ExtremeCloud IQ CoPilot Deployment Guide

Version 23.6.2

Table of Contents

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

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

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[  ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
`x | y`	A vertical bar separates mutually exclusive elements.
`< >`	Nonprinting characters, such as passwords, are enclosed in angle brackets.
…	Repeat the previous element, for example, `member[member...]`.
`\`	In command examples, the backslash indicates a "soft" line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation

Release Notes

Hardware and Software Compatibility for Extreme Networks products

Extreme Optics Compatibility

Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

Help and Support

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

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

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

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

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

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

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

Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.

Welcome to ExtremeCloud IQ CoPilot

This guide is for administrators who want to deploy the CoPilot solution. We assume that your ExtremeCloud IQ network is already deployed and operational. This guide provides the necessary information to get up and running with your 30-day ExtremeCloud IQ CoPilot trial, and includes information about license requirements and management.

For information about supported devices, see the *ExtremeCloud IQ Release Notes*.

For information about ExtremeCloud IQ deployment and management, see the ExtremeCloud IQ User Guide.

CoPilot Overview

ExtremeCloud IQ CoPilot is an AIOps solution that leverages Explainable Machine Learning (ML). With CoPilot, your IT operations teams become more data-driven and proactive. The CoPilot dashboard provides access to in-depth information anomalies and client connectivity for your Extreme Networks cloud-managed wired and wireless networks. Your ExtremeCloud IQ CoPilot subscription provides the following benefits:

- CoPilot simplifies troubleshooting by providing auditable recommendations to reduce the number of out-of-context alerts that can waste time and effort.
- CoPilot identifies anomalies and alerts you, providing an explanation and the best options for resolution.
- CoPilot proactively reduces risk by looking for patterns ahead of time to identify significant anomalies so IT can address them early.
- CoPilot utilizes continuous learning and bidirectional communication to provide the best and most accurate recommendations for your network.
- CoPilot summarizes the client connectivity experience into a single quality index score, and helps you to easily track, identify, and troubleshoot connectivity issues.

For more information, see Reduce Mean-Time-To-Resolution with ExtremeCloud IQ CoPilot.

Related Topics

Deploy ExtremeCloud IQ CoPilot

The topics in this section provide detailed procedures for deploying CoPilot.

> **Note**
>
> The ExtremeCloud IQ user interface and this deployment guide use the term *VIQ* to refer to an instance of ExtremeCloud IQ. If you have multiple VIQs, each instance is independent, but they can use the same license pool.

Deployment Tasks

Use one of the following procedures to set up your CoPilot trial or subscription.

Enable CoPilot on page 9, or use Enable CoPilot for the VIQ on page 10.

Enable CoPilot

Use this procedure to enable CoPilot and start your 30-day trial.

> **Note**
>
> When you enable CoPilot, you consent to being contacted by Extreme Networks.

1. In ExtremeCloud IQ, select .
2. (Optional) To purchase licenses, select **Contact Sales**.

   If you prefer to start your trial first, you can contact sales later.

3. On the ExtremeCloud IQ CoPilot tab, select **Enable CoPilot**.
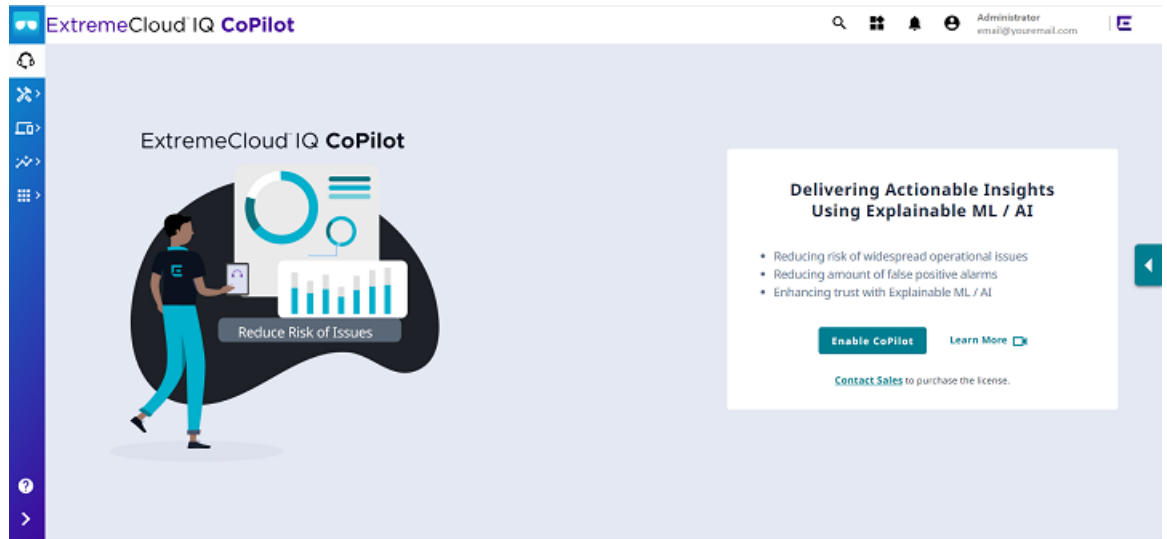
The grace period begins for each managed CoPilot-eligible device. The grace period is 30 days and cannot be paused or restarted.

Related Topics

Purchase CoPilot Licenses on page 38
Deployment Tasks on page 9

Enable CoPilot for the VIQ

Use the following procedure to enable CoPilot for the VIQ. If you have multiple VIQs, you can use this procedure to disable CoPilot for specific VIQs.

1. Go to **Global Settings** > **VIQ Management**.
2. To enable CoPilot, slide the **Enable CoPilot feature for this VIQ** toggle to **ON**.

Related Topics

Deployment Tasks on page 9

Use the ExtremeCloud IQ CoPilot Dashboard

To access the ExtremeCloud IQ CoPilot dashboard, log in to ExtremeCloud IQ and select ⬚ from the left navigation panel.

You can access the dashboard from anywhere, by using the ExtremeCloud IQ Companion mobile app for AIOps.

Legacy View

By default, the CoPilot dashboard opens to the **New View**. To switch, select **Legacy View**. ExtremeCloud IQ saves your selection for the next session.

> **Note**
> A new notification banner appears in the CoPilot dashboard. The banner announces the upcoming deprecation of **Legacy View** in Release 23.7.1. The banner appears only once per user and can be dismissed.

Data for the **Legacy View** is organized into interactive widgets:

- Account Insight Widgets on page 12
- Adverse Traffic Patterns Widget on page 13
- Assurance Scans Widget on page 14
- DFS Recurrence Widget on page 14
- PoE Stability Widget on page 14
- Port Efficiency Widget on page 16
- Wi-Fi Capacity Widget on page 16
- Wi-Fi Efficiency Widget on page 17
- Wired Connectivity Experience Widget on page 17
- Wireless Connectivity Experience Widget on page 17

Related Topics

Widget Tools

Many of the dashboard widgets are interactive. The following list describes common tools for interacting with the widgets:

Tool Tips

Hover over any gray circle with a white "i" for an explanatory tool tip.

Sort

Widget data can be sorted by location, anomaly severity, and most recent occurrence.

Learn More

Select the camera icon to watch a video that explains more about the widget.

Pin

Select the pushpin icon to pin an anomaly to the top of the anomalies list.

Mute or Delete

Select **...** to mute or delete an anomaly. You can mute or delete recurring anomalies for which there is no action, or about which you are not concerned.

Hide Muted Anomalies

Select **Hide Muted** at the bottom of the widget to hide all recurring muted anomalies.

Anomaly details

Select anywhere inside a widget anomaly pane to see more details about that anomaly, including recommended remedial actions. You can make the following selections from inside the details panel:

- Select the down arrow to see more information about a specific anomaly, including recommended remedial actions.
- Select the pushpin icon to pin this anomaly to the top of the list of anomalies.
- Select the thumbs-up icon if this information was helpful and the thumbs-down icon if it was not. Your responses here are analyzed and used to improve this information in future product releases.

Need Help

Select **Need Help** if the suggested remedies do not correct an anomaly. Follow the instructions to have ExtremeCloud IQ generate a support ticket.

Related Topics

Account Insight Widgets

The following account insight widgets appear in a column to the right of the page:

Account Summary

Shows general information about the VIQ.

Devices by OS

Shows device inventory counts by OS version.

Devices by Type

Shows device inventory counts by device type or network function.

Device Uptime

Shows the daily number and percentage of connected devices and offline devices.

ExtremeCloud IQ Applications

Shows additional applications that are available for the account.

Licenses

The **Licenses** widget displays the number of used and available licenses for ExtremeCloud IQ Pilot and ExtremeCloud IQ CoPilot for APs and switches, and ExtremeCloud IQ Navigator for WiNG devices.

To go to the **Licensing** window, select **Manage**. Select to return to the CoPilot dashboard from the **Licensing** window.

Usage

Shows the daily amount of client data handled by infrastructure devices and the number of unique clients.

Related Topics

Adverse Traffic Patterns Widget

The **Adverse Traffic Patterns** widget displays anomalies caused by TX and RX traffic loads that result in high resource use of multicast and broadcast communications. Use of multicast and broadcast requires devices to clone packets, which reduces CPU availability. This is usually not a problem, unless the traffic load begins to exceed the available CPU capacity. The CPU threshold for APs is 90%. The CPU threshold for switches is 50%. Exceeding the CPU capacity can increase latency and packet loss, and might even bring a device down.

The widget displays the following data for active devices:

- Maximum and average CPU and memory usage over time for wired and wireless devices.
- Client counts over time for wired and wireless devices.
- TX and RX unicast, multicast, and broadcast byte counts over time for backhaul interfaces on wired and wireless devices.

Related Topics

Assurance Scans Widget

The **Assurance Scans** widget uses a timeline to show the cumulative number of anomalies found, per day. Hover over a bar in the timeline to see the date and types of anomalies identified for that day.

Related Topics

DFS Recurrence Widget

The **DFS Recurrence** widget displays anomalies related to radar-influenced channel changes. When an access point switches channels, the quality of service for connected clients can decrease temporarily, while repeated channel changes can degrade the client experience for extended periods of time.

When an AP detects a radar pulse on the DFS channel it is using, regulations require that it switch to a non-DFS channel for at least 30 minutes. This widget identifies APs that repeatedly switch from a wireless channel within the DFS range (channels 50-144, inclusive) to a channel outside the range because it detects third party radar pulses.

ExtremeCloud IQ records the DFS channels that are affected by radar pulses. Radar is usually not in use across the entire DFS channel range (50-144). If ExtremeCloud IQ determines that only a subset of the range is in use, you can disable only those channels. The AP continues to use DFS channels that are not affected by radar. If ExtremeCloud IQ determines that the entire range of DFS channels is affected, the best practice is to completely disable DFS for the affected AP.

The severity of a DFS anomaly is classified as:
- High—Many (more than 12) radar events in the past 24 hours
- Medium—Moderate (8-12) number of radar events in the past 24 hours
- Low—Small (5-8) number of radar events in the past 24 hours

Related Topics

PoE Stability Widget

APs commonly receive power through an Ethernet backhaul cable connection to an upstream switch. This method is known as Power over Ethernet or PoE. When an AP first boots, it selects a power mode based on the available PoE protocols. The AP can start with PoE and move to PoE+ after a brief interval. It uses the selected power mode until it reboots.

The **PoE Stability** widget displays anomalies related to PoE flapping and sudden changes in power draw. Data is presented over a 24-hour period, and includes date and time details.

The severity definitions for PoE anomalies are based on the average number of clients connected to an AP on a given day. If there are fewer than 10 clients, the anomaly severity is considered low. If there are 50 or more clients on a given day, the severity level is considered high. If there are between 10 and 50 clients, the severity level is considered medium.

Occasionally, poorly installed cabling or MDU closet wiring, lack of power on the upstream switch, or a failing power supply on either the AP or the switch can all cause APs to cycle through power modes, while never reaching a steady state. There are three types of PoE stability anomalies:

SUB_OPTIMAL

   The AP negotiates down to AF, even though it requires AT or a higher level for optimal performance and full capacity.

FLIP

   The AP switches PoE modes more than 10 times within a 24-hour period, indicating an unstable connection.

TIME

   The AP spends less than 80% of its time operating in a single PoE mode, indicating an unstable connection.

To open the **PoE Stability Anomaly** panel, select a location (place) for which anomalies have been detected. To view more information about an anomaly, select the corresponding down arrow. The **PoE Stability Anomaly** panel includes the following information:

Issue

   A description of the problem, including the anomaly type (SUB-OPTIMAL, FLIP, TIME, or a combination)

Recommended Actions

   Best practices to resolve the anomaly

PoE Mode Changes

   A graph showing the number of changes and the dates they occurred, color coded for severity

   Note
   The **PoE Mode Changes** graph appears for FLIP or TIME PoE anomalies, and for anomalies that are a combination of FLIP or TIME and SUB_OPTIMAL. The graph does not appear if the only wired or wireless PoE anomaly type is SUB_OPTIMAL.

Related Topics

Port Efficiency Widget

The **Port Efficiency** widget identifies wired and wireless device interfaces that are not making efficient use of their uplink backhaul connection. This inefficiency can occur in the following scenarios:

• An interface might only use half-duplex communication—only 50% of the available throughput capacity.

• An interface can occasionally flip between full-duplex and half-duplex modes. If this happens too often, it indicates that the interface cannot maintain a full-duplex connection and is considered an anomaly.

• An interface might use an inefficient data rate relative to its capability. Allowable data rates are 10 Mbps, 100 Mbps, 1000 Mbps, 2500 Mbps, 5000Mbps, and 10000 Mbps. A data rate of 10 Mbps is considered inefficient, while 100 Mbps and higher data rates are considered normal.

• An interface might occasionally flip between data rates, for example, from 2500 Mbps to 1000 Mbps. When this happens on a regular basis, it indicates that there is a wider issue preventing the interface from maintaining the higher data rate.

The **Port Efficiency** widget displays the following graphs:

• Port Supported Speed and Full/Half Duplex Negotiation

• Number of Changes (Speed or Duplex)

> **Note**
> Both graphs appear for wired and wireless duplex mode anomalies, and speed change anomalies; and for anomalies that are a combination of SUB_OPTIMAL and FLIP anomalies. The Number of Changes graph does not appear if the only anomalies are wired or wireless SUB_OPTIMAL Speed Changes or Duplex Changes.

Related Topics

Wi-Fi Capacity Widget

The **Wi-Fi Capacity** widget displays anomalies related to access point (AP) capacity and airtime usage. You can sort the data by location, severity, and most recent occurrence. This data contains statistical information such as client connection duration and the channel utilization information related to wireless APs. Information reported in this widget includes:

• Total time that a channel was in use.

• Total time that peak usage for the channel was 80% or higher.

• The total number of peak and non-peak intervals (80% or more) recorded on the channel.

- The average number of clients during peak and non-peak intervals.
- The average total TX and RX usage during peak and non-peak intervals.
- The average interference during peak and non-peak intervals.
- An indication of whether or not the channel is anomalous.
- An indication of the severity of the anomaly (low, medium, high, or null).
- Date and time of the analysis (typically over the last 24 hours).
- The Regional Data Center (RDC) from which the data was obtained.

Related Topics

Wi-Fi Efficiency Widget

The **Wi-Fi Efficiency** widget displays anomalies related to wireless communication between clients and APs. You can sort the data by location, severity, and most recent occurrence. This widget presents packet data anomalies and information about them.

Related Topics

Wired Connectivity Experience Widget

The **Wired Connectivity Experience** widget displays information about connectivity for wired devices, such as switches. Data is reported for each unit of hardware, even for stacked switches. The actions and options are similar to the Wireless Connectivity widget. For wired devices, you can only view by location. In this widget, the details panel is labeled **Hardware** and displays port errors.

Related Topics

Wireless Connectivity Experience Widget

The **Wireless Connectivity Experience** widget displays information in the form of a data quality index. Use the drop-down menus to customize the display. Choose how many results to show and customize the display according to

- Location, SSID, or Client type, or by
- Name or Quality Index, in ascending or descending order.

Many parts of the widget contents are interactive. Hover to see more details.

The quality index scores client connectivity experiences from 1 (worst) to 10 (best). In an ideal scenario, the quality index should be 10 consistently over time, while any decline in the index value indicates a degraded experience. This index is calculated for every client, every time new client metrics are obtained. By default, this interval is every 10 minutes.

Quality index scoring provides more granularity and better control. It can help mitigate the effects of single (random) events. The following tools are available in the quality index:

- Select the = or arrow symbols next to the rating to see a comparison to the rating 24 hours previous. The = symbol means the rating is the same, and the up and down arrows indicate that the rating has dropped or climbed compared to the prior 24 hours. The timeline displays the data from the previous 24 hours on the left; the most current data appears on the right side of the timeline.

- Select inside the widget, either over the location, SSID, or client type, or directly inside the timeline chart to see the **Connectivity Details** panel. In this panel, you can use drop-down lists to view different locations. Use the type-ahead search field to search for locations. You can change the time view from one hour up to the last 90 days. Hover over the timeline for more information about connections, including the following:
  - Time to associate
  - Time to authenticate
  - Total number of unique clients
  - Number of clients above the threshold (if you are viewing for the last seven days or fewer)

- Select the timestamp to drill down for details about specific events and clients. In the details panel, use the time window button on the left to display data for a 10 minute or one hour period for anything you select on the timeline. The details table has a search field, and any table header with an arrow can be sorted. Select the client MAC address to see the Client 360 view.

- In the **Connectivity Experience** panel, if you view by location, there are no other filter options. If you view by SSID or client type, you can filter by location using the filter icon in the right top corner.

- The Aggregated Quality Index in this panel displays data for the times and filters selected. The **Time to Connect** section displays the quality index by time to associate and time to authenticate. All timelines in this panel are synchronized. To zoom in to details on a timeline, drag and select across the timeline. Select again, or deselect to return to the normal view.

Thresholds: The global threshold is dynamically calculated based on information from all clients in the Regional Data Center. The system dynamically calculates the local threshold per location and SSID type (PSK vs Open vs Enterprise), and uses the lower threshold.

Related Topics

New View

The CoPilot dashboard **New View** is a more streamlined way to view CoPilot data for your network. When you navigate to the CoPilot dashboard, the **Legacy View** opens by default. Select **New View** to switch views.
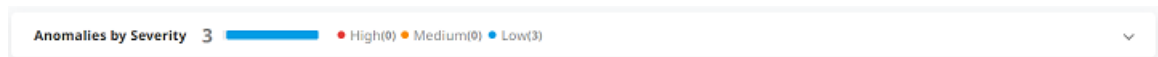
Data for the **New View** is organized into the following tabs:

Anomalies

The **Anomalies** tab uses the following interactive widgets and a table to display information about anomalies:

To hide the widgets and display a streamlined view of **Anomalies by Severity**, select ⌃ .

To display the widgets again, select ⌄ .

Use the controls found at the top of the page to customize your view of the widgets and the table:

Site

Display all sites (default) or select a specific site from the menu. You can search the menu for a site.

Severity

Display all severity levels (default) or select a severity level from the menu.

Anomaly Type

Display all anomaly types (default) or select a specify type of anomaly from the menu.

Duration

Select to specify whether to display anomalies for the past 24 hours (default), or the past 7 days.

Exclude Muted

Select the toggle to hide or display previously muted anomalies.

Trends

Select **Trends** to display a graph that shows anomalies for all sites and severities for the past 90 days. View all anomalies (default) or select a specific **Anomaly Type** from the menu. You can drag along the graph to zoom in on a time period, and then select **Reset Zoom** to zoom back out.

Refresh

Select to refresh the display.

Top Anomalies By Site Widget

Figure 1: Top Anomalies By Site

The **Top Anomalies By Site** widget shows the sites with the most anomalies. Select a site in the widget to view only the anomalies for that site. The other widgets and the table update to show only the anomalies for the selected site.

Related Topics

Anomalies By Severity Widget

Figure 2: Anomalies By Severity

The **Anomalies By Severity** widget shows the number of anomalies for each severity level. Select a level to display only the anomalies of that severity. The other widgets and the table update to show only anomalies of the selected severity.

Related Topics

> Anomalies on page 19

Top Anomalies By Type Widget
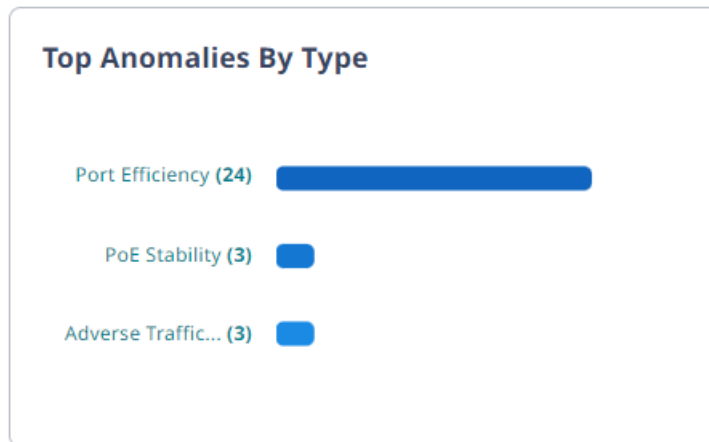
Figure 3: Top Anomalies By Type

The **Top Anomalies By Type** widget shows the most common types of anomalies for your network. Select an anomaly type to display only anomalies of that type. The other widgets and table update to display only anomalies of that type.

Related Topics

> Anomalies on page 19

Anomalies Table

This interactive table displays the following information about anomalies:

- **Device**
- **Interface**
- **Severity**
- **Site**
- **Category**
- **Type**
- **Muted**

> **Note**
> This column appears only when the **Exclude Muted** toggle is set to off. The possible values for this column are **Yes** and **No**.

- **Last detected**

Figure 4: Anomalies

You can display the anomalies in ascending or descending order by column, except for the **Interface** column. You can also search for anomalies by device, site, or anomaly type. Use the **Items per page** menu to specify the maximum number of results to show, per page.

To download a CSV file that contains the same information, select ⤓.

Some recurring anomalies are not problematic; you can mute or dismiss them. Select the corresponding check box(es) for one or more anomalies and the select **...** > **Mute** or > **Dismiss**.

Related Topics

Anomaly Information for a Device

Select a device to open a panel with detailed information about the anomaly, including a description of the issue and recommended actions for resolution. To open the page for the device, select **Go to Device**.

Figure 5: Detailed Information
If you find the detailed information helpful, select **Useful**. If you did not find the information helpful, select **Not Useful**. To get help, select **Need Help**.

Drag the bars on the timeline to show data for a specific date or days.
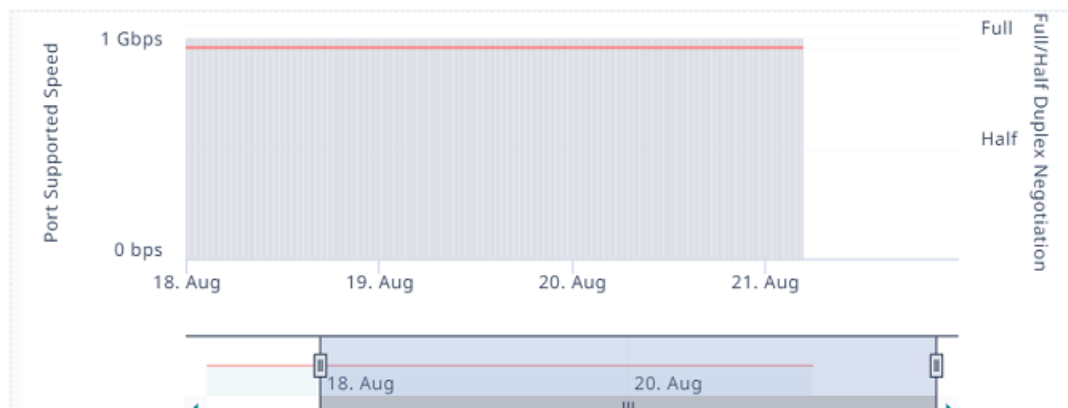

Figure 6: Detailed Information for Specific Days

Related Topics

Submit a Support Ticket

You can trigger ExtremeCloud IQ to open a support ticket if an issue cannot be resolved using the data provided by Insights. ExtremeCloud IQ collects data from the Insight and attaches an output report from the affected device to send to GTAC.

Select **Need Help** and follow the instructions.

> **Note**
>
> This option is only available for devices covered by an ExtremeWorks maintenance contract.

*NEW!*Connectivity Experiences

The **Connectivity Experiences** tab uses an interactive table to display information about connection quality.
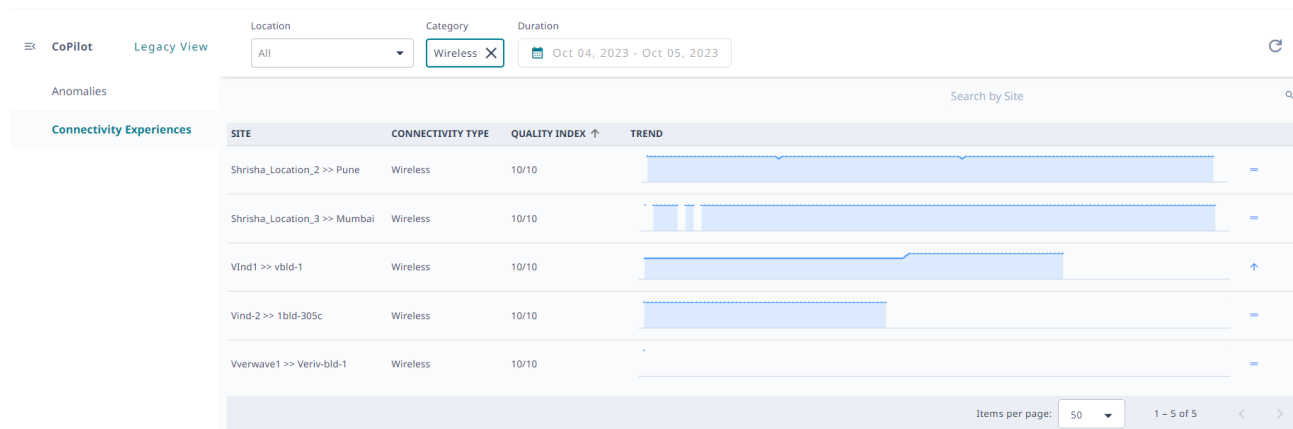
Figure 7: Connectivity Experiences (Wireless)
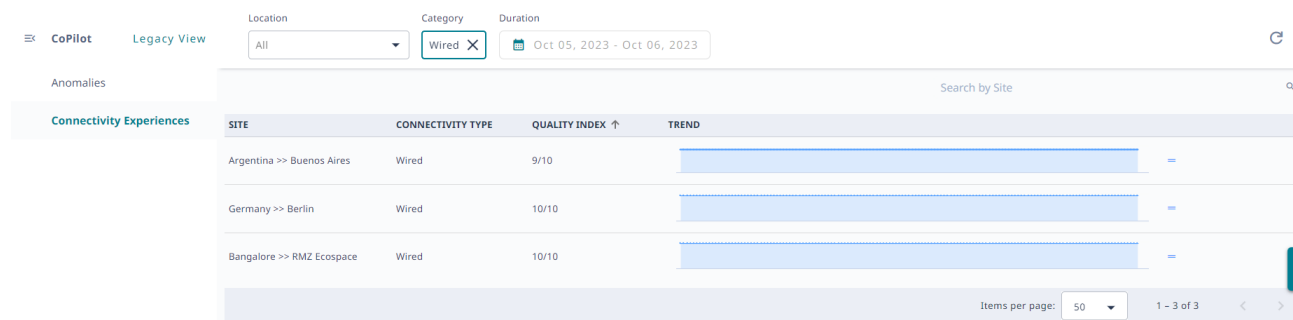
Figure 8: Connectivity Experiences (Wired)

The table displays connection quality information for the previous 24 hours. Use the controls found at the top of the page to customize your view of the table:

Location

Display all sites (default) or select a specific site from the menu. You can search the menu for a site.

Category

Display only wireless clients (default), or only wired clients.

Search by Site

Search for and display connection quality information for a site. Select **X** to return to the previous table view.

To sort the table results according to **Site** or **Quality Index**, hover the mouse to the right of the corresponding column label, and select the ⬆. To change the sort order of the same column, select the ⬆.

The **Trend** column displays the quality index trend, and provides a comparison with the previous 24 hour period. The following indicators show how the current quality index compares to the quality index from 24 hours ago:

- Up from 24 hours ago: ↑
- Equal to 24 hours ago: =
- Down from 24 hours ago: ↓

Related Topics

Connectivity Experiences Panel (Wireless)

To open the **Connectivity Experiences** panel for a site, select the site. Mouse-over a point on the graph to display the following metrics at that time:

- Quality Index
- Time to Connect
- Performance

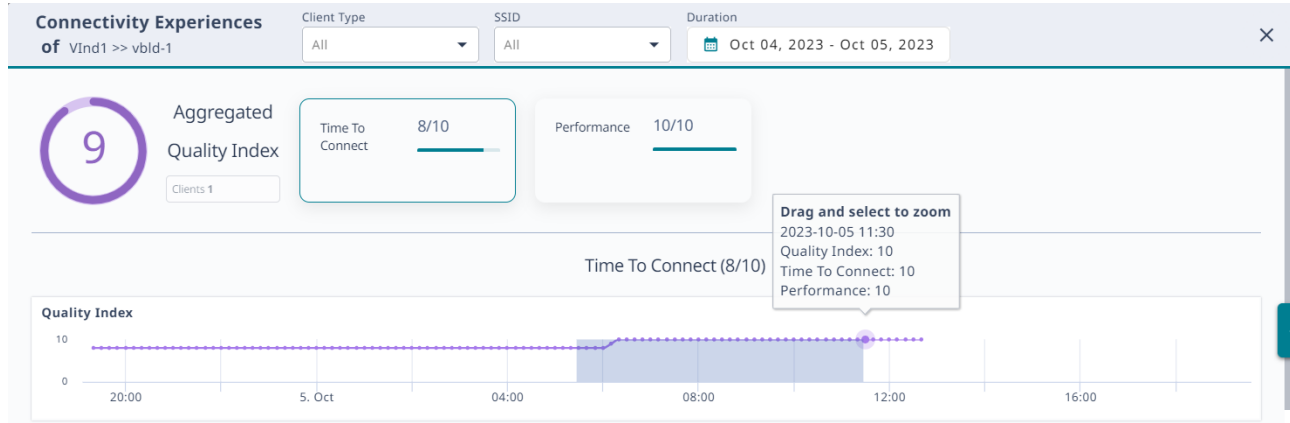To zoom in, drag and select a time period on the **Quality Index** graph.

Figure 9: Connectivity Experiences Panel (Wireless)

Your selection and the zoom function apply to all graphs that appear on the site **Connectivity Experiences** panel.
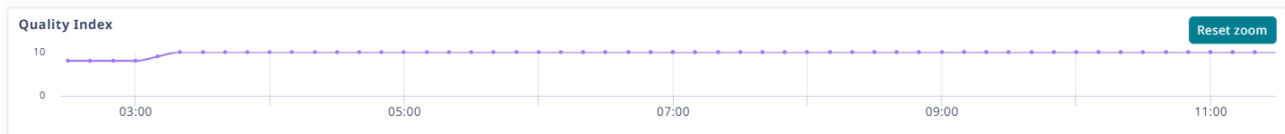

Figure 10: Quality Index Zoom

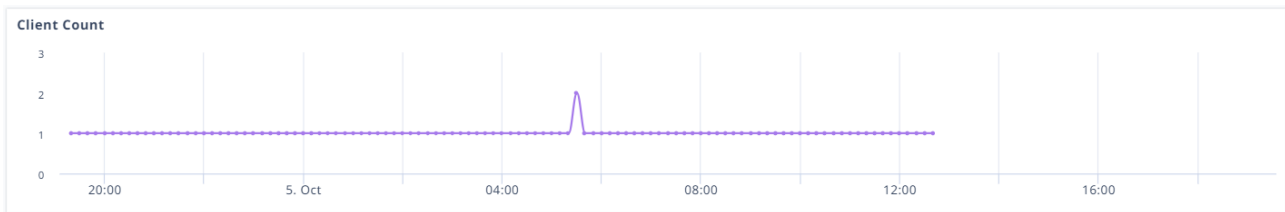To see the number of unique clients at a particular time, mouse over a point in the **Client Count** graph.

Figure 11: Client Count

Related Topics

Client Association (Wireless)

Mouse over a point in the **Client Association** graph to see a summary of the following information:

- Date and time stamp
- Total Unique Clients
- Time to Associate
- Clients Above Association Threshold
- Time to Authenticate
- Clients Above Authentication Threshold

- Time to Obtain IP Address
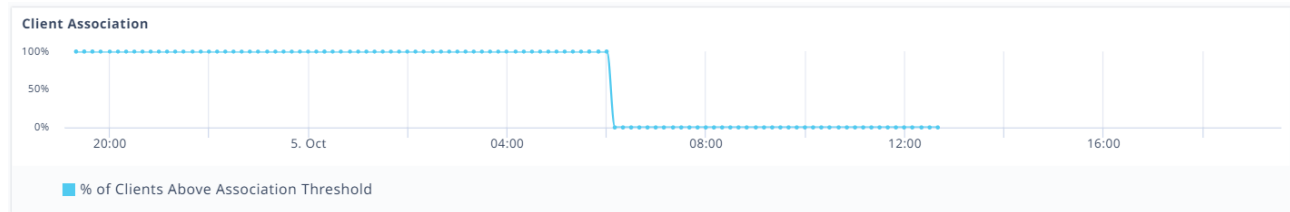- Clients Above DHCP Threshold

Figure 12: Client Association

To open the **Client Association** panel and see more details, select a point on the graph.

Figure 13: Client Association Panel

To zoom in, drag and select a time period. To zoom back out, select **Reset zoom**. To return to the **Default View**, select the back arrow.

Mouse over a point on the graph to see the following information:

- Date and time stamp
- Total Unique Clients
- Time to Associate
- Clients Above Association Threshold

For more information, select a point on the graph for which there are clients above the association threshold. The table updates to show the affected unique clients. To open the connection details panel, select the link from the **HOST NAME** or the **MAC** column.
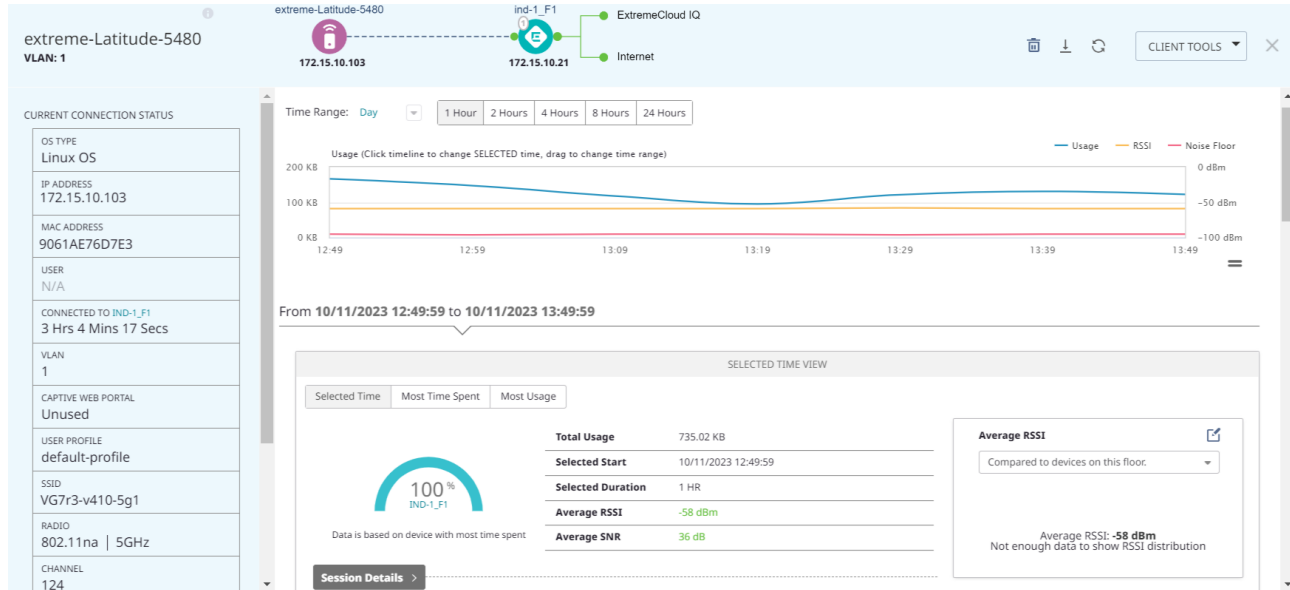
Figure 14: Connection Details Panel

Related Topics

Client Authentication (Wireless)

Mouse over a point in the **Client Authentication** graph to see a summary of the following information:

- Date and time stamp
- Total Unique Clients
- Time to Associate
- Clients Above Association Threshold
- Time to Authenticate
- Clients Above Authentication Threshold
- Time to Obtain IP Address
- Clients Above DHCP Threshold
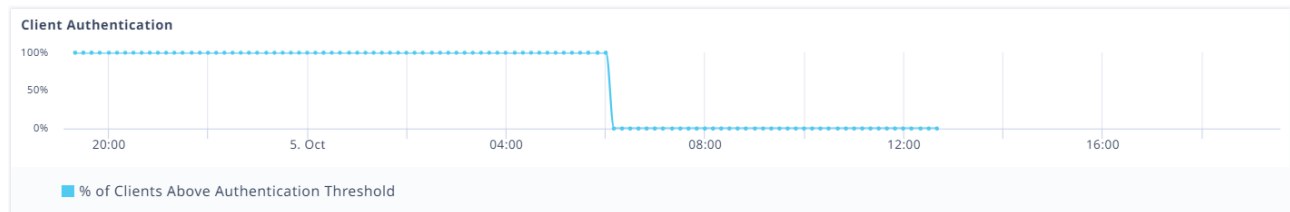
Figure 15: Client Authentication

To open the **Client Authentication** panel and see more details, select a point on the graph.

Figure 16: Client Authentication Panel

To zoom in, drag and select a time period. To zoom back out, select **Reset zoom**. To return to the **Default View**, select the back arrow.

Mouse over a point on the graph to see the following information:

- Date and time stamp
- Total Unique Clients
- Time to Authenticate
- Clients Above Authentication Threshold

For more information, select a point on the graph for which there are clients above the association threshold. The table updates to show the affected unique clients. To open the connection details panel, select the link from the **HOST NAME** or the **MAC** column.

Figure 17: Connection Details Panel

Related Topics

Time to Obtain IP Address (Wireless)

Mouse over a point in the **Time To Obtain IP Address** graph to see a summary of the following information:

- Date and time stamp
- Total Unique Clients
- Time to Associate
- Clients Above Association Threshold
- Time to Authenticate
- Clients Above Authentication Threshold
- Time to Obtain IP Address
- Clients Above DHCP Threshold
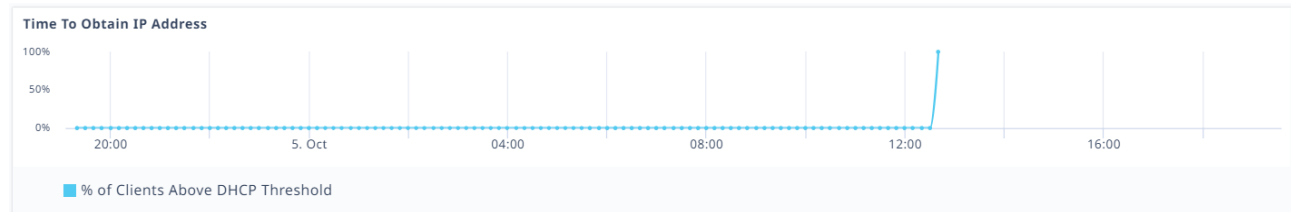
Figure 18: Time To Obtain IP Address

To open the **Time To Obtain IP Address** panel and see more details, select a point on the graph.
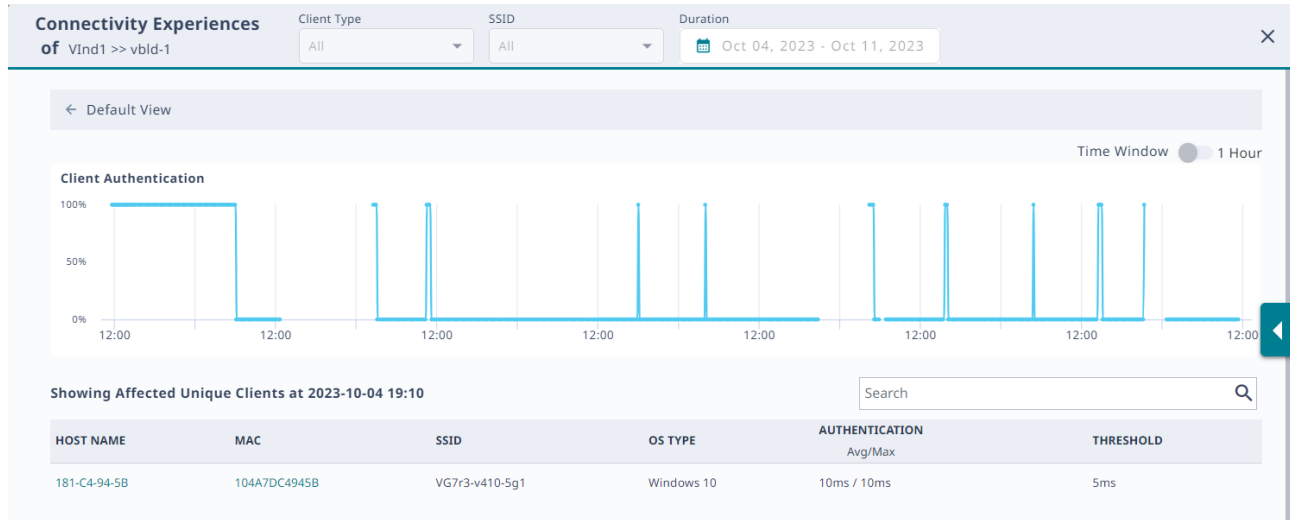

Figure 19: Time To Obtain IP Address Panel

To zoom in, drag and select a time period. To zoom back out, select **Reset zoom**. To return to the **Default View**, select the back arrow.

Mouse over a point on the graph to see the following information:

- Date and time stamp
- Total Unique Clients
- Time to Obtain IP Address
- Clients Above DHCP Threshold

For more information, select a point on the graph for which there are clients above the association threshold. The table updates to show the affected unique clients. To open the connection details panel, select the link from the **HOST NAME** or the **MAC** column.
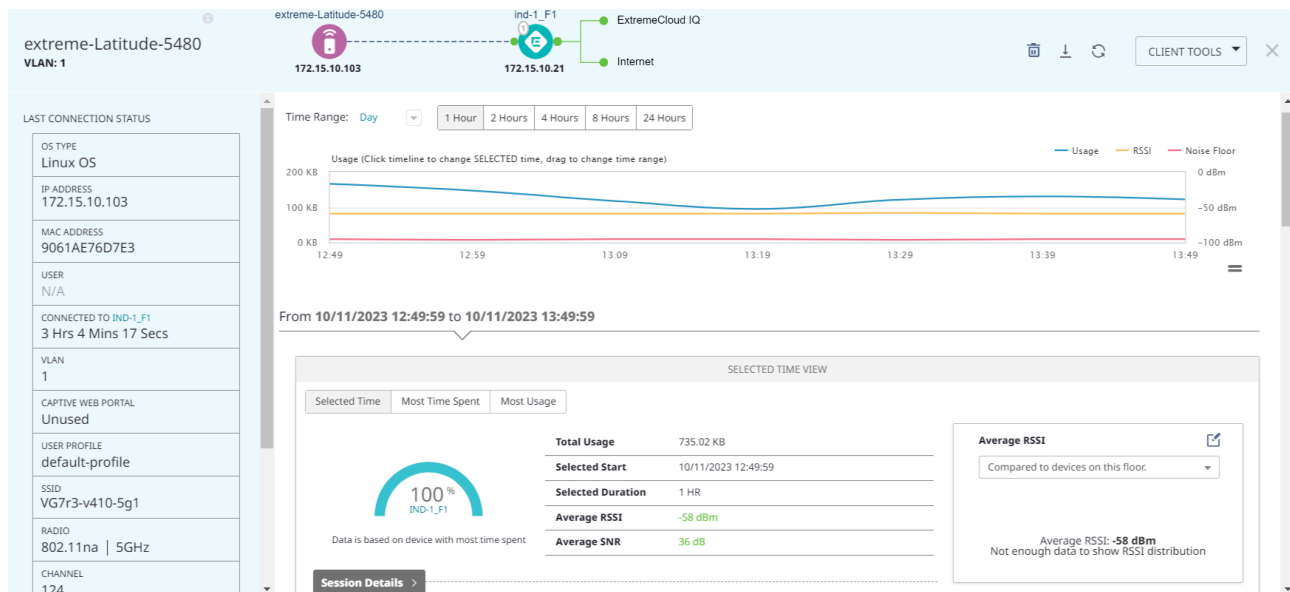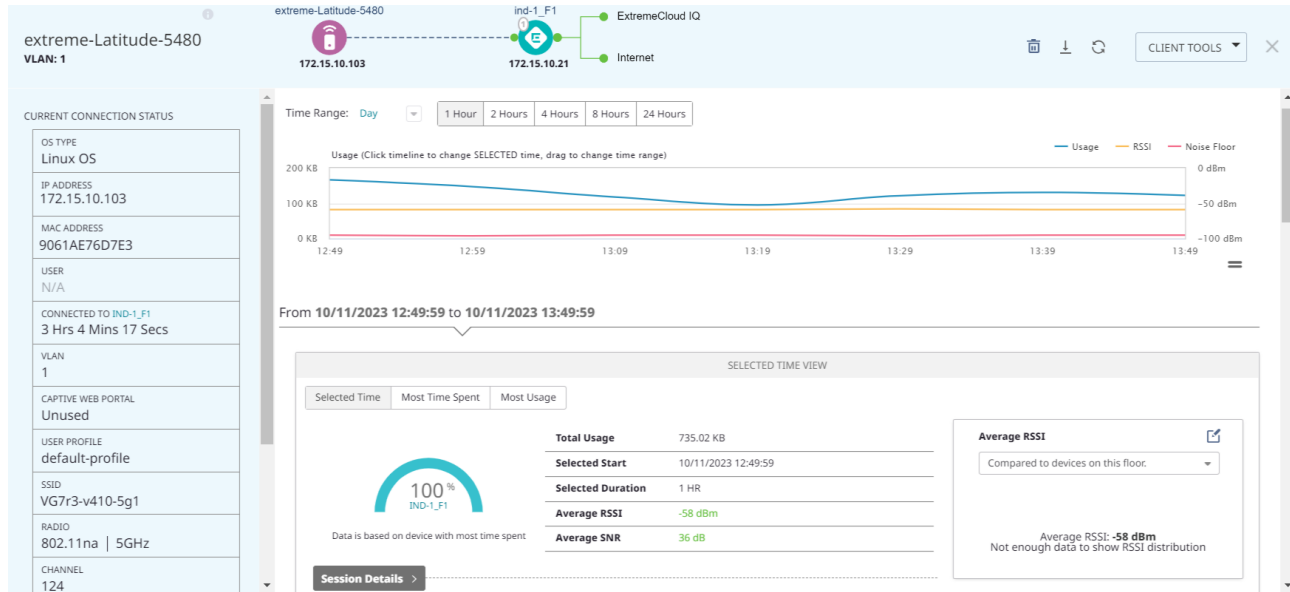

Figure 20: Connection Details Panel

Related Topics

Connectivity Experiences Panel (Wired)

To open the **Connectivity Experiences** panel for a site, select the site. To zoom in, drag and select a time period on the **Quality Index** graph. To zoom back out again, select **Reset zoom**.
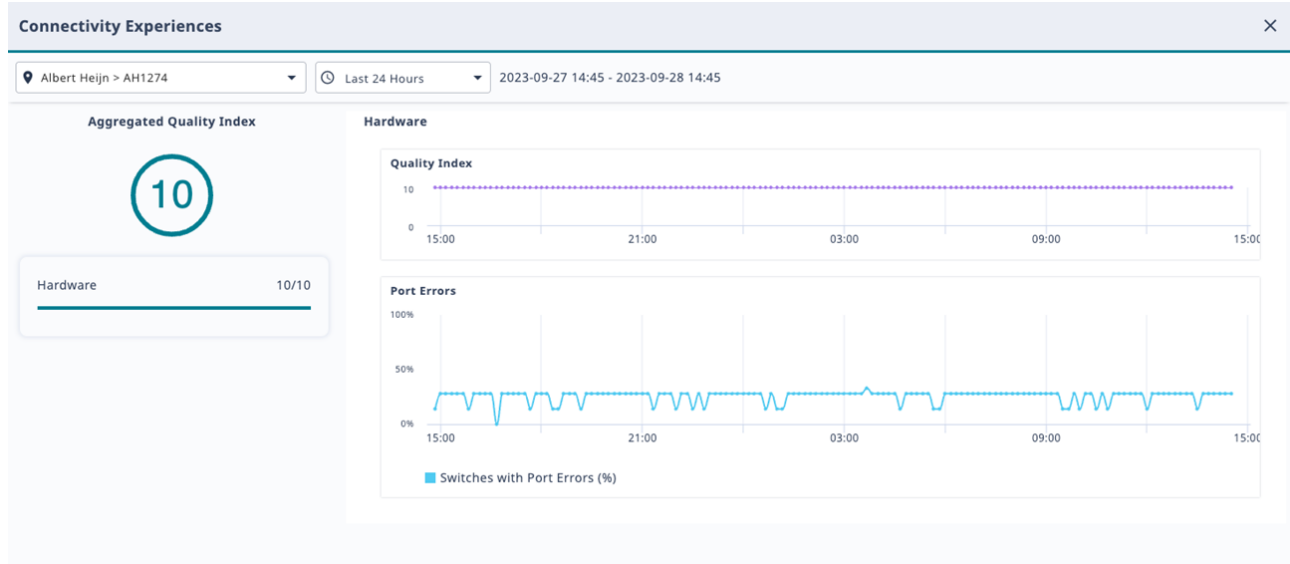
Figure 21: Connectivity Experiences Panel (Wired)

To see high-level information about a port error, mouse over a point in the **Port Errors** graph.

To open the detailed **Port Errors** panel, select the **Port Errors** graph.

Related Topics

Port Errors

To zoom in on the **Port Errors** graph, drag and select a time period.

Figure 22: Port Errors

To zoom back out again, select **Reset zoom**. To return to the **Default View**, select the back arrow.
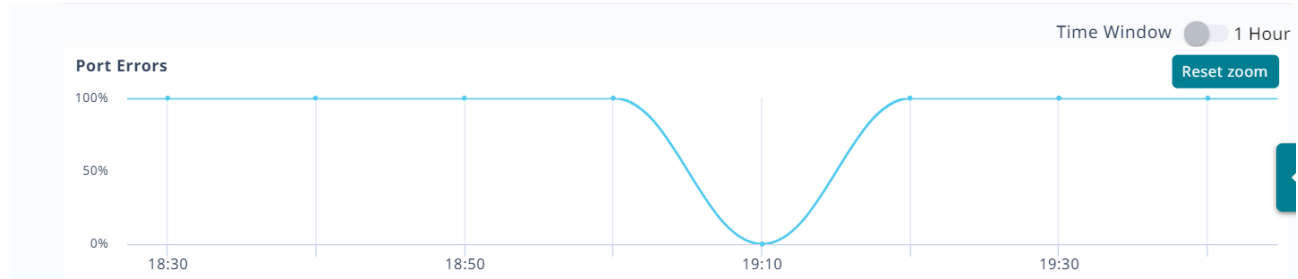
Figure 23: Port Errors Zoom

Select a point on the **Port Errors** graph to update the table with relevant information.

Figure 24: Affected Ports Table

The system calculates the metrics that appear in the graph and in the table over a 10-minute period. To change the period to one hour, select the **Time Window** toggle.

Search the table by host name, MAC address, SSID, or operating system (OS).

Related Topics

Manage ExtremeCloud IQ CoPilot Licenses

During your free trial, there are no CoPilot licenses to manage, because your managed CoPilot-eligible devices use the 30-day grace period.

The following sections provide high-level information about CoPilot license management, including how to obtain CoPilot licenses. Use this information to inform your evaluation, and to prepare for an uninterrupted transition to your new CoPilot subscription.

For more information about CoPilot and other ExtremeCloud IQ licenses, see the *ExtremeCloud IQ Licensing Guide*.

CoPilot Licenses

CoPilot licenses offer eligible devices the additional functionality of ExtremeCloud IQ Pilot. You must have an ExtremeCloud IQ Pilot or an ExtremeCloud IQ Legacy Entitlement Key to use an ExtremeCloud IQ CoPilot license. ExtremeCloud IQ CoPilot is available for all ExtremeCloud IQ Pilot accounts, but is not available for Extreme Connect accounts or Navigator accounts. After you link your account to the Extreme Portal, ExtremeCloud IQ obtains the CoPilot licenses from the license pool.

The following devices are **NOT** eligible for ExtremeCloud IQ CoPilot licenses:

- ExtremeCloud IQ Controller
- Extreme Campus Controller
- Devices onboarded through Extreme Campus Controller
- WiNG devices
- Devices onboarded through ExtremeCloud IQ Controller

- Devices onboarded through ExtremeCloud IQ - Site Engine
- Digital Twin devices
- Simulated devices
- SR (legacy switch) devices reporting directly to ExtremeCloud IQ
- Dell N-series devices reporting directly to ExtremeCloud IQ
- Devices onboarded as **Managed Locally**
- Devices for which the license was revoked by using the **Actions** menu.

   Actions > **Change CoPilot License Status** > **Revoke CoPilot License**
- Unmanaged devices

Related Topics

CoPilot License Status

The following license status values can apply to CoPilot-eligible devices:

None

This status appears for the following reasons:

- CoPilot is not enabled for the VIQ.
- The device is not CoPilot compatible.
- The device is unmanaged.
- An administrator revoked the license.

Active

The CoPilot license is in use (consumed).

Grace Period

The CoPilot license is expired and the device is using the grace period.

Unlicensed

The CoPilot license and the grace period are expired.

Trial

CoPilot is enabled for the trial VIQ (90 days).

CoPilot Grace Period

ExtremeCloud IQ provides a 30-day grace period for unlicensed CoPilot-eligible devices. In the following cases, the grace period may apply to some of your devices:

- You enable the CoPilot feature.
- You onboard CoPilot eligible devices.
- A CoPilot license expires.

If you have fewer CoPilot licenses than CoPilot-eligible devices, the oldest (first onboarded) devices get CoPilot licenses first. The grace period applies to the newer devices that are not assigned a license. If a device is a stack and there are sufficient licenses to cover the stack, the system assigns the licenses to all stack units.

> **Note**
> After the CoPilot grace period begins, it cannot be paused or restarted. The grace period is a total of 30 days for each serial number.

Related Topics

Manage ExtremeCloud IQ CoPilot Licenses on page 34

Grace Period Notifications

When you have devices using the 30-day grace period, the user interface displays a banner to let you know.

LICENSE VIOLATION - Grace period is active. Check affected devices here.

You can enable email notifications and receive an email indicating that you have devices using the grace period, and again when the grace period expires.

Related Topics

Manage ExtremeCloud IQ CoPilot Licenses on page 34

CoPilot License Violations

If there are fewer ExtremeCloud IQ CoPilot licenses in the license pool than CoPilot-eligible devices, the 30-day grace period activates for some of your devices. If you have devices using the grace period, a banner displays the following information:

LICENSE VIOLATION - Grace period is active. Check affected devices here

After the grace period for a device expires, the device is CoPilot unlicensed. The CoPilot feature excludes unlicensed devices and does not process data from those devices. Anomalies and statistical reports are not reported in the CoPilot dashboard. If you have devices for which the grace period has expired, a banner displays the following information:

Some CoPilot eligible devices do not have a CoPilot license allocated. To benefit from the full value of CoPilot, consider adding CoPilot licenses for all devices that are eligible. Contact your Extreme or partner representative for assistance. Check affected devices here.

While the ExtremeCloud IQ CoPilot license violation is active, standard ExtremeCloud IQ Pilot features are not affected unless there is an active Pilot license violation. CoPilot license violations and Pilot license violations can be active at the same time.

To resolve an ExtremeCloud IQ CoPilot license violation:

- Contact Extreme Networks or your Extreme Networks Partner Sales Representative to purchase the required number of licenses, or renew expired licenses.
- Revoke CoPilot licenses for some devices. Go to **Manage** > **Devices**, select CoPilot-licensed devices, and then select **Actions** > **Change CoPilot License Status** > **Revoke CoPilot License**.
- Synchronize license information from your Extreme Portal account. Go to **Global Settings** > **Administration** > **License Management** and select **Synchronize**.
- Unlink and relink your Extreme Portal account to change the license pool.
- Change managed CoPilot-eligible devices to unmanaged.
- Disable CoPilot functions by turning off the feature. Go to **Global Settings** > **Administration** > **VIQ Management** and slide the toggle to **Off**.

Multiple accounts

To help prevent license shortages, you can select which VIQs (accounts) use CoPilot. Enable or disable ExtremeCloud IQ CoPilot for each ExtremeCloud IQ account in **Global Settings** > **Administration** > **VIQ Management** > **Enable/Disable CoPilot feature for this VIQ**.

> **Note**
>
> If you have multiple ExtremeCloud IQ accounts with ExtremeCloud IQ CoPilot linked to the same license pool, there might not be enough licenses to satisfy your requirements. For example, if two branches in different geolocations share the same pool, the first come, first served rule applies. To resolve this situation, do one of the following:
>
> - Disable ExtremeCloud IQ CoPilot for the ExtremeCloud IQ account that is in violation.
> - Add the required number of ExtremeCloud IQ CoPilot licenses.

Related Topics

Activate or Revoke a CoPilot License

ExtremeCloud IQ CoPilot must be enabled and the device must be CoPilot-eligible.

Use the following procedure to choose whether a CoPilot-eligible device gets a license. This procedure is useful if you have fewer CoPilot licenses than eligible devices.

1. Go to **Manage** > **Devices**.
2. Select the device for which you want to activate or revoke the CoPilot license.
3. From the **Actions** menu, select **Change CoPilot License Status** > **Activate CoPilot License** or **Revoke CoPilot License**.

Purchase CoPilot Licenses

Contact Extreme Networks, or your Extreme Networks Partner Sales Representative, or use the following procedure to obtain CoPilot licenses.

Use this procedure any time that you want to purchase more licenses.

➡️ **Important**

When you add new licenses to your linked Extreme Portal account, ExtremeCloud IQ automatically assigns the licenses to eligible devices and ends the trial period.

If the 90-day trial of ExtremeCloud IQ is active, linking your Extreme Portal account ends the trial.

1. Go to **Global Settings** > **License Management**.
2. Select **Contact Sales**.
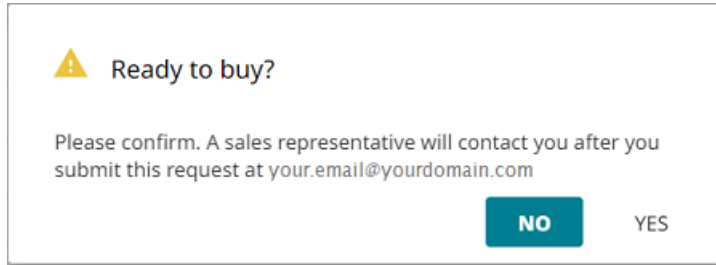3. On the **Ready to buy?** dialog, select **Yes**.

⚠️ **Ready to buy?**

Please confirm. A sales representative will contact you after you submit this request at your.email@yourdomain.com

NO   YES

Figure 25: Ready to buy?

4. Use the following part numbers to order ExtremeCloud IQ CoPilot licenses:

Table 4: Part Numbers

Part Number	Description
XIQ-COPILOT-S-C-PWP	ExtremeCloud IQ CoPilot SaaS Subscription PartnerWorks Plus SaaS Support for one device for one year
XIQ-COPILOT-S-C-EW	ExtremeCloud IQ CoPilot SaaS Subscription ExtremeWorks SaaS Support for one device for one year

Related Topics

Manage ExtremeCloud IQ CoPilot Licenses on page 34