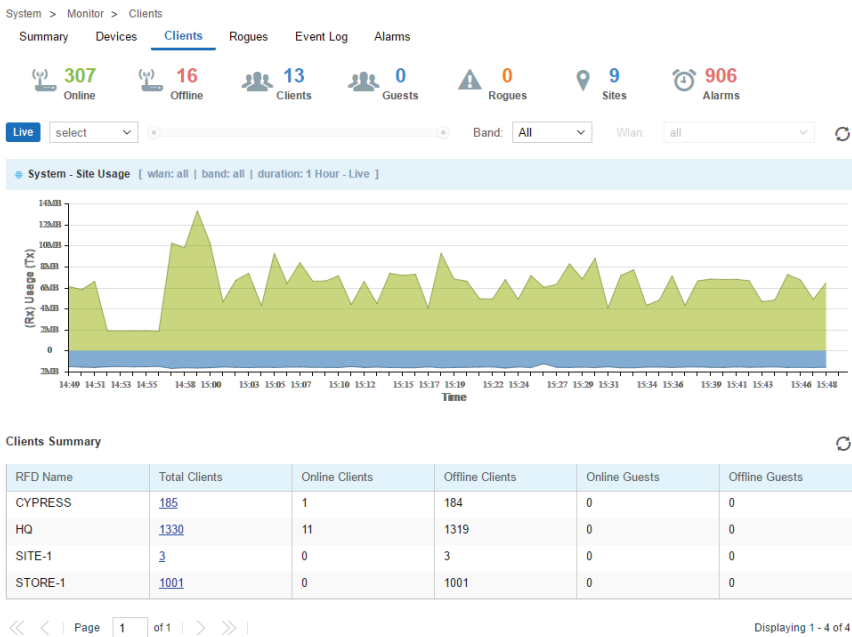


4. Select **Live** to view the current device details in real time. Use the pull-down menu or the sliders to specify a time period to display device data from.
5. After selecting a time period use the **Band** pull-down menu to select the RF band(s) to display device details for. Details can be displayed 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 Nsight managed clients:

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



Note

Usage data is displayed in green and blue. Green represents upstream data and is shown on the upper half of the graph. Green upstream data is shown in the upper half of the graph and blue downstream data is shown on the lower half.

3. Review the following information for wireless clients connected to the NSight managed network:

<b>Status</b>	Displays the online status of each NSight managed client. If a device is online, it displays a green checkmark. If the device is offline, it displays a red "X".
<b>MAC Address</b>	Displays the <i>Media Access Control</i> (MAC) address factory assigned to each device as its unique hardware network identifier.
<b>Name</b>	Displays the client's unique administrator assigned name provided upon initial adoption.
<b>Vendor</b>	Displays the device manufacturer for each wireless client connected to the managed network.
<b>IP Address</b>	Displays the current IP address the device is using as its network identifier.
<b>User Name</b>	Displays the username associated with each wireless client on the managed network.
<b>BSSID</b>	Displays the <i>Broadcast Service Set ID</i> (BSSID) MAC address used for matching and filtering with the signature.
<b>WLAN</b>	Displays the WLAN associated with each wireless client on the managed network.



<b>Channel</b>	Displays the channel setting for each listed NSight managed client. Country requirements restrict Access Point radio and connected client transmissions, so ensure each Access Point and their connected clients are operating legally in respect to its approved channel list.
----------------	---

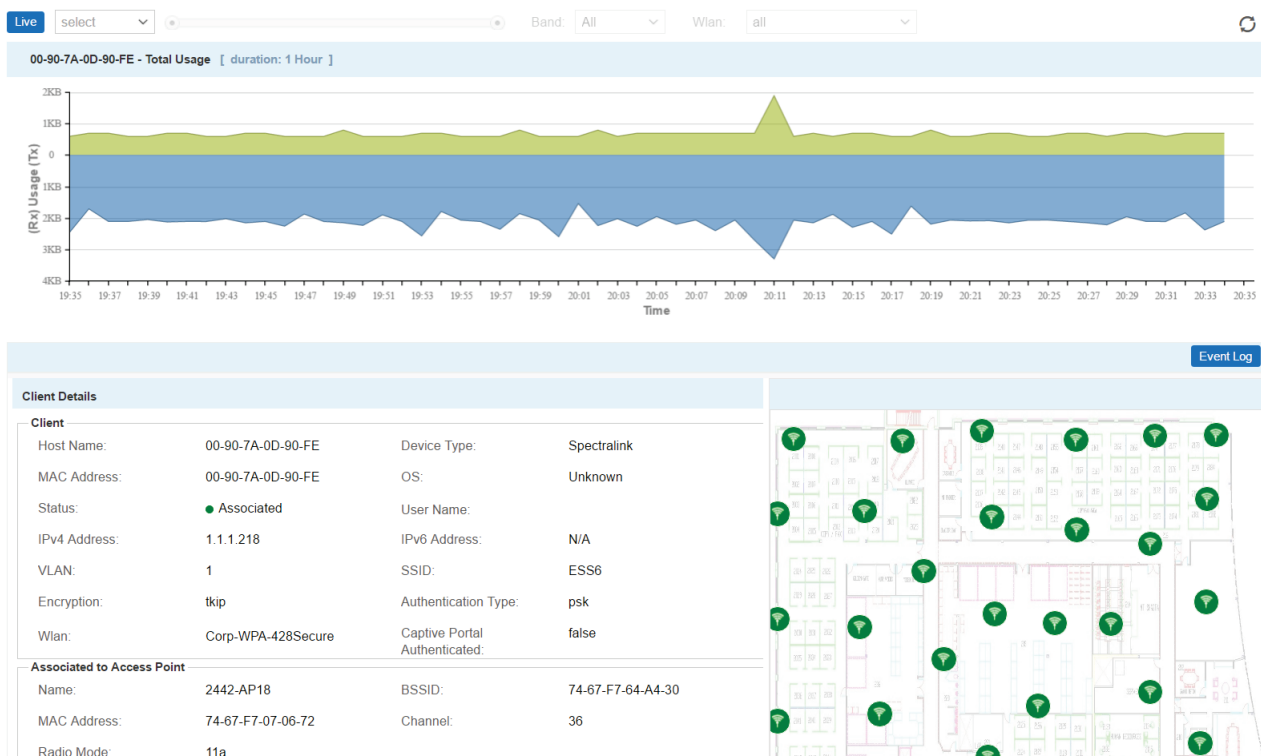
**Note**

The BSSID column is not affected when resetting the columns in the clients grid.

## Client Details

To view details of a NSight manage client:

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

- 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 NSight administrator as a known device.

To view a summary of all rogue APs:

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

The Rogue APs screen displays.

RF Domain	Total Rogue AP	Rogue AP	Interfering Rogue AP	Friendly Rouge AP	Unsanctioned AP
EMEATECH	75	0	0	0	75
home-udolini	58	0	0	0	58
OUTDOOR	52	0	0	0	52
ZEBRA-PRG	26	5	0	1	20

- Review the following rogue device information detected within the NSight managed network:

<b>Status</b>	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".
<b>BSSID</b>	Displays the <i>Broadcast Service Set ID (BSSID)</i> used for matching and filtering.
<b>Vendor</b>	Lists the manufacturer of the detected Access Point as an additional means of assessing its potential threat.
<b>SSID</b>	Displays the <i>Service Set ID (SSID)</i> of the network to which the detected Access Point belongs.
<b>Signal Strength</b>	Displays the signal strength of the detected Access Point. Use this variable to help determine whether an additional Access Point radio would improve network coverage or add noise.
<b>First Seen</b>	Provides a timestamp when the detected Access Point was first detected.
<b>Top Reporter</b>	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.
<b>RF Domain</b>	The displays the reporting Access Point's RF Domain. This Access Point's RF Domain members are potentially at risk from the rogue device.
<b>Reason</b>	Displays the system assigned reason the detected device is marked as rogue.

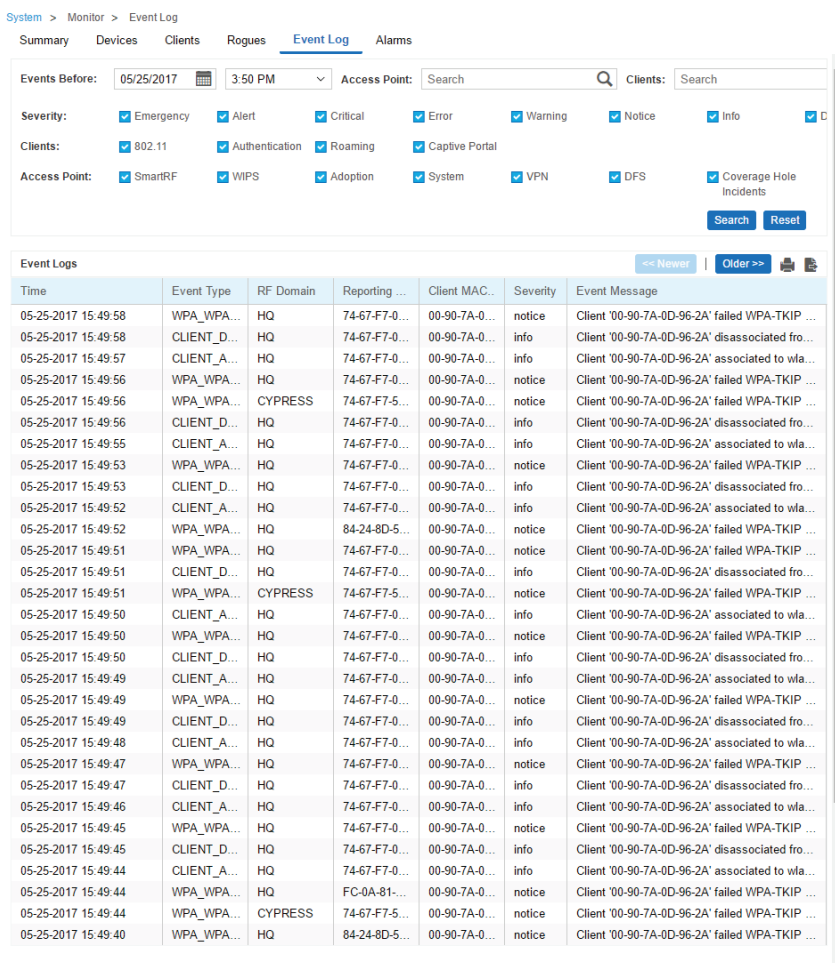
## Event Log

The Event Log provides customizable access to network statistics and log information 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 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.



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:

<b>Events Before</b>	Specify a date and time data collection interval for event data collection.
<b>Access Point (Search)</b>	Enter a search string to limit the data displayed in the event logs to Access Points whose event log entries match the search string.

<b>Clients (Search)</b>	Enter a search string to limit the data displayed in the event logs to clients whose event log entries match the search string.
<b>Clients: 802.11</b>	Select to include client 802.11 entries in the log entries displayed.
<b>Clients: Authentication</b>	Select to include client authentication entries in the log entries displayed.
<b>Clients: Roaming</b>	Select to include client roaming entries in the log entries displayed.
<b>Access Points: Smart RF</b>	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.
<b>Access Points: WIPS</b>	Select to include Access Point <i>Wireless Intrusion Protection System (WIPS)</i> entries in the log entries displayed.
<b>Access Points: Adoption</b>	Select to include Access Point adoption entries in the log entries displayed.
<b>Access Points: System</b>	Select to include Access Point System entries in the log entries displayed.
<b>Access Points: VPN</b>	Select to include Access Point <i>Virtual Private Networking (VPN)</i> entries in the log entries displayed.
<b>Access Points: DFS</b>	Select to include Access Point DFS entries in the log entries displayed.

- When the desired filters and devices are selected, select **Search** to populate the **Event Logs**.
- The **Event Logs** table displays the following log information:

<b>Time</b>	Displays the timestamp (in the browser's timezone) when each log entry was created.
<b>Event Type</b>	Displays the message type displayed in the event log table.
<b>RF Domain</b>	Displays the log originator's RF Domain membership.
<b>AP MAC</b>	Displays the hardware encoded MAC address of the Access Point associated with each event message.
<b>Client MAC</b>	Displays the hardware encoded MAC address of the client associated with each event message.
<b>Severity</b>	Lists the severity for each analytic event. Severity levels include 0 - <i>Emergency</i> , 1 - <i>Alert</i> , 2 - <i>Critical</i> , 3 - <i>Errors</i> , 4 - <i>Warning</i> , 5 - <i>Notice</i> , 6 - <i>Info</i> and 7 - <i>Debug</i> .
<b>Event Message</b>	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.

- 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 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 than events, which are enabled/disabled and raised without a defined threshold being exceeded and a rate limit logic.

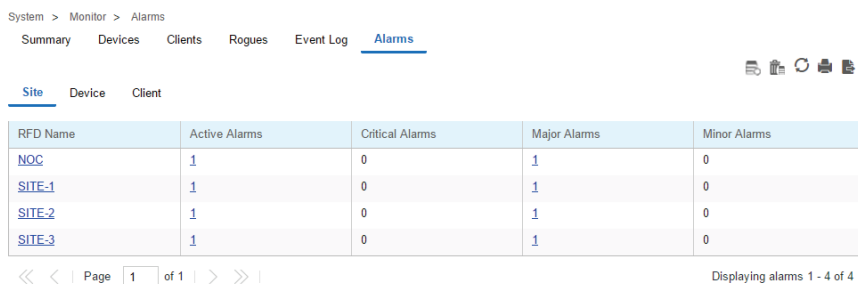
A consolidated summary of alarms (in the form of graphs and charts) is available in the Dashboard. Users can drill down into the graphs and charts to review granular alarm details and their history.

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 **Alarm** from the menu

The most recent 30 **Alarms** display.



3. Refer to the following alarm information:

<b>RFD Name</b>	Displays the RF Domain name whose member devices the alarm is associated with.
<b>Active Alarms</b>	Displays the number of enabled alarms associated with each RF Domain.
<b>Severity</b>	Use the drop-down menu to specify a severity at which the alarm is triggered. Severity options and colors include:  <i>Critical</i> - Immediate action needed (red)  <i>Major</i> - Action needed as soon as possible (orange)  <i>Minor</i> - Watch the situation carefully (yellow)  <i>Clear</i> - Moves an alarm from an active (raised alarm state) to a cleared state.
<b>Critical Alarm</b>	Displays the number of critical level alarms associated with each RF Domain in red. Critical alarms require immediate action.

<b>Major Alarm</b>	Displays the number of major level alarms associated with each RF Domain in orange. Major alarms require action as soon as possible.
<b>Minor Alarm</b>	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.
<b>Impacted Devices</b>	Displays the number of devices in the associated RF Domain impacted by the <i>Critical Alarm</i> , <i>Major Alarm</i> and <i>Minor Alarm</i> .

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 string *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.

# Reports

## Reports Overview

The Reports screen provides report generation and viewing tools in six categories. Reports can be run manually or scheduled at a certain time or 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.

System > Reports > Generated Reports

Generated Reports    Manage Reports    Scheduled Reports    Report Builder

<input type="checkbox"/>	Report	Template Name	User	Start Date	End Date	Run on	Actions
<input type="checkbox"/>	<a href="#">All Clients</a>	All Clients	admin	2017-03-18	2017-05-31	2017-05-25 01:0...	
<input type="checkbox"/>	<a href="#">All RF</a>	All RF	admin	2017-03-18	2017-06-30	2017-05-25 01:0...	
<input type="checkbox"/>	<a href="#">PCI Compliance</a>	PCI Compliance...	admin	2017-03-18	2017-06-30	2017-05-25 01:0...	
<input type="checkbox"/>	<a href="#">All Utilization</a>	All Utilization	admin	2017-05-15	2017-06-30	2017-05-25 01:0...	
<input type="checkbox"/>	<a href="#">All AVC</a>	All AVC	admin	2017-03-18	2017-06-30	2017-05-25 01:0...	
<input type="checkbox"/>	<a href="#">All Network</a>	All Network	admin	2017-03-18	2017-06-30	2017-05-25 01:0...	
<input type="checkbox"/>	<a href="#">All Device</a>	All Device	admin	2017-05-15	2017-06-30	2017-05-25 01:0...	
<input type="checkbox"/>	<a href="#">Clients</a>	All Clients	admin	N/A	N/A	2017-05-24 02:4...	
<input type="checkbox"/>	<a href="#">client</a>	All Clients	admin	N/A	N/A	2017-05-24 12:2...	
<input type="checkbox"/>	<a href="#">All Device</a>	All Device	admin	2017-05-15	2017-06-30	2017-05-24 01:0...	
<input type="checkbox"/>	<a href="#">PCI Compliance</a>	PCI Compliance...	admin	2017-03-18	2017-06-30	2017-05-24 01:0...	
<input type="checkbox"/>	<a href="#">All Utilization</a>	All Utilization	admin	2017-05-15	2017-06-30	2017-05-24 01:0...	
<input type="checkbox"/>	<a href="#">All AVC</a>	All AVC	admin	2017-03-18	2017-06-30	2017-05-24 01:0...	
<input type="checkbox"/>	<a href="#">All Network</a>	All Network	admin	2017-03-18	2017-06-30	2017-05-24 01:0...	
<input type="checkbox"/>	<a href="#">All Clients</a>	All Clients	admin	2017-03-18	2017-05-31	2017-05-24 01:0...	
<input type="checkbox"/>	<a href="#">All RF</a>	All RF	admin	2017-03-18	2017-06-30	2017-05-24 01:0...	
<input type="checkbox"/>	<a href="#">All Clients</a>	All Clients	admin	2017-03-18	2017-05-31	2017-05-23 01:1...	
<input type="checkbox"/>	<a href="#">All AVC</a>	All AVC	admin	2017-03-18	2017-06-30	2017-05-23 01:0...	
<input type="checkbox"/>	<a href="#">All Utilization</a>	All Utilization	admin	2017-05-15	2017-06-30	2017-05-23 01:0...	
<input type="checkbox"/>	<a href="#">All Network</a>	All Network	admin	2017-03-18	2017-06-30	2017-05-23 01:0...	
<input type="checkbox"/>	<a href="#">All Device</a>	All Device	admin	2017-05-15	2017-06-30	2017-05-23 01:0...	
<input type="checkbox"/>	<a href="#">All RF</a>	All RF	admin	2017-03-18	2017-06-30	2017-05-23 01:0...	
<input type="checkbox"/>	<a href="#">PCI Compliance</a>	PCI Compliance...	admin	2017-03-18	2017-06-30	2017-05-23 01:0...	
<input type="checkbox"/>	<a href="#">All Clients</a>	All Clients	admin	2017-03-18	2017-05-31	2017-05-22 01:3...	
<input type="checkbox"/>	<a href="#">All Device</a>	All Device	admin	2017-05-15	2017-06-30	2017-05-22 01:0...	
<input type="checkbox"/>	<a href="#">All Utilization</a>	All Utilization	admin	2017-05-15	2017-06-30	2017-05-22 01:0...	
<input type="checkbox"/>	<a href="#">All Network</a>	All Network	admin	2017-03-18	2017-06-30	2017-05-22 01:0...	
<input type="checkbox"/>	<a href="#">All AVC</a>	All AVC	admin	2017-03-18	2017-06-30	2017-05-22 01:0...	
<input type="checkbox"/>	<a href="#">PCI Compliance</a>	PCI Compliance...	admin	2017-03-18	2017-06-30	2017-05-22 01:0...	
<input type="checkbox"/>	<a href="#">All RF</a>	All RF	admin	2017-03-18	2017-06-30	2017-05-22 01:0...	

<< < Page 1 of 12 >> >>>

Displaying 1 - 30 of 346

Delete

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

<b>Report</b>	Displays the user configured report name for each scheduled report.
<b>Template Name</b>	Displays the name of the template selected when generating each report.
<b>User</b>	Displays the name of the user that generated the report.
<b>Start Date</b>	Lists each report's compilation start time. Report information is gathered from this time through the listed end date.
<b>End Date</b>	Lists each report's compilation end time. Information is not trended and reported after this date, so ensure the trending period is long enough to apply significance to the report data.
<b>Run On</b>	Displays the ending date and time that each report was finished.
<b>Actions</b>	<p>Select the report output best suited to your reporting needs. Options include:</p> <p><i>PDF</i>: Generates a PDF containing the select alarm details.</p> <p><i>CSV</i>: Generates a <i>Comma Separated Values</i> (CSV) file containing the selected alarm details.</p> <p><i>Delete</i>: Selecting "X" will delete the selected alarm from the generated report.</p>

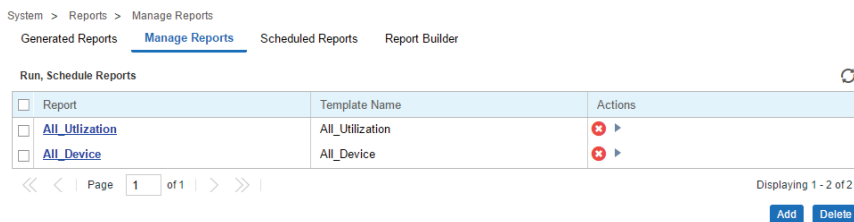


## Manage Reports

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.



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

<b>Report</b>	Displays the user configured report name for each managed report.
<b>Category</b>	<p>Displays the report category for each managed report. The categories are:</p> <ul style="list-style-type: none"> <li>Device Type / Firmware Summary</li> <li>Device Summary</li> <li>Client Inventory</li> <li>PCI Report</li> <li>Network Usage</li> <li>RF Health</li> </ul> <p>Selecting the <i>Category</i> column allows sorting reports by category and customizing the <i>Columns</i> available.</p>
<b>Options</b>	Displays the report options selected and utilized for each listed report.

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

<b>Title</b>	Enter a descriptive title for the report. This is the report name that displays in the <b>Manage Reports</b> and <b>Generated Reports</b> screen.
--------------	---

<p><b>Type</b></p>	<p>Select a report type from the pull-down menu. Available report types are:</p> <p><b>Device Type / Firmware Summary</b></p> <p><b>Device Summary</b></p> <p><b>Client Inventory</b></p> <p><b>PCI Report</b></p> <p><b>Network Usage</b></p> <p><b>RF Health</b></p>
<p><b>Scope Type</b></p>	<p>Select <i>System</i> or <i>Site Group</i> to specify where the report will be run. This is used in conjunction with <i>Scope</i> to customize report information.</p>
<p><b>Scope</b></p>	<p>If <i>System</i> is selected, optionally use the pull-down menu to specify an RF Domain for the report to be run on. Leaving <i>System</i> selected will run the report on the entire system. If <i>Site Group</i> is selected use the pull-down menu to specify a site group for the report to run on.</p>
<p><b>Period</b></p>	<p>Select a time period for report data from the pull-down menu. Available time period options are:</p> <p><b>Last Hour</b></p> <p><b>Last Day</b></p> <p><b>Last Week</b></p> <p><b>Last Month</b></p> <p><b>Custom</b> When <i>Custom</i> is selected specify a <i>Start Date</i> and <i>Time</i> and an <i>End Date</i> and <i>Time</i> for the report range.</p>
<p><b>Schedule</b></p>	<p>Select <i>Schedule</i> to enable the report to be run at specific intervals. When <i>Schedule</i> is enabled, specify a <i>Start Date</i> and <i>End Date</i> and specify the frequency in the <i>Recurrence</i> field.</p>
<p><b>Recurrence</b></p>	<p>When <i>Schedule</i> 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 the time of day that the report should run.</p>
<p><b>Format</b></p>	<p>Select one or more report output formats. Reports can be output in PDF format or <i>Comma Separated Values</i> (CSV) format. Both formats may be selected simultaneously.</p>
<p><b>Destination</b></p>	<p>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.</p>

## 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.

Scheduled Reports								
Report	Type	Subject	User	Start Date	End Date	Frequency	Actions	
<input type="checkbox"/>	Test Report	Device Summary	Test Report	techpub	Sun Jun 12 2016 0...	Sun Jun 19 2016 0...	Daily	
<input type="checkbox"/>	Test Report	Device Summary	Test Report	techpub	Sun Jun 12 2016 0...	Sun Jun 19 2016 0...	Daily	

Page 1 of 1 | Displaying 1 - 2 of 2 | [Delete](#)

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

<b>Report</b>	Displays the user configured report name for each generated report.
<b>Type</b>	Displays the report category for each scheduled report. The categories are:  <b>Device Type / Firmware Summary</b>  <b>Device Summary</b>  <b>Client Inventory</b>  <b>PCI Report</b>  <b>Network Usage</b>  <b>RF Health</b>
<b>Subject</b>	Displays the user configured subject line for scheduled E-mail reports.
<b>User</b>	Displays the name of the administrator generating the report.
<b>Start Date</b>	Lists each report's compilation start time. Report information is gathered from this time through the listed end date.
<b>End Date</b>	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.
<b>Frequency</b>	Displays the frequency in days, hours and minutes each report is scheduled to run.
<b>Actions</b>	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**.

System > Reports > Report Builder

Generated Reports   Manage Reports   Scheduled Reports   Report Builder

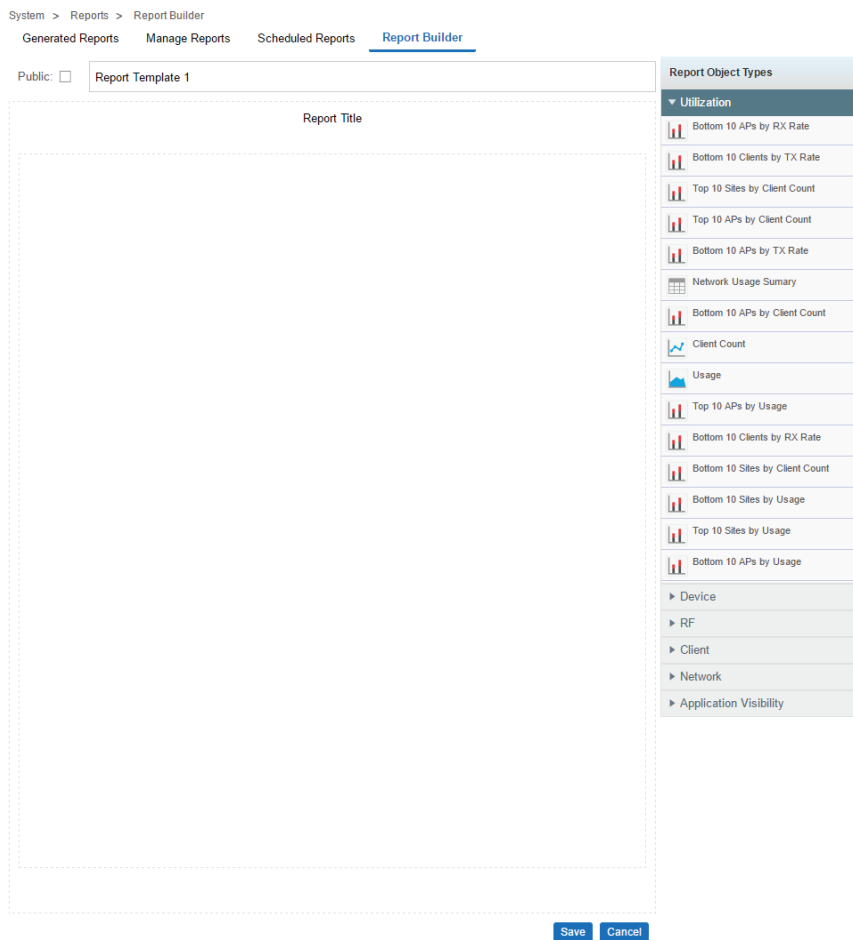
Report Templates ↻ +

Templates	Created BY	Actions
PCI Compliance Report	system	  
All RF	admin	  
All Clients	admin	  
All Network	admin	  
All AVC	admin	  
All_Utilization	admin	  
All_Device	admin	  

4. The **Report Templates** table contains the following:

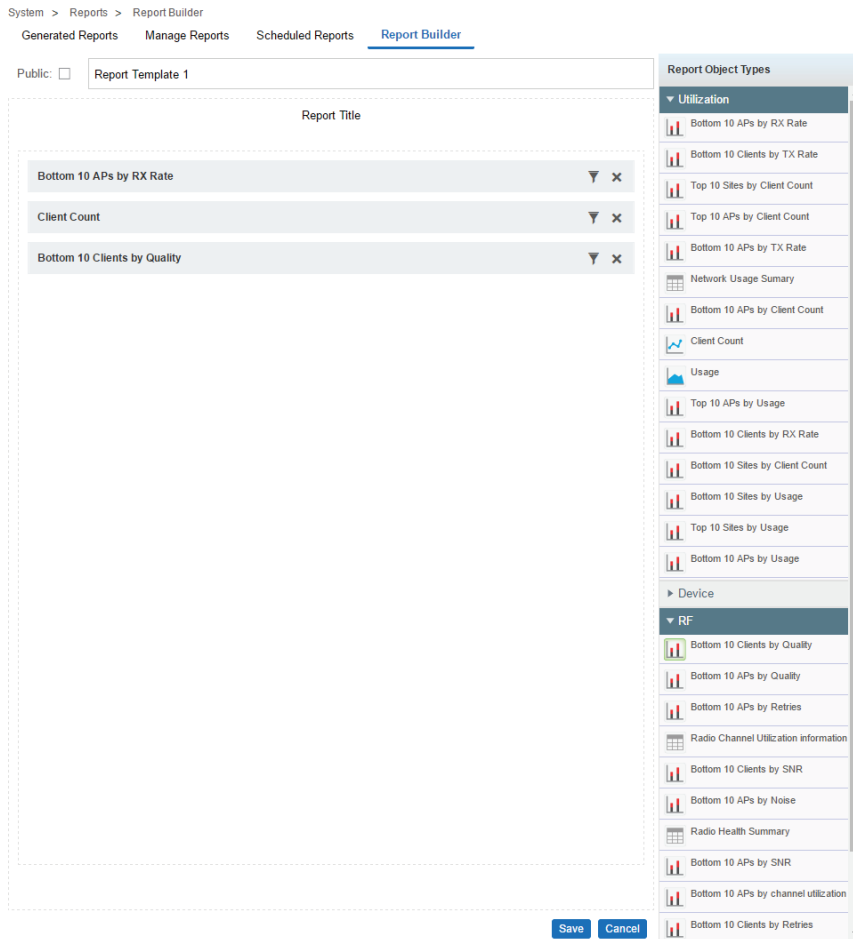
<b>Templates</b>	Displays the name of each configured report template. To edit the title of a template select the <i>Edit Reports Template</i> button associated with that report.
<b>Created By</b>	Displays the user that created each report template. Templates created by the system can be viewed and copied, but man not be edited or deleted.
<b>Actions</b>	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.

5. 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**.

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



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

<b>Public</b>	Select <i>Public</i> to make the report template available to all users on the system.
<b>Report Name</b>	Specify a unique Report Name used to identify each report template.
<b>Report Object Types</b>	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: <i>Device, RF, Network, Utilization, Client</i> and <i>Application Visibility</i> .

- 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**.
- To create a report template from scratch select the + in the upper right of the Report Templates section. In the report template specify the following values:

<b>Public</b>	Select <i>Public</i> to make the report template available to all users on the system.
<b>Report Name</b>	Specify a unique Report Name used to identify each report template.

<b>Report Object Types</b>	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: <i>Device, RF, Network, Utilization, Client</i> and <i>Application Visibility</i> .
----------------------------	---

9. To remove a report template, select the **Delete Report Template** button next to the report template you wish to delete.





# Tools

## Tools Overview

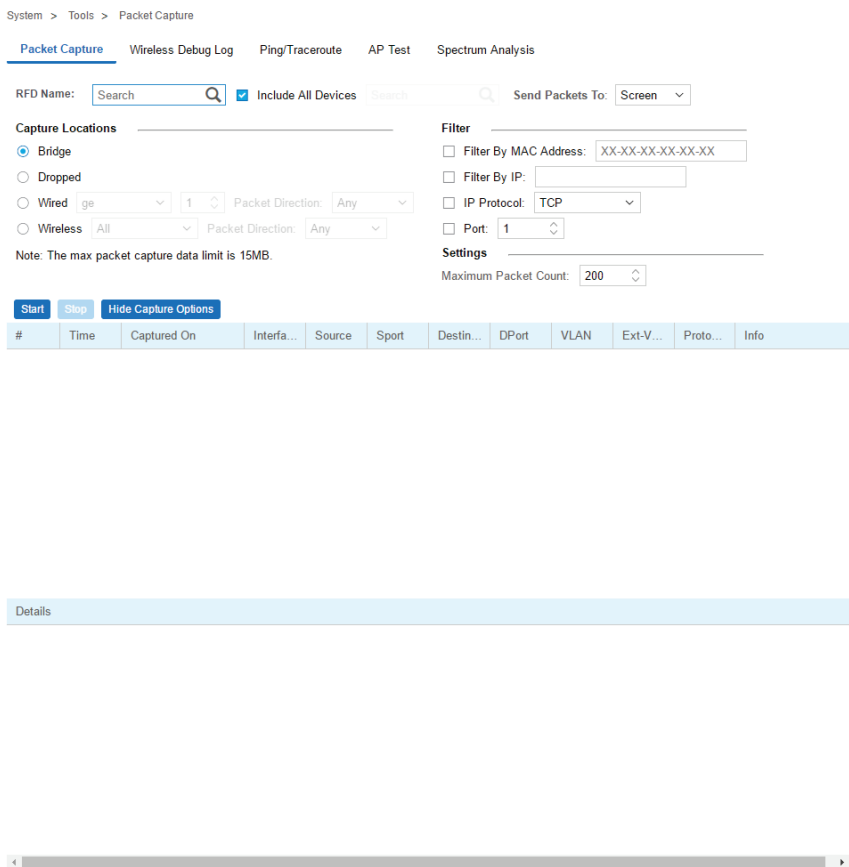
The **Tools** screen provides network troubleshooting tools to help diagnose connectivity and quality issues on the managed network. The **Tools** screen provides tools for packet capture, wireless debugging, ping / traceroute, AP testing and Spectrum Analysis.

## Packet Capture

Periodically launch the packet capture tool to save capture information on a local file to share with the interested parties.

To access **Packet Capture**:

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



<b>RFD Name</b>	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.
<b>Include All Devices</b>	Select this option to include all device types from the specified RF Domain in the packet capture.
<b>Send Packets To</b>	Use the <i>Send Packets To</i> drop-down menu to select where packet capture messages are archived. If <i>Screen</i> is selected, packet capture information is sent to the section at the bottom of the dialog window. If <i>File</i> is selected, the file location must be specified in the <i>File Location</i> section of the window.
<b>Dropped</b>	Select <i>Dropped</i> to create an event entry each time a packet is dropped from a RF Domain member connected client.. 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.
<b>Capture Location</b>	Specify a <i>Capture Location</i> on a specific RF Domain member interface. Select <i>All Wired Interfaces</i> to capture packets from all wired interfaces. Selecting <i>Dropped</i> will only capture dropped packets. If <i>Wired</i> or <i>Wireless</i> is selected, specify the interface name, number and <i>Packet Direction</i> .
<b>Filter (MAC, IP, Protocol, Port)</b>	Filter packet captures based on specific criteria. Select one or more of the following and specify the relevant information:  <b>Filter by MAC</b>  <b>Filter By IP</b>  <b>IP Protocol</b>  <b>Port</b>
<b>Maximum Packet Count</b>	Set the <i>Maximum Packet Count</i> to limit the number of packets captured for trending. Set between 1 - 4000 packets, with a default value of 200.

3. Select **Start** to begin the packet capture. Information displays in the lower portion of the window. If the data is sent to a file, that file populates with the packet capture. If setting a long message capture and wish to end early, select **Stop**.

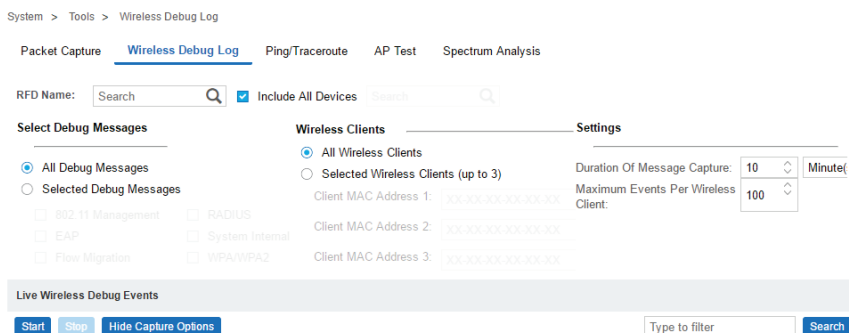
<span>Packet Capture</span> <span>Wireless Debug Log</span> <span>Ping/Traceroute</span>											
<span>Start</span> <span>Stop</span> <span>Show Capture Options</span> <span>Save To Disk</span> <span style="float: right;">Type to search</span>											
#	Time	Captured On	Interf...	Source	Sport	Desti...	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

## 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.



3. The **Wireless Debug Log** tab displays the following:

<b>RFD Name</b>	Displays the RF Domain whose member devices contribute wireless client debug information to the log.
<b>Include All Devices</b>	Use the <i>Include All Devices</i> option to include debug messages from all clients, their connected Access Points and managing controllers or service platforms in the selected RF Domain.
<b>Select Debug Messages</b>	<p>Select <i>All Debug Messages</i>, to display all wireless client debug information for selected RF Domain member clients. Choose <i>Selected Debug Messages</i> to specify which wireless client debug messages to display. If <i>Selected Debug Messages</i> is selected, displays information for any combination of the following:</p> <p><b>802.11 Management</b></p> <p>EAP</p> <p>Flow Migration</p> <p>RADIUS</p> <p>System Internal</p> <p>WPA/WPA2</p>
<b>Wireless Clients</b>	Select <i>All Wireless Clients</i> to display debug information for each client connected to a RF Domain member Access Point radio. Choose <i>Selected Wireless Clients</i> to display information only for specific wireless clients (between 1 and 3). If <i>Selected Wireless Clients</i> 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.
<b>Duration of Message Capture</b>	Use the spinner controls to select how long to capture wireless client debug information. Select from 1 second to 24 hours, with the default value of 1 minute.
<b>Maximum Events Per Wireless Client</b>	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.

<b>File Location</b>	<p>When the <i>Send Data To</i> field is set to File, the <i>File Location</i> configuration displays below the configuration section. If <i>Basic</i> is selected, enter the URL in the following format:</p> <p><i>URL Syntax:</i>  <code>tftp://&lt;hostname IP&gt;[:port]/path/file</code>  <code>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</code></p> <p><i>IPv6 URL Syntax:</i>  <code>tftp://&lt;hostname [IPv6]&gt;[:port]/path/file</code>  <code>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname [IPv6]&gt;[:port]/path/file</code></p> <p>If <i>Advanced</i> 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.</p>
<b>Live Wireless Debug Events</b>	<p>When the <i>Send Data To</i> field is set to <i>Screen</i>, this area displays live debug information for connected wireless clients in the selected RF Domain.</p>

1. When all configuration fields are complete, select **Start** to begin 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. Select **Stop** if you set a long message capture and wish to end the capture early.

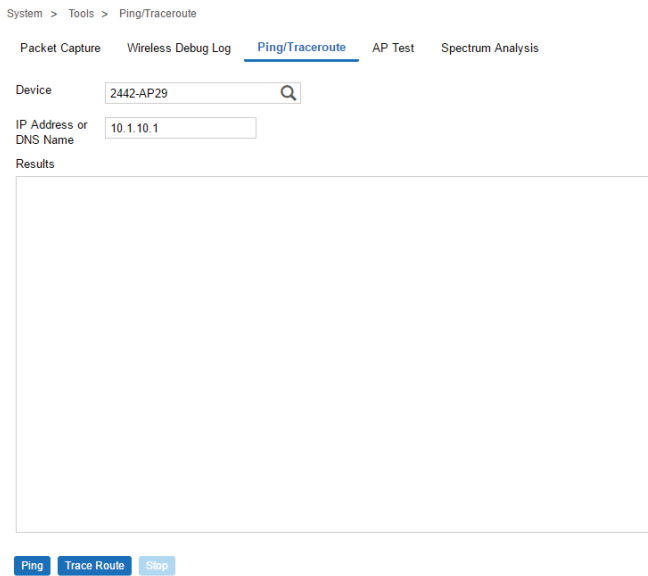
## Ping and Traceroute

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.



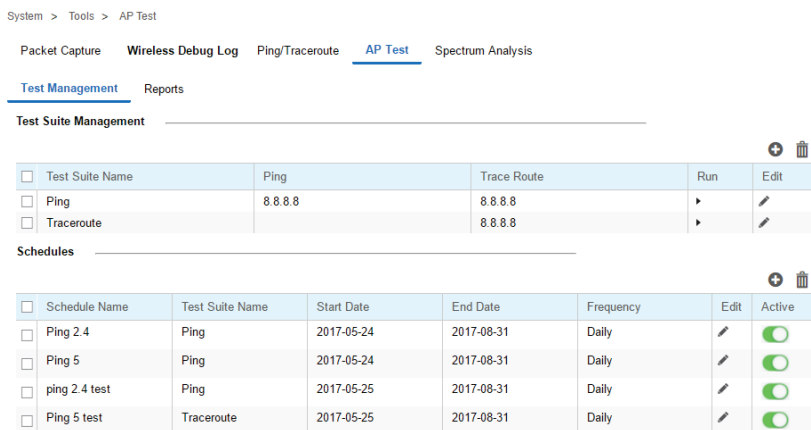
3. Enter the hostname for the device to ping or trace in the **Device** field.
4. Enter the IP address for the device to ping or trace in the **IP Address** field.
5. Once the **Device** or **IP Address** field is populated, select **Ping** to test the reachability of a specified host. Select **Trace 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.

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.

<b>Test Suite Name</b>	Displays the user generated name for each Test Suite.
<b>Ping</b>	Displays the IP address or hostname tested in the ping test if a Ping test is selected as part of the test suite.
<b>Traceroute</b>	Displays the IP address or hostname tested in the Traceroute if a Traceroute is selected as part of the test suite.
<b>Run</b>	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.

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

<b>Test Suite Name</b>	Enter a descriptive name for the new test suite. This name cannot be changed once the Test Suite has been created.
<b>New/Clone</b>	Select <i>New</i> to create a new Test Suite. Select <i>Clone</i> 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.
<b>Ping Test</b>	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.
<b>Traceroute Test</b>	Select to enable a network test that will show the intermediary IPs between the test site and the specified Hostname or Target IP address.
<b>Throughput Test</b>	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 <i>Download</i> or <i>Upload</i> . 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.
<b>Wireless Client</b>	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.

- 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.

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

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

<b>Schedule Name</b>	Specify a descriptive name for the schedule. This name cannot be changed after the schedule has been created.
<b>Test Suite List</b>	Select an existing Test Suite to include it in the schedule.
<b>SSID</b>	Select the WLAN tested during the scheduled tests.
<b>Band</b>	Select the 2.4 Ghz or 5 Ghz wireless Band to isolate in the test data.
<b>Target Device</b>	Once a SSID and band is selected, use the pull-down menu to specify device(s) to test. Multiple target devices may be specified to run during a single test.
<b>Start Date</b>	Enter a starting test date or use the calendar icon to specify the start date.
<b>End Date</b>	Enter an end test date or use the calendar icon to specify the end date.
<b>Recurrence</b>	Specify the interval the scheduled test is run. Select Daily, Weekly or Monthly and the test will be performed at that interval between the Start and End Dates at the specified time.
<b>Time</b>	Use the pull-down menu to specify the starting time of day that the schedule will be run at. Times are available in 15 minute increments.



System > Tools > AP Test

Packet Capture Wireless Debug Log Ping/Traceroute **AP Test** Spectrum Analysis

Test Management **Reports**

1 week 1 mon 3 mon custom

Search  Records: 30

<input type="checkbox"/>	Test Suite Name	Schedule Name	SSID	Target Device	Tested On	Status	R...
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP34</a>	2017-05-25 11:01 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP07</a>	2017-05-25 11:01 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP22</a>	2017-05-25 11:01 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP37</a>	2017-05-25 11:01 ...		
<input checked="" type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP36</a>	2017-05-25 11:01 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP35</a>	2017-05-25 11:01 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">CYPR-AP06</a>	2017-05-25 11:01 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP18</a>	2017-05-25 11:01 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP26</a>	2017-05-25 11:01 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP13</a>	2017-05-25 11:01 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">CYPR-AP11</a>	2017-05-25 11:01 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP29</a>	2017-05-25 11:01 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP14</a>	2017-05-25 11:01 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">CYPR-AP08</a>	2017-05-25 11:01 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP12</a>	2017-05-25 11:00 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP09</a>	2017-05-25 11:00 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP21</a>	2017-05-25 11:00 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP24</a>	2017-05-25 11:00 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">CYPR-AP01</a>	2017-05-25 11:00 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP05</a>	2017-05-25 11:00 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP31</a>	2017-05-25 11:00 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP33</a>	2017-05-25 11:00 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">CYPR-AP07</a>	2017-05-25 11:00 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP27</a>	2017-05-25 11:00 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP02</a>	2017-05-25 11:00 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP20</a>	2017-05-25 11:00 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP11</a>	2017-05-25 11:00 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP04</a>	2017-05-25 11:00 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP28</a>	2017-05-25 11:00 ...		
<input type="checkbox"/>	Traceroute	Ping 5 test	gable	<a href="#">2442-AP16</a>	2017-05-25 11:00 ...		

<< < Page 1 of 22 >> | Displaying reports 1 - 30 of 645

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.

<b>Schedule Name</b>	Displays the user generated name assigned to the schedule at its creation.
<b>SSID</b>	Displays the name of the WLAN tested for each report.
<b>Target Device</b>	Displays the MAC Address of the target device(s) tested in each report.
<b>Tested On</b>	Displays the date each test was executed.
<b>Status</b>	Displays the status of the test if not completed.

<p><b>Report</b></p>	<p>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.</p>
----------------------	--

## Spectrum Analysis

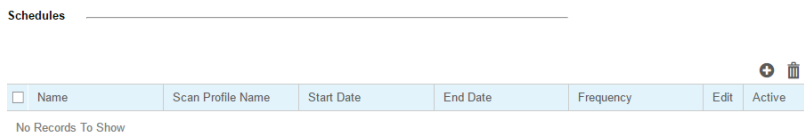
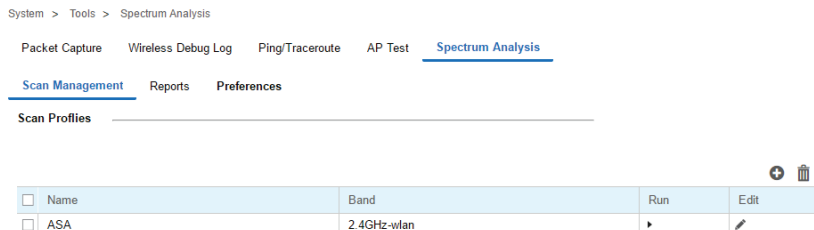
802.11 devices operate in unlicensed 2.4GHz and 5GHz bands and as a result, 802.11 devices experience noise and interference from both neighboring 802.11 networks operating in the same channel and non-802.11 wireless devices such as cordless telephones, wireless cameras, Bluetooth, weather radars, microwave 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.

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:

<b>Name</b>	Displays the user generated name for each <i>Scan Profile</i> .
<b>Band</b>	Displays the RF band that the spectrum analysis will be performed on. The band may be 2.4GHz, 5GHz or both.
<b>Run</b>	Select the <i>Run</i> 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.
<b>Edit</b>	To modify a scan profile select the edit button next to the profile you wish to change.
<b>Add</b>	To create a new scan profile, select the + button in the upper right of the Scan Profiles table.
<b>Delete</b>	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.

**Create Scan Profile**

Name: \*

New  Clone Profiles List:

Dwell Time(in ms):

Duration(in mins):

2.4GHz  5GHz  Both

**2.4GHz Configuration**

Signal Threshold(dbm):

Duty Cycle Threshold(dbm):

Channel Range:

**5GHz Configuration**

Signal Threshold(dbm):


Duty Cycle Threshold(dbm):

Channel Range:

**Chart Group Selection**

Utilization  Physical Layer  Interference  Spectrum Detail  Custom

**Utilization Charts**



Duty Cycle

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

<b>Name</b>	Create a unique name for each <i>Scan Profile</i> . This name will be used to identify each profile.
<b>New / Clone</b>	Select <i>New</i> to create a scan profile from scratch. Select <i>Clone</i> to populate all of the values of the scan profile using the values from another scan profile.
<b>Dwell Time</b>	Specify an amount of time in milliseconds for the scanning radio to stay on each channel during a scan.

<b>Duration</b>	Specify the total amount of time a scan should run for in minutes.
<b>Band</b>	Select the RF band that the spectrum analysis will be performed on. The band may be <i>2.4GHz</i> , <i>5GHz</i> or <i>Both</i> .
<b>Signal Threshold</b>	Specify a signal power cutoff value, in dBm. The 2.4GHz and 5GHz bands can have different threshold values.
<b>Duty Cycle Threshold</b>	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.
<b>Channel Range</b>	Use the sliders to specify a starting and ending channel range for the 2.4GHz and 5GHz spectrum used in the scan.
<b>Chart Group Selection</b>	The <i>Chart Group</i> 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, <i>Custom</i> may be selected and any combination of <i>Spectrogram</i> , <i>Spectral Density</i> , <i>FFT</i> , <i>Duty Cycle</i> or <i>Interference</i> may be added to the scan report.

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

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

**Create New Schedule**

Schedule Name: \*  Profiles List: \*

Target Device: \*

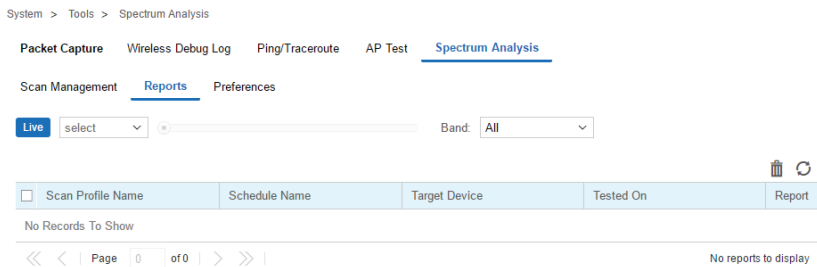
**Schedule Details**

Start Date: \*  End Date: \*

Recurrence:  Time:

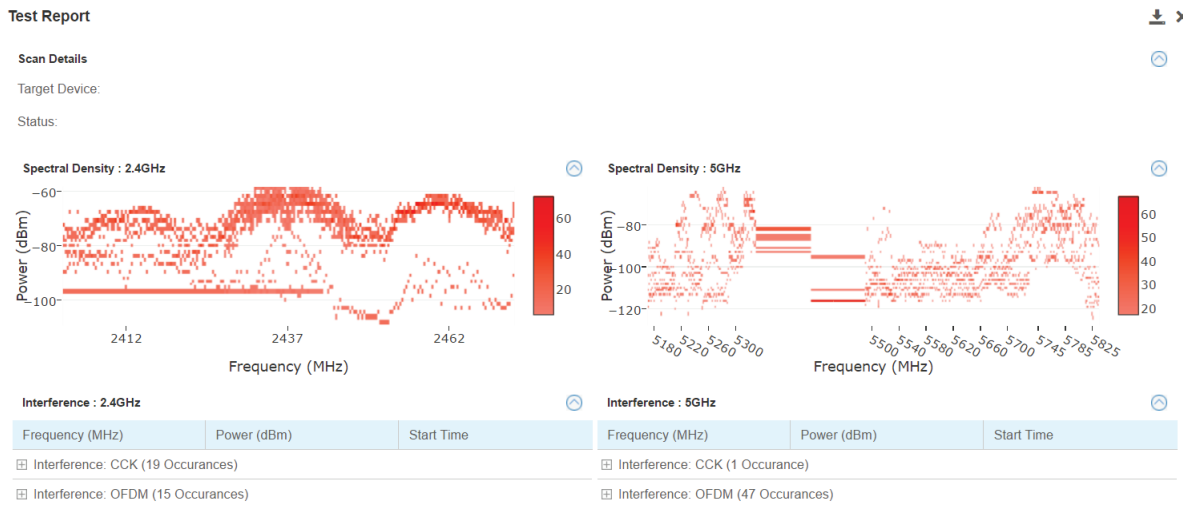
- To create a new scan **Schedule**, select the + button in the upper right of the **Schedules** table and configure the following:

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

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

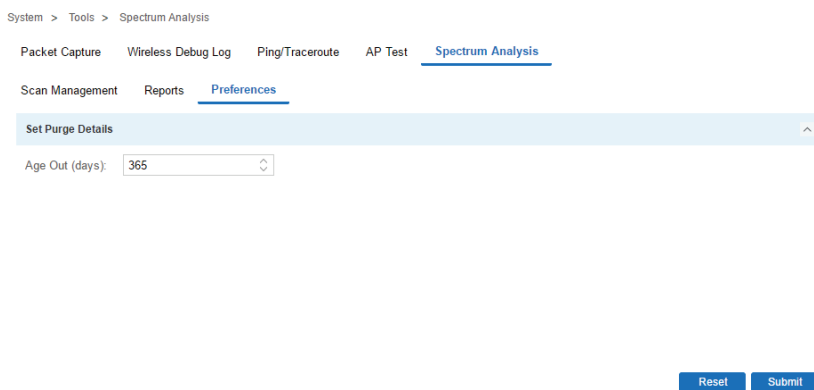


12. The Test Report page displays the following data from the spectrum analysis scan:

<b>Spectrogram</b>	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.
<b>Spectral Density</b>	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.
<b>FFT (Fast Fourier Transformation)</b>	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.
<b>Duty Cycle</b>	<p>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:</p> <p>Current duty cycle: Duty cycle % of latest scanning of that frequency</p> <p>Average duty cycle: Average duty cycle % of that frequency from when this scan was started</p>

<b>Interference</b>	<p>The Interference section displays any of the following non-802.11 wireless devices that are interfering with the sensor:</p> <ul style="list-style-type: none"> <li>CW</li> <li>microwave oven</li> <li>Bluetooth short</li> <li>Bluetooth long</li> <li>cordless phone</li> <li>cck (802.11b)</li> <li>ofdm (802.11a/g)</li> <li>jammer/wideband CW</li> <li>constant transmitter/narrowband CW</li> <li>Proximity Detector</li> </ul> <p>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.</p>
---------------------	--

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.



## Preferences

---

### Alarm Configuration

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 Type	Time Window (Min)	Raising Threshold	Clearing Threshold
DHCP Failure	5	150	100
DNS Failure	5	150	100
Low SNR	5	15	25
Low RSSI	5	-90	-70
High Retries	5	96	60
High Channel Utilization	5	99	60

802.11 EAP Authentication Failure	5	100	50
802.11 EAP Server Timeout	5	100	50
802.11 EAP Client Timeout	5	100	50
High DNS RTT	5	150	50
Site Offline	5	70	50

The *Time Window* in the alarm threshold configuration defines the available time window (in minutes) to detect any alarm. This value is configurable from 0 to 60 (minutes). If this value is set to 0 there's no activity for that alarm.

The *Raising Threshold* defines when a specific alarm is triggered.

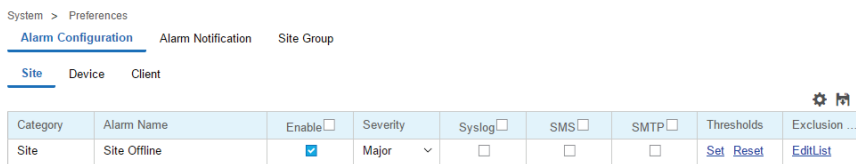
The *Clearing Threshold* defines when an existing alarm is cleared from the system.

With *Radio* alarms (Low SNR, Low RSSI, High Retries and High Channel Utilization), the alarm engine looks at the threshold value per radio (2.4 Ghz, 5 Ghz), and treats them as different alarms. If low RSSI values are detected on both radios, the alarm engine triggers a Low RSSI alarm the for 2.4 GHz and 5 GHz radio separately.

To manage alarms:

1. Select **Preferences** from the upper menu bar.
2. Select the **Alarm Configuration** tab.

The **Alarm Configuration** configurations screen displays.



3. To configure details for each alarm, refer to the following:

<b>Category</b>	Displays the alarm category type. Each alarm falls into a broader alarm category specifying where the alarm took place.
<b>Alarm Name</b>	Displays the name of the alarm type. The Alarm Name is a high level description of what triggered the alarm.

<b>Severity</b>	Use the drop-down menu to specify a severity at which the alarm is triggered. Severity options and their color codes include:  <b>Critical</b> - Immediate action needed (Red)  <b>Major</b> - Action needed as soon as possible (Orange)  <b>Minor</b> - Watch the situation carefully (Yellow)  <b>Clear</b> - Once the alarm status has been cleared
<b>Syslog</b>	Select this option to send alarm notifications to the syslog server(s). The syslog servers are configured in the Alarm Notification tab.
<b>SMS</b>	Select this option to send alarm notifications using SMS. SMS enables users to register with their E-mail or mobile device ID as the primary key for authentication. The SMS service is configured in the Alarm Notification tab.
<b>SMTP</b>	Select this option to send alarm notifications using an outgoing SMTP mail server. The SMTP server and E-mail is configured in the Alarm Notification tab.
<b>Thresholds</b>	To set threshold values for an alarm, select <i>Set</i> and configure the <i>Clearing Value</i> , <i>Time Window</i> , and <i>Trigger Value</i> . Select <i>Reset</i> to return thresholds to their default values.
<b>Exclusions</b>	To exclude clients from the alarm, select <i>Edit List</i> from the <i>Exclusion</i> column and enter a string that matches a client hostname or a string that matches multiple client hostnames.

4. An administrator can apply widgets for an Alarm summary from the widget tables in *Main Tab > Dashboard > Select Widgets*. Available alarm widgets include:

<b>Alarm Summary by Group</b>	Alarm summary information by alarm group.
<b>Alarm Summary by Severity</b>	Alarm summary information by alarm severity.
<b>Alarm Summary by Type</b>	Alarm summary information by alarm type.
<b>Alarm Summary by Sites</b>	Alarm summary information by alarm sites.
<b>Alarm Summary by Devices</b>	Alarm summary information by alarm devices.
<b>Alarm Summary by Timelines</b>	Alarm summary information by alarm timeline.

## Alarm Notification

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.

Note

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

To create or manage Alarm Notifications:

1. Select **Preferences** from the upper menu bar.
2. Select the **Alarm Notifications** tab.

The **Alarm Notifications** configurations tab displays.

System > Preferences

Alarm Configuration **Alarm Notification** Site Group

**Set Purge Details**

Threshold Limit: 50000  
Age Out (days): 365

**SYSLOG**

Syslog Server: server ip address

**SMS**

User Name: username  
Password: password  Show password  
API ID: api-id  
User Agent: user agent  
Source Number: source number  
Send to Number: send to number

**E-Mail**

SMTP Server: smtp-server  
Security: security  
User Name: username  
Password: password  Show password  
Sender: sender  
Recipient Email: recipient  
Sent to Email: send to email

Reset Submit

3. Set Purge Details as follows to configure when alarms are removed:

<b>Threshold Limit</b>	Use the spinner controls or manually enter the maximum number of alarms in the system before old entries are purged.
<b>Age Out (days)</b>	Use the spinner controls or type a number, in days, to specify how many days an alarm is be kept before it is purged.

4. Add the IP address(es) of any additional Syslog Server logging alarms. Select + to add additional syslog servers and specify their IP addresses in the newly added fields.
5. Set the following for the SMS service if using Clickatell **SMS** for alarm notifications:

<b>User Name</b>	Specify the username for the Clickatell SMS account used to send alarm notifications.
<b>Password</b>	Specify the password for the Clickatell SMS account used to send alarm notifications.

<b>API ID</b>	Specify the API ID used in conjunction with the Clickatell SMS account.
<b>Source Number</b>	Specify the source number SMS notifications originate from. This is determined in the Clickatell account.
<b>Send to Number</b>	Specify the destination phone number where SMS alarm notifications are sent. Select + to add additional phone numbers.

6. Set the following if using E-mail for alarm notifications:

<b>SMTP Server</b>	Specify the IP address or hostname of the outgoing mail server send alarm notifications.
<b>Security</b>	Specify the security used by the outgoing SMTP mail server. Examples include open and SSL.
<b>User Name</b>	Specify the user name sending the outgoing mail on the SMTP server.
<b>Password</b>	Specify the password for outgoing mail on the SMTP server.
<b>Sender</b>	Specify the sender listed in the from field of the outgoing E-mail.
<b>Recipient Email</b>	Specify the destination E-mail address indicated in the from field of the outgoing E-mail.
<b>Sent to Email</b>	Specify the destination E-mail address where alarm notifications are sent. Select + to add additional addresses.

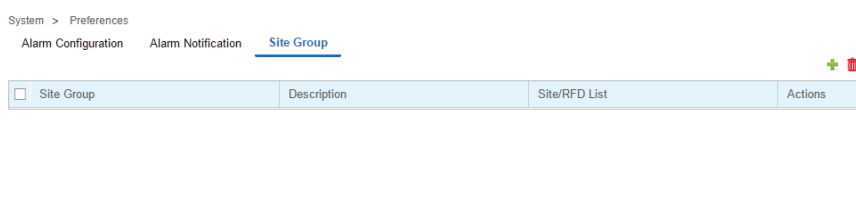
## Site Group

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:

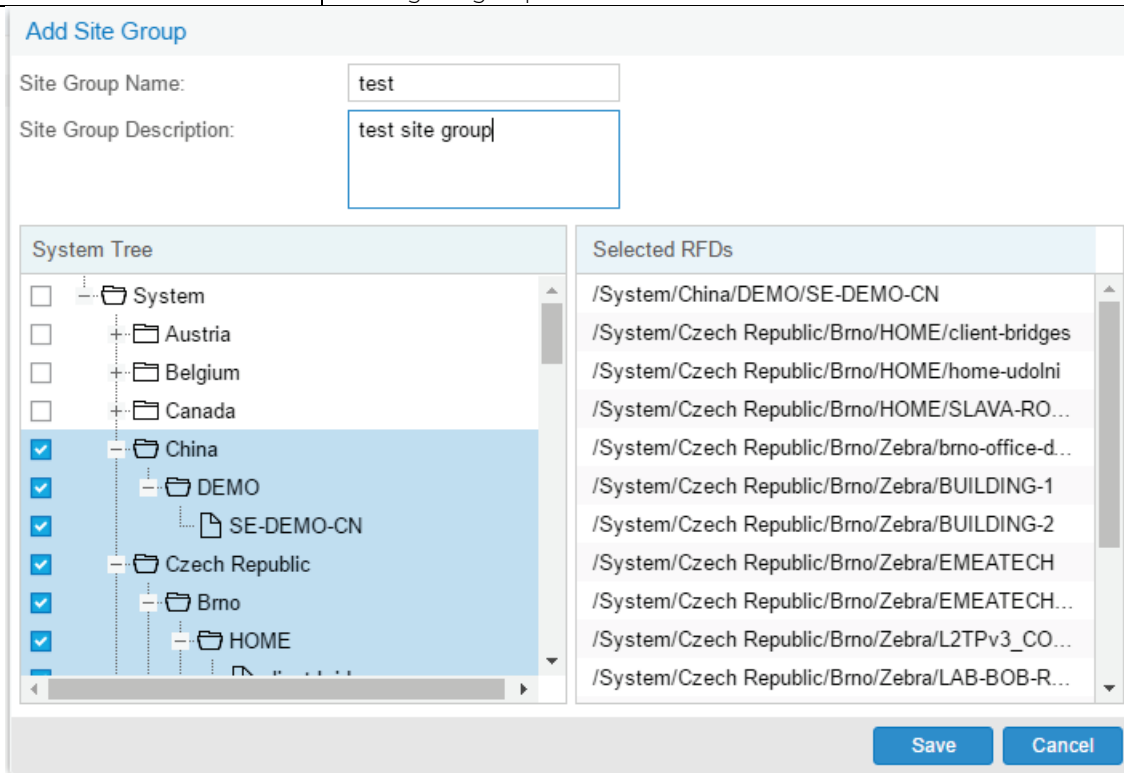
1. Select **Preferences** from the upper menu bar.
2. Select the **Site Group** tab.

The **Site Group** management tab displays.



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

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



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