NSight 5.8.2

User Guide

MN-002679-01

Contents

OVERVIEW

In This Chapter

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, Zebra 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 Zebra NSight is continued to be supported on the NX (95xx & 96xx) & VX platforms as a launch-able application with WING. With flexible deployment options, Zebra NSight can now scale to support 40,000 Access Points.

Zebra 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.

Zebra 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 (helpdesk, 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:

- Packet capture
- Wireless Debug log access
- TCP/IP Ping & Traceroute

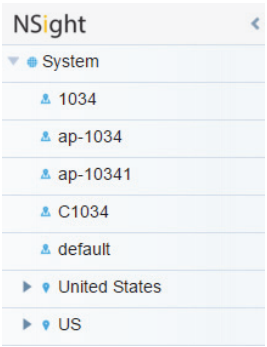
When reviewing Access Point details or a client details page, an administrator can review a summary of each event related to the device by launching the event log browser with appropriate filters applied for the device and, if desired, launch the packet capture tool and save the capture information to 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

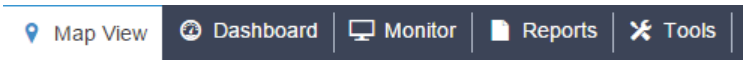
Zebra's NSight user interface is navigated using two primary menus, the Left Nav and the Top Nav.



The Left Nav displays a hierarchical view of locations and sites in the network. Selecting a site from the Left Nav will update the data displayed 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. 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 information. KMS also displays 2.4GHz and 5GHz frequency bands for specific RF Domains. Clicking on a specific RF Domain displays additional details.

MAP VIEW

In This Chapter

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 that includes RF channel assignments, SNR, retries, power, throughput, client count and other data.

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

Map View (System)

To view geographical or site based network maps:

1 Select **Map View** from the upper menu bar.

2 In the Left Nav select **System**.

The system level network map displays.

At the system level the Map View displays all the sites with site locations displayed geographically for immediate visualization of the entire network. The Map View also displays 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 that includes RF channel assignments, SNR, retries, power, throughput, client count and other data.

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

To customize a site level map:

APs & Radios: Online	Select this option to show all online APs and radios in the site map. Deselecting this option hides all online APs and Radios.
APs & Radios: Offline	Select this option to show all offline APs and radios in the site map. Deselecting this option hides all offline APs and Radios.
APs & Radios: 2.4 GHz / 5.0 GHz	Select either 2.4 GHz or 5.0 GHz to define which RF band to show on the floor map.
RF Attributes: Channel	Select this option to display RF channels on the floor map. Deselecting this option hides RF channel information.
RF Attributes: Power	Select this option to display power levels on the floor map. Deselecting this option hides power level information.
RF Attributes: SNR	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. Deselecting this option hides signal to noise ratio information.
Utilization: Throughput	Select this option to display data throughput speed on the floor map. This value helps administrators assess the level of radio interference that can be tolerated within the network. Deselecting this option hides data throughput speed information.
Utilization: Client Count	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. Deselecting this option hides adopted client count information.
Utilization: Usage	Select this option to display usage information on the floor map. Deselecting this option hides usage information from the floor map.

Utilization: Retries	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. Deselecting this option hides client retry information from the floor map.
Show: Heat Map	Select this option to display RF heat map information in the floor map. The heat map information displays RF coverage levels from red to green based on signal strength. Deselecting this option will hide heat map from the floor map.
Show: Floor Map	Select this option to display the Floor Map image. The floor map is an image showing geographical map of the site. Deselecting this option will hide the floor map image.
Show: Clients	Select this option to display client details on the floor map. Clients are represented by blue dots on the floor map. Deselecting this option hides client information from the floor map.
Show: Table	Select this option to display a table with RF attributes for each AP and radio in the site.
Apply Filters: SNR	When *SNR* 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.
Apply Filters: Power	When *Power* is selected in RF Attributes, use the slider to filter the information based on selected power range.
Apply Filters: Throughput	When *Throughput* is enabled in *Utilization*, use the *Throughput* pull-down menu to filter information based on selected throughput range.

DASHBOARD

In This Chapter

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 geographical location or site from the Left Nav.

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

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

Create customized 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:

- Select a Dashboard theme to define the number of panels and their order on the Dashboard
- Drag and drop Dashboard widgets (from the Dashboard widget library) to define what data is displayed in each panel
- Name the Dashboard and save

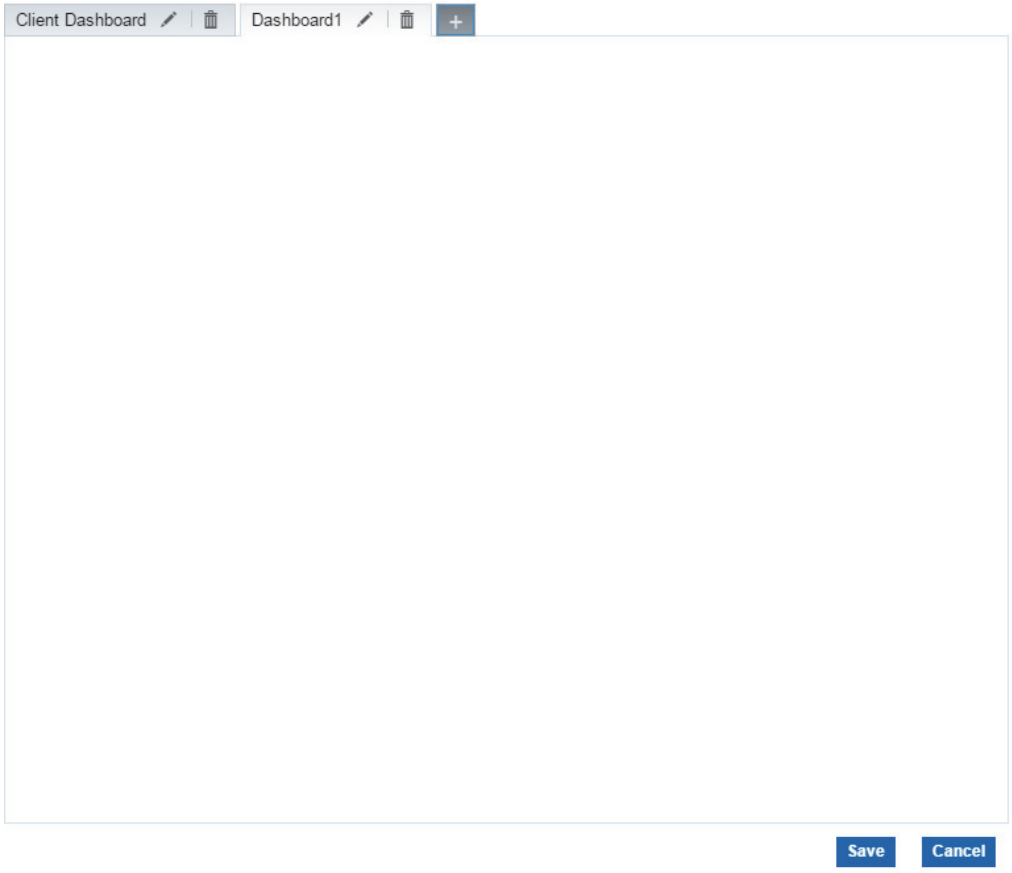
To create a new (blank) Dashboard that can be manually populated with customized data (widgets):

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

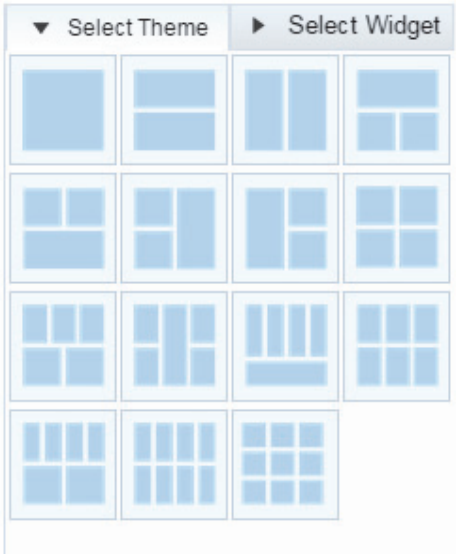
Note: Selecting **System**, locations or sites from the Left Nav changes the network information displayed. However Dashboard tabs are system-wide and not associated with a specific site or location.

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

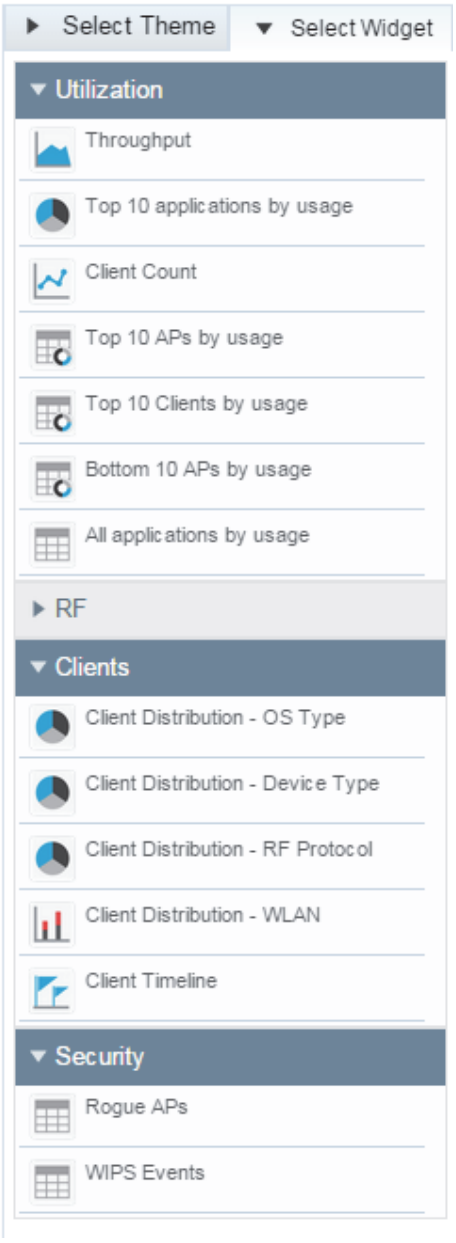
A blank **Dashboard** tab displays.



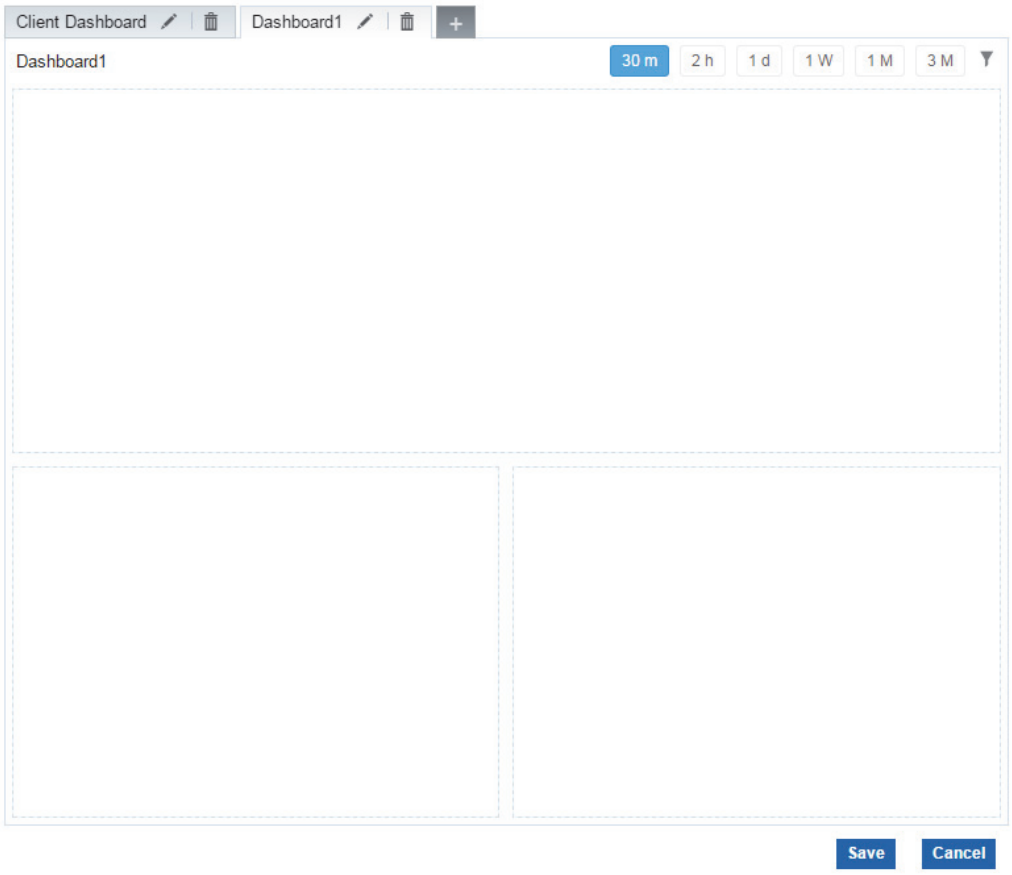
3 From the **Select Theme** menu, choose a theme (screen panel layout) and drag the theme into the blank Dashboard.



4 From the **Select Widget** menu, select either **Utilization**, **RF**, **Clients** or **Security** 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 panels is populated.



6 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.

7 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.

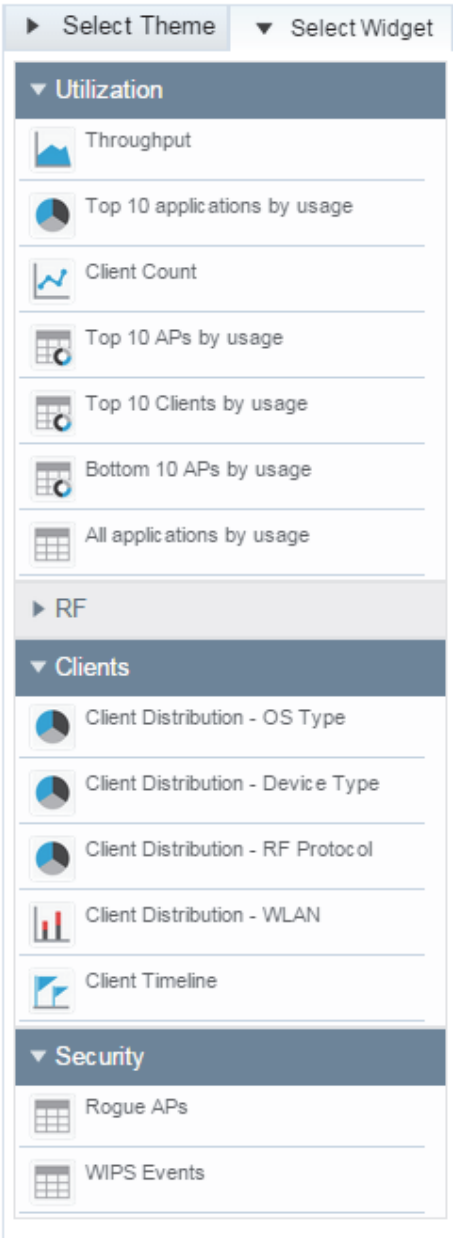
To modify the configuration of an existing Dashboard:

8 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.

9 Select the pencil icon at the top of the page next to any existing tab to edit that tab's name.

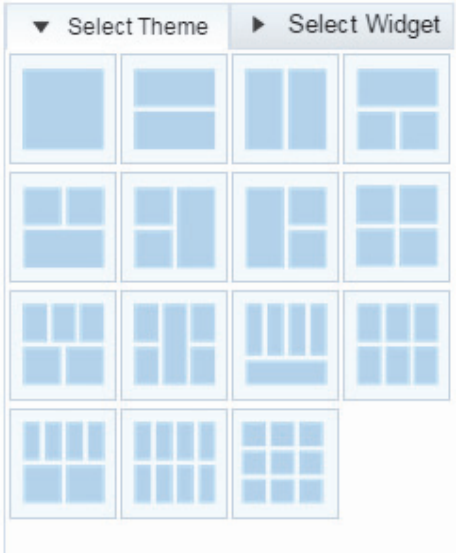
10 To replace existing widgets, select either **Utilization**, **RF**, **Clients** or **Security** from the **Select Widget** menu and use the arrow to expand the list.



11 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.

12 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.

13 To change the layout of an existing tab from the **Select Theme** menu, choose a page layout and drag that layout to the existing tab. The existing tab layout and widgets are replaced by the new layout.



14 Select **Save** to commit the changes to the **Dashboard** tab or **Cancel** to undo any unsaved changes.

MONITOR

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

In This Chapter

Summary (System)

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

To view a summary of all monitored devices:

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

2 In the Left Nav select **Summary**.

The summary screen displays.

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

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

WLAN	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.
Band	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 2.5 and 5 GHz radio bands.
Trending Period	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.
Refresh	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:

AP Name	Lists the administrator assigned name of each top performing Access Points. The name displays as a link that can be selected to display this Access Point's information in greater detail.
IP Address	Lists the Access Point IP address used as its network identifier.
RF Domain	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.

Channel	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.
Usage	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.
Clients	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.

WLAN Name	Lists each top performing WLAN whose member Access Points and connected clients report the highest usage.
Usage	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.
Clients	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 and displayed as a graph.

Device Name	Lists each top performing device's name (by manufacturer) whose connected clients report the highest network utilization (in Megabytes).
Usage	Lists each top performing device's network utilization in megabytes. Assess this integer in respect to the number of connected clients for consistency.
Clients	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 and displayed as a graph.

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 and displayed as a graph. 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 represents upstream data and is shown on the upper half of the graph. Blue represents downstream data and is shown on the lower half of the graph.

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

WLAN	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.
Band	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 2.5 and 5 GHz radio bands.
Trending Period	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.
Refresh	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 for specific WLANs and radio bands.

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:

AP Name	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.
IP Address	Lists the Access Point IP address used as each Access Point's network identifier.
RF Domain	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.

Channel	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.
Usage	Lists top performing Access Point throughput in megabytes. Assess this integer in respect to the number of connected clients.
Clients	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 wireless LANs by data usage, displayed in MegaBytes, ordered from highest to lowest and displayed as a graph.

WLAN Name	Lists each top performing WLAN name whose member Access Points and connected clients report the highest usage.
Usage	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.
Clients	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 mobile devices by data usage, displayed in MegaBytes, ordered from highest to lowest and displayed as a graph.

Device Name	Lists each top performing device name whose connected clients report the highest network utilization (in Megabytes).
Usage	Lists each top performing device's network utilization in megabytes. Assess this integer in respect to the number of connected clients for consistency.
Clients	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 the top 10 client operating systems by data usage, displayed in MegaBytes, ordered from highest to lowest and displayed as a graph.

11 **Top Applications by Usage** displays the top 10 client applications by data usage, displayed in MegaBytes, ordered from highest to lowest and displayed as a graph.

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

12 **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.

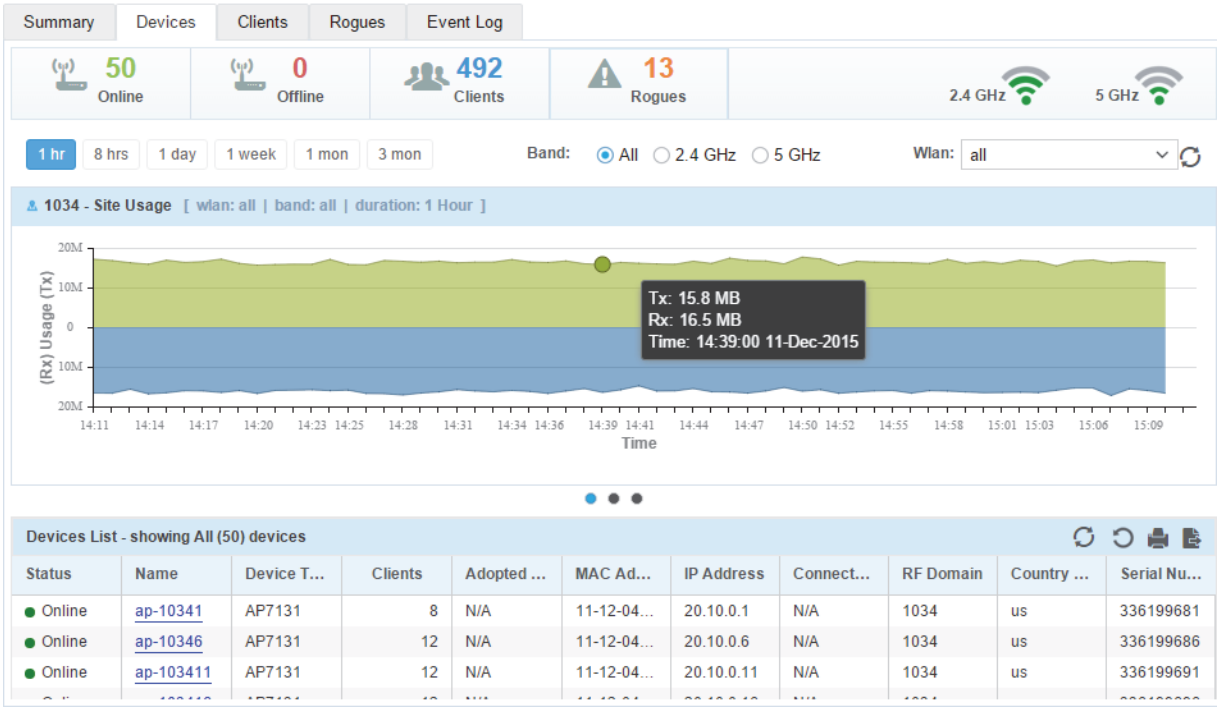
Devices

To view a summary of all APs and devices:

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

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

The Devices 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. Blue represents downstream data and is shown on the lower half of the graph.

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

Status	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".
Name	Displays the Access Point's unique administrator assigned name provided upon initial configuration.
Device Type	Displays the model number for NSight managed devices to help assess the diversity of connected devices.
Clients	Displays the number of wireless client connected to each NSight managed device.
Adopted For	Displays the amount of time in days, hours and minutes the Access Point or client has been adopted.

MAC Address	Displays the *Media Access Control* (MAC) address factory assigned to each device as its unique hardware network identifier.
IP Address	Displays the current IP address the device is using as its network identifier.
RF Domain	Displays the name of the RF Domain associated with each NSight managed device.
Serial Number	Displays the unique hardware serial number assigned to each device.

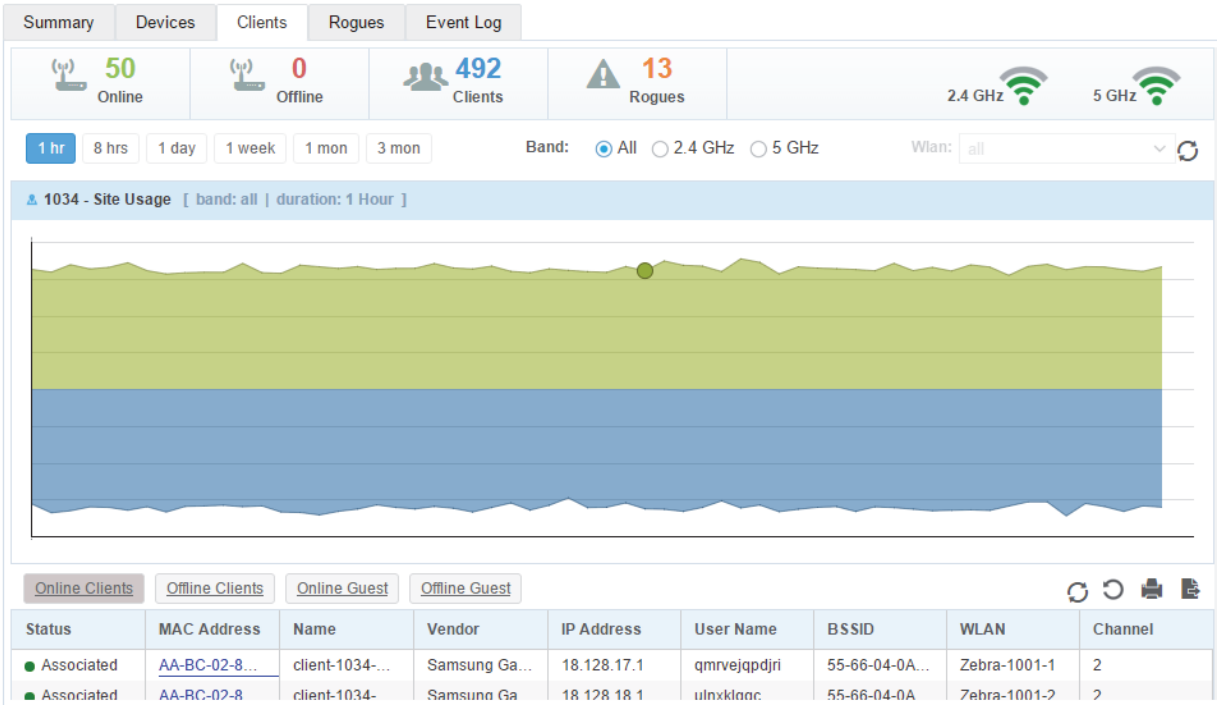
Clients

To view a summary of all client devices:

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

2 In the Left Nav select **Clients**.

The clients screen displays.



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

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

Status	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".

MAC Address	Displays the *Media Access Control* (MAC) address factory assigned to each device as its unique hardware network identifier.
Name	Displays the client's unique administrator assigned name provided upon initial adoption.
Vendor	Displays the device manufacturer for each wireless client connected to the managed network.
IP Address	Displays the current IP address the device is using as its network identifier.
User Name	Displays the username associated with each wireless client on the managed network.
BSSID	Displays the *Broadcast Service Set ID (BSSID)* MAC address used for matching and filtering with the signature.
WLAN	Displays the WLAN associated with each wireless client on the managed network.
Channel	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: When resetting the columns in the clients grid the BSSID column is not affected.

Rogues

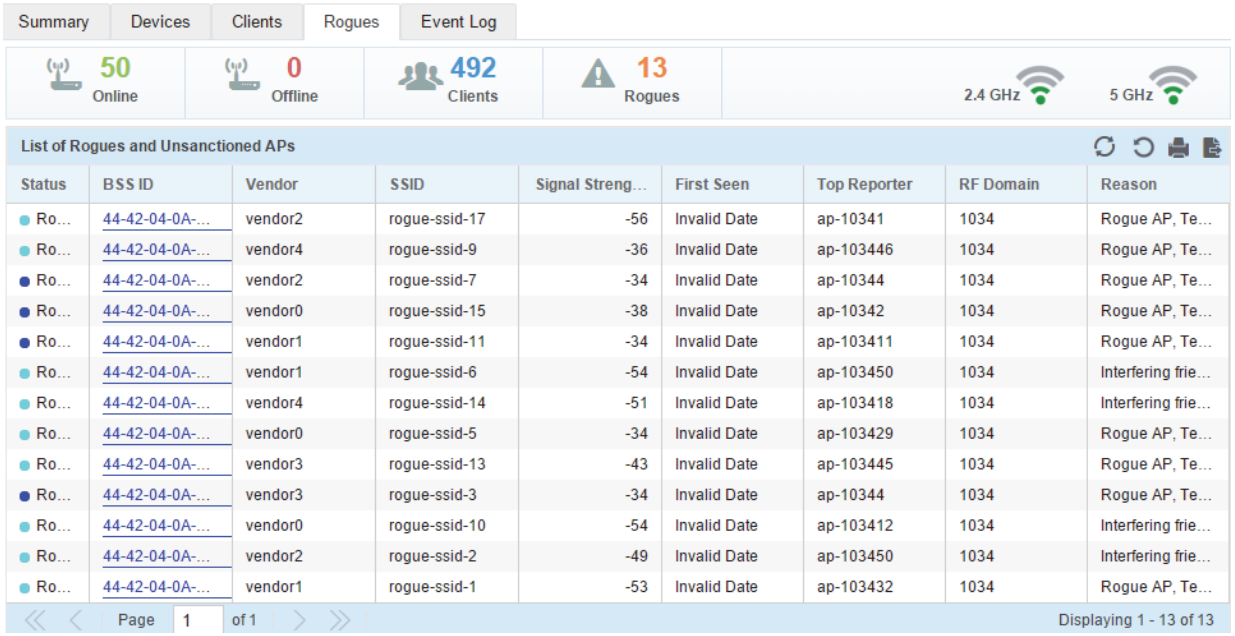
Rogue devices are those devices detected in a sanctioned radio coverage area but have not been deployed by the NSight administrator as a known device.

To view a summary of all rogue APs:

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

2 In the Left Nav select **Rogues**.

The Rogue APs screen displays.



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

Status	Displays the online status of each client. If a device is online, it displays a green checkmark. If the device is offline, it displays a red "X".
BSSID	Displays the *Broadcast Service Set ID (BSSID)* used for matching and filtering.
Vendor	Lists the manufacturer of the detected Access Point as an additional means of assessing its potential threat to the members of this RF Domain.
SSID	Displays the *Service Set ID* (SSID) of the network to which the detected Access Point belongs.
Signal Strength	Displays the signal strength of the detected Access Point. Use this variable to help determine whether a device connection would improve network coverage or add noise.
First Seen	Provides a timestamp when the detected Access Point was first detected by a RF Domain member device.
Top Reporter	Lists the administrator assigned hostname of the top performing RF Domain member detecting the listed Access Point MAC address. Consider this top performer the best resource for information on the detected Access Point and its potential threat.
RF Domain	Displays the RF Domain which the rogue device is associated to.
Reason	Displays the system assigned reason the Access Point is marked as rogue.

Event Log

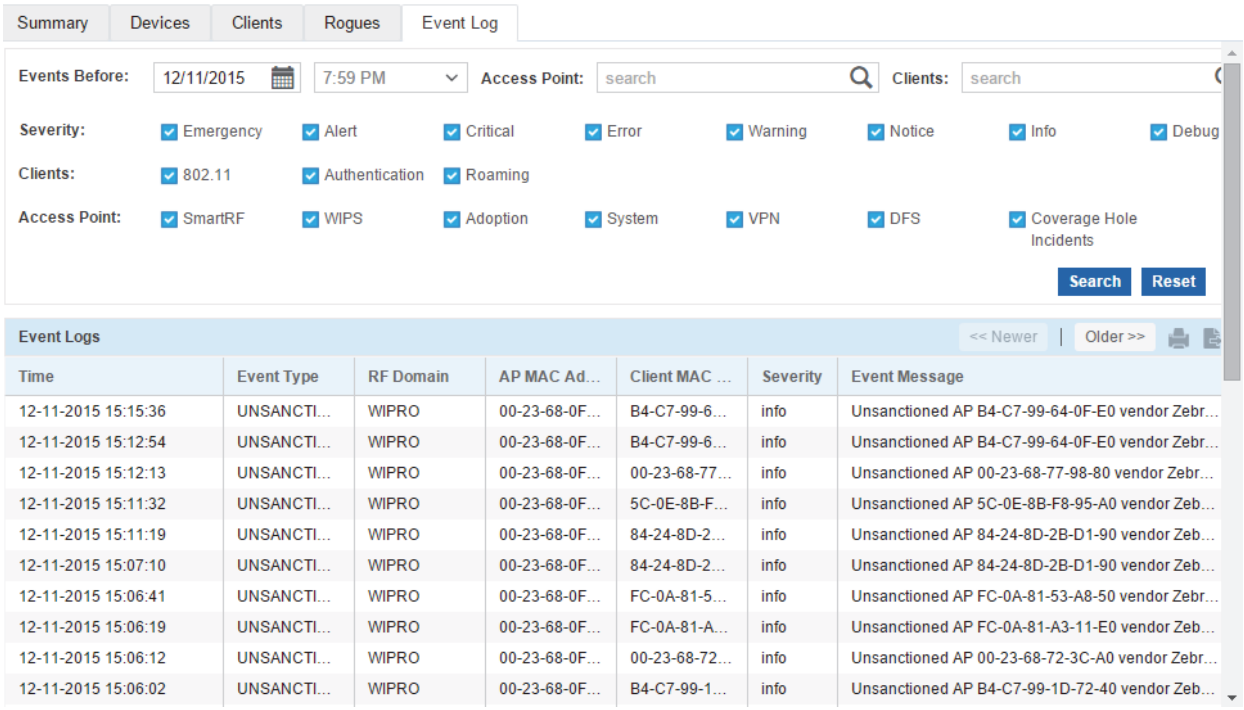
The Event Log provides customizable access to network statistics and log information which can be used by network administrators to troubleshoot connectivity or other network issues. The Event Log screen filters information by time, Access Points or clients and allows searching for specific Access Points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

To view customizable log information:

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

2 In the Left Nav select **Event Log** from the menu

Event Log information specific to the selected item displays.



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

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

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

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

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

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

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

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

REPORTS

In This Chapter

Reports Overview

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

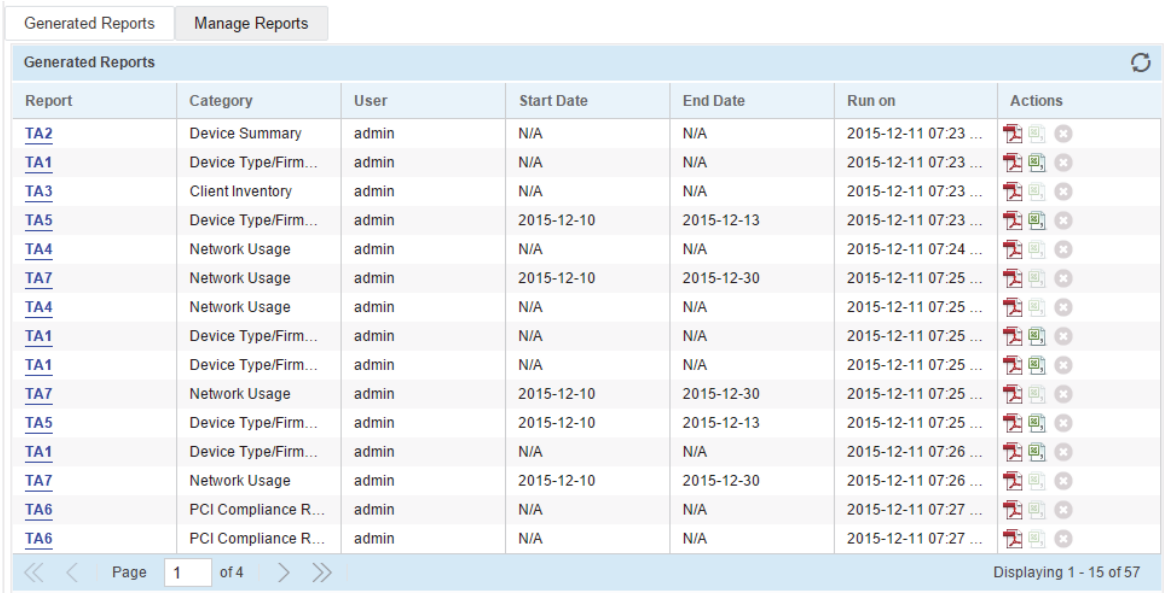
Generated Reports

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

To view report information:

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

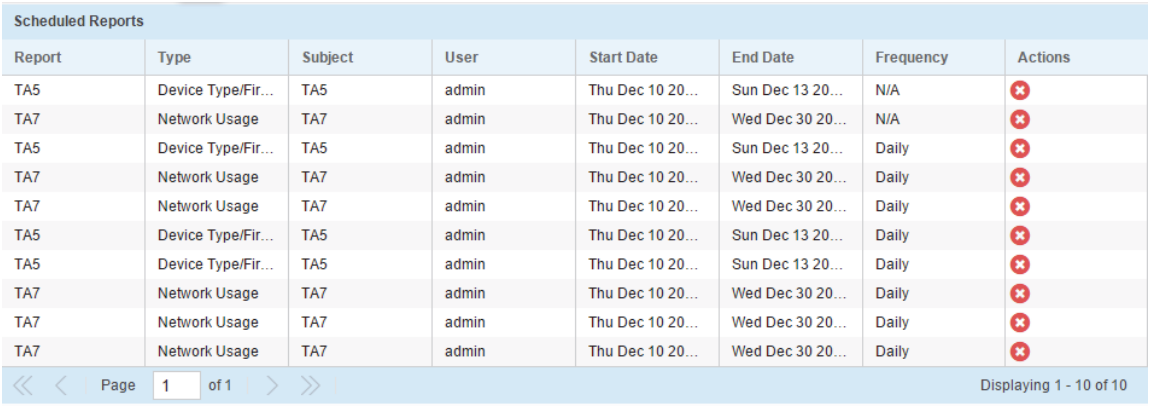
The Generated Reports tab is separated into **Generated Reports** and **Scheduled Reports**. **Generated Reports** displays reports created manually or already run according to schedule. **Scheduled Reports** have been configured to run at a scheduled date and time.



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

Report	Displays the user configured report name for each scheduled report.
Category	Displays the report category for each generated report. The categories are: ♦ *Device Type / Firmware Summary* ♦ *Device Summary* ♦ *Client Inventory* ♦ *PCI (3.1) Report* ♦ *Network Usage* ♦ *RF Health*
User	Displays the name of the user that generated the report.
Start Date	Lists each report's compilation start time. Report information is gathered from this time through the listed end date.
End Date	Lists each report's compilation end time. Information is no longer trended and reported after this date, so ensure the trending period is long enough to apply significance to the report data.

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



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

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

Frequency	Displays the frequency in days, hours and minutes each report is scheduled to run.
Actions	Selecting "X" will delete the selected alarm from the generated reports.

Manage Reports

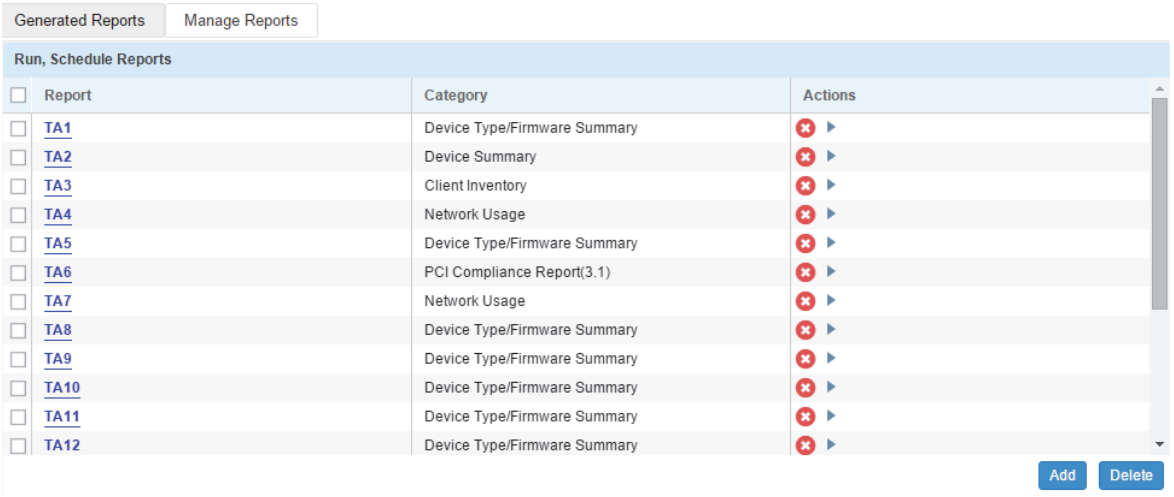
Use the Manage Reports tab to manually generate and schedule reports. Existing scheduled reports can be edited within this tab.

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:

Report	Displays the user configured report name for each managed report.
Category	Displays the report category for each managed report. The categories are: ♦ *Device Type / Firmware Summary* ♦ *Device Summary* ♦ *Client Inventory* ♦ *PCI Report* ♦ *Network Usage* ♦ *RF Health* Selecting the *Category* column allows sorting reports by category and customizing the *Columns* available.
Options	Displays the report options selected and utilized for each listed report.

TOOLS

In This Chapter

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 and traceroute.

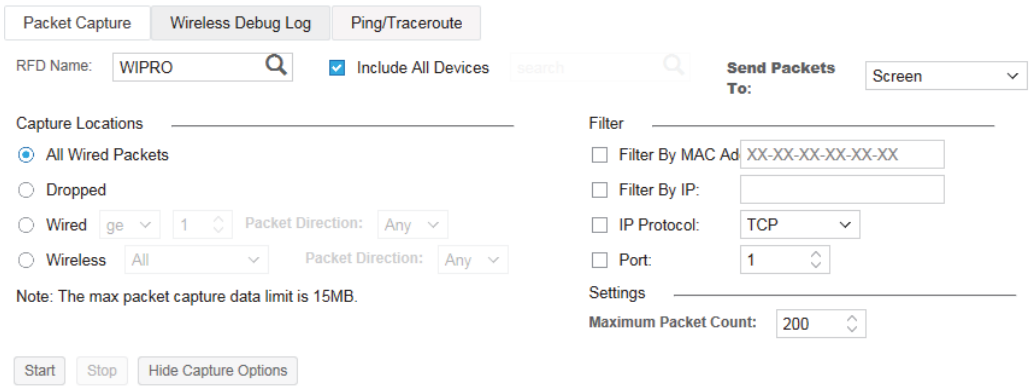
Packet Capture

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

To access **Packet Capture**:

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

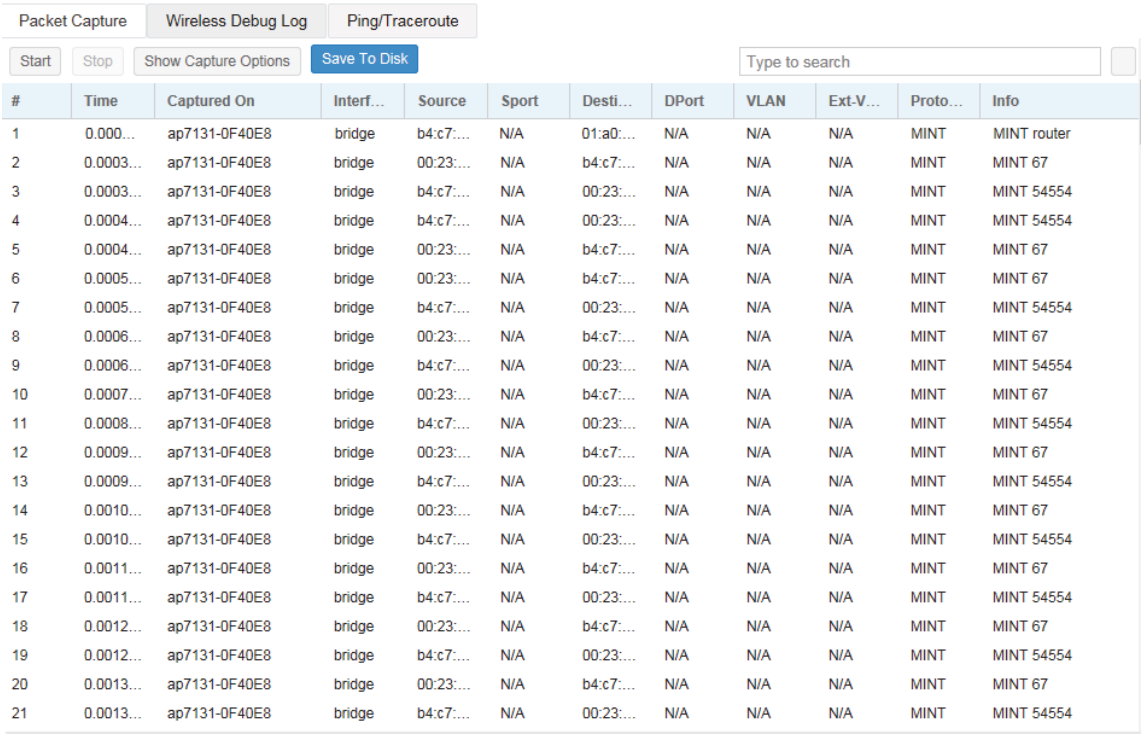
2 Select the **Packet Capture** tab.



RFD Name	Lists the name of the RF Domain whose member devices are subject to the packet capture. RF Domains allow administrators to assign

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

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



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

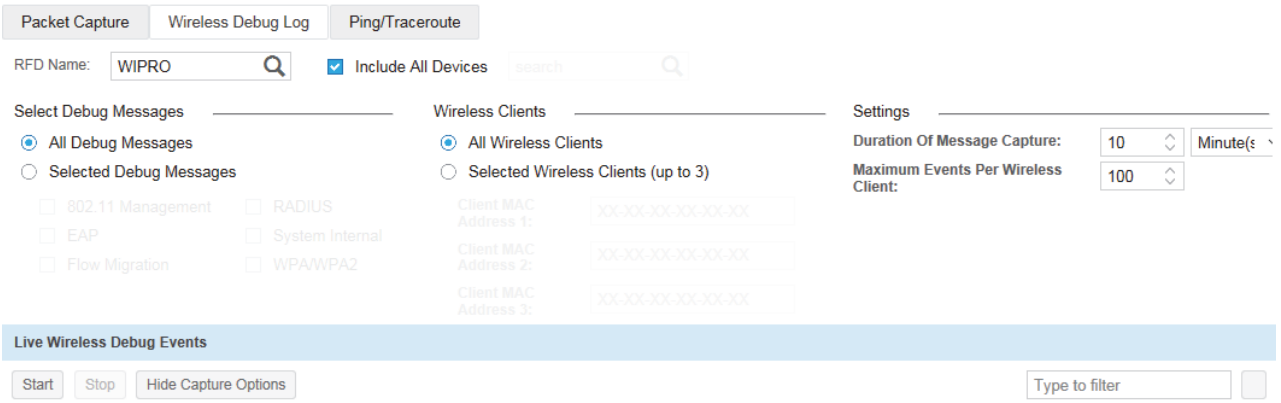
Wireless Debug Log

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 with the following options and information:

RFD Name	Displays the administrator assigned name of the selected RF Domain used for wireless client debugging. RF Domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area, such as in a floor, building or site.
Include All Devices	Use the *Include All Devices* option to include debug messages from all clients, their connected Access Points and managing controllers or service platforms in the selected RF Domain.
Select Debug Messages	Select *All Debug Messages,* to display all wireless client debug information for selected RF Domain member clients. Select *Selected Debug Messages* to specify which wireless client debug messages to display. If Selected Debug Messages is selected, displays information for any combination of the following: ♦ *802.11 Management* ♦ *EAP* ♦ *Flow Migration* ♦ *RADIUS* ♦ *System Internal* ♦ *WPA/WPA2*
Wireless Clients	Select *All Wireless Clients* to display debug information for each client connected to a RF Domain member Access Point radio. Choose *Selected Wireless Clients* to display information only for specific wireless clients (between 1 and 3). If Selected Wireless Clients is selected, enter the MAC address for up to three wireless clients. The information displayed or logged will only be from the specified wireless clients.
Duration of Message Capture	Use the spinner controls to select how long to capture wireless client debug information. This can range between 1 second and 24 hours, with the default value of 1 minute.
Maximum Events Per Wireless Client	Use the spinner controls to select the maximum number of debug messages displayed per wireless client. Set the number of messages from 1 - 9999 events, with the default of 100 events.
File Location	When the *Send Data To* field is set to File, the *File Location* configuration displays below the configuration section. If *Basic* is selected, enter the URL in the following format: *URL Syntax:* *tftp://<hostname|IP>[:port]/path/file* *ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file* *IPv6 URL Syntax:* *tftp://<hostname|[IPv6]>[:port]/path/file* *ftp://<user>:<passwd>@<hostname|[IPv6]>[:port]/path/file* If *Advanced* is selected, configure the Target, Port, Host/IP, User, Password and optionally the path for the wireless client debug log file you wish to create.

Live Wireless Debug Events	When the *Send Data To* field is set to *Screen*, this area displays live debug information for connected wireless clients in the selected RF Domain.

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

Ping and Traceroute

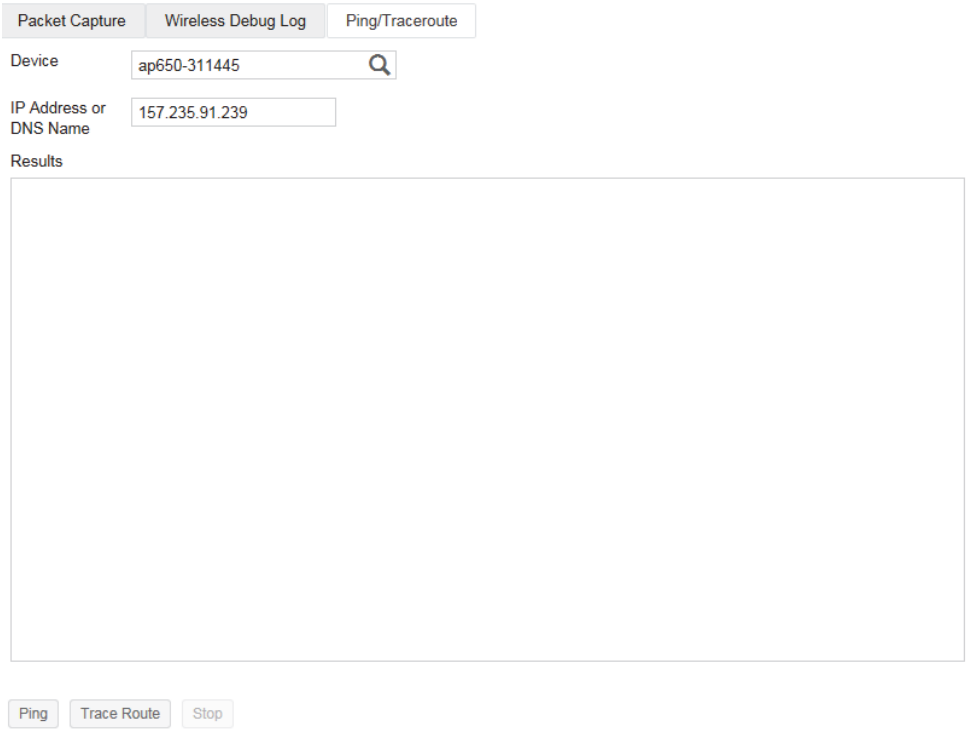
Use a ping to test the reachability of a host on an IP network and measure the round trip time from originating host to destination and back again.

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

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

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

2 Select the **Ping/Traceroute** tab.



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.

6

CUSTOMER-SUPPORT

Support Center

If you have a problem with your equipment, contact support for your region. Support and issue resolution is provided for products under warranty or that are covered by a services agreement. Contact information and Web self-service is available by visiting www.zebra.com/support

When contacting support, please provide the following information:

- Serial number of the unit
- Model number or product name
- Software type and version number

Support responds to calls by email or telephone within the time limits set forth in support agreements. If you purchased your product from a business partner, contact that business partner for support.

Customer Support Web Site

The Support Web site, located at www.zebra.com/support provides information and online assistance including developer tools, software downloads, product manuals, support contact information and online repair requests.

Manuals

www.zebra.com/support

Zebra Technologies Corporation
Lincolnshire, IL 60069 USA

MN-002679-01 Revision A December 2015