ExtremeCloud IQ CoPilot Deployment Guide

Version 24.4.0

9038925-00 Rev AA
May 2024

Copyright © 2024 Extreme Networks, Inc. All rights reserved.

Legal Notice

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

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

Trademarks

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

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

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

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

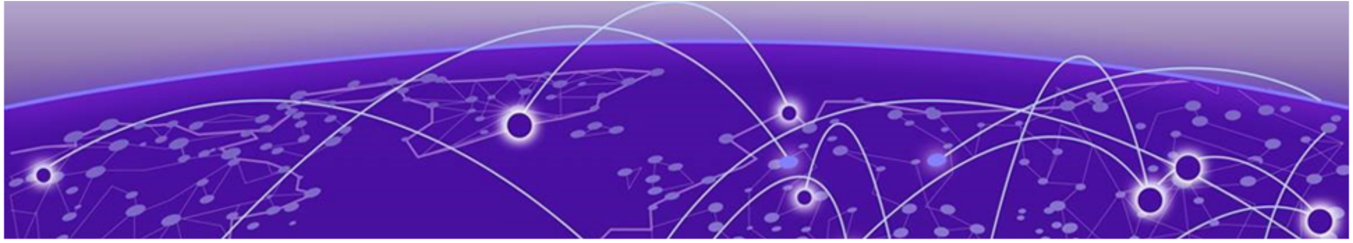


Table of Contents

Preface..... 5

Text Conventions..... 5

Documentation and Training..... 6

Open Source Declarations..... 7

Training..... 7

Help and Support..... 7

Subscribe to Product Announcements..... 8

Send Feedback..... 8

Welcome to ExtremeCloud IQ CoPilot..... 9

CoPilot Overview..... 9

Instant Anomaly Detection..... 10

Deploy ExtremeCloud IQ CoPilot..... 12

Deployment Tasks..... 12

Enable CoPilot..... 12

Enable CoPilot for the VIQ..... 13

Use the ExtremeCloud IQ CoPilot Dashboard..... 14

Connectivity Experiences..... 14

Quality Index for Wireless Devices Widget..... 15

Quality Index for Wired Devices Widget..... 15

Connectivity Experiences Table..... 16

Connectivity Experiences Panel (Wireless)..... 17

Client Association (Wireless)..... 18

Client Authentication (Wireless)..... 20

Time to Obtain IP Address (Wireless)..... 22

Connectivity Experiences Panel (Wired)..... 23

Port Errors..... 24

Anomalies..... 25

Instant Anomaly Detection..... 26

Top Anomalies by Site Widget..... 27

Anomalies by Severity Widget..... 27

Top Anomalies by Type Widget..... 28

Anomalies Table..... 33

Anomaly Trends..... 36

Manage ExtremeCloud IQ CoPilot Licenses..... 38

CoPilot Licenses..... 38

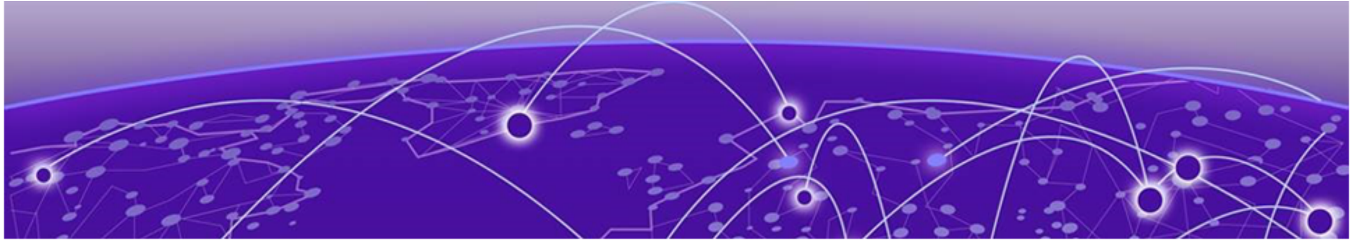
CoPilot License Status..... 39

CoPilot Grace Period..... 39

Grace Period Notifications..... 40

Enable or Disable Proactive Email Notifications..... 40

CoPilot License Violations 40
  Multiple accounts 41
Activate or Revoke a CoPilot License 42
Purchase CoPilot Licenses 42



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 Extreme Networks 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.

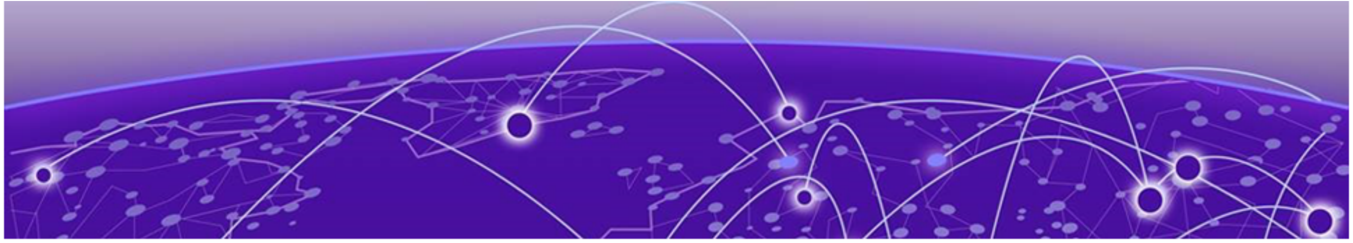
Send Feedback

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

CoPilot Overview on page 9
Instant Anomaly Detection on page 10

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:

- Simplifies troubleshooting by providing auditable recommendations to reduce the number of out-of-context alerts that can waste time and effort
- Identifies anomalies and alerts you, providing an explanation and the best options for resolution
- Reduces risk by proactively looking for patterns ahead of time to identify significant anomalies so IT can address them early

- Utilizes continuous learning and bidirectional communication to provide the best and most accurate recommendations for your network
- Summarizes the client connectivity experience into a single quality index score, and helps you to easily track, identify, and troubleshoot connectivity issues

Table 4: Copilot Capabilities Summary

Capability	Wireless Network	Wired Network	Description
Connectivity Experiences	♦	♦	Summarizes the client experience into a single quality index score to easily track, identify, and troubleshoot connectivity issues.
Wi-Fi Capacity Anomaly	♦		Access points (APs) with unusually high channel utilization, reporting instances of excessive recurrence and duration.
Wi-Fi Efficiency Anomaly	♦		Unusually high channel utilization, reporting instances of excessive recurrence and duration.
DFC Recurrence Anomaly	♦		Access points with excessive channel changes due to external 5Ghz interference, such as radar.
Port Efficiency Anomaly	♦	♦	Access point and Switch (SW) ports with bad cabling, faulty ports, auto-negotiation issues.
PoE Stability Anomaly	♦	♦	Access point and SW ports with bad cabling, power supply consistency issues, insufficient power provided.
Adverse Traffic Patterns Anomaly	♦	♦	Access points and switches with traffic loading issues that cause excessive usage of CPU and memory resources.

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

Related Topics

Instant Anomaly Detection on page 10

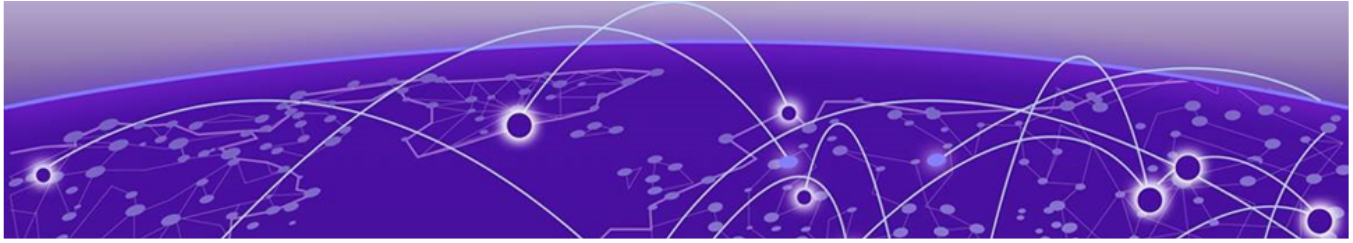
Use the ExtremeCloud IQ CoPilot Dashboard on page 14

Instant Anomaly Detection

CoPilot provides instant anomaly detection, so no tuning is required. Instant anomaly detection provides the following benefits:

- Automatically applies and updates the historical data for newly added or licensed devices.
- CoPilot aggregates and correlates historical and latest data streams.
- Algorithms identify normal patterns and establish dynamic baselines.

- To reduce bias and false positives, CoPilot determines dynamic baselines by considering local and regional values.
- CoPilot identifies anomalies at multiple levels: local device, installed location, associated devices, and across multiple sites.



Deploy ExtremeCloud IQ CoPilot

Deployment Tasks on page 12
Enable CoPilot on page 12
Enable CoPilot for the VIQ on page 13

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

- Enable CoPilot on page 12
- Enable CoPilot for the VIQ on page 13

> **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 12, or use Enable CoPilot for the VIQ on page 13.

Enable CoPilot

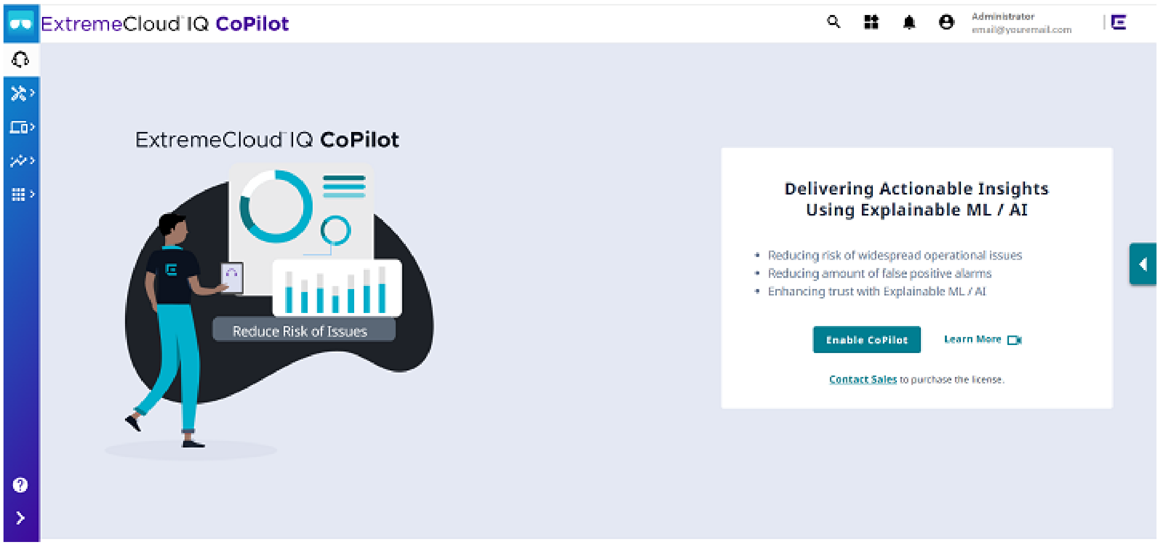
Use this procedure to enable CoPilot and start your 30-day trial.

> **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**.



ExtremeCloud IQ CoPilot

Administrator
email@youremail.com

ExtremeCloud IQ CoPilot

Delivering Actionable Insights
Using Explainable ML / AI

- Reducing risk of widespread operational issues
- Reducing amount of false positive alarms
- Enhancing trust with Explainable ML / AI

Contact Sales to purchase the license.

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 42

Deployment Tasks on page 12

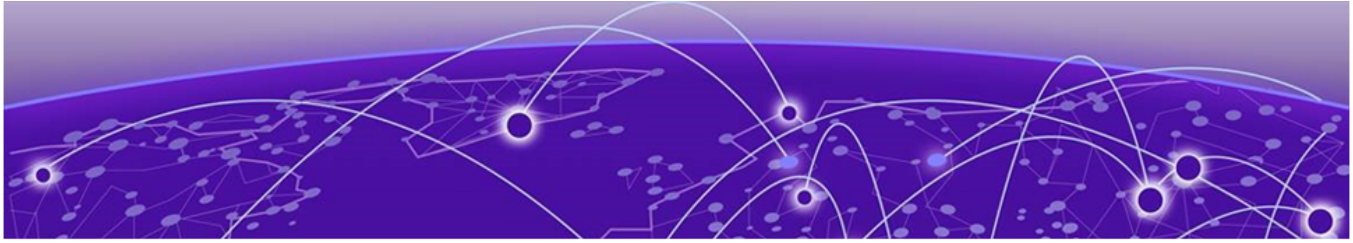
Enable CoPilot for the VIQ

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 12



Use the ExtremeCloud IQ CoPilot Dashboard

Connectivity Experiences on page 14
Anomalies on page 25

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:

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

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.

NEW! Connectivity Experiences

The quality index scores client connectivity experiences from 1 (worst) to 10 (best). In an ideal scenario, the quality index is 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 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.

The **Connectivity Experiences** tab uses the following widgets and a table to display information about connection quality:

- Quality Index for Wireless Devices Widget on page 15
- Quality Index for Wired Devices Widget on page 15

The widgets and table are interactive. Mouse over them to see more details.

To hide the widgets and display a streamlined view of **Sites by Quality Index**, select ⌃.

To display the widgets again, select ⌄.

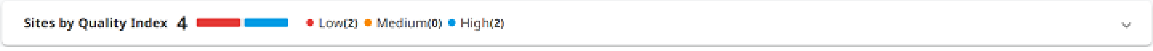


Figure 1: Sites by Quality Index Streamlined View

Related Topics

Quality Index for Wireless Devices Widget on page 15
Quality Index for Wired Devices Widget on page 15
Connectivity Experiences Table on page 16
Connectivity Experiences Panel (Wired) on page 23
Connectivity Experiences Panel (Wireless) on page 17

*NEW!*Quality Index for Wireless Devices Widget

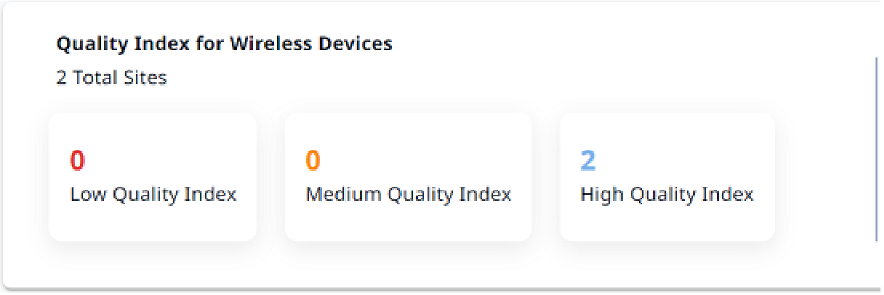


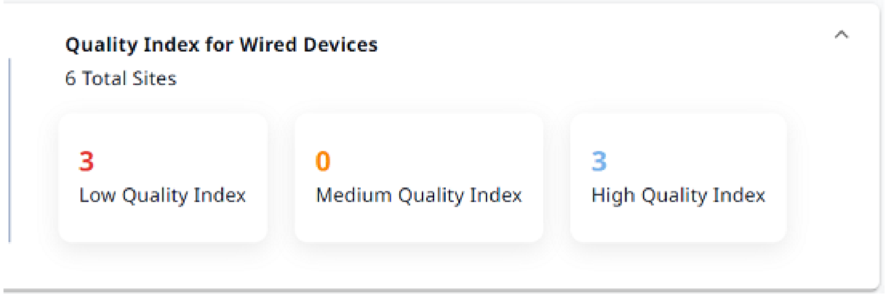
Figure 2: Quality Index for Wireless Devices

The **Quality Index for Wireless Devices** widget shows the number of wireless sites for each quality index category: Low, Medium, and High. Select a quality index category to update the table to show only sites with the selected quality index.

Related Topics

Connectivity Experiences on page 14

NEW! Quality Index for Wired Devices Widget



Quality Index for Wired Devices

6 Total Sites

3 Low Quality Index

0 Medium Quality Index

3 High Quality Index

Figure 3: Quality Index for Wired Devices

The **Quality Index for Wired Devices** widget shows the number of wired sites for each quality index category: Low, Medium, and High. Select a quality index category to update the table to show only sites with the selected quality index.

Related Topics

Connectivity Experiences on page 14

NEW! Connectivity Experiences Table

The **Connectivity Experiences** table displays connection quality information for the previous 24 hours, and includes the following information for each entry:

- **Site**
- **Connectivity Type**
- **Quality Index**
- **Trend**

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:

Site

Display all sites (default) or select a specific site from the menu. Start typing a site name to search the menu for a particular site.

To return to the default view, select **X**.

Connectivity Type

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

To return to the default view, select **X**.

Quality Index

Select Low (1–5), Medium (6–8), or High (8–9). The table updates to display the wired and wireless sites that match your selection.

To return to the default view, select **X**.

Time Range

Use the calendar control to select the time period for which you want to display connection quality trends information. Select the calendar control to open it and then select one of the options:

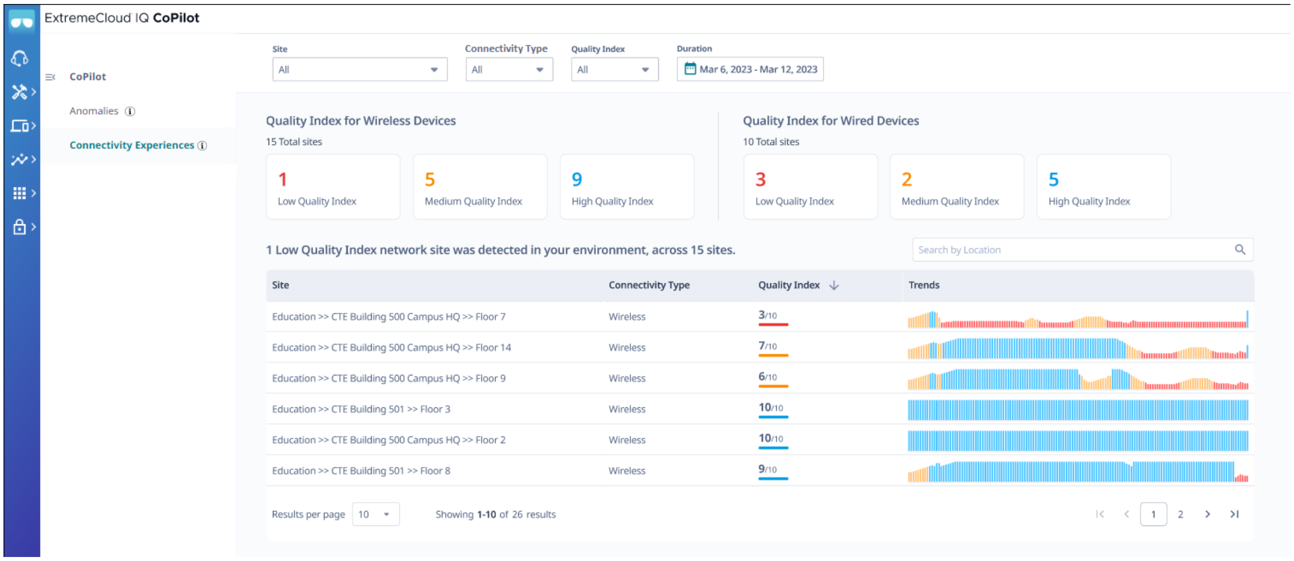
- Last 24 Hours
- 7 Days
- Custom

  Select the start date and time, and then select the end date and time for the period.

Search by Location

Start typing a site name to search the table for a site. Select **X** to clear the search string and return to the previous table view.

To sort the table results in ascending or descending order according to **Site**. Hover the mouse to the right of the corresponding column label, and select the ↑. To change the sort order again, select the ↑. You can also search for connection quality information by site. Use the **Items per page** menu to specify the maximum number of results to show, per page.



Site: All
Connectivity Type: All
Quality Index: All
Duration: Mar 6, 2023 - Mar 12, 2023

Quality Index for Wireless Devices
15 Total sites
1 Low Quality Index
5 Medium Quality Index
9 High Quality Index

Quality Index for Wired Devices
10 Total sites
3 Low Quality Index
2 Medium Quality Index
5 High Quality Index

1 Low Quality Index network site was detected in your environment, across 15 sites.

Search by Location

Site	Connectivity Type	Quality Index ↓	Trends
Education >> CTE Building 500 Campus HQ >> Floor 7	Wireless	3/10	
Education >> CTE Building 500 Campus HQ >> Floor 14	Wireless	7/10	
Education >> CTE Building 500 Campus HQ >> Floor 9	Wireless	6/10	
Education >> CTE Building 501 >> Floor 3	Wireless	10/10	
Education >> CTE Building 500 Campus HQ >> Floor 2	Wireless	10/10	
Education >> CTE Building 501 >> Floor 8	Wireless	9/10	

Results per page 10   Showing **1-10** of 26 results   1 2

Figure 4: Connectivity Experiences table

Related Topics

Connectivity Experiences on page 14

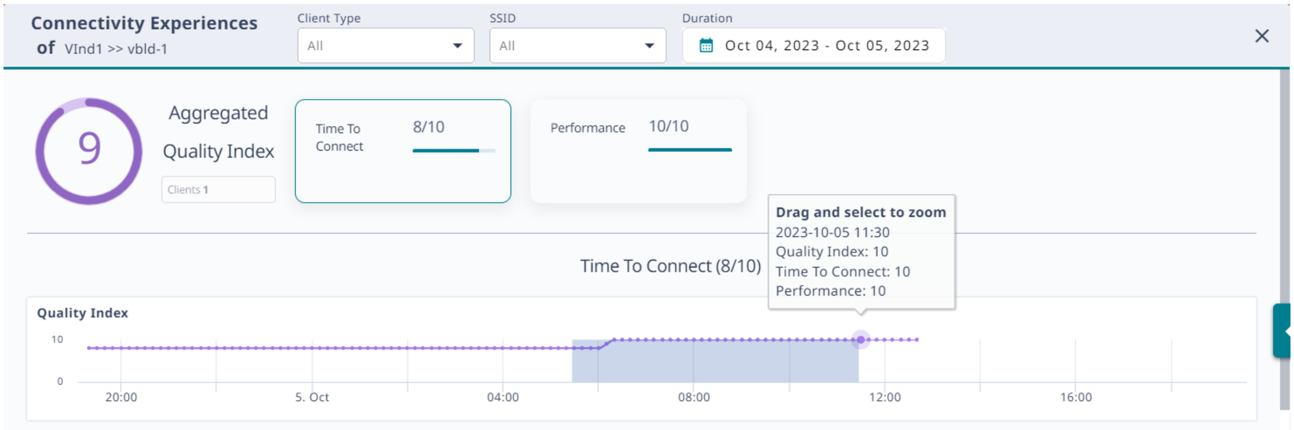
Connectivity Experiences Panel (Wireless)

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.



Connectivity Experiences of VInd1 >> vbld-1

Client Type: All

SSID: All

Duration: Oct 04, 2023 - Oct 05, 2023

9 Aggregated Quality Index

Clients 1

Time To Connect 8/10

Performance 10/10

Drag and select to zoom
2023-10-05 11:30
Quality Index: 10
Time To Connect: 10
Performance: 10

Figure 5: Connectivity Experiences Panel (Wireless)

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

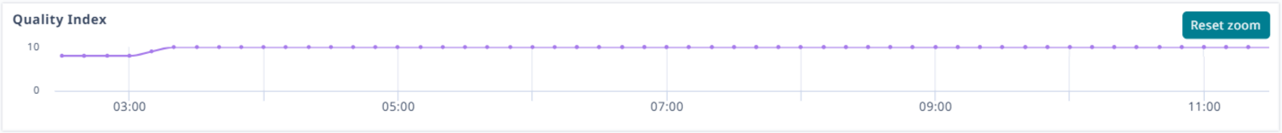


Figure 6: Quality Index Zoom

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

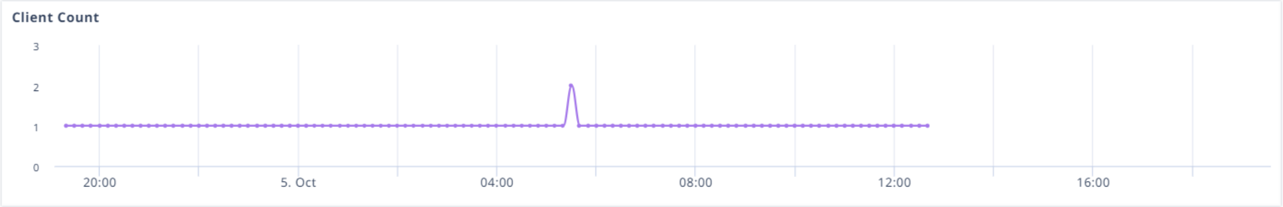


Figure 7: Client Count

Related Topics

Connectivity Experiences on page 14

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

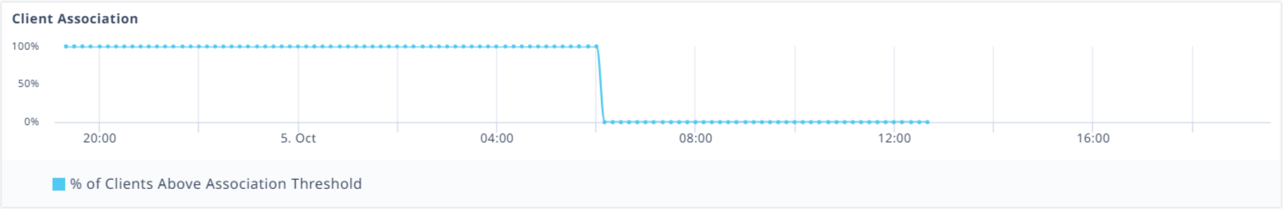
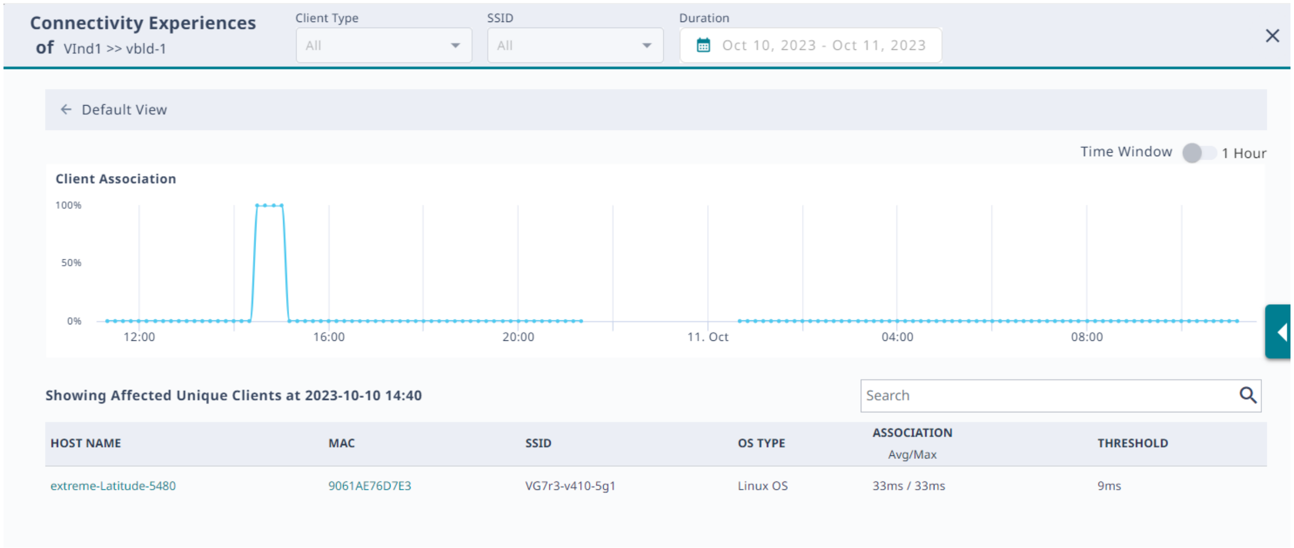


Figure 8: Client Association

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



Client Type: All

SSID: All

Duration: Oct 10, 2023 - Oct 11, 2023

Time Window 1 Hour

Showing Affected Unique Clients at 2023-10-10 14:40

HOST NAME	MAC	SSID	OS TYPE	ASSOCIATION Avg/Max	THRESHOLD
extreme-Latitude-5480	9061AE76D7E3	VG7r3-v410-5g1	Linux OS	33ms / 33ms	9ms

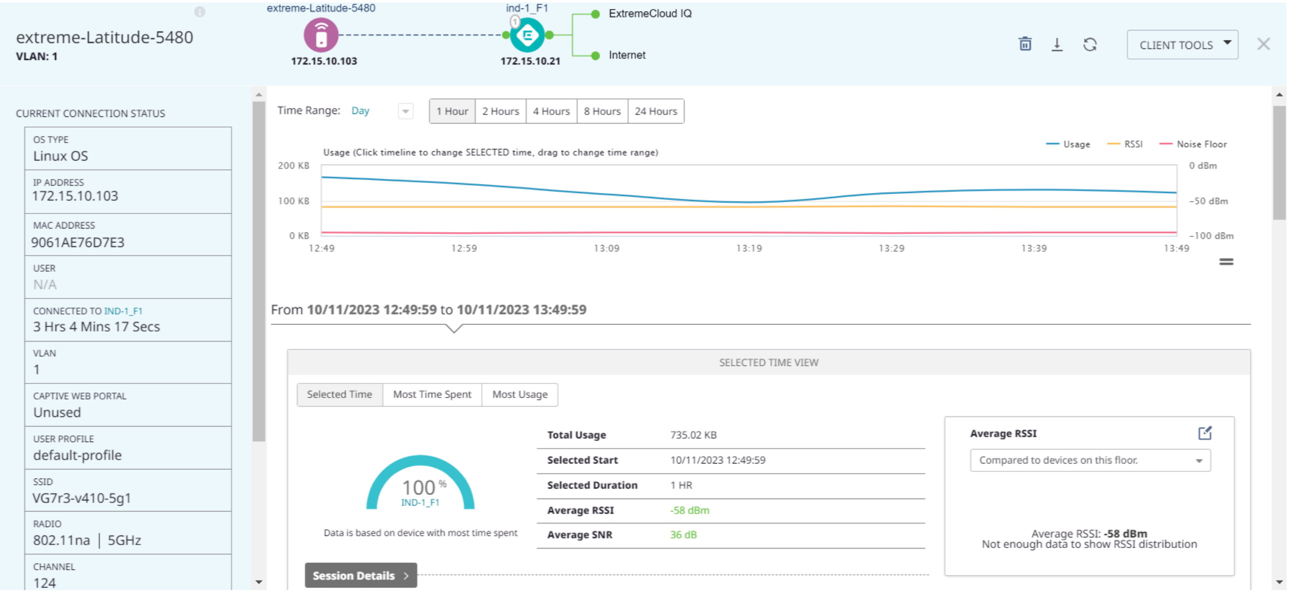
Figure 9: Client Association Panel

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.



extreme-Latitude-5480
VLAN: 1

CURRENT CONNECTION STATUS

OS TYPE	Linux OS
IP ADDRESS	172.15.10.103
MAC ADDRESS	9061AE76D7E3
USER	N/A
CONNECTED TO IND-1_F1	3 Hrs 4 Mins 17 Secs
VLAN	1
CAPTIVE WEB PORTAL	Unused
USER PROFILE	default-profile
SSID	VG7r3-v410-5g1
RADIO	802.11na | 5GHz
CHANNEL	124

From 10/11/2023 12:49:59 to 10/11/2023 13:49:59

Data is based on device with most time spent

Total Usage	735.02 KB
Selected Start	10/11/2023 12:49:59
Selected Duration	1 HR
Average RSSI	-58 dBm
Average SNR	36 dB

Average RSSI

Compared to devices on this floor.

Average RSSI: -58 dBm
Not enough data to show RSSI distribution

Figure 10: Connection Details Panel

Related Topics

Connectivity Experiences on page 14

Connectivity Experiences Panel (Wireless) on page 17

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

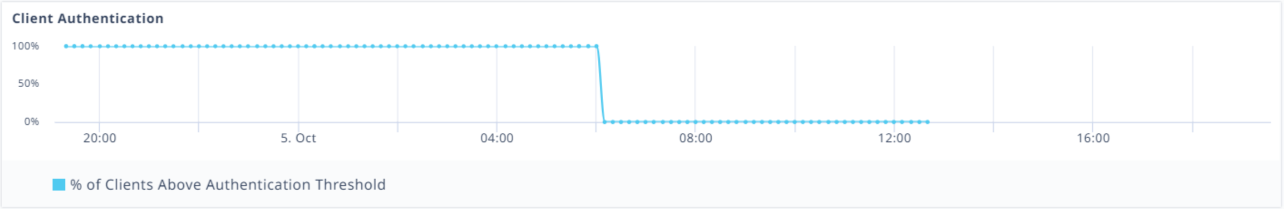
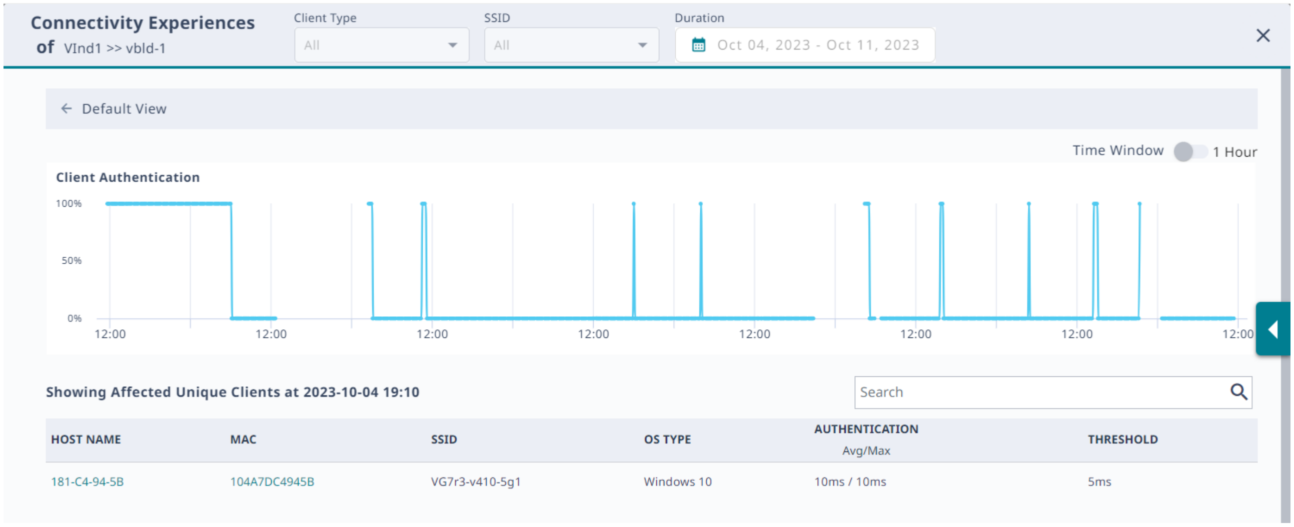


Figure 11: Client Authentication

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



Connectivity Experiences of Vlnd1 >> vbld-1

Client Type: All

SSID: All

Duration: Oct 04, 2023 - Oct 11, 2023

← Default View

Time Window 1 Hour

Showing Affected Unique Clients at 2023-10-04 19:10

HOST NAME	MAC	SSID	OS TYPE	AUTHENTICATION Avg/Max	THRESHOLD
181-C4-94-5B	104A7DC4945B	VG7r3-v410-5g1	Windows 10	10ms / 10ms	5ms

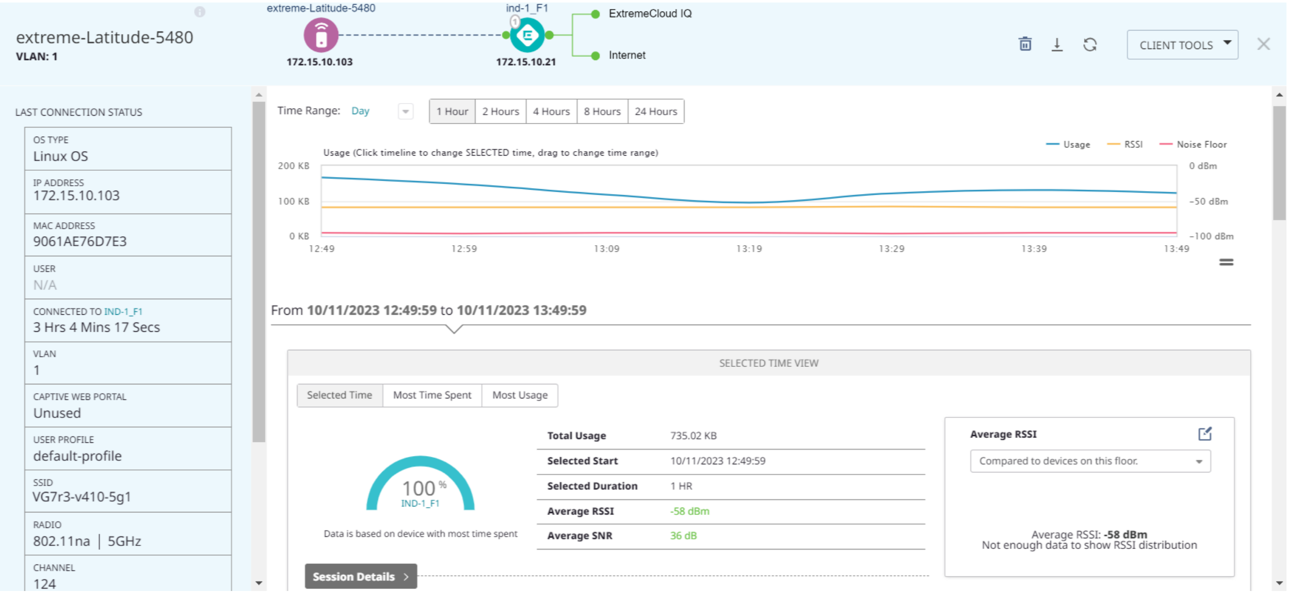
Figure 12: Client Authentication Panel

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.



extreme-Latitude-5480
VLAN: 1

LAST CONNECTION STATUS

OS TYPE	Linux OS
IP ADDRESS	172.15.10.103
MAC ADDRESS	9061AE76D7E3
USER	N/A
CONNECTED TO IND-1_F1	3 Hrs 4 Mins 17 Secs
VLAN	1
CAPTIVE WEB PORTAL	Unused
USER PROFILE	default-profile
SSID	VG7r3-v410-5g1
RADIO	802.11na | 5GHz
CHANNEL	124

Time Range: Day

From **10/11/2023 12:49:59** to **10/11/2023 13:49:59**

SELECTED TIME VIEW

Data is based on device with most time spent

Total Usage	735.02 KB
Selected Start	10/11/2023 12:49:59
Selected Duration	1 HR
Average RSSI	-58 dBm
Average SNR	36 dB

Average RSSI

Compared to devices on this floor.

Average RSSI: **-58 dBm**
Not enough data to show RSSI distribution

Figure 13: Connection Details Panel

Related Topics

Connectivity Experiences Panel (Wireless) on page 17

Connectivity Experiences on page 14

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

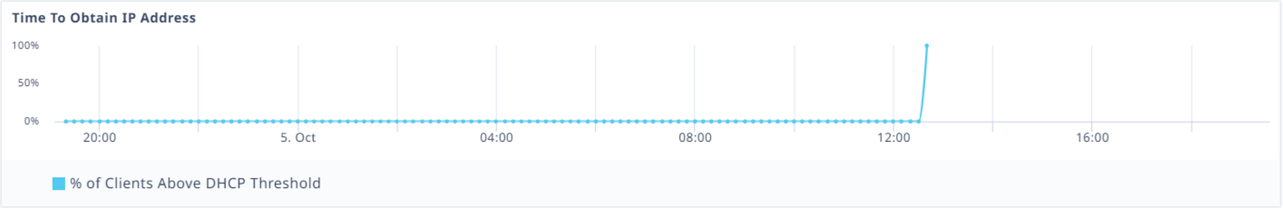
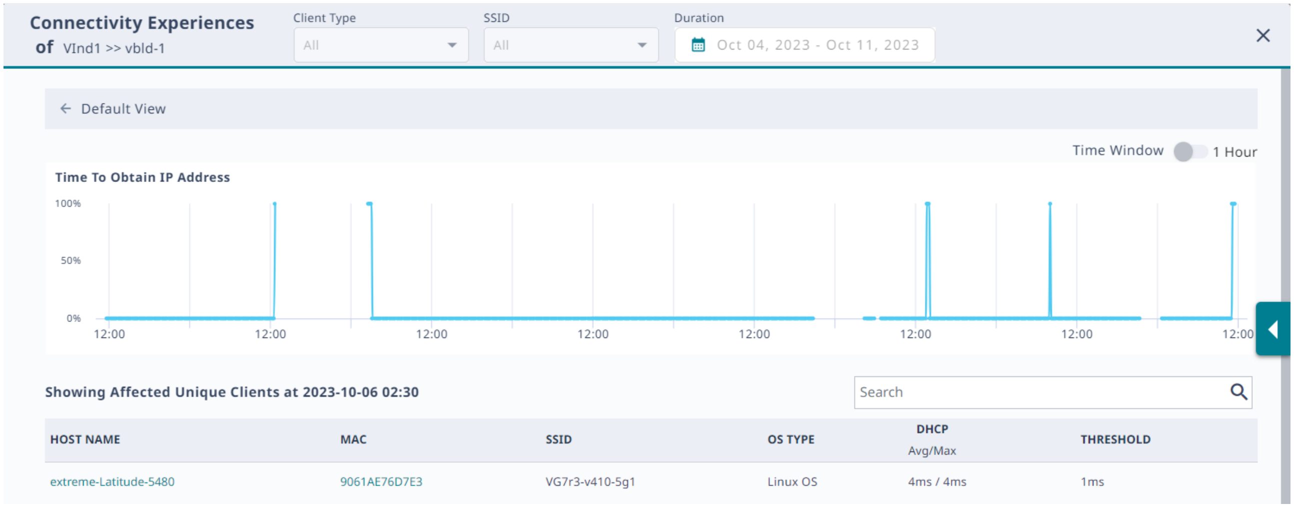


Figure 14: Time To Obtain IP Address

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



Showing Affected Unique Clients at 2023-10-06 02:30

HOST NAME	MAC	SSID	OS TYPE	DHCP Avg/Max	THRESHOLD
extreme-Latitude-5480	9061AE76D7E3	VG7r3-v410-5g1	Linux OS	4ms / 4ms	1ms

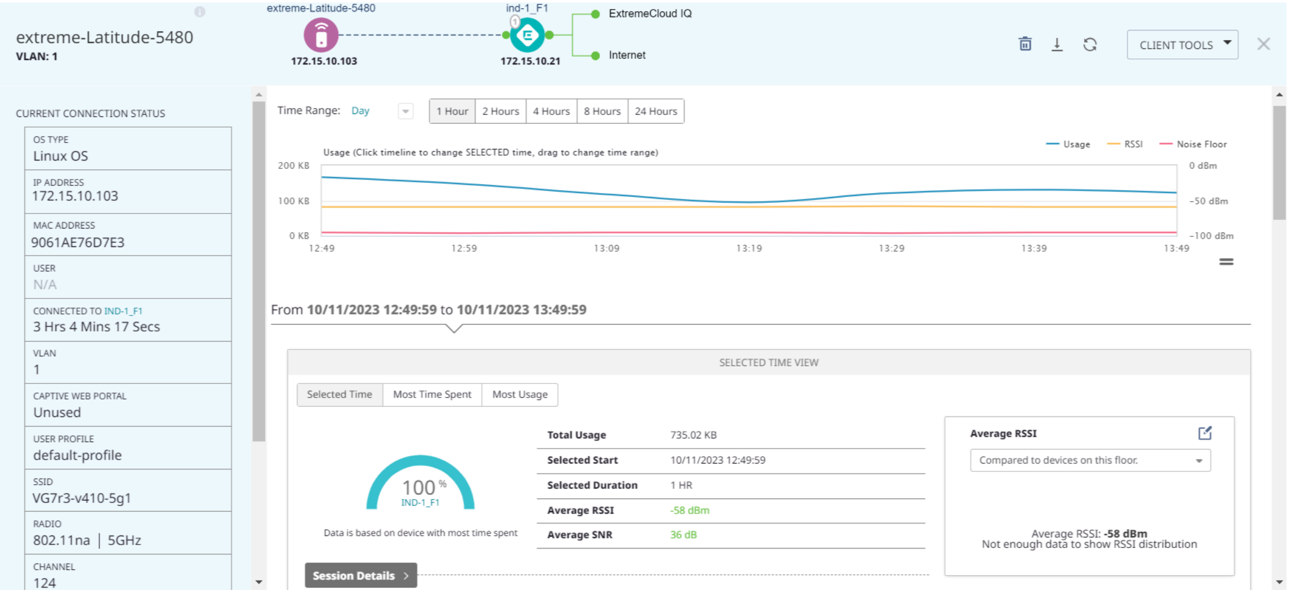
Figure 15: Time To Obtain IP Address Panel

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.



extreme-Latitude-5480
VLAN: 1

CURRENT CONNECTION STATUS

OS TYPE	Linux OS
IP ADDRESS	172.15.10.103
MAC ADDRESS	9061AE76D7E3
USER	N/A
CONNECTED TO IND-1_F1	3 Hrs 4 Mins 17 Secs
VLAN	1
CAPTIVE WEB PORTAL	Unused
USER PROFILE	default-profile
SSID	VG7r3-v410-5g1
RADIO	802.11na | 5GHz
CHANNEL	124

From **10/11/2023 12:49:59** to **10/11/2023 13:49:59**

Data is based on device with most time spent

Total Usage	735.02 KB
Selected Start	10/11/2023 12:49:59
Selected Duration	1 HR
Average RSSI	-58 dBm
Average SNR	36 dB

Average RSSI

Compared to devices on this floor.

Average RSSI: **-58 dBm**
Not enough data to show RSSI distribution

Figure 16: Connection Details Panel

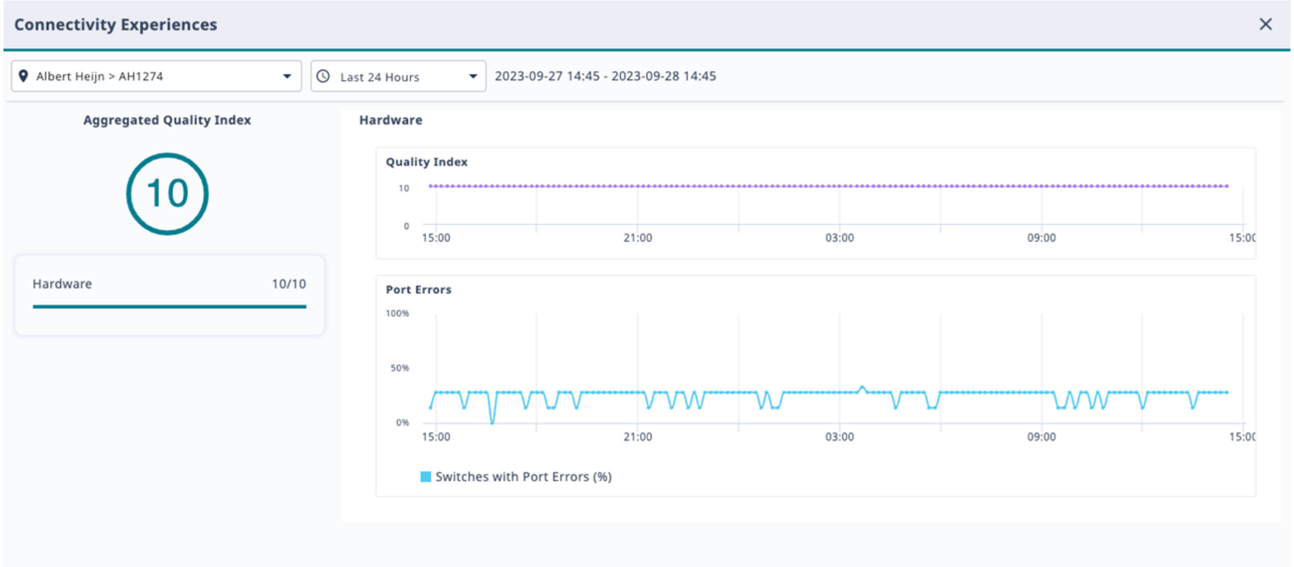
Related Topics

Connectivity Experiences Panel (Wireless) on page 17

Connectivity Experiences on page 14

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**.



Connectivity Experiences

Albert Heijn > AH1274

Last 24 Hours

2023-09-27 14:45 - 2023-09-28 14:45

Figure 17: 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.

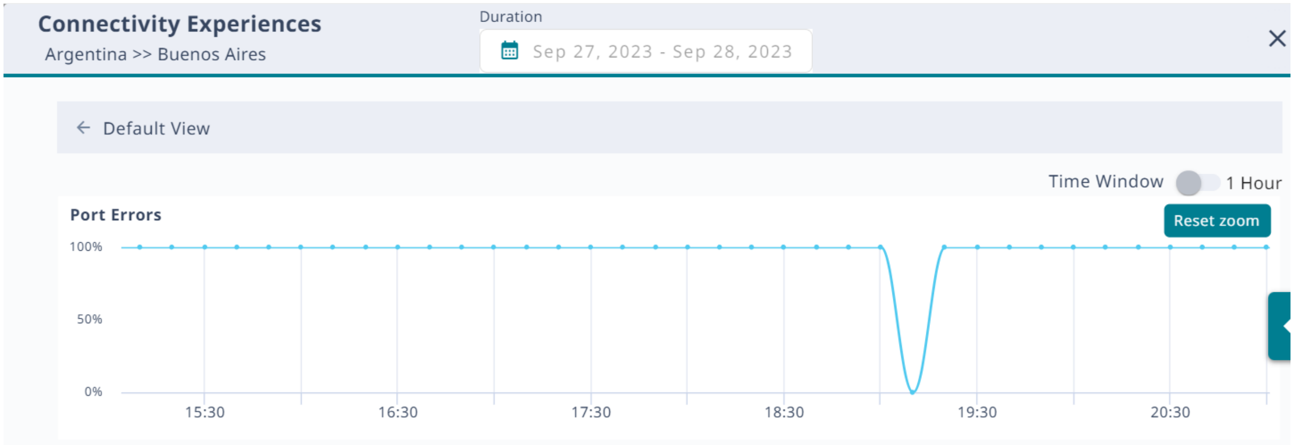
Related Topics

Port Errors on page 24

Connectivity Experiences on page 14

Port Errors

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



Connectivity Experiences

Argentina >> Buenos Aires

Duration

Sep 27, 2023 - Sep 28, 2023

Figure 18: Port Errors

To zoom back out again, select **Reset zoom**. To return to the **Default View**, select the back arrow.

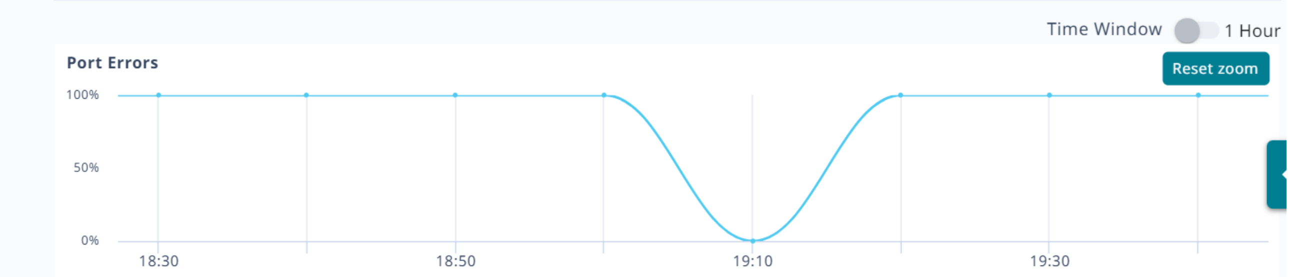
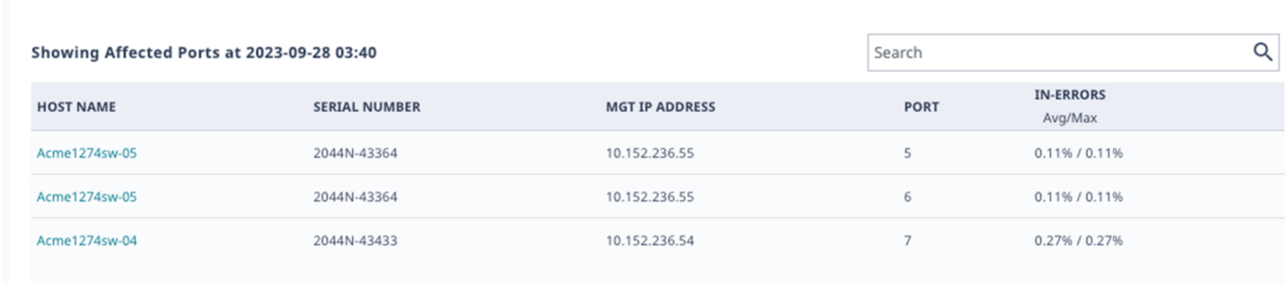


Figure 19: Port Errors Zoom

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



Showing Affected Ports at 2023-09-28 03:40

Search

HOST NAME	SERIAL NUMBER	MGT IP ADDRESS	PORT	IN-ERRORS Avg/Max
Acme1274sw-05	2044N-43364	10.152.236.55	5	0.11% / 0.11%
Acme1274sw-05	2044N-43364	10.152.236.55	6	0.11% / 0.11%
Acme1274sw-04	2044N-43433	10.152.236.54	7	0.27% / 0.27%

Figure 20: 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

Connectivity Experiences Panel (Wired) on page 23

Anomalies

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

- Top Anomalies by Site Widget on page 27
- Anomalies by Severity Widget on page 27
- Top Anomalies by Type Widget on page 28

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

To display the widgets again, select ⌄ .

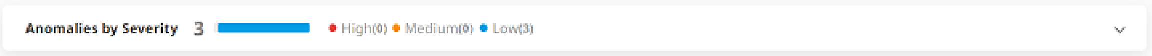


Figure 21: Anomalies by Severity Streamlined View

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 type of anomaly from the menu.

Duration

Display anomalies for the past 24 hours (default), or the past 7 days.

Exclude Muted

Toggle to hide or display previously muted anomalies.

Trends

Display the **Anomaly Trends** graph that shows anomalies for all sites and severities for the past 90 days.

Refresh

Refresh the display by selecting ↻.

Related Topics

Top Anomalies by Site Widget on page 27
Anomalies by Severity Widget on page 27
Top Anomalies by Type Widget on page 28
Anomaly Trends on page 36

Instant Anomaly Detection

CoPilot provides instant anomaly detection, so no tuning is required. Instant anomaly detection provides the following benefits:

- Automatically applies and updates the historical data for newly added or licensed devices.
- CoPilot aggregates and correlates historical and latest data streams.
- Algorithms identify normal patterns and establish dynamic baselines.
- To reduce bias and false positives, CoPilot determines dynamic baselines by considering local and regional values.
- CoPilot identifies anomalies at multiple levels: local device, installed location, associated devices, and across multiple sites.

Top Anomalies by Site Widget

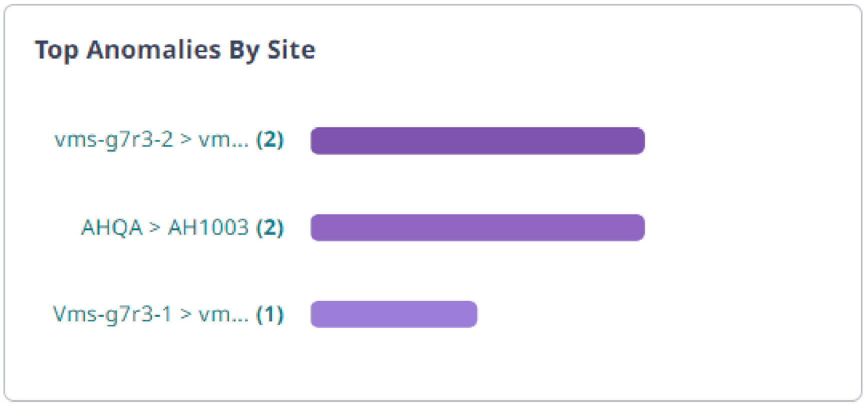


Figure 22: Top Anomalies By Site

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 on page 25

Anomalies by Severity Widget

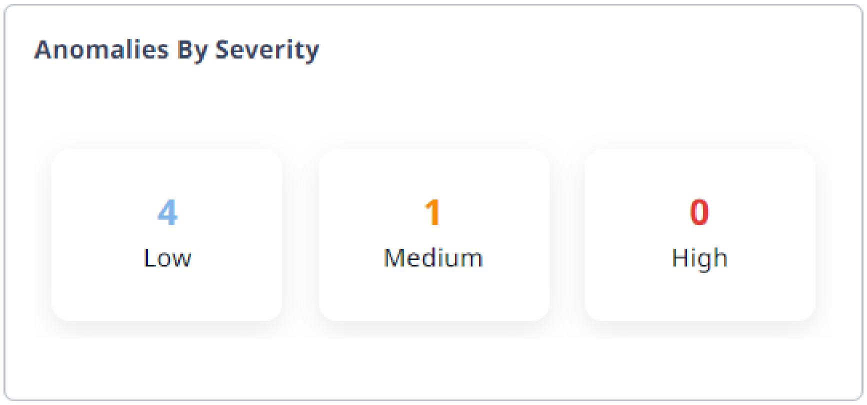


Figure 23: Anomalies By Severity

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 25

Top Anomalies by Type Widget

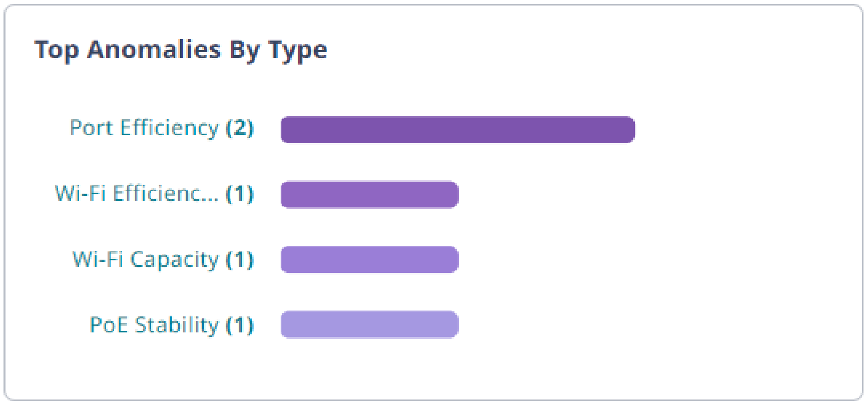


Figure 24: Top Anomalies By Type

The **Top Anomalies By Type** widget shows the most common types of anomalies for your network. From the menu, 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

Adverse Traffic Patterns on page 28
DFS Recurrence on page 28
PoE Stability on page 29
Port Efficiency on page 32
Wi-Fi Capacity on page 33
Wi-Fi Efficiency on page 33
Anomalies on page 25

Adverse Traffic Patterns

Adverse traffic patterns are caused by TX and RX traffic loads that result in high resource use of multicast and broadcast communications. The 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.

Related Topics

Top Anomalies by Type Widget on page 28

DFS Recurrence

Dynamic Frequency Selection (DFS) recurrence anomalies are related to radar-influenced channel changes. When an access point switches channels, the quality of service for connected clients might decrease temporarily, while repeated channel changes might 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 being:

- 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

Top Anomalies by Type Widget on page 28

NEW! *PoE Stability*

Access Points (AP) 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 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.

Table 5: PoE Standards

Standard	Description
PoE (AF)	IEEE 802.3af
PoE+ (AT)	IEEE 802.3at
PoE++ (BT)	IEEE 802.3bt

PoE stability anomalies are related to sudden changes in power draw. Data is presented over a 48-hour period, and includes date and time details. When an AP negotiates down to AF, even though it requires AT or a higher level for optimal performance and full capacity, CoPilot reports a PoE anomaly.

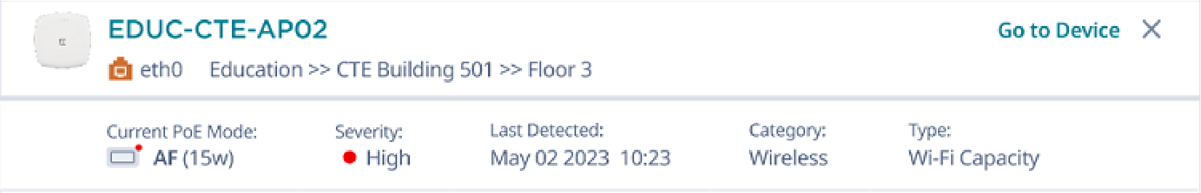
The severity definitions for PoE anomalies are based on the average number of clients connected to an AP on a given day. If there are fewer than 10 clients, the anomaly severity is considered low. If there are 50 or more clients on a given day, the severity level is considered high. If there are between 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 might cause APs to cycle through power modes, while never reaching a steady state.

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

Header

This section provides general information about the anomaly.



EDUC-CTE-AP02

eth0 Education >> CTE Building 501 >> Floor 3

Current PoE Mode: AF (15w)

Severity: ● High

Last Detected: May 02 2023 10:23

Category: Wireless

Type: Wi-Fi Capacity

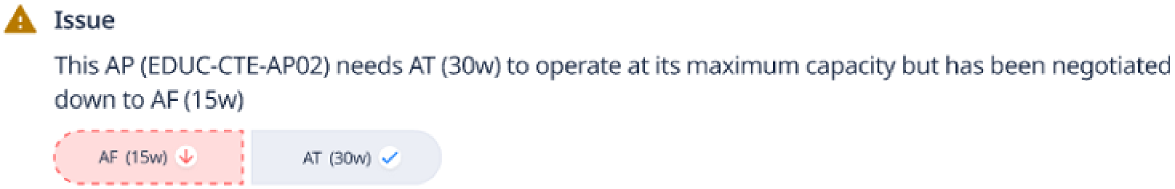
Figure 25: PoE Stability Anomaly Header

The **Current PoE Mode** shows whether the affected device is online and the current power mode—AF, AT or BT. If the AP is offline, the status is **Disconnected**.

To get more information about the device, select **Go to Device**.

Issue

This section provides a description of the problem, including the actual PoE mode and the desired PoE mode.



Issue

This AP (EDUC-CTE-AP02) needs AT (30w) to operate at its maximum capacity but has been negotiated down to AF (15w)

Figure 26: Issue

Impact

This section describes the effect the anomaly has on the system, for example: *Lower coverage and performance in the coverage area*

Recommendation

This section provides steps to resolve the anomaly, for example:

1. Verify whether there is sufficient PoE budget on the upstream switch.
2. Verify that the network cable length is not beyond 100 meters (328 feet), is properly connected to the AP, and that the cable does not have any signs of damage.

PoE Trend

The **PoE Trend** graph shows the pattern of changes in PoE mode for the 48 hours prior to the last detected timestamp. To view the graph, select the down arrow.

The graph indicates the three power modes: AF, AT and BT Type 3. Red indicates a low power mode.

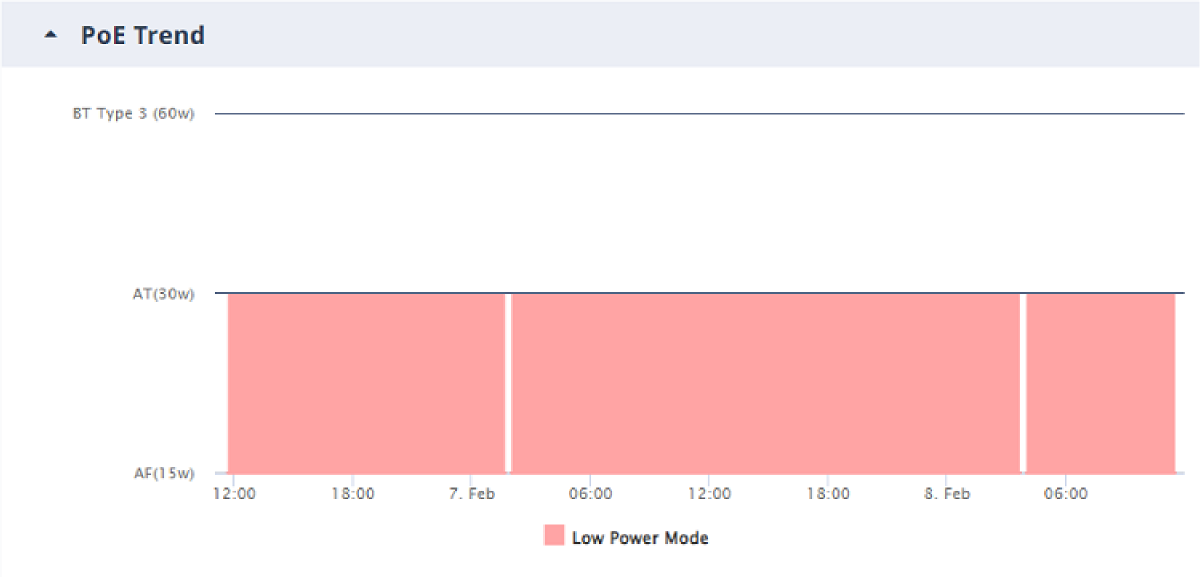


Figure 27: PoE Trend

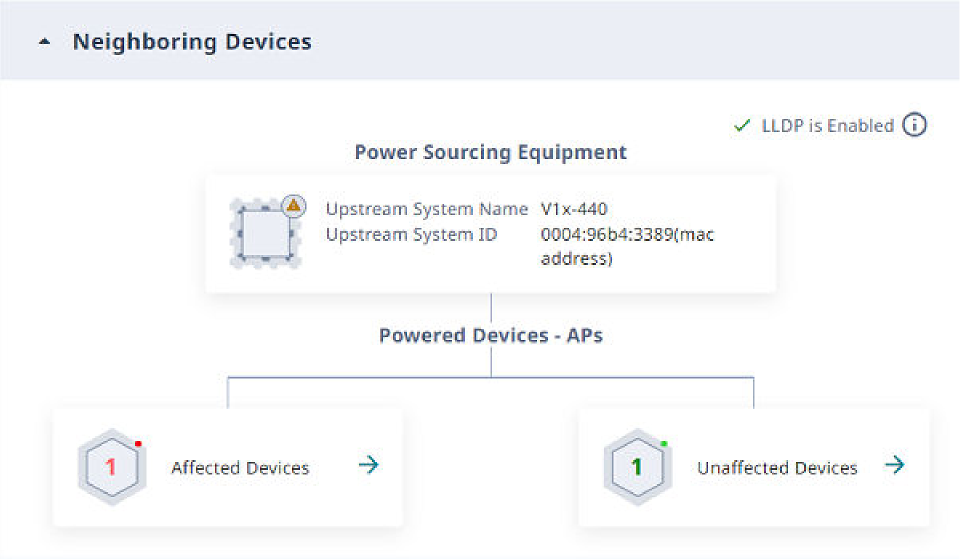
Select and drag across the timeline to zoom in on a section. Select **Reset zoom** to return to view the entire timeline.

Neighboring Devices

If LLDP is enabled on the AP, the **Neighboring Devices** section provides useful information for troubleshooting power sourcing equipment, and nearby APs connected to the affected AP. To expand this section, select the down arrow.

Note

If LLDP is enabled and the upstream device is an Extreme switch managed by the current VIQ, the **Upstream System Name** value appears as a link that opens the D360 page for the switch.



Upstream System Name V1x-440
Upstream System ID 0004:96b4:3389(mac address)

Figure 28: Neighboring Devices

Select **Affected Devices** to view a list of devices affected by the anomaly. ExtremeCloud IQ icons indicate whether the affected device is the current access point, or a neighboring access point.

Select **Unaffected Devices** to view a list of devices not affected by the anomaly.

The device lists include the following details when LLDP is enabled:

- **AP Name** (**Host Name** when LLDP is disabled)
- **AP Model** (**Product Type** when LLDP is disabled
- **AP Interface** (**Interface** when LLDP is disabled
- **PSE Port** (**Port** when LLDP is disabled
- **Last Detected Time** (only for affected devices)

If LLDP is not enabled, ExtremeCloud IQ reports the affected building and the floor, the number of devices affected by the anomaly, and the number of devices not affected.

The device lists include the following details when LLDP is enabled:

- **Host Name**
- **Product Type**
- **Interface**
- **Port**
- **Last Detected Time** (only for affected devices)

Related Topics

Top Anomalies by Type Widget on page 28

Port Efficiency

Port efficiency anomalies identify wired and wireless device interfaces that are not making efficient use of the uplink backhaul connection. This inefficiency might occur in the following scenarios:

- An interface might only use half-duplex communication—only 50% of the available throughput capacity.
- An interface might 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, 5000 Mbps, 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.

To display the following graphs, select a site with a **Port Efficiency** anomaly:

- Port Supported Speed and Full/Half Duplex Negotiation

- Number of Changes (Speed or Duplex)

Note

The **Number of Changes** graph appears only for the following anomaly types:

- Wired and wireless duplex mode anomalies
- Wired and wireless data rate inconsistency anomalies
- Anomalies that are a combination of duplex mode or data rate inconsistency and sub-optimal anomalies

Related Topics

Top Anomalies by Type Widget on page 28

Wi-Fi Capacity

Wi-Fi capacity anomalies are 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. Wi-Fi capacity anomaly reports include the follow information:

- Total time a channel was in use.
- Total time 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

Top Anomalies by Type Widget on page 28

Wi-Fi Efficiency

Wi-Fi efficiency anomalies are related to wireless communication between clients and APs. For more information about packet data anomalies, select a location (site) that has a Wi-Fi efficiency anomaly. You can sort the data by location, severity, and most recent occurrence.

Related Topics

Top Anomalies by Type Widget on page 28

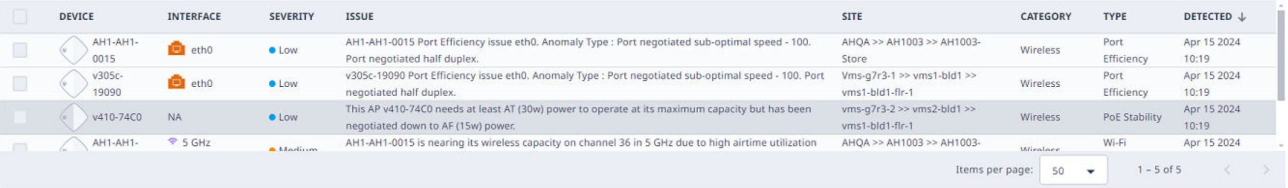
NEW! Anomalies Table

The **Anomalies** table is interactive, and displays the following information for each anomaly:

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

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

- **Last detected**



□	DEVICE	INTERFACE	SEVERITY	ISSUE	SITE	CATEGORY	TYPE	DETECTED ↓
□	AH1-AH1-0015	eth0	● Low	AH1-AH1-0015 Port Efficiency issue eth0. Anomaly Type : Port negotiated sub-optimal speed - 100. Port negotiated half duplex.	AHQA >> AH1003 >> AH1003-Store	Wireless	Port Efficiency	Apr 15 2024 10:19
□	v305c-19090	eth0	● Low	v305c-19090 Port Efficiency issue eth0. Anomaly Type : Port negotiated sub-optimal speed - 100. Port negotiated half duplex.	Vms-g7r3-1 >> vms1-bld1 >> vms1-bld1-flr-1	Wireless	Port Efficiency	Apr 15 2024 10:19
□	v410-74C0	NA	● Low	This AP v410-74C0 needs at least AT (30w) power to operate at its maximum capacity but has been negotiated down to AF (15w) power.	vms-g7r3-2 >> vms2-bld1 >> vms1-bld1-flr-1	Wireless	PoE Stability	Apr 15 2024 10:19
□	AH1-AH1-	5 GHz	● Medium	AH1-AH1-0015 is nearing its wireless capacity on channel 36 in 5 GHz due to high airtime utilization	AHQA >> AH1003 >> AH1003-	Wireless	Wi-Fi	Apr 15 2024

Items per page: 50 ▾ 1 – 5 of 5

Figure 29: Anomalies

You can display the anomalies in ascending or descending order by column, except for the **Interface** and **Issue** columns. 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 and you can mute or dismiss them. Select the corresponding check boxes for these anomalies, and then select **...** > **Mute** or **...** > **Dismiss**.

Related Topics

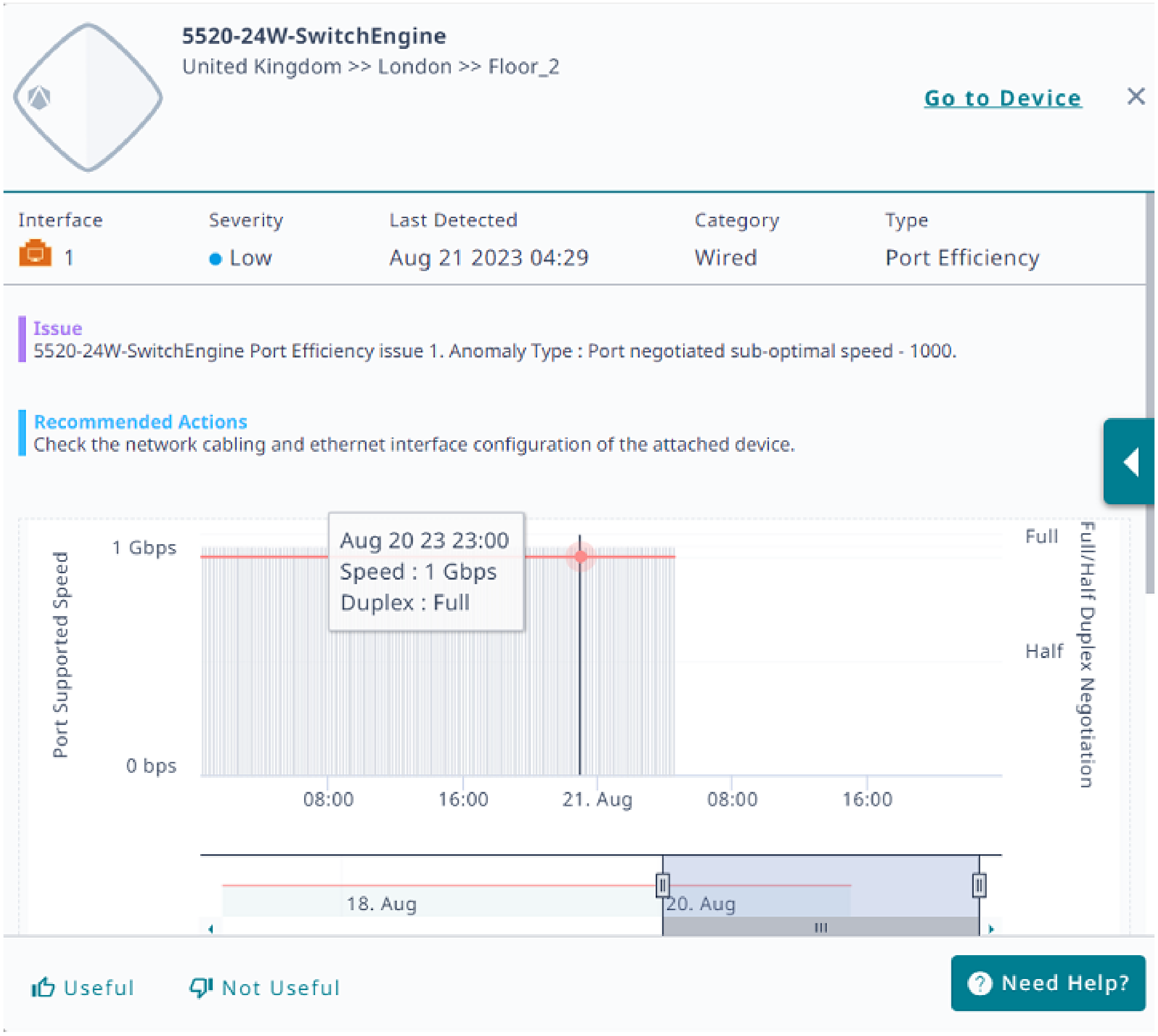
Anomaly Information for a Device on page 34

Anomalies on page 25

NEW! *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**.

The panel graphs display up to 3 days worth of data, including the 48 hours prior to the time stamp for the last detected anomaly.



5520-24W-SwitchEngine

United Kingdom >> London >> Floor_2

Interface	Severity	Last Detected	Category	Type
1	● Low	Aug 21 2023 04:29	Wired	Port Efficiency

Issue

5520-24W-SwitchEngine Port Efficiency issue 1. Anomaly Type : Port negotiated sub-optimal speed - 1000.

Recommended Actions

Check the network cabling and ethernet interface configuration of the attached device.

Figure 30: 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**.

Select a bar to see details; select a bar and drag along the timeline to show data for a range of time.

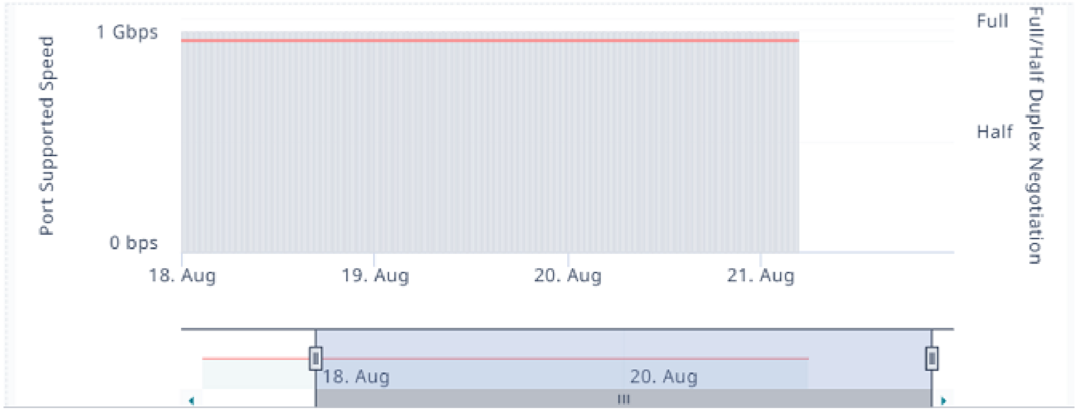


Figure 31: Detailed Information for Specific Days

Related Topics

Anomalies Table on page 33

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

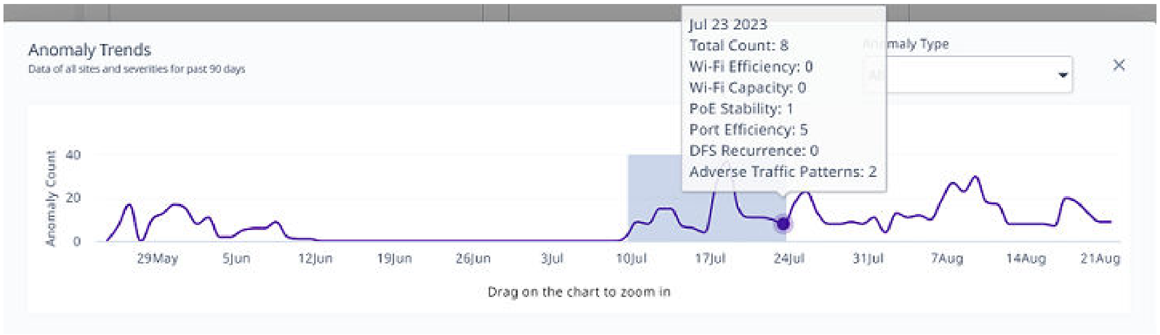
This option is only available for devices covered by an ExtremeWorks maintenance contract.

Anomaly Trends

To open the **Anomaly Trends** graph, go to **CoPilot** > **Anomalies** and select Trends.

Mouse over a bar in the timeline to see the date and types of anomalies identified for that day.

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.



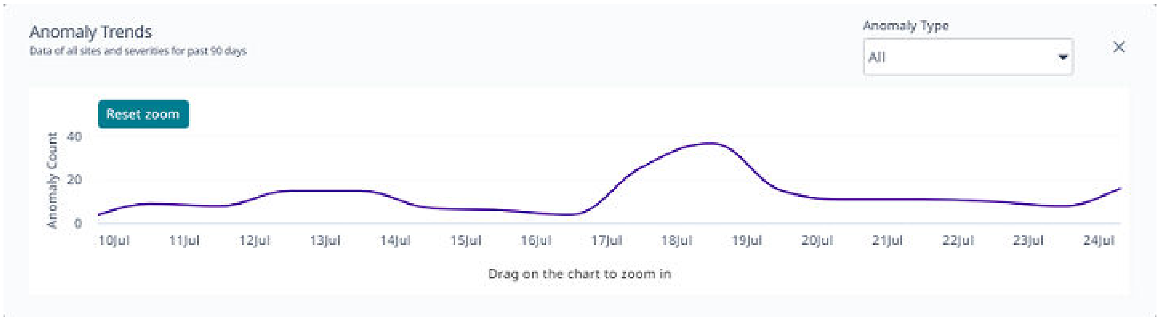
Anomaly Trends

Data of all sites and severities for past 90 days

Jul 23 2023
Total Count: 8
Wi-Fi Efficiency: 0
Wi-Fi Capacity: 0
PoE Stability: 1
Port Efficiency: 5
DFS Recurrence: 0
Adverse Traffic Patterns: 2

Drag on the chart to zoom in

Figure 32: Anomaly Trends graph



Anomaly Trends

Data of all sites and severities for past 90 days

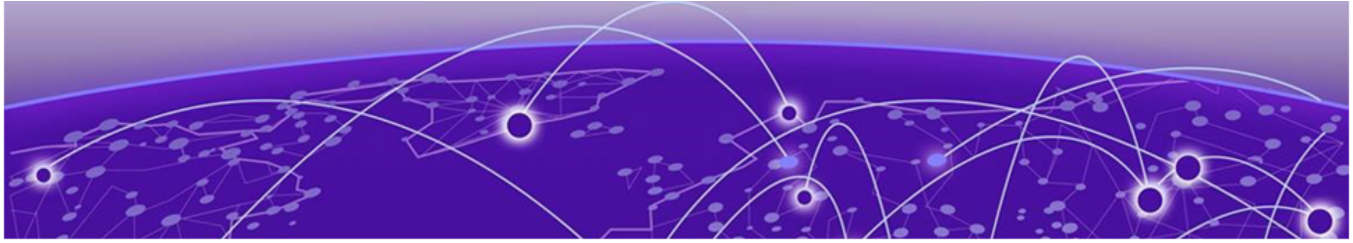
Anomaly Type: All

Drag on the chart to zoom in

Figure 33: Anomaly Trends graph, zoomed in view

Related Topics

Anomalies on page 25



Manage ExtremeCloud IQ CoPilot Licenses

CoPilot Licenses on page 38
CoPilot License Status on page 39
CoPilot Grace Period on page 39
Grace Period Notifications on page 40
CoPilot License Violations on page 40
Activate or Revoke a CoPilot License on page 42
Purchase CoPilot Licenses on page 42

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 applications and 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

Manage ExtremeCloud IQ CoPilot Licenses on page 38

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 might 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 38

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 38

Enable or Disable Proactive Email Notifications

A banner introducing this feature appears once for each administrator, at login:

Email notifications about upcoming license expiration dates can be enabled/disabled here.

Select the link to open the **Global Settings** > **Account Details** page. If you select **X** to close the banner, it does not appear again. Use the following procedure to enable or disable notification emails.

1. Go to **Global Settings** > **Account Details**.
2. To receive notification emails, set the **Proactive license warning email messages** toggles to **ON**.

   If you want to opt out of receiving notification emails, set the toggles to **OFF**.

   There is a toggle for your primary **Email**, and one for your **Alternate Email**. You can set one or both toggles to **ON** or **OFF**.

CoPilot License Violations

If there are fewer 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

This message warns you that your devices have entered the 30 day grace period, after which you can no longer manage them.

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 CoPilot. 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.

The banner appears only on the CoPilot dashboard. After you dismiss the banner, it does not reappear for a week.

While the CoPilot license violation is active, standard CoPilot 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 a CoPilot license violation:

- Contact your Extreme Networks or Extreme Networks Partner Sales Representative to purchase the required number of licenses, or renew expired licenses.
- Change managed CoPilot-eligible devices to unmanaged.
- To update the cached information from the license pool, go to **Global Settings** > **Administration** > **License Management** and select **Synchronize**.

  Alternately, you can unlink from and relink to the Extreme Portal using your Extreme Portal credentials.
- Disable CoPilot functions in **Global Settings** > **Administration** > **VIQ Management** > **Disable CoPilot feature for this device**.

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

Manage ExtremeCloud IQ CoPilot Licenses on page 38

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.

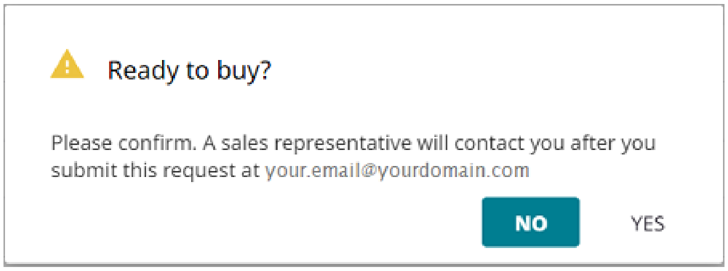
Use this procedure to purchase more licenses.

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

Figure 34: Ready to buy?

A sales representative will contact you to discuss your requirements and to help you place your order.

Table 6: ExtremeCloud IQ CoPilot Part Numbers

Part Number	Description
XIQ-COPILOT-S-C-PWP	One device, one year—PartnerWorks Plus support
XIQ-COPILOT-S-C-EW	One device, one year—ExtremeWorks support

Related Topics

Manage ExtremeCloud IQ CoPilot Licenses on page 38