Engineering
Simplicity

Juniper Mist AI-Native Operations Guide

Published
2025-01-13

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Juniper Mist AI-Native Operations Guide

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

Table of Contents

1

CHAPTER

Get Started with AI Ops

AI Native Operations Overview

SUMMARY

This topic introduces the benefits of the AI Native Operations features in your Juniper Mist™ portal.

IN THIS SECTION

If your job involves troubleshooting problems, investigating user complaints, or tracking network performance, you'll find that all these tasks become easier with the AI-native operations (AIOps) features in your Juniper Mist portal.

AIOps is embedded into Juniper Mist, enabling your IT operations team to stay on top of and manage all the complexity of your distributed networks. Mist AI applies big data, analytics, and machine learning capabilities to intelligently sift through network information to pinpoint events and recognize patterns that indicate potential issues. Mist AI can also diagnose the root cause of an issue and recommend action.

These features shorten the time spent on troubleshooting and empower you to take proactive actions to ensure positive user experiences. No more guessing about the scope of an incident. No more needle-in-a-haystack searches through log files to identify root causes. No more struggling to reproduce issues so that you can capture packets.

What is AIOps?

Video: NOW in 60: What is AIOps?

10-Minute Troubleshooting Video Demo

In this demo, you see how you can use the Monitor page, Marvis actions, and the Marvis query language for troubleshooting.

Video: 10-Minute Troubleshooting

Dashboards

With the Juniper Mist dashboards, you'll see:

- Success/failure indicators that you can interpret at a glance
- Visualizations that show exactly when and where an issue originated
- Packet captures for every incident
- Root-cause analysis

And even better, you can discover many issues before they have an impact. With the Service Level Expectations dashboards, you can quickly spot any conditions that don't meet your expectations. Take action before incidents occur.

Marvis

If you have a Marvis Virtual Network Assistant subscription, you also get:

- AI-recommended actions to improve network performance and user experiences
- Conversational support with issue identification and troubleshooting
- Robust query language for more structured inquiries
- Proactive identification of potential issues

RELATED DOCUMENTATION

All YouTube Videos for Juniper Networks

Explainable AI

SUMMARY

Get familiar with the AI technology behind the Juniper Mist™ features.

IN THIS SECTION

AI Technology and Juniper Mist

Here's a quick introduction to the AI technology that powers Juniper Mist.

Video: Explainable AI Whiteboard Technical Series: Overview

Key concepts:

- Mutual Information
- Decision Tree
- LSTM (Long Short-Term Memory) Networks
- Reinforcement Learning

Natural Language Processing

Natural Language Processing (NLP) is used to help power your human language engagements with Marvis (the AI engine) when asking about network health, troubleshooting, or when taking corrective actions.

Video: Explainable AI Whiteboard Technical Series: Natural Language Processing

Key concepts:

- NLP
- AIOps (AI for IT Operations)
- Tokenization
- Featurization
- Sentence Encoded Vectors
- Embedding Models
- Transfer Learning

Mutual Information and Juniper Mist SLE Metrics

Mutual Information is used to figure out which network features are having the most impact on the failure or success of your SLE (Service Level Expectation) metrics and services.

Video: Explainable AI Whiteboard Technical Series: Mutual Information

Key concepts:

- Mutual Information
- Pearson Correlation
- Entropy

Reinforcement Learning and Juniper Mist Radio Resource Management

Reinforcement Learning is used to intelligently and dynamically optimize RF (Radio Frequency) in real time for the best Wi-Fi coverage, capacity, and connectivity possible. This is a far superior approach to the use of manual settings or traditional fixed algorithms and is totally custom on a per site basis.

Video: Explainable AI Whiteboard Technical Series: Reinforcement Learning

Key concepts:

- Reinforcement Learning

- Value Function
- Future Rewards

Decision Trees and Issue Detection

Decision Trees are used to identify common network issues like faulty cables, access point and switch health, and wireless coverage. This is a form of supervised learning and can be used to isolate faults.

Video: Explainable AI Whiteboard Technical Series: Decision Trees

Key concepts:

- Decision Trees
- Random Forest
- Gradient Boosting
- XGBoost
- Gini Impurity
- Information Gain

RELATED DOCUMENTATION

All AI Technical White Board YouTube Videos

Requirements

SUMMARY

Your access depends on your role in the Juniper Mist™ portal and the subscriptions that you've activated for your organization.

IN THIS SECTION

User Role

The following user roles can access monitoring information in the Juniper Mist portal:

- Super User
- Network Admin
- Observer
- Helpdesk
- Super Observer

NOTE: For information about configuring user roles, see the Juniper Mist Management Guide.

Subscriptions

Your subscriptions determine the features that are available to you in the Juniper Mist portal.

- Base Subscription—With the base subscription, you can:
  - View AI-native insights and easy-to-interpret graphs for site events, client events, AP events, and more.
  - Configure alerts to get notified when events happen in your Juniper Mist organization.
  - With a subscription for Wireless Assurance, Wired Assurance, or WAN Assurance, you can monitor service levels and investigate issues impacting user experiences.
- Marvis Virtual Network Assistant Subscription—With a Marvis Virtual Network Assistant subscription, you can:
  - Chat with your conversational network assistant to ask questions and troubleshoot issues.
  - Submit structured queries using Marvis Query Language.
  - View the Marvis Actions page, which identifies issues, presents a root cause analysis, and recommends actions.
  - Use the Marvis Windows and Android client.
  - Integrate Juniper Mist with apps such as Microsoft Teams, ChatGPT, Zoom, and more.

RELATED DOCUMENTATION

Requirements | 6

AIOps in Action

SUMMARY

To gain a deeper understanding of AI-native operations, watch how an operations engineer, François, troubleshoots user issues. Compare different approaches including the Marvis conversational assistant and the Service Level Expectations (SLE) dashboard. See where to go for technical details, audit logs, and dynamic packet captures.

IN THIS SECTION

Scenario 1: Troubleshooting with Marvis Queries

In this scenario, François uses Marvis queries for help with troubleshooting.

- Often, you can get the information you need with only a basic query.
- Optionally, you can make a few extra clicks to view more details.
- If more questions come to mind while you're troubleshooting, you can refine the query.
- If you want more technical information, you can easily navigate to other Juniper Mist pages to investigate further.

Entering a Basic Query

To get started, François enters a basic query. Marvis provides fact-based, action-oriented answers in plain English. François quickly gets the insights that he needs to address the issue.

Video: Basic Query and Response

Viewing More Details

Continuing this scenario, François clicks the Investigate button to learn more.

Video: Viewing More Details

Refining Your Query

François refines the query to focus on a specific timeframe.

Video: Refining a Query

Investigating Further

Now François is curious to see more technical information. He easily navigates to other Juniper Mist pages to investigate client events, WAN edge performance, audit logs, and more.

Video: Investigating Further

Scenario 2: Troubleshooting with Service Level Expectations (SLEs)

In this scenario, François uses Service Level Expectations (SLEs) to get a quick snapshot of all issues affecting user experience and to explore the root causes of these issues.

- Use the SLE dashboard to see how your organization is performing against various success factors. View the Root Cause Analysis for current issues.
- Go to the Client Events page for deeper insights. Download a dynamic packet capture to learn more.
- Investigate further by viewing the technical details for network devices and by checking the audit logs.

Viewing the SLEs and Root Cause Analysis

François gets started by going to the SLE dashboard and viewing the Root Cause Analysis for current issues.

Video: Introduction to Troubleshooting with SLEs

Getting Deeper Insights

Now François wants to see technical information about client events. Here, he also sees that a dynamic packet capture is available to download.

Video: Viewing Deeper Insights (SLEs)

Using Dynamic Packet Captures

François opens the packet capture in Wireshark and analyzes the data.

Video: Dynamic PCAP

Investigating Further

François views technical details for the DHCP server (the WAN Edge) and explores the audit logs.

Video: Investigating Further (SLEs)

Explore Further

SUMMARY

Explore additional information to understand the full scope of features available to you through the Monitor and Marvis menus in the Juniper Mist™ portal.

- Service Levels—To get started with Service Levels, see:
  - "Insights Overview" on page 12
  - "Service Level Expectations (SLE)" on page 0
- Alerts—To get started with Alerts, see: "Alerts Overview" on page 96
- Marvis—To get started with Marvis, see: "Marvis Virtual Network Assistant Overview" on page 114

2

CHAPTER

Insights

Insights Overview

SUMMARY

Get familiar with the major features of the Insights page.

IN THIS SECTION

The Insights page provides useful information about current conditions. Use this information to correct issues, make changes, and ensure a good network experience for your users.

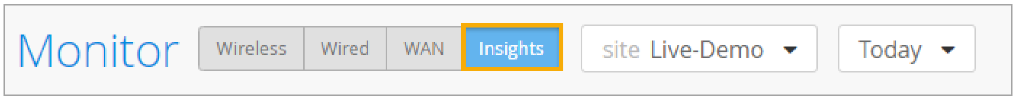
What Data Are Used for Insights?

- Telemetry data from:
  - Juniper wired switches
  - Edge devices supported by Juniper Mist WAN Assurance
  - Juniper Mist Edge device
- Time to connect data from wireless clients
- Coverage, roaming, and throughput data from access points
- Throughput data for network applications.
- Dwell time and other location data from Bluetooth Low Energy (BLE) tags

Use these insights to correct issues, make changes, and ensure a good network experience for your users.

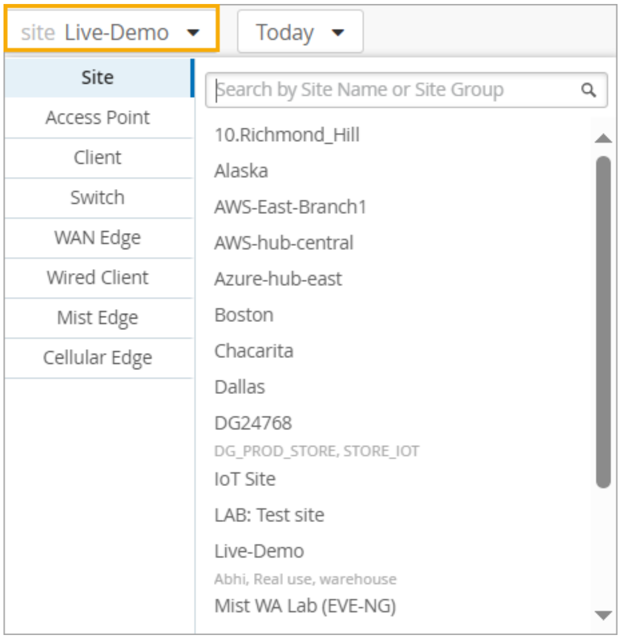
Finding the Insights Page

To view the Insights page, select **Monitor** > **Service Levels** from the left menu. Then click the **Insights** button at the top of the Monitor page.

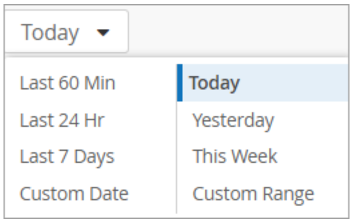


Selecting the Context and Time Period

At the top of the Monitor page, click the **Site** menu to see the context options. Explore the menu to select an entire site, a device, or a client. The Insights page reloads to show the relevant events and information.



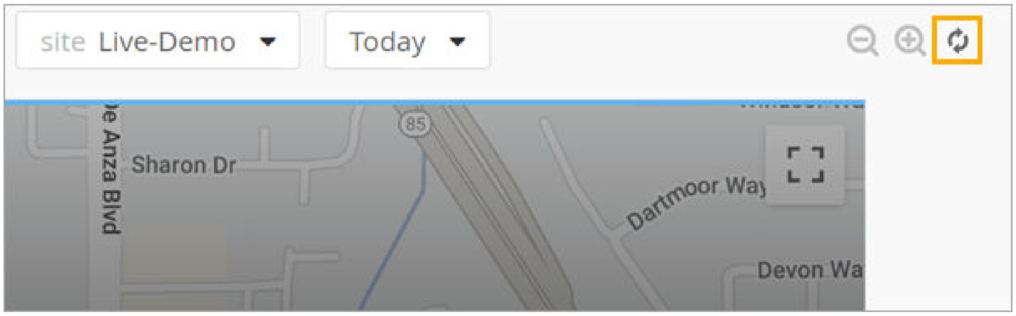
Click the **Today** menu to select a time period, such the last 60 minutes, the last 7 days, or a date range.



NOTE: The Insights page displays data as recent as the past 60 minutes or as far back as the last 7 days. If you purchase a Premium Analytics subscription, you can access up to 3 years' worth of wireless network insights and other data. To access the information available through your Premium Analytics subscription, select **Analytics** > **Premium Analytics** from the left menu.

Refresh Button

To see the latest available data, click the **Refresh** button at the top-right corner of the Insights page.



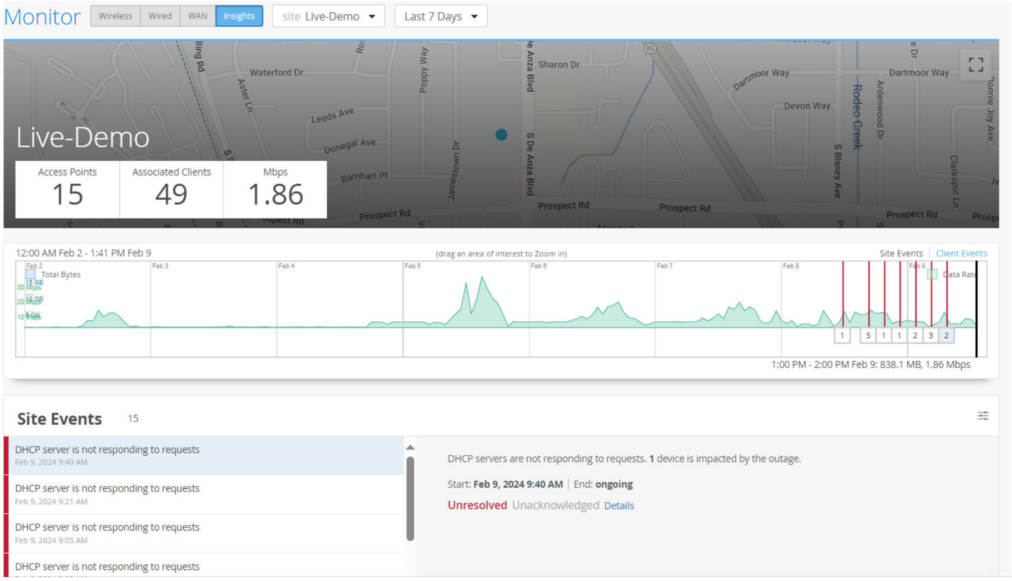
Map Image

The image at the top of the page represents the physical location of the selected site, AP, or client.

- If you selected a site, the map shows the geographic location of the site.
- If you selected a device or client, the map shows its location on the site floorplan.
- If you select a site or device that is not associated with a floorplan, the map area is blank.

Insights Timeline

Directly below the map, the timeline shows the data rate across the selected time period. You can drag your mouse across the graph to select a time period to zoom in on. Other sections of the page refresh to show the data for the zoomed-in area of the timeline.



Access Points	Associated Clients	Mbps
15	49	1.86

12:00 AM Feb 2 - 1:41 PM Feb 9

(drag an area of interest to Zoom in)

1:00 PM - 2:00 PM Feb 9: 838.1 MB, 1.86 Mbps

Site Events 15

DHCP server is not responding to requests
Feb 9, 2024 9:40 AM

DHCP server is not responding to requests
Feb 9, 2024 9:21 AM

DHCP server is not responding to requests
Feb 9, 2024 9:05 AM

DHCP server is not responding to requests

DHCP servers are not responding to requests. **1** device is impacted by the outage.

Start: **Feb 9, 2024 9:40 AM** | End: **ongoing**

Unresolved Unacknowledged Details

NOTE: The timeline selection doesn't affect the Current Values section of the page. This section always shows current data.

Using the Insights Page

For help using the various sections of the Insights page, explore the other topics in this chapter.

Site Insights

SUMMARY

Investigate issues affecting devices, clients, applications, and servers for your site.

IN THIS SECTION

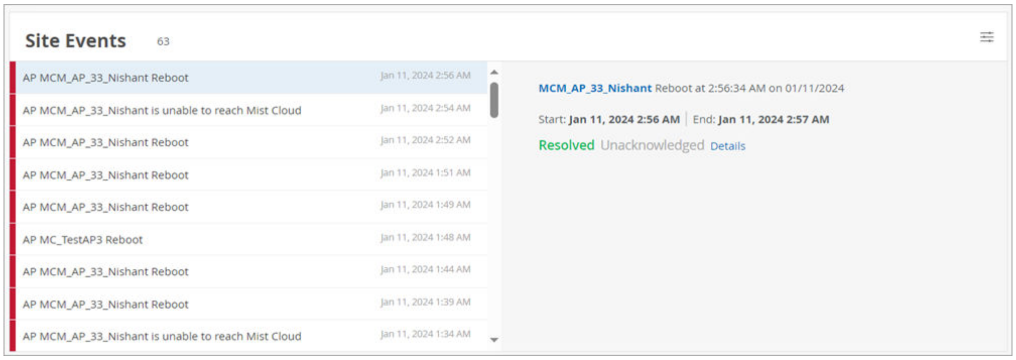
Finding the Site Insights

Go to the "Insights page" on page 12, click the **site** menu at the top of the page, and then select the site that you want to view.

Site Events

Site events appears near the top of the Insights page when you've selected a site or an access point as the context.

Click an event to see a summary on the right side of the page.



Site Events 63

AP MCM_AP_33_Nishant Reboot	Jan 11, 2024 2:56 AM
AP MCM_AP_33_Nishant is unable to reach Mist Cloud	Jan 11, 2024 2:54 AM
AP MCM_AP_33_Nishant Reboot	Jan 11, 2024 2:52 AM
AP MCM_AP_33_Nishant Reboot	Jan 11, 2024 1:51 AM
AP MCM_AP_33_Nishant Reboot	Jan 11, 2024 1:49 AM
AP MC_TestAP3 Reboot	Jan 11, 2024 1:48 AM
AP MCM_AP_33_Nishant Reboot	Jan 11, 2024 1:44 AM
AP MCM_AP_33_Nishant Reboot	Jan 11, 2024 1:39 AM
AP MCM_AP_33_Nishant is unable to reach Mist Cloud	Jan 11, 2024 1:34 AM

MCM_AP_33_Nishant Reboot at 2:56:34 AM on 01/11/2024

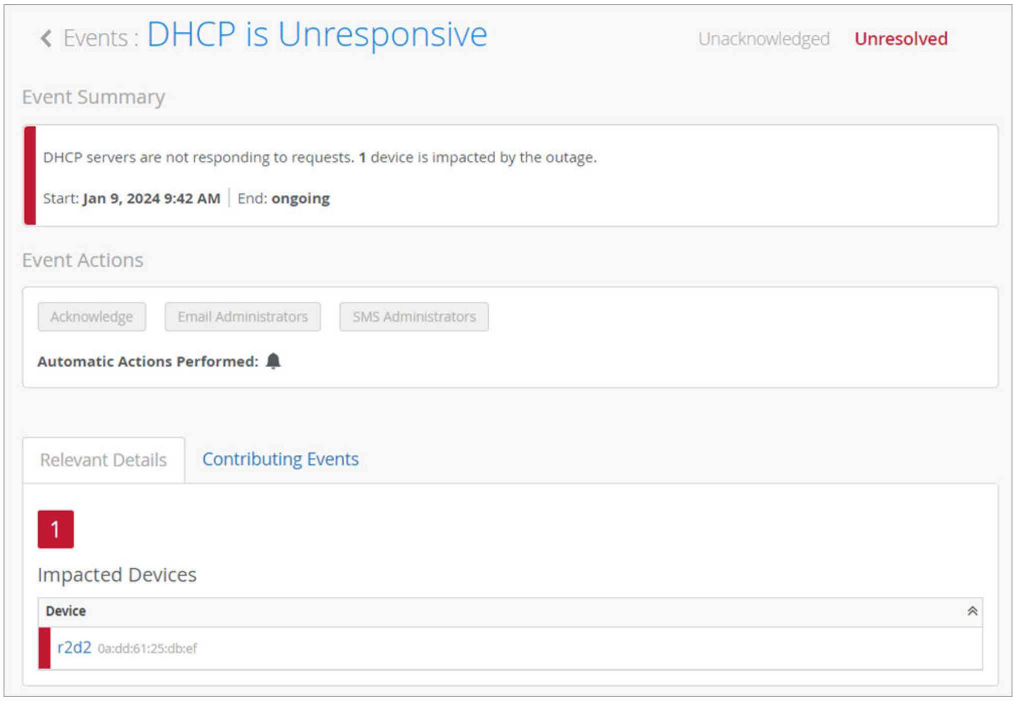
Start: **Jan 11, 2024 2:56 AM** | End: **Jan 11, 2024 2:57 AM**

Resolved Unacknowledged Details

Other options:

- Click the settings button in the top-right corner of the Site Events section to select an event type. For more information, see "Site Event Types" on page 17.
- Device Link—For events involving APs, click the AP name to go to the Access Points page.
- Details Link—Click **Details** to view full event details. The Events page lists the impacted devices and the contributing events. For certain events, an impact map might be available as well.

  Here's an example of the event details page for a DHCP server event.



< Events : DHCP is Unresponsive

Unacknowledged Unresolved

Event Summary

DHCP servers are not responding to requests. **1** device is impacted by the outage.

Start: **Jan 9, 2024 9:42 AM** | End: **ongoing**

Event Actions

Automatic Actions Performed:

Relevant Details | Contributing Events

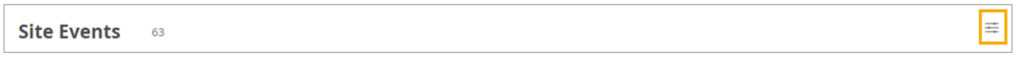
1

Impacted Devices

Device
r2d2 0a:dd:61:25:db:ef

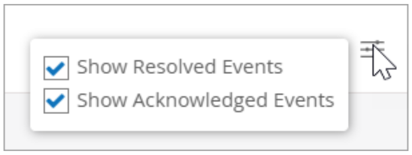
Site Event Types

To select the events to include, click the settings button at the top-right corner of the Site Events section.



Site Events 63

In the Site Filter pop-up window, select or clear the check boxes to show or hide the events based on their status: Resolved or Acknowledged.



☑ Show Resolved Events
☑ Show Acknowledged Events

Related Events and Information for Sites

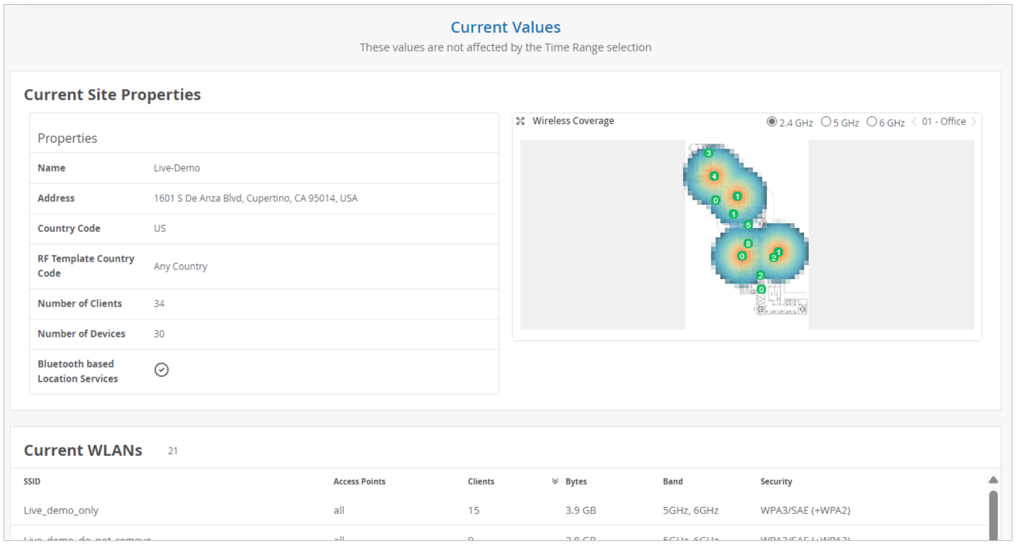
When you select a site at the top of the Insights page, related events and information also appear. For help with these sections of the page, go to these topics:

- "Client Events (Wireless Clients)" on page 22

- "Applications" on page 55
- "Meeting Insights Chart" on page 56
- "Network Servers" on page 59
- "Pre-Connection and Post-Connection Charts" on page 60

Current Values for Sites

The **Current Values** section appears toward the bottom of the Insights page.



Current Values

These values are not affected by the Time Range selection

Current Site Properties

Properties

Name	Live-Demo
Address	1601 S De Anza Blvd, Cupertino, CA 95014, USA
Country Code	US
RF Template Country Code	Any Country
Number of Clients	34
Number of Devices	30
Bluetooth based Location Services	✓

Wireless Coverage

● 2.4 GHz ○ 5 GHz ○ 6 GHz ‹ 01 - Office ›

Current WLANs 21

SSID	Access Points	Clients	Bytes	Band	Security
Live_demo_only	all	15	3.9 GB	5GHz, 6GHz	WPA3/SAE (+WPA2)
Live-demo-do-not-remove	all	9	2.8 GB	5GHz, 6GHz	WPA3/SAE (+WPA2)

NOTE: The values in this section are not impacted by the time range selection at the top of the page.

When a site is selected as the context, this section includes:

- Current Site Properties—Site name, address, number of clients and devices, and status of Bluetooth-based location services. Also provides a visualization of the wireless coverage at the site. Use the buttons above the visualization to select the radio band to view.
- Current WLANs—SSID, number of APs and clients, bytes, bands, and security type.
- Access Points—Status (connected, rebooting, disconnected), MAC address, uptime, number of clients, bytes, LLDP name and port.
  - Use the tabs at the top of this section to show all APs or currently connected APs.

  - Click the name of an AP to reload the Insights page with the data for that AP.
- Clients—MAC address, IP address, device type, protocol, band, RSSI, SSID, SNR, bytes, and connected time. Click a hyperlink to reload the Insights page to show only the data for that client.
  - Use the tabs at the top of this section to show all clients or connected clients.
  - Click the name of a client to reload the Insights page with the data for that client.
- Wired Switches—IP address, number of APs and clients, model, firmware version, and total power draw.

Access Point Insights

SUMMARY

Investigate issues affecting access points (APs).

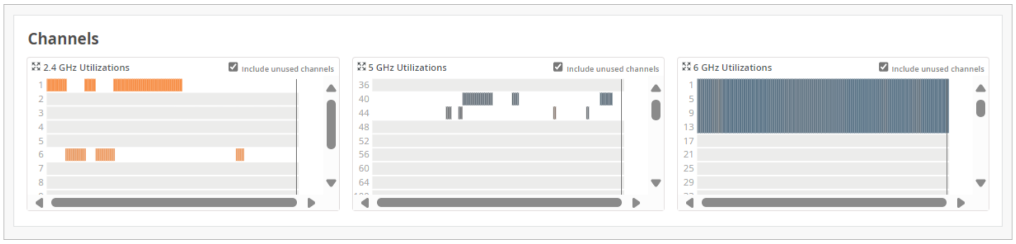
IN THIS SECTION

Finding the AP Insights

Go to the "Insights page" on page 12, click the **site** menu at the top of the page, then click **Access Point** on the left, and then click the AP that you want to view.

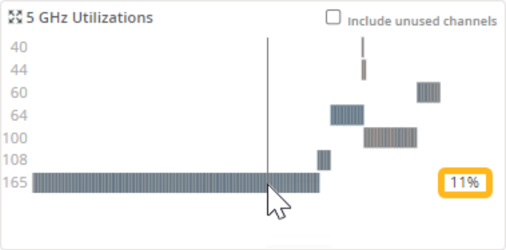
Channels

These charts show channel utilization for all frequency bands (as applicable to the selected AP).



- Use the checkbox above the graph to show or hide the unused channels.

- Hover your mouse pointer over any segment of the chart to show the percent utilized at that point in time. As shown in this example, the percentage appears on the right side of the chart.



Related Events and Information for APs

When you select an AP at the top of the Insights page, related events and information also appear. For help with these sections of the page, go to these topics:

- "Client Events (Wireless Clients)" on page 22

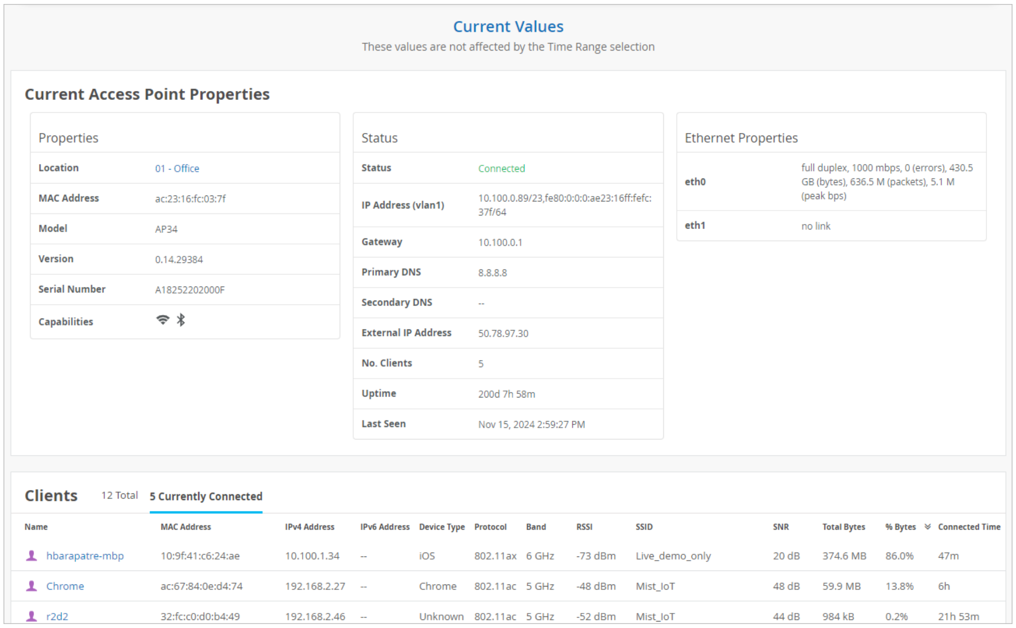
- "Site Events" on page 16

- "Applications" on page 55

- "Post-Connection Charts" on page 61

Current Values for APs

The **Current Values** section appears toward the bottom of the Insights page.



Current Values

These values are not affected by the Time Range selection

Current Access Point Properties

Properties

Location	01 - Office
MAC Address	ac:23:16:fc:03:7f
Model	AP34
Version	0.14.29384
Serial Number	A18252202000F
Capabilities	

Status

Status	Connected
IP Address (vlan1)	10.100.0.89/23,fe80:0:0:0:ae23:16ff:fefc:37f/64
Gateway	10.100.0.1
Primary DNS	8.8.8.8
Secondary DNS	--
External IP Address	50.78.97.30
No. Clients	5
Uptime	200d 7h 58m
Last Seen	Nov 15, 2024 2:59:27 PM

Ethernet Properties

eth0	full duplex, 1000 mbps, 0 (errors), 430.5 GB (bytes), 636.5 M (packets), 5.1 M (peak bps)
eth1	no link

Clients 12 Total 5 Currently Connected

Name	MAC Address	IPv4 Address	IPv6 Address	Device Type	Protocol	Band	RSSI	SSID	SNR	Total Bytes	% Bytes	Connected Time
hbarapatre-mbp	10:9f:41:c6:24:ae	10.100.1.34	--	iOS	802.11ax	6 GHz	-73 dBm	Live_demo_only	20 dB	374.6 MB	86.0%	47m
Chrome	ac:67:84:0e:d4:74	192.168.2.27	--	Chrome	802.11ac	5 GHz	-48 dBm	Mist_IoT	48 dB	59.9 MB	13.8%	6h
r2d2	32:fc:c0:d0:b4:49	192.168.2.46	--	Unknown	802.11ac	5 GHz	-52 dBm	Mist_IoT	44 dB	984 kB	0.2%	21h 53m

NOTE: The values in this section are not impacted by the time range selection at the top of the page.

When an AP is selected as the context, this section includes:

- Current Access Point Properties
  - Properties—Location, MAC address, model, and more
  - Status—Current status (connected, rebooting, disconnected), IP address, gateway, DNS, number of clients, uptime, and more
  - Ethernet Properties—Ethernet details for each port
- Clients—MAC address, IP address, device type, protocol, band, RSSI, SSID, SNR, bytes, and connected time.
  - Use the tabs at the top of this section to show all clients or connected clients.
  - Click the name of a client to reload the Insights page with the data for that client.

Wireless Client Insights

SUMMARY

Investigate issues affecting wireless clients, such as cell phones and laptop computers.

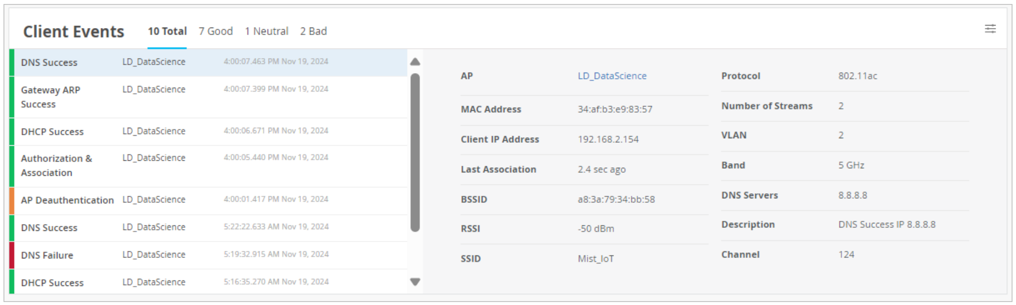
IN THIS SECTION

Finding the Wireless Client Insights

Go to the "Insights page" on page 12, click the **site** menu at the top of the page, then click **Client** on the left, and then click the client that you want to view.

Client Events

Click an event to see a summary on the right side of the page.



Client Events 10 Total 7 Good 1 Neutral 2 Bad

DNS Success	LD_DataScience	4:00:07.463 PM Nov 19, 2024
Gateway ARP Success	LD_DataScience	4:00:07.399 PM Nov 19, 2024
DHCP Success	LD_DataScience	4:00:06.671 PM Nov 19, 2024
Authorization & Association	LD_DataScience	4:00:05.440 PM Nov 19, 2024
AP Deauthentication	LD_DataScience	4:00:01.417 PM Nov 19, 2024
DNS Success	LD_DataScience	5:22:22.633 AM Nov 19, 2024
DNS Failure	LD_DataScience	5:19:32.915 AM Nov 19, 2024
DHCP Success	LD_DataScience	5:16:35.270 AM Nov 19, 2024

AP	LD_DataScience	Protocol	802.11ac
MAC Address	34:af:b3:e9:83:57	Number of Streams	2
Client IP Address	192.168.2.154	VLAN	2
Last Association	2.4 sec ago	Band	5 GHz
BSSID	a8:3a:79:34:bb:58	DNS Servers	8.8.8.8
RSSI	-50 dBm	Description	DNS Success IP 8.8.8.8
SSID	Mist_IoT	Channel	124

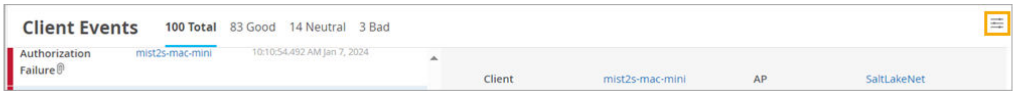
NOTE: Client Events appear on the Insights page when you select a site, AP, or client as the context.

Options:

- Use the tabs at the top of this section to show all, good, neutral, or bad events.
- To select the event types to include, click the settings button at the top-right corner of the Client Events section. For more information, see "Client Event Types" on page 23.
- Links—Click a link to view more information.
- Packet Capture—Juniper APs have a built-in packet buffer. For certain events such as authorization failures, Juniper Mist keeps the buffer information and makes it available as a dynamic packet capture. A paperclip icon appears on the event if a cpature is available. In the summary, click **Download Packet Capture** to save the file. You can then open the file and analyze the details.

Client Event Types

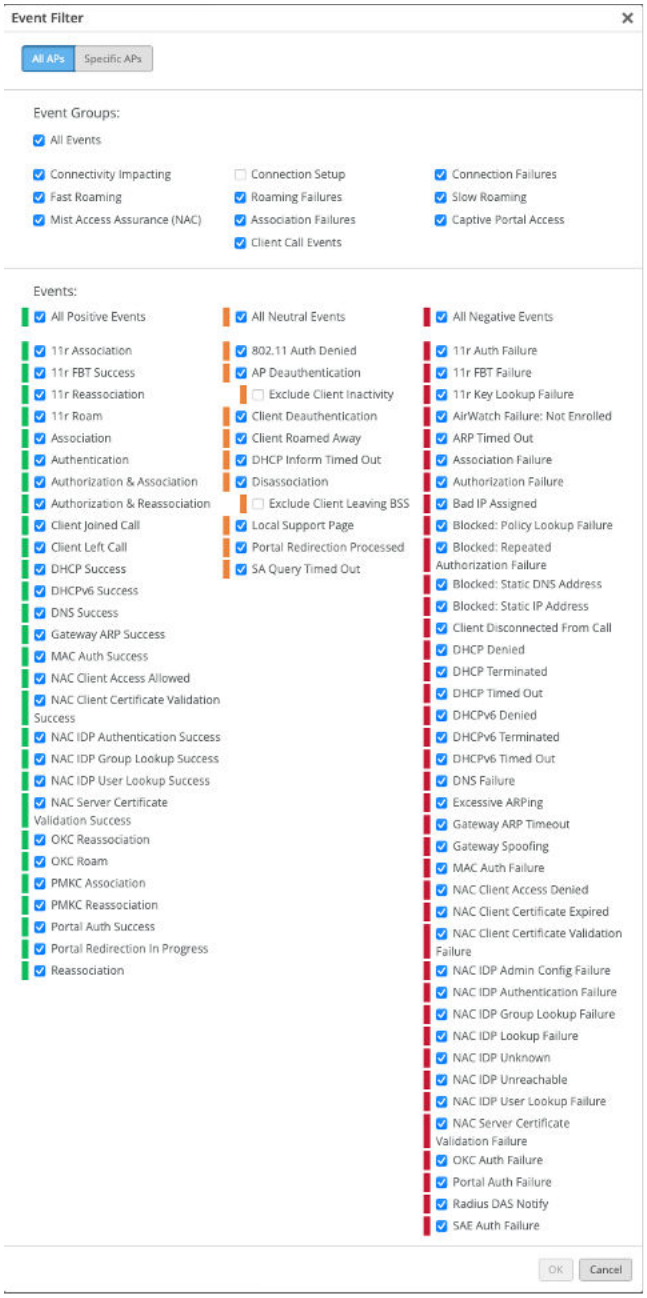
To select the event types to include, click the settings button at the top-right corner of the Client Events section.



Authorization Failure mist2s-mac-mini 10:10:54.492 AM Jan 7, 2024

Client mist2s-mac-mini AP SaltLakeNet

In the Event Filter pop-up window, select or clear the check boxes to show or hide the events. Click **OK** to save your settings.



Event Filter ✕

Event Groups:

☑ All Events

☑ Connectivity Impacting
☑ Fast Roaming
☑ Mist Access Assurance (NAC)

□ Connection Setup
☑ Roaming Failures
☑ Association Failures
☑ Client Call Events

☑ Connection Failures
☑ Slow Roaming
☑ Captive Portal Access

Events:

☑ All Positive Events

☑ 11r Association
☑ 11r FBT Success
☑ 11r Reassociation
☑ 11r Roam
☑ Association
☑ Authentication
☑ Authorization & Association
☑ Authorization & Reassociation
☑ Client Joined Call
☑ Client Left Call
☑ DHCP Success
☑ DHCPv6 Success
☑ DNS Success
☑ Gateway ARP Success
☑ MAC Auth Success
☑ NAC Client Access Allowed
☑ NAC Client Certificate Validation Success
☑ NAC IDP Authentication Success
☑ NAC IDP Group Lookup Success
☑ NAC IDP User Lookup Success
☑ NAC Server Certificate Validation Success
☑ OKC Reassociation
☑ OKC Roam
☑ PMKC Association
☑ PMKC Reassociation
☑ Portal Auth Success
☑ Portal Redirection In Progress
☑ Reassociation

☑ All Neutral Events

☑ 802.11 Auth Denied
☑ AP Deauthentication
  □ Exclude Client Inactivity
☑ Client Deauthentication
☑ Client Roamed Away
☑ DHCP Inform Timed Out
☑ Disassociation
  □ Exclude Client Leaving BSS
☑ Local Support Page
☑ Portal Redirection Processed
☑ SA Query Timed Out

☑ All Negative Events

☑ 11r Auth Failure
☑ 11r FBT Failure
☑ 11r Key Lookup Failure
☑ AirWatch Failure: Not Enrolled
☑ ARP Timed Out
☑ Association Failure
☑ Authorization Failure
☑ Bad IP Assigned
☑ Blocked: Policy Lookup Failure
☑ Blocked: Repeated Authorization Failure
☑ Blocked: Static DNS Address
☑ Blocked: Static IP Address
☑ Client Disconnected From Call
☑ DHCP Denied
☑ DHCP Terminated
☑ DHCP Timed Out
☑ DHCPv6 Denied
☑ DHCPv6 Terminated
☑ DHCPv6 Timed Out
☑ DNS Failure
☑ Excessive ARPing
☑ Gateway ARP Timeout
☑ Gateway Spoofing
☑ MAC Auth Failure
☑ NAC Client Access Denied
☑ NAC Client Certificate Expired
☑ NAC Client Certificate Validation Failure
☑ NAC IDP Admin Config Failure
☑ NAC IDP Authentication Failure
☑ NAC IDP Group Lookup Failure
☑ NAC IDP Lookup Failure
☑ NAC IDP Unknown
☑ NAC IDP Unreachable
☑ NAC IDP User Lookup Failure
☑ NAC Server Certificate Validation Failure
☑ OKC Auth Failure
☑ Portal Auth Failure
☑ Radius DAS Notify
☑ SAE Auth Failure

Table 1: Client Event Types

Positive Client Events	Neutral Client Events	Negative Client Events
11r Association 11r FBT Success 11r Reassociation 11r Roam Association Authentication Authorization & Association Authorization & Reassociation Client Joined Call Client Left Call DHCP Success DHCPv6 Success DNS Success Gateway ARP Success MAC Auth Success NAC Client Access Allowed NAC Client Certificate Validation Success NAC Machine Certificate Validation Success NAC User Certificate Validation Success NAC CoA Disconnect	802.11 Auth Denied AP Deauthentication Exclude Client Inactivity Client Deauthentication Client Roamed Away DHCP Inform Timed Out Disassociation Exclude Client Leaving BSS Local Support Page NAC MDM Device Not Found Portal Redirection Processed SA Query Timed Out	11r Auth Failure 11r FBT Failure 11r Key Lookup Failure AirWatch Failure: Not Enrolled ARP Timed Out Association Failure Authorization Failure Bad IP Assigned Blocked: Policy Lookup Failure Blocked: Repeated Authorization Failure Blocked: Static DNS Address Blocked: Static IP Address Client Disconnected From Call DHCP Denied DHCP Terminated DHCP Timed Out DHCPv6 Denied DHCPv6 Terminated DHCPv6 Timed Out DNS Failure Excessive ARPing

Table 1: Client Event Types *(Continued)*

Positive Client Events	Neutral Client Events	Negative Client Events
• NAC CoA Reauthenticate • NAC IDP Authentication Success • NAC IDP Group Lookup Success • NAC IDP User Lookup Success • NAC MDM Lookup Success • NAC Server Certificate Validation Success • OKC Association • OKC Reassociation • OKC Roam • PMKC Association • PMKC Reassociation • Portal Auth Success • Portal Redirection In Progress • Reassociation		• Gateway ARP Timeout • Gateway Spoofing • MAC Auth Failure • NAC Client Access Denied • NAC Client Cert Revoked • NAC Client Certificate Expired • NAC Client Certificate Validation Failure • NAC Machine Certificate Expired • NAC Machine Certificate Revoked • NAC Machine Certificate Validation Failure • NAC User Certificate Expired • NAC User Certificate Revoked • NAC User Certificate Validation Failure • NAC IDP Admin Config Failure • NAC IDP Admin Config Failure • NAC IDP Authentication Failure • NAC IDP Group Lookup Failure • NAC IDP Lookup Failure • NAC IDP Unknown

Table 1: Client Event Types *(Continued)*

Positive Client Events	Neutral Client Events	Negative Client Events
		- NAC IDP Unreachable - NAC IDP User Disabled - NAC IDP User Lookup Failure - NAC MDM Lookup Failure - NAC Server Certificate Validation Failure - OKC Auth Failure - Portal Auth Failure - Radius DAS Notify - SAE Auth Failure

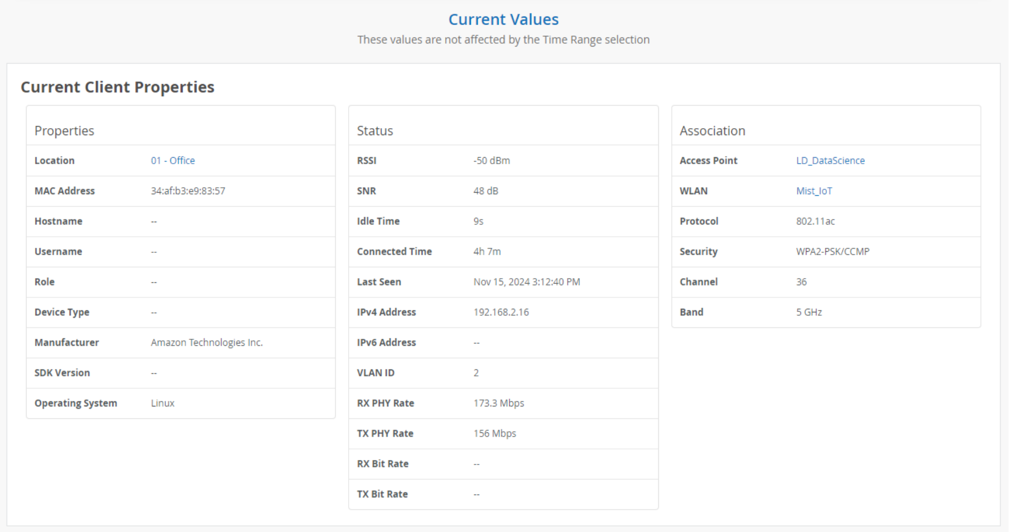
Related Events and Information for Wireless Clients

When you select a wireless client at the top of the Insights page, related events and information also appear. For help with these sections of the page, go to these topics:

- "Applications" on page 55
- "Meeting Insights Charts" on page 56 (including Meeting Details)
- "Pre-Connection and Post-Connection Charts" on page 61

Current Values for Wireless Clients

The **Current Values** section appears toward the bottom of the Insights page.



Current Values

These values are not affected by the Time Range selection

Current Client Properties

Properties	
Location	01 - Office
MAC Address	34:af:b3:e9:83:57
Hostname	--
Username	--
Role	--
Device Type	--
Manufacturer	Amazon Technologies Inc.
SDK Version	--
Operating System	Linux

Status	
RSSI	-50 dBm
SNR	48 dB
Idle Time	9s
Connected Time	4h 7m
Last Seen	Nov 15, 2024 3:12:40 PM
IPv4 Address	192.168.2.16
IPv6 Address	--
VLAN ID	2
RX PHY Rate	173.3 Mbps
TX PHY Rate	156 Mbps
RX Bit Rate	--
TX Bit Rate	--

Association	
Access Point	LD_DataScience
WLAN	Mist_IoT
Protocol	802.11ac
Security	WPA2-PSK/CCMP
Channel	36
Band	5 GHz

NOTE: The values in this section are not impacted by the time range selection at the top of the page.

When a wireless client is selected as the context, this section includes Current Client Properties:

- Properties—Location, MAC address, hostname, manufacturer, OS, and more
- Status—Details such as RSSI, SNR, idle time, connected time, IP address, RX/TX rates, and more
- Association—Names of the associated AP and WLAN, along with protocol, security type, channel, and band.
  - Click the AP hyperlink to go to the AP details page.
  - Click the WLAN hyperlink to go to the WLAN details page.

Switch Insights

SUMMARY

Investigate issues affecting switches.

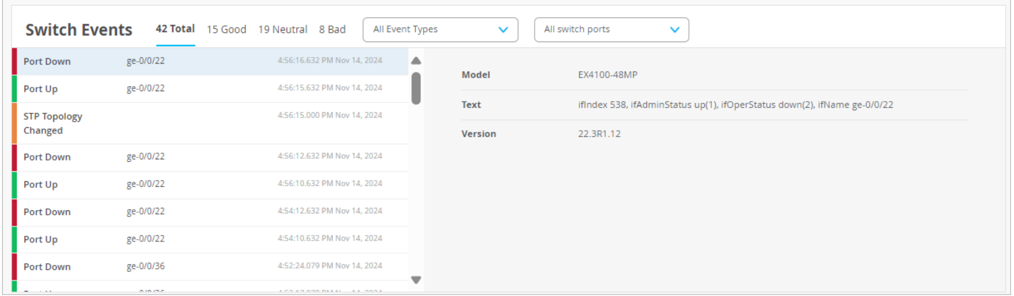
IN THIS SECTION

Finding the Switch Insights

Go to the "Insights page" on page 12, click the **site** menu at the top of the page, then click **Switch** on the left, and then click the switch that you want to view.

Switch Events

In the event list, click an event to see a summary on the right side of the page.



Switch Events

Port Down	ge-0/0/22	4:56:16.632 PM Nov 14, 2024
Port Up	ge-0/0/22	4:56:15.632 PM Nov 14, 2024
STP Topology Changed		4:56:15.000 PM Nov 14, 2024
Port Down	ge-0/0/22	4:56:12.632 PM Nov 14, 2024
Port Up	ge-0/0/22	4:56:10.632 PM Nov 14, 2024
Port Down	ge-0/0/22	4:54:12.632 PM Nov 14, 2024
Port Up	ge-0/0/22	4:54:10.632 PM Nov 14, 2024
Port Down	ge-0/0/36	4:52:24.079 PM Nov 14, 2024

Model	EX4100-48MP
Text	ifIndex 538, ifAdminStatus up(1), ifOperStatus down(2), ifName ge-0/0/22
Version	22.3R1.12

Other options:

- Use the tabs at the top of this section to show all, good, neutral, or bad events.
- Use the Event Types menu to show all events or select an event type. For more information, see "Switch Event Types" on page 29.
- Use the Switch Ports menu to show all ports or select a port.

Switch Event Types

The Event Types options include:

- Alarm Chassis FAN
- Alarm Chassis Hot
- Alarm Chassis Partition
- Alarm Chassis PEM
- Alarm Chassis POE
- Alarm Chassis PSU
- Alarm POE Controller Upgrade Available
- Assigned
- Auth Session Deleted
- BFD Session Disconnected
- BFD Session Established
- BGP Neighbor Down
- BGP Neighbor Up
- Bounce Port
- Chassis Alarm Cleared
- Checksum Complete during ZTP
- Checksum Error while downloading image via ZTP
- Claimed
- Config Changed by User
- Config Failed
- Configuration Applied via ZTP
- Configuration Error in Additional CLI
- Configured
- DDOS Protocol Violation Clear
- DDOS Protocol Violation Set
- Download Images

- Dynamic Port Profile Assigned
- EVPN Core Isolated
- EVPN Core Isolation Cleared
- EVPN Duplicate Mac Detected
- FPC Offline
- FPC Online
- Get Support Files
- Get Support Files by User
- HTTP error while downloading image via ZTP
- Image download via ZTP Complete
- Image installation via ZTP failed
- Image installation via ZTP in progress
- Image Installed
- LACP Rx Stale Stats
- MAC Limit Exceeded
- MAC Limit Reset
- Member on Recovery
- Non DHCP Client Detected
- OSPF Neighbor Adjacency Failed
- OSPF Neighbor Down
- OSPF Neighbor UP
- Overlay BGP Peer State Change
- Port BPDU Blocked
- Port BPDU Error Cleared
- Port Down
- Port Storm Control

- Port Up
- Primary on Recovery
- Radius Server Unresponsive
- Reassigned
- Recovery Snapshot Failed
- Recovery Snapshot Not Needed
- Recovery Snapshot Requested
- Recovery Snapshot Succeeded
- Recovery Snapshot Unsupported
- Restart by User
- Restarted
- Retry Install Images
- Rogue DHCP Server Detected
- Software Connection Failed during ZTP
- Starting to download image via ZTP
- Storage Cleanup During Upgrade
- STP Topology Changed
- Switch Connected
- Switch DHCP Pool Exhausted
- Switch Disconnected
- Switch Port Loop Detected
- Switch Rebooting after Image Installation via ZTP
- Unassigned
- Unclaimed
- Undefined Image Version for this Model
- Updating Images

- Upgrade Failed
- Upgrade Pending
- Upgraded by User
- User Access Denied
- User Authenticated
- User Authenticated on Server Reject VLAN
- User Disconnected Manually
- User Session Deleted
- User Session Disconnected
- User Session Held
- VC Backup Elected
- VC Member Added
- VC Member Deleted
- VC Member Restarted
- VC Primary Changed
- Version Selected to Upgrade does not Support CloudX
- Virtual Chassis Port Down
- Virtual Chassis Port UP
- ZTP Configuration Failed
- ZTP Failed
- ZTP Finished
- ZTP Post Script Success
- ZTP Pre Script Complete
- ZTP Started

Table Capacity

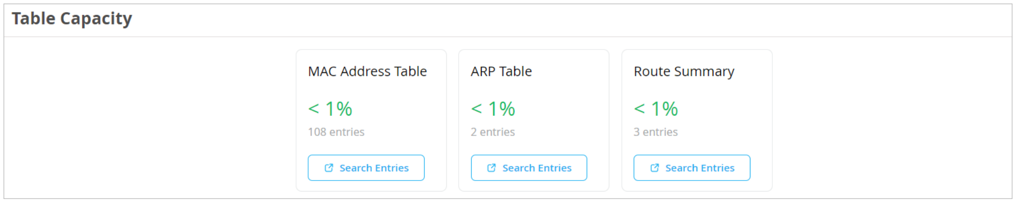


Table Capacity

MAC Address Table
< 1%
108 entries

ARP Table
< 1%
2 entries

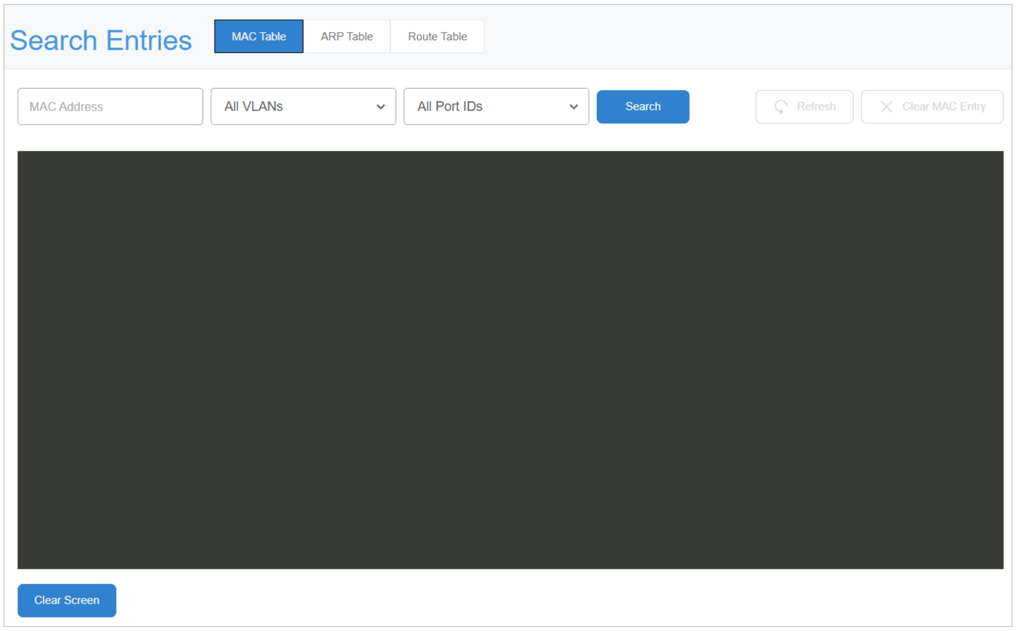
Route Summary
< 1%
3 entries

This section shows the utilization and number of entries for these tables:

- MAC Address Table
- ARP Table
- Route Summary

To explore the entries in a table, click the **Search Entries** button. In the Search Entries window, enter the your search term (MAC address, IP address, or prefix, depending on the selected table). Apply optional filters. Use the tabs at the top to explore other tables.

This example shows the Search Entries window for the MAC table.



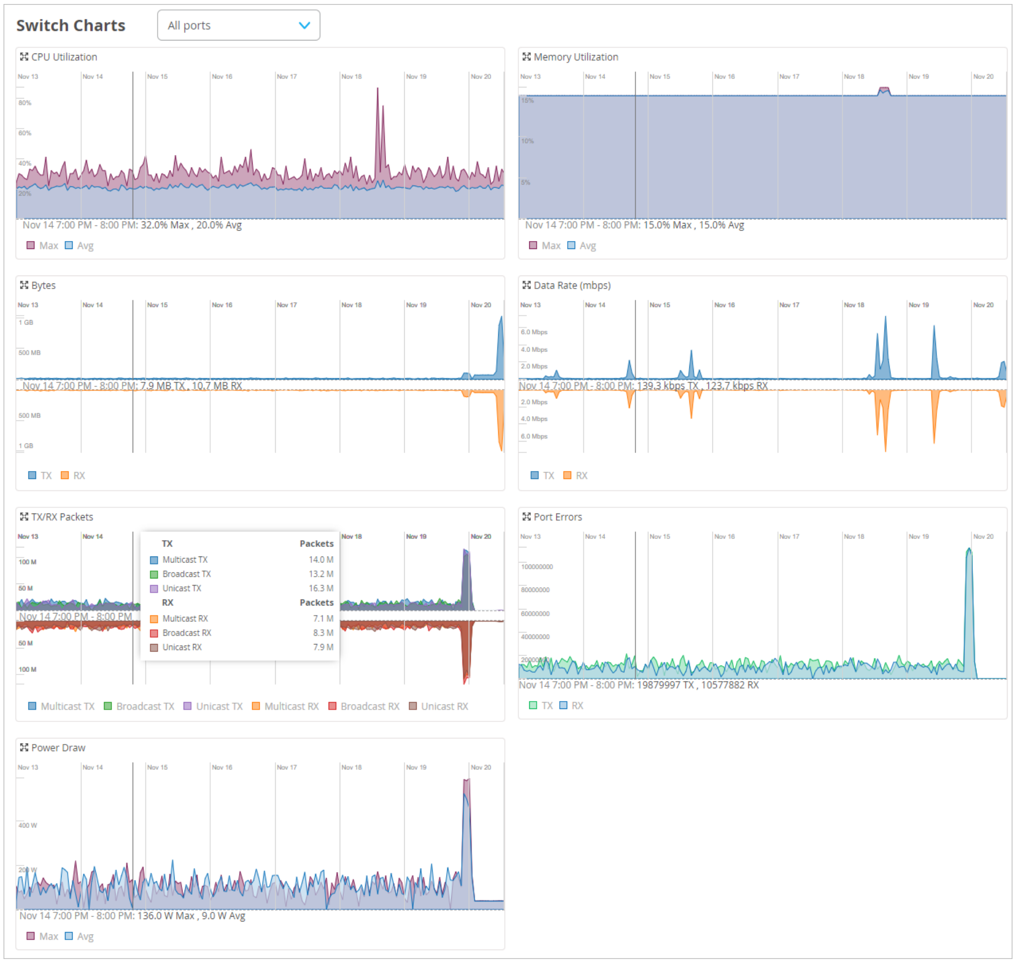
Search Entries

Switch Charts

Explore various charts to gain insights into switch events and health status.

At the top of this section, select All Ports or a specific port.

In each chart, hover your mouse pointer over any data point to see the details.



Nov 14 7:00 PM - 8:00 PM: 32.0% Max , 20.0% Avg

Nov 14 7:00 PM - 8:00 PM: 15.0% Max , 15.0% Avg

Nov 14 7:00 PM - 8:00 PM: 7.9 MB TX , 10.7 MB RX

Nov 14 7:00 PM - 8:00 PM: 139.3 kbps TX , 123.7 kbps RX

Nov 14 7:00 PM - 8:00 PM

TX	Packets
Multicast TX	14.0 M
Broadcast TX	13.2 M
Unicast TX	16.3 M
RX	**Packets**
Multicast RX	7.1 M
Broadcast RX	8.3 M
Unicast RX	7.9 M

Nov 14 7:00 PM - 8:00 PM: 19879997 TX , 10577882 RX

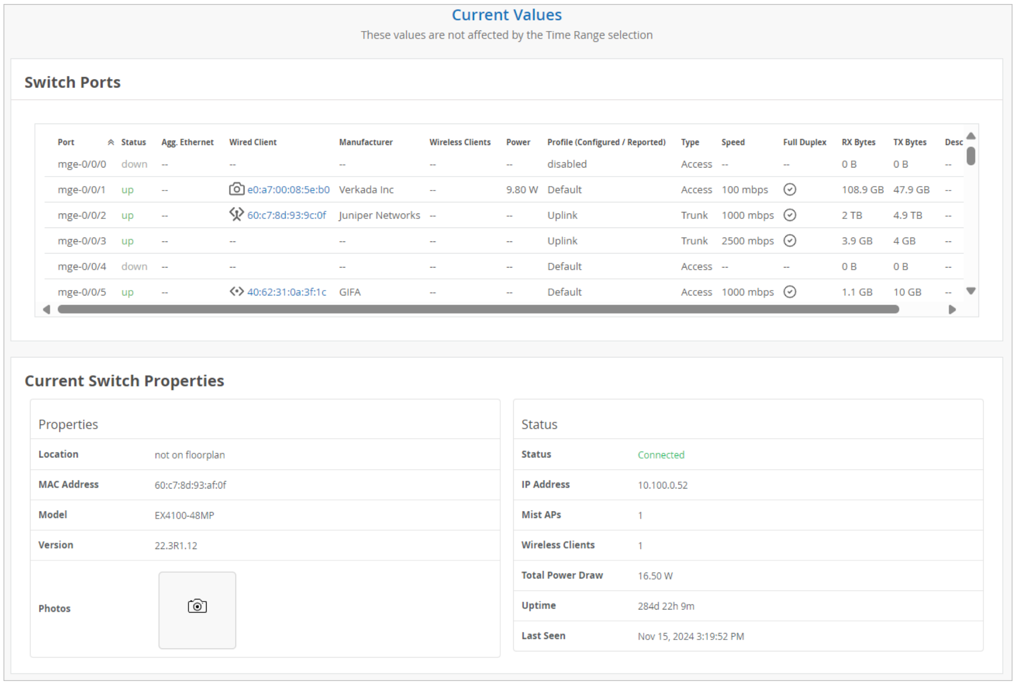
Nov 14 7:00 PM - 8:00 PM: 136.0 W Max , 9.0 W Avg

The charts include:

- CPU Utilization
- Memory Utilization
- Bytes
- Data Rate
- TX/RX Packets
- Port Errors
- Power Draw

Current Values for Switches

The **Current Values** section appears toward the bottom of the Insights page.



Current Values

These values are not affected by the Time Range selection

Switch Ports

Port	Status	Agg. Ethernet	Wired Client	Manufacturer	Wireless Clients	Power	Profile (Configured / Reported)	Type	Speed	Full Duplex	RX Bytes	TX Bytes	Desc
mge-0/0/0	down	--	--	--	--	--	disabled	Access	--	--	0 B	0 B	--
mge-0/0/1	up	--	e0:a7:00:08:5e:b0	Verkada Inc	--	9.80 W	Default	Access	100 mbps	✓	108.9 GB	47.9 GB	--
mge-0/0/2	up	--	60:c7:8d:93:9c:0f	Juniper Networks	--	--	Uplink	Trunk	1000 mbps	✓	2 TB	4.9 TB	--
mge-0/0/3	up	--	--	--	--	--	Uplink	Trunk	2500 mbps	✓	3.9 GB	4 GB	--
mge-0/0/4	down	--	--	--	--	--	Default	Access	--	--	0 B	0 B	--
mge-0/0/5	up	--	40:62:31:0a:3f:1c	GIFA	--	--	Default	Access	1000 mbps	✓	1.1 GB	10 GB	--

Current Switch Properties

Properties

Location	not on floorplan
MAC Address	60:c7:8d:93:af:0f
Model	EX4100-48MP
Version	22.3R1.12
Photos	

Status

Status	Connected
IP Address	10.100.0.52
Mist APs	1
Wireless Clients	1
Total Power Draw	16.50 W
Uptime	284d 22h 9m
Last Seen	Nov 15, 2024 3:19:52 PM

> **NOTE**: The values in this section are not impacted by the time range selection at the top of the page.

When a switch is selected as the context, the Current Values section includes:

- Switch Ports—Details such as status (down or up), manufacturer, client, power, profile, type, speed, and RX/TX bytes. Click a client name to reload the Insights page showing only the data for that client.
- Current Switch Properties
  - Properties—Location, MAC address, model, and firmware version
  - Status—Current status, IP address, number of APs and clients, power draw, and uptime

WAN Edge Insights

SUMMARY

Investigate issues affecting WAN Edges.

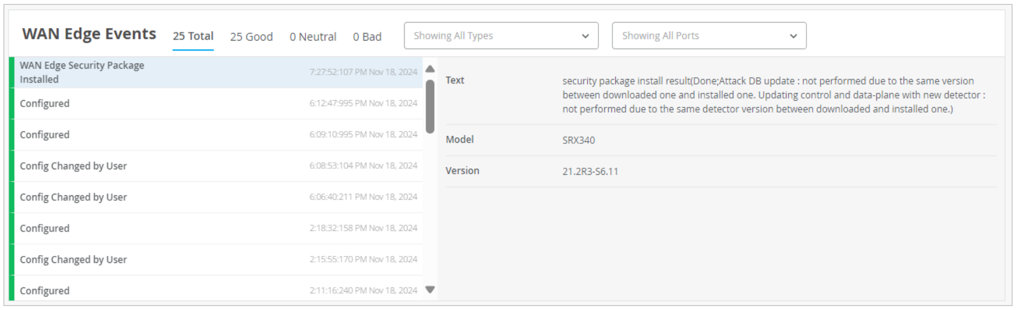
IN THIS SECTION

Finding the Insights for WAN Edges

Go to the "Insights page" on page 12, click the **site** menu at the top of the page, then click **WAN Edge** on the left, and then click the WAN Edge that you want to view.

WAN Edge Events

Click an event to see a summary on the right side of the page.



WAN Edge Security Package Installed	7:27:52:107 PM Nov 18, 2024
Configured	6:12:47:995 PM Nov 18, 2024
Configured	6:09:10:995 PM Nov 18, 2024
Config Changed by User	6:08:53:104 PM Nov 18, 2024
Config Changed by User	6:06:40:211 PM Nov 18, 2024
Configured	2:18:32:158 PM Nov 18, 2024
Config Changed by User	2:15:55:170 PM Nov 18, 2024
Configured	2:11:16:240 PM Nov 18, 2024

Text	security package install result(Done;Attack DB update : not performed due to the same version between downloaded one and installed one. Updating control and data-plane with new detector : not performed due to the same detector version between downloaded and installed one.)
Model	SRX340
Version	21.2R3-S6.11

Other options:

- Use the tabs at the top of this section to show all, good, neutral, or bad events.

- Use the Types drop-down menu to show all types or select an event type. For more information, see "WAN Edge Event Types" on page 38.
- Use the Ports drop-down menu to show all ports or select a port.

WAN Edge Event Types

At the top of the WAN Edge Events section, use the Types drop-down menu to show all types or select an event type. The even types include:

- Assigned
- BGP Peer State Changed
- Bounce Port
- Claimed
- Config Changed by Mist
- Config Changed by User
- Config Failed
- Configuration Error in Additional CLI
- Configured
- Get Support Files
- HA control Link Down
- HA Control Link Up
- HA Health Weight Low
- HA Health Weight Recovery
- OSPF Neighbor Down
- OSPF Neighbor Up
- Path Down
- Path Up
- Peer Down

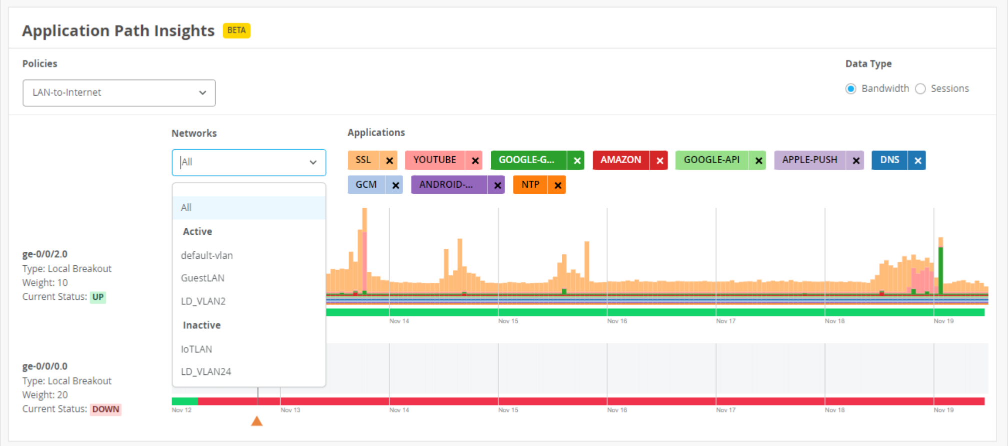
- Peer Up
- Port Down
- Port Up
- Reassigned
- Restarted by User
- RG State Change
- Unassigned
- Unclaimed
- WAN Edge Alarm
- WAN Edge App package Install Failed
- WAN Edge ARP Failure
- WAN Edge ARP Success
- WAN Edge BGP Neighbor Down
- WAN Edge BGP Neighbor Up
- WAN Edge Certificate Regenerated
- WAN Edge Conductor Connected
- WAN Edge Conductor Disconnected
- WAN Edge Config Lock Failed
- WAN Edge Connected
- WAN Edge DHCP Failure
- WAN Edge DHCP Pool Exhausted
- WAN Edge DCHP Success
- WAN Edge Disconnected
- WAN Edge Disconnected Long
- WAN Edge Download Initiated (from Scheduled Operation)
- WAN Edge Download Initiated by User

- WAN Edge Fib Count Returned to Normal
- WAN Edge Fib Count Threshold Exceeded
- WAN Edge Firmware Downloaded
- WAN Edge Flow Count Returned to Normal
- WAN Edge Flow Count Threshold Succeeded
- WAN Edge OSPF Neighbor Adjacency Failed
- WAN Edge PoE Controller Upgrade Available Alarm
- WAN Edge Port Redundancy Group State Changed
- WAN Edge Process Sart
- WAN Edge Rebooting for Upgrade
- WAN Edge Recovery Snapshot Failed
- WAN Edge Recovery Snapshot Not Needed
- WAN Edge Recovery Snapshot Not Supported
- WAN Edge Recovery Snapshot Requested
- WAN Edge Recovery Snapshot Succeeded
- WAN Edge Redundancy Group State Changed
- WAN Edge Restarted
- WAN Edge Security Package Install Failed
- WAN Edge Security Package Installed
- WAN Edge Source NAT Pool Threshold Succeeded
- WAN Edge SSH Reject Error
- WAN Edge Support Files Upload Failed
- WAN Edge Support Files Uploaded Successfully
- WAN Edge Tunnel Auto Provision Failed
- WAN Edge Tunnel Auto Provision Succeeded
- WAN Edge Tunnel Down

- WAN Edge Tunnel Up
- WAN Edge Upgrade by Mist
- WAN Edge Upgrade Complete
- WAN Edge Upgrade Failed
- WAN Edge Upgrade Image Uploaded
- WAN Edge Upgrade Initiated (from Scheduled Operation)
- WAN Edge Upgrade Initiated by User
- WAN Edge Upgrade Pending
- WAN Edge Upgrade Software Add
- WAN Edge Upgrade Software Add Retry
- WAN Edge Upgrade Storage Cleanup
- ZTP Configuration Applied
- ZTP Configuration Failed
- ZTP Failed
- ZTP Finished
- ZTP Post Script Success
- ZTP Post Script Complete
- ZTP Started

Application Path Insights (Beta)

NOTE: Application Path Insights are available to beta customers.


Application Path Insights BETA

Policies: LAN-to-Internet

Data Type: ● Bandwidth ○ Sessions

Networks: All

Applications: SSL ✕ YOUTUBE ✕ GOOGLE-G... ✕ AMAZON ✕ GOOGLE-API ✕ APPLE-PUSH ✕ DNS ✕ GCM ✕ ANDROID-... ✕ NTP ✕

ge-0/0/2.0
Type: Local Breakout
Weight: 10
Current Status: UP

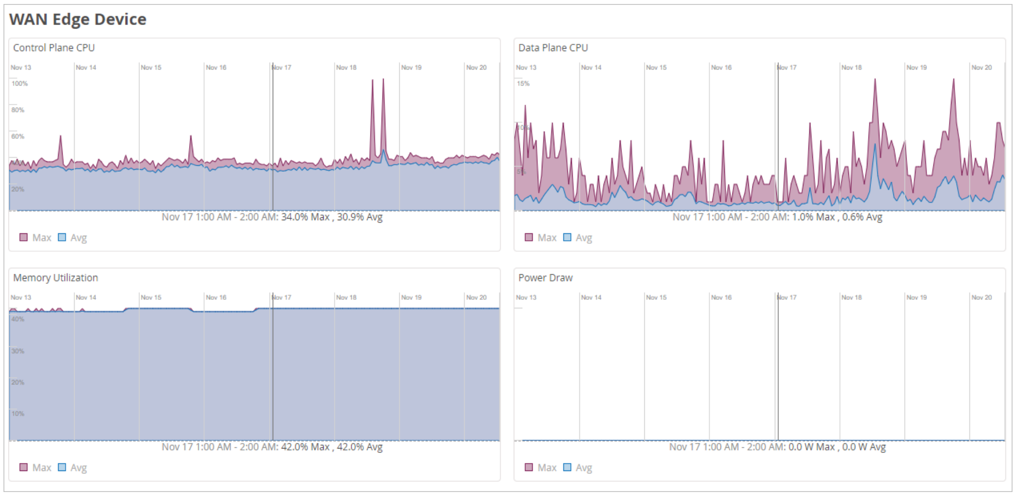
ge-0/0/0.0
Type: Local Breakout
Weight: 20
Current Status: DOWN

You can select the information to show the chart:

- **Policies**—Select the policy to show.
- **Data Type**—Select **Bandwidth** or **Sessions.**
- **Networks**—Select all networks or one network.
- **Applications**—Click **X** to remove an application. Click **+** to add an application. (The **+** button appears only if applications are hidden.)

WAN Edge Device Charts

Explore these charts to gain insights into device status.


WAN Edge Device

Control Plane CPU
Nov 17 1:00 AM - 2:00 AM: 34.0% Max , 30.9% Avg

Data Plane CPU
Nov 17 1:00 AM - 2:00 AM: 1.0% Max , 0.6% Avg

Memory Utilization
Nov 17 1:00 AM - 2:00 AM: 42.0% Max , 42.0% Avg

Power Draw
Nov 17 1:00 AM - 2:00 AM: 0.0 W Max , 0.0 W Avg

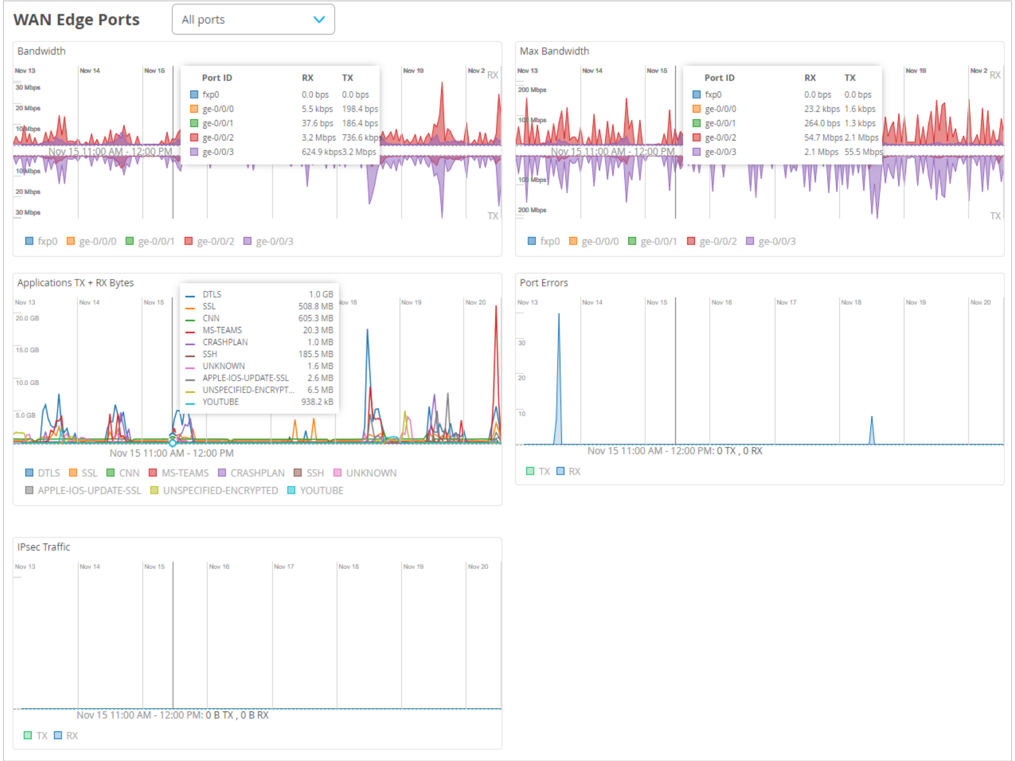
These charts include:

- Control Plane CPU

- Data Plane CPU
- Memory Utilization
- Power Draw

WAN Edge Ports

Explore these charts to gain insights into activity on each port.



WAN Edge Ports

All ports

Bandwidth

Port ID	RX	TX
🟦 fxp0	0.0 bps	0.0 bps
🟧 ge-0/0/0	5.5 kbps	198.4 bps
🟩 ge-0/0/1	37.6 bps	186.4 bps
🟥 ge-0/0/2	3.2 Mbps	736.6 kbps
🟪 ge-0/0/3	624.9 kbps	3.2 Mbps

Max Bandwidth

Port ID	RX	TX
🟦 fxp0	0.0 bps	0.0 bps
🟧 ge-0/0/0	23.2 kbps	1.6 kbps
🟩 ge-0/0/1	264.0 bps	1.3 kbps
🟥 ge-0/0/2	54.7 Mbps	2.1 Mbps
🟪 ge-0/0/3	2.1 Mbps	55.5 Mbps

Applications TX + RX Bytes

DTLS	1.0 GB
SSL	508.8 MB
CNN	605.3 MB
MS-TEAMS	20.3 MB
CRASHPLAN	1.0 MB
SSH	185.5 MB
UNKNOWN	1.6 MB
APPLE-IOS-UPDATE-SSL	2.6 MB
UNSPECIFIED-ENCRYPT...	6.5 MB
YOUTUBE	938.2 kB

Port Errors

Nov 15 11:00 AM - 12:00 PM: 0 TX , 0 RX

IPsec Traffic

Nov 15 11:00 AM - 12:00 PM: 0 B TX , 0 B RX

Nov 13
Nov 14
Nov 15
Nov 16
Nov 17
Nov 18
Nov 19
Nov 20
Nov 2
RX
TX
30 Mbps
20 Mbps
10 Mbps
200 Mbps
100 Mbps
Nov 15 11:00 AM - 12:00 PM
🟦 fxp0 🟧 ge-0/0/0 🟩 ge-0/0/1 🟥 ge-0/0/2 🟪 ge-0/0/3
20.0 GB
15.0 GB
10.0 GB
5.0 GB
🟦 DTLS 🟧 SSL 🟩 CNN 🟥 MS-TEAMS 🟪 CRASHPLAN 🟫 SSH 🟪 UNKNOWN
⬜ APPLE-IOS-UPDATE-SSL 🟨 UNSPECIFIED-ENCRYPTED 🟦 YOUTUBE
30
20
10
🟩 TX 🟦 RX

At the top of this section, select All Ports or a specific port.

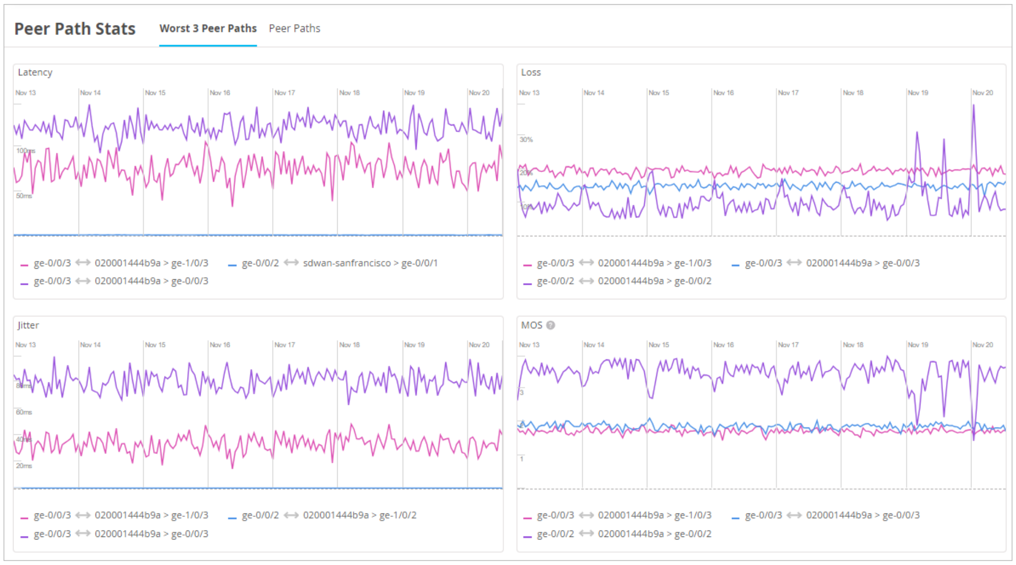
In each chart, hover your mouse pointer over any data point to see the details in a pop-up box.

The charts include:

- Bandwidth
- Max Bandwidth
- Applications TX + RX Bytes
- Port Errors
- IPSec Traffic

Peer Path Stats

Explore latency, loss, jitter, and Mean Opinion Score for all peer paths or the worst three peer paths.


Peer Path Stats
Worst 3 Peer Paths
Peer Paths
Latency
Nov 13
Nov 14
Nov 15
Nov 16
Nov 17
Nov 18
Nov 19
Nov 20
100ms
50ms
ge-0/0/3 ↔ 020001444b9a > ge-1/0/3
ge-0/0/2 ↔ sdwan-sanfrancisco > ge-0/0/1
ge-0/0/3 ↔ 020001444b9a > ge-0/0/3
Loss
30%
20%
10%
ge-0/0/3 ↔ 020001444b9a > ge-1/0/3
ge-0/0/3 ↔ 020001444b9a > ge-0/0/3
ge-0/0/2 ↔ 020001444b9a > ge-0/0/2
Jitter
80ms
60ms
40ms
20ms
ge-0/0/3 ↔ 020001444b9a > ge-1/0/3
ge-0/0/2 ↔ 020001444b9a > ge-1/0/2
ge-0/0/3 ↔ 020001444b9a > ge-0/0/3
MOS
3
1
ge-0/0/3 ↔ 020001444b9a > ge-1/0/3
ge-0/0/3 ↔ 020001444b9a > ge-0/0/3
ge-0/0/2 ↔ 020001444b9a > ge-0/0/2

At the top of this section, use the tabs to show only the worst three paths or all paths.

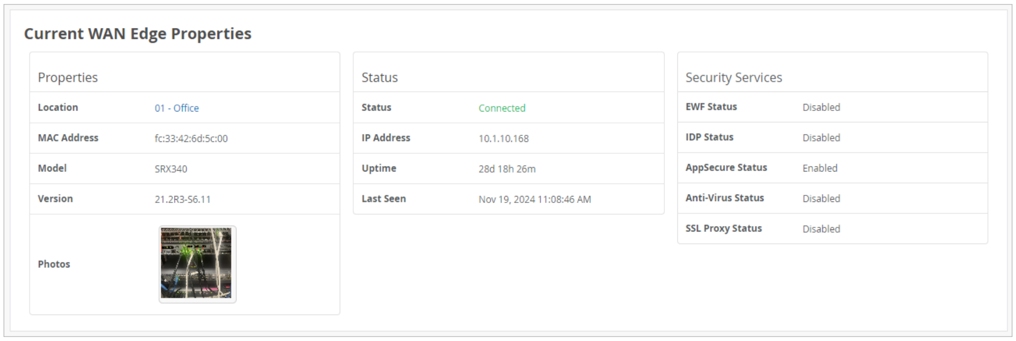
In each chart, hover your mouse pointer over any data point to see the details in a pop-up box.

The charts include:

- Latency
- Loss
- Jitter
- MOS (Mean Opinion Score)

Current Values for WAN Edges

The **Current Values** section appears toward the bottom of the Insights page.



Current WAN Edge Properties

Properties	
Location	01 - Office
MAC Address	fc:33:42:6d:5c:00
Model	SRX340
Version	21.2R3-S6.11
Photos	

Status	
Status	Connected
IP Address	10.1.10.168
Uptime	28d 18h 26m
Last Seen	Nov 19, 2024 11:08:46 AM

Security Services	
EWF Status	Disabled
IDP Status	Disabled
AppSecure Status	Enabled
Anti-Virus Status	Disabled
SSL Proxy Status	Disabled

NOTE: The values in this section are not impacted by the time range selection at the top of the page.

When a WAN Edge is selected as the context, the Current Values section includes the Current WAN Edge Properties:

- Properties—Location, MAC address, model, and firmware version
- Status—Current status, IP address, and uptime
- Security Services enabled or disabled

Wired Client Insights

SUMMARY

Investigate issues affecting wired clients.

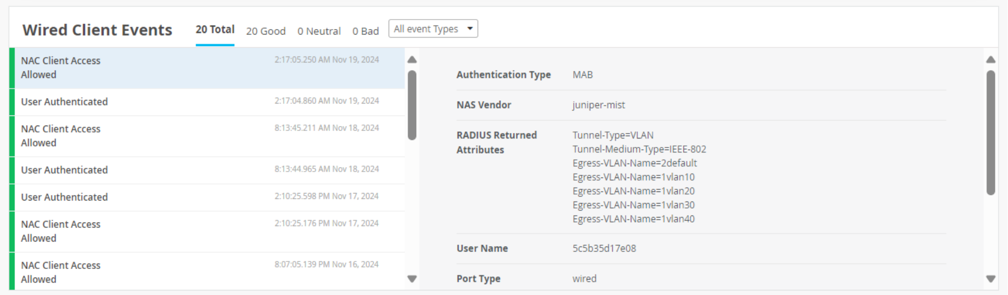
IN THIS SECTION

Finding the Wired Client Insights

Go to the "Insights page" on page 12, click the **site** menu at the top of the page, then click **Wired Client** on the left, and then click the client that you want to view.

Wired Client Events

Click an event to see a summary on the right side of the page, as shown in the following example.



NAC Client Access Allowed	2:17:05.250 AM Nov 19, 2024
User Authenticated	2:17:04.860 AM Nov 19, 2024
NAC Client Access Allowed	8:13:45.211 AM Nov 18, 2024
User Authenticated	8:13:44.965 AM Nov 18, 2024
User Authenticated	2:10:25.598 PM Nov 17, 2024
NAC Client Access Allowed	2:10:25.176 PM Nov 17, 2024
NAC Client Access Allowed	8:07:05.139 PM Nov 16, 2024

Authentication Type	MAB
NAS Vendor	juniper-mist

RADIUS Returned Attributes	Tunnel-Type=VLAN
	Tunnel-Medium-Type=IEEE-802
	Egress-VLAN-Name=2default
	Egress-VLAN-Name=1vlan10
	Egress-VLAN-Name=1vlan20
	Egress-VLAN-Name=1vlan30
	Egress-VLAN-Name=1vlan40

User Name	5c5b35d17e08
Port Type	wired

Other options:

- Use the tabs at the top of this section to show all, good, neutral, or bad events.
- To show only one event type, use the Event Types menu. For more information, see "Wired Client Event Types" on page 46
- For NAC client access events, the summary includes an **Auth Rule** link that you can click to view the relevant authentication policies.

Wired Client Event Types

To select an event type, click the Event Types drop-down menu at the top of the Wired Client Events section.

- Access Guest
- Duplicate IP Address Detected
- NAC Client Access Allowed
- NAC Client Access Denied
- NAC Client Cert Revoked

- NAC Client Certificate Expired
- NAC Client Certificate Validation Failure
- NAC Client Certificate Validation Success
- NAC Client Machine Certificate Expired
- NAC Client Machine Certificate Revoked
- NAC Client Machine Certificate Validation Failure
- NAC Client Machine Certificate Validation Success
- NAC Client User Certificate Expired
- NAC Client User Certificate Revoked
- NAC Client User Certificate Validation Failure
- NAC Client User Certificate Validation Success
- NAC CoA Disconnect
- NAC CoA Reauthenticate
- NAC IDP Admin Config Failure
- NAC IDP Authentication Failure
- NAC IDP Authentication Success
- NAC IDP Group Lookup Failure
- NAC IDP Group Lookup Success
- NAC IDP Lookup Failure
- NAC IDP Unknown
- NAC IDP Unreachable
- NAC IDP User Disabled
- NAC IDP User Lookup Failure
- NAC IDP User Lookup Success
- NAC MDM Device Not Found
- NAC MDM Lookup Failure

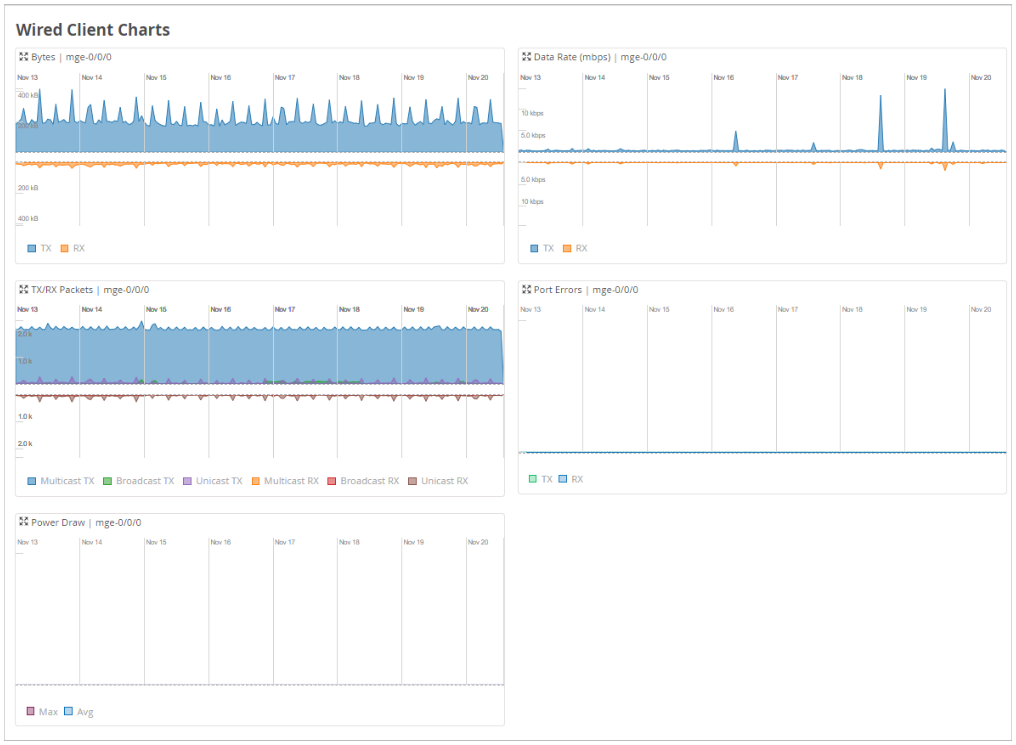
- NAC MDM Lookup Success
- NAC Server Certificate Validation Failure
- NAC Server Certificate Validation Success
- User Access Denied
- User Authenticated
- User Authenticated on Server Reject VLAN
- User Disconnected Manually
- User Session Deleted
- User Session Disconnected
- User Session Held

Related Events and Information for Wired Clients

When you select a wired client at the top of the Insights page, related events and information also appear. For help with these sections of the page, go to these topics:

- "Switch Events" on page 29
- "Meeting Insights" on page 56 (including Meeting Details)

Wired Client Charts

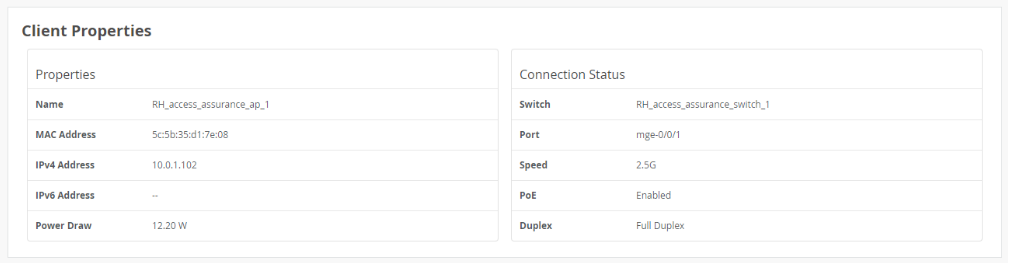


This section includes the following charts:

- Bytes
- Data Rate
- TX/RX Packets
- Port Errors
- Power Draw

Current Values for Wired Clients

The **Current Values** section appears toward the bottom of the Insights page.



Client Properties

Properties	
Name	RH_access_assurance_ap_1
MAC Address	5c:5b:35:d1:7e:08
IPv4 Address	10.0.1.102
IPv6 Address	--
Power Draw	12.20 W

Connection Status	
Switch	RH_access_assurance_switch_1
Port	mge-0/0/1
Speed	2.5G
PoE	Enabled
Duplex	Full Duplex

NOTE: The values in this section are not impacted by the time range selection at the top of the page.

When a wired client is selected as the context, the Current Values section includes only Client Properties.

- Properties—Location, MAC address, IP address, power draw
- Connection Status—Switch, port, speed, PoE enabled or disabled, and duplex

Mist Edge Insights

SUMMARY

Investigate issues affecting Mist Edges.

IN THIS SECTION

Finding the Insights for Mist Edges

Go to the "Insights page" on page 12, click the **site** menu at the top of the page, then click **Mist Edge** on the left, and then click the Mist Edge that you want to view.

Mist Edge Events

Click an event to see a summary on the right side of the page.

Use the tabs at the top of this section to show all, good, neutral, or bad events.

Event Types

Events include:

- AP Auto Preemption skipped
- Mist Edge Config changed by user
- Mist Edge Configured
- Mist Edge Connected
- Mist Edge Disconnected
- Mist Edge Restarted by user
- Mist Edge Restarted
- Mist Edge package update by user
- Mist Edge package installed
- Mist Edge package install failed
- Mist Edge package uninstalled
- Mist Edge package uninstall failed
- Mist Edge package updated
- Mist Edge package update failed
- Mist Edge service started
- Mist Edge service stopped
- Mist Edge service restarted
- Mist Edge service crashed
- Mist Edge service failed

- TunTerm ports bounce requested by user
- TunTerm ports bounced successfully
- TunTerm ports bounce failed
- TunTerm AP disconnect requested by user
- TunTerm AP successfully disconnected
- TunTerm AP failed to disconnect
- Mist Edge memory usage high
- Mist Edge memory usage warning
- Mist Edge memory usage normal
- Mist Edge CPU usage high
- Mist Edge CPU usage warning
- Mist Edge CPU usage normal
- Mist Edge disk usage high
- Mist Edge disk usage warning
- Mist Edge disk usage normal
- Mist Edge fan plugged
- Mist Edge fan unplugged
- Mist Edge PSU plugged
- Mist Edge PSU unplugged
- Mist Edge power input connected
- Mist Edge power input disconnected
- TunTerm (Tunnel Termination) tunnels lost
- TunTerm (Tunnel Termination) tunnel(s) up
- TunTerm (Tunnel Termination) port in blocked state
- TunTerm (Tunnel Termination) port recovered from blocked state
- TunTerm (Tunnel Termination) port link down

- TunTerm (Tunnel Termination) port link restored
- Data port dropped from LACP
- Data port joined LACP
- First Data port joined LACP
- Last Data port dropped from LACP
- All Data ports dropped from LACP
- Inactive vlans reported by data port
- TunTerm monitored resource failed
- TunTerm monitored resource recovered

Port Charts

The charts show TX/DX data for each port.

In each chart, hover your mouse pointer over any data point to see the details.

Current Values for Mist Edges

The **Current Values** section appears toward the bottom of the Insights page. The context at the top of the page determines the information that you'll see here.

NOTE: The values in this section are not impacted by the time range selection at the top of the page.

When a Mist Edge is selected as the context, the Current Values section includes:

- Properties
- Status
- LACP Status
- Port Stats
- LLDP Stats

Cellular Edge Insights

SUMMARY

Investigate issues affecting Cellular Edges.

IN THIS SECTION

Finding the Insights for Cellular Edges

Go to the "Insights page" on page 12, click the **site** menu at the top of the page, then click **Cellular Edge** on the left, and then click the Cellular Edge that you want to view.

Cellular Edge Events

The Cellular Edge Events section provides a list of events.

Use the tabs at the top of this section to show all, good, neutral, or bad events.

Click an event to see a summary on the right side of the page.

Current Values for Cellular Edges

The **Current Values** section appears toward the bottom of the Insights page.

NOTE: The values in this section are not impacted by the time range selection at the top of the page.

When a Cellular Edge is selected as the context, the Current Values section includes:

- Current Cellular Edge Properties—MAC address, model, version, connection status, and uptime
- Interfaces—RX/TX Bytes and related information for all LAN and WAN interfaces

Application Insights

SUMMARY

Investigate issues affecting applications.

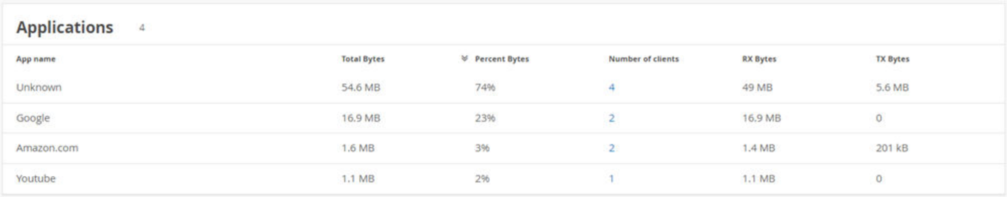
IN THIS SECTION

Finding the Applications Insights

The **Applications** section appears on the "Insights page" on page 12 when a **site, access point, client, or WAN Edge** is selected from the context menu at the top of the page.

Applications

In the Applications list, you'll see the name of each application along with the number of clients and the bytes sent and received.



Applications 4

App name	Total Bytes	Percent Bytes	Number of clients	RX Bytes	TX Bytes
Unknown	54.6 MB	74%	4	49 MB	5.6 MB
Google	16.9 MB	23%	2	16.9 MB	0
Amazon.com	1.6 MB	3%	2	1.4 MB	201 kB
Youtube	1.1 MB	2%	1	1.1 MB	0

To view more information, click the hyperlink in the **Number of Clients** column. In the pop-up window, you'll see the name, MAC address, and other details for each client.

Meeting Insights

SUMMARY

Use the Insights dashboard to view information about Zoom and Microsoft Teams meetings.

IN THIS SECTION

Finding the Meeting Insights

The **Meeting Insights** section appears on the "Insights page" on page 12 when a **site, client, or wired client** from the context menu at the top of the Monitor page.

The **Meeting Details** section appears when a **client or wired client** is selected.

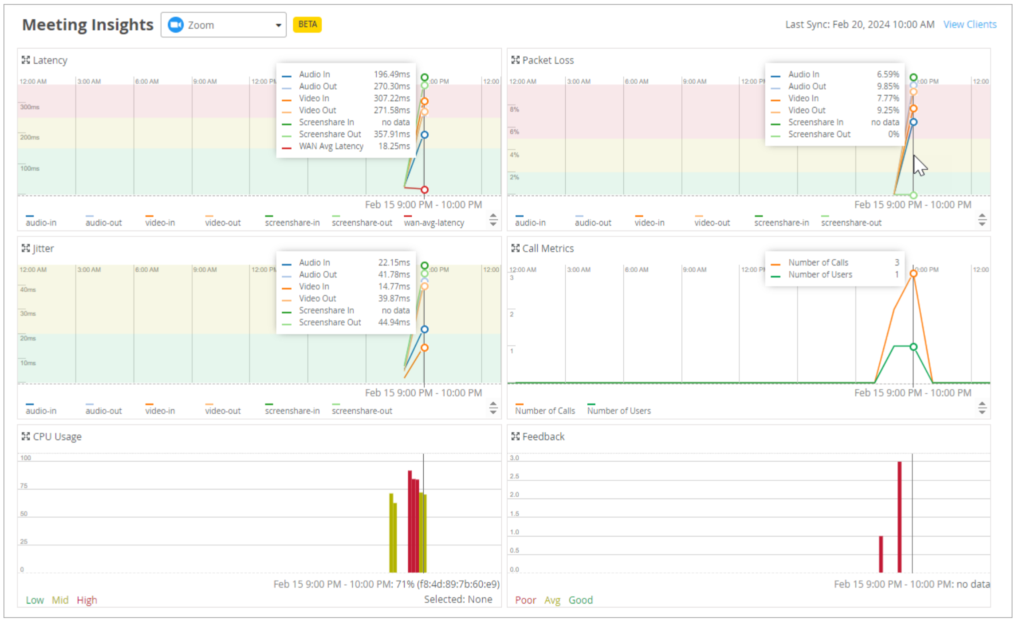
NOTE: This feature is in Beta release.

Meeting Insights Charts

This section shows charts for latency, packet loss, jitter, call metrics, CPU usage, and feedback.

At the top of this section, use the drop-down menu to select the type of meeting to view.

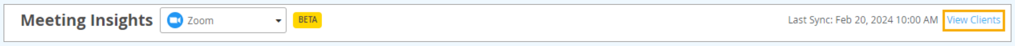
Hover your mouse over a point on a chart to see the details in a pop-up message or in a line of text below the graph (depending on the type of chart). The charts are synchronized so that all of them show the details for the selected point. In the example below, the mouse pointer is hovering over a point on the Packet Loss chart. All charts show details for that same point.



Meeting Details Table

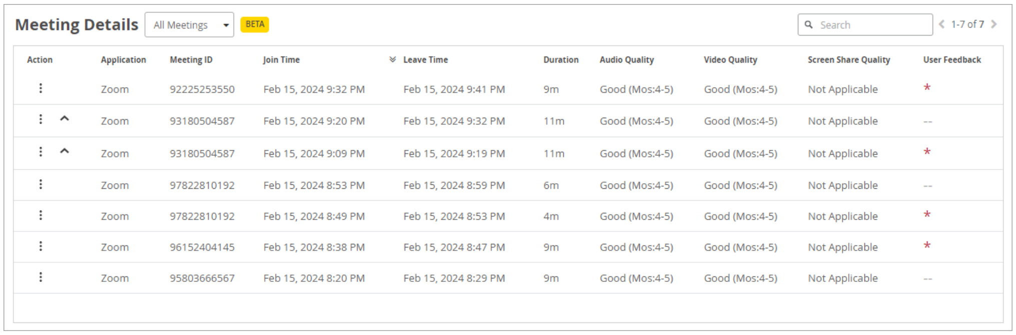
The Meeting Details table appears only when a **wireless or wired client** is selected as the context.

NOTE: If you're viewing Meeting Insights with a site as the context, you can go to the Client Insights page by clicking the **View Clients** link.



After you select a client, the Insights page reloads with that client as the context. You can then scroll down to see the Meeting Insights and Meeting Details for the selected client.

Details include the meeting ID, join and leave time, and quality ratings for audio, video, and screenshare.



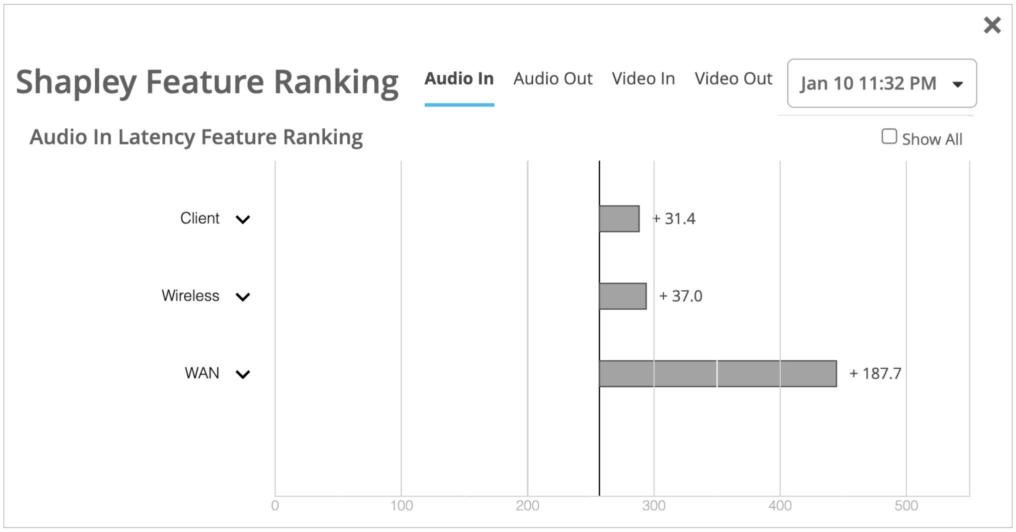
Action	Application	Meeting ID	Join Time	Leave Time	Duration	Audio Quality	Video Quality	Screen Share Quality	User Feedback
⋮	Zoom	92225253550	Feb 15, 2024 9:32 PM	Feb 15, 2024 9:41 PM	9m	Good (Mos:4-5)	Good (Mos:4-5)	Not Applicable	*
⋮ ^	Zoom	93180504587	Feb 15, 2024 9:20 PM	Feb 15, 2024 9:32 PM	11m	Good (Mos:4-5)	Good (Mos:4-5)	Not Applicable	--
⋮ ^	Zoom	93180504587	Feb 15, 2024 9:09 PM	Feb 15, 2024 9:19 PM	11m	Good (Mos:4-5)	Good (Mos:4-5)	Not Applicable	*
⋮	Zoom	97822810192	Feb 15, 2024 8:53 PM	Feb 15, 2024 8:59 PM	6m	Good (Mos:4-5)	Good (Mos:4-5)	Not Applicable	--
⋮	Zoom	97822810192	Feb 15, 2024 8:49 PM	Feb 15, 2024 8:53 PM	4m	Good (Mos:4-5)	Good (Mos:4-5)	Not Applicable	*
⋮	Zoom	96152404145	Feb 15, 2024 8:38 PM	Feb 15, 2024 8:47 PM	9m	Good (Mos:4-5)	Good (Mos:4-5)	Not Applicable	*
⋮	Zoom	95803666567	Feb 15, 2024 8:20 PM	Feb 15, 2024 8:29 PM	9m	Good (Mos:4-5)	Good (Mos:4-5)	Not Applicable	--

In the Actions column, you can:

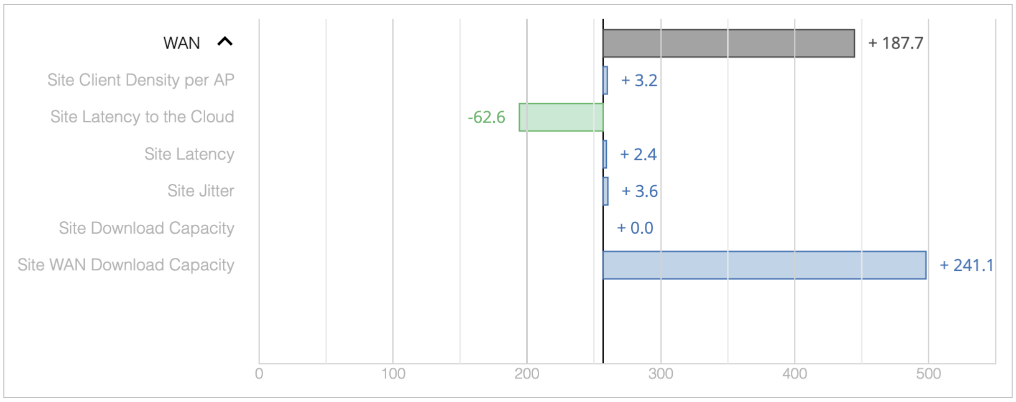
- Troubleshoot—If you have a Marvis subscription, you can click the ellipsis button to get troubleshooting help from the Marvis Conversational Assistant.
- View the Shapley Feature Ranking—A carat ^ icon appears if a user reports a bad experience. Click the ^ icon to view the Shapley Feature Ranking.

Shapley Feature Ranking Example

This example shows how you can use Shapley feature ranking to discover the root causes of poor user experiences. In this example, WAN has the largest latency as compared to Client or Wireless.



You can click the down-arrow to expand the WAN section, as shown below. Now you can see which factors contributed to the high latency for WAN. The Site WAN Download Capacity was the major issue.



Network Server Insights

SUMMARY

Investigate issues affecting RADIUS, DHCP, and DNS servers.

IN THIS SECTION

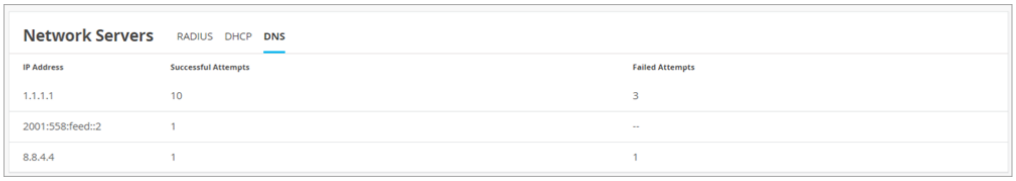
Finding the Network Servers Information

The **Network Servers** section appears toward the middle of the "Insights page" on page 12 when a **site** is selected from the context menu at the top of the page.

Network Servers Table

Use the tabs at the top of the Network Servers section to select the type of server: RADIUS, DHCP, or DNS.

As shown in this example, you'll see a list of servers and the number of successful and failed attempts. Use this information to identify overused servers and servers with a high number of failures. You can then adjust server allocation to improve user experiences.



IP Address	Successful Attempts	Failed Attempts
1.1.1.1	10	3
2001:558:feed::2	1	--
8.8.4.4	1	1

Pre-Connection and Post-Connection Charts

SUMMARY

See pre- and post-connection data to gain insight into network issues.

IN THIS SECTION

Finding the Pre- and Post-Connection Information

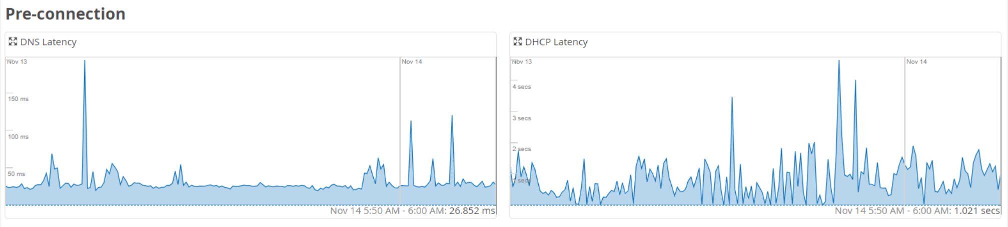
The Pre-Connection and Post-Connection Charts appear on the "Insights page" on page 12 when you select a site or wireless client from the context menu.

Only the Post-Connection Charts appear when you select an access point or a Cellular Edge.

Pre-Connection Charts

The Pre-Connection charts include **DNS Latency** and **DHCP Latency**. These numbers reflect how quickly a wireless client connects to the wireless network.

Hover your mouse over any point on a chart to see the specific data and timestamp below the chart.

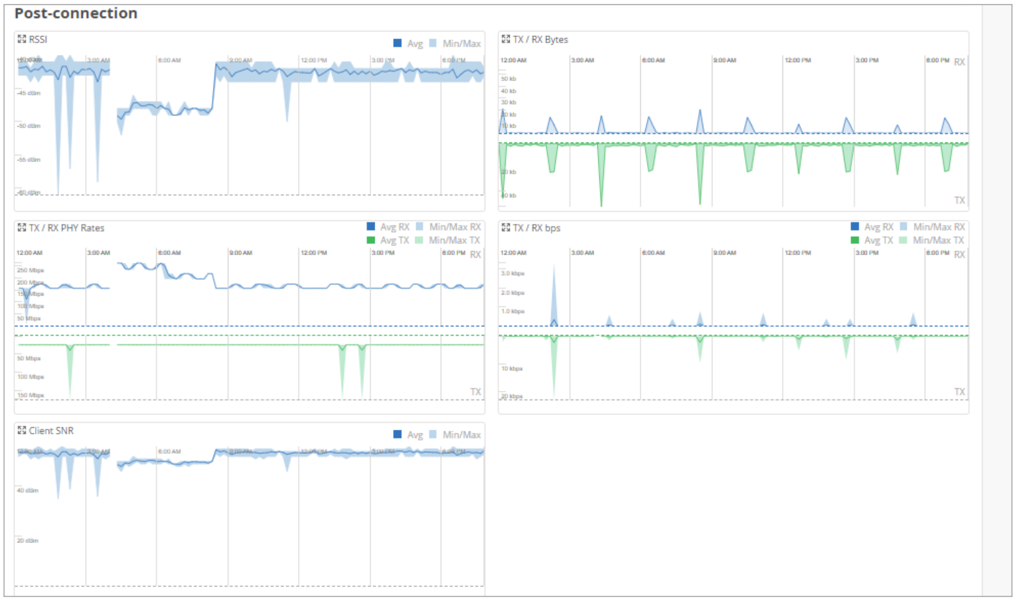


Nov 14 5:50 AM - 6:00 AM: 26.852 ms

Nov 14 5:50 AM - 6:00 AM: 1.021 secs

Post-Connection Charts

The Post-Connection charts display minimum/maximum/average statistics for the connected clients over the selected time period. You can use these charts to gain additional insights about a client.



The standard Post-Connection charts are:

- Associated Clients
- TX/RX Bytes

If your organization has an active Marvis for Wireless subscription, you'll also see these charts:

- RSSI
- TX/RX PHY Rates,
- TX/RX bps
- Client SNR (Signal-to-Noise Ratio)

Current Values

SUMMARY

Get a snapshot of the various elements affecting current user experiences on your network.

IN THIS SECTION

Finding the Current Values on the Insights Dashboard

The **Current Properties** section always appears at the bottom of the "Insights page" on page 12.

Viewing the Current Values

The available information depends on the selected context (site, AP, client, and so on).

NOTE: The values in this section are not impacted by the time range selection at the top of the page.

For more information, go to these topics:

- "Current Values for Sites" on page 18
- "Current Values for Access Points" on page 20
- "Current Values for Wireless Clients" on page 27
- "Current Values for Switches" on page 36
- "Current Values for WAN Edges" on page 44
- "Current Values for Wired Clients" on page 49
- "Current Values for Mist Edges" on page 53
- "Current Values for Cellular Edge" on page 54

3

CHAPTER

Service Level Expectations (SLE)

Wireless SLEs Dashboard

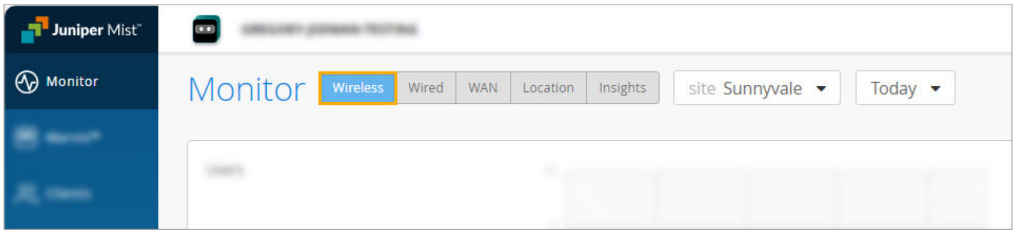
SUMMARY

Get started using the wireless service-level experience (SLE) dashboard to assess the service levels for user-impacting factors such as throughput, signal strength, roaming, and more.

IN THIS SECTION

Finding the Wireless SLEs Dashboard

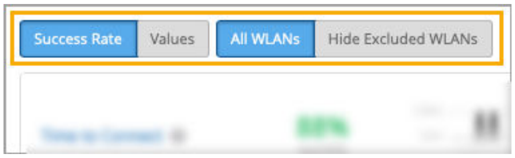
Select **Monitor** > **Service Levels** from the left menu, and then click the **Wireless** button.



NOTE: Your subscriptions determine which buttons appear (for example, you need a Juniper Mist Wi-Fi Assurance subscription for Wireless SLEs).

Additional Filters for the Wireless SLEs

Above the Wireless SLEs, you'll see the usual buttons to show **Success Rate** or **Values**. You'll also see buttons that allow you to show **All WLANs** or **Hide Excluded WLANs**.



Wireless SLEs Video Deep Dive

Watch this 37-minute video to explore Wireless SLEs in depth.

Video: SLE v2

Using the Wireless SLEs Dashboard

For help interpreting the wireless SLEs and classifiers, explore the other Wireless SLE topics in this chapter.

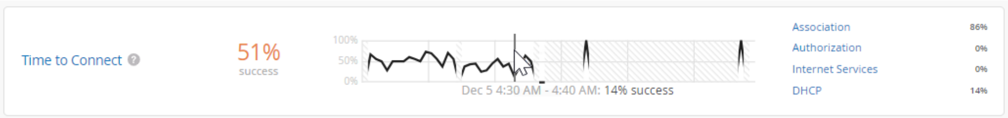
Time to Connect SLE

SUMMARY

Use the Time to Connect SLE to assess your users' experience connecting to the Internet through your wireless network.

IN THIS SECTION

Time to Connect is one of the wireless Service-Level Expectations (SLEs) that you can track on the Wireless SLEs dashboard.


Dec 5 4:30 AM - 4:40 AM: 14% success

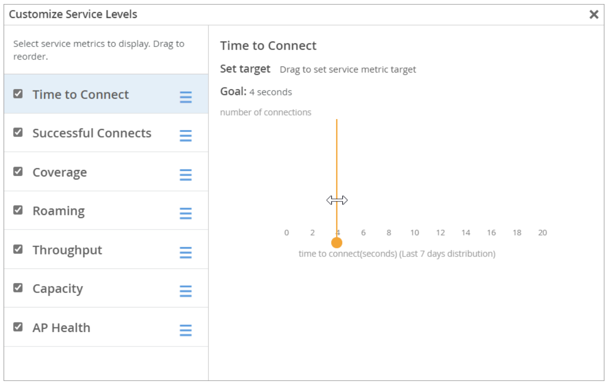
Association	86%
Authorization	0%
Internet Services	0%
DHCP	14%

NOTE: To find the Wireless SLEs dashboard, select **Monitor** > **Service Levels** from the left menu, and then click the **Wireless** button.

What Does the Time to Connect SLE Measure?

Time to Connect is the number of seconds that elapse between the point when a client sends an association packet and the moment when the client can successfully move data.

You can click the **Settings** button (above the SLE blocks) to set the number of seconds to use as the success threshold for this SLE.


Customize Service Levels ✕

Select service metrics to display. Drag to reorder.

- ☑ Time to Connect
- ☑ Successful Connects
- ☑ Coverage
- ☑ Roaming
- ☑ Throughput
- ☑ Capacity
- ☑ AP Health

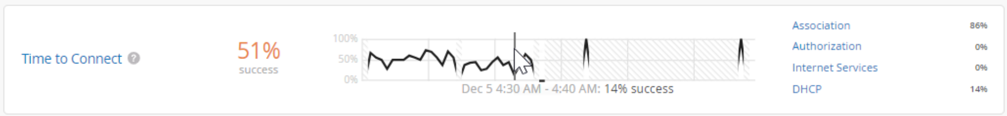
Time to Connect

Set target Drag to set service metric target

Goal: 4 seconds

Classifiers

When the Time to Connect threshold is not met, Juniper Mist sorts the issues into classifiers. The classifiers appear on the right side of the SLE block. In this example, 86 percent of the issues were attributed to Association and 14 percent to DHCP. (See the classifier descriptions below the example.)


Time to Connect

51% success

Dec 5 4:30 AM - 4:40 AM: 14% success

Association	86%
Authorization	0%
Internet Services	0%
DHCP	14%

- **Authorization**—The time to go past the authentication state was more than 2 sigma from the average authentication latency for this site.

- **Association**—The time to go past the association state was more than 2 sigma from the average association latency for this site.

- **Internet Services** —The time to access external networks was more than 2 sigma from the moving average for this site.

- **DHCP**—(DCHP timeouts) The time to connect to Dynamic Host Configuration Protocol (DHCP) was more than 2 sigma from the average time for fully completed successful connections for this site.

Sub-Classifiers for DHCP:

- Stuck
- Nack
- Unresponsive

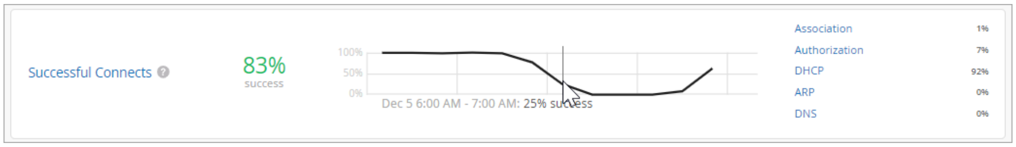
Wireless Successful Connects SLE

SUMMARY

Use the Wireless Successful Connects SLE to assess your users' experiences connecting to your wireless network.

IN THIS SECTION

Successful Connects is one of the wireless Service-Level Expectations (SLEs) that you can track on the Wireless SLEs dashboard.



NOTE: To find the Wireless SLEs dashboard, select **Monitor** > **Service Levels** from the left menu, and then click the **Wireless** button.

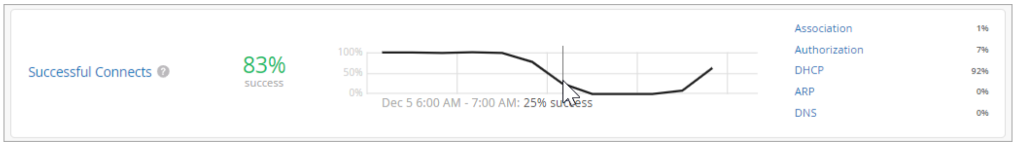
What Does the Wireless Successful Connects SLE Measure?

Juniper Mist tracks the success or failure of authorization, association, DHCP, ARP, and DNS attempts. These connection attempts include initially connecting to the network, roaming from one AP to another, and ongoing connectivity.

You don't need to set up a threshold for this SLE. It's assumed that you want 100 percent successful connects.

Classifiers

When connection attempts fail, Juniper Mist sorts the issues into classifiers. The classifiers appear on the right side of the SLE block. In this example, 92 percent of issues happened during the DHCP process. Another 7 percent failed during authorization, and 1 percent failed during association. No issues (0 percent) were attributed to the other classifiers. (See the classifier descriptions below the example.)



Association	1%
Authorization	7%
DHCP	92%
ARP	0%
DNS	0%

- **Association**—The connection failed during the association process.
- **Authorization**—The connection failed during the authorization process.
- **DHCP**—The connection failed during the DHCP process (DCHP timeouts).

  The DHCP classifier has four sub-classifiers:

  - Renew Unresponsive
  - Nack
  - Incomplete
  - Discover Unresponsive
- **ARP**—The client experienced one of these problems:
  - ARP failure for the default gateway during the initial connection
  - ARP gateway failures after the initial connection or roam
- **DNS**—The client experienced DNS failures during or after the connection process.

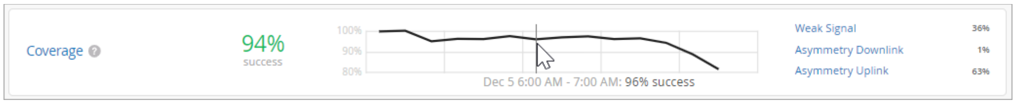
Wireless Coverage SLE

SUMMARY

Use the Wireless Coverage SLE to assess your users' experiences with signal strength.

IN THIS SECTION

Wireless Coverage is one of the Service-Level Expectations (SLEs) that you can track on the Wireless SLEs dashboard.

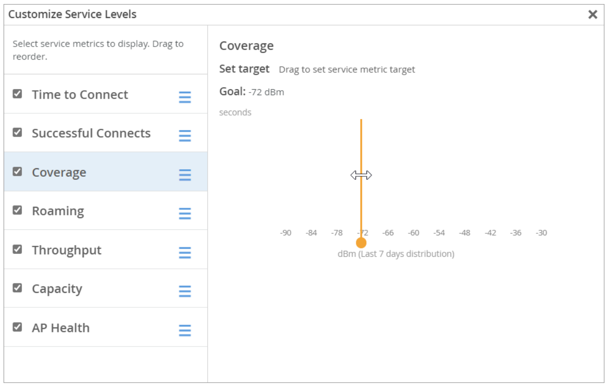


NOTE: To find the Wireless SLEs dashboard, select **Monitor** > **Service Levels** from the left menu, and then click the **Wireless** button.

What Does the Wireless Coverage SLE Measure?

Juniper Mist tracks active clients' Received Signal Strength Indicator (RSSI), as measured by the access point. Use this SLE to determine if you have enough access points.

You can click the **Settings** button to set the RSSI level that you want to use as the success threshold for this SLE.


Customize Service Levels

Select service metrics to display. Drag to reorder.

- ☑ Time to Connect
- ☑ Successful Connects
- ☑ Coverage
- ☑ Roaming
- ☑ Throughput
- ☑ Capacity
- ☑ AP Health

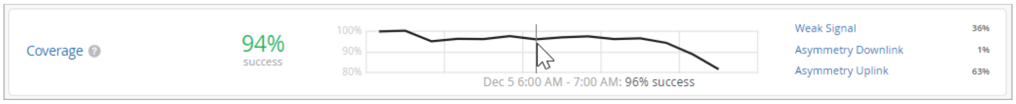
Coverage

Set target Drag to set service metric target

Goal: -72 dBm

Classifiers

When the RSSI threshold is not met, Juniper Mist sorts the issues into classifiers. The classifiers appear on the right side of the SLE block. In this example, 36 percent of issues were attributed to Weak Signal, 1 percent to Asymmetry Downlink, and 63 percent to Asymmetry Uplink. (See the classifier descriptions below the example.)



- **Weak Signal**—Clients received a weak signal due to other factors.
- **Asymmetry Downlink**—Clients received a weak signal due to asymmetric downlink transmission strength between the AP and a client device. (The traffic going from the AP to the client is called downlink traffic.)
- **Asymmetry Uplink**—Clients received a weak signal due to asymmetric uplink strength between the AP and the client device. (Uplink traffic is the traffic going from the client to the AP, and then to the Internet.) Asymmetry can occur for various reasons, such as clients being too far from the AP.

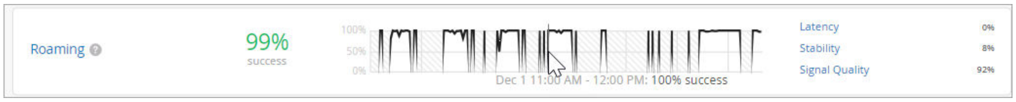
Roaming SLE

SUMMARY

Use the Roaming SLE to track successful and unsuccessful roams between access points.

IN THIS SECTION

Roaming is one of the wireless Service-Level Expectations (SLEs) that you can track on the Monitor page.



NOTE: To find the Wireless SLEs dashboard, select **Monitor** > **Service Levels** from the left menu, and then click the **Wireless** button.

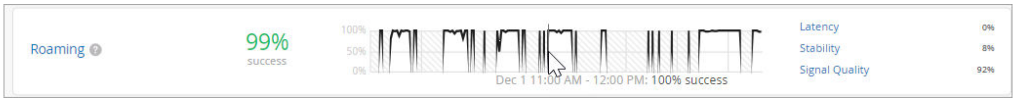
What Does the Roaming SLE Measure?

Juniper Mist tracks the percentage of successful roams between access points and assigns a quality score from 1 to 5. A score of 1 indicates excellent roaming, and a score of 5 indicates poor roaming.

You don't need to set this threshold. It's assumed that you want very good to excellent roaming, so this threshold is automatically set to 2.

Classifiers

When the roaming threshold is not met, Juniper Mist sorts the issues into classifiers. The classifiers appear on the right side of the SLE block. In this example, 8 percent of the issues were attributed to Stability and 92 percent to Signal Quality. (See the classifier descriptions below the example.)



Latency 0%
Stability 8%
Signal Quality 92%

- **Latency**—Roaming time was excessive.

  Latency has different sub-classifiers for different roaming options:

  - **Slow 11r Roams**—This classifier applies to fast roaming as defined by 802.11r. The roaming time exceeded 400 ms.

  - **Slow Standard Roams**—This classifier applies to standard roaming. The roaming time exceeded 2 seconds.

  - **Slow OKC Roams**—This classifier applies to clients using RADIUS-based authentication with Opportunistic Key Caching (OKC). The roaming time exceeded 2 seconds.

- **Stability**—This classifier tracks the consistency of AP choice and 11r usage during client roams. Juniper Mist assigns this classifier if a user capable of fast roaming on a fast- roaming enabled SSID experiences slow roaming for more than 2 seconds. This classifier contains one sub-classifier: **Failed to fast Roam**.

- **Signal Quality**—This classifier tracks the RSSI of clients during a roaming event.

- - **Interband Roam**—This sub-classifier tracks when clients roam between bands.

  - **Suboptimal Roam**—This sub-classifier tracks when clients roam to an AP:

    - With more than 6 dBm decrease in RSSI compared to the client's RSSI in the previous AP

    - If the RSSI in the new connection is worse than the configured coverage SLE threshold. Note that the default coverage SLE threshold is 72 dBm.

- **Sticky Client**—This sub-classifier tracks the events when a client remains connected to an AP even when more roaming options are available to improve the RSSI by more than 6 dBm.

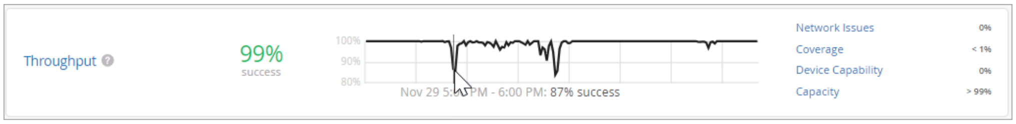
Wireless Throughput SLE

SUMMARY

Use the Throughput SLE to assess users' experiences with throughput on your wireless network.

IN THIS SECTION

Throughput is one of the wireless Service-Level Expectations (SLEs) that you can track on the Wireless SLEs dashboard.

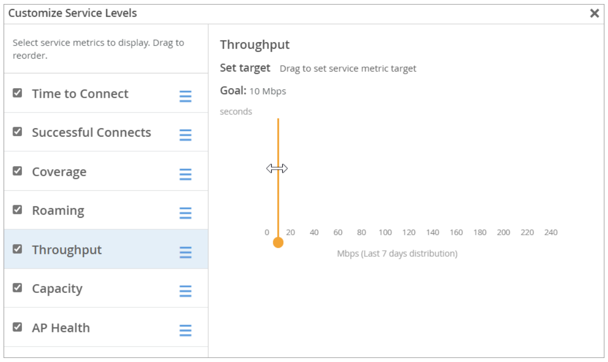


NOTE: To find the Wireless SLEs dashboard, select **Monitor** > **Service Levels** from the left menu, and then click the **Wireless** button.

What Does the Wireless Throughput SLE Measure?

Juniper Mist calculates the estimated throughput on a per-client basis for the entire site. This calculation is done for every client every minute. The estimator considers effects such as AP bandwidth, load, interference events, the type of wireless device, signal strength, and wired bandwidth, to arrive at the probabilistic throughput.

You can click the **Settings** button to set the success threshold for this SLE.



Customize Service Levels ✕

Select service metrics to display. Drag to reorder.

- ☑ Time to Connect
- ☑ Successful Connects
- ☑ Coverage
- ☑ Roaming
- ☑ Throughput
- ☑ Capacity
- ☑ AP Health

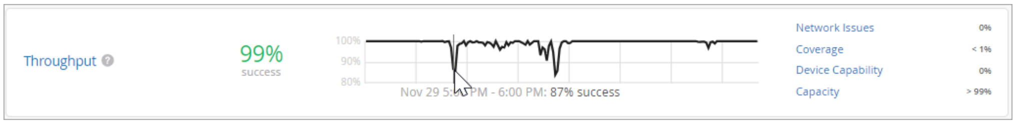
Throughput

Set target Drag to set service metric target

Goal: 10 Mbps

Classifiers

When the throughput threshold is not met, Juniper Mist sorts the issues into classifiers. The classifiers appear on the right side of the SLE block. In this example, less than 1 percent of the issues were attributed to Coverage, and more than 99 percent were due to Capacity. (See the classifier descriptions below the example.)



Throughput 99% success

Network Issues	0%
Coverage	< 1%
Device Capability	0%
Capacity	> 99%

- **Network Issues**—Low throughput is primarily due to the capacity of the wired network.
- **Coverage**—Low throughput is primarily due to the client's weak signal strength.
- **Device Capability**—Low throughput is primarily due to issues with the device capability. For example, throughput issues can occur if a device only supports 20 MHz wide channels, one spatial stream, or a lower version of Wi-Fi (802.11 g/802.11 n).
- **Capacity**—Low throughput is due either to the load on the AP or interference on the channel.

  The capacity classifier has four sub-classifiers:

  - High Bandwidth Utilization
  - Non Wi-Fi Interference
  - Excessive Client Load
  - Wi-Fi Interference

  You can use these sub-classifiers to analyze users and APs below the SLE goal, the timeline of failures and system changes, and the distribution of failures. You can also analyze related network processes that these sub-classifiers can influence.

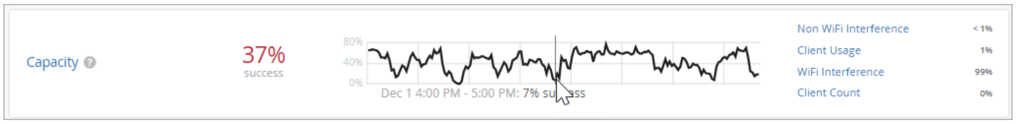
Wireless Capacity SLE

SUMMARY

Use the Wireless Capacity SLE to track user experiences with RF channel capacity (bandwidth) on your wireless network.

IN THIS SECTION

Capacity is one of the wireless Service-Level Expectations (SLEs) that you can track on the Wireless SLEs dashboard. Understand what's measured by this SLE and what issues can contribute to a low SLE.



Dec 1 4:00 PM - 5:00 PM: 7% success

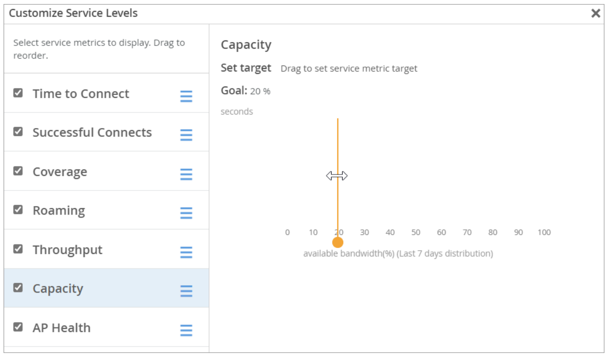
Non WiFi Interference	< 1%
Client Usage	1%
WiFi Interference	99%
Client Count	0%

NOTE: To find the Wireless SLEs dashboard, select **Monitor** > **Service Levels** from the left menu, and then click the **Wireless** button.

What Does the Capacity SLE Measure?

Juniper Mist monitors the percentage of the total RF channel capacity that is available to clients.

You can click the **Settings** button to set the success threshold for this SLE. For example, you might want 20 percent of the RF channel capacity (bandwidth) to be available to clients at any time.



Customize Service Levels

Select service metrics to display. Drag to reorder.

- ☑ Time to Connect
- ☑ Successful Connects
- ☑ Coverage
- ☑ Roaming
- ☑ Throughput
- ☑ Capacity
- ☑ AP Health

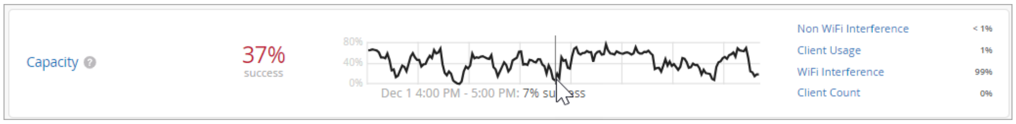
Capacity

Set target Drag to set service metric target

Goal: 20 %

Classifiers

When the capacity threshold is not met, Juniper Mist sorts the issues into classifiers. The classifiers appear on the right side of the SLE block. In this example, 99 percent of issues were attributed to Wi-Fi interference. The remaining issues were due to Non Wi-Fi Interference and Client Usage. (See the classifier descriptions below the example.)



- **Non-Wi-Fi interference**—Low capacity is due to non-wireless interference.
- **Client Usage**—Low capacity is due to a high client load.
- **Wi-Fi interference**—Low capacity is due to wireless interference.
- **Client Count**—Low capacity is due to a high number of attached clients.

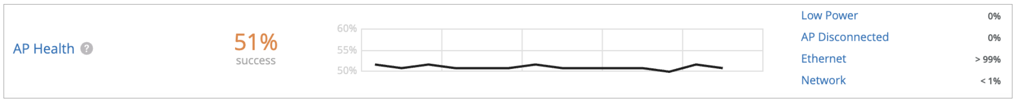
AP Health SLE

SUMMARY

Use the AP Health SLE to assess your users' experience with AP availability.

IN THIS SECTION

AP Health is one of the wireless Service-Level Expectations (SLEs) that you can track on the Wireless SLEs dashboard.



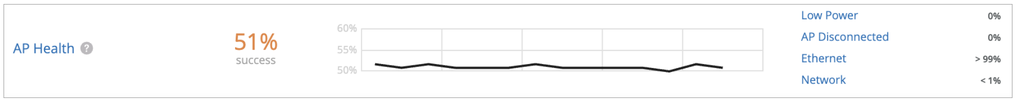
NOTE: To find the Wireless SLEs dashboard, select **Monitor** > **Service Levels** from the left menu, and then click the **Wireless** button.

What Does the AP Health SLE Measure?

Juniper Mist tracks the percentage of time the APs are operational without rebooting or losing connectivity to the cloud.

Classifiers

When AP Health is poor, Juniper Mist sorts the issues into classifiers. The classifiers appear on the right side of the SLE block. In this example, 66 percent of issues were attributed to Low Power, less than 1 percent to AP Disconnected, and 34 percent to Ethernet. (See the classifier descriptions below the example.)



- **Low Power**—An AP received insufficient power from its Power over Ethernet (PoE) connection.
- **AP Disconnected**—One of these conditions occurred:
  - Switch Down—Multiple APs that were connected to the same switch lost cloud connectivity.
  - Site Down—All the APs on the site were unreachable.
  - AP Unreachable—An AP lost cloud connectivity.
  - AP Reboot—An AP rebooted.
- **Ethernet**—One of these conditions occurred:
  - Speed Mismatch—Juniper Mist detected a speed or duplex mismatch between an upstream device and an AP.
  - Ethernet Errors—Juniper Mist detected cyclic redundancy check (CRC) errors on the Ethernet interface of the AP.
- **Network**—AP health is degraded by network-related issues due to round-trip time, packet loss, and Mist Edge tunnel unreachability.
  - Latency
  - Jitter
  - Tunnel Down

Wired SLEs Dashboard

SUMMARY

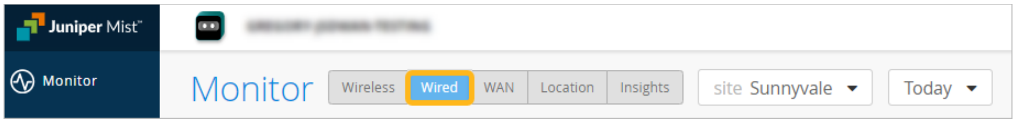
Get started using the wired service-level experience (SLE) dashboard to assess the service levels for user-impacting factors such as throughput, connectivity, and switch health.

IN THIS SECTION

Juniper Mist™ cloud continuously collects network telemetry data and uses machine learning to analyze the end-user experience. You can access this information through the Juniper Mist wired service-level expectation (SLE) dashboards, which help you assess the network's user experience and resolve any issues proactively. The wired SLE dashboards show the user experience of the wired clients on your network at any given point in time. You can use these interactive dashboards to measure and manage your network proactively by identifying any user pain points before they become too big of an issue.

Finding the Wired SLEs Dashboard

To find the Wired SLEs dashboard, select **Monitor** > **Service Levels** from the left menu, and then click the **Wired** button.



NOTE: The buttons appear only if you have the required subscriptions. For information about these requirements, see the Juniper Mist AI-Native Operations Guide.

Wired Assurance: Day 2 - Wired Service Level Expectations (SLEs) Video Overview

Video: Wired Assurance: Day 2 - Wired Service Level Expectations (SLEs)

Using the Wired SLE Dashboard

For a general introduction to SLEs, see "Service Level Expectations (SLE)" on page 0 .

For help interpreting the wired SLEs and classifiers, explore the other Wired SLE topics in this chapter.

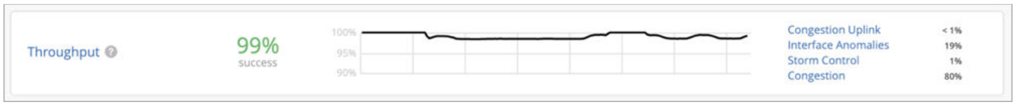
Wired Throughput SLE

SUMMARY

Use the Wired Throughput SLE to assess users' experiences with throughput on your wired network.

IN THIS SECTION

Throughput is one of the Service-Level Expectations (SLEs) that you can track on the wired SLEs dashboard.



Congestion Uplink	< 1%
Interface Anomalies	19%
Storm Control	1%
Congestion	80%

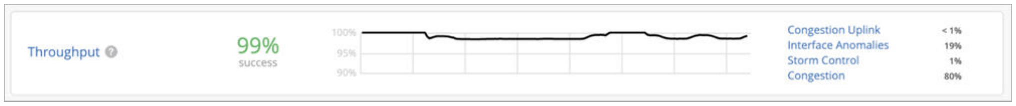
NOTE: To find the Wired SLEs dashboard, select **Monitor** > **Service Levels** from the left menu, and then click the **Wired** button.

What Does the Wired Throughput SLE Measure?

This SLE represents the ability of wired users to pass traffic without impedance.

Classifiers

When the throughput threshold is not met, Juniper Mist sorts the issues into classifiers. The classifiers appear on the right side of the SLE block. In this example, less than 1 percent of the issue were attributed to Congestion Uplink, 19 percent to Interface Anomalies, 1 percent to Storm Control, and 80 percent to Congestion. (See the classifier descriptions below the example.)



Throughput

99%
success

Congestion Uplink	< 1%
Interface Anomalies	19%
Storm Control	1%
Congestion	80%

- **Congestion Uplink**—The SLE dashboard shows high congestion uplink when:
  - One of the neighbors is a switch or a router (known through LLDP).
  - The port is a Spanning Tree Protocol (STP) root port.
  - The uplink port has a higher number of transmitted and received packets compared to the other ports.
  - Aggregated Links. Congestion can also be caused by aggregated Ethernet links and module ports.
- **Interface Anomalies**—The details for interface anomalies are all obtained from the switch. The Interface Anomalies classifier contains three sub-classifiers: MTU Mismatch, Cable Issues, and Negotiation Failed.
  - **MTU Mismatch**—As an administrator, you can set an MTU value for each interface. The default value for Gigabit Ethernet interfaces is 1514 . To support jumbo frames, you must configure an MTU value of 9216, which is the upper limit for jumbo frames on a routed virtual LAN (VLAN) interface. It's important to ensure that the MTU value is consistent along the packet's path, as any MTU mismatch will result in discarded or fragmented packets. In Juniper Networks switches, you can check for MTU mismatches in the **MTU Errors** and **Input Errors** sections of the `show interface extensive` command output. Each input error or MTU error contributes to a "bad user minute" under MTU mismatch.
  - **Cable Issues**—This sub-classifier shows the user minutes affected by faulty cables in the network.
  - **Negotiation Failed**—Latency on ports can happen due to autonegotiation failure, duplex conflicts, or user misconfiguration of device settings. Moreover, older devices may fail to achieve maximum speed and could operate at a slower link speed of 100 Mbps. This sub-classifier identifies and helps mitigate instances of bad user time caused by these issues.
- **Storm Control**—Storm control allows the device to monitor traffic levels and drop broadcast, unknown unicast, and multicast packets when they exceed a set threshold or traffic level. This threshold is known as a storm control level or storm control bandwidth. The default storm control level is 80 percent of the combined broadcast, multicast, and unknown unicast traffic on all Layer 2 interfaces of Juniper switches. Storm control helps prevent traffic storms, but it can also potentially

throttle applications or client devices. This classifier identifies these conditions and helps users proactively mitigate throughput issues.

- **Congestion**—This classifier measures the number of output drops. When packets come into a switch interface, they are placed in an input queue (buffer). When the buffer becomes full, it will start to drop packets (TxDrops). We use a formula that takes into account the following ratios to determine if there is a 'bad user minute' due to congestion:
  - TxDrops to TxPackets—Total transmitted bytes dropped to total packets transmitted.
  - Txbps to Link speed—Total bytes transmitted per second to link speed.
  - RxSpeed to Link speed—Total bytes received per second to link speed.

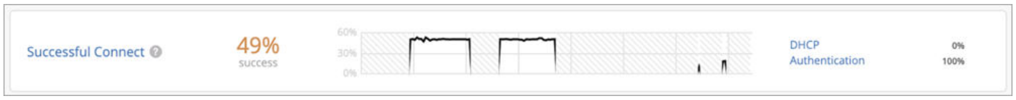
Wired Successful Connect SLE

SUMMARY

Use the Wired Successful Connect SLE to assess clients' experiences connecting to your wired network.

IN THIS SECTION

Successful Connect is one of the Service-Level Expectations (SLEs) that you can track on the Wired SLEs dashboard.



NOTE: To find the Wired SLEs dashboard, select **Monitor** > **Service Levels** from the left menu, and then click the **Wired** button.

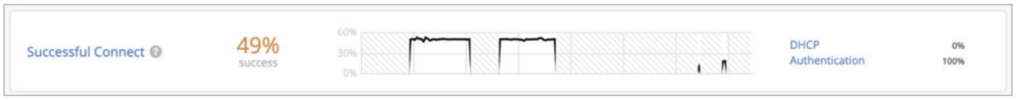
What Does the Wired Successful Connect SLE Measure?

Juniper Mist monitors client connection attempts and identifies failures. This SLE helps you to assess the impact of these failures and to identify the issues to address.

NOTE: This SLE will show data only if you use 802.1X on the wired network to authenticate clients or if you have DHCP snooping configured.

Classifiers

When connection attempts are unsuccessful, Juniper Mist sorts the issues into classifiers. The classifiers appear on the right side of the SLE block. In this example, 100 percent of the issues are attributed to Authentication. (See the classifier descriptions below the example.)



- **DHCP**—Dynamic Host Configuration Protocol (DHCP) snooping enables the switch to examine the DHCP packets and keep track of the IP-MAC address binding in the snooping table. This classifier adds a failure event every time a client connects to a network and fails to reach the 'bound' state within a minute (DCHP timeouts).

  NOTE: The SLE dashboard shows DHCP failures only for those switches that have DHCP snooping configured.

- **Authentication**—Each time a client authenticates, a client event is generated. These could either be successful or failed events. This classifier helps you identify issues that caused authentication failures. Here's a list of possible reasons for an 802.1X authentication failure:

  - If a single switch port fails to authenticate, it could be due to a user error or misconfigured port.

  - If all switch ports fail to authenticate, it could be because:

    - The switch is not added as a NAS client in the RADIUS server.

    - A routing issue exists between the switch and the RADIUS server.

    - The RADIUS server is down.

  - If all switch ports on all the switches fail to authenticate, it could indicate a temporary failure with the RADIUS server at that specific moment.

  - If a specific type of device, such as a Windows device, fails to authenticate, it may suggest an issue related to certifications.

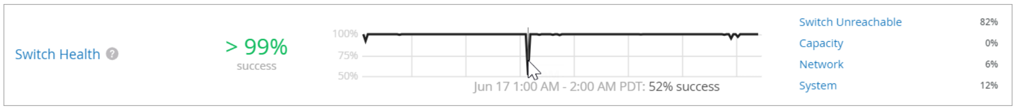
Switch Health SLE

SUMMARY

Use the Switch Health SLE to assess switch performance and to identify user-impacting issues with switch reachability, memory, CPU, and more.

IN THIS SECTION

Switch Health is one of the Service-Level Expectations (SLEs) that you can track on the Wired SLEs dashboard.



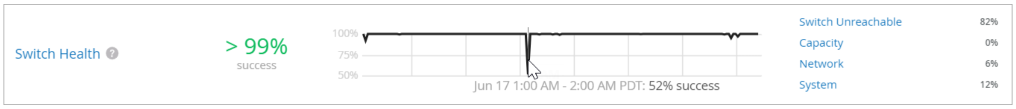
NOTE: To find the Wired SLEs dashboard, select **Monitor** > **Service Levels** from the left menu of the Juniper Mist™ portal, and then select the **Wired** button.

What Does the Switch Health SLE Measure?

Juniper Mist™ monitors your switches' operating temperatures, power consumption, CPU, and memory usage. Monitoring switch health is crucial because issues such as high CPU usage can directly impact connected clients. For instance, if CPU utilization spikes to 100 percent, the connected APs may lose connectivity, affecting the clients' experience.

Classifiers

When the Switch Health threshold is not met, Juniper Mist sorts the issues into classifiers. The classifiers appear on the right side of the SLE block. In this example, 82 percent of the issues are attributed to Switch Unreachable and 12 percent to System. (See the classifier descriptions below the example.)



- **Switch Unreachable**—The switch can't be accessed.
- Capacity

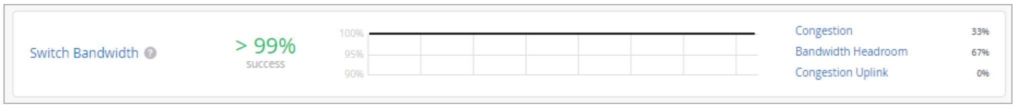
  - **ARP Table**—Usage exceeded 80 percent of the Address Resolution Protocol (ARP) table capacity.
  - **Route Table**—Usage exceeded 80 percent of the routing table capacity.
  - **MAC Table**—Usage exceeded 80 percent of the MAC table capacity.

- **Network**—You can use this classifier to monitor user minutes when the throughput is lower than expected due to uplink capacity limitations. It identifies issues based on the round-trip time (RTT) value of packets sent from the switch to the Mist cloud. The Network classifier has two sub-classifiers that help you identify these issues:
  - **WAN Latency**—Displays user minutes affected by latency. The latency value is calculated based on the average value of RTT over a period of time.
  - **WAN Jitter**—Displays user minutes affected by jitter. The jitter value is calculated by comparing the standard deviation of RTT within a small period (last 5 or 10 minutes) with the overall deviation of RTT over a longer period (day or week). You can view this information for a particular switch or site.
- **System**
  - **CPU**—The CPU usage of the switch is above 90 percent.
  - **Memory**—The memory utilization is above 80 percent.
  - **Temp**—The operating temperature of the switch is outside the prescribed threshold range, going either above the maximum limit or below the minimum requirement.
  - **Power**—The switch is consuming over 90 percent of the available power.

Switch Bandwidth SLE

IN THIS SECTION

Switch Bandwidth is one of the Service-Level Expectations (SLEs) that you can track on the Wired SLEs dashboard.


Switch Bandwidth
> 99%
success

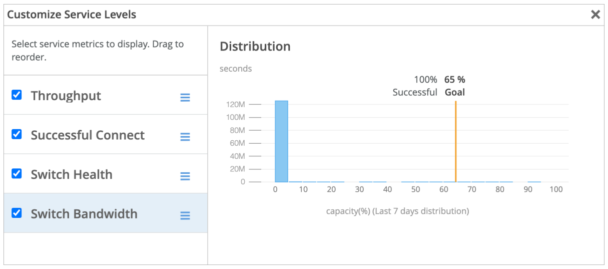
Congestion 33%
Bandwidth Headroom 67%
Congestion Uplink 0%

NOTE: To find the Wired SLEs dashboard, select **Monitor** > **Service Levels** from the left menu, and then click the **Wired** button.

What Does the Switch Bandwidth SLE Measure?

Juniper Mist™ measures the available bandwidth on your network based on the queued packets and dropped packets for each configured queue. The ratio between total_DropppedPackets and total_QueuedPackets is used to determine congestion at the interface level. Thee most dropped queue is also noted in the details for distribution/affected items. This SLE can help you to determine if you need more wired bandwidth on your site.

You can click the **Settings** button (above the SLE blocks) to set the percentage to use as the success threshold for this SLE. The percentage represents the total_DropppedPackets as a portion of total_QueuedPackets.


Customize Service Levels ✕

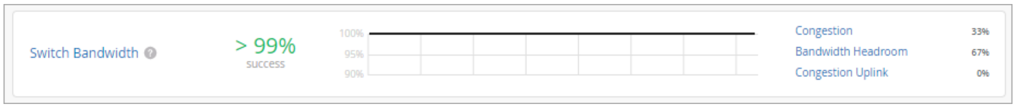
Select service metrics to display. Drag to reorder.

☑ Throughput
☑ Successful Connect
☑ Switch Health
☑ Switch Bandwidth

Distribution

Classifiers

When the Switch Bandwidth threshold is not met, Juniper Mist sorts the issues into classifiers. The classifiers appear on the right side of the SLE block. In this example, 33 percent of the issues are attributed to Congestion and 67% to Bandwidth Headroom. (See the classifier descriptions below the example.)


Switch Bandwidth
> 99%
success

Congestion 33%
Bandwidth Headroom 67%
Congestion Uplink 0%

- **Congestion**—This classifier measures the number of output drops. When packets come into a switch interface, they are placed in an input queue (buffer). When the buffer becomes full, it will start to drop packets (TxDrops). We use a formula that takes into account the following ratios to determine if there are bad user minutes due to congestion:
  - TxDrops to TxPackets—Total transmitted bytes dropped to total packets transmitted.

  - Txbps to Link speed—Total bytes transmitted per second to link speed.
  - RxSpeed to Link speed—Total bytes received per second to link speed.
- **Bandwidth Headroom**—This classifier is triggered if the bandwidth usage exceeds the threshold for this SLE.
- **Congestion Uplink**—The SLE dashboard shows high congestion uplink when:
  - One of the neighbors is a switch or a router (known through LLDP).
  - The port is a Spanning Tree Protocol (STP) root port.
  - The uplink port has a higher number of transmitted and received packets compared to the other ports.
  - There is congestion due to aggregated Ethernet links and module ports.

WAN SLEs Dashboard

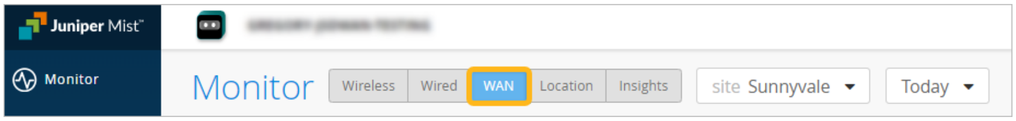
SUMMARY

Get started using the WAN Service-Level Experiences (SLEs) dashboard to assess the service levels for user-impacting factors such as WAN Edge health, WAN link health, and application health.

IN THIS SECTION

Finding the WAN SLEs Dashboard

To find the WAN SLEs dashboard, select **Monitor** > **Service Levels** from the left menu, and then click the **WAN** button.

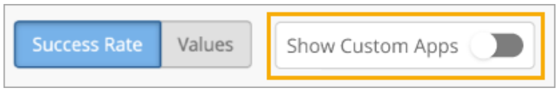


NOTE: The buttons appear only if you have the required subscriptions. See "Requirements" on page 6.

Additional Filters for WAN SLEs

Above the WAN SLEs, you'll see the usual buttons to show **Success Rate** or **Values**. You'll also see a button to **Show Custom Apps**.

In the example below, the button is in the Off position, so all applications are included. Drag the button to the On position to show only your custom applications.



Video: WAN Assurance Overview

Video: WAN Assurance Video Overview

Using the WAN SLE Dashboard

For a general introduction to SLEs, see "Service Level Expectations (SLE)" on page 0 .

For help interpreting the WAN SLEs and classifiers, explore the other WAN SLE topics in this chapter.

Video: Troubleshoot WAN Issues with SLEs

Video: SLE Example

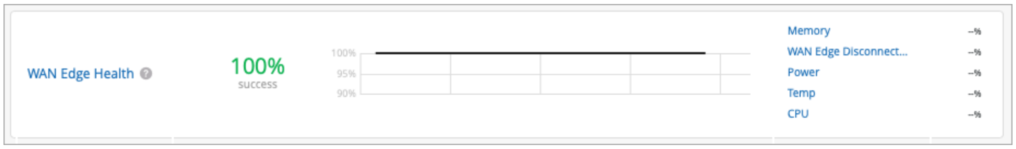
WAN Edge Health SLE

SUMMARY

Use the WAN Edge Health SLE to assess service levels for your WAN edge devices.

IN THIS SECTION

WAN Edge Health is one of the Service-Level Expectations (SLEs) that you can track on the WAN SLEs dashboard.



NOTE: To find the WAN SLEs dashboard, select **Monitor** > **Service Levels** from the left menu, and then click the **WAN** button.

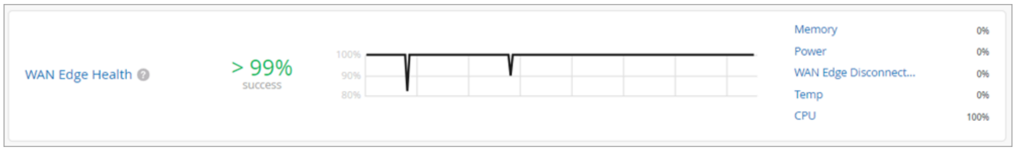
What Does the WAN Edge Health SLE Measure?

Juniper Mist monitors the user minutes when the health or performance of the WAN edge device is not optimal. Suboptimal health lowers the device's ability to pass traffic, thus directly affecting any clients connected to the device.

Juniper Mist analyzes various factors that affect WAN edge health and assigns a score. You can click the **Settings** button to set the success threshold.

Classifiers

When the WAN Edge Health threshold is not met, Juniper Mist sorts the issues into classifiers. The classifiers appear on the right side of the SLE block. In this example, 100 percent of the issues are attributed to CPU. (See the classifier descriptions below the example.)



- - **Memory**—Juniper Mist triggers this classifier when the WAN edge memory utilization is above 80 percent.

- **Power**—Juniper Mist triggers this classifier when power consumption is above 90 percent of the available power.

- **WAN Edge Disconnected**—Juniper Mist triggers this classifier when the WAN edge device disconnects from the Juniper Mist cloud.

- **Temp**—Juniper Mist triggers this classifier when the operating temperature of the WAN edge device exceeds the prescribed threshold range, either going above the maximum limit or below the minimum requirement.

    - **CPU**—Juniper Mist triggers this sub-classifier when the CPU temperature exceeds the prescribed threshold range.

    - **Chassis**—Juniper Mist triggers this sub-classifier when the chassis temperature exceeds the prescribed threshold range.

- **CPU**—Juniper Mist triggers this classifier when the CPU utilization is above 90 percent. When the CPU utilization spikes on a Juniper WAN edge device, downstream devices can lose their connectivity. Therefore, clients fail to pass traffic.

    - **Data Plane**—Juniper Mist triggers this sub-classifier when the Data Plane CPU utilization is above 90 percent.

    - **Control Plane**—Juniper Mist triggers this sub-classifier when control plane CPU utilization is above 90 percent.

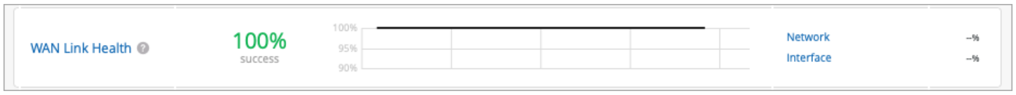
WAN Link Health SLE

SUMMARY

Use the WAN Link Health SLE to assess service levels for your WAN links.

IN THIS SECTION

WAN Link Health is one of the Service-Level Expectations (SLEs) that you can track on the WAN SLEs dashboard in the Juniper Mist™ portal.



NOTE: To find the WAN SLEs dashboard, select **Monitor** > **Service Levels** from the left menu, and then select the **WAN** button.

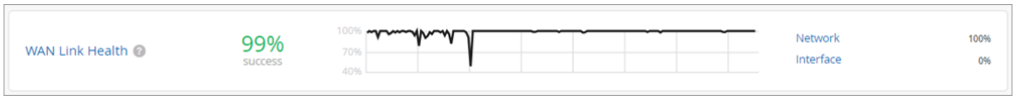
What Does the WAN Link Health SLE Measure?

Juniper Mist monitors the user minutes when the WAN link health meets or fails to meet the SLE threshold. Poor WAN link health lowers the device's ability to pass traffic, thus directly affecting any clients using that link.

You can click the **Settings** button to set the success threshold.

Classifiers

When the WAN Link threshold is not met, Juniper Mist sorts the issues into classifiers. The classifiers appear on the right side of the SLE block. In this example, 100 percent of the issues are attributed to Network. (See the classifier descriptions below the example.)



- **Network**—Network issues affected the WAN link.

  The Network classifier has three sub-classifiers:

  - **Latency**—WAN link traffic showed latency. Juniper Mist calculates latency by using the average value of round-trip time (RTT) for traffic over a period of time.

  - **IPSec Tunnel Down**—One of the Overlay IPsec tunnels was down.

  - **Jitter**—The WAN link experienced jitter. Juniper Mist calculates jitter by using the variation (standard deviation) of RTT within a period of 5 to 10 minutes for a particular WAN link. We compare the calculated value with the average deviation of RTT over a day or a week.

- **Interface**—Interface issues affected the WAN link. The Interface classifier has three sub-classifiers:

  - **Congestion**—Congestion affected the WAN link. The Congestion sub-classifier measures the number of output packet drops. When packets enter an interface, they go in a queue for buffering. When the buffer becomes full it starts to drop packets (TxDrops).

  - **Cable Issues**—Faulty cables affected the WAN link.

  - **VPN**—VPN performance issue occurred.

WAN Gateway Bandwidth SLE

SUMMARY

Use the WAN Gateway Bandwidth SLE to track if the gateway bandwidth met or failed to meet the threshold.

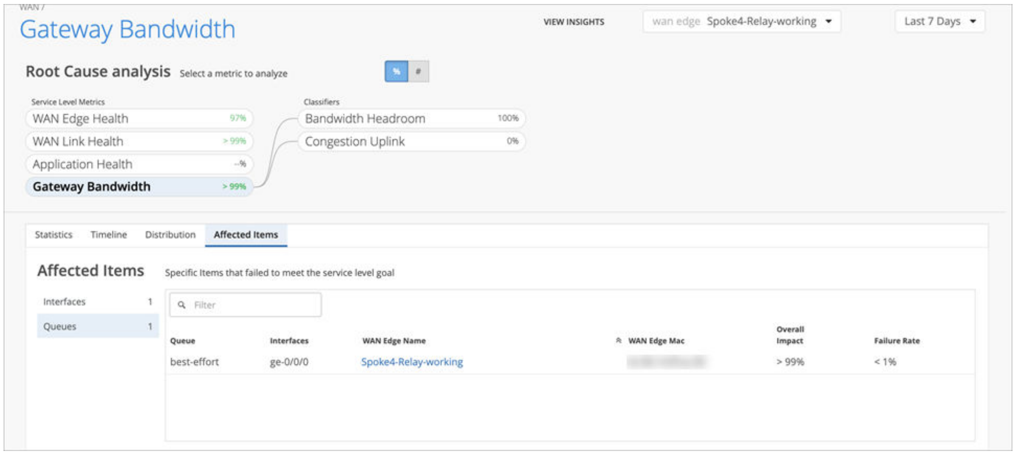
IN THIS SECTION

WAN Gateway Bandwidth is one of the Service-Level Expectations (SLEs) that you can track on the WAN SLEs dashboard in the Juniper Mist™ portal.

Get familiar with the Service Level Expectations (SLEs) and the SLE dashboard. See "Service Level Expectations (SLE)" on page 0 .

To find the WAN SLEs dashboard, select **Monitor** > **Service Levels** from the left menu, and then click the **WAN** button.

Figure 1: Gateway Bandwidth SLE



Queue	Interfaces	WAN Edge Name	WAN Edge Mac	Overall Impact	Failure Rate
best-effort	ge-0/0/0	Spoke4-Relay-working	[redacted]	> 99%	< 1%

The metric beside the **Gateway Bandwidth** indicates the percentage of the time the Gateway Bandwidth was healthy for a given time range. A 100% success rate indicates that there were no failures for that metric. When the success rate is less than 100%, it signifies that failures occurred on the Site/WAN Edge corresponding to that metric. In such cases, classifiers display the details of the failures.

NOTE: The gateway bandwidth SLE is unique to the SRX Series Firewall and the WAN Gateway Bandwidth SLE evaluates the IPsec overlay that constitutes the SD-WAN.

What Does the WAN Gateway Bandwidth SLE Measure?

This SLE covers packet drops due to congestion (congestion classifier) and high bandwidth usage (headroom classifier). If the ratio of dropped packets to total queued packets is significant, the congestion classifier is displayed along with the queue experiencing the most drops. If there are no dropped packets but bandwidth usage exceeds a certain upper threshold, a headroom classifier is shown along with the most utilized queue. The headroom threshold is determined based on maximum usage statistics from the past two weeks.

Use this SLE to determine if you need more WAN bandwidth on your site.

Classifiers

When the WAN Bandwidth threshold is not met, Juniper Mist sorts the issues into classifiers. The classifiers appear on the right side of the SLE block.

- Bandwidth Headroom—This classifier is activated when bandwidth usage surpasses the SLE threshold. It indicates the percentage of time the gateway bandwidth SLE was not met due to exceeding the headroom threshold. The headroom is an estimated baseline of available WAN bandwidth, based on the highest usage over the past 14 days. The classifier triggers when current usage exceeds this baseline.

- Congestion Uplink—This classifier indicates the percentage of time the Gateway Bandwidth SLE was not met due to uplink congestion. This classifier measures the number of output drops. That is, the classifier uses the ratio of total transmitted bytes dropped to total packets transmitted (tx_drops/tx_packets) to determine if there are bad user minutes due to congestion.

For more details on SLE blocks, see Understanding the SLE Blocks.

RELATED DOCUMENTATION

WAN SLEs Dashboard | 85

WAN Edge Health SLE | 87

WAN Link Health SLE | 88

WAN Application Health SLE | 92

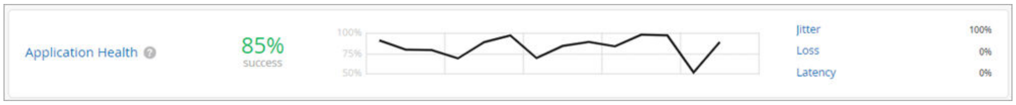
WAN Application Health SLE

SUMMARY

Use the WAN Application Health SLE to assess service levels for your applications.

IN THIS SECTION

WAN Application Health is one of the Service-Level Expectations (SLEs) that you can track on the WAN SLEs dashboard in the Juniper Mist™ portal.

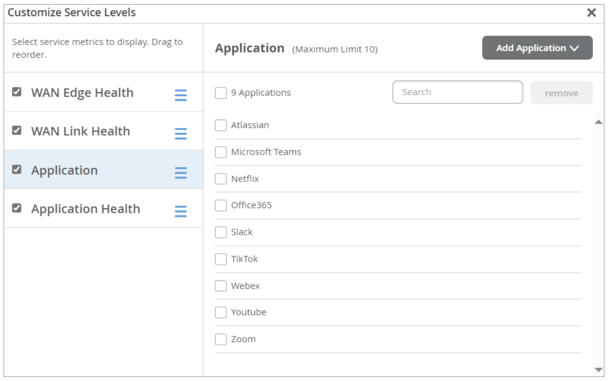


NOTE: To find the WAN SLEs dashboard, select **Monitor** > **Service Levels** from the left menu, and then click the **WAN** button.

What Does the WAN Application Health SLE Measure?

Juniper Mist monitors the latency of WAN applications to identify applications that are performing sub-optimally. This SLE can help you to understand the end users' experiences when accessing applications. For example, a weak network connection might give good user experiences for FTP or SMTP-based applications, but bad user experiences for VoIP applications. The Application Health SLE will help you identify which applications are giving you trouble.

For fine-tuning, you can click the **Settings** button to select individual applications to include or exclude.



Customize Service Levels ×

Select service metrics to display. Drag to reorder.

- ☑ WAN Edge Health
- ☑ WAN Link Health
- ☑ Application
- ☑ Application Health

Application (Maximum Limit 10) Add Application

□ 9 Applications Search remove

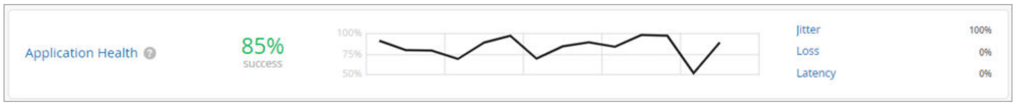
- □ Atlassian
- □ Microsoft Teams
- □ Netflix
- □ Office365
- □ Slack
- □ TikTok
- □ Webex
- □ Youtube
- □ Zoom

- To remove applications from this SLE—Select the check box for each application, and then click **Remove**.

- To add applications to this SLE—Click **Add Application**, then select the check box for the application, and then click **Add**. Or click **Create Custom** to add another application.

Classifiers

When the Application threshold is not met, Juniper Mist sorts the issues into classifiers. The classifiers appear on the right side of the SLE block. In this example, 100 percent of the issues are attributed to Jitter. (See the classifier descriptions below the example.)



- Jitter—Inconsistent packet transmit times can impact users' experiences with applications, especially real-time applications such as VoIP and video.

- Latency—Slow response time (lag) can impact users' experiences by, for example, causing webpages to load slowly or interrupting video and audio streams.

- Loss—Packet loss can cause application usage problems, such as bad audio or video.

- Application Services (applicable to Session Smart Routers only)—Slow responses to application requests, recurring disconnects, and insufficient bandwidth usage by applications can impact users' experiences. The Application Services classifier has three subclassifiers that help you identify these issues:

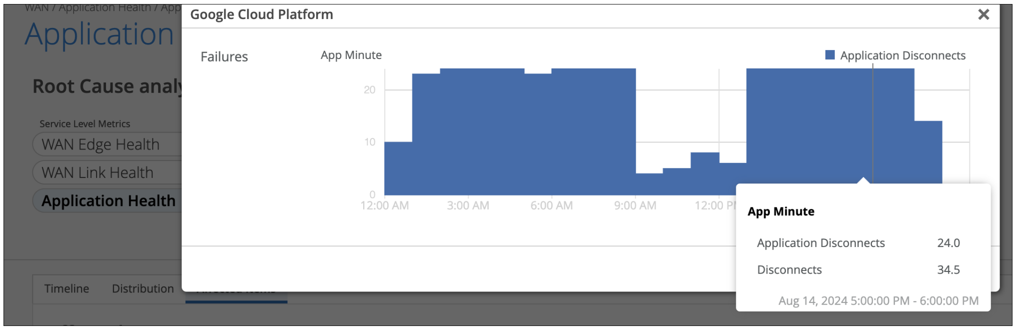
  - Slow Application

  - Application Bandwidth

  - Application Disconnects

  Here are two examples that show how Mist displays the Application Services information.

In this example, Application Disconnects value indicates the bad user minutes caused by application disconnect events. The Disconnects value indicates the number of disconnect events observed per minute.

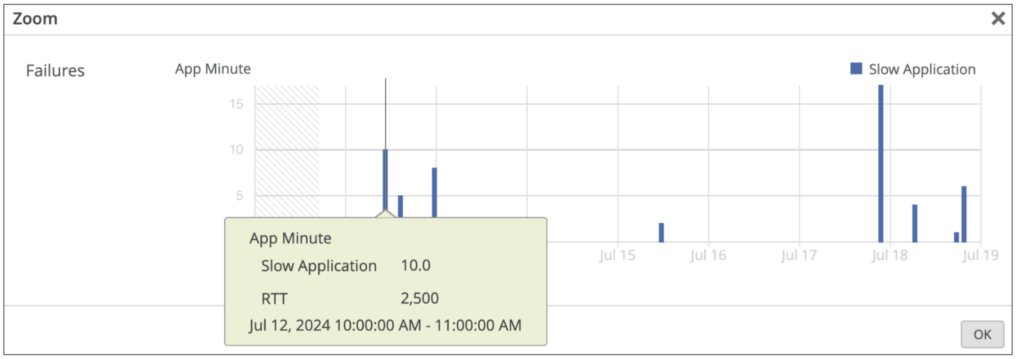


App Minute

Application Disconnects	24.0
Disconnects	34.5

Aug 14, 2024 5:00:00 PM - 6:00:00 PM

Here is another example that shows the Slow Application value, which indicates the number of bad user minutes caused by slow applications. The RTT value shows the RTT (in seconds) associated with the slow applications.



App Minute

Slow Application	10.0
RTT	2,500

Jul 12, 2024 10:00:00 AM - 11:00:00 AM

4

CHAPTER

Alerts

Alerts Overview

SUMMARY

Get familiar with Juniper Mist™ alerts and the Alerts dashboard in the Juniper Mist portal.

IN THIS SECTION

What Are Alerts?

Alerts represent network and device issues that are ongoing. Juniper Mist™ categorizes them as follows:

- Infrastructure Alerts—This category includes issues that can potentially affect a large number of clients. For example, an event during which a Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), or RADIUS server is unreachable can affect many clients. Similarly, if a power supply on a switch is in alarm state, a large number of clients and a large amount of traffic could be affected.

- Marvis Alerts—The Predictive Analytics and Correlation Engine (PACE) raises Marvis alerts for the events that Marvis tracks. For example, if an access point (AP) regularly fails health checks, Marvis notices and tracks this event.

- Security Alerts—Security alerts are raised by repeated events that could dramatically affect network security. For example, if a rogue AP is detected, that represents a potential security problem and if a client connects to a rogue AP, that could be even worse.

NOTE:

- For information about alerts, see "Juniper Mist Alert Types" on page 100.

- To enable the alerts that you want to include on the Alerts dashboard, see "Juniper Mist Alert Types" on page 100.

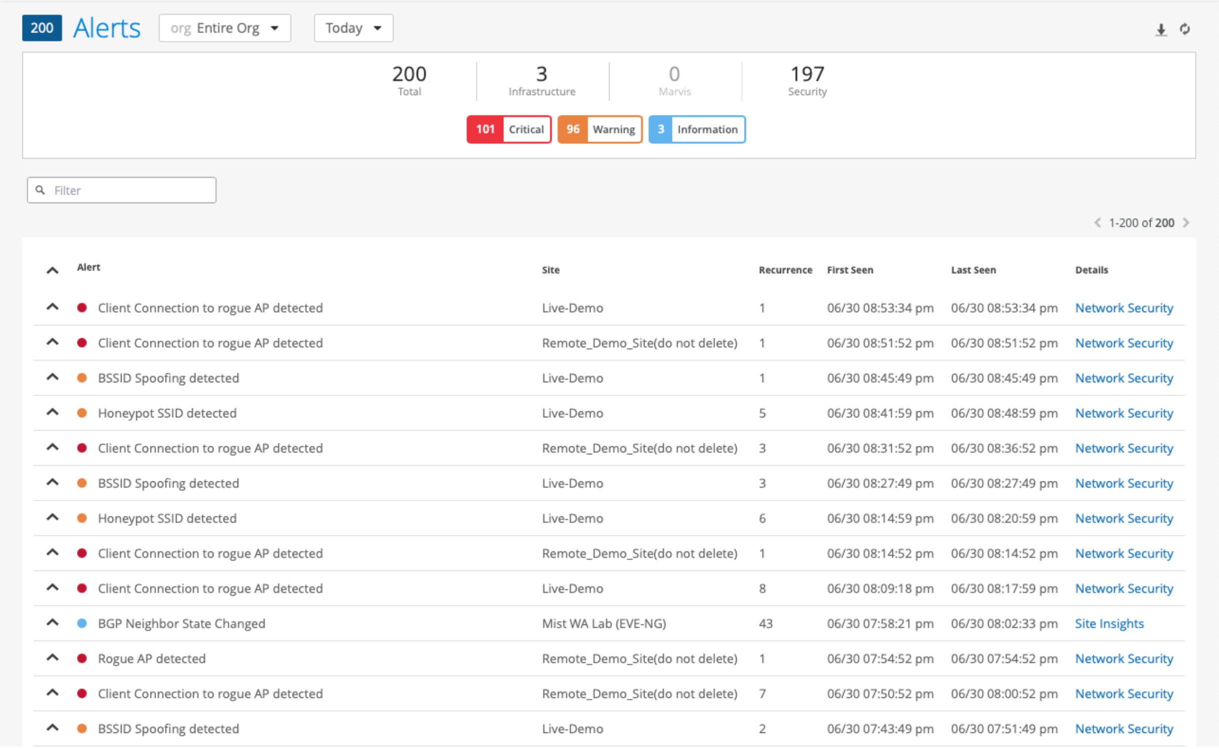
Finding the Alerts Dashboard

The Alerts dashboard is your alerts log. This dashboard provides information about all alerts that are enabled on the Alerts Configuration page.

NOTE: For help configuring alerts, see "Configure Alerts and Email Notifications" on page 109.

To view the Alerts dashboard, select **Monitor** > **Alerts** from the left menu.

In the following example, you can see the major elements of the Alerts dashboard.



Alert	Site	Recurrence	First Seen	Last Seen	Details
● Client Connection to rogue AP detected	Live-Demo	1	06/30 08:53:34 pm	06/30 08:53:34 pm	Network Security
● Client Connection to rogue AP detected	Remote_Demo_Site(do not delete)	1	06/30 08:51:52 pm	06/30 08:51:52 pm	Network Security
● BSSID Spoofing detected	Live-Demo	1	06/30 08:45:49 pm	06/30 08:45:49 pm	Network Security
● Honeypot SSID detected	Live-Demo	5	06/30 08:41:59 pm	06/30 08:48:59 pm	Network Security
● Client Connection to rogue AP detected	Remote_Demo_Site(do not delete)	3	06/30 08:31:52 pm	06/30 08:36:52 pm	Network Security
● BSSID Spoofing detected	Live-Demo	3	06/30 08:27:49 pm	06/30 08:27:49 pm	Network Security
● Honeypot SSID detected	Live-Demo	6	06/30 08:14:59 pm	06/30 08:20:59 pm	Network Security
● Client Connection to rogue AP detected	Remote_Demo_Site(do not delete)	1	06/30 08:14:52 pm	06/30 08:14:52 pm	Network Security
● Client Connection to rogue AP detected	Live-Demo	8	06/30 08:09:18 pm	06/30 08:17:59 pm	Network Security
● BGP Neighbor State Changed	Mist WA Lab (EVE-NG)	43	06/30 07:58:21 pm	06/30 08:02:33 pm	Site Insights
● Rogue AP detected	Remote_Demo_Site(do not delete)	1	06/30 07:54:52 pm	06/30 07:54:52 pm	Network Security
● Client Connection to rogue AP detected	Remote_Demo_Site(do not delete)	7	06/30 07:50:52 pm	06/30 08:00:52 pm	Network Security
● BSSID Spoofing detected	Live-Demo	2	06/30 07:43:49 pm	06/30 07:51:49 pm	Network Security

This table includes:

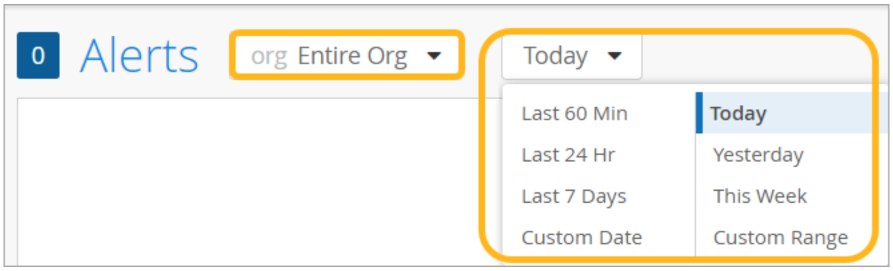
- Alert—The name of the alert, along with an icon representing the severity level. For more information about the color codes and severity levels, see the "Severity Filters" on page 99 table later in this topic.
- Site—The name of the site where this issue occurred.
- Recurrence—The number of times that this issue occurred.
- First Seen and Last Seen—The time period when this issue occurred.
- Details—The affected component (as listed below), with a link that you can click for more details.

These links include:

- Device Insights—Click the link to view the Insights page for the selected site. This page shows a timeline of events and full details for client events, AP events, and site events. You'll also see details for all applications.
- Marvis—Click the link to view the Marvis Actions page.
- Network Security—Click the link to view the Wireless Security page. This page shows all security issues for each SSID. You'll see information such as the type of issue, number of affected clients, band, channel, RSSI, and floorplan location.
- WAN Edge Details—Click the link to view the Insights page for WAN Edges at the selected site. This page shows details for WAN Edge events, applications, application policies, WAN Edge devices, ports, peer path stats, and more.

Selecting the Context and Time Period

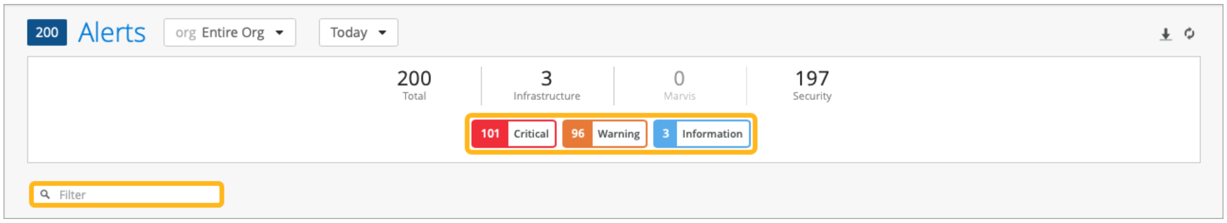
At the top of the Alerts page, select the context, which can be an entire organization or a single site. Also select a time period, such the last 60 minutes, the last 7 days, or a date range.



NOTE: The Alerts page displays data as recent as the past 60 minutes or as far back as the last 7 days. If you purchase a Premium Analytics subscription, you can access up to 3 years' worth of wireless network insights and other data. To access the information available through your Premium Analytics subscription, select **Analytics** > **Premium Analytics** from the left menu.

Filtering the Display

You can apply filters to show only the alerts that you want to see.



Severity Filters

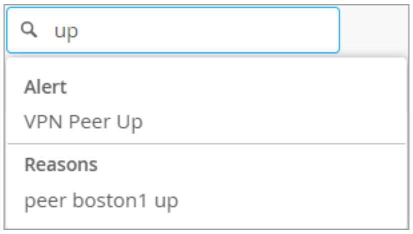
Juniper Mist ranks alerts by severity. The severity buttons at the top of the Alerts page show the number of issues for each severity level. Click a button to show only the alerts for that severity level.

Table 2: Severity Levels

Severity	Color Code	Recommended Action
Critical	Red	Take immediate action.
Warning	Orange	Continue monitoring if the event continues.
Informational	Blue	No action is required.

Filter Box

Above the list of alerts, you can use the Filter box to enter text to filter by. As you start typing, matching alerts appear in the drop-down list. Click one of them to apply the filter.



Juniper Mist Alert Types

SUMMARY

Juniper Mist™ provides various alerts that you can enable to track ongoing issues.

IN THIS SECTION

Infrastructure Alerts

Infrastructure alerts are for events that potentially affect a large number of clients. For example, an unreachable Domain Name System (DNS) or a bad power supply on a switch can affect a large number of clients and a large amount of traffic.

Table 3: Infrastructure Alerts by Severity

Severity	Alert Name
Critical (red icon)	ARP Failure
	DHCP Failure
	DNS Failure
	Mist Edge Fan Unplugged
	Mist Edge cpu usage high
	Mist Edge disconnected from cloud
	Mist Edge disk usage high
	Mist Edge memory usage high
	Mist Edge power input disconnected

Table 3: Infrastructure Alerts by Severity *(Continued)*

Severity	Alert Name
	Mist Edge service failed to start
	Mist Edge unplugged from power
	Switch Fan Alarm
	Virtual Chassis - Backup Member Elected
	Virtual Chassis - New device elected for Active Role
	Virtual Chassis Member Deleted
	Virtual Chassis Port Down
Informational (blue)	BGP Neighbor State Changed
	BGP Neighbor Up
	Cellular Edge Connected to NCM
	Cellular Edge Disconnected from NCM
	Cellular Edge Firmware Upgraded
	Cellular Edge Login Failure
	Cellular Edge Login Success
	Cellular Edge Rebooted
	Cellular Edge SIM Door Closed
	Cellular Edge SIM Door Opened
	Cellular Edge WAN Cellular Connected
	Cellular Edge WAN Cellular Service Type Changed

Table 3: Infrastructure Alerts by Severity *(Continued)*

Severity	Alert Name
	Cellular Edge WAN Ethernet Connected
	Cellular Edge WAN Ethernet Plugged
	Critical Switch Port Up **NOTE**: If you enable this alert, you also need to update the switch configuration to identify the critical ports. To do this: 1. In your switch template, under **Select Switches Configuration**, select the rule for the ports that you want to configure. (Or add a new rule.) 2. On the **Port Config** tab, select the port or port range that you want to configure. 3. In the settings window, select the **Enable critical alerts** check box. 4. Repeat these steps for all critical ports. For more information about port configuration, see the Juniper Mist Wired Assurance Configuration Guide.
	Critical WAN Edge Port Up **NOTE**: If you enable this alert, you also need to update the WAN or LAN configuration to identify the critical ports. To do this: 1. In your WAN Edge template, select the WAN or LAN configuration that you want to update. (Or add a new configuration.) 2. Under **Interface**, enter the port or ports, and then select the **Enable critical alerts** check box. 3. Repeat these steps for all critical ports. For more information about WAN Edges configuration, see the Juniper Mist WAN Assurance Configuration Guide.
	Device restarted
	Mist Edge connected to cloud
	Mist Edge cpu usage normal
	Mist Edge disk usage normal

Table 3: Infrastructure Alerts by Severity *(Continued)*

Severity	Alert Name
	Mist Edge memory usage normal
	Mist Edge plugged to power
	Mist Edge power input connected
	New tunnel(s) formed
	Switch Radius Server Unresponsive
	Switch restarted
	Virtual Chassis Member Added
	Virtual Chassis Port Up
Warning	Mist Edge Fan Plugged
	All data ports dropped from LACP
	All tunnels are disconnected
	BGP Neighbor Down
	Cellular Edge WAN Cellular Disconnected
	Cellular Edge WAN Ethernet Disconnected
	Cellular Edge WAN Ethernet Unplugged

Table 3: Infrastructure Alerts by Severity *(Continued)*

Severity	Alert Name
	Critical Switch Port Down **NOTE**: If you enable this alert, you also need to update the switch configuration to identify the critical ports. To do this: 1. In your switch template, under **Select Switches Configuration**, select the rule for the ports that you want to configure. (Or add a new rule.) 2. On the **Port Config** tab, select the port or port range that you want to configure. 3. In the settings window, select the **Enable critical alerts** check box. 4. Repeat these steps for all critical ports. For more information about switch configuration, see the Juniper Mist Wired Assurance Configuration Guide.
	Critical WAN Edge Port Down **NOTE**: If you enable this alert, you also need to update the WAN or LAN configuration to identify the critical ports. To do this: 1. In your WAN Edge template, select the WAN or LAN configuration that you want to update. (Or add a new configuration.) 2. Under **Interface**, enter the port or ports, and then select the **Enable critical alerts** check box. 3. Repeat these steps for all critical ports. For more information about WAN Edges configuration, see the Juniper Mist WAN Assurance Configuration Guide.
	Device offline
	EVPN detected a duplicate MAC address
	Fpc Management Ethernet Link Down
	HA Control Link Down
	Last data port dropped from LACP
	Loop detected (by AP)

Table 3: Infrastructure Alerts by Severity *(Continued)*

Severity	Alert Name
	Mist Edge service crashed
	Switch BPDU Error
	Switch Bad Optics
	Switch DHCP Pool Exhausted
	Switch High Temperature
	Switch PEM Alarm
	Switch PoE Alarm
	Switch Power Supply Alarm
	Switch Storage Partition Alarm
	Switch offline
	Tunnel down
	VPN Peer Down
	Virtual Chassis Member Restarted
	WAN Edge BGP Neighbor Down
	WAN Edge DHCP Pool Exhausted
	WAN Edge Flow Count Threshold Exceeded
	WAN Edge Forwarding Information Base Count Threshold Exceeded
	WAN Edge Source NAT Pool Threshold Exceeded
	WAN Edge Offline

Marvis Alerts

Marvis alerts are tied into the Marvis Action Dashboard. These alerts are triggered whenever the corresponding Marvis Action is detected in your organization. For example, if an access point (AP) regularly fails health checks, Marvis notices and tracks this event.

Table 4: Marvis Alerts by Severity

Severity	Applies To	Alert Name
Critical	AP	AP health check failed
		AP insufficient capacity
		AP insufficient coverage
		Bad cable
		Non-compliant
		Offline (Marvis)
		AP Loop due to Switch Port Flap
		AP Loop due to duplicated WLAN paths
	Connectivity	ARP failure (Marvis)
		Authentication failure (Marvis)
		DHCP failure (Marvis)
		DNS failure (Marvis)
	WAN Edge	Bad WAN Uplink
		Bad cable
		Device Problem
		MTU mismatch

Table 4: Marvis Alerts by Severity *(Continued)*

Severity	Applies To	Alert Name
		Negotiation mismatch
		VPN Path Down
	Switch	Bad cable
		Missing VLAN
		Negotiation mismatch
		Port Stuck
		Switch STP Loop
Warning	Switch	Port flap

Security Alerts

Security alerts warn you of activities or events on the network that can cost you in terms of lost data, unauthorized access to the network, or traffic that matches known security threats. Security alerts are raised by repeated events that could dramatically affect network security. For example, if a rogue AP is detected, that represents a potential security problem. If a client connects to a rogue AP, that could be even worse.

Juniper Mist lists all security alerts except those that relate to intrusion detection and prevention (IDP) or URL filtering on the Monitor > Alerts page. You can find IDP and URL filtering events and their severity on the **Site** > **WAN Edge** > **Secure WAN Edge IDP/URL Events** page.

Table 5: Security Alerts by Severity

Severity	Alert Name
Critical	Client Connection to rogue AP detected
	Rogue AP detected

Table 5: Security Alerts by Severity *(Continued)*

Severity	Alert Name
Informational	Air Magnet Scan detected
	EAP Handshake Flood detected
Warning	Active Watched Station detected
	Adhoc Network detected
	BSSID Spoofing detected
	Disassociation Attack detected
	EAP Dictionary Attack detected
	EAP Failure Injection detected
	EAP Spoofed Success detected
	EAPOL-Logoff Attack detected
	ESL Hung
	ESL Recovered
	ESSID Jack detected
	Excessive Clients detected
	Excessive EAPOL-Start detected
	Fake AP Flooding detected
	Honeypot SSID detected
	IDP attack detected
	Monkey Jack detected

Table 5: Security Alerts by Severity *(Continued)*

Severity	Alert Name
	Out of Sequence detected
	Repeated Client Authentication Failures
	Replay Injection detected - KRACK Attack
	SSID Injection detected
	Security Policy Violation
	TKIP ICV Attack
	URL blocked
	Vendor IE Missing
	Zero SSID Association Request detected

Configure Alerts and Email Notifications

SUMMARY

Enable the alerts that you want to see on the Alerts dashboard. Optionally, enable email notifications for issues that you want to monitor closely.

Video Overview

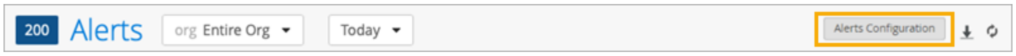
This video provides an overview of the procedure for configuring alerts.

Video: Alert Configuration Overview

Procedure

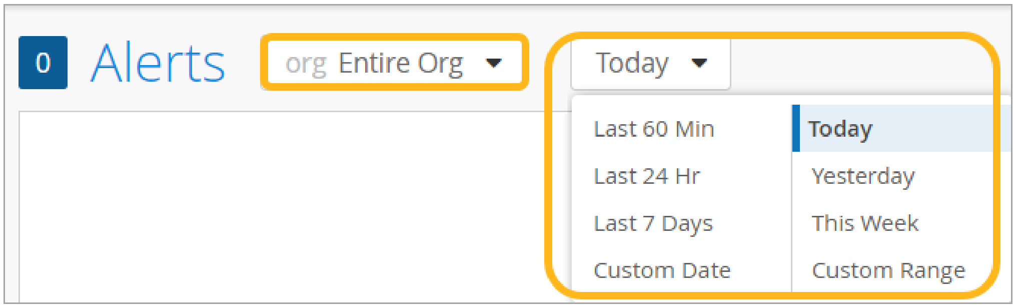
To configure alerts:

1. From the left menu, select **Monitor** > **Alerts**.
2. Click the **Alerts Configuration** button near the top-right corner of the page.

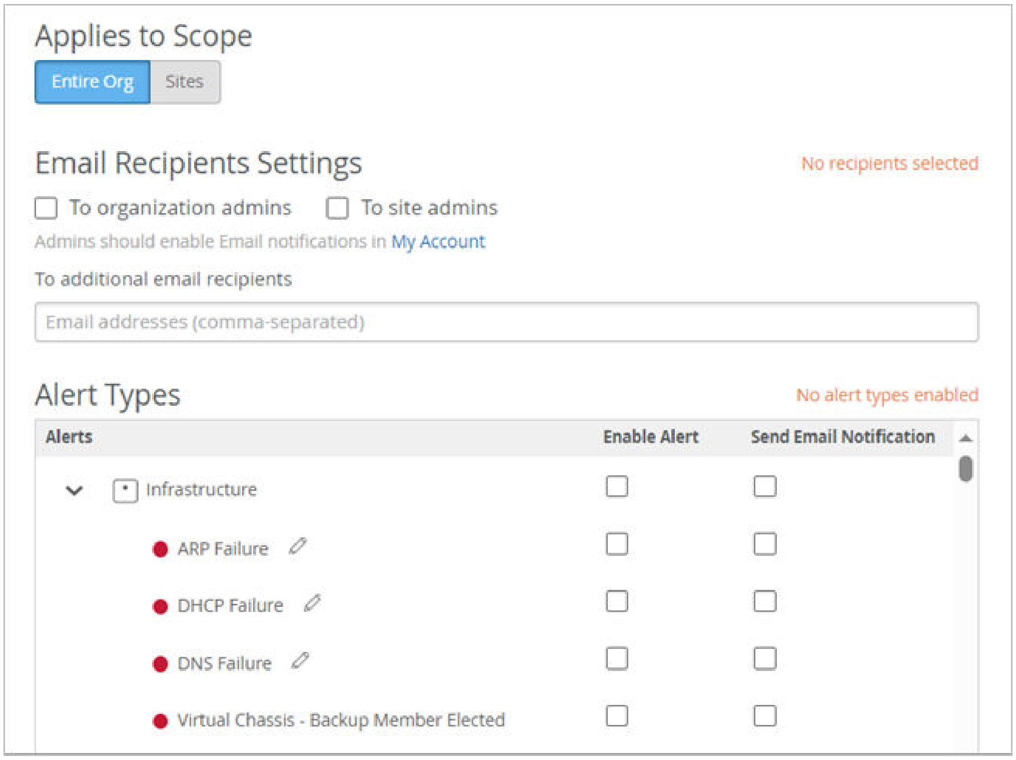


3. At the top of the page, select the context and time period.

   The context can be your entire organization or a single site. There are various options for the time period, such the last 60 minutes, the last 7 days, or a date range.



4. Select the scope, email notification settings (optional) and the alerts to show on the Alerts page.



Email Recipients Settings

No recipients selected

□ To organization admins □ To site admins

Admins should enable Email notifications in My Account

To additional email recipients

Email addresses (comma-separated)

Alert Types

No alert types enabled

Alerts	Enable Alert	Send Email Notification
Infrastructure	□	□
● ARP Failure	□	□
● DHCP Failure	□	□
● DNS Failure	□	□
● Virtual Chassis - Backup Member Elected	□	□

   a. Select the scope.

   - **Entire Org**—Click this button to configure the alerts for the entire organization.

- **Sites**—Click this button to configure the alerts for one or more sites that you want to monitor differently than the org. To identify the site(s), click the **Sites** button, then click the plus sign, and then click a site. Repeat as needed to add more sites to the list.

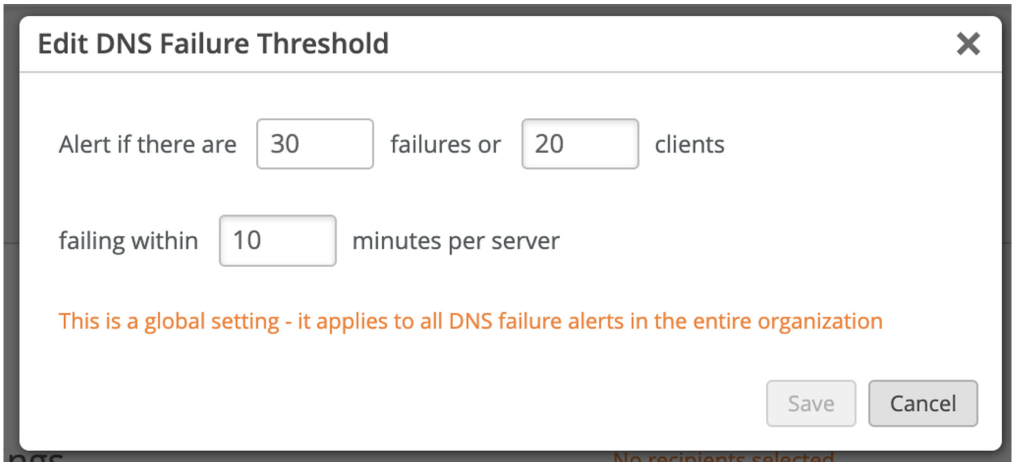
b. (Optional) Enable email notifications for alerts that you want to monitor closely.

- In the **Email Recipients Settings** section, identify the people to receive the email notifications:
  - **To organization admins**—Notifications will be sent to all admins whose permissions allow access to the entire organization.
  - **To site admins**—Notifications will be sent to all admins whose permissions allow access to the sites that you identified in the scope section.
  - **To additional email recipients**—Notifications will be sent to all email addresses that you enter in this box. This option is useful if you want to send notifications to personnel who do not have admin accounts for your Juniper Mist organization. To enter multiple email addresses, separate them with commas.
- In the **Alert Types** section, select the **Send Email Notification** check boxes for the alerts that you want to send emails for. For information about the various alerts, see "Juniper Mist Alert Types" on page 100.

c. In the **Alert Types** section, select the **Enable Alert** check boxes for the alerts that you want to see on the Alerts page. For information about the various alerts, see "Juniper Mist Alert Types" on page 100.

d. If the alert has a pencil icon, click it to configure the settings.

For example, when you click the pencil icon for DNS Failure, you can set the alert threshold by entering the number of failures and the number of clients that are impacted within the specified period of time. In this example, the alert occurs if a server has 30 failures or 20 impacted clients within a 10 minute period.



Edit DNS Failure Threshold

Alert if there are 30 failures or 20 clients

failing within 10 minutes per server

This is a global setting - it applies to all DNS failure alerts in the entire organization

5. After enabling all desired alerts and notifications, click **Save** at the top-left corner of the Alerts Configuration page.

5

CHAPTER

Get Started with Marvis

Marvis Virtual Network Assistant Overview

SUMMARY

Get familiar with the many features that are available with Marvis Virtual Network Assistant.

Marvis® Virtual Network Assistant is a virtual network assistant that streamlines network operations, simplifies troubleshooting, and provides an enhanced user experience. With real-time network visibility, Marvis provides a comprehensive view of your network from an organizational level to a client level with detailed insights.

Video: NOW in 60: Marvis Virtual Network Assistant (VNA)

As Mist AI monitors your network, it constantly learns from the telemetry data it collects. Marvis uses this data to deliver better insights and automation that are customized for your network.

Mist AI collects data from wireless LAN (WLAN), LAN, and WAN domains in your network. In addition to Juniper devices, Marvis also provides visibility into third-party switches connected to Juniper access points (APs) through Link Layer Discovery Protocol (LLDP). Marvis can provide health statistics for third-party switches. Examples include Power over Ethernet (PoE) compliance status, misconfigured VLANs, and switch uptime.

Marvis proactively identifies issues, interprets the scope and magnitude of the impact, identifies the root causes, and recommends fixes.

Here are the main components of Marvis:

- **Marvis Actions**—Marvis Actions is a one-stop information center that provides visibility into ongoing site-wide network issues that affect user experience in an organization. Marvis recommends fixes and provides insight into root causes. By default, the landing page of Marvis shows the Actions dashboard for an organization. All super users can view the Marvis Actions dashboard. Other admin roles can view the dashboard if they have organization-level access.

- **Marvis Minis**—Marvis Minis is a network digital twin that validates the network and application services for your network. By simulating user connections, Marvis Minis quickly detects and resolves issues before they impact users. Marvis Minis is always on and can detect issues even when clients are not connected to the network. In addition to detecting issues, it also ascertains the overall impact of the issue—that is, whether the issue impacts an entire site, a specific switch, WLAN, VLAN, server, or AP.

- **Conversational Assistant**—Marvis's AI-based conversation interface enables you to ask questions and get actionable insights into your network in no time. Marvis uses Natural Language Processing (NLP) with Natural Language Understanding (NLU) to contextualize requests, which accelerates the troubleshooting workflow. The conversational assistant provides real-time answers for your queries related to troubleshooting and documentation.

- **Marvis Client**—A software agent installed on client devices such as a mobile phone or laptop to collect the client's parameters that help represent its network view. The Marvis Android client, along with the Zebra wireless insights, provides enhanced telemetry and visibility into the Zebra client experience.

- **Marvis Query Language**—A structured format for asking Marvis a question to get data to monitor or troubleshoot your users' experiences and evaluate the overall health of your network.

With additional updates in 2023, Marvis provides even more functionality, including integrations with ChatGPT, Microsoft Teams, and Zoom. Watch this video to learn more.

Video: Marvis + Chat GPT + Zoom Integration Demo

Subscriptions for Marvis

To use Marvis, you must have the following active subscriptions in association with the Wireless Assurance, WAN Assurance, or Wired Assurance base license:

- Marvis for Wired

- Marvis for WAN

- Marvis for Wireless

You'll need an Assurance subscription and a Marvis subscription per device.

For more information about subscription options, activating subscriptions, and related topics, see the Juniper Mist Management Guide.

RELATED DOCUMENTATION

https://www.juniper.net/us/en/products/cloud-services.html

6

CHAPTER

Marvis Actions

Marvis Actions Overview

SUMMARY

Get started with Marvis Actions and get familiar with the major features of the Marvis Actions dashboard.

IN THIS SECTION

What Are Marvis Actions?

Marvis® leverages the Mist AI to identify the root cause of issues. Marvis can automatically fix issues (self-driving mode) or recommend actions that require user intervention (driver-assist mode). The Marvis Actions page lists the high-impact network issues that Marvis detects. Marvis Actions also displays the recommended actions for your organization's network. Marvis Actions provides insight into issues across the wired, WAN, and wireless networks, at the managed service provider (MSP) level, organization level, and site level. With Marvis Actions, you can track firmware compliance on APs, identify bad cables, locate L2 loops, detect WAN link outages, and more—all from a single page.

With real-time AI-native insight into your network, Marvis Actions enables proactive issue detection and resolution, resulting in a significant reduction in troubleshooting effort and time.

This video provides an introduction to Marvis Actions.

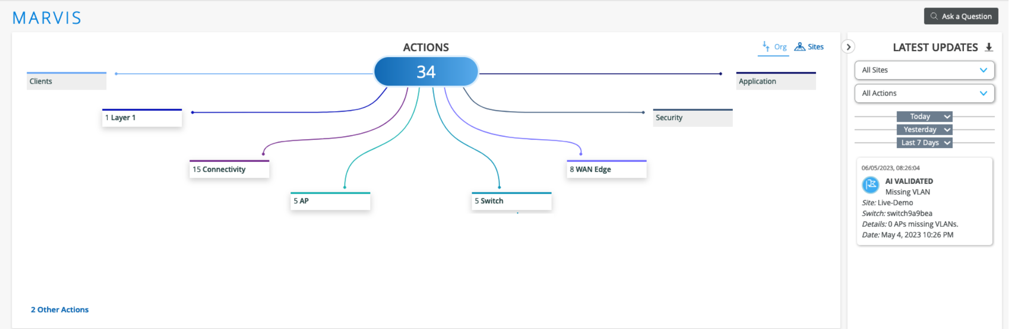
Video: Marvis Actions

Marvis Actions Dashboard

The Marvis Actions dashboard is a one-stop information center that provides visibility into ongoing site-wide network issues that affect user experience in an organization. Super users can view Marvis Actions. Users with other roles can view Marvis Actions if they are not assigned to any site. You can review the information to prioritize the issues that need immediate attention.

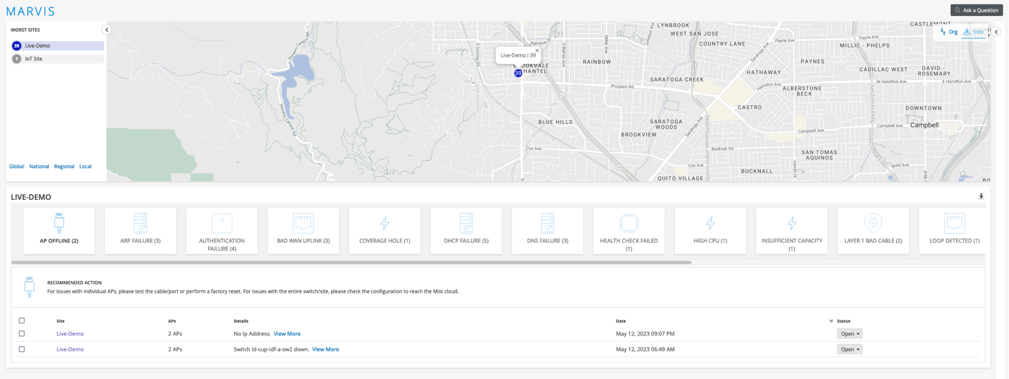
To view the Marvis Actions dashboard, select **Marvis > Marvis Actions** from the left menu of the Juniper Mist™ portal.

Here’s what the Marvis Actions page looks like. You'll notice that the page displays the information under different categories. Marvis indicates the number of issues detected for a category. For example, in the following screenshot, you'll notice that Marvis lists 15 issues for the Connectivity category.



06/05/2023, 08:26:04
AI VALIDATED
Missing VLAN
Site: Live-Demo
Switch: switch9a9bea
Details: 0 APs missing VLANs.
Date: May 4, 2023 10:26 PM

You can also view the issues for a site by selecting the **Sites** tab. The **Sites** tab displays a Google Maps view of all sites and issues detected.



RECOMMENDED ACTION
For issues with individual APs, please test the cable/port or perform a factory reset. For issues with the entire switch/site, please check the configuration to reach the Mist cloud.

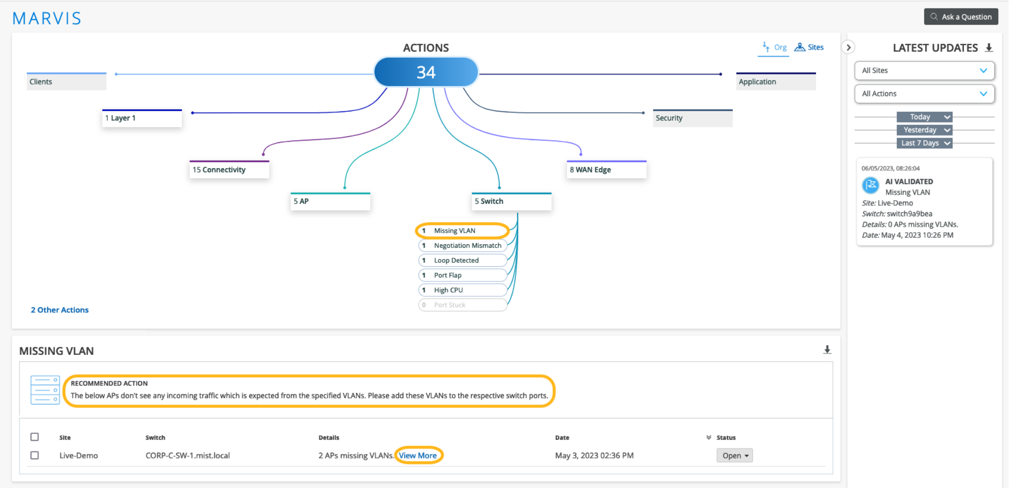
☐	Site	APs	Details	Date	Status
☐	Live-Demo	2 APs	No Ip Address. View More	May 12, 2023 09:07 PM	Open
☐	Live-Demo	2 APs	Switch ld-cup-idf-a-sw2 down. View More	May 12, 2023 06:49 AM	Open

Detailed View of Issues and Marvis Recommended Actions

Each category has a group of actions under it. Each action can have one or multiple issues associated with it. If Marvis does not detect any anomalies associated with an action, the action appears dimmed.

You can click a category to view the actions under that category. If you click an action, you'll see a detailed view, which includes the issue and recommended action. Marvis provides a recommended action for all issues.

Here’s the Marvis Actions view after drilling down into the Missing VLAN action under the Switch category. Notice that Marvis provides the details of the site, switch, and the issue (two APs with missing VLANs). You’ll also see that the recommended solution from Marvis is to add the VLAN configuration to the switch configuration.



06/05/2023, 08:26:04

AI VALIDATED

Missing VLAN

Site: Live-Demo

Switch: switch9a9bea

Details: 0 APs missing VLANs.

Date: May 4, 2023 10:26 PM

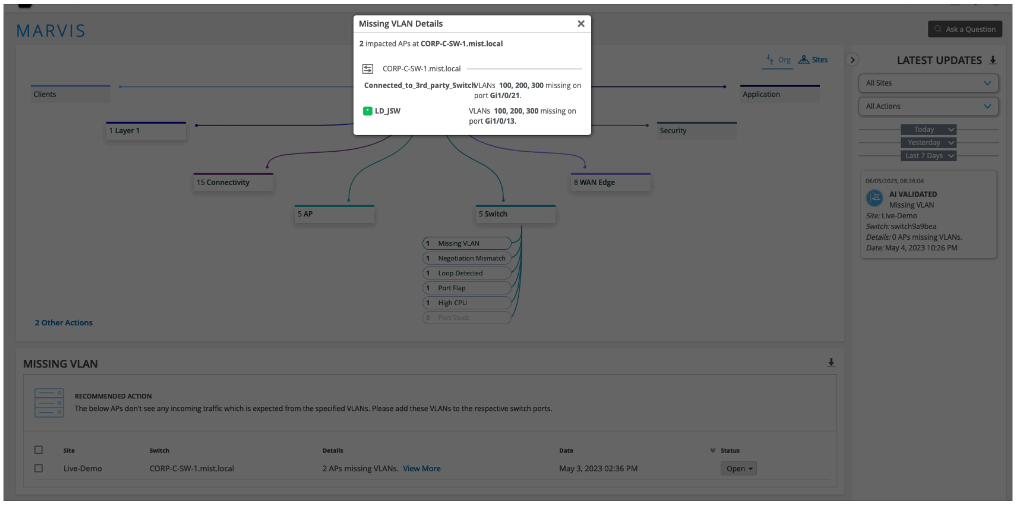
MISSING VLAN

RECOMMENDED ACTION

The below APs don't see any incoming traffic which is expected from the specified VLANs. Please add these VLANs to the respective switch ports.

□	Site	Switch	Details	Date	Status
□	Live-Demo	CORP-C-SW-1.mist.local	2 APs missing VLANs. View More	May 3, 2023 02:36 PM	Open ▾

You can use the **View More** link in the **Details** column to view specific details about the ports on which the VLANs are missing. Here's an example of the page showing the port details.



Missing VLAN Details ✕

2 impacted APs at **CORP-C-SW-1.mist.local**

CORP-C-SW-1.mist.local

Connected_to_3rd_party_Switch	VLANs **100, 200, 300** missing on port **Gi1/0/21**.
LD_JSW	VLANs **100, 200, 300** missing on port **Gi1/0/13**.

MARVIS
Ask a Question
Org
Sites
Clients
Application
1 Layer 1
Security
15 Connectivity
8 WAN Edge
5 AP
5 Switch
1 Missing VLAN
1 Negotiation Mismatch
1 Loop Detected
1 Port Flap
1 High CPU
0 Port Stuck
2 Other Actions
LATEST UPDATES
All Sites
All Actions
Today
Yesterday
Last 7 Days
06/05/2023, 08:26:04
AI VALIDATED
Missing VLAN
Site: Live-Demo
Switch: switch9a9bea
Details: 0 APs missing VLANs.
Date: May 4, 2023 10:26 PM
MISSING VLAN
RECOMMENDED ACTION
The below APs don't see any incoming traffic which is expected from the specified VLANs. Please add these VLANs to the respective switch ports.
Site Switch Details Date Status
Live-Demo CORP-C-SW-1.mist.local 2 APs missing VLANs. View More May 3, 2023 02:36 PM Open

Downloadable List of Issues

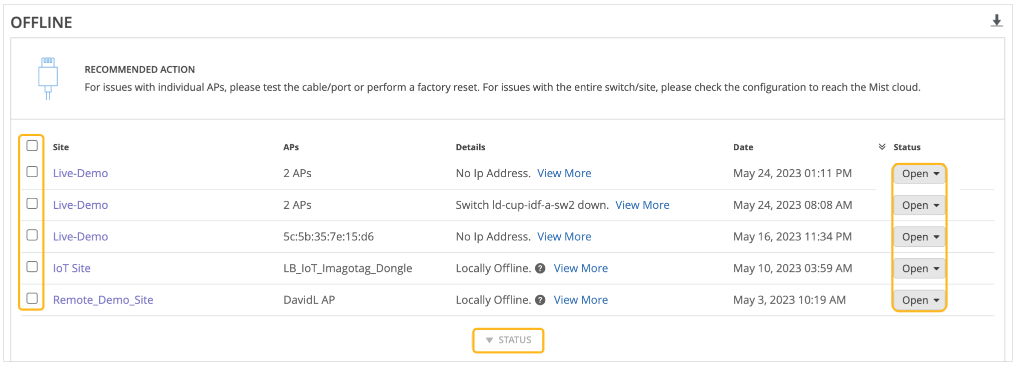
You can download the list of issues to a .CSV file format. The CSV file contains all the details visible on the Actions page, including the reason for failure and the device details. You can find the download (down arrow) icon on the upper-right corner of the Details section.

Issue Resolution

After you resolve an issue, you can change the status of an issue or multiple issues.

- To update one issue—Click the **Status** button at the end of the row, and then click the new status.

- To update multiple issues—Select the check box for each issue to update, or select the top check box to select all issues. Click the **Status** button at the bottom of the page, and then click the new status. This status will be applied to all selected issues.

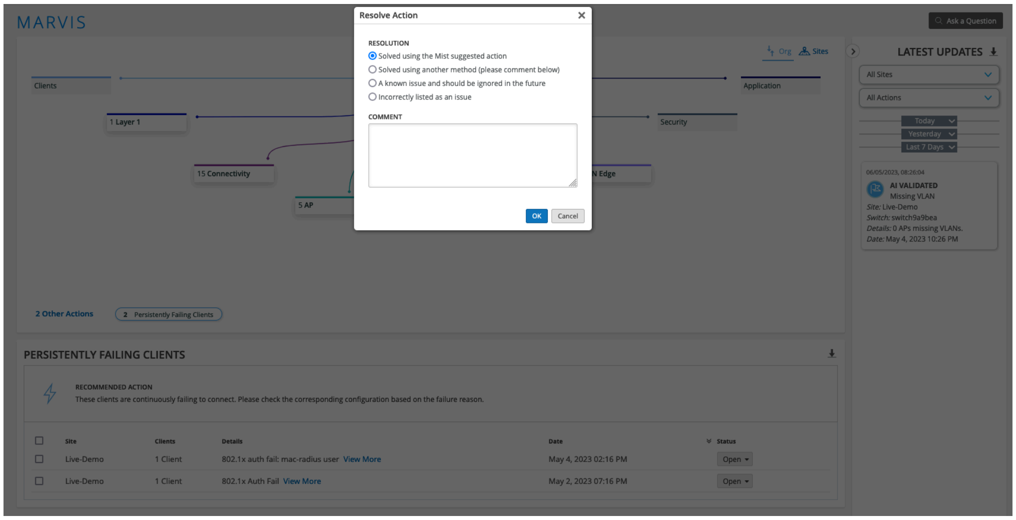


OFFLINE

RECOMMENDED ACTION
For issues with individual APs, please test the cable/port or perform a factory reset. For issues with the entire switch/site, please check the configuration to reach the Mist cloud.

□	Site	APs	Details	Date	Status
□	Live-Demo	2 APs	No Ip Address. View More	May 24, 2023 01:11 PM	Open ▾
□	Live-Demo	2 APs	Switch ld-cup-idf-a-sw2 down. View More	May 24, 2023 08:08 AM	Open ▾
□	Live-Demo	5c:5b:35:7e:15:d6	No Ip Address. View More	May 16, 2023 11:34 PM	Open ▾
□	IoT Site	LB_IoT_Imagotag_Dongle	Locally Offline. ? View More	May 10, 2023 03:59 AM	Open ▾
□	Remote_Demo_Site	DavidL AP	Locally Offline. ? View More	May 3, 2023 10:19 AM	Open ▾

Marvis prompts you for feedback, which Mist uses internally to determine the efficacy of the action.



Resolve Action

RESOLUTION
● Solved using the Mist suggested action
○ Solved using another method (please comment below)
○ A known issue and should be ignored in the future
○ Incorrectly listed as an issue

COMMENT

OK Cancel

06/05/2023, 08:26:04
AI VALIDATED
Missing VLAN
Site: Live-Demo
Switch: switch9a9bea
Details: 0 APs missing VLANs.
Date: May 4, 2023 10:26 PM

PERSISTENTLY FAILING CLIENTS

RECOMMENDED ACTION
These clients are continuously failing to connect. Please check the corresponding configuration based on the failure reason.

□	Site	Clients	Details	Date	Status
□	Live-Demo	1 Client	802.1x auth fail: mac-radius user View More	May 4, 2023 02:16 PM	Open ▾
□	Live-Demo	1 Client	802.1x Auth Fail View More	May 2, 2023 07:16 PM	Open ▾

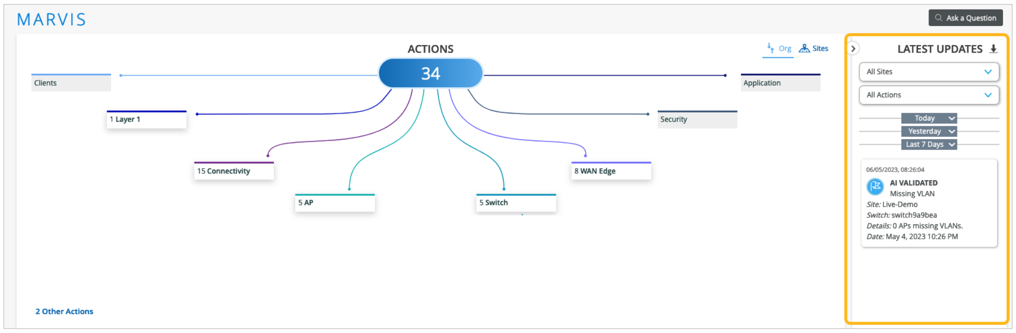
Latest Updates About Issues

The LATEST UPDATES section on the right of the Marvis Actions page provides a list of issues that were resolved over the past seven days. Marvis classifies the issues under one of the following states:

- **AI Validated**—Lists issues (such as an AP missing a VLAN) that are no longer active. If you update the status of an issue to Resolve, Marvis verifies that the issue is resolved and classifies the issue as AI Validated. If you fix an issue but don't update the status, Marvis detects that the issue is resolved and moves it to the Latest Updates section.

- **Resolved**—Lists automated actions (such as auto upgrade, auto RMA) or manual actions (such as manual AP upgrade or manual RMA request) that completed successfully. Marvis classifies an issue as Resolved only if you trigger the action from the Actions page.

- **Reoccurring Issue**—Lists resolved issues that are either still not resolved or have reoccurred. At times, Marvis might find that an issue you marked as resolved is still not resolved completely. Marvis then classifies the issue as a reoccurring issue.



06/05/2023, 08:26:04
AI VALIDATED
Missing VLAN
Site: Live-Demo
Switch: switch9a9bea
Details: 0 APs missing VLANs.
Date: May 4, 2023 10:26 PM

You can click the download (down arrow) icon next to the Latest Updates text to download the list of actions for your organization in CSV format. You can download either the complete list or the list for a specific type of failure.

Video: Troubleshooting Bad Signal Strength

In this video demo, Marvis recommends actions for bad signal strength.

Video: Marvis Actions Example

Subscription Requirements for Marvis Actions

SUMMARY

Understand how your subscriptions determine the actions that you'll see on the Actions dashboard. Also get familiar with the different actions that are available for different subscription types (Marvis for Wired, Marvis for Wireless, and Marvis for WAN).

IN THIS SECTION

Subscription Types

Your Marvis subscriptions determine the actions that you'll see on the Actions dashboard. Be aware of the requirements for the *types* of subscription and purchase the subscriptions that you need for your network.

Different Marvis subscriptions enable different Marvis actions. For example, you need a Marvis for Wired subscription to see Wired actions. The actions for each type of subscription are shown in the tables in the section of this topic.

NOTE: If you are using a trial subscription type, you can view all Marvis Actions until the trial subscription ends.

Available Actions for Your Subscriptions

Available actions vary for different subscriptions, as appropriate for the types of devices that are associated with these subscriptions. The following tables show the available actions for each subscription type.

Table 7: Marvis for Wired Actions

Category	Marvis for Wired Actions
Connectivity	Authentication Failure
	DHCP Failure
Switch	Negotiation Incomplete
	MTU Mismatch
	Loop Detected
	Network Port Flap
	High CPU
	Port Stuck

Table 7: Marvis for Wired Actions *(Continued)*

Category	Marvis for Wired Actions
	Traffic Anomaly
Other Actions	Persistently Failing Clients
	Access Port Flap

Table 8: Marvis for WAN Actions

Category	Marvis for WAN Actions
WAN Edge	MTU Mismatch
	Bad WAN Uplink
	VPN Path Down
	Non-Compliant

Table 9: Marvis for Wireless Actions

Category	Marvis for Wireless Actions
Layer 1	Bad Cable
Connectivity	Authentication Failure
	DHCP Failure
	ARP Failure
	DNS Failure
AP	Offline
	Health Check Failed
	Non-compliant

Table 9: Marvis for Wireless Actions *(Continued)*

Category	Marvis for Wireless Actions
	Coverage Hole
	Insufficient Capacity
	AP Loop Detected
Switch	Missing VLAN
Other Actions	Persistently Failing Clients

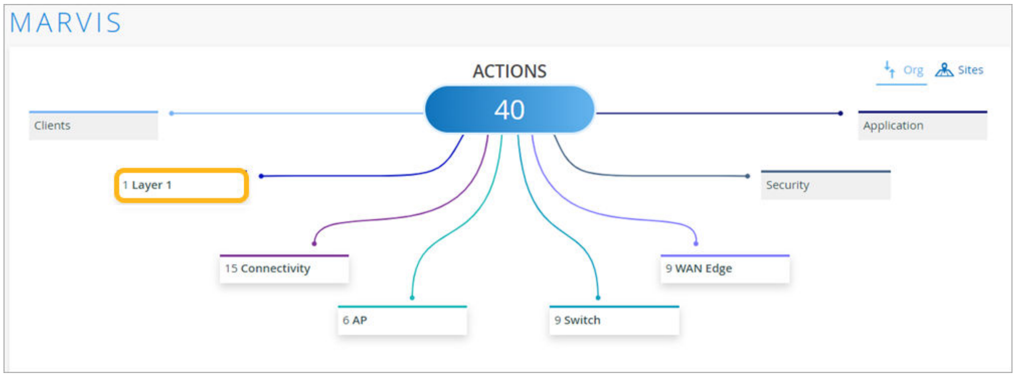
Layer 1 Actions

SUMMARY

Use the Actions dashboard to resolve Layer 1 issues.

IN THIS SECTION

When you click the Layer 1 button on the Action dashboard, all available Layer 1 actions appear. Currently there is only one type of action for this category: bad cable.



NOTE: Your subscriptions determine the actions that you can see on the Actions dashboard. For more information, see "Subscription Requirements for Marvis Actions " on page 121.

Bad Cable

Marvis can detect a faulty cable that is connected to an access point (AP), a switch, or a WAN Edge device.

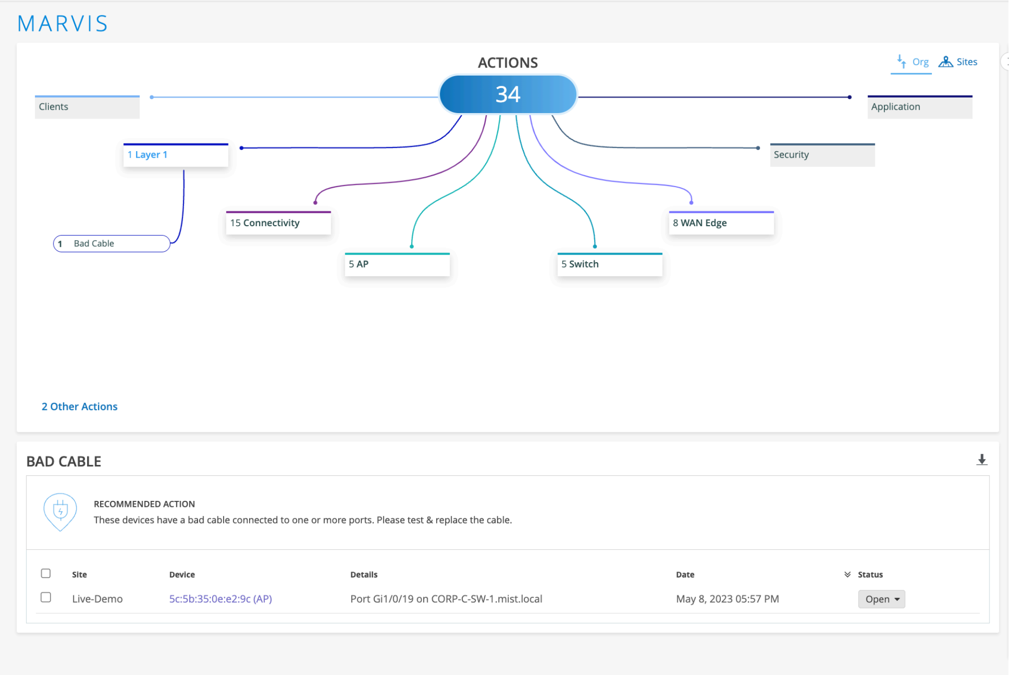
A faulty cable is one of the root causes of network issues, which manifest as user experience issues. It is a difficult and time-consuming task to manually identify a faulty cable. Marvis can detect bad cables easily by using cable data such as frame errors, link statistics, link errors, and traffic patterns.

A bad cable action indicates cable issues that APs, Switches, and WAN edge devices detect at a site. The details section indicates if a switch, an AP, or a WAN edge device detected the issue.

For a WAN Edge detected issue, you'll need to perform the following steps:

- Ensure that the duplex setting is full duplex on both sides of the link.
- Change the cable to rule out issues due to a defective cable.
- Change the SFP and check the status.
- Change the port to rule out any NIC card issues.
- Change the Layer2 device (modem or router).

The following sample illustrates the issue:



BAD CABLE

RECOMMENDED ACTION
These devices have a bad cable connected to one or more ports. Please test & replace the cable.

□	Site	Device	Details	Date	Status
□	Live-Demo	5c:5b:35:0e:e2:9c (AP)	Port Gi1/0/19 on CORP-C-SW-1.mist.local	May 8, 2023 05:57 PM	Open

After you fix the issue, Mist AI monitors the AP, switch, or WAN edge for a certain period and ensures that the cable issue is indeed resolved. Hence, it might take up to 24 hours for the Bad Cable action to automatically resolve and appear in the Latest Updates section.

Video: Bad Cable

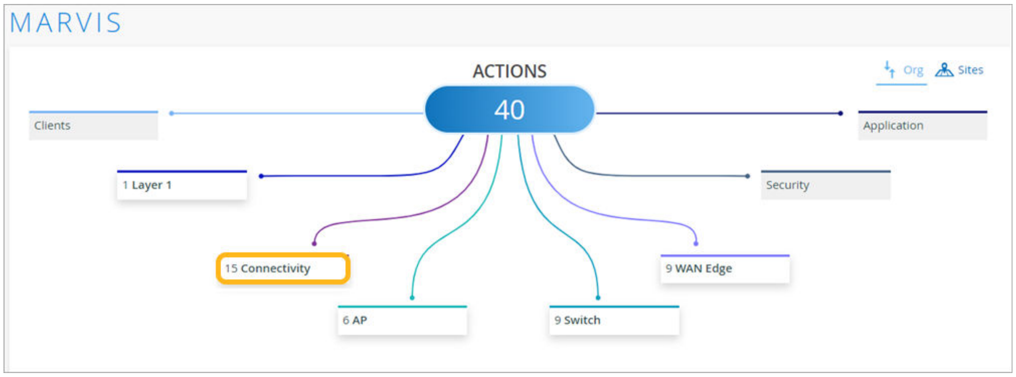
Connectivity Actions

SUMMARY

Use the Actions dashboard to resolve client connectivity failures.

IN THIS SECTION

When you click the Connectivity button on the Actions dashboard, you'll see a list of all available actions. You can then click an action to investigate further. Available actions are described later in this topic.



NOTE: Your subscriptions determine the actions that you can see on the Actions dashboard. For more information, see "Subscription Requirements for Marvis Actions " on page 121.

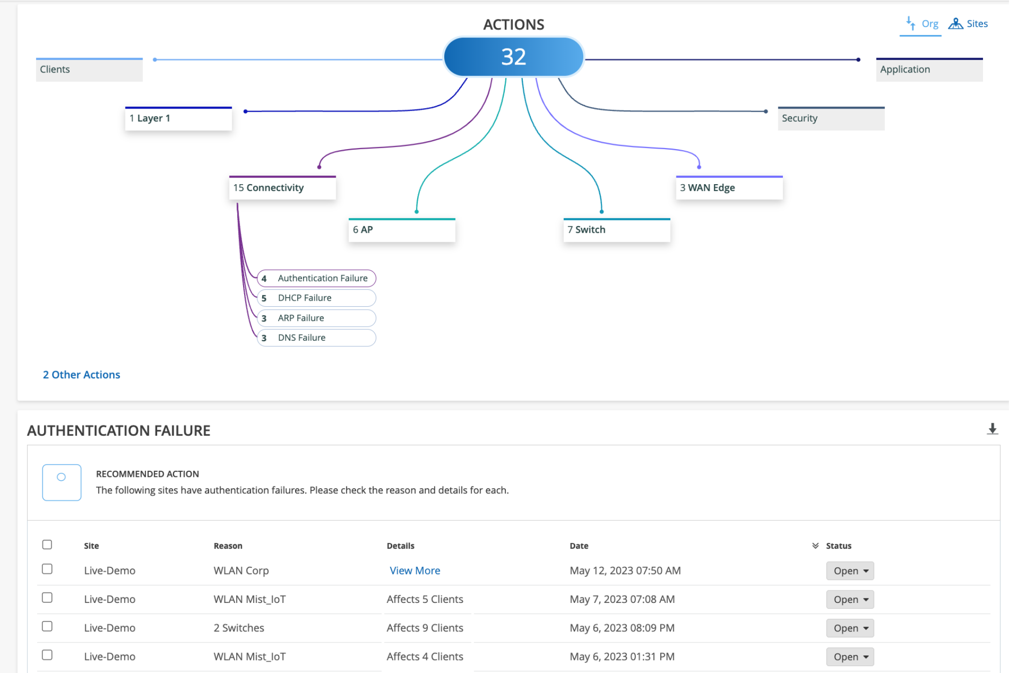
How Are Connectivity Failures Detected?

Marvis uses anomaly detection or scope analysis to detect connectivity failures, as follows:

- **Anomaly Detection**—Marvis detects issues when they start to occur at your site, such as multiple clients failing for the same reason. Anomalies are failures that occur across most, but not all, devices on your site. The Details page (Anomaly Detection Event Card), which you can open with the **View More** link, lists the component that probably caused the failure. For more information about anomaly detection, see "Anomaly Detection Event Card" on page 155.

  After you fix the issue, the action automatically resolves and appears in the Latest Updates section within 24 hours.

- **Scope Analysis**—When the failure rate across all clients at your site is 100 percent, Marvis performs a scope analysis on the issue to determine the root cause of such a failure. Marvis provides the details of the affected clients—MAC address, VLAN, and WLAN for which Marvis triggers the scope anomaly. Marvis indicates the issue that needs to be fixed, whether it is a RADIUS, Domain Name System (DNS), or Dynamic Host Configuration Protocol (DHCP) server; a WLAN; or an access point (AP). Here is an example that shows how Marvis reports an issue based on scope analysis:



AUTHENTICATION FAILURE

RECOMMENDED ACTION
The following sites have authentication failures. Please check the reason and details for each.

	Site	Reason	Details	Date	Status
□	Live-Demo	WLAN Corp	View More	May 12, 2023 07:50 AM	Open
□	Live-Demo	WLAN Mist_IoT	Affects 5 Clients	May 7, 2023 07:08 AM	Open
□	Live-Demo	2 Switches	Affects 9 Clients	May 6, 2023 08:09 PM	Open
□	Live-Demo	WLAN Mist_IoT	Affects 4 Clients	May 6, 2023 01:31 PM	Open

After you fix the issue, the action automatically resolves and appears in the Latest Updates section within an hour.

Authentication Failure

The Authentication Failure action shows both 802.1x and preshared key (PSK) failures. Click the Authentication Failures button to see the impacted devices and the recommended actions in the lower part of the page.

NOTE: If you see a **View More** link in the Authentication Failure table, click the link to open the Event Card. For more information, see "Anomaly Detection Event Card" on page 155.

802.1x Failures

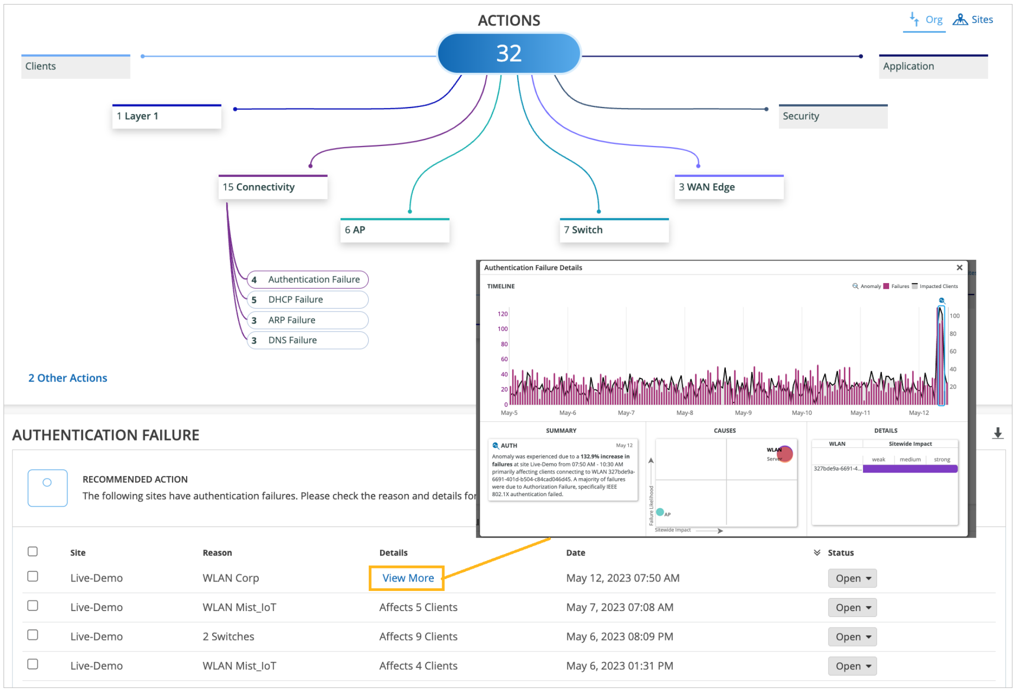
The 802.1x failures include the following:

- **RADIUS Server Missing Events**: These events are triggered when a RADIUS server at a site does not respond to Extensible Authentication Protocol (EAP) requests. This failure to respond results in a high number of clients failing 802.1X authentication on the wireless LAN (WLAN). Marvis might detect failures across multiple APs broadcasting to the same 802.1x WLAN. These failures indicate that a

RADIUS server is either configured wrong or is missing from the network. In this case, you'll need to check if the RADIUS server is online and reachable.

- **RADIUS Missing AP Events**: These events are triggered when clients connecting to a few APs fail to authenticate to a WLAN that has a RADIUS server configured for EAP authentication. This RADIUS event indicates that you have not configured these APs as network access service (NAS) clients on the RADIUS server. You must add the missing APs to the RADIUS configuration to resolve the issue.

Here's an example that shows how Marvis Actions reports an 802.1x authentication failure. Note the Authentication Failure Details page showing the information:



AUTH May 12

Anomaly was experienced due to a **132.9% increase in failures** at site Live-Demo from 07:50 AM - 10:30 AM primarily affecting clients connecting to WLAN 327bde9a-6691-401d-b504-c84cad046d45. A majority of failures were due to Authorization Failure, specifically IEEE 802.1X authentication failed.

AUTHENTICATION FAILURE

RECOMMENDED ACTION

The following sites have authentication failures. Please check the reason and details for

□	Site	Reason	Details	Date	Status
□	Live-Demo	WLAN Corp	View More	May 12, 2023 07:50 AM	Open ▾
□	Live-Demo	WLAN Mist_IoT	Affects 5 Clients	May 7, 2023 07:08 AM	Open ▾
□	Live-Demo	2 Switches	Affects 9 Clients	May 6, 2023 08:09 PM	Open ▾
□	Live-Demo	WLAN Mist_IoT	Affects 4 Clients	May 6, 2023 01:31 PM	Open ▾

> **NOTE**: Marvis detects authentication failures even in wired-only deployments.

PSK Failures

Marvis detects PSK failures when an unusually high number of clients fail to authenticate to a PSK WLAN due to a PSK mismatch. To resolve PSK failure errors, you'll need to verify the PSK for your WLAN and clients. A possible cause could be a recent PSK change that was not communicated to users.

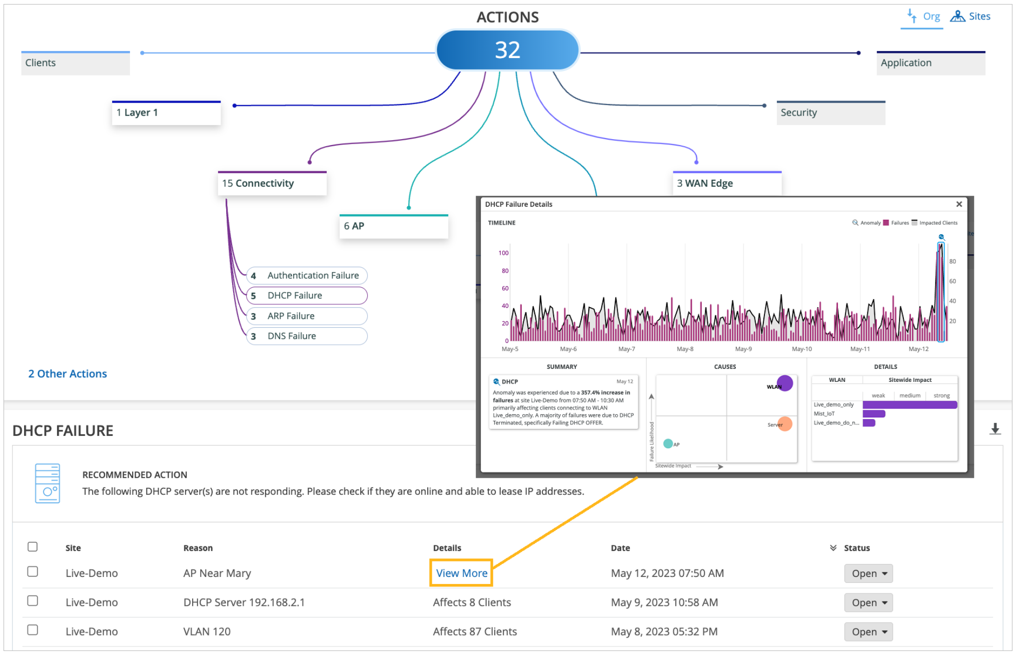
DHCP Failure

The DHCP Failure action appears when Marvis detects DHCP failures due to offline or unresponsive DHCP servers (DCHP timeouts).

Marvis provides details about these DHCP servers, enabling you to troubleshoot and resolve the problem quickly. When you see a DHCP Failure action, ensure that the DHCP servers are online and can lease IP addresses.

> **NOTE**: For wired-only deployments, you must enable DHCP snooping for Marvis to detect DHCP failures.

If you see a **View More** link in the DHCP Failure table, click the link to open the Event Card. For more information, see "Anomaly Detection Event Card" on page 155.



DHCP May 12

Anomaly was experienced due to a **357.4% increase in failures** at site Live-Demo from 07:50 AM - 10:30 AM primarily affecting clients connecting to WLAN Live_demo_only. A majority of failures were due to DHCP Terminated, specifically Failing DHCP OFFER.

DHCP FAILURE

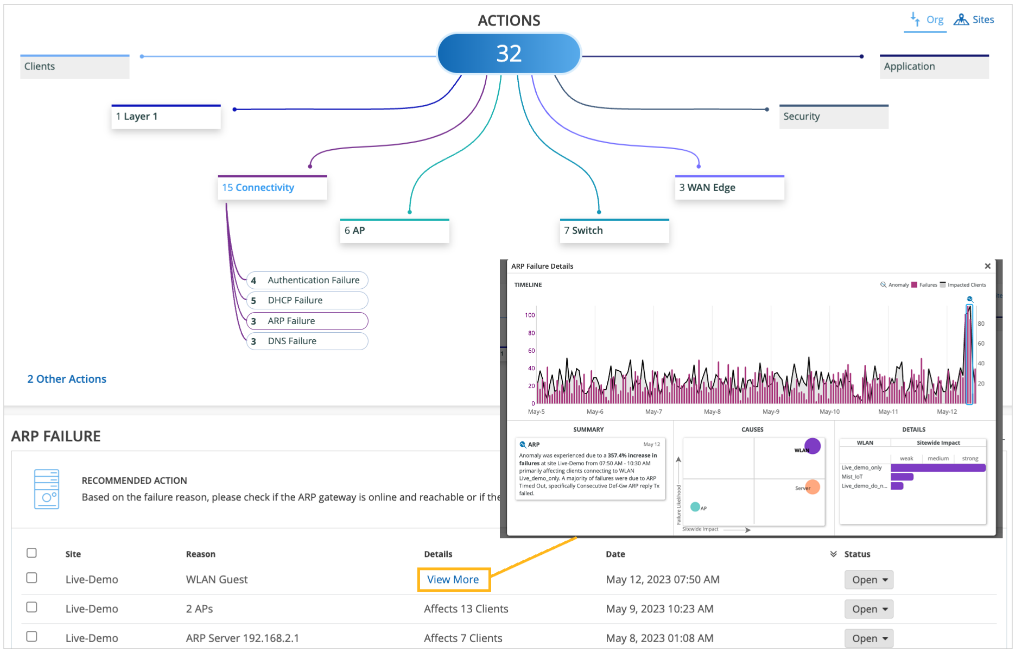
RECOMMENDED ACTION

The following DHCP server(s) are not responding. Please check if they are online and able to lease IP addresses.

□	Site	Reason	Details	Date	Status
□	Live-Demo	AP Near Mary	View More	May 12, 2023 07:50 AM	Open ▾
□	Live-Demo	DHCP Server 192.168.2.1	Affects 8 Clients	May 9, 2023 10:58 AM	Open ▾
□	Live-Demo	VLAN 120	Affects 87 Clients	May 8, 2023 05:32 PM	Open ▾

ARP Failure

An Address Resolution Protocol (ARP) Failure action appears when an unusually large number of clients experience issues with the ARP gateway. These issues include Gateway ARP timeout and excessive ARP. When you see an ARP Failure action, you must verify that the gateway is online and reachable. You must also ensure that the network is free of congestion.



ARP FAILURE

RECOMMENDED ACTION

Based on the failure reason, please check if the ARP gateway is online and reachable or if the

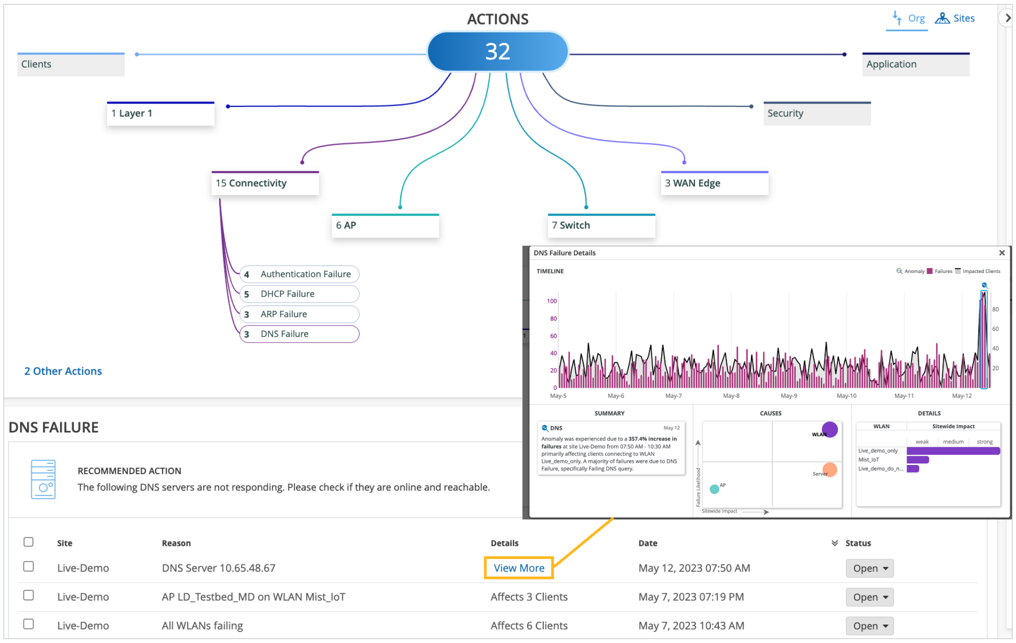
ARP May 12

Anomaly was experienced due to a **357.4% increase in failures** at site Live-Demo from 07:50 AM - 10:30 AM primarily affecting clients connecting to WLAN Live_demo_only. A majority of failures were due to ARP Timed Out, specifically Consecutive Def-Gw ARP reply Tx failed.

	Site	Reason	Details	Date	Status
□	Live-Demo	WLAN Guest	View More	May 12, 2023 07:50 AM	Open ▾
□	Live-Demo	2 APs	Affects 13 Clients	May 9, 2023 10:23 AM	Open ▾
□	Live-Demo	ARP Server 192.168.2.1	Affects 7 Clients	May 8, 2023 01:08 AM	Open ▾

DNS Failure

Marvis Actions detect unresponsive DNS servers for your site if a large number of clients experience DNS errors when using the network. If you see this action on your dashboard, you need to check that all your DNS servers are online and reachable.



DNS FAILURE

RECOMMENDED ACTION

The following DNS servers are not responding. Please check if they are online and reachable.

DNS May 12

Anomaly was experienced due to a **357.4% increase in failures** at site Live-Demo from 07:50 AM - 10:30 AM primarily affecting clients connecting to WLAN Live_demo_only. A majority of failures were due to DNS Failure, specifically Failing DNS query.

	Site	Reason	Details	Date	Status
□	Live-Demo	DNS Server 10.65.48.67	View More	May 12, 2023 07:50 AM	Open ▾
□	Live-Demo	AP LD_Testbed_MD on WLAN Mist_IoT	Affects 3 Clients	May 7, 2023 07:19 PM	Open ▾
□	Live-Demo	All WLANs failing	Affects 6 Clients	May 7, 2023 10:43 AM	Open ▾

NOTE: If you see a **View More** link in the DNS Failure table, click the link to open the Event Card. For more information, see "Anomaly Detection Event Card" on page 155.

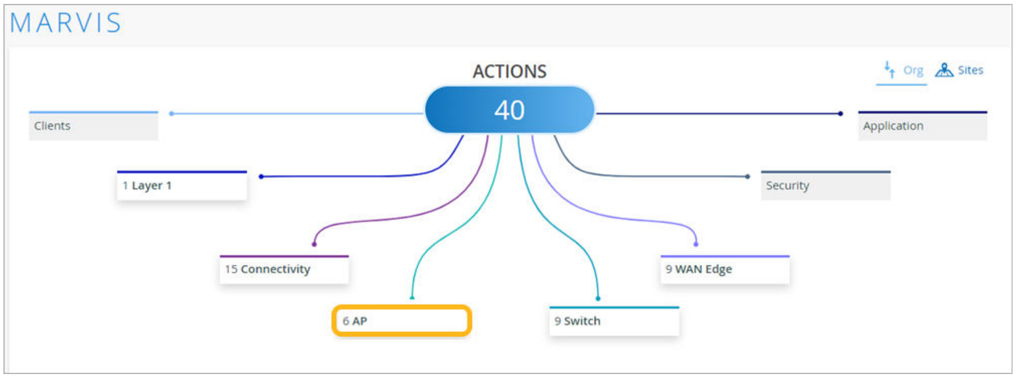
AP Actions

SUMMARY

Use the Actions dashboard to resolve issues affecting your access points (APs).

IN THIS SECTION

When you click the AP button on the Actions dashboard, you'll see a list of all available actions. You can then click an action to investigate further. Available actions are described later in this topic.



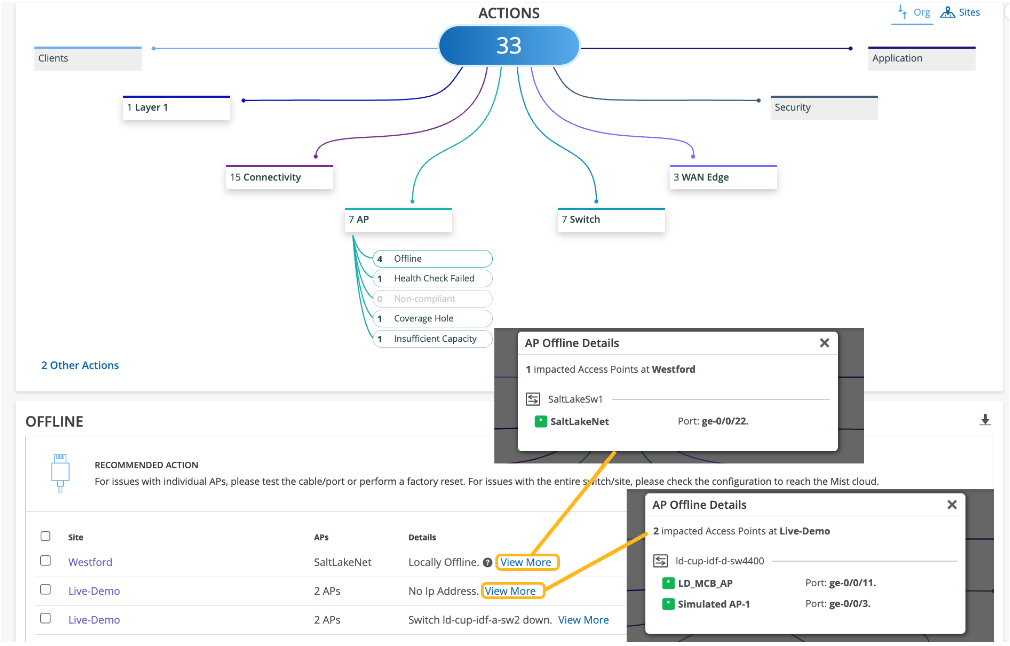
NOTE: Your subscriptions determine the actions that you can see on the Actions dashboard. For more information, see "Subscription Requirements for Marvis Actions " on page 121.

Offline

Marvis detects APs that are offline due to lack of power, loss of cloud connectivity, or any other issue. Marvis can determine the scope of Offline AP actions such as these:

- A site is down and all APs at the site have lost cloud connectivity.
- A switch is down and all APs connected to the switch have lost cloud connectivity.
- An AP is locally online (that is, the AP is heard locally but has lost cloud connectivity).
- An AP is locally offline (that is, the AP is not heard locally and has also lost cloud connectivity).

Here's an example of an Offline action where Marvis identifies three APs that are offline:



OFFLINE

RECOMMENDED ACTION
For issues with individual APs, please test the cable/port or perform a factory reset. For issues with the entire switch/site, please check the configuration to reach the Mist cloud.

☐	Site	APs	Details
☐	Westford	SaltLakeNet	Locally Offline. ? View More
☐	Live-Demo	2 APs	No Ip Address. View More
☐	Live-Demo	2 APs	Switch ld-cup-idf-a-sw2 down. View More

AP Offline Details ✕

1 impacted Access Points at **Westford**

SaltLakeSw1

🟩 **SaltLakeNet**	Port: **ge-0/0/22.**

AP Offline Details ✕

2 impacted Access Points at **Live-Demo**

ld-cup-idf-d-sw4400

🟩 **LD_MCB_AP**	Port: **ge-0/0/11.**
🟩 **Simulated AP-1**	Port: **ge-0/0/3.**

Health Check Failed

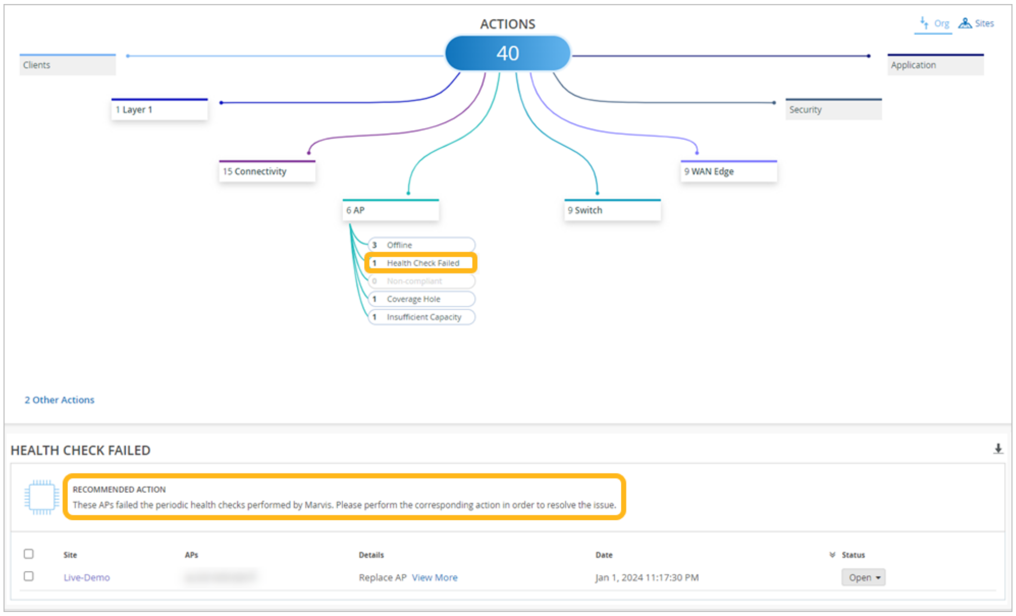
Marvis reports health check failures when it detects potential hardware or software issues.

Marvis shows the Health Check Failed action for these types of issues:

- Issues that cannot be debugged, meaning that the AP needs to be replaced.
- A software issue that a newer firmware resolves. You can use the **Upgrade** button to upgrade the firmware directly from this page.

NOTE: After you fix the hardware or software issue, Mist AI monitors the AP for a certain period and ensures that it is operating normally. Hence, it might take up to 24 hours for the Health Check Failed action to automatically resolve and appear in the Latest Updates section.

In this example, Marvis identifies an AP that failed the periodic health checks and needs to be replaced.



HEALTH CHECK FAILED

RECOMMENDED ACTION

These APs failed the periodic health checks performed by Marvis. Please perform the corresponding action in order to resolve the issue.

□	Site	APs	Details	Date	Status
□	Live-Demo	[redacted]	Replace AP View More	Jan 1, 2024 11:17:30 PM	Open ▾

Non-Compliant

Marvis monitors the firmware version running on all the APs at a site. The Non-Compliant action flags APs running a firmware version that is older than the version running on the other APs of the same model at the site. You can upgrade the APs from the Marvis Actions page without having to visit the site.

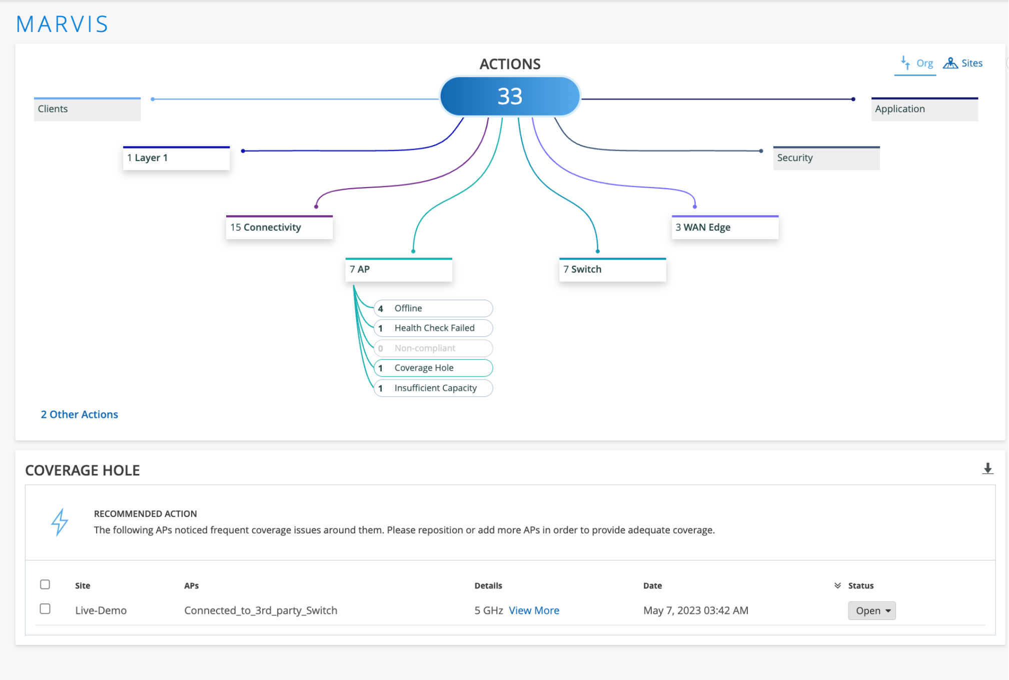
After you upgrade the APs to the proper version, the Non-Compliant action automatically resolves and appears in the Latest Updates section within 30 minutes.

Coverage Hole

The Coverage Hole action detects coverage issues at your site and provides a floor plan visual indicating the APs experiencing these issues. You can use this visual representation to locate areas with low coverage and make necessary improvements such as adding APs, upgrading AP models, changing the placement of existing APs, or increasing the power output of existing APs.

NOTE: You need to have a floor plan already set up in **Location Live View** to take advantage of the Coverage Hole visibility.

In the following example, Marvis pinpoints a site that is facing frequent coverage issues:



MARVIS

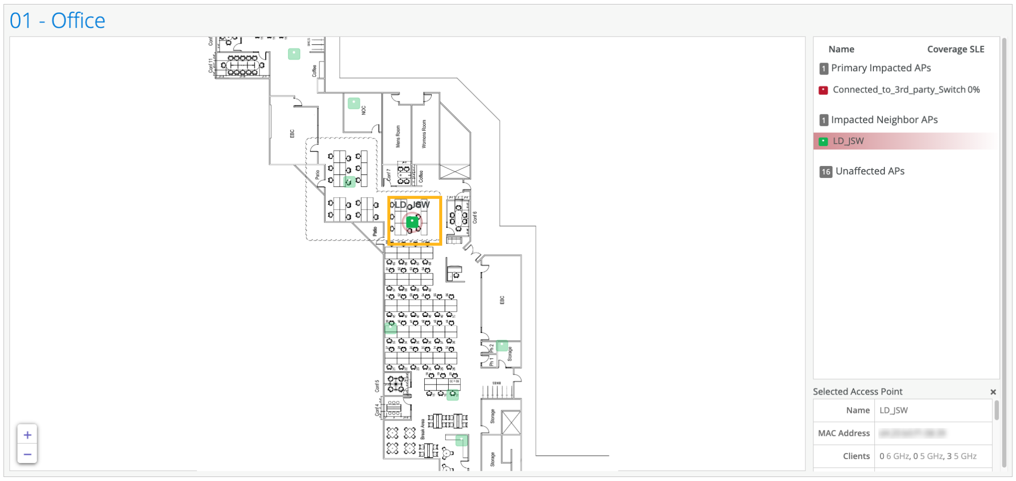
COVERAGE HOLE

RECOMMENDED ACTION

The following APs noticed frequent coverage issues around them. Please reposition or add more APs in order to provide adequate coverage.

□	Site	APs	Details	Date	Status
□	Live-Demo	Connected_to_3rd_party_Switch	5 GHz View More	May 7, 2023 03:42 AM	Open ▾

Here’s the floor plan visual showing the affected AP (highlighted):



01 - Office

Name	Coverage SLE
1 Primary Impacted APs	
🟥 Connected_to_3rd_party_Switch	0%
1 Impacted Neighbor APs	
🟩 LD_JSW	
16 Unaffected APs	

Selected Access Point ×

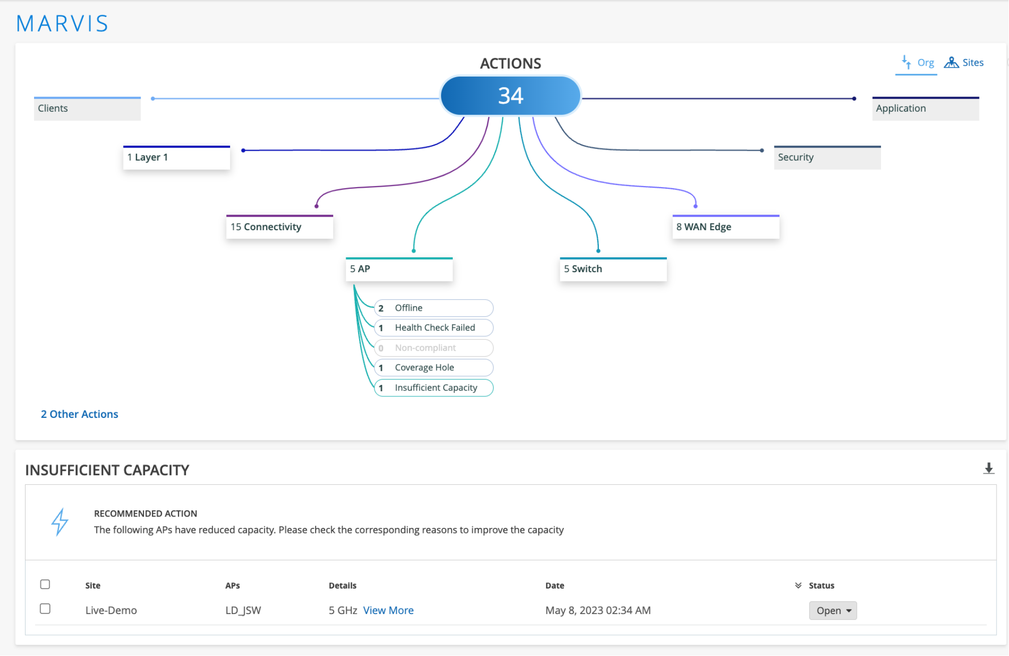
Name	LD_JSW
MAC Address	[redacted]
Clients	0 6 GHz, 0 5 GHz, 3 5 GHz

After you fix the issue in your network, Mist AI monitors the network for a certain period and ensures that the coverage is sufficient for the network. Hence, it might take up to 24 hours for the Coverage Hole action to automatically resolve and appear in the Latest Updates section.

Insufficient Capacity

The Insufficient Capacity action detects capacity issues related to an abnormal increase in an AP's utilization. This action usually occurs when client traffic peaks significantly. Marvis provides a floor plan visual indicating the APs experiencing capacity issues. You can use this visual representation to find the affected APs and make design improvements.

NOTE: You need to have a floor plan already set up in **Location Live View** to take advantage of the Insufficient Capacity visibility.



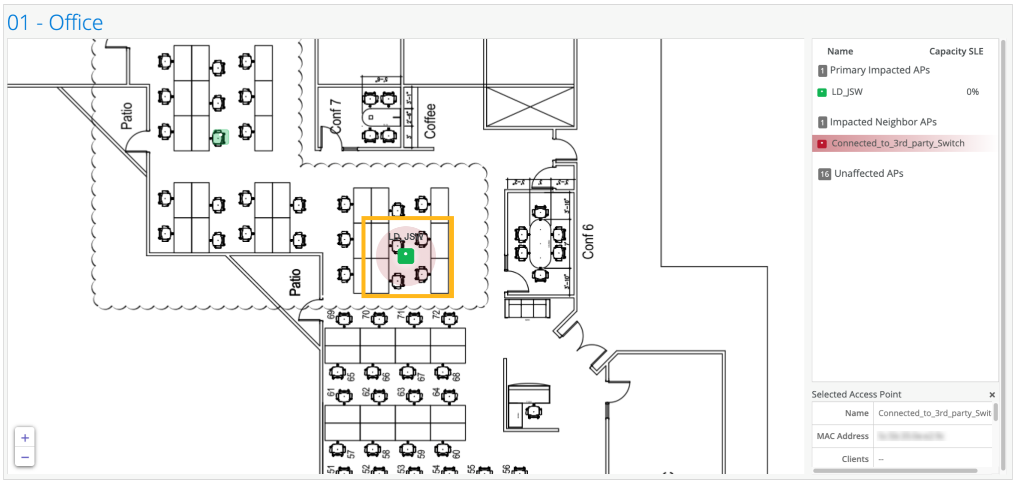
INSUFFICIENT CAPACITY

RECOMMENDED ACTION

The following APs have reduced capacity. Please check the corresponding reasons to improve the capacity

□	Site	APs	Details	Date	Status
□	Live-Demo	LD_JSW	5 GHz View More	May 8, 2023 02:34 AM	Open ▾

Here's the floor plan visual showing the affected AP (highlighted):


01 - Office

Name	Capacity SLE
1 Primary Impacted APs	
🟩 LD_JSW	0%
1 Impacted Neighbor APs	
🟥 Connected_to_3rd_party_Switch	
16 Unaffected APs	

Selected Access Point ×

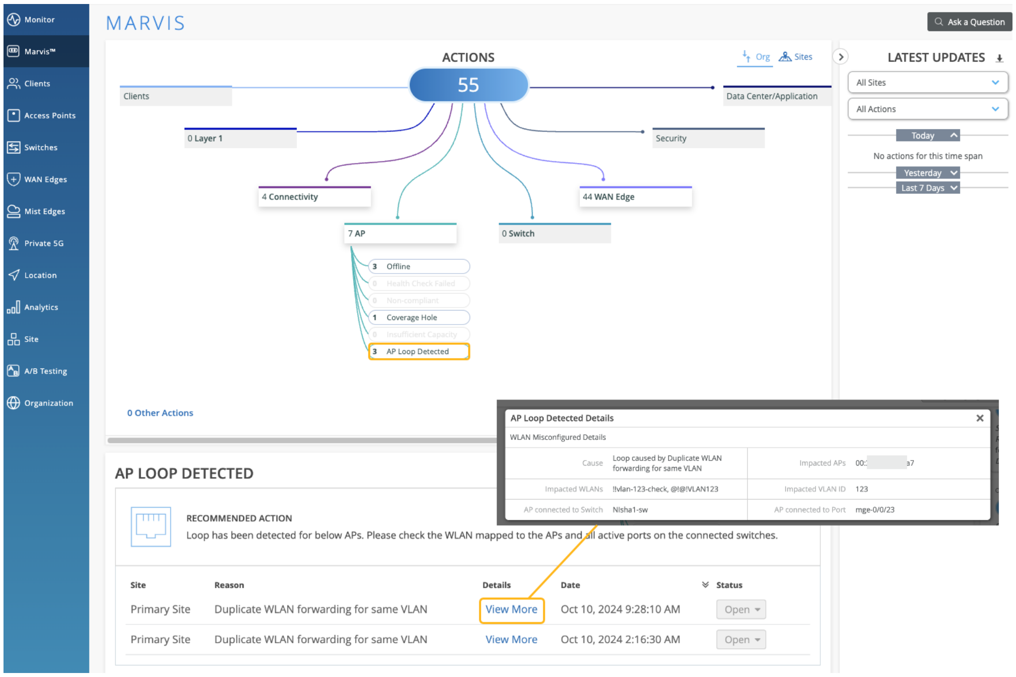
Name	Connected_to_3rd_party_Swit
MAC Address	[redacted]
Clients	--

AP Loop Detected

Marvis can detect a loop in your network based on the AP receiving the same packet that it sent out. With AP-based loop detection, Marvis detects loops caused by duplicate data paths in the following scenarios;

- Traffic from the same VLAN tunneled to the Mist Edge device and locally bridged to the switch port to which the AP is connected.
- Traffic from the same VLAN transported through two different tunnels to a Mist Edge device.
- Port flapping caused by persistent Spanning Tree Protocol (STP) topology changes.

Marvis identifies the exact location at your site where the traffic loop is occurring and shows you the affected switch and AP. Here's an example. You can use the **View More** link in the Details column to view specific details about the issue. In this example, you can see that Marvis provides the cause for the loop, the VLAN ID, details of the AP, and the switch to which the AP is connected,



AP Loop Detected Details

WLAN Misconfigured Details

Cause	Loop caused by Duplicate WLAN forwarding for same VLAN	Impacted APs	00:[redacted]a7
Impacted WLANs	!!vlan-123-check, @!@!VLAN123	Impacted VLAN ID	123
AP connected to Switch	NIsha1-sw	AP connected to Port	mge-0/0/23

AP LOOP DETECTED

RECOMMENDED ACTION

Loop has been detected for below APs. Please check the WLAN mapped to the APs and all active ports on the connected switches.

Site	Reason	Details	Date	Status
Primary Site	Duplicate WLAN forwarding for same VLAN	View More	Oct 10, 2024 9:28:10 AM	Open
Primary Site	Duplicate WLAN forwarding for same VLAN	View More	Oct 10, 2024 2:16:30 AM	Open

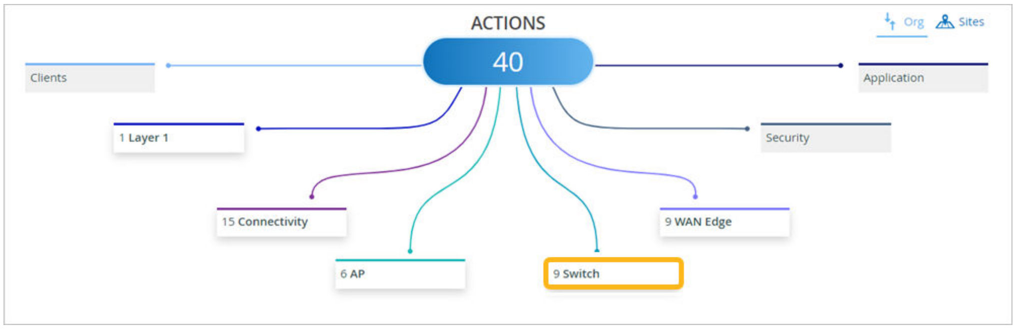
Switch Actions

SUMMARY

Use the Actions dashboard to resolve issues affecting your switches.

IN THIS SECTION

When you click the Switch button on the Actions dashboard, you'll see a list of all available actions. You can then click an action to investigate further. Available actions are described later in this topic.

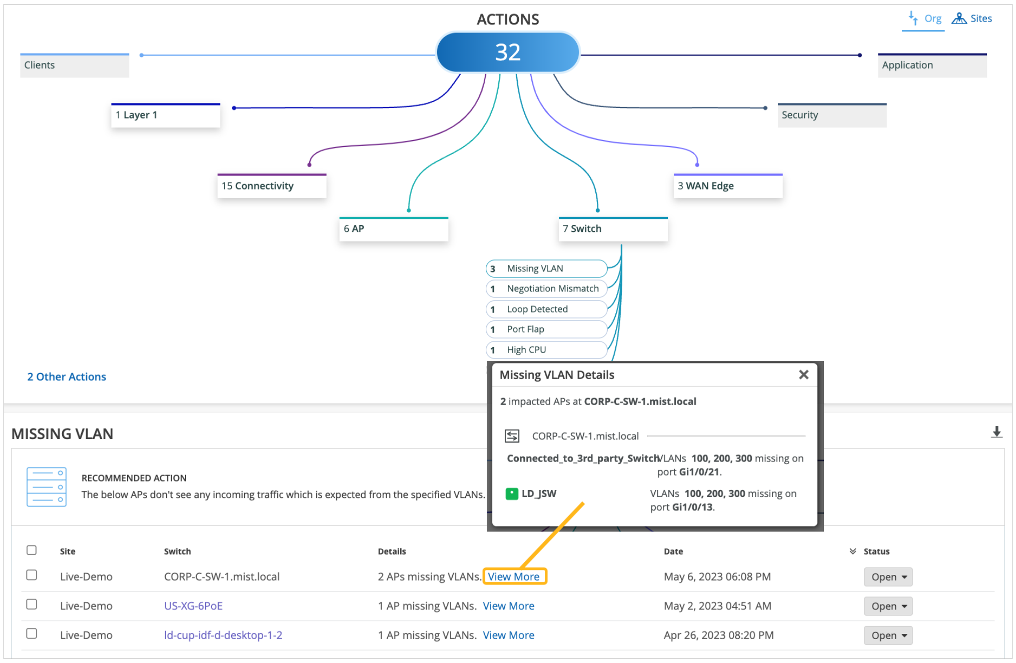


NOTE: Your subscriptions determine the actions that you can see on the Actions dashboard. For more information, see "Subscription Requirements for Marvis Actions " on page 121.

Missing VLAN

The Missing VLAN action indicates that a VLAN is configured on an AP but not on the switch port. As a result, clients are unable to communicate on a specific VLAN and are also unable to get an IP address from the DHCP server. Marvis compares the VLAN on the AP traffic with the VLAN on the switch port traffic and determines which device is missing the VLAN configuration.

In the following example, Marvis identifies two APs that do not see any incoming traffic due to a missing VLAN configuration. Marvis also identifies the specific switches that are missing the VLAN configuration and provides the port information, thereby enabling you to mitigate this issue with ease.



Missing VLAN Details ✕

2 impacted APs at **CORP-C-SW-1.mist.local**

CORP-C-SW-1.mist.local

Connected_to_3rd_party_Switch VLANs **100, 200, 300** missing on port **Gi1/0/21**.

LD_JSW VLANs **100, 200, 300** missing on port **Gi1/0/13**.

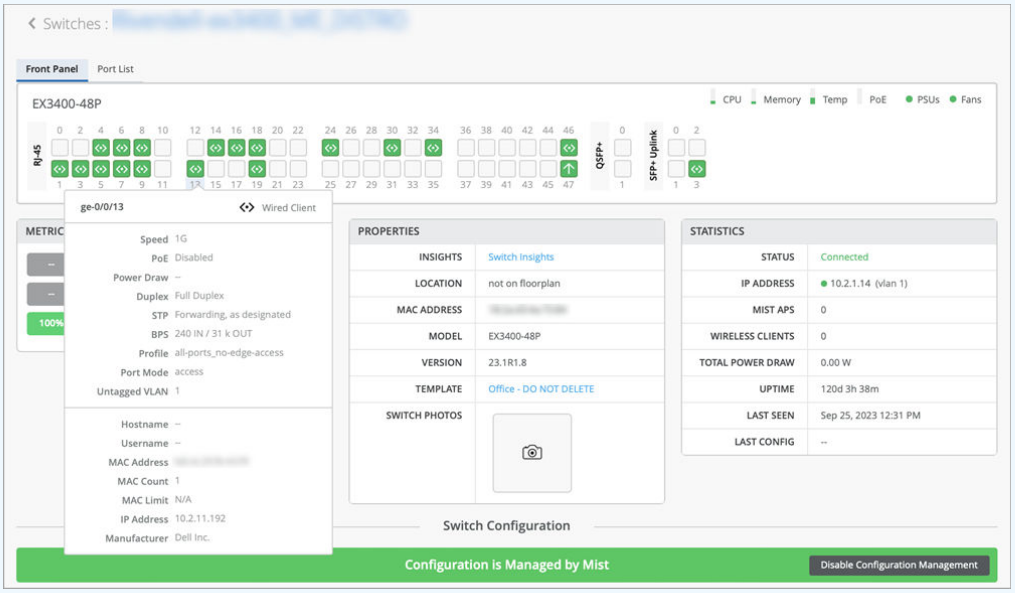
MISSING VLAN

RECOMMENDED ACTION

The below APs don't see any incoming traffic which is expected from the specified VLANs.

□	Site	Switch	Details	Date	Status
□	Live-Demo	CORP-C-SW-1.mist.local	2 APs missing VLANs. View More	May 6, 2023 06:08 PM	Open ▾
□	Live-Demo	US-XG-6PoE	1 AP missing VLANs. View More	May 2, 2023 04:51 AM	Open ▾
□	Live-Demo	ld-cup-idf-d-desktop-1-2	1 AP missing VLANs. View More	Apr 26, 2023 08:20 PM	Open ▾

NOTE: If you need more information, you also can use the left menu to go to the Switches page. There, click on the switch to view the information for each port, including VLANs.



ge-0/0/13 <·> Wired Client

Speed 1G
PoE Disabled
Power Draw –
Duplex Full Duplex
STP Forwarding, as designated
BPS 240 IN / 31 k OUT
Profile all-ports_no-edge-access
Port Mode access
Untagged VLAN 1

Hostname –
Username –
MAC Address [redacted]
MAC Count 1
MAC Limit N/A
IP Address 10.2.11.192
Manufacturer Dell Inc.

PROPERTIES

INSIGHTS	Switch Insights
LOCATION	not on floorplan
MAC ADDRESS	[redacted]
MODEL	EX3400-48P
VERSION	23.1R1.8
TEMPLATE	Office - DO NOT DELETE
SWITCH PHOTOS	

STATISTICS

STATUS	Connected
IP ADDRESS	● 10.2.1.14 (vlan 1)
MIST APS	0
WIRELESS CLIENTS	0
TOTAL POWER DRAW	0.00 W
UPTIME	120d 3h 38m
LAST SEEN	Sep 25, 2023 12:31 PM
LAST CONFIG	--

Configuration is Managed by Mist

After you fix the issue in your network, Mist AI monitors the switch for a certain period and ensures that the missing VLAN issue is indeed resolved. Hence, it might take up to 30 minutes for the Missing VLAN action to automatically resolve and appear in the Latest Updates section.

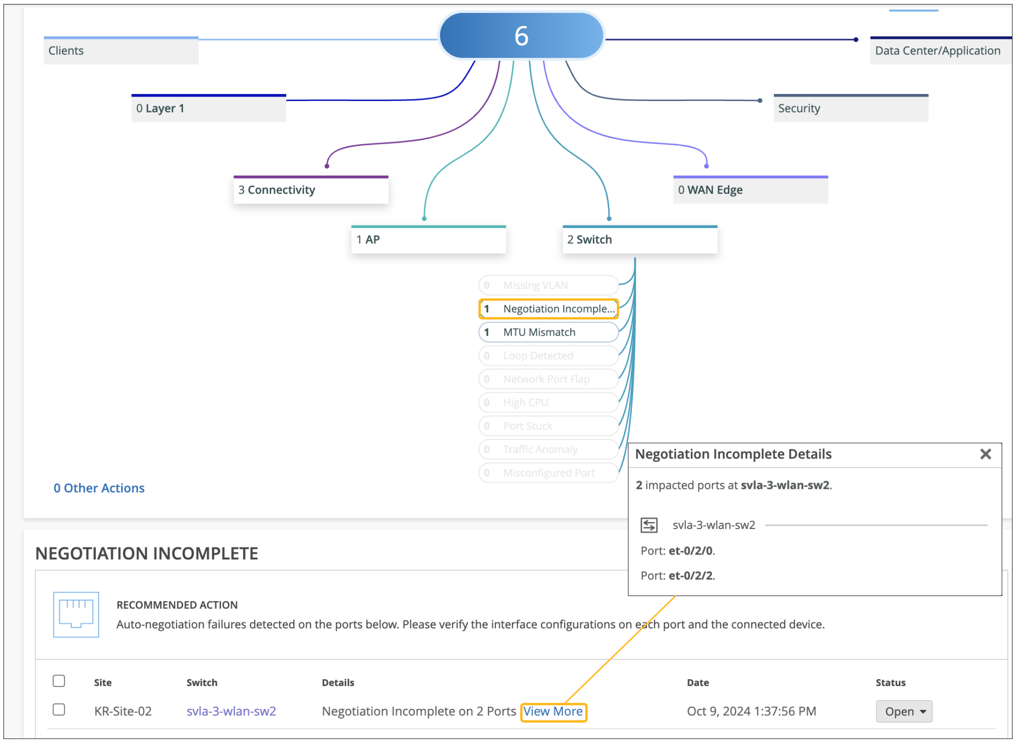
For more information about the Missing VLAN action, watch the following video:

Video: Missing VLANs

Negotiation Incomplete

The Negotiation Incomplete action detects instances on switch ports where autonegotiation failures occur. This issue can occur when Marvis detects a duplex mismatch between devices due to the autonegotiation failing to set the correct duplex mode. Marvis provides details about the affected port. You can check the configuration on the port and the connected device to resolve the issue.

The following example shows the details for the Negotiation Incomplete action. Notice that Marvis lists the switch and the port on which the autonegotiation failed.



Negotiation Incomplete Details ✕

2 impacted ports at **svla-3-wlan-sw2**.

svla-3-wlan-sw2

Port: **et-0/2/0**.

Port: **et-0/2/2**.

NEGOTIATION INCOMPLETE

RECOMMENDED ACTION

Auto-negotiation failures detected on the ports below. Please verify the interface configurations on each port and the connected device.

□	Site	Switch	Details	Date	Status
□	KR-Site-02	svla-3-wlan-sw2	Negotiation Incomplete on 2 Ports View More	Oct 9, 2024 1:37:56 PM	Open ▾

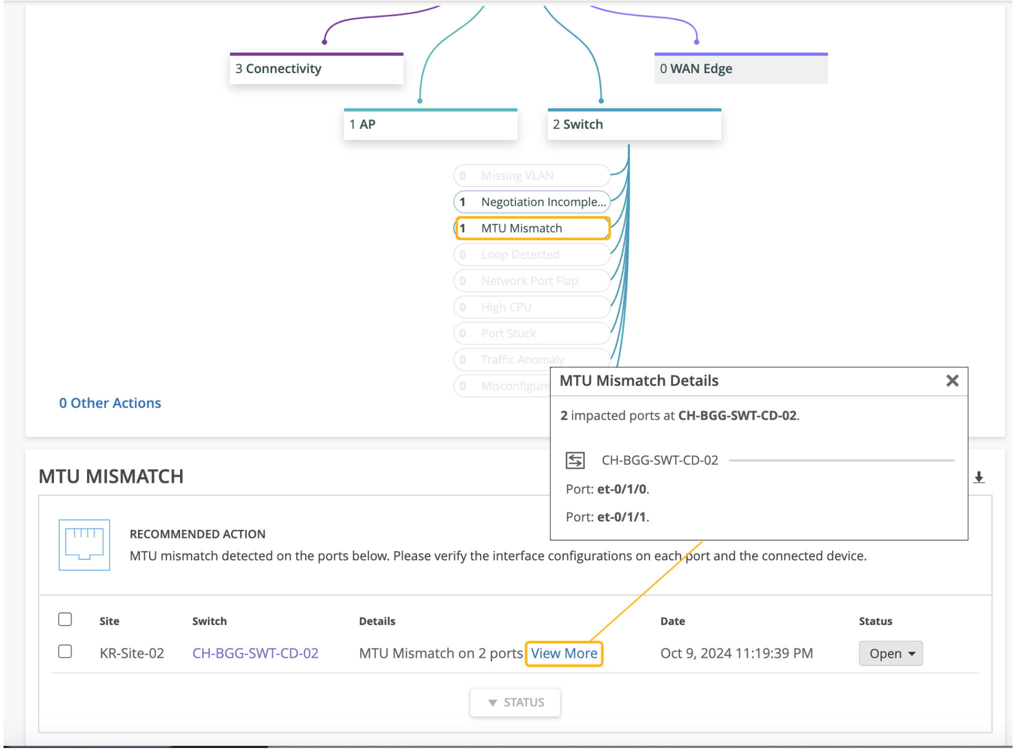
After you fix the issue in your network, the Negotiation Incomplete action automatically resolves and appears in the Latest Updates section within an hour.

MTU Mismatch

Marvis detects MTU mismatches between the port on a switch and the port on the device that is connected directly to that switch port. All devices on the same Layer 2 (L2) network must have the same

MTU size. When an MTU mismatch occurs, devices might fragment packets resulting in a network overhead. The **Details** column lists the port on which the mismatch occurs.

You'll need to review the port configuration on the switch and the connected device to resolve the issue. Here’s an example of an MTU mismatch identified by Marvis.



MTU Mismatch Details

2 impacted ports at **CH-BGG-SWT-CD-02**.

CH-BGG-SWT-CD-02

Port: **et-0/1/0**.

Port: **et-0/1/1**.

MTU MISMATCH

RECOMMENDED ACTION

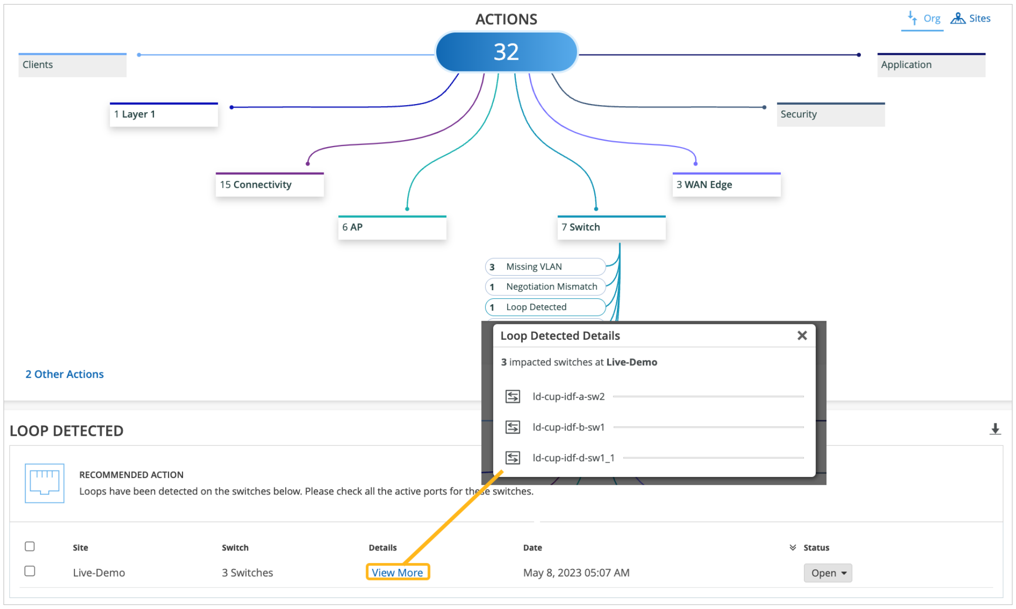
MTU mismatch detected on the ports below. Please verify the interface configurations on each port and the connected device.

□	Site	Switch	Details	Date	Status
□	KR-Site-02	CH-BGG-SWT-CD-02	MTU Mismatch on 2 ports View More	Oct 9, 2024 11:19:39 PM	Open

Loop Detected

The Loop Detected action indicates a loop in your network resulting in the switch receiving the same packet that it sent out. A loop occurs when multiple links exist between devices. Redundant links are a common cause for L2 loops. A redundant link serves as a backup link for the primary link. If both links are active at the same time and protocols such as the Spanning Tree Protocol (STP) are not deployed properly, a switching loop occurs.

Marvis identifies the exact location at your site where the traffic loop is occurring and shows you the affected switches. Here's an example:



Loop Detected Details

3 impacted switches at **Live-Demo**

ld-cup-idf-a-sw2

ld-cup-idf-b-sw1

ld-cup-idf-d-sw1_1

LOOP DETECTED

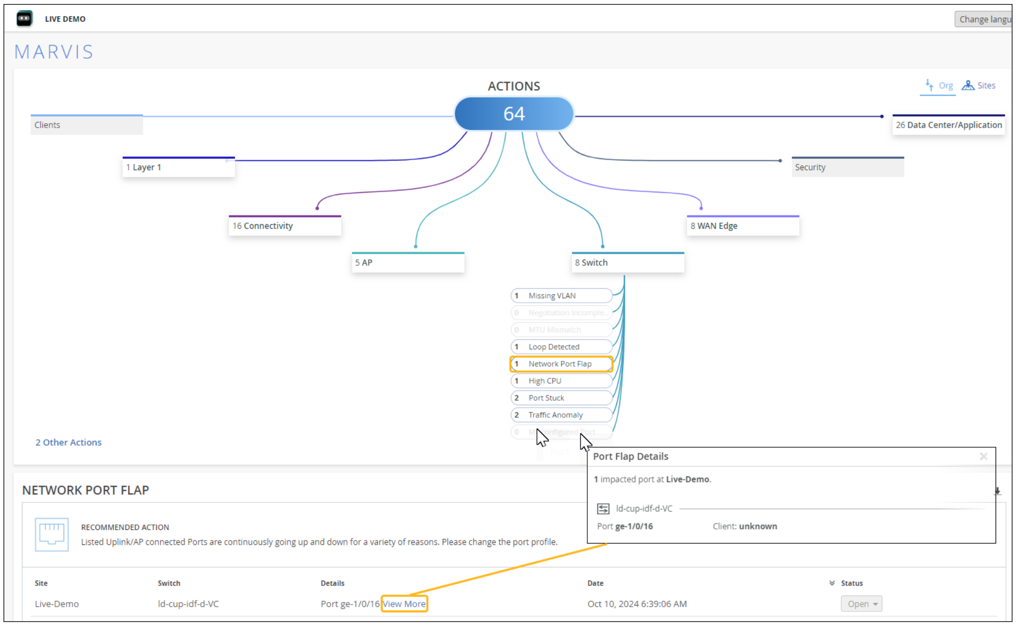
RECOMMENDED ACTION

Loops have been detected on the switches below. Please check all the active ports for these switches.

	Site	Switch	Details	Date	Status
☐	Live-Demo	3 Switches	View More	May 8, 2023 05:07 AM	Open ▾

Network Port Flap

The Network Port Flap action identifies trunk ports that bounce persistently for at least an hour. For example, three flaps per minute for an hour. Ports configured as trunk ports are used to connect to other switches, gateways, or APs as individual trunk ports, or as part of a port channel. Port flapping can occur due to a bad cable or transceiver causing one-way traffic or LACPDU exchange, or continuous rebooting of an end device connected to the port. The following example shows the details that Marvis Actions provides for a Network Port Flap action:



Port Flap Details

1 impacted port at **Live-Demo**.

ld-cup-idf-d-VC

Port **ge-1/0/16** Client: **unknown**

NETWORK PORT FLAP

RECOMMENDED ACTION

Listed Uplink/AP connected Ports are continuously going up and down for a variety of reasons. Please change the port profile.

Site	Switch	Details	Date	Status
Live-Demo	ld-cup-idf-d-VC	Port ge-1/0/16 View More	Oct 10, 2024 6:39:06 AM	Open ▾

You can disable a persistently flapping port directly from the Marvis Actions page. In the Network Port Flap actions section, select the switch on which you want to disable a port and click the **DISABLE PORT** button.

The Disable Port page appears, listing the ports that you can disable. You cannot select a port if it is already disabled (either previously through the Actions page or manually from the Switch Details page).

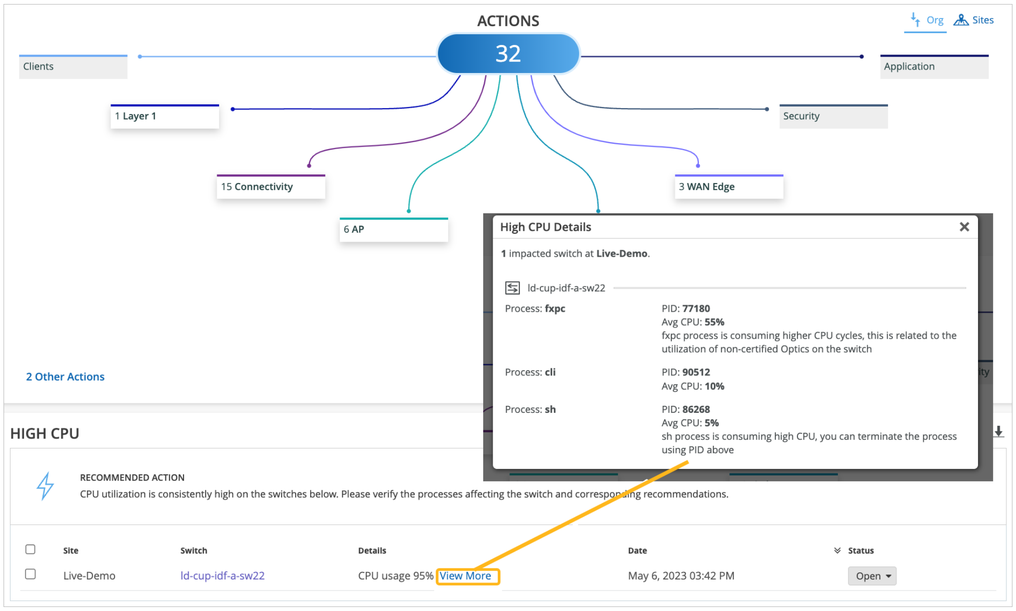
When you disable a port, the port configurations on the selected ports change to disabled and the ports go down. After you fix the issue, you can re-enable these ports by editing the port configuration on the Switch Details page. After you re-enable the ports, you can reconnect the devices to the ports.

After you fix the issue in your network, the Port Flap action automatically resolves and appears in the Latest Updates section within an hour.

Video: Port Flap

High CPU

Marvis detects switches that constantly have high CPU utilization. Various factors can cause high CPU utilization: multicast traffic, network loops, hardware issues, device temperature, and so on. The High CPU action lists the switches, the processes running on the switch along with the CPU utilization rate, and the reason for the high utilization. In the following example, you see that the fxpc process has high CPU utilization, and the cause for the high utilization is the use of noncertified optics on the switch:



High CPU Details ✕

1 impacted switch at **Live-Demo**.

ld-cup-idf-a-sw22

Process: **fxpc** PID: **77180**
Avg CPU: **55%**
fxpc process is consuming higher CPU cycles, this is related to the utilization of non-certified Optics on the switch

Process: **cli** PID: **90512**
Avg CPU: **10%**

Process: **sh** PID: **86268**
Avg CPU: **5%**
sh process is consuming high CPU, you can terminate the process using PID above

HIGH CPU

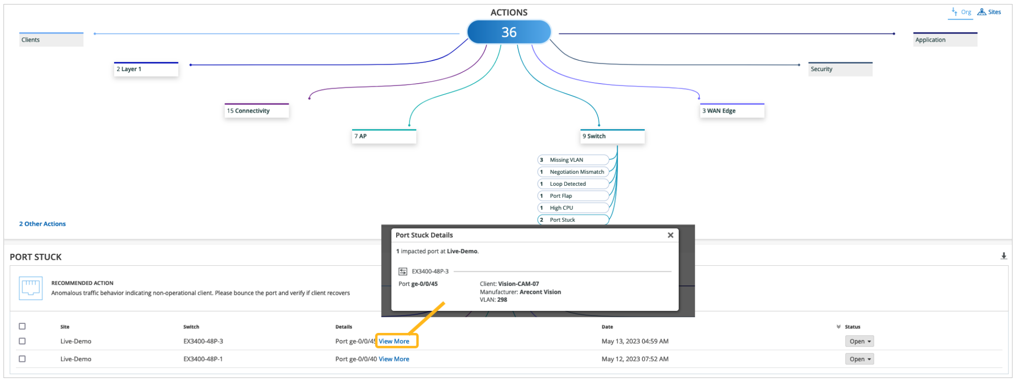
RECOMMENDED ACTION

CPU utilization is consistently high on the switches below. Please verify the processes affecting the switch and corresponding recommendations.

□	Site	Switch	Details	Date	Status
□	Live-Demo	ld-cup-idf-a-sw22	CPU usage 95% View More	May 6, 2023 03:42 PM	Open ▾

Port Stuck

The Port Stuck action detects a difference in traffic pattern on a switch port, such as no transmitted or received packets, indicating that the client connected to the port is not operating normally. In the following example, you'll see that Marvis Actions recommends that you bounce the port and verify if the client starts operating normally. Notice that in addition to the port number, Marvis also lists the client (in this case, a camera) that is connected to the port and the associated VLAN.



Port Stuck Details

1 impacted port at **Live-Demo**.

EX3400-48P-3

Port **ge-0/0/45**

Client: **Vision-CAM-07**
Manufacturer: **Arecont Vision**
VLAN: **298**

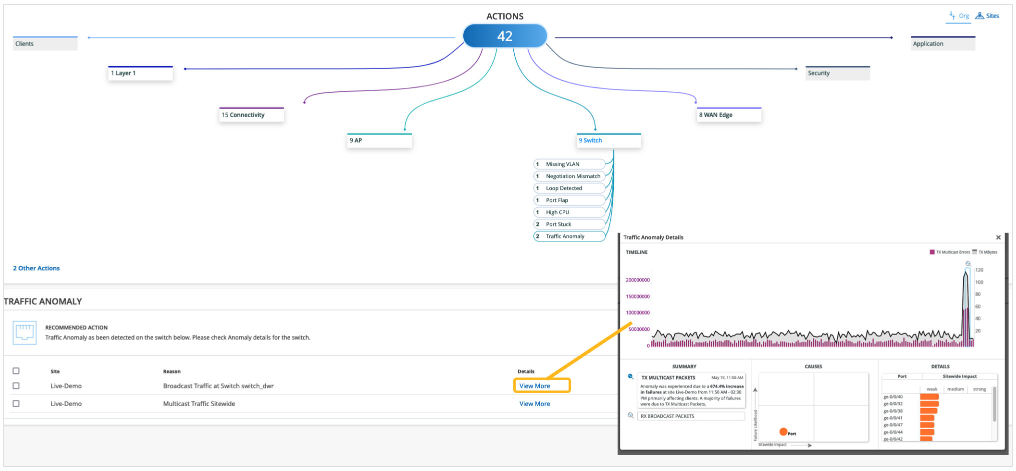
PORT STUCK

RECOMMENDED ACTION
Anomalous traffic behavior indicating non-operational client. Please bounce the port and verify if client recovers

□	Site	Switch	Details	Date	Status
□	Live-Demo	EX3400-48P-3	Port ge-0/0/45 View More	May 13, 2023 04:59 AM	Open ▾
□	Live-Demo	EX3400-48P-1	Port ge-0/0/40 View More	May 12, 2023 07:52 AM	Open ▾

Traffic Anomaly

Marvis detects an unusual drop or increase in broadcast and multicast traffic on a switch. It also detects any unusually high transmit or receive errors. Like the Anomaly Detection view for connectivity failures, the Details view shows a timeline, the description of the anomaly, and details of the affected ports. If the issue affects an entire site, Marvis displays the details of the affected switches and port details for each affected switch.



TRAFFIC ANOMALY

RECOMMENDED ACTION
Traffic Anomaly as been detected on the switch below. Please check Anomaly details for the switch.

□	Site	Reason	Details
□	Live-Demo	Broadcast Traffic at Switch switch_dwr	View More
□	Live-Demo	Multicast Traffic Sitewide	View More

Traffic Anomaly Details

SUMMARY

TX MULTICAST PACKETS May 19, 11:50 AM

Anomaly was experienced due to a **674.4% increase in failures** at site Live-Demo from 11:50 AM - 02:30 PM primarily affecting clients. A majority of failures were due to TX Multicast Packets.

RX BROADCAST PACKETS

DETAILS

Port	Sitewide Impact
	weak / medium / strong
ge-0/0/40	weak
ge-0/0/32	weak
ge-0/0/38	weak
ge-0/0/41	weak
ge-0/0/47	weak
ge-0/0/44	weak
ge-0/0/42	weak

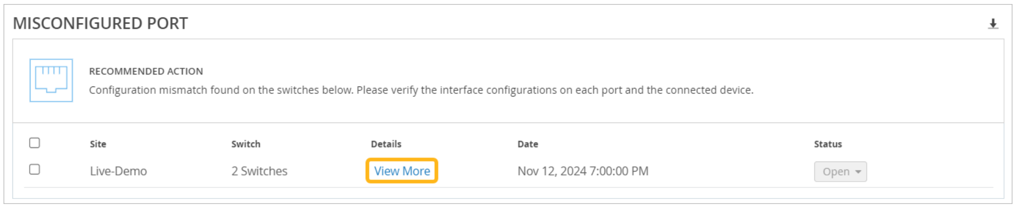
Video: Marvis Can Detect Switch Traffic Anomalies

Misconfigured Port

When a switch is connected to another switch, communication requires common properties on the ports. To detect misconfiguration, Marvis compares these properties:

- Speed
- Duplex
- Native VLAN
- Allowed VLAN
- MTU
- Port Mode (both ports “access” or both ports “trunk”)
- STP Mode (both ports “forwarding”)

On the Actions dashboard, click **Switch** > **Misconfigured Port** to see the issues and the recommended action in the lower part of the screen.



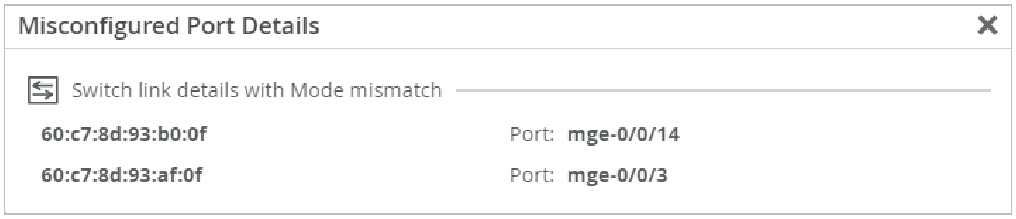
MISCONFIGURED PORT

RECOMMENDED ACTION

Configuration mismatch found on the switches below. Please verify the interface configurations on each port and the connected device.

□	Site	Switch	Details	Date	Status
□	Live-Demo	2 Switches	View More	Nov 12, 2024 7:00:00 PM	Open

Click the **View More** link to see the MAC addresses and ports.



Misconfigured Port Details

Switch link details with Mode mismatch

60:c7:8d:93:b0:0f	Port: mge-0/0/14
60:c7:8d:93:af:0f	Port: mge-0/0/3

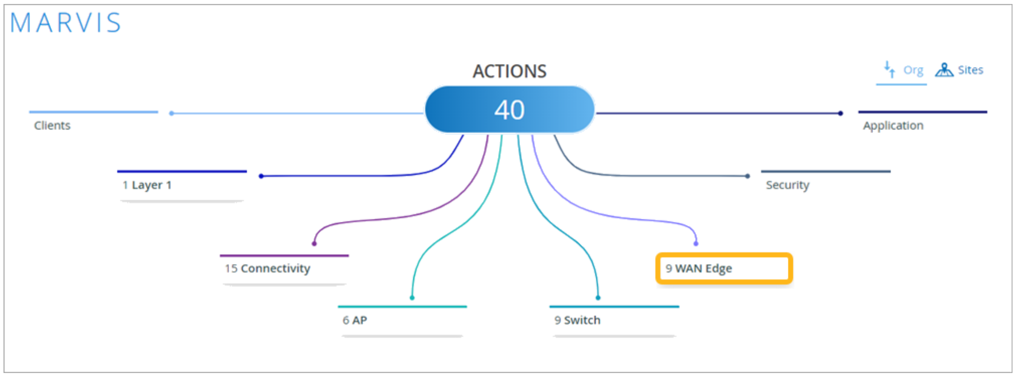
WAN Edge Actions

SUMMARY

Use the Actions dashboard to resolve issues affecting your WAN Edge devices.

IN THIS SECTION

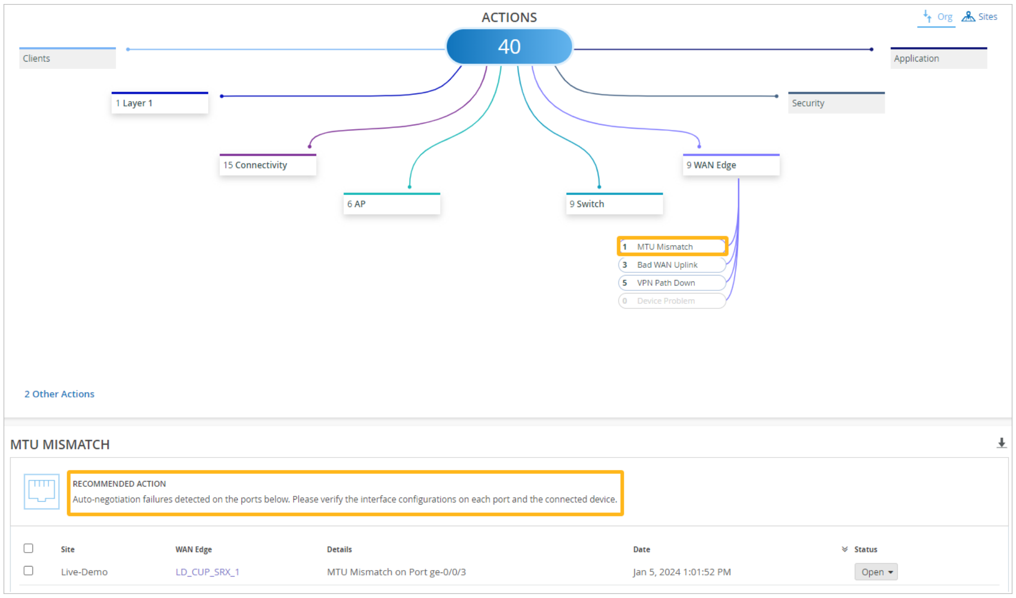
When you click the WAN Edge button on the Actions dashboard, you'll see a list of all available actions. You can then click an action to investigate further. Available actions are described later in this topic.



NOTE: Your subscriptions determine the actions that you can see on the Actions dashboard. For more information, see "Subscription Requirements for Marvis Actions " on page 121.

MTU Mismatch

Marvis detects MTU mismatches between a port on the WAN Edge device and a port on the directly connected device. All devices on the same Layer 2 (L2) network must have the same MTU size. When an MTU mismatch occurs, devices might either fragment packets resulting in a network overhead or discard packets. The Details column lists the port on which the mismatch occurs. You'll need to review the port configuration on the WAN edge device and the connected device to resolve the issue.



MTU MISMATCH

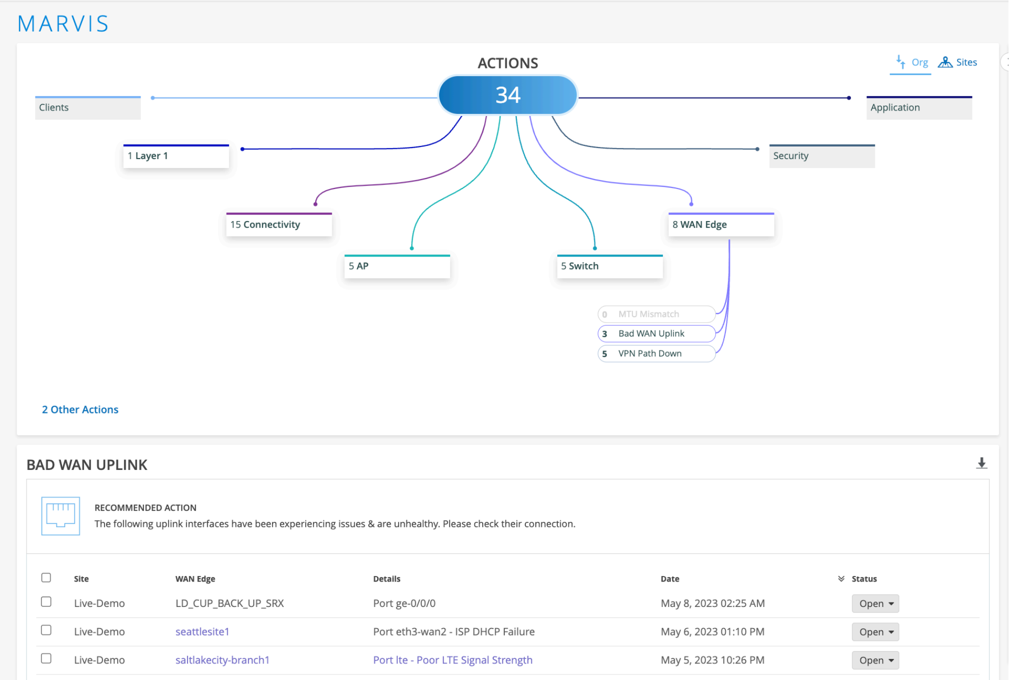
RECOMMENDED ACTION
Auto-negotiation failures detected on the ports below. Please verify the interface configurations on each port and the connected device.

□	Site	WAN Edge	Details	Date	Status
□	Live-Demo	LD_CUP_SRX_1	MTU Mismatch on Port ge-0/0/3	Jan 5, 2024 1:01:52 PM	Open

Bad WAN Uplink

The Bad WAN Uplink action identifies instances where the uplink interfaces on your Juniper Networks® SRX Series Firewall or Session Smart™ Router are experiencing issues. Marvis identifies interface-related issues (such as cable issues, congestion) or it could be network-related (high latency, packet drops, and jitter). These issues can cause poor user experience and result in an unhealthy WAN link. You might see errors in the overlay even though there are no issues in the underlay.

When you see a Bad WAN Uplink action, we recommend that you check the uplink connection on your device to troubleshoot the issue. Marvis highlights the issue indicating the need to check the connection as shown in the following example:



BAD WAN UPLINK

RECOMMENDED ACTION

The following uplink interfaces have been experiencing issues & are unhealthy. Please check their connection.

□	Site	WAN Edge	Details	Date	Status
□	Live-Demo	LD_CUP_BACK_UP_SRX	Port ge-0/0/0	May 8, 2023 02:25 AM	Open ▾
□	Live-Demo	seattlesite1	Port eth3-wan2 - ISP DHCP Failure	May 6, 2023 01:10 PM	Open ▾
□	Live-Demo	saltlakecity-branch1	Port lte - Poor LTE Signal Strength	May 5, 2023 10:26 PM	Open ▾

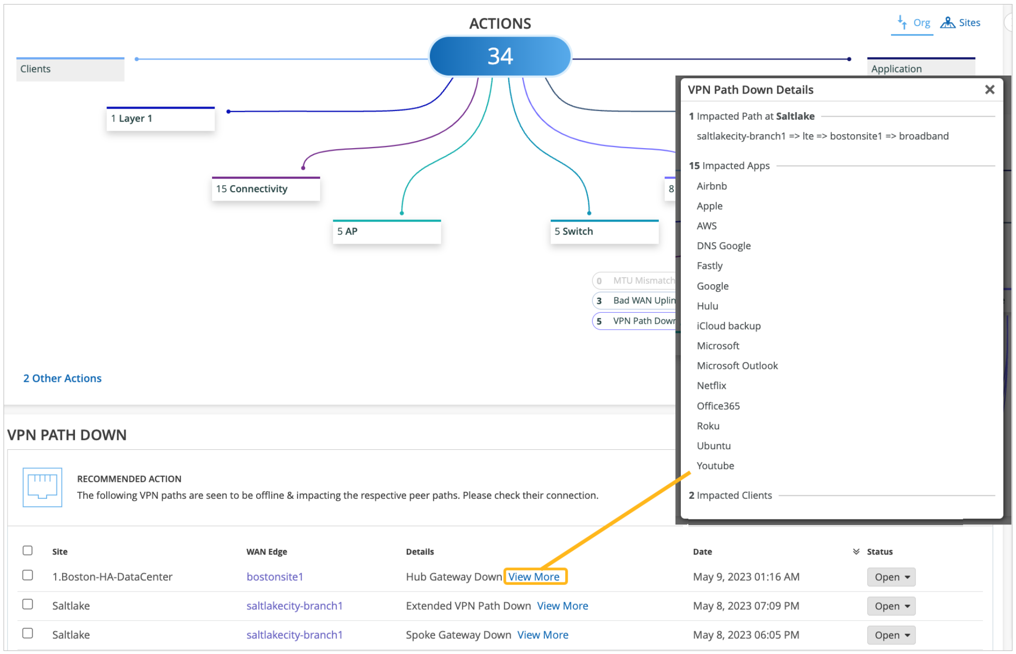
Poor LTE connectivity can cause uplink issues. For a bad LTE WAN link, Marvis shows a timeline of affected clients and signal strength. This timeline view is like the Anomaly Detection view for connectivity failures. Marvis automatically finds and displays the worst signal strength metric during this time. Marvis displays any one of the following signal strength metrics:

- Received signal strength indicator (RSSI)
- Reference Signal Received Power (RSRP)
- Signal-to-noise ratio (SNR)

After you fix the issue in your network, Mist AI monitors the WAN link for a certain period of time to see if users are experiencing any issues. Hence, it might take up to 24 hours for the Bad WAN Uplink action to automatically resolve and appear in the Latest Updates section.

VPN Path Down

Marvis monitors the VPN paths that are associated with WAN edge nodes (Juniper Networks® SRX Series Firewall or Session Smart™ Router) in the overlay network. If all VPN tunnels or peer paths towards a hub go down, Marvis displays the VPN Path Down action so that you can take immediate action. In the following example, Marvis reports that a hub gateway is down. Notice that Marvis provides detailed information such as the impacted sites, applications, and clients.



VPN Path Down Details ✕

1 Impacted Path at **Saltlake**

saltlakecity-branch1 => lte => bostonsite1 => broadband

15 Impacted Apps

Airbnb
Apple
AWS
DNS Google
Fastly
Google
Hulu
iCloud backup
Microsoft
Microsoft Outlook
Netflix
Office365
Roku
Ubuntu
Youtube

2 Impacted Clients

VPN PATH DOWN

RECOMMENDED ACTION

The following VPN paths are seen to be offline & impacting the respective peer paths. Please check their connection.

□	Site	WAN Edge	Details	Date	Status
□	1.Boston-HA-DataCenter	bostonsite1	Hub Gateway Down View More	May 9, 2023 01:16 AM	Open ▾
□	Saltlake	saltlakecity-branch1	Extended VPN Path Down View More	May 8, 2023 07:09 PM	Open ▾
□	Saltlake	saltlakecity-branch1	Spoke Gateway Down View More	May 8, 2023 06:05 PM	Open ▾

For SSR Series Routers, the VPN Path Down action lists the specific type of peer path that is down:

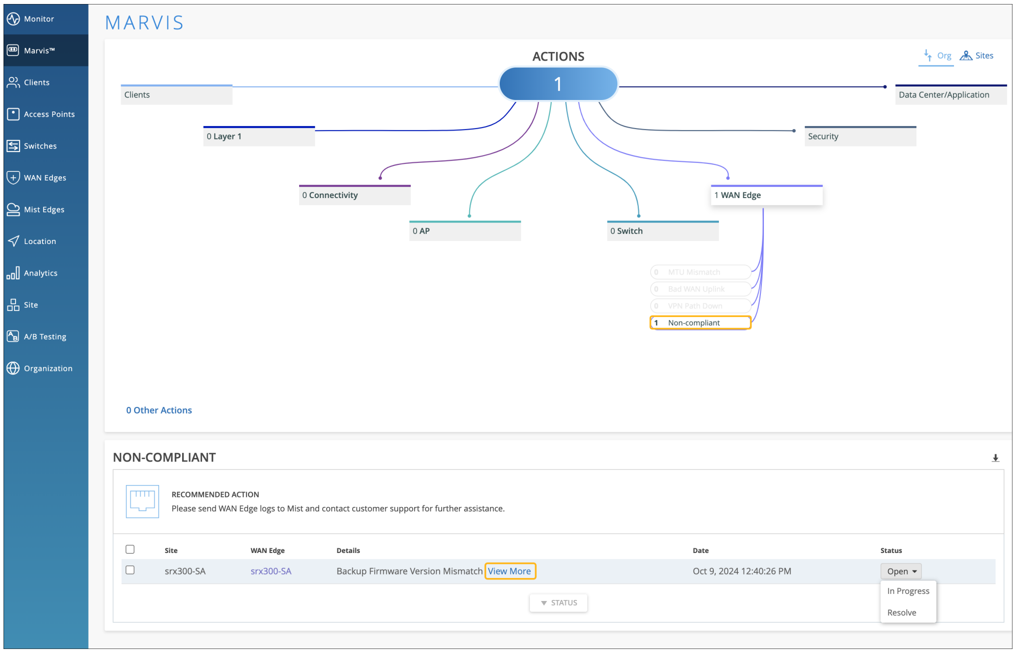
- Spoke Interface Unreachable—All the peer paths originating from a spoke interface are down as the interface is down.
- Spoke Gateway Unreachable—All the paths originating from a spoke are experiencing a peer path down issue.
- Hub Gateway Unreachable—All the paths terminating at a hub are experiencing a peer path down issue.
- Hub Interface Down—All the paths to a hub interface are down as the hub interface is down.

After you fix the issue in your network, Mist AI monitors the VPN path for a certain period of time to see if users are experiencing any issues. Hence, it might take up to 24 hours for the VPN Path Down action to automatically resolve and appear in the Latest Updates section.

Non-Compliant

Marvis monitors the Junos OS version running on the primary and backup partitions on SRX Series devices at a site. The Non-Compliant action flags an SRX device if the Junos OS version on the backup partition is different from the version running on the primary partition.

The following example shows the details for the Non-Compliant action. You can click the **View More** link to view the details.



RECOMMENDED ACTION

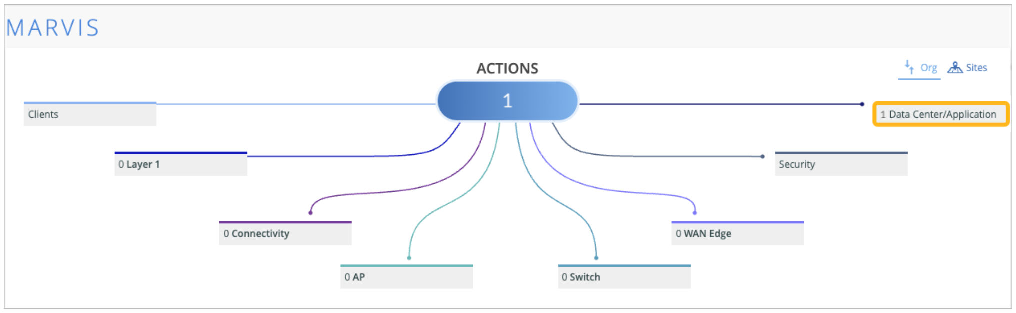
Please send WAN Edge logs to Mist and contact customer support for further assistance.

□	Site	WAN Edge	Details	Date	Status
□	srx300-SA	srx300-SA	Backup Firmware Version Mismatch View More	Oct 9, 2024 12:40:26 PM	Open

After you upgrade the backup partition on the SRX Series device to the proper version, the Non-Compliant action automatically resolves and appears in the Latest Updates section within 30 minutes.

Data Center/Application Actions

If you manage your enterprise network with Juniper Mist and your data centers with Juniper Apstra, you can click the **Data Center/Applications** Action button in Marvis to quickly view what the Marvis Virtual Network Assistant for Data Center has collected.

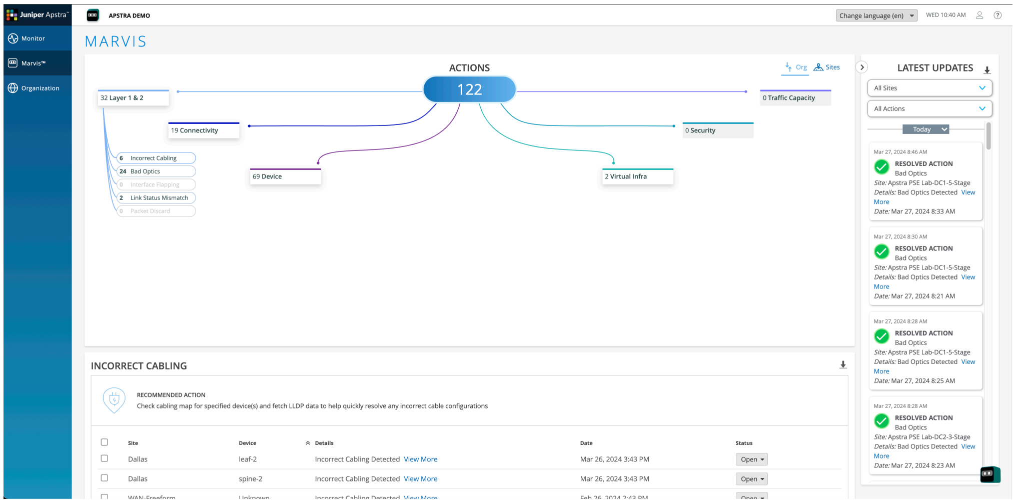


NOTE: Before the **Data Center/Application** button will work, you must perform some configuration in both your Mist portal and your Juniper Apstra Cloud Services portal. See Access Apstra Cloud Services.

Unlike the other actions on this page which expand in place, the **Data Center/Application** action button launches a new browser window or tab that opens to the Marvis Actions page in your Juniper Apstra Cloud Services portal. See Figure 1 on page 152.

> **NOTE**: To launch Apstra Cloud Services portal, you need a user role that provides access to Marvis Actions (organization-level view).

Figure 2: Marvis Actions Page on Juniper Apstra Cloud Services Portal



Mar 27, 2024 8:46 AM
RESOLVED ACTION
Bad Optics
Site: Apstra PSE Lab-DC1-5-Stage
Details: Bad Optics Detected View More
Date: Mar 27, 2024 8:33 AM

Mar 27, 2024 8:30 AM
RESOLVED ACTION
Bad Optics
Site: Apstra PSE Lab-DC1-5-Stage
Details: Bad Optics Detected View More
Date: Mar 27, 2024 8:21 AM

Mar 27, 2024 8:28 AM
RESOLVED ACTION
Bad Optics
Site: Apstra PSE Lab-DC1-5-Stage
Details: Bad Optics Detected View More
Date: Mar 27, 2024 8:25 AM

Mar 27, 2024 8:28 AM
RESOLVED ACTION
Bad Optics
Site: Apstra PSE Lab-DC2-3-Stage
Details: Bad Optics Detected View More
Date: Mar 27, 2024 8:23 AM

INCORRECT CABLING

RECOMMENDED ACTION
Check cabling map for specified device(s) and fetch LLDP data to help quickly resolve any incorrect cable configurations

□	Site	Device	Details	Date	Status
□	Dallas	leaf-2	Incorrect Cabling Detected View More	Mar 26, 2024 3:43 PM	Open
□	Dallas	spine-2	Incorrect Cabling Detected View More	Mar 26, 2024 3:43 PM	Open
□	WAN-Freeform	Unknown	Incorrect Cabling Detected View More	Feb 26, 2024 2:43 PM	Open

RELATED DOCUMENTATION

https://www.juniper.net/documentation/us/en/software/mist/mist-management/topics/task/mist-to-apstra-link.html

https://www.juniper.net/documentation/us/en/software/juniper-apstra-cloud-services/user-guide/topics/concept/datacenter-assurance-overview.html

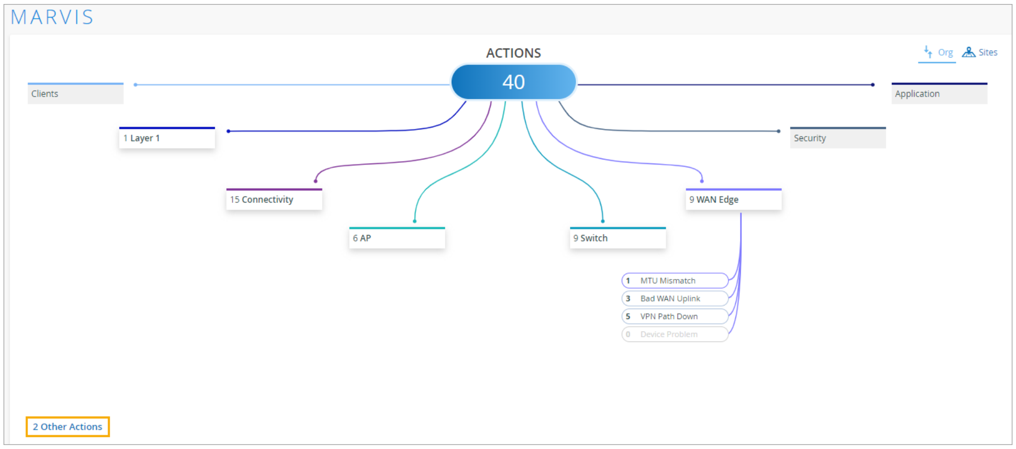
Other Marvis Actions

SUMMARY

Use the Actions dashboard to resolve issues with persistently failing clients.

IN THIS SECTION

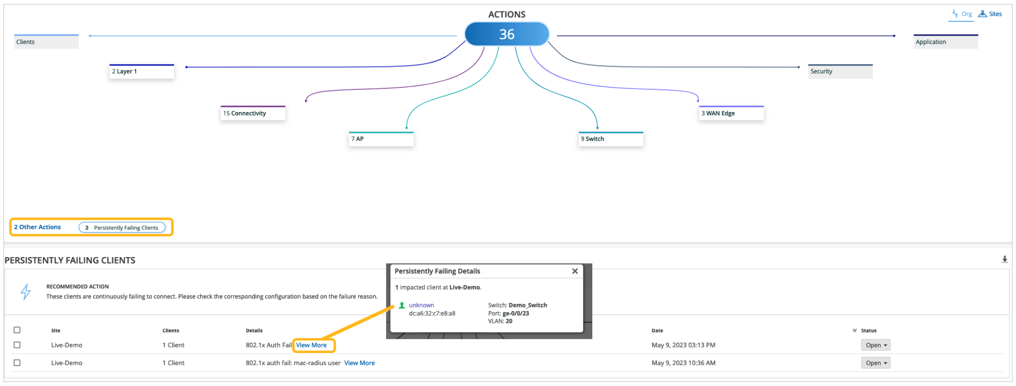
When you click the Other Actions link on the Action dashboard, all available actions appear. Currently there are two types of actions for this category: Persistently Failing Clients and Access Port Flap.



NOTE: Your subscriptions determine the actions that you can see on the Actions dashboard. For more information, see "Subscription Requirements for Marvis Actions " on page 121.

Persistently Failing Clients

Marvis identifies wired or wireless clients that continuously fail to connect due to a client-specific issue; that is, the scope of failure isn't the access point (AP), switch, wireless LAN (WLAN), or server. The failure can be due to authentication failures from entering the wrong preshared key (PSK) or failures caused by incorrect 802.1x configuration. Marvis displays the list of clients experiencing a failure and the WLANs they are trying to connect to.



PERSISTENTLY FAILING CLIENTS

RECOMMENDED ACTION
These clients are continuously failing to connect. Please check the corresponding configuration based on the failure reason.

Persistently Failing Details

1 impacted client at **Live-Demo**.

unknown
dc:a6:32:c7:e8:a8

Switch: **Demo_Switch**
Port: **ge-0/0/23**
VLAN: **20**

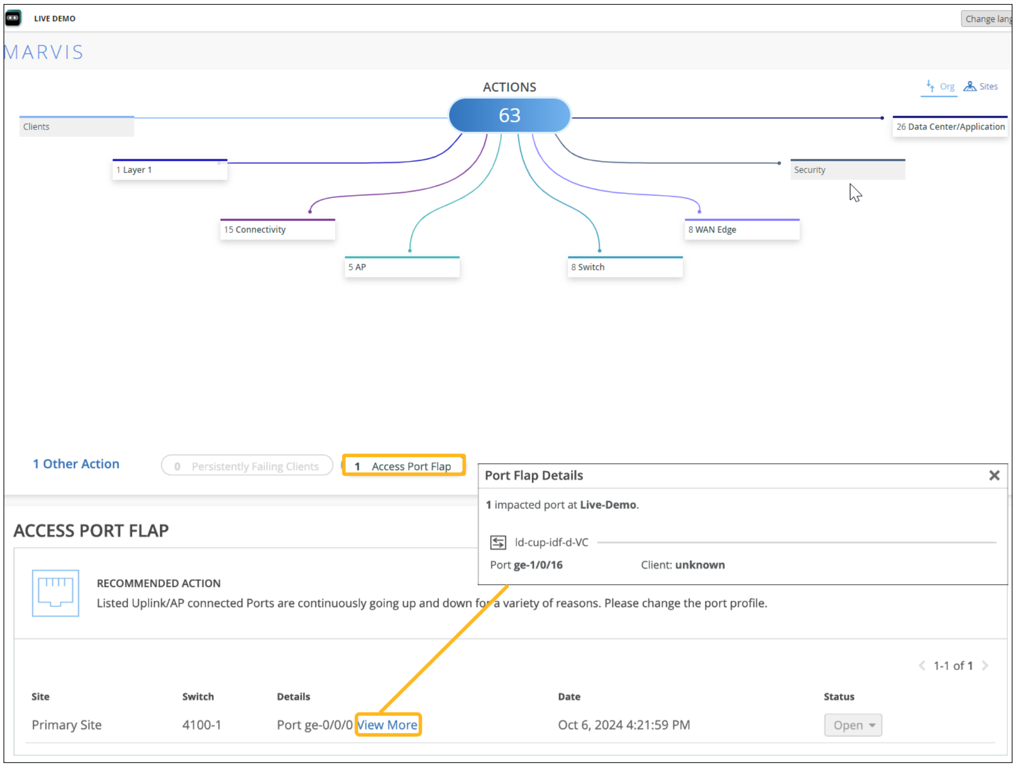
□	Site	Clients	Details	Date	Status
□	Live-Demo	1 Client	802.1x Auth Fail View More	May 9, 2023 03:13 PM	Open ▾
□	Live-Demo	1 Client	802.1x auth fail: mac-radius user View More	May 9, 2023 10:36 AM	Open ▾

NOTE: After you fix this issue, the Persistently Failing Clients action automatically resolves within an hour. As this action is considered low priority, Marvis does not list the Persistently Failing Clients action in the Latest Updates section or on the Sites tab.

Video: Persistently Failing Clients

Access Port Flap

The Access Port Flap action identifies ports that bounce persistently over a short time interval, indicating that a port or connected wired client has an issue. A port flap can occur due to unreliable connections, continuous rebooting of a device connected to the port, or incorrect duplex configurations. The following example shows the details that Marvis Actions provides for an Access Port Flap action:



Port Flap Details

1 impacted port at Live-Demo.

ld-cup-idf-d-VC

Port ge-1/0/16 Client: unknown

Listed Uplink/AP connected Ports are continuously going up and down for a variety of reasons. Please change the port profile.

Site	Switch	Details	Date	Status
Primary Site	4100-1	Port ge-0/0/0 View More	Oct 6, 2024 4:21:59 PM	Open

Anomaly Detection Event Card

SUMMARY

Use the Anomaly Detection Event Card for additional information about issues and actions.

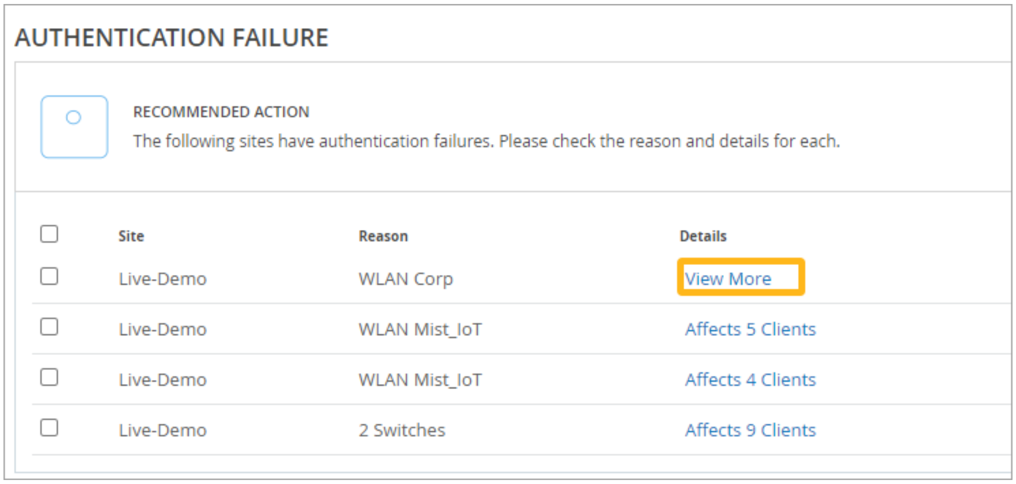
The Anomaly Detection Event Card provides a more detailed diagnosis about the anomalies for some of the actions that Marvis suggests. The Event Card is available for these types of failures:

- Authentication Failures
- Domain Name System (DNS) Failures
- Dynamic Host Control Protocol (DHCP) Failures

Watch this video to see an example.

Video: Marvis Can Detect Switch Traffic Anomalies

If an event card is available, you'll see a **View More** link, as shown in this example.



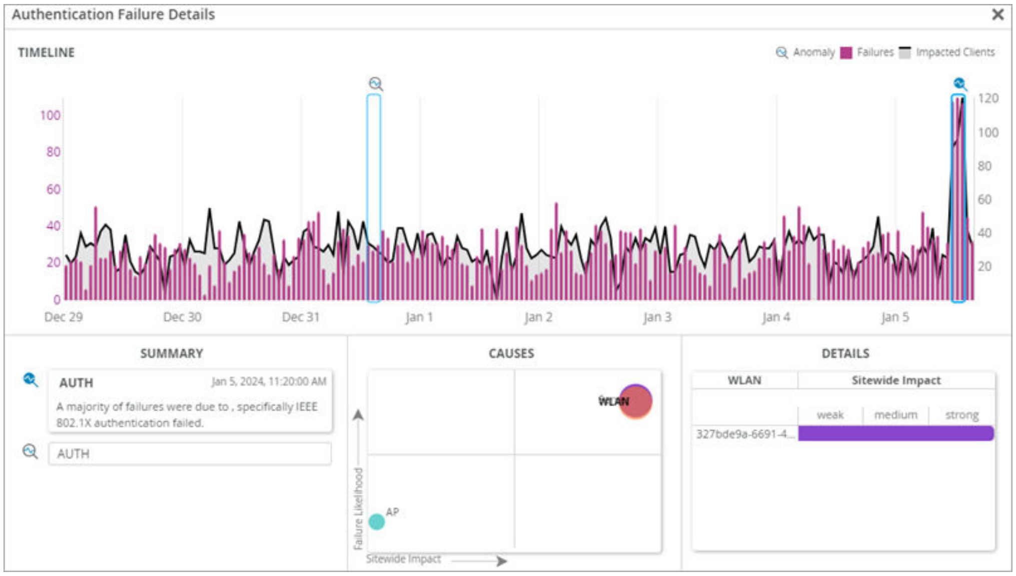
AUTHENTICATION FAILURE

RECOMMENDED ACTION

The following sites have authentication failures. Please check the reason and details for each.

□	Site	Reason	Details
□	Live-Demo	WLAN Corp	View More
□	Live-Demo	WLAN Mist_IoT	Affects 5 Clients
□	Live-Demo	WLAN Mist_IoT	Affects 4 Clients
□	Live-Demo	2 Switches	Affects 9 Clients

When you click **View More**, the card appears in a pop-up window. Here's a sample event card for an authentication failure.



AUTH Jan 5, 2024, 11:20:00 AM

A majority of failures were due to , specifically IEEE 802.1X authentication failed.

AUTH

The event card includes these sections:

- **Timeline**—The number of failure events at each point in time. Marvis highlights the anomalies with a magnifying glass icon. Click the icon to select an anomaly and view the details.
- **Summary**—A description of each anomaly and the most likely cause. It also indicates if the clients mostly failed on a certain radio band, access point (AP), or wireless LAN (WLAN). You can select different anomalies by clicking their titles.

- **Causes**—A graphical representation of the relative impact of the AP, WLAN, and radio band. The size of the circle indicates the correlation to failure, and the positions on the graph show the Failure Likelihood and the sitewide impact. You can click a device to display the information in the **Details** section.

- **Details**—A list of the impacted devices. The details change when you click a device type in the Causes graph. For example, click the AP icon in the graph to see the details for the APs.

Access Points Deployment Assessment

IN THIS SECTION

Overview

Read this topic to understand how to evaluate the sufficiency of the access points deployed at your site using Juniper Mist's Marvis Actions, Wireless Service Level Expectation (SLE), and RF Health and Utilization dashboard in Premium Analytics. You can use the details that are covered in this topic to determine if additional access points are required for optimal connectivity and user experience.

Methodology

Use the following tools and features to conduct the assessment:

- **Marvis Actions**: Utilize Marvis, the virtual network assistant, to analyze network issues, troubleshoot problems, and optimize performance.

- **Wireless SLE**: Monitor key performance indicators related to coverage, roaming, throughput, and capacity to gauge the effectiveness of the current access point deployment.

- **RF Health and Utilization dashboard in Premium Analytics**: Evaluate the radio frequency (RF) health, interference, and utilization to identify potential areas of improvement in the wireless network.

Assessment Criteria

The assessment will focus on the following aspects:

1. **Signal Coverage**: Analyze the signal strength and quality across the site to ensure comprehensive coverage and minimal dead zones.
2. **Roaming Performance**: Assess the seamless transition of client devices between access points to maintain uninterrupted connectivity.
3. **Throughput Analysis**: Evaluate the data transfer speeds and capacity to accommodate the expected user load and application demands.
4. **RF Health and Utilization**: Monitor RF health, interference, and spectrum utilization to optimize the performance of the wireless network.

Juniper Mist Tools

Juniper Mist™ is a subscription-based service. For more details about Juniper Mist subscriptions, see Juniper Mist Subscriptions and Subscription Requirements for Marvis Actions.

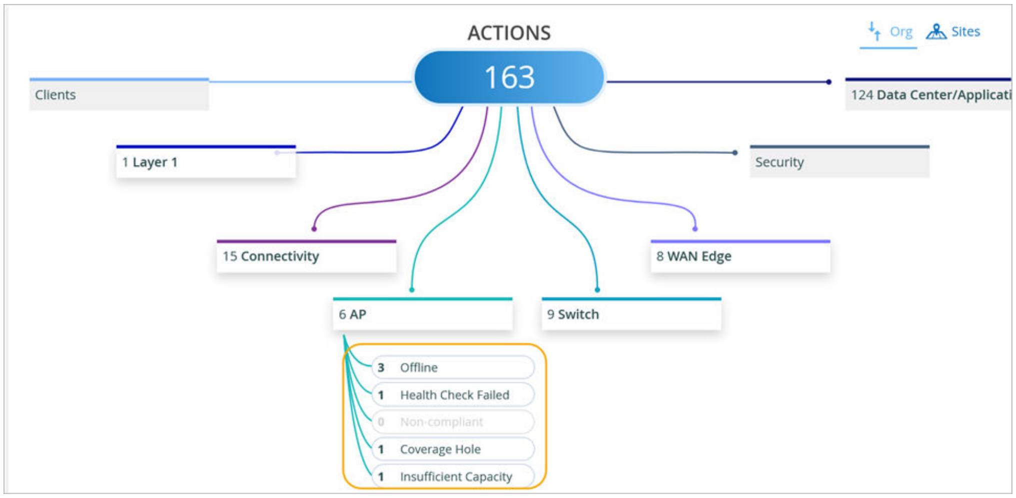
Marvis Actions

In order to ensure optimal network performance and coverage, it is essential to regularly assess the sufficiency of the Access Points (APs) deployed within your network. By leveraging the Marvis Actions in Juniper Mist portal, you can efficiently identify and address any issues affecting your APs.

To view the Marvis Actions dashboard, select **Marvis** > **Marvis Actions** from the left menu.

When you click the **AP** button on the Actions dashboard, you'll see a list of all available actions. You can then click an action to investigate further.

Figure 3: Marvis Actions



See Marvis Actions Overview for details.

Offline AP Detection

Marvis can detect APs that are offline due to various reasons, such as power loss or loss of cloud connectivity. This report indicates a need for further investigation or potential troubleshooting to restore connectivity.

Investigate the Offline AP action on the Actions dashboard to address any APs that are showing as offline. This report help in restoring network connectivity and ensuring seamless operation.

If Marvis identifies multiple APs as offline, it signals the need for immediate attention to resolve the connectivity issues impacting network performance.

Health Check Failures

Health check failures reported by Marvis might indicate underlying hardware or software issues affecting APs within the network. Swift action is required to rectify these issues to prevent any network disruptions.

Use the Health Check Failed action to investigate and address any APs experiencing health check failures. Consider hardware replacement or firmware upgrades as necessary steps to resolve the issue.

An AP that continuously fails health checks may need to be replaced or have its firmware upgraded to ensure proper functioning within the network.

Non-Compliant Firmware

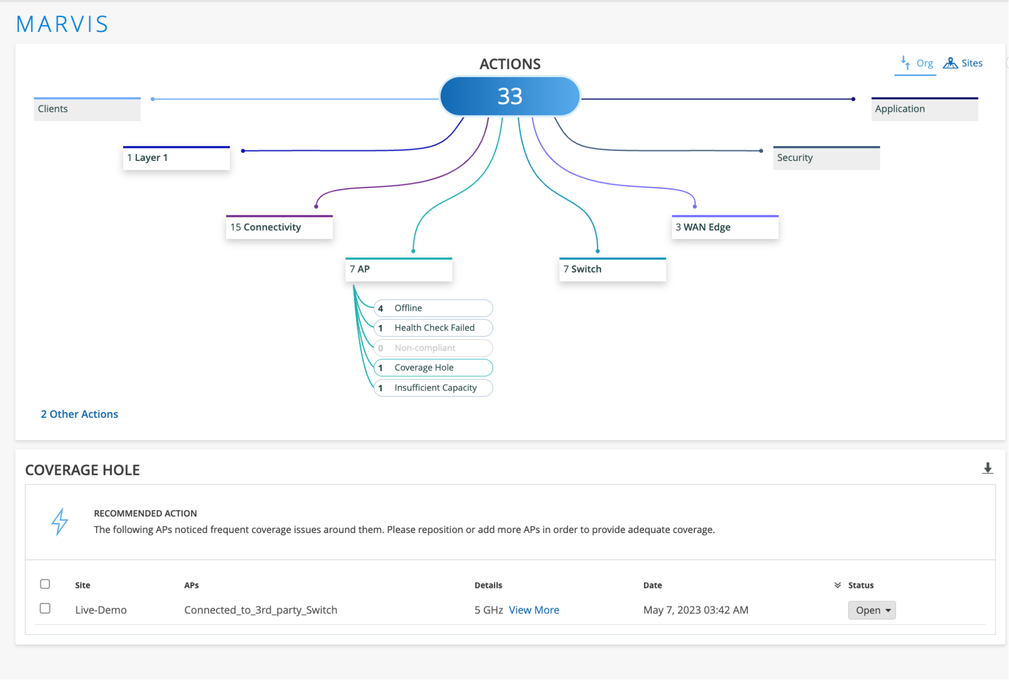
The Non-Compliant action flags APs running outdated firmware versions compared to other APs of the same model at the site. Updating firmware is crucial to ensure security, stability, and performance improvements.

Upgrade the firmware of Non-Compliant APs from the Marvis Actions page to align with the latest version. This step helps in maintaining consistency across APs and mitigating potential vulnerabilities.

A prompt upgrade of firmware on Non-Compliant APs can enhance network security and performance, ensuring all APs operate optimally within the network.

Coverage Hole Detection

The Coverage Hole action identifies areas within your network experiencing poor coverage, allowing you to optimize placement and configuration of APs to improve network efficiency.

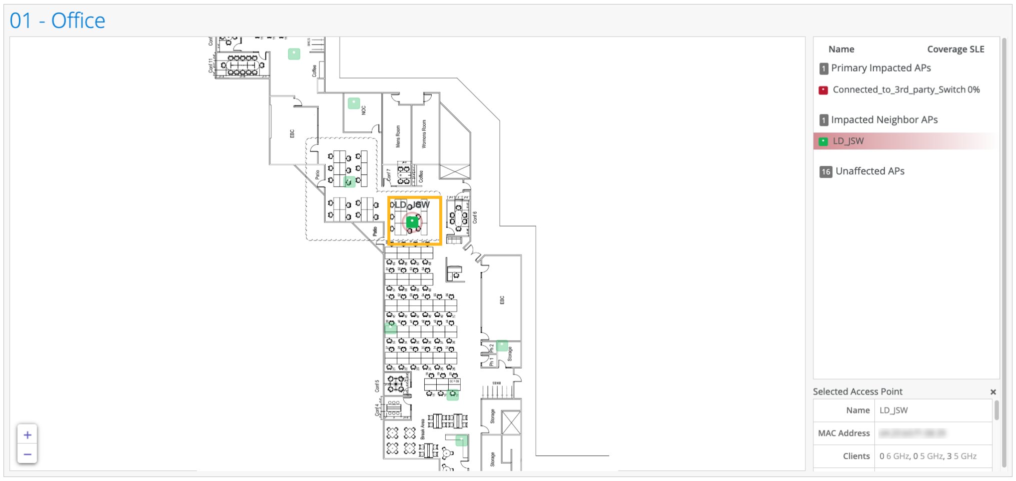


COVERAGE HOLE

RECOMMENDED ACTION
The following APs noticed frequent coverage issues around them. Please reposition or add more APs in order to provide adequate coverage.

☐	Site	APs	Details	Date	Status
☐	Live-Demo	Connected_to_3rd_party_Switch	5 GHz View More	May 7, 2023 03:42 AM	Open

Utilize the floor plan visual provided by Marvis to pinpoint areas with coverage issues and take necessary steps such as adding APs, adjusting placements, or increasing power output to address the coverage gaps.



01 - Office

Name	Coverage SLE
1 Primary Impacted APs	
🟥 Connected_to_3rd_party_Switch	0%
1 Impacted Neighbor APs	
🟩 LD_JSW	
16 Unaffected APs	

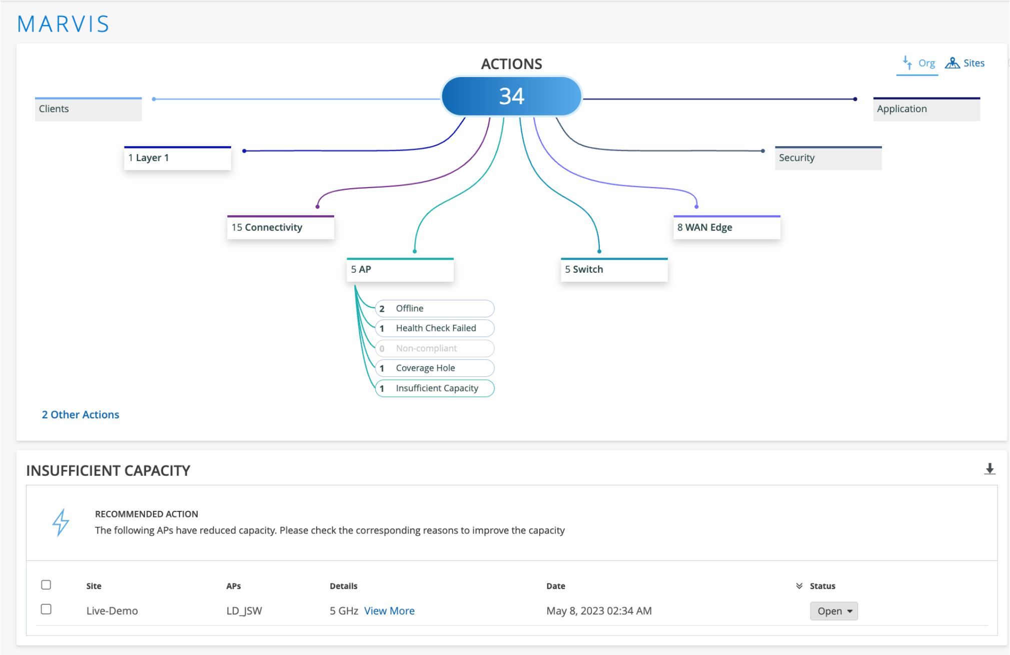
Selected Access Point ×

Name	LD_JSW
MAC Address	[redacted]
Clients	0 6 GHz, 0 5 GHz, 3 5 GHz

By identifying and resolving coverage holes promptly, you can enhance network connectivity and user experience, ensuring seamless communication across all areas.

Insufficient Capacity Alert

The Insufficient Capacity action detects capacity issues arising from increased utilization, especially during peak client traffic. Addressing capacity constraints is vital to maintain network performance and avoid congestion.



MARVIS

ACTIONS

34

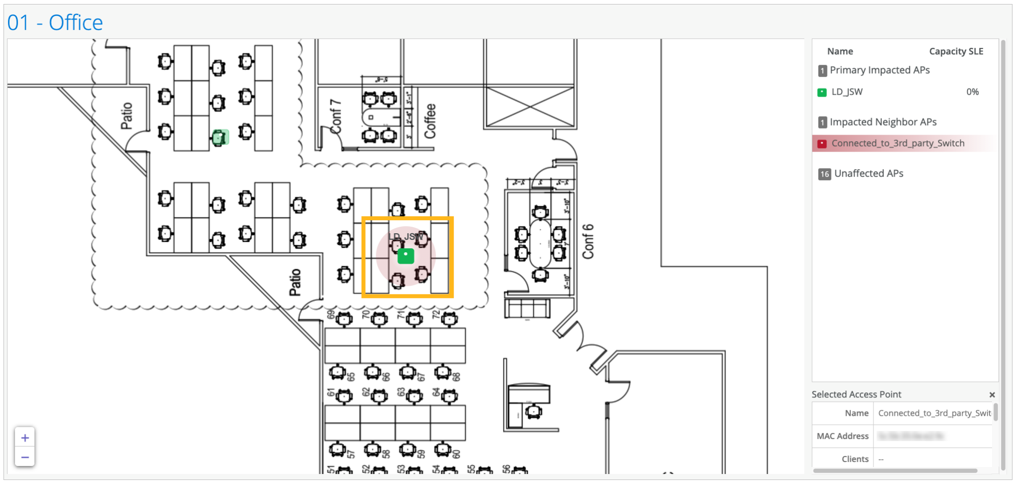
INSUFFICIENT CAPACITY

RECOMMENDED ACTION

The following APs have reduced capacity. Please check the corresponding reasons to improve the capacity

☐	Site	APs	Details	Date	Status
☐	Live-Demo	LD_JSW	5 GHz View More	May 8, 2023 02:34 AM	Open ▾

Analyze the floor plan visual provided by Marvis to identify APs experiencing capacity issues and make design improvements to alleviate congestion and optimize network capacity.



Name	Capacity SLE
1 Primary Impacted APs	
🟩 LD_JSW	0%
1 Impacted Neighbor APs	
🟥 Connected_to_3rd_party_Switch	
16 Unaffected APs	

Selected Access Point ×

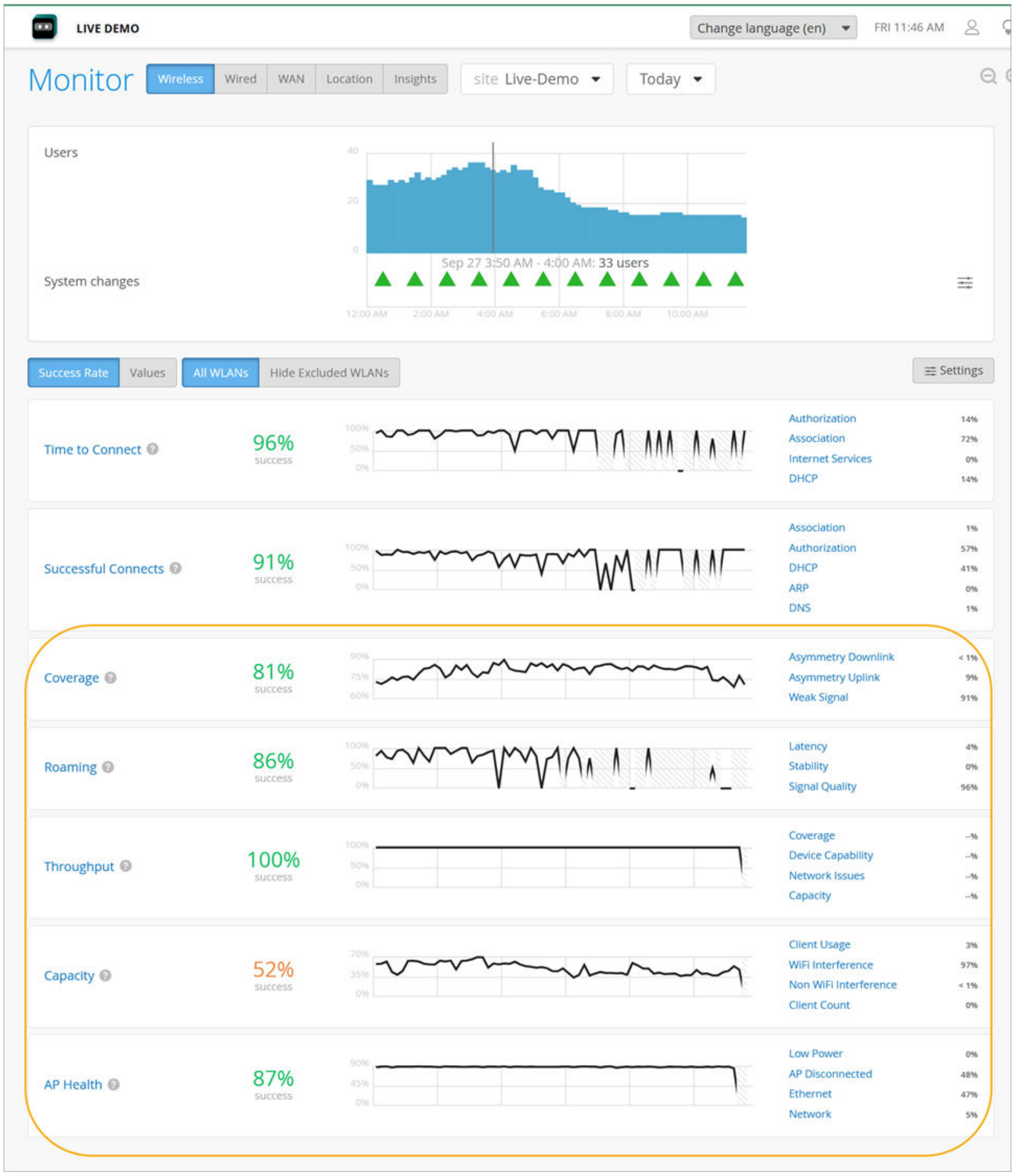
Name	Connected_to_3rd_party_Swit
MAC Address	[redacted]
Clients	--

Wireless SLE Analysis

Juniper Mist uses Service Level Expectations (SLEs) to measure user experiences, with customizable thresholds for factors like throughput, capacity, and device health. If experiences fall short, Juniper Mist identifies the root causes and provides detailed information for resolution. The SLE dashboard offers a quick overview of service levels and issues needing attention.

See Wireless SLEs Dashboard for more information.

Select **Monitor** > **Service Levels** from the left menu, and then click the **Wireless** button.



Time to Connect	96% success	Authorization 14% Association 72% Internet Services 0% DHCP 14%
Successful Connects	91% success	Association 1% Authorization 57% DHCP 41% ARP 0% DNS 1%
Coverage	81% success	Asymmetry Downlink < 1% Asymmetry Uplink 9% Weak Signal 91%
Roaming	86% success	Latency 4% Stability 0% Signal Quality 96%
Throughput	100% success	Coverage --% Device Capability --% Network Issues --% Capacity --%
Capacity	52% success	Client Usage 3% WiFi Interference 97% Non WiFi Interference < 1% Client Count 0%
AP Health	87% success	Low Power 0% AP Disconnected 48% Ethernet 47% Network 5%

Use the following SLE to assess your users' experiences with signal strength, throughput, RF channel capacity, roaming between APs, and APs availability.

1. **Signal Coverage:** Analyze the Received Signal Strength Indicator (RSSI) and signal quality data to identify areas with weak coverage or potential signal asymmetry.

2. **Roaming Performance:** Evaluate the success rate of client device roams between access points and identify any issues related to latency or signal stability.

3. **Throughput Analysis:** Assess the estimated per-client throughput and investigate any capacity or coverage-related constraints impacting user experience.

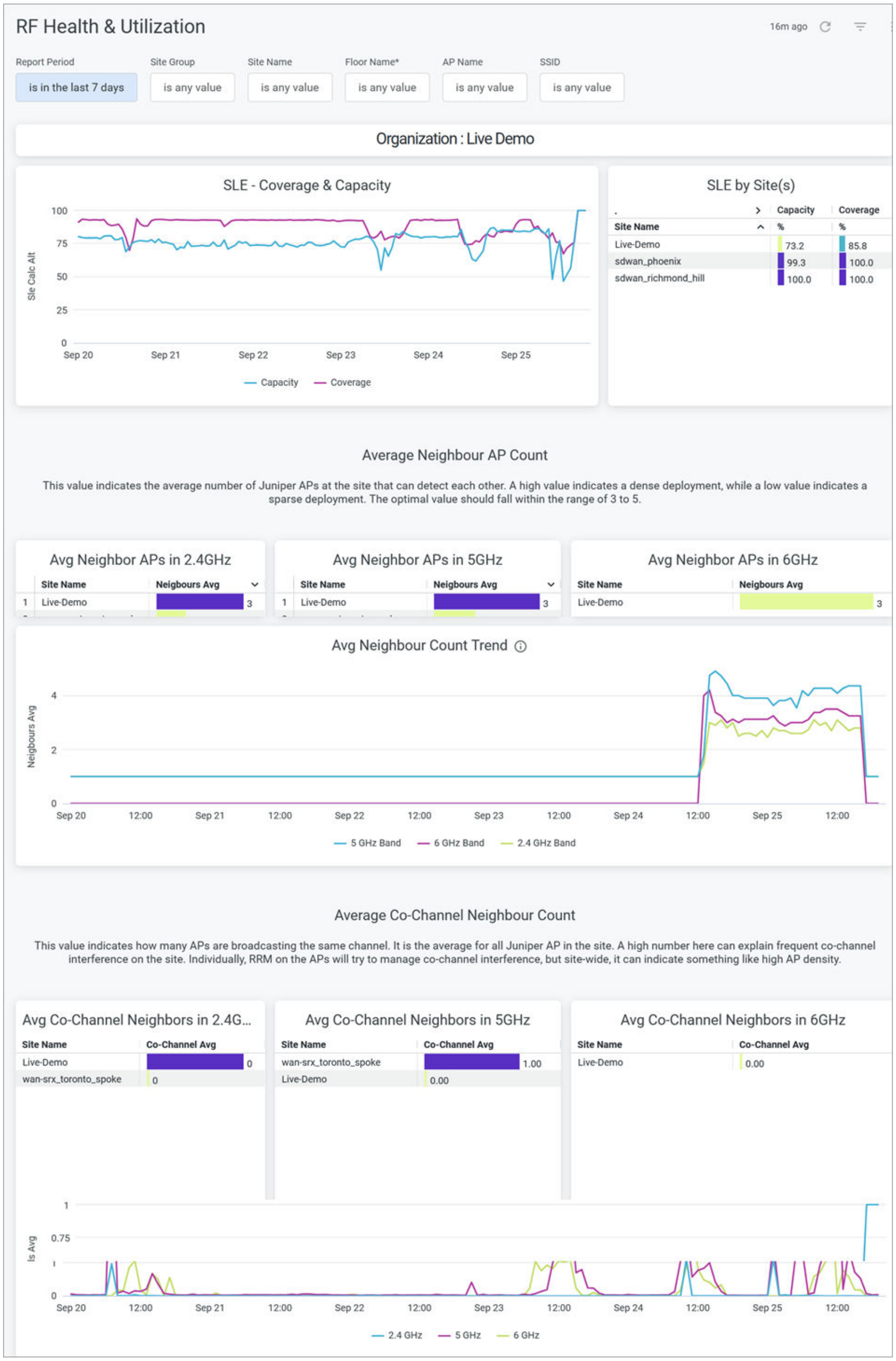
4. **Capacity Analysis:** Review the RF channel capacity availability and potential limitations due to interference or client usage.

5. **AP Health Status:** Track AP health to assess your users' experience with AP availability. Get percentage of time the APs are operational without rebooting or losing connectivity to the cloud.

RF Health and Utilization Dashboard in Premium Analytics

The RF Health and Utilization dashboard provides long-term radio frequency (RF) health and utilization pattern for your network. With the information, you can analyze channel utilization trends for different radio bands across various sites, floors, and access points (APs), ensuring optimal performance and capacity planning.

In Juniper Mist portal, click **Analytics** > **Premium Analytics**. On the Premium Analytics page, click **RF Health and Utilization**.



RF Health & Utilization

16m ago

Report Period	Site Group	Site Name	Floor Name*	AP Name	SSID
is in the last 7 days	is any value	is any value	is any value	is any value	is any value

Organization : Live Demo

SLE - Coverage & Capacity

SLE by Site(s)

.	Capacity	Coverage
Site Name	%	%
Live-Demo	73.2	85.8
sdwan_phoenix	99.3	100.0
sdwan_richmond_hill	100.0	100.0

Average Neighbour AP Count

This value indicates the average number of Juniper APs at the site that can detect each other. A high value indicates a dense deployment, while a low value indicates a sparse deployment. The optimal value should fall within the range of 3 to 5.

Avg Neighbor APs in 2.4GHz

	Site Name	Neigbours Avg
1	Live-Demo	3

Avg Neighbor APs in 5GHz

	Site Name	Neigbours Avg
1	Live-Demo	3

Avg Neighbor APs in 6GHz

Site Name	Neigbours Avg
Live-Demo	3

Avg Neighbour Count Trend

Average Co-Channel Neighbour Count

This value indicates how many APs are broadcasting the same channel. It is the average for all Juniper AP in the site. A high number here can explain frequent co-channel interference on the site. Individually, RRM on the APs will try to manage co-channel interference, but site-wide, it can indicate something like high AP density.

Avg Co-Channel Neighbors in 2.4G...

Site Name	Co-Channel Avg
Live-Demo	0
wan-srx_toronto_spoke	0

Avg Co-Channel Neighbors in 5GHz

Site Name	Co-Channel Avg
wan-srx_toronto_spoke	1.00
Live-Demo	0.00

Avg Co-Channel Neighbors in 6GHz

Site Name	Co-Channel Avg
Live-Demo	0.00

Here you can analyze channel utilization trends for different access points (APs).

SLE Coverage and Capacity: This report evaluates the SLE coverage and capacity across APs and sites, identifying sites with poor signal strength, high interference, or coverage gaps. By analyzing these metrics, you can determine where additional APs are needed to improve coverage and signal quality.

Average Neighbor AP Count: This value indicates the average number of APs at the site that can detect each other. A high count signifies a dense deployment, while a low count indicates a sparse deployment. Ideally, the value should range between 3 and 5 for optimal performance.

Average Co-Channel Neighbor Count: This value represents the number of APs broadcasting on the same channel, averaged across all Juniper APs at the site. A high count suggests frequent co-channel interference on the site. While individual APs use Radio Resource Management (RRM) to mitigate interference, a high site-wide count points to broader density challenges.

By using RF health and utilization data, you can make informed decisions about where to place new APs to balance the network load and enhance overall performance.

See RF Health and Utilization for details.

Recommendations

Based on the assessment findings, the following recommendations are proposed:

- Optimize the placement and configuration of existing access points to improve signal coverage and address any identified dead zones. See Access Point Placement for Location Services
- Implement recommended actions provided by Marvis to address ongoing network issues and enhance overall network performance. See Marvis Actions Overview.
- Consider the deployment of additional access points in areas with high client density or limited coverage to improve user experience and accommodate growing demand.
- Mitigate any identified RF interference sources and optimize spectrum utilization to ensure a healthy RF environment for the wireless network.

Regularly monitoring and addressing the actions highlighted by Marvis can help you maintain an efficient and reliable network infrastructure. This action ensures that the deployed APs are functioning optimally and meet the demands of your network environment.

RELATED DOCUMENTATION

AP Actions | 132

Service Level Expectations (SLE) | 0

No Link Title

No Link Title

7

CHAPTER

Marvis Minis

Marvis Minis Overview

SUMMARY

Get familiar with Marvis Minis and learn how it proactively validates your network and application services.

IN THIS SECTION

What Is Marvis Minis?

Marvis Minis is a network digital twin, which uses your network infrastructure to assess the network connectivity and service reachability of your network. By proactively simulating user connections through an access point (AP), Marvis Minis can help detect and resolve issues before they impact users. Marvis Minis is always on and can be initiated on-demand.

Marvis Minis runs validations automatically at regular intervals. Marvis can also trigger Marvis Minis validations automatically when it observes any imminent network service failures—even when users aren't connected to the network. If Marvis Minis observes a network service failure, it revalidates the failure and expands the validation scope of the failure to other APs and switches. By expanding the validation scope, Marvis Minis can identify the overall impact of the issue—that is, whether the issue impacts an entire site, a specific switch, WLAN, VLAN, server, or AP. Marvis Minis automatically scopes and validates any changes (such as new device additions, configuration changes, and so on) related to APs, switches, and WAN Edges.

Marvis Minis can run the validation across multiple sites in an organization or on a single site. Marvis automatically learns about the active APs, VLANs, and the applications that are being used on each site. This capability helps Marvis Minis to validate all user VLANs and specific APs without having to validate all APs. Data from Marvis Minis also serves as an additional source of information for Marvis.

Dynamic packet capture, client insights, and Marvis Actions provide insights and details of a failure. With these insights, you can identify the scope of the failure and resolve issues such as users being unable to connect to the network. By simulating actual user experience in a constant contextual learned scope, Marvis Minis identifies and resolves the same issue without putting additional stress on network services. For example, consider a site with 2000 APs connected to 200 switches. Marvis triggers Marvis Minis on approximately 200 APs. Based on the failure that Marvis Minis observes, it expands the validation scope to other APs only if necessary. This capability ensures that the network services do not experience additional load.

This video provides an introduction to Marvis Minis.

Video: Marvis Minis: Move from Reactive to Proactive Network Management (demo)

Software Requirements

All Juniper Mist™ AP models support Marvis Minis. Marvis Minis is enabled by default on APs running firmware version 0.14.29313 and later. Marvis Minis does not require any additional software or external sensor hardware.

> **NOTE**: All APs in the site must run firmware version 0.14 or later for Marvis Minis to run validations.

Subscriptions for Marvis Minis

Marvis Minis does not require a separate subscription. Any organization with an active Marvis for Wireless subscription is automatically entitled for Marvis Minis support.

Marvis Minis Tests

Marvis Minis learns all the APs, WLANs, switches, and active VLANs in a site and automatically creates the tests to run. Marvis Minis builds and updates its testing scopes for any new additions or changes in the site such as adding new APs, WLANs, or VLANs.

Marvis Minis runs validations when all the APs in the site are running firmware version 0.14.29313 or later. The automatic validations are run on an hourly basis. You can also trigger a Marvis Minis validation manually by using the **Test Now** button on the Marvis Minis site-level page.

Marvis Minis updates the scope every hour based on the active client VLAN and RRM details. The Marvis Minis validation scope includes only the WLAN-to-VLAN mapping if no clients are connected to the network.

Marvis Minis validates the following network services for all the active VLANs on the enabled wireless LANs to ensure that the site is operational:

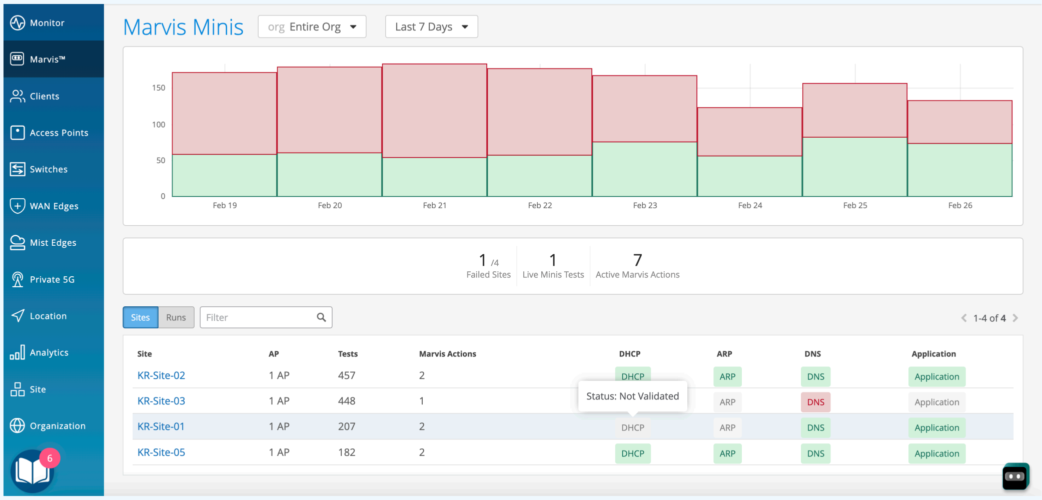
- Dynamic Host Configuration Protocol (DHCP)
- Address Resolution Protocol (ARP)
- Domain Name System (DNS)
- Application reachability

Marvis Minis simulates a user connection on active user VLANs and validates the connectivity process using the following steps:

1. Sends a DHCP request for a client VLAN and reports whether the VLAN obtains an IP address. The AP sends both broadcast discovers and unicast renews.
2. Generates an ARP request for the gateway.
3. Resolves DNS queries against all the DNS server IP addresses received in the DHCP offer.
4. Verifies Internet reachability by validating application reachability. Marvis Minis verifies application reachability by using default Internet connectivity URLs such as captive.apple.com, connectivitycheck.gstatic.com, office.com, and teams.microsoft.com. Marvis Minis also validates reachability for Office365. You can define custom user applications in the organization or site settings.
5. Explicitly releases the DHCP lease on the tested VLAN.

NOTE: When the client VLAN is the same as the AP management VLAN, the AP would have obtained an IP address already and resolved ARP. In such a scenario, Marvis Minis validates only DNS and application reachability as part of the preconnect failure checks. It does not send a DHCP request, nor does it revalidate ARP resolution for the AP management VLAN.

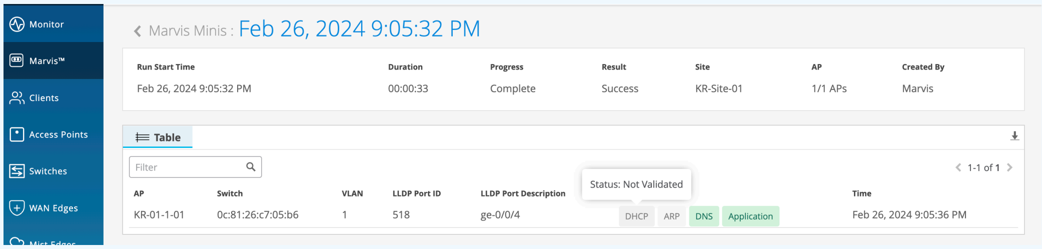
Here is an example that shows the Marvis Minis dashboard for this scenario. Notice that Marvis Minis reports the status for only DNS and Application for the site KR-Site-01. If you hover your mouse over DHCP and ARP, you'll see the status as **Not Validated**.



1 /4 Failed Sites | 1 Live Minis Tests | 7 Active Marvis Actions

Site	AP	Tests	Marvis Actions	DHCP	ARP	DNS	Application
KR-Site-02	1 AP	457	2	DHCP	ARP	DNS	Application
KR-Site-03	1 AP	448	1	Status: Not Validated	ARP	DNS	Application
KR-Site-01	1 AP	207	2	DHCP	ARP	DNS	Application
KR-Site-05	1 AP	182	2	DHCP	ARP	DNS	Application

Here's the detailed view when you click the site.



Marvis Minis : Feb 26, 2024 9:05:32 PM

Run Start Time	Duration	Progress	Result	Site	AP	Created By
Feb 26, 2024 9:05:32 PM	00:00:33	Complete	Success	KR-Site-01	1/1 APs	Marvis

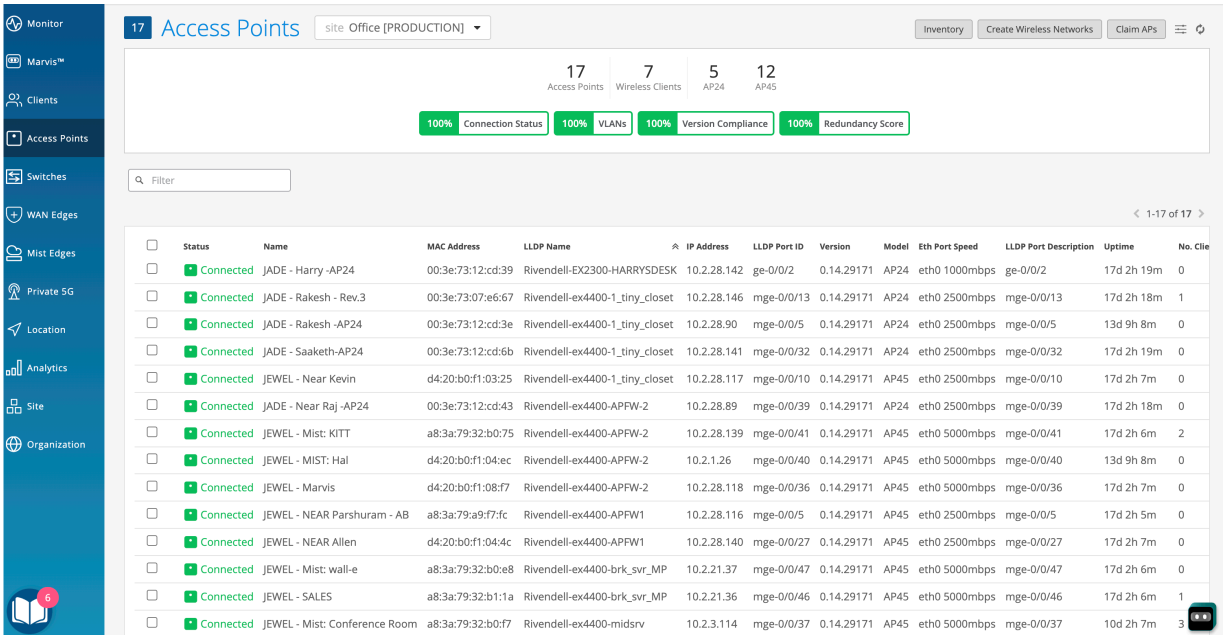
Status: Not Validated

AP	Switch	VLAN	LLDP Port ID	LLDP Port Description		Time
KR-01-1-01	0c:81:26:c7:05:b6	1	518	ge-0/0/4	DHCP ARP DNS Application	Feb 26, 2024 9:05:36 PM

If Marvis Minis detects any failure in DHCP, ARP, DNS, and application reachability on any VLAN, it performs the following checks to understand the scope of failure—whether it is limited to an AP, a switch, or an entire site:

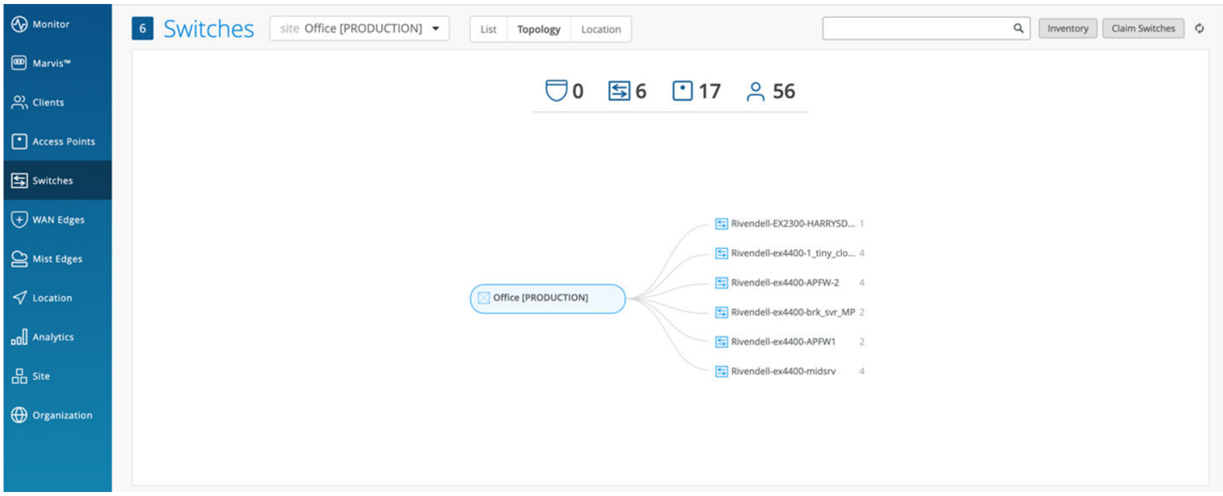
1. Retests the connectivity on the failed AP.
2. Tests whether the issue occurs on another AP connected to the same switch.
3. Tests whether the issue occurs on an AP connected to a different switch.
4. Verifies whether the failure scope is limited to an AP, a switch, or a site for that VLAN.

In the following example, a site has 17 APs connected across 6 switches. The validation scope includes 6 APs - one AP connected to each switch and the relevant VLANs.

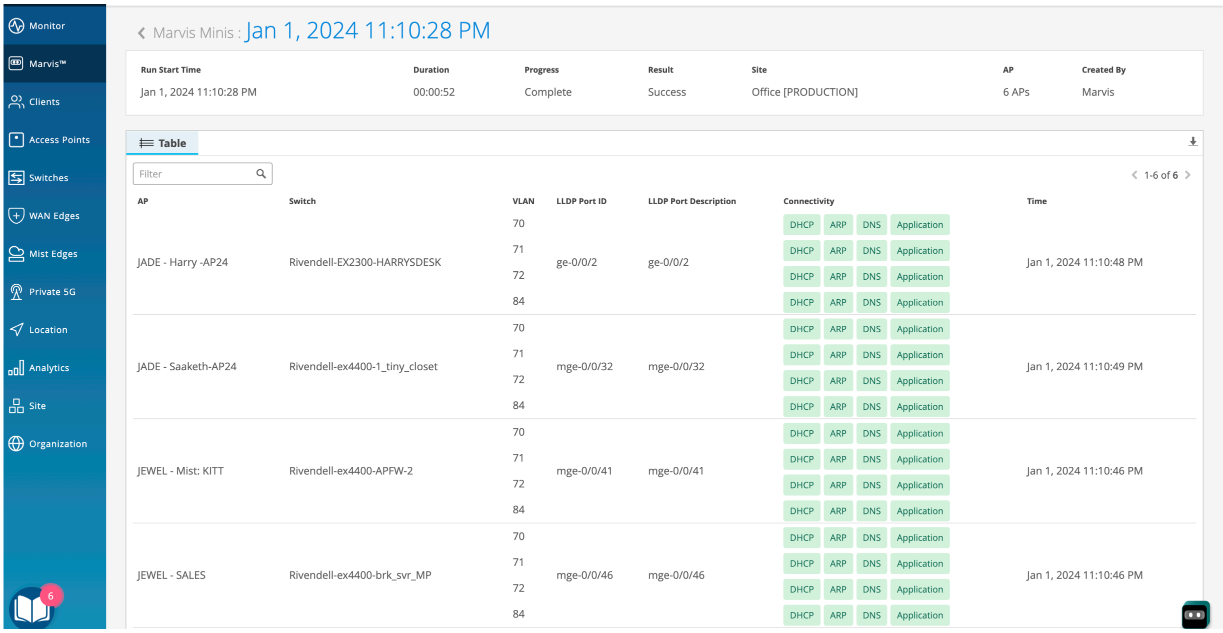


□	Status	Name	MAC Address	LLDP Name	IP Address	LLDP Port ID	Version	Model	Eth Port Speed	LLDP Port Description	Uptime	No. Clie
□	Connected	JADE - Harry -AP24	00:3e:73:12:cd:39	Rivendell-EX2300-HARRYSDESK	10.2.28.142	ge-0/0/2	0.14.29171	AP24	eth0 1000mbps	ge-0/0/2	17d 2h 19m	0
□	Connected	JADE - Rakesh - Rev.3	00:3e:73:07:e6:67	Rivendell-ex4400-1_tiny_closet	10.2.28.146	mge-0/0/13	0.14.29171	AP24	eth0 2500mbps	mge-0/0/13	17d 2h 18m	1
□	Connected	JADE - Rakesh -AP24	00:3e:73:12:cd:3e	Rivendell-ex4400-1_tiny_closet	10.2.28.90	mge-0/0/5	0.14.29171	AP24	eth0 2500mbps	mge-0/0/5	13d 9h 8m	0
□	Connected	JADE - Saaketh-AP24	00:3e:73:12:cd:6b	Rivendell-ex4400-1_tiny_closet	10.2.28.141	mge-0/0/32	0.14.29171	AP24	eth0 2500mbps	mge-0/0/32	17d 2h 19m	0
□	Connected	JEWEL - Near Kevin	d4:20:b0:f1:03:25	Rivendell-ex4400-1_tiny_closet	10.2.28.117	mge-0/0/10	0.14.29171	AP45	eth0 2500mbps	mge-0/0/10	17d 2h 7m	0
□	Connected	JADE - Near Raj -AP24	00:3e:73:12:cd:43	Rivendell-ex4400-APFW-2	10.2.28.89	mge-0/0/39	0.14.29171	AP24	eth0 2500mbps	mge-0/0/39	17d 2h 18m	0
□	Connected	JEWEL - Mist: KITT	a8:3a:79:32:b0:75	Rivendell-ex4400-APFW-2	10.2.28.139	mge-0/0/41	0.14.29171	AP45	eth0 5000mbps	mge-0/0/41	17d 2h 6m	2
□	Connected	JEWEL - MIST: Hal	d4:20:b0:f1:04:ec	Rivendell-ex4400-APFW-2	10.2.1.26	mge-0/0/40	0.14.29171	AP45	eth0 5000mbps	mge-0/0/40	13d 9h 8m	0
□	Connected	JEWEL - Marvis	d4:20:b0:f1:08:f7	Rivendell-ex4400-APFW-2	10.2.28.118	mge-0/0/36	0.14.29171	AP45	eth0 5000mbps	mge-0/0/36	17d 2h 7m	0
□	Connected	JEWEL - NEAR Parshuram - AB	a8:3a:79:a9:f7:fc	Rivendell-ex4400-APFW1	10.2.28.116	mge-0/0/5	0.14.29171	AP45	eth0 2500mbps	mge-0/0/5	17d 2h 5m	0
□	Connected	JEWEL - NEAR Allen	d4:20:b0:f1:04:4c	Rivendell-ex4400-APFW1	10.2.28.140	mge-0/0/27	0.14.29171	AP45	eth0 2500mbps	mge-0/0/27	17d 2h 7m	0
□	Connected	JEWEL - Mist: wall-e	a8:3a:79:32:b0:e8	Rivendell-ex4400-brk_svr_MP	10.2.21.37	mge-0/0/47	0.14.29171	AP45	eth0 5000mbps	mge-0/0/47	17d 2h 6m	0
□	Connected	JEWEL - SALES	a8:3a:79:32:b1:1a	Rivendell-ex4400-brk_svr_MP	10.2.21.36	mge-0/0/46	0.14.29171	AP45	eth0 5000mbps	mge-0/0/46	17d 2h 6m	1
□	Connected	JEWEL - Mist: Conference Room	a8:3a:79:32:b0:f7	Rivendell-ex4400-midsrv	10.2.3.114	mge-0/0/37	0.14.29171	AP45	eth0 5000mbps	mge-0/0/37	10d 2h 7m	3

The **Switches > Topology** page shows the six switches to which the APs are connected.



Here is the Marvis Minis page that shows the validation results:



Marvis Minis : Jan 1, 2024 11:10:28 PM

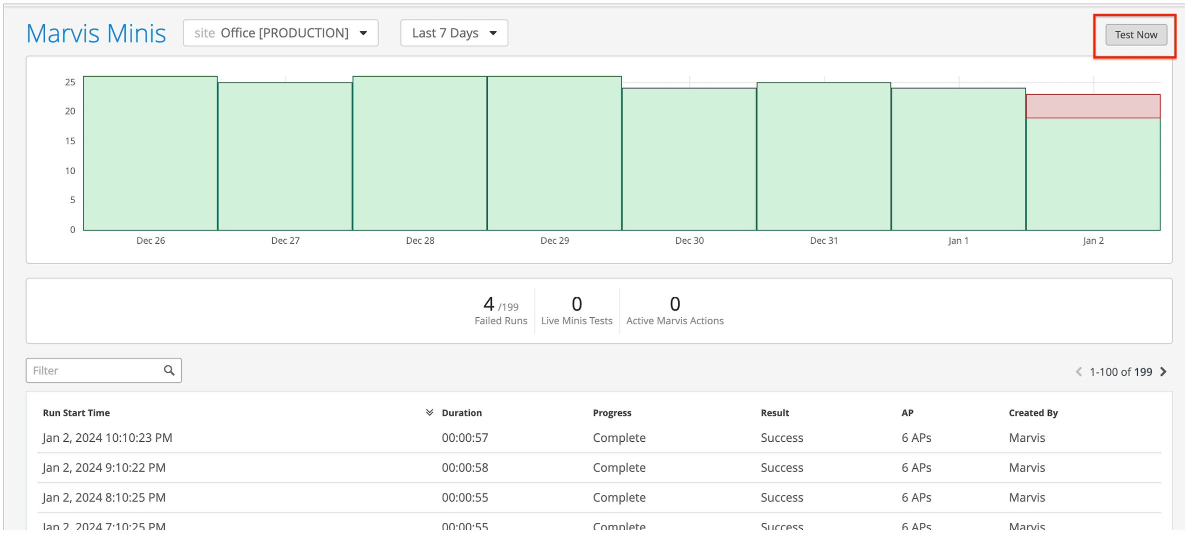
Run Start Time	Duration	Progress	Result	Site	AP	Created By
Jan 1, 2024 11:10:28 PM	00:00:52	Complete	Success	Office [PRODUCTION]	6 APs	Marvis

AP	Switch	VLAN	LLDP Port ID	LLDP Port Description	Connectivity	Time
JADE - Harry -AP24	Rivendell-EX2300-HARRYSDESK	70	ge-0/0/2	ge-0/0/2	DHCP ARP DNS Application	Jan 1, 2024 11:10:48 PM
		71			DHCP ARP DNS Application	
		72			DHCP ARP DNS Application	
		84			DHCP ARP DNS Application	
JADE - Saaketh-AP24	Rivendell-ex4400-1_tiny_closet	70	mge-0/0/32	mge-0/0/32	DHCP ARP DNS Application	Jan 1, 2024 11:10:49 PM
		71			DHCP ARP DNS Application	
		72			DHCP ARP DNS Application	
		84			DHCP ARP DNS Application	
JEWEL - Mist: KITT	Rivendell-ex4400-APFW-2	70	mge-0/0/41	mge-0/0/41	DHCP ARP DNS Application	Jan 1, 2024 11:10:46 PM
		71			DHCP ARP DNS Application	
		72			DHCP ARP DNS Application	
		84			DHCP ARP DNS Application	
JEWEL - SALES	Rivendell-ex4400-brk_svr_MP	70	mge-0/0/46	mge-0/0/46	DHCP ARP DNS Application	Jan 1, 2024 11:10:46 PM
		71			DHCP ARP DNS Application	
		72			DHCP ARP DNS Application	
		84			DHCP ARP DNS Application	

Marvis Minis Validation Frequency

Marvis Minis validations can be triggered either automatically or manually.

- Automatic validation—Marvis Minis runs the validation every hour even if no clients are connected to the network. If only a few clients experience network failures, Marvis Minis runs a validation to confirm whether the issue is specific to a client or whether it is a network issue.
- Manual (on-demand) validation—As an administrator, you can initiate an on-demand Marvis Minis validation at any time. When a configuration change or hardware change occurs in the network, administrators can click the **Test Now** button in the top-right corner of the Marvis Minis page to initiate the validation immediately. Ensure that you have selected the site you want to test from the site selector drop-down list.

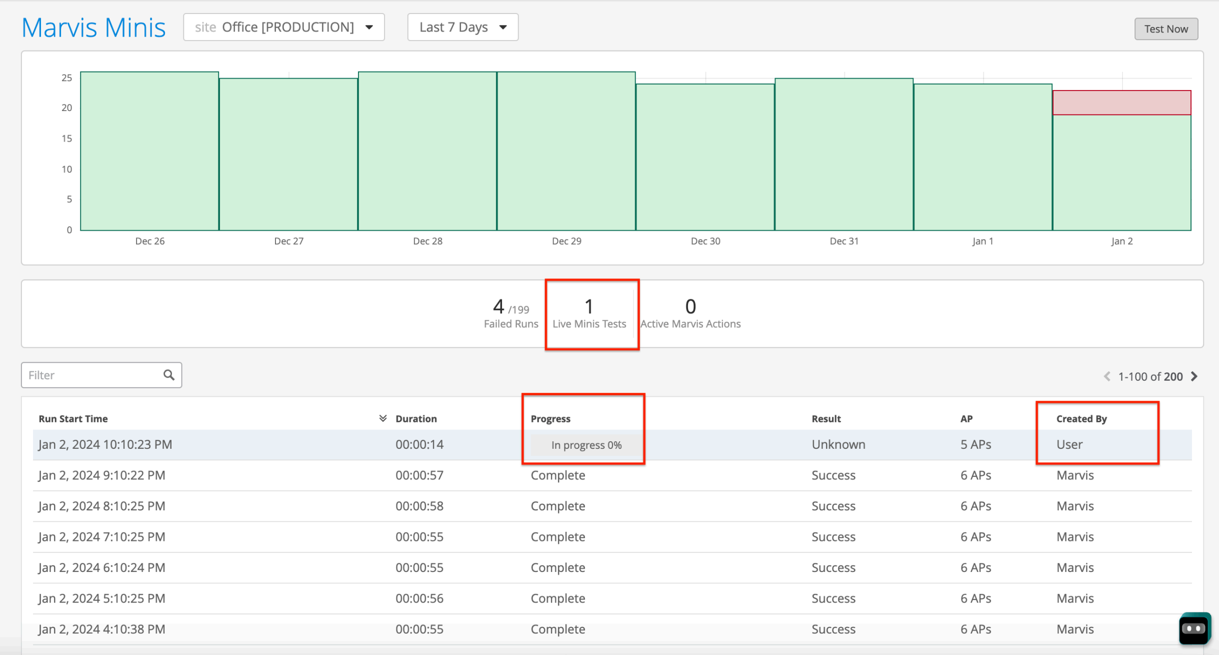


4 /199 Failed Runs | 0 Live Minis Tests | 0 Active Marvis Actions

Run Start Time	Duration	Progress	Result	AP	Created By
Jan 2, 2024 10:10:23 PM	00:00:57	Complete	Success	6 APs	Marvis
Jan 2, 2024 9:10:22 PM	00:00:58	Complete	Success	6 APs	Marvis
Jan 2, 2024 8:10:25 PM	00:00:55	Complete	Success	6 APs	Marvis
Jan 2, 2024 7:10:25 PM	00:00:55	Complete	Success	6 APs	Marvis

> **NOTE**: At any point in time, Marvis Minis runs only one validation per site. If an automated validation is in progress, you cannot trigger a manual validation.

Notice that the **Live Minis Tests** statistic shows a value of 1, which indicates that a validation is in progress. The table also shows the progress of the validation. Also, note that the **Created By** column lists *User* because the validation was triggered manually.

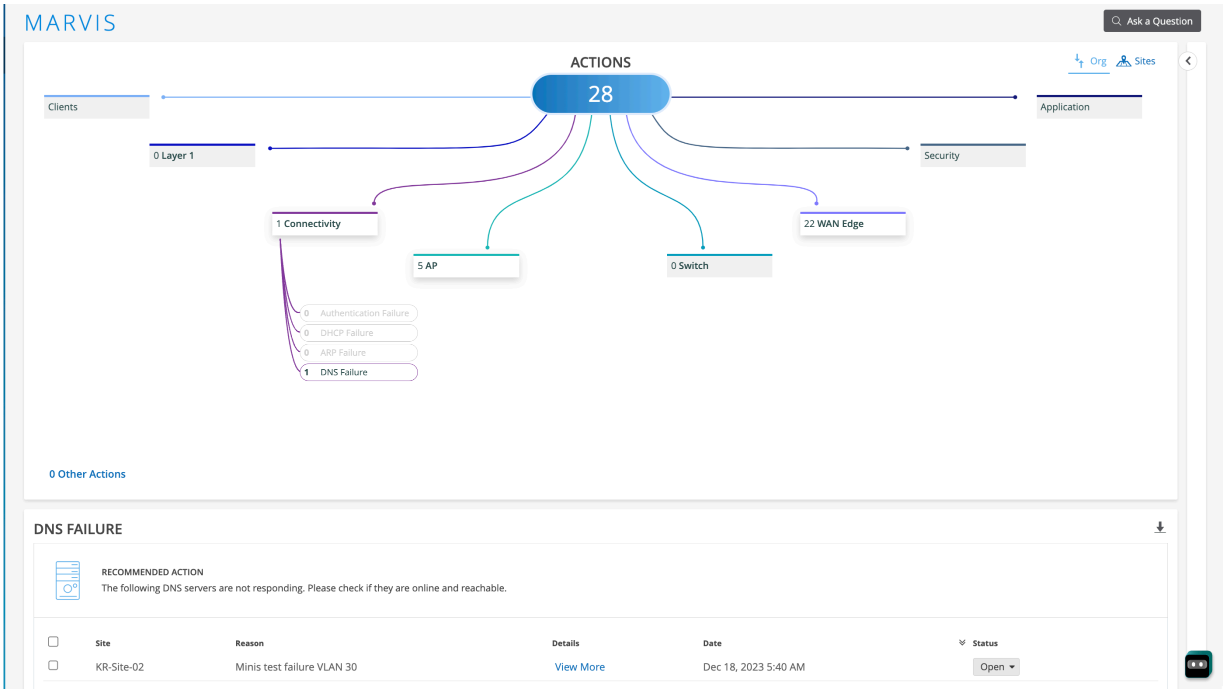


4 /199 Failed Runs | 1 Live Minis Tests | 0 Active Marvis Actions

Run Start Time	Duration	Progress	Result	AP	Created By
Jan 2, 2024 10:10:23 PM	00:00:14	In progress 0%	Unknown	5 APs	User
Jan 2, 2024 9:10:22 PM	00:00:57	Complete	Success	6 APs	Marvis
Jan 2, 2024 8:10:25 PM	00:00:58	Complete	Success	6 APs	Marvis
Jan 2, 2024 7:10:25 PM	00:00:55	Complete	Success	6 APs	Marvis
Jan 2, 2024 6:10:24 PM	00:00:55	Complete	Success	6 APs	Marvis
Jan 2, 2024 5:10:25 PM	00:00:56	Complete	Success	6 APs	Marvis
Jan 2, 2024 4:10:38 PM	00:00:55	Complete	Success	6 APs	Marvis

Marvis Actions for Marvis Minis

Marvis constantly receives data observed by Marvis Minis. Marvis ingests this additional data and lists Marvis Minis-detected failures under the **Connectivity** category on the Marvis Actions page. Marvis Actions provides visibility into all the ongoing issues that impact user experience in an organization. Here is an example that shows how a Marvis Minis-detected failure is listed as an action. Notice that Marvis attributes the failure reason to Marvis Minis validation.



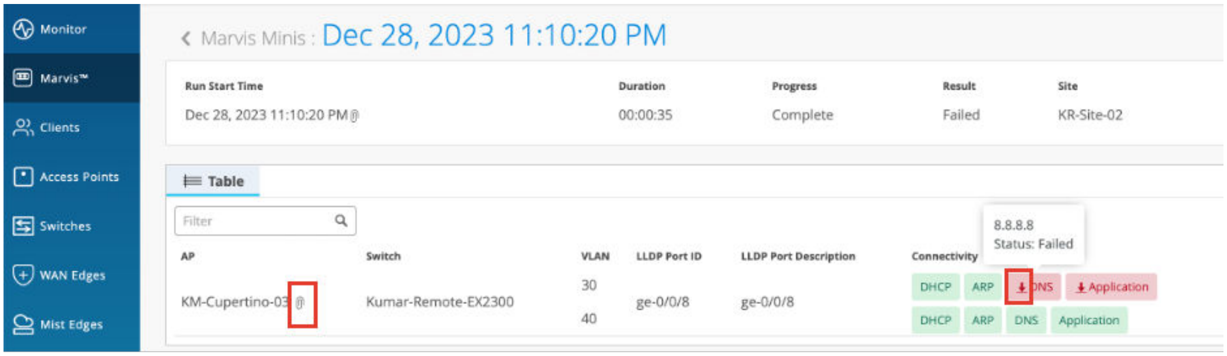
DNS FAILURE

RECOMMENDED ACTION

The following DNS servers are not responding. Please check if they are online and reachable.

□	Site	Reason	Details	Date	Status
□	KR-Site-02	Minis test failure VLAN 30	View More	Dec 18, 2023 5:40 AM	Open ▾

You can click the **View More** link to view the details and scope of the failure on the Marvis Minis page. You can download the dynamic packet capture (.pcap) file for any Marvis Minis-observed failure in the same way as you would for an end-user client. A paper clip icon adjacent to the AP name indicates that dynamic packet capture is available for the AP. The following screenshot shows the location of the paper clip icon. Click the Download (↓) button to access the packet capture.



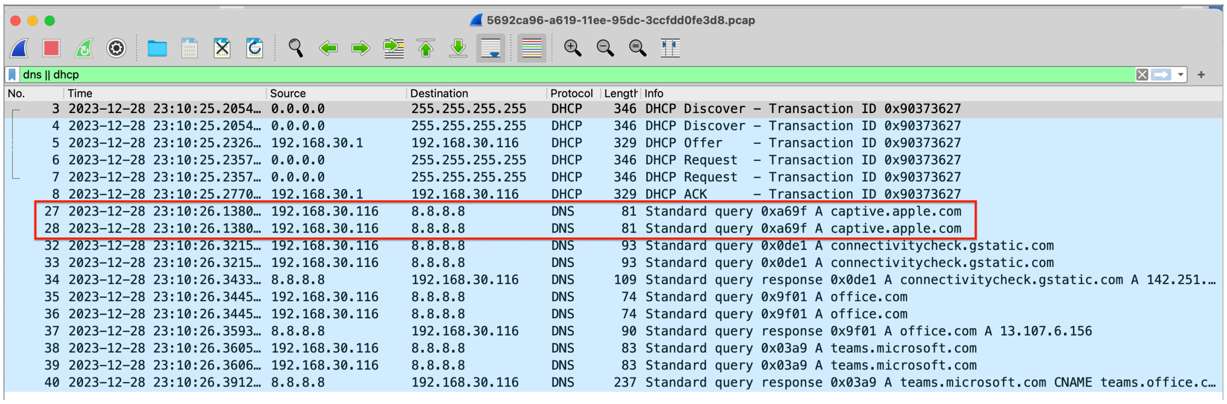
Marvis Minis : Dec 28, 2023 11:10:20 PM

Run Start Time	Duration	Progress	Result	Site
Dec 28, 2023 11:10:20 PM	00:00:35	Complete	Failed	KR-Site-02

8.8.8.8
Status: Failed

AP	Switch	VLAN	LLDP Port ID	LLDP Port Description	Connectivity
KM-Cupertino-03	Kumar-Remote-EX2300	30 40	ge-0/0/8	ge-0/0/8	DHCP ARP DNS Application DHCP ARP DNS Application

Here is a sample of a downloaded packet capture:



5692ca96-a619-11ee-95dc-3ccfdd0fe3d8.pcap

dns || dhcp

```
No. Time                     Source          Destination      Protocol Length Info
  3 2023-12-28 23:10:25.2054… 0.0.0.0         255.255.255.255  DHCP     346 DHCP Discover - Transaction ID 0x90373627
  4 2023-12-28 23:10:25.2054… 0.0.0.0         255.255.255.255  DHCP     346 DHCP Discover - Transaction ID 0x90373627
  5 2023-12-28 23:10:25.2326… 192.168.30.1    192.168.30.116   DHCP     329 DHCP Offer    - Transaction ID 0x90373627
  6 2023-12-28 23:10:25.2357… 0.0.0.0         255.255.255.255  DHCP     346 DHCP Request  - Transaction ID 0x90373627
  7 2023-12-28 23:10:25.2357… 0.0.0.0         255.255.255.255  DHCP     346 DHCP Request  - Transaction ID 0x90373627
  8 2023-12-28 23:10:25.2770… 192.168.30.1    192.168.30.116   DHCP     329 DHCP ACK      - Transaction ID 0x90373627
 27 2023-12-28 23:10:26.1380… 192.168.30.116  8.8.8.8          DNS       81 Standard query 0xa69f A captive.apple.com
 28 2023-12-28 23:10:26.1380… 192.168.30.116  8.8.8.8          DNS       81 Standard query 0xa69f A captive.apple.com
 32 2023-12-28 23:10:26.3215… 192.168.30.116  8.8.8.8          DNS       93 Standard query 0x0de1 A connectivitycheck.gstatic.com
 33 2023-12-28 23:10:26.3215… 192.168.30.116  8.8.8.8          DNS       93 Standard query 0x0de1 A connectivitycheck.gstatic.com
 34 2023-12-28 23:10:26.3433… 8.8.8.8         192.168.30.116   DNS      109 Standard query response 0x0de1 A connectivitycheck.gstatic.com A 142.251.…
 35 2023-12-28 23:10:26.3445… 192.168.30.116  8.8.8.8          DNS       74 Standard query 0x9f01 A office.com
 36 2023-12-28 23:10:26.3445… 192.168.30.116  8.8.8.8          DNS       74 Standard query 0x9f01 A office.com
 37 2023-12-28 23:10:26.3593… 8.8.8.8         192.168.30.116   DNS       90 Standard query response 0x9f01 A office.com A 13.107.6.156
 38 2023-12-28 23:10:26.3605… 192.168.30.116  8.8.8.8          DNS       83 Standard query 0x03a9 A teams.microsoft.com
 39 2023-12-28 23:10:26.3606… 192.168.30.116  8.8.8.8          DNS       83 Standard query 0x03a9 A teams.microsoft.com
 40 2023-12-28 23:10:26.3912… 8.8.8.8         192.168.30.116   DNS      237 Standard query response 0x03a9 A teams.microsoft.com CNAME teams.office.c…
```

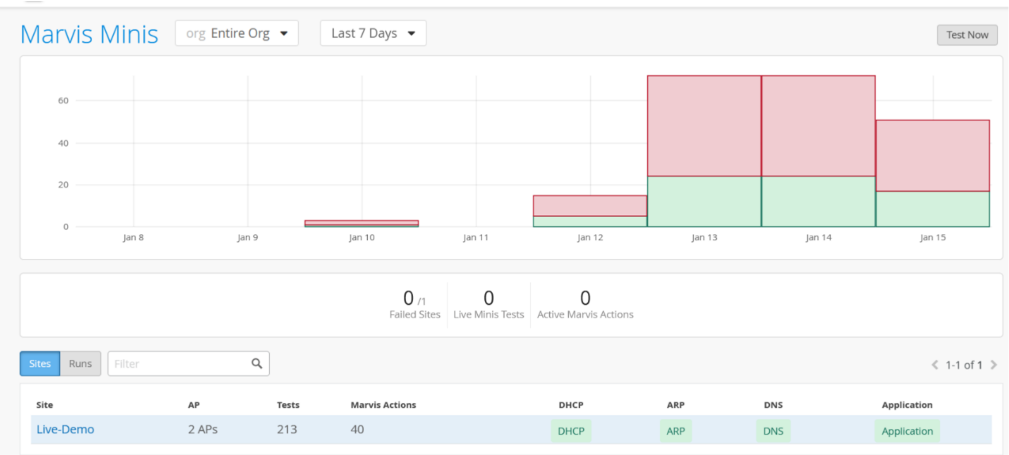
NOTE: After you fix the Marvis Minis detected issue, it might take up to 24 hours for the Marvis action to be automatically resolved—that is, the issue is no longer listed on the Marvis Actions page after 24 hours. This resolution time ensures that Marvis does not generate the same action again and rules out reoccurrences of the same issue within 24 hours.

Marvis Minis Dashboard Overview

IN THIS SECTION

The Marvis Minis dashboard provides visibility into the validation results. To view the Marvis Minis dashboard, select **Marvis** > **Marvis Minis** from the left menu.

In this example, you'll see the major elements of the dashboard:



0 /1 Failed Sites
0 Live Minis Tests
0 Active Marvis Actions

Site	AP	Tests	Marvis Actions	DHCP	ARP	DNS	Application
Live-Demo	2 APs	213	40	DHCP	ARP	DNS	Application

At the top of the page, you'll see a graphical representation of the total validations executed, with the green block indicating the number of successful validations. You can click each block to view the details of each validation.

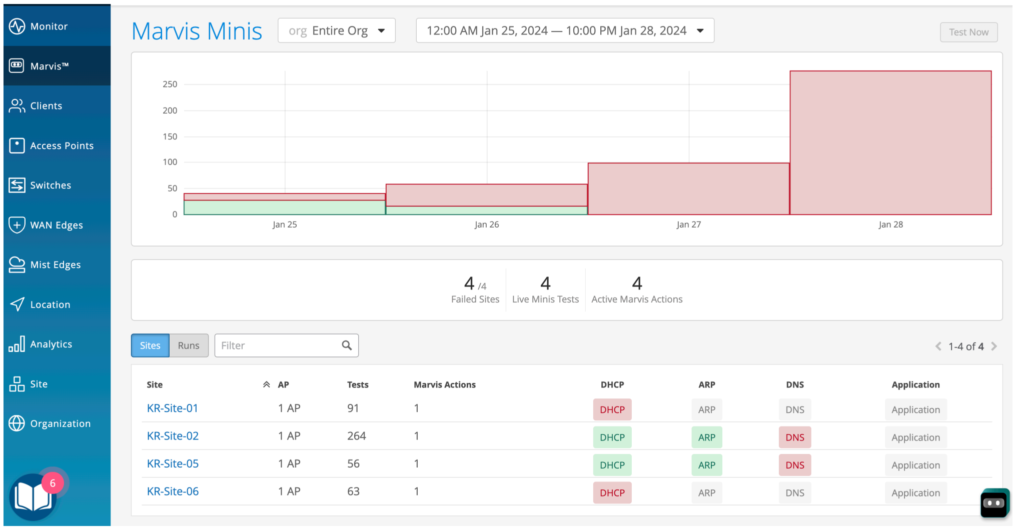
Directly below the graph, you'll see the following statistics for the organization:

- Failed sites—Number of sites that failed the validation.
- Live Minis Tests—Number of validations that are being run currently. Marvis runs only one validation per site at a time. You cannot trigger a manual validation when an automated validation is in progress.
- Active Marvis Actions—Number of actions detected by Marvis Minis at the organization level.

The table at the bottom of the page displays the results that are based on the context you select—an entire organization or a single site.

Organization-Level Marvis Minis Dashboard

Here is an example of the Marvis Minis dashboard view for an organization:



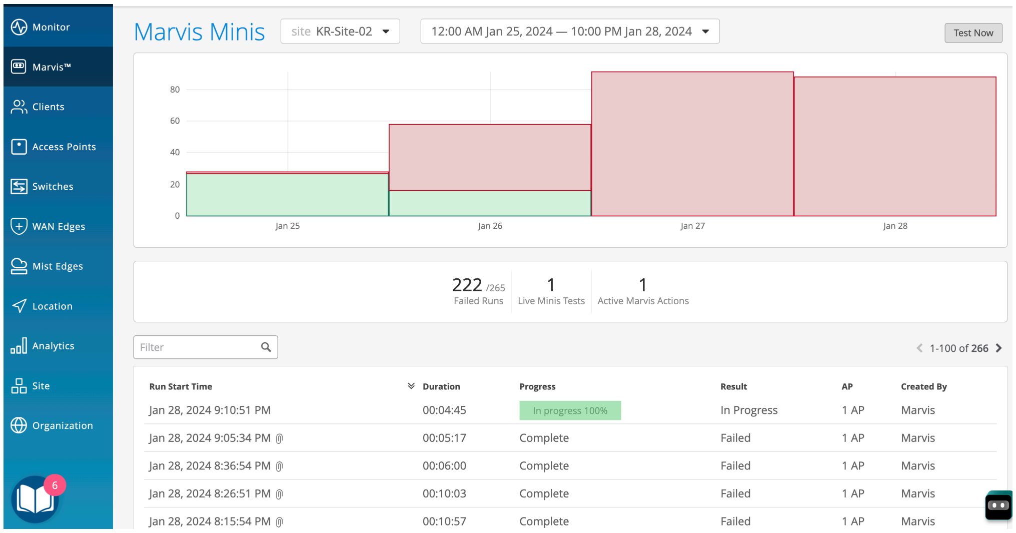
4 /4 Failed Sites | 4 Live Minis Tests | 4 Active Marvis Actions

Site	AP	Tests	Marvis Actions	DHCP	ARP	DNS	Application
KR-Site-01	1 AP	91	1	DHCP	ARP	DNS	Application
KR-Site-02	1 AP	264	1	DHCP	ARP	DNS	Application
KR-Site-05	1 AP	56	1	DHCP	ARP	DNS	Application
KR-Site-06	1 AP	63	1	DHCP	ARP	DNS	Application

The **Sites** tab displays all the sites in the organization. The table includes:

- Site—The name of the site where the validation was run.
- AP—APs on which Marvis Minis validation is triggered.
- Tests—The number of times the validation was run on the site for the selected timeline (automated and triggered).
- Marvis Actions—Lists the number of Marvis Actions detected by Marvis Minis for the site.
- Network and application services—Marvis Minis provides the validation results for a site for the following network and application services:
  - DHCP
  - ARP
  - DNS
  - Application connectivity

You can view the details of each validation run on a site by clicking the site name. In this example, you can see the validations run on a site.

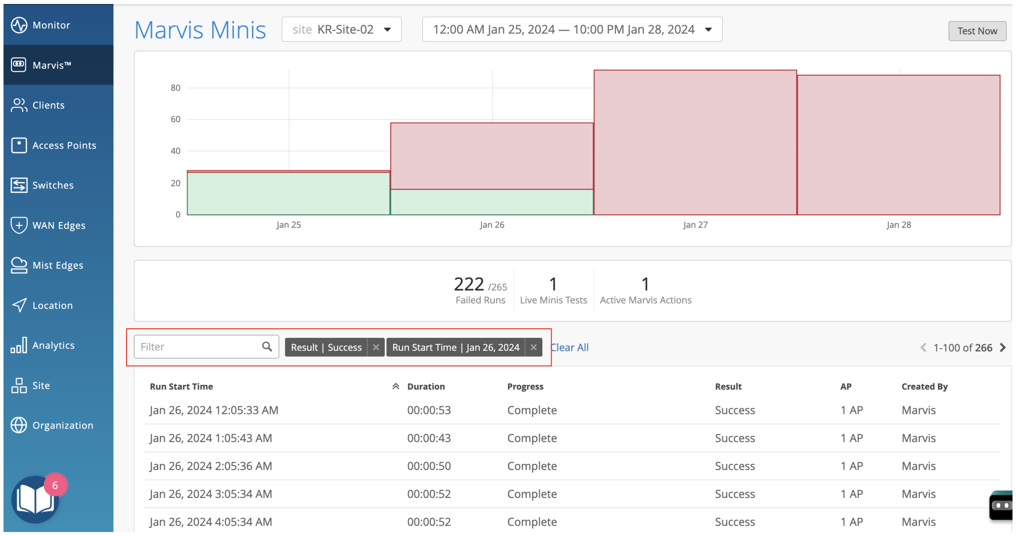


Run Start Time	Duration	Progress	Result	AP	Created By
Jan 28, 2024 9:10:51 PM	00:04:45	In progress 100%	In Progress	1 AP	Marvis
Jan 28, 2024 9:05:34 PM	00:05:17	Complete	Failed	1 AP	Marvis
Jan 28, 2024 8:36:54 PM	00:06:00	Complete	Failed	1 AP	Marvis
Jan 28, 2024 8:26:51 PM	00:10:03	Complete	Failed	1 AP	Marvis
Jan 28, 2024 8:15:54 PM	00:10:57	Complete	Failed	1 AP	Marvis

The **Created By** column indicates who initiated the validation:

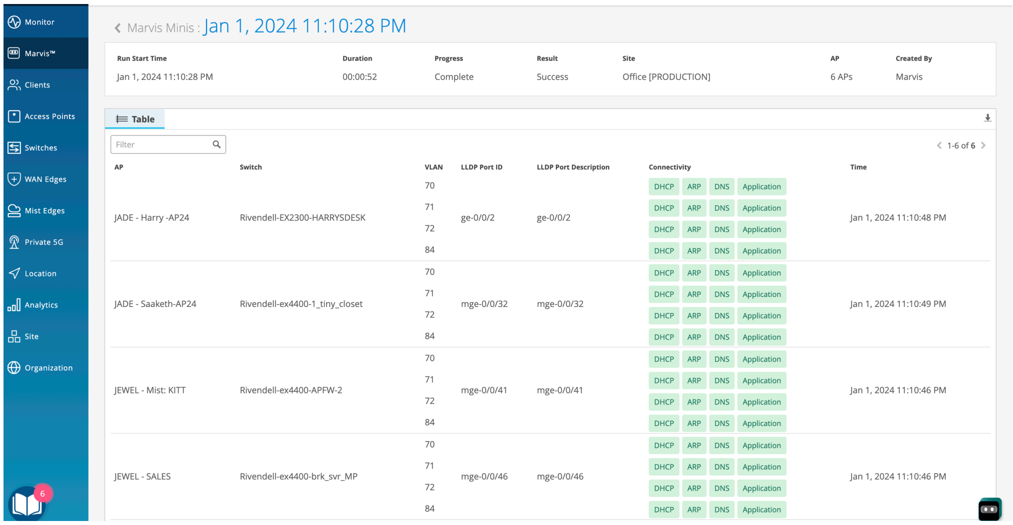
- Marvis—Indicates that Marvis initiated the validation automatically
- User—Indicates that a user initiated the validation manually

You can also use the **Filter** option to view specific validations. In the following example, we show you the filtered results for tests run on a specific date.



Run Start Time	Duration	Progress	Result	AP	Created By
Jan 26, 2024 12:05:33 AM	00:00:53	Complete	Success	1 AP	Marvis
Jan 26, 2024 1:05:43 AM	00:00:43	Complete	Success	1 AP	Marvis
Jan 26, 2024 2:05:36 AM	00:00:50	Complete	Success	1 AP	Marvis
Jan 26, 2024 3:05:34 AM	00:00:52	Complete	Success	1 AP	Marvis
Jan 26, 2024 4:05:34 AM	00:00:52	Complete	Success	1 AP	Marvis

To view more information about each validation, click each row. You'll see the details for a validation. The table lists all the APs at the site, the switch to which each AP is connected, VLANs, LLDP port information, and the status for DHCP, ARP, DNS, and application connectivity.



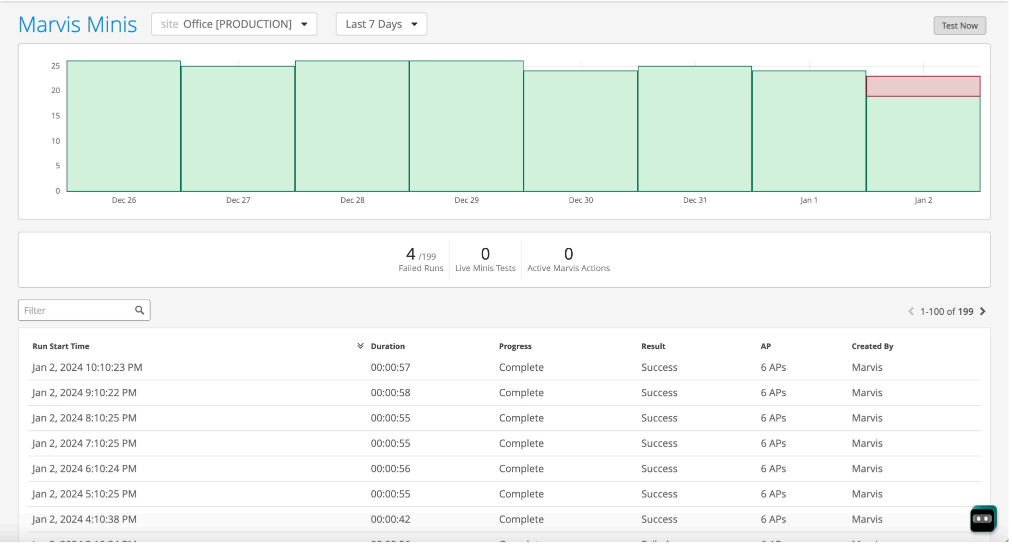
Marvis Minis : Jan 1, 2024 11:10:28 PM

Run Start Time	Duration	Progress	Result	Site	AP	Created By
Jan 1, 2024 11:10:28 PM	00:00:52	Complete	Success	Office [PRODUCTION]	6 APs	Marvis

AP	Switch	VLAN	LLDP Port ID	LLDP Port Description	Connectivity	Time
JADE - Harry -AP24	Rivendell-EX2300-HARRYSDESK	70 71 72 84	ge-0/0/2	ge-0/0/2	DHCP ARP DNS Application DHCP ARP DNS Application DHCP ARP DNS Application DHCP ARP DNS Application	Jan 1, 2024 11:10:48 PM
JADE - Saaketh-AP24	Rivendell-ex4400-1_tiny_closet	70 71 72 84	mge-0/0/32	mge-0/0/32	DHCP ARP DNS Application DHCP ARP DNS Application DHCP ARP DNS Application DHCP ARP DNS Application	Jan 1, 2024 11:10:49 PM
JEWEL - Mist: KITT	Rivendell-ex4400-APFW-2	70 71 72 84	mge-0/0/41	mge-0/0/41	DHCP ARP DNS Application DHCP ARP DNS Application DHCP ARP DNS Application DHCP ARP DNS Application	Jan 1, 2024 11:10:46 PM
JEWEL - SALES	Rivendell-ex4400-brk_svr_MP	70 71 72 84	mge-0/0/46	mge-0/0/46	DHCP ARP DNS Application DHCP ARP DNS Application DHCP ARP DNS Application DHCP ARP DNS Application	Jan 1, 2024 11:10:46 PM

Site-Level Dashboard

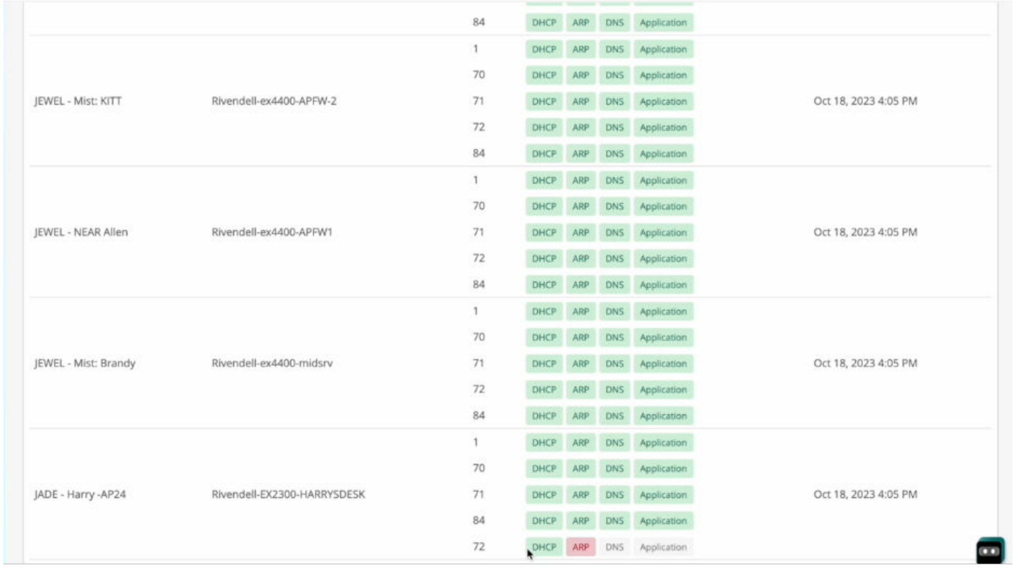
Here's an example of the Marvis Minis page for a site. In this case, as it is a single site, you'll see only the validations run on that site. You can click each row to view the details as described in the previous section.



4 /199 Failed Runs | 0 Live Minis Tests | 0 Active Marvis Actions

Run Start Time	Duration	Progress	Result	AP	Created By
Jan 2, 2024 10:10:23 PM	00:00:57	Complete	Success	6 APs	Marvis
Jan 2, 2024 9:10:22 PM	00:00:58	Complete	Success	6 APs	Marvis
Jan 2, 2024 8:10:25 PM	00:00:55	Complete	Success	6 APs	Marvis
Jan 2, 2024 7:10:25 PM	00:00:55	Complete	Success	6 APs	Marvis
Jan 2, 2024 6:10:24 PM	00:00:56	Complete	Success	6 APs	Marvis
Jan 2, 2024 5:10:25 PM	00:00:55	Complete	Success	6 APs	Marvis
Jan 2, 2024 4:10:38 PM	00:00:42	Complete	Success	6 APs	Marvis

Here's an example of a validation that detected an ARP failure on one of the APs.



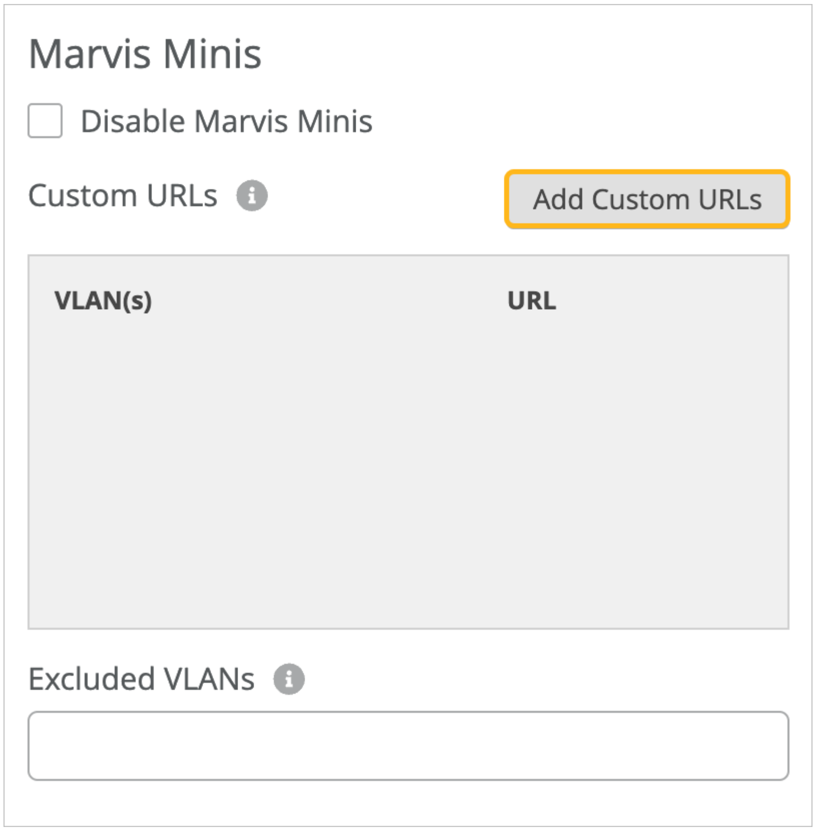
		84	DHCP	ARP	DNS	Application	
JEWEL - Mist: KITT	Rivendell-ex4400-APFW-2	1	DHCP	ARP	DNS	Application	Oct 18, 2023 4:05 PM
		70	DHCP	ARP	DNS	Application	
		71	DHCP	ARP	DNS	Application	
		72	DHCP	ARP	DNS	Application	
		84	DHCP	ARP	DNS	Application	
JEWEL - NEAR Allen	Rivendell-ex4400-APFW1	1	DHCP	ARP	DNS	Application	Oct 18, 2023 4:05 PM
		70	DHCP	ARP	DNS	Application	
		71	DHCP	ARP	DNS	Application	
		72	DHCP	ARP	DNS	Application	
		84	DHCP	ARP	DNS	Application	
JEWEL - Mist: Brandy	Rivendell-ex4400-midsrv	1	DHCP	ARP	DNS	Application	Oct 18, 2023 4:05 PM
		70	DHCP	ARP	DNS	Application	
		71	DHCP	ARP	DNS	Application	
		72	DHCP	ARP	DNS	Application	
		84	DHCP	ARP	DNS	Application	
JADE - Harry -AP24	Rivendell-EX2300-HARRYSDESK	1	DHCP	ARP	DNS	Application	Oct 18, 2023 4:05 PM
		70	DHCP	ARP	DNS	Application	
		71	DHCP	ARP	DNS	Application	
		84	DHCP	ARP	DNS	Application	
		72	DHCP	ARP	DNS	Application	

Marvis Minis retests each failure for confirmation. It also expands the scope to additional APs to identify whether the failure is limited to a specific VLAN, AP, or switch or whether it is a sitewide issue.

Add Custom URLs for Marvis Minis Validation

Marvis Minis runs the validation on a set of default URLs. As an administrator, you can add Amazon Web Services and Microsoft Azure workload application URLs for inclusion in the validation. To add custom URLs:

1. From the left menu, select **Organization** > **Admin** > **Settings**.
2. Navigate to the Marvis Minis section on the Organization Settings page.
3. Click **Add Custom URLs**.



□ Disable Marvis Minis

4. Enter the URL or fully qualified domain name (FQDN) of the site and the VLANs that you want Marvis Minis to validate.

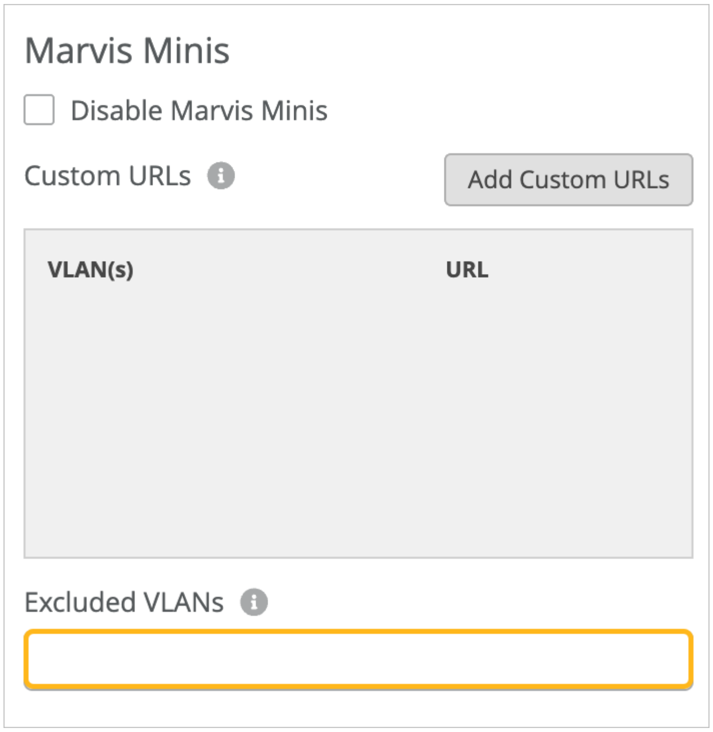
> **NOTE**: Remember that Marvis Minis learns all the APs, WLANs, switches, and active VLANs in a site and automatically creates the tests to run. Marvis Minis doesn't restrict the validations to the VLANs that you specify for a custom URL. Marvis Minis runs the validations on all the active VLANs in a site in addition to the VLANs that you specify for a custom URL. If you want to exclude any VLANs from the validation scope, you'll need to add them to the **Excluded VLANs** list. See "Exclude VLANs from Marvis Minis Validation" on page 183.

5. Click **Add**.
6. Click **Save** in the top-right corner of the Organization Settings page.

Exclude VLANs from Marvis Minis Validation

You can add a list of all the VLANs for which you do not want Marvis Minis to run an application reachability check. To exclude VLANs:

1. From the left menu, select **Organization** > **Admin** > **Settings**.
2. Navigate to the Marvis Minis section on the Organization Settings page.
3. In the **Excluded VLANs** field, enter the VLANs that you want Marvis Minis to exclude during the validation.



4. Click **Save** in the top-right corner of the Organization Settings page.

Disable Marvis Minis

Marvis Minis is enabled by default on all sites with APs running firmware version 0.14.29313 and later. You can opt to disable Marvis Minis for a specific site or organization. Note that the site-level settings override the organization-level settings.

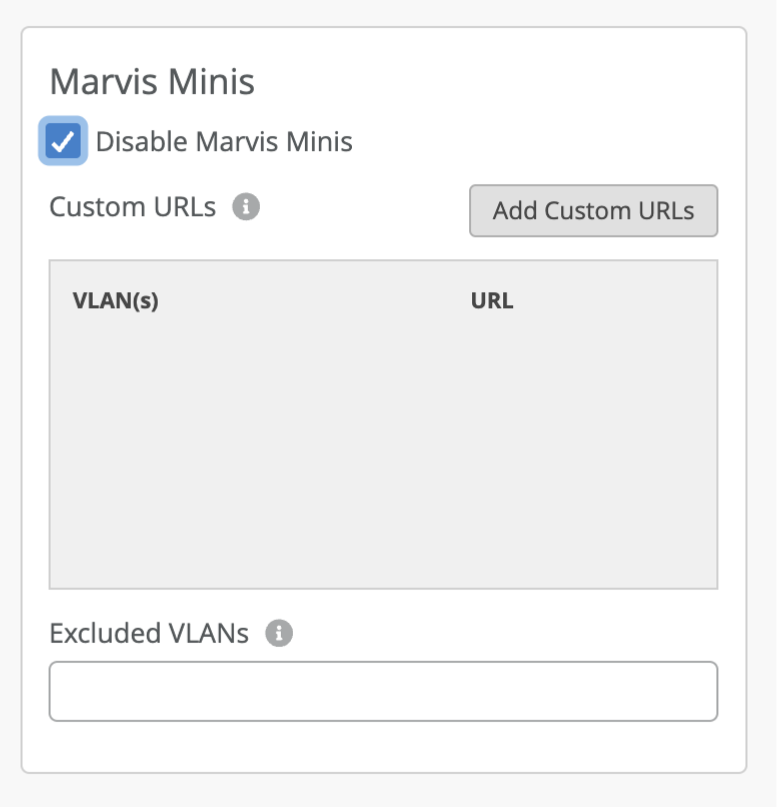
To disable Marvis Minis:

You can re-enable Marvis Minis any time at the organization level or site level by clearing the **Disable Marvis Minis** check box. You can re-enable Marvis Minis at the site level only if Marvis Minis is enabled at the organization level.

1. Navigate to the settings that you want to change:
   - To disable Marvis Minis at the organization level—Select **Organization** > **Admin** > **Settings** from the left menu.

- To disable Marvis Minis at the site level—Select **Organization** > **Admin** > **Site Configuration** from the left menu.

2. In the Marvis Minis section, select the **Disable Marvis Minis** check box.



Marvis Minis

☑ Disable Marvis Minis

3. Click **Save** in the top-right corner of the page.

Marvis Minis are disabled. You can re-enable Marvis Minis anytime by returning to the settings page and clearing the check box.

> **NOTE**: You can re-enable Marvis Minis at the site level only if Marvis Minis is enabled at the organization level.

Network and Application Monitoring with Marvis Minis

IN THIS SECTION

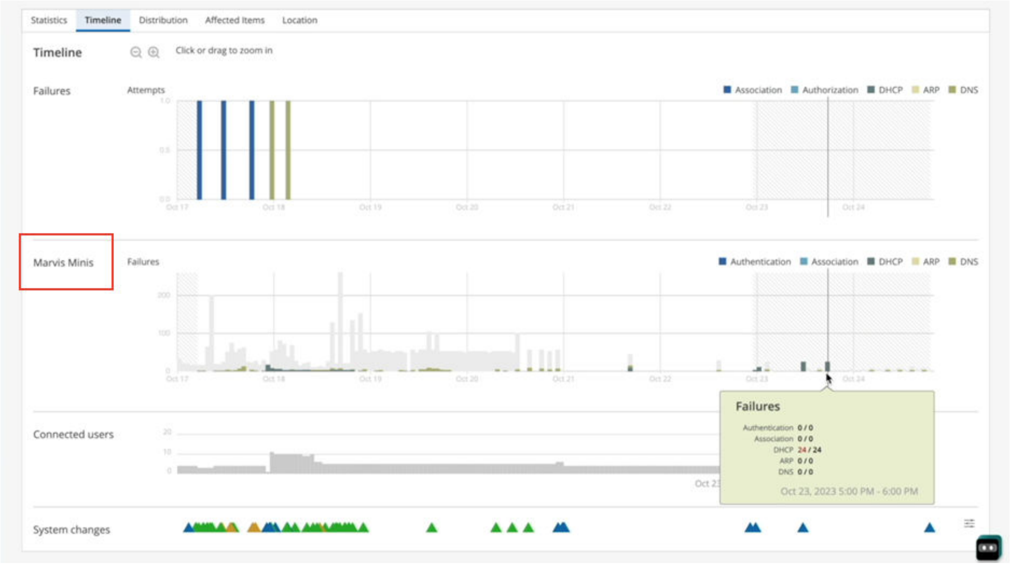
Juniper Mist™ uses data from Marvis Minis to analyze the end-user experience and provides the overlay of Marvis Minis runs in the wireless service-level expectation (SLE) dashboards. You can use the information to analyze connectivity failure trends and manage your network proactively by identifying issues before they escalate to a larger issue affecting the end-user experience.

View the Marvis Minis Timeline in the Successful Connect SLE

The Successful Connect SLE for wireless provides a timeline that shows the actual failed connection attempts for connected users to indicate the connection failure trend. If Marvis Minis is enabled for your organization, the timeline includes Marvis Minis-observed failures. You can analyze the information to correlate the Marvis Minis-reported failure and end-user-reported failures.

To view the Marvis Minis timeline:

1. Select **Monitor** > **Service Levels** from the left menu, and then click the **Wireless** tab.
2. Scroll down, click the **Successful Connects** metric, and then click the **Timeline** tab.
   Here's a sample timeline that shows the Marvis Minis-observed failures. The timeline highlights the validations run and the failures observed against connection attempts. In this example, notice that Marvis Minis made 24 DHCP requests and all the requests failed. The example also highlights the fact that Marvis Minis runs validations even when no users are connected to the network.



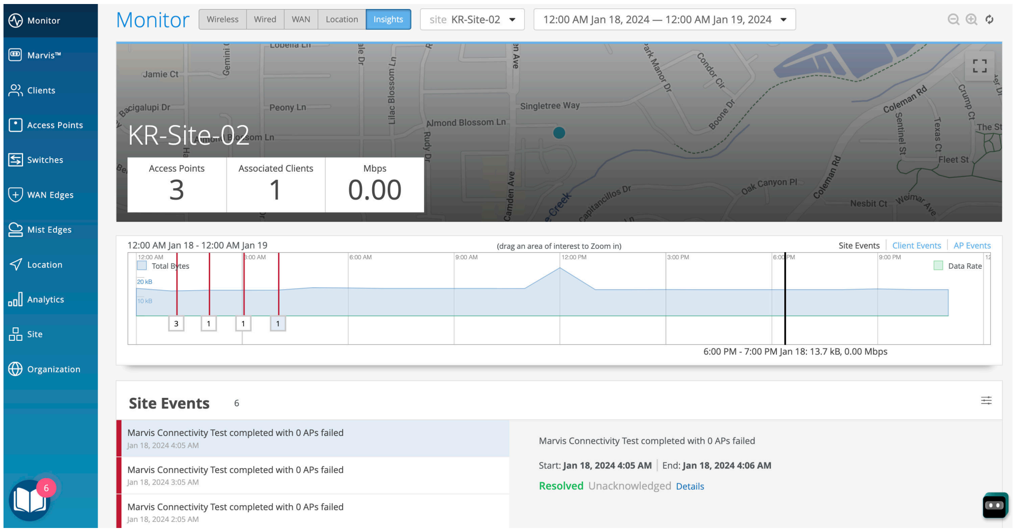
View Site Insights for Marvis Minis

Every time Marvis Minis runs a network validation, it updates the site events to provide a high-level audit of the validation. You can view the site events on the Insights dashboard. You can view more details on the Marvis Minis dashboard for the site.

To view the Insights dashboard:

1. Select **Monitor** > **Service Levels** from the left menu.
2. Click the **Insights** tab at the top of the Monitor page.
3. Select the site and the duration for which you want to view the details.

   Here's an example that shows the site events captured for a Marvis Mini validation.



Site Events 6

Marvis Connectivity Test completed with 0 APs failed
Jan 18, 2024 4:05 AM

Marvis Connectivity Test completed with 0 APs failed
Jan 18, 2024 3:05 AM

Marvis Connectivity Test completed with 0 APs failed
Jan 18, 2024 2:05 AM

Marvis Connectivity Test completed with 0 APs failed

Start: **Jan 18, 2024 4:05 AM** | End: **Jan 18, 2024 4:06 AM**

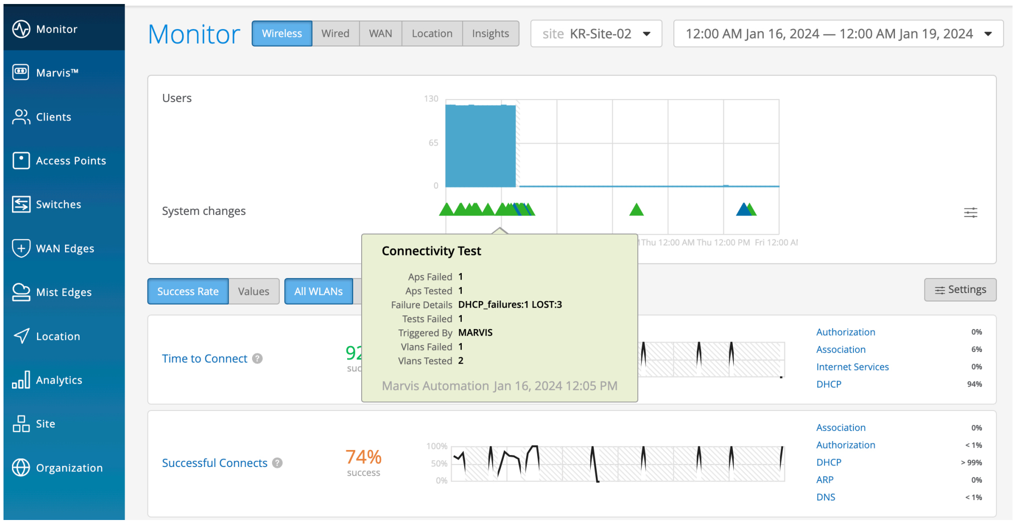
Resolved Unacknowledged Details

View System Events for Marvis Minis

Mist displays all Marvis Minis connectivity validations executed on a site as part of the system events. With this information, you can keep track of the connectivity validations from the Wireless SLE page.

Select **Monitor** > **Service Levels** from the left menu, and then click the **Wireless** tab.

You'll see the timeline for System Changes as shown here. This example shows the audit for a Marvis Minis connectivity validation for DHCP.

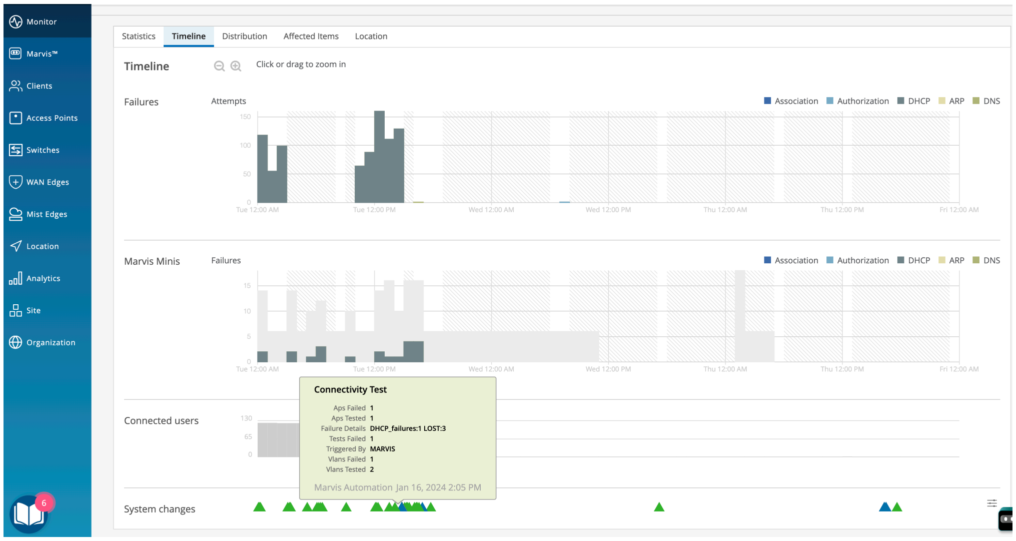


Connectivity Test

Aps Failed 1
Aps Tested 1
Failure Details DHCP_failures:1 LOST:3
Tests Failed 1
Triggered By MARVIS
Vlans Failed 1
Vlans Tested 2

Marvis Automation Jan 16, 2024 12:05 PM

You can also access the System Changes information from the Successful Connect Timeline view.



Connectivity Test

Aps Failed 1
Aps Tested 1
Failure Details DHCP_failures:1 LOST:3
Tests Failed 1
Triggered By MARVIS
Vlans Failed 1
Vlans Tested 2

Marvis Automation Jan 16, 2024 2:05 PM

8

CHAPTER

Conversations and Queries

Marvis Conversations and Queries Overview

You can interact with Marvis by using the Marvis Conversational Assistant or by entering structured queries using the Marvis Query Language.

Marvis Conversational Assistant Video Demo

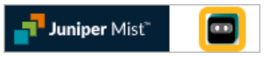
In this video demo, Marvis helps to troubleshoot an issue with Microsoft Teams.

Video: Marvis Conversational Assistant Example

> **NOTE**: You also can enter structured queries by using the Marvis Query Language. For more information, see "Marvis Query Language" on page 194.

Get started:

- To use the Conversational Assistant—Click the Marvis icon at the top-left corner or bottom-right corner of the Juniper Mist portal. For more information about the conversational assistant, see "Marvis Conversational Assistant" on page 190.

- To use the structured query language—Select **Marvis** > **Marvis Actions** from the left menu. Then click the **Ask a Question** button at the top-right corner of the page. For more information about the query language, see "Marvis Query Language" on page 194.

Marvis Conversational Assistant

SUMMARY

Get started using the Marvis Conversational Assistant to get information about your network, troubleshoot issues, and find documentation.

IN THIS SECTION

The conversational assistant offers help by using natural language processing (NLP) and natural language understanding (NLU) capabilities. It continues to improve its responses by learning from user feedback.

Marvis can:

- Provide information about sites, devices, clients, and applications
- Help troubleshoot issues with sites, devices, clients, and applications

You can interact with the conversational assistant by following prompts or by entering questions and statements like you would in a normal conversation. For example, you can ask, “How many switches are connected?” or “How is the primary site working?”

Video Demo

Watch a user interact with the Marvis conversational assistant.

Video: Marvis Conversational Assistant

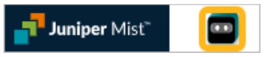
Requirements

To use the conversational assistant, you must:

- Meet the subscription requirements. For more information, see "Subscriptions for Marvis" on page 115.
- Have a user account with permission to access all sites in your organization.

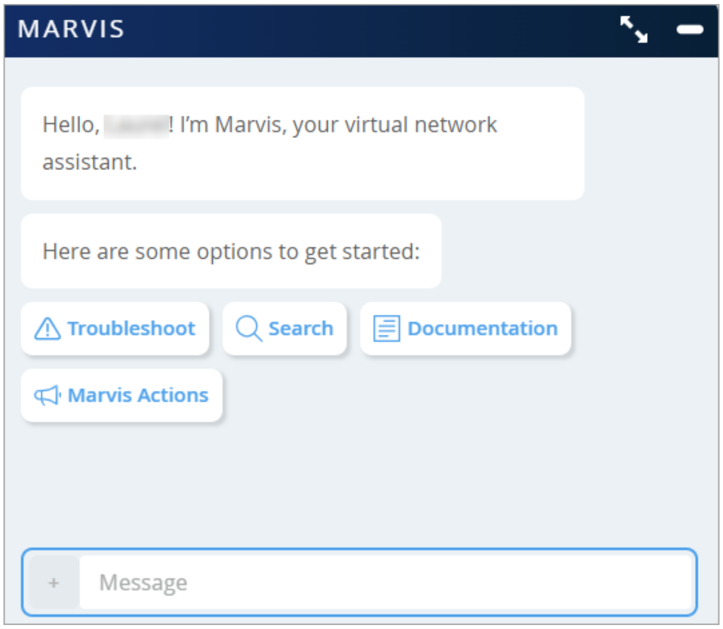
Finding the Conversational Assistant

Click the Marvis icon at the top-left corner or bottom-right corner of the Juniper Mist portal.



Using Natural Language

Click the Marvis icon, and then enter your question or concern in the **Message** box at the bottom of the Marvis window.

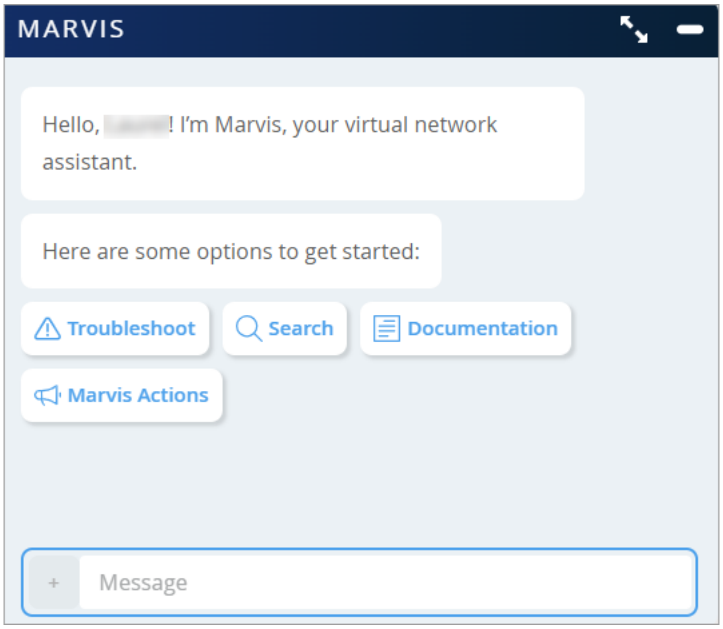


Hello, [redacted]! I'm Marvis, your virtual network assistant.

Here are some options to get started:

Following Prompts

Click the Marvis icon, and then click one of the buttons that Marvis displays.



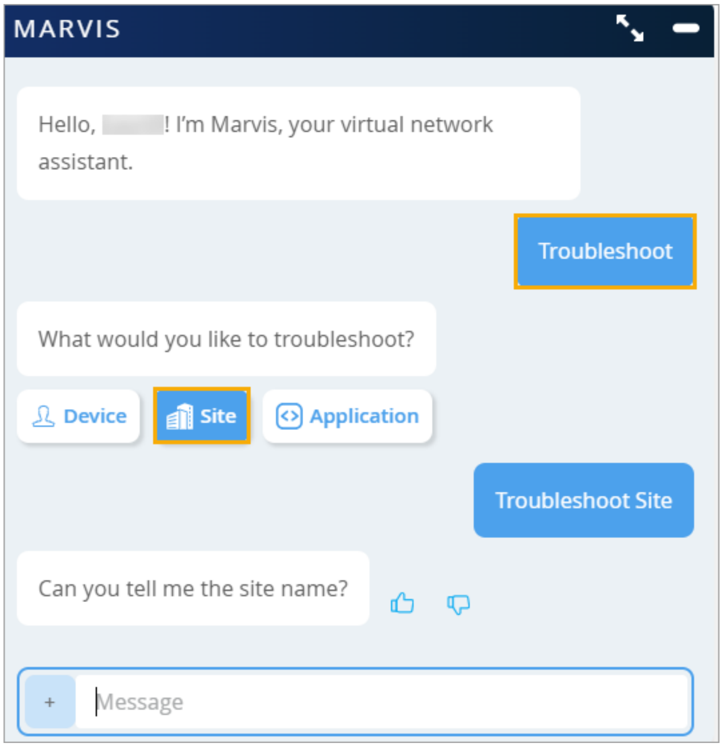
Hello, [redacted]! I'm Marvis, your virtual network assistant.

Here are some options to get started:

The initial prompts include:

- Troubleshoot—Click this option to troubleshoot issues with a site, application, device, and wired or wireless client.
- Search—Click this option to search for users, devices, and sites.
- Documentation—Click this option to search for documentation.
- Marvis Actions—Click this option to see pending actions from the Actions dashboard.

After you respond to a prompt, Marvis continues the conversation by displaying another prompt. In the following example, you can see the interaction between Marvis and a user who wants to troubleshoot issues with a site.



Hello, [redacted]! I'm Marvis, your virtual network assistant.

Troubleshoot

What would you like to troubleshoot?

Troubleshoot Site

Can you tell me the site name?

NOTE: You can also access the conversational assistant from the support ticket creation page to quickly troubleshoot impacted sites, devices, and clients before submitting a support ticket. For more information, see Create a Support Ticket.

Marvis Query Language

SUMMARY

Start using the Marvis Query Language to structure queries that pull data from Marvis.

IN THIS SECTION

The Marvis Query Language provides a structured framework for querying Marvis to get data that helps you monitor or troubleshoot your network. You can use queries to quickly find details about an event or failure in your network and about the affected devices.

Video Demo

Video: Marvis Query Language

Marvis Query Language Structure

A query can contain the following elements:

- Query Type—Defines what you want Marvis to do (for example, COUNT, LIST, RANK, LOCATE, or TROUBLESHOOT).
- Value—Specifies a unique value that is specific to an organization, such as a client's name.
- Query Object—Indicates Mist-defined objects (for example, APEvents, ClientEvents)
- Clause—Acts as a qualifier for the overall query (for example, of, with, or by).
- Filter Type—Narrows the results based on pre-defined filter types.

You can also add a duration to the end of a Marvis query. Note that you need to press the **space bar** after entering each element to see the available options.

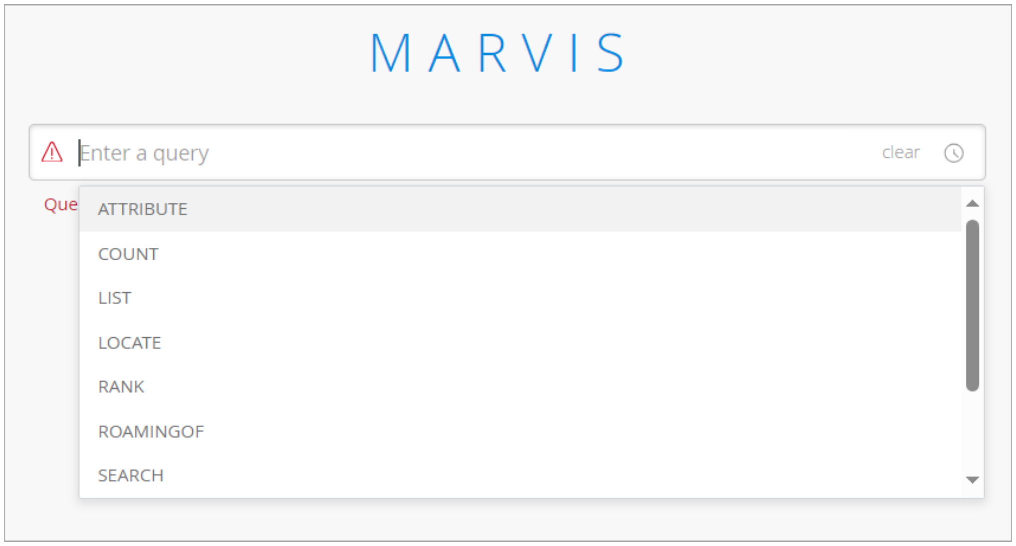
Finding the Marvis Query Page

Select **Marvis** > **Marvis Actions** from the left menu. Then click the **Ask a Question** button at the top-right corner of the page.

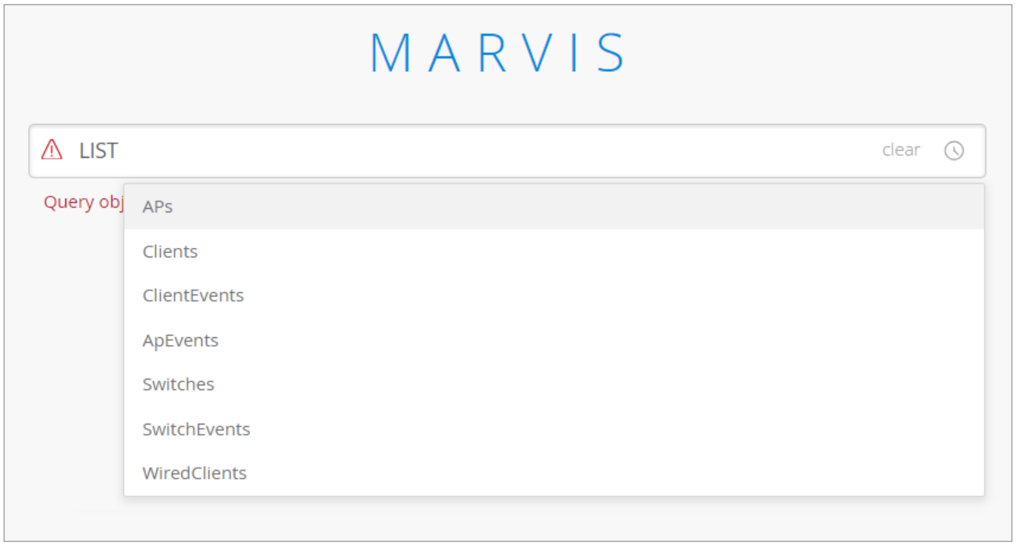
Entering a Structured Query

Marvis guides you step by step to enter the required elements in the query.

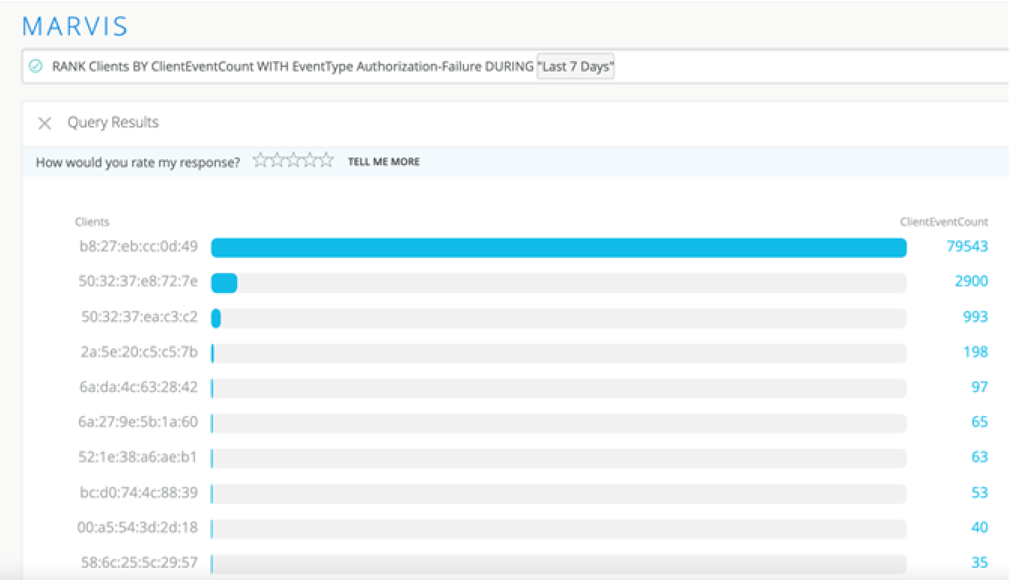
To get started, click in the **Enter a query** text box. Then click one of the options in the drop-down menu.



After you click an option, it appears in the query box. Press the space bar, and Marvis displays the available options. Here's an example of the options for the LIST query type.



Continue pressing the space bar and selecting options until you've entered a complete query. Here's an example of a RANK query that ranks clients based on the authentication failures:



```
RANK Clients BY ClientEventCount WITH EventType Authorization-Failure DURING "Last 7 Days"
```

Clients	ClientEventCount
b8:27:eb:cc:0d:49	79543
50:32:37:e8:72:7e	2900
50:32:37:ea:c3:c2	993
2a:5e:20:c5:c5:7b	198
6a:da:4c:63:28:42	97
6a:27:9e:5b:1a:60	65
52:1e:38:a6:ae:b1	63
bc:d0:74:4c:88:39	53
00:a5:54:3d:2d:18	40
58:6c:25:5c:29:57	35

For more information about useful queries, see "Troubleshoot Using Marvis Query Language" on page 197.

Troubleshoot Using Marvis Query Language

SUMMARY

Use these examples to see how you can use Marvis queries to monitor and troubleshoot your network.

IN THIS SECTION

View Event and Device Details

To troubleshoot problems and understand network behavior, you might need to look at event details or device details. You can use the LIST query to view details for the following:

- Access points (APs)
- Clients (including wired clients)

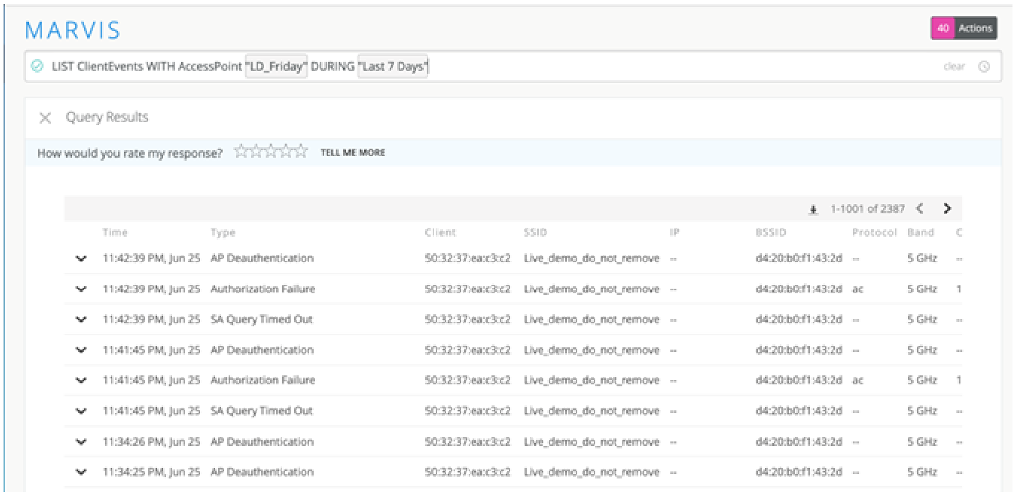
- Switches
- AP events
- Client events
- Switch events
- Mist Edges
- Mist Edge events

Table 10 on page 198 and Table 11 on page 199 provide a few LIST queries that you can use as a reference to build queries based on your requirements.

Table 10: Key LIST Queries to View Events

If you want to view	Use
Client events for an AP during a specific time interval	**LIST ClientEvents WITH AccessPoint *<AP name>* DURING *<time duration>***
All events for an AP	**LIST ApEvents WITH AccessPoint *<AP name>***
Events of a specific type for an AP	**LIST ApEvents WITH ApEventType *<event-type>* AND AccessPoint *<ap-name>***
All events for a switch	**LIST SwitchEvents WITH Switch *<switch name>***
Events of a specific type for a switch	**LIST SwitchEvents WITH SwitchEventType *<event-type>* AND Switch *<switch-name>***
All events for Mist Edges at a specific site	**LIST MistEdgeEvents WITH Site *<site-name>***

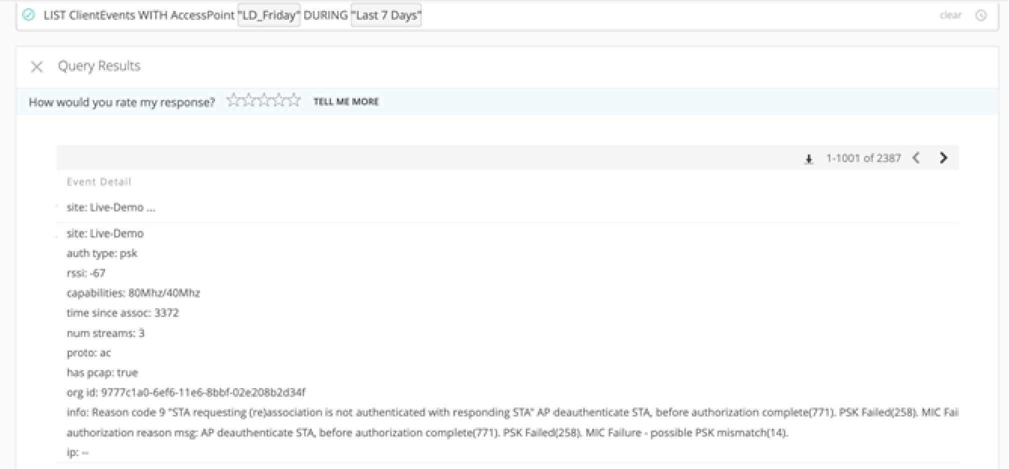
The following example shows the events for all clients associated with a particular AP. To view more details about an event, you can click the arrow in the first column of the table.



LIST ClientEvents WITH AccessPoint "LD_Friday" DURING "Last 7 Days"

Time	Type	Client	SSID	IP	BSSID	Protocol	Band	C
11:42:39 PM, Jun 25	AP Deauthentication	50:32:37:ea:c3:c2	Live_demo_do_not_remove	--	d4:20:b0:f1:43:2d	--	5 GHz	--
11:42:39 PM, Jun 25	Authorization Failure	50:32:37:ea:c3:c2	Live_demo_do_not_remove	--	d4:20:b0:f1:43:2d	ac	5 GHz	1
11:42:39 PM, Jun 25	SA Query Timed Out	50:32:37:ea:c3:c2	Live_demo_do_not_remove	--	d4:20:b0:f1:43:2d	--	5 GHz	--
11:41:45 PM, Jun 25	AP Deauthentication	50:32:37:ea:c3:c2	Live_demo_do_not_remove	--	d4:20:b0:f1:43:2d	--	5 GHz	--
11:41:45 PM, Jun 25	Authorization Failure	50:32:37:ea:c3:c2	Live_demo_do_not_remove	--	d4:20:b0:f1:43:2d	ac	5 GHz	1
11:41:45 PM, Jun 25	SA Query Timed Out	50:32:37:ea:c3:c2	Live_demo_do_not_remove	--	d4:20:b0:f1:43:2d	--	5 GHz	--
11:34:26 PM, Jun 25	AP Deauthentication	50:32:37:ea:c3:c2	Live_demo_do_not_remove	--	d4:20:b0:f1:43:2d	--	5 GHz	--
11:34:25 PM, Jun 25	AP Deauthentication	50:32:37:ea:c3:c2	Live_demo_do_not_remove	--	d4:20:b0:f1:43:2d	--	5 GHz	--

This example shows the list for a specific event type:



LIST ClientEvents WITH AccessPoint "LD_Friday" DURING "Last 7 Days"

Event Detail

site: Live-Demo ...

site: Live-Demo
auth type: psk
rssi: -67
capabilities: 80Mhz/40Mhz
time since assoc: 3372
num streams: 3
proto: ac
has pcap: true
org id: 9777c1a0-6ef6-11e6-8bbf-02e208b2d34f
info: Reason code 9 "STA requesting (re)association is not authenticated with responding STA" AP deauthenticate STA, before authorization complete(771). PSK Failed(258). MIC Fai
authorization reason msg: AP deauthenticate STA, before authorization complete(771). PSK Failed(258). MIC Failure - possible PSK mismatch(14).
ip: --

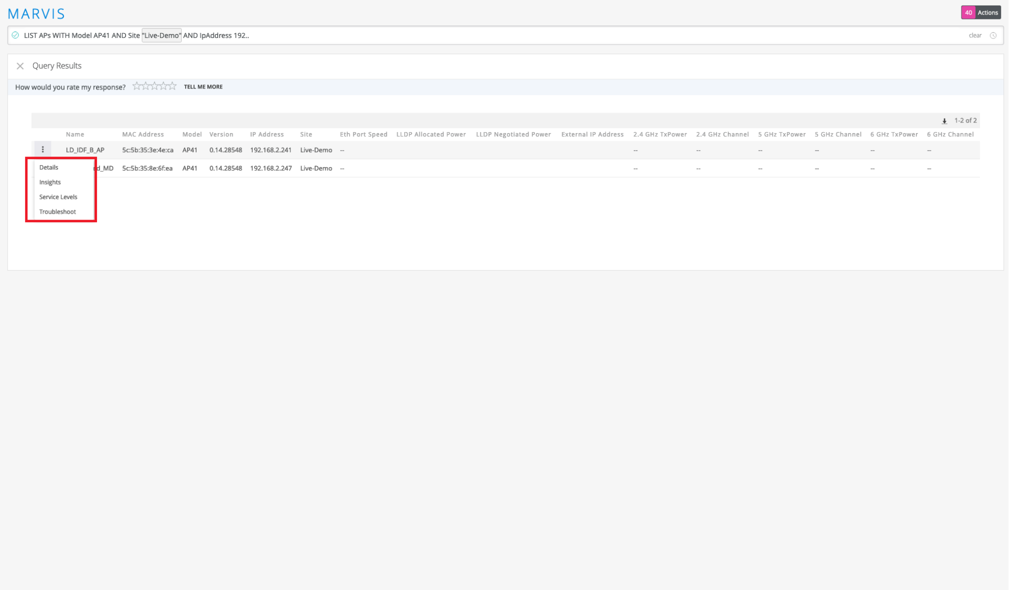
Table 11: Key LIST Queries to View Devices

If you want to view	Use
Switches of a particular model in a site	**LIST Switches WITH Model *<model number>* AND Site *<site name>***
Clients connected to an AP	**LIST Clients WITH AccessPoint *<AP name>***
APs of a specific model in a site	**LIST APs WITH Model *<model number>* AND Site *<site name>***
All the wired clients in a site	**LIST WiredClients WITH Site *<site name>***

Table 11: Key LIST Queries to View Devices *(Continued)*

If you want to view	Use
Mist Edges in a site	**LIST MistEdges WITH Site *<site name>***

The following example shows the output for a LIST query. Note that you can enter a partial IP address to search for devices in specific subnets. For additional actions, you can click the More Options icon at the top-left corner of the table.



LIST APs WITH Model AP41 AND Site "Live-Demo" AND IpAddress 192..

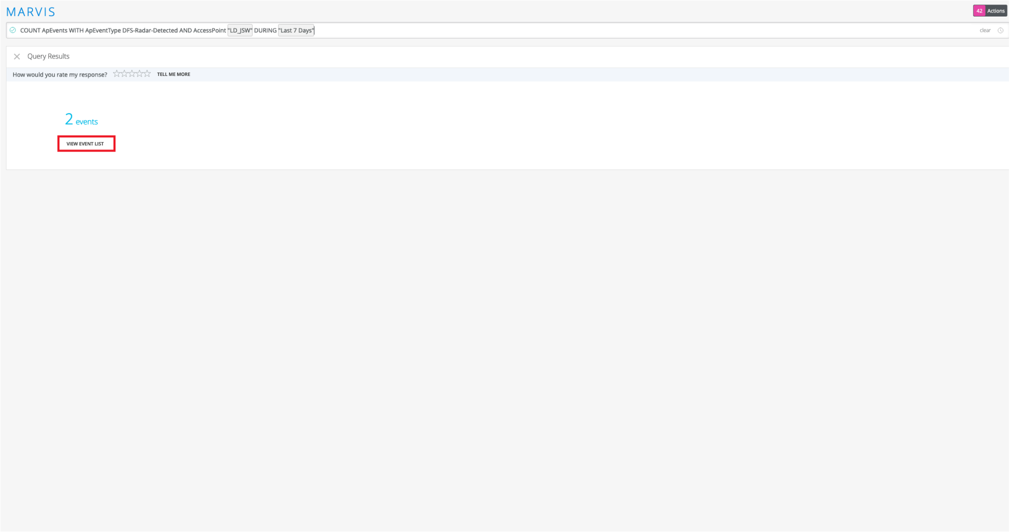
Query Results

How would you rate my response? ☆☆☆☆☆ TELL ME MORE

1-2 of 2

Name	MAC Address	Model	Version	IP Address	Site	Eth Port Speed	LLDP Allocated Power	LLDP Negotiated Power	External IP Address	2.4 GHz TxPower	2.4 GHz Channel	5 GHz TxPower	5 GHz Channel	6 GHz TxPower	6 GHz Channel
LD_IDF_B_AP	5c:5b:35:3e:4e:ca	AP41	0.14.28548	192.168.2.241	Live-Demo	--				--	--	--	--	--	--
d_MD	5c:5b:35:8e:6f:ea	AP41	0.14.28548	192.168.2.247	Live-Demo	--				--	--	--	--	--	--

In addition to the LIST query, you can use the COUNT query to get a count of events or devices that match the query. The COUNT query uses the same structure as the LIST query. Here is a screenshot that shows a sample output for the COUNT query. You can click **VIEW EVENT LIST** to see the event details.



COUNT ApEvents WITH ApEventType DFS-Radar-Detected AND AccessPoint "LD_JSW" DURING "Last 7 Days"

Query Results

How would you rate my response?

2 events

View Roaming Details of a Client

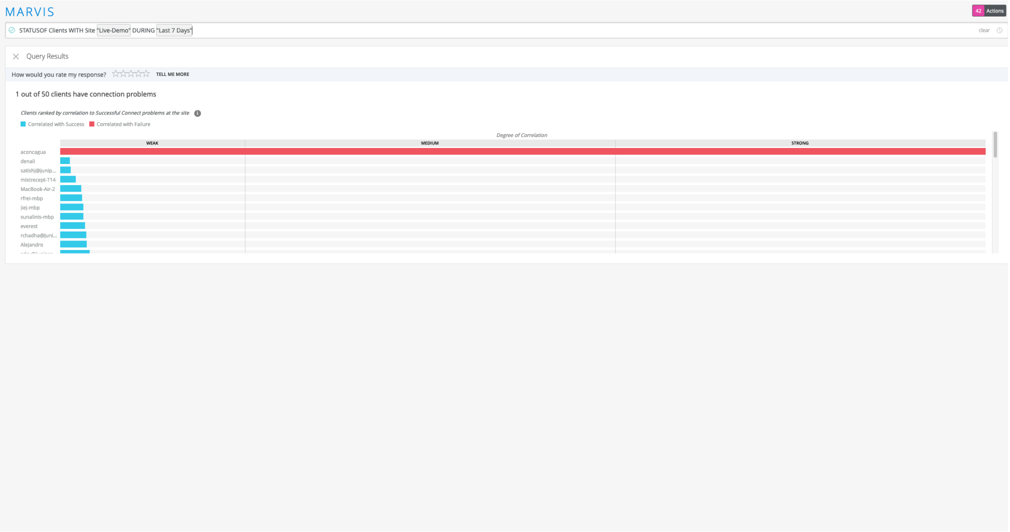
You can use the ROAMINGOF query to see a graphical view of a client roaming between different APs.

ROAMINGOF *<client name>* DURING *<time interval>*

View Status of a Client

The STATUSOF query provides an overview of clients that are facing connectivity issues in a site or wireless LAN (WLAN). The query output displays a ranked list of clients, starting with the clients experiencing the greatest number of issues. With this query, you can quickly identify clients facing connectivity issues in your site. You can use this query at the start of a troubleshooting session to identify the affected clients. You can then drill down into the client details to find the root cause of the issue. You can click a client to look at its service levels or insights, or to initiate the TROUBLESHOOT query on Marvis.

STATUSOF Clients WITH Site *<site name>*



STATUSOF Clients WITH Site "Live-Demo" DURING "Last 7 Days"

Query Results

How would you rate my response? ☆☆☆☆☆ TELL ME MORE

1 out of 50 clients have connection problems

Clients ranked by correlation to Successful Connect problems at the site

You can also view clients facing specific problems such as coverage issues, throughput problems, connectivity issues, and so on. For example, the query **STATUSOF Clients WITH Problem Capacity** lists all clients experiencing capacity issues in your organization.

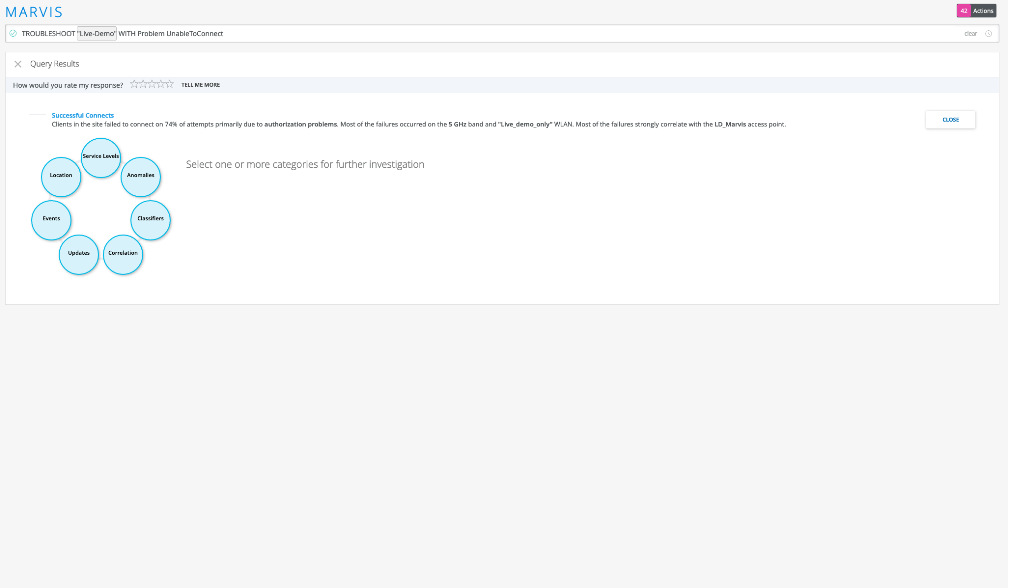
Troubleshoot APs, Sites, or Clients

Table 12 on page 202 lists a few TROUBLEHOOT queries that you can use to troubleshoot a site, a client, or an AP.

Table 12: TROUBLESHOOT Queries

If you want to troubleshoot	Use
A client, an AP, or a site	**TROUBLESHOOT *<client/site/AP name>***
A wireless client, an AP, or a site facing connectivity issues	**TROUBLESHOOT *<client/site/AP name>* WITH Problem SlowToConnect** **TROUBLESHOOT *<client/site/AP name>* WITH Problem UnableToConnect**
A wireless client, an AP, or a site facing connectivity issues for a specific duration	**TROUBLESHOOT *<client/site/AP name>* WITH Problem UnableToConnect DURING *<time duration>***

The following screenshot shows the output for the **TROUBLESHOOT <site name> WITH Problem UnableToConnect** query. You'll see that Marvis provides data such as the cause of the issue, the band, and the WLAN on which the issue occurred.



MARVIS

TROUBLESHOOT "Live-Demo" WITH Problem UnableToConnect

Query Results

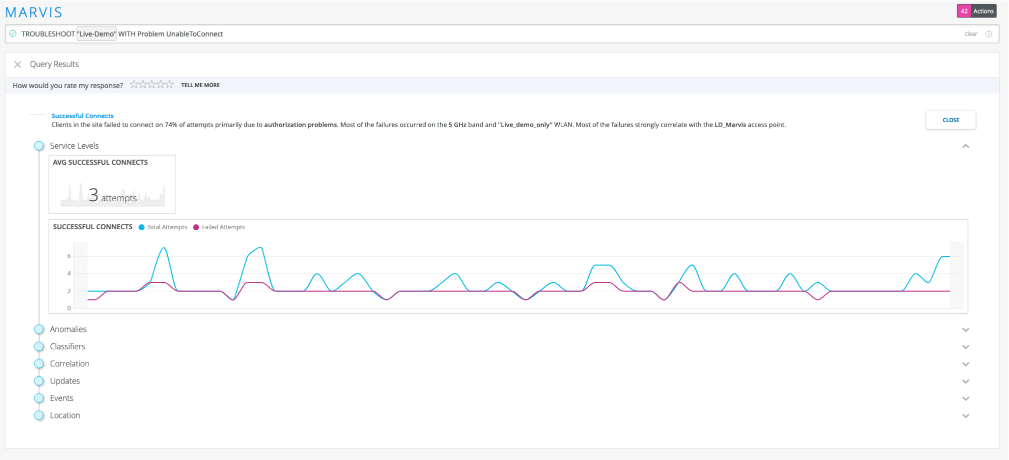
How would you rate my response? ☆☆☆☆☆ TELL ME MORE

Successful Connects

Clients in the site failed to connect on 74% of attempts primarily due to **authorization problems**. Most of the failures occurred on the **5 GHz** band and **"Live_demo_only"** WLAN. Most of the failures strongly correlate with the **LD_Marvis** access point.

Select one or more categories for further investigation

You can drill down into more details by clicking each of the categories. If you click the **Service Levels** category, Marvis provides more details about the issue as shown in the following screenshot:



MARVIS

TROUBLESHOOT "Live-Demo" WITH Problem UnableToConnect

Query Results

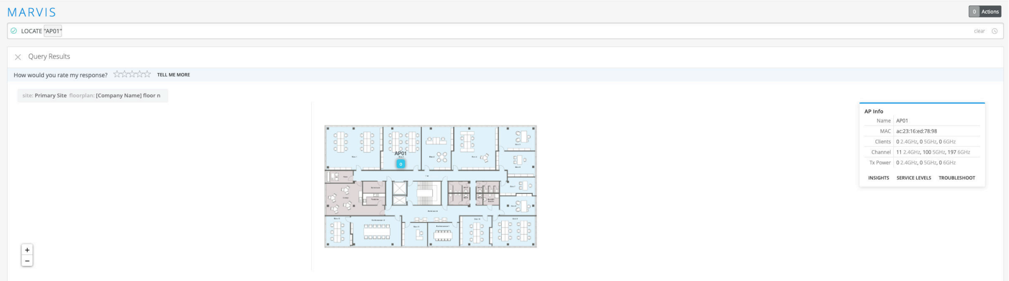
How would you rate my response? ☆☆☆☆☆ TELL ME MORE

Successful Connects

Clients in the site failed to connect on 74% of attempts primarily due to **authorization problems**. Most of the failures occurred on the **5 GHz** band and **"Live_demo_only"** WLAN. Most of the failures strongly correlate with the **LD_Marvis** access point.

Locate APs, Sites, or Clients

You can use the LOCATE query to find your site, AP, or client. The query output displays a map view of the site location that you configured in **Organization > Site Configuration**. For APs and clients, Marvis shows the location of these devices on your floorplan. Marvis also displays additional information and provides links to the Insights, Service Levels, and Troubleshoot pages.



LOCATE "AP01"

How would you rate my response? ☆☆☆☆☆

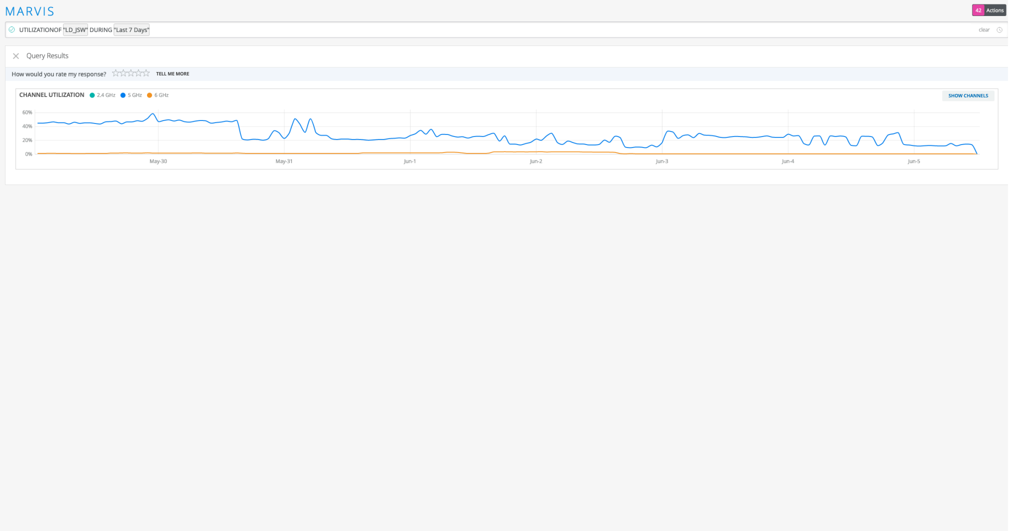
site: Primary Site floorplan: [Company Name] floor n

AP Info

Name	AP01
MAC	ac:23:16:ed:78:98
Clients	0 2.4GHz, 0 5GHz, 0 6GHz
Channel	11 2.4GHz, 100 5GHz, 197 6GHz
Tx Power	0 2.4GHz, 0 5GHz, 0 6GHz

View Channel Utilization of an AP

You can use the UTILIZATIONOF query to view the channels that an AP is broadcasting and the usage levels between the 2.4 GHz, 5 GHz, and 6 GHz bands. You can click **Show Channels** to see a breakdown of all specific channels that the AP uses.



UTILIZATIONOF "LD_JSW" DURING "Last 7 Days"

How would you rate my response? ☆☆☆☆☆

Client Roaming Visualization

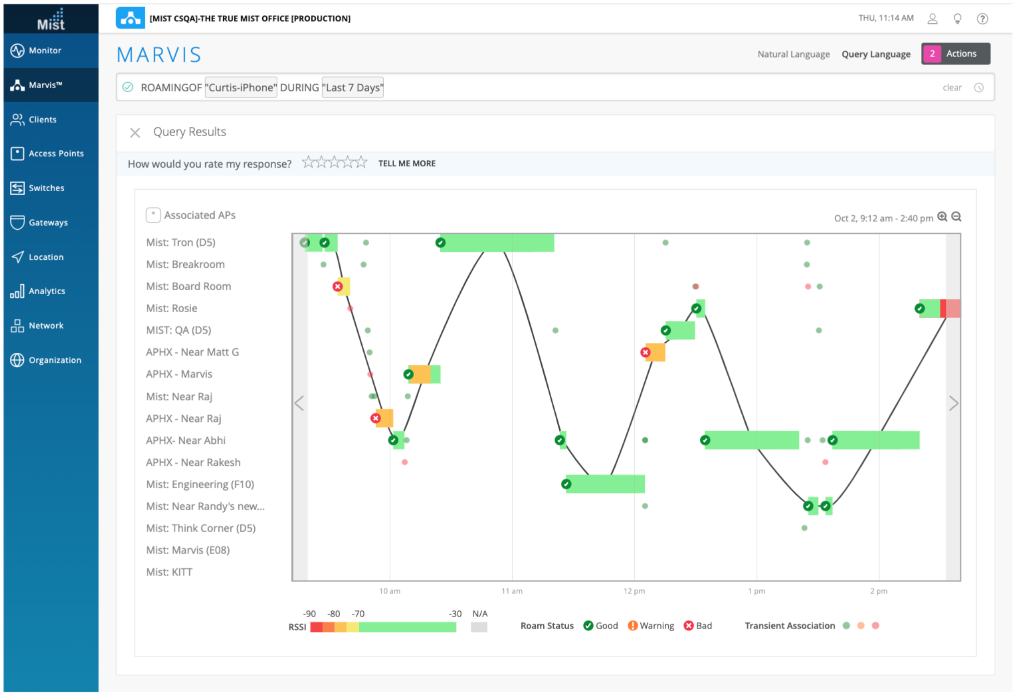
SUMMARY

Gain additional insights by using the ROAMINGOF query to view the client roaming status.

Marvis provides a visualization of your device’s roaming history and behavior. It includes information about the access points (APs) and radio bands the device connects to, and the received signal strength indicator (RSSI) values of the connection. Marvis uses the data from **Client Events** to provide a visual of the path your device takes and its transitions between various APs. Marvis indicates a Bad roaming status when the RSSI is low and a warning roaming status when the client switches to a different radio band or wireless LAN (WLAN) while roaming.

You need to use the Marvis query (ROAMINGOF) to view the client roaming status. If you want to get a more detailed view of the visualization, you can zoom in. Use the magnifier buttons on the top right of the timeline or click and drag your cursor in a particular section to zoom in on a specific time interval.

Marvis highlights information such as the roaming status, RSSI value, and transitions, to improve troubleshooting. The dots you see in this screenshot indicate Transient Associations, which means that the device was associated with the AP for a very short time.



[MIST CSQA]-THE TRUE MIST OFFICE [PRODUCTION]

THU, 11:14 AM

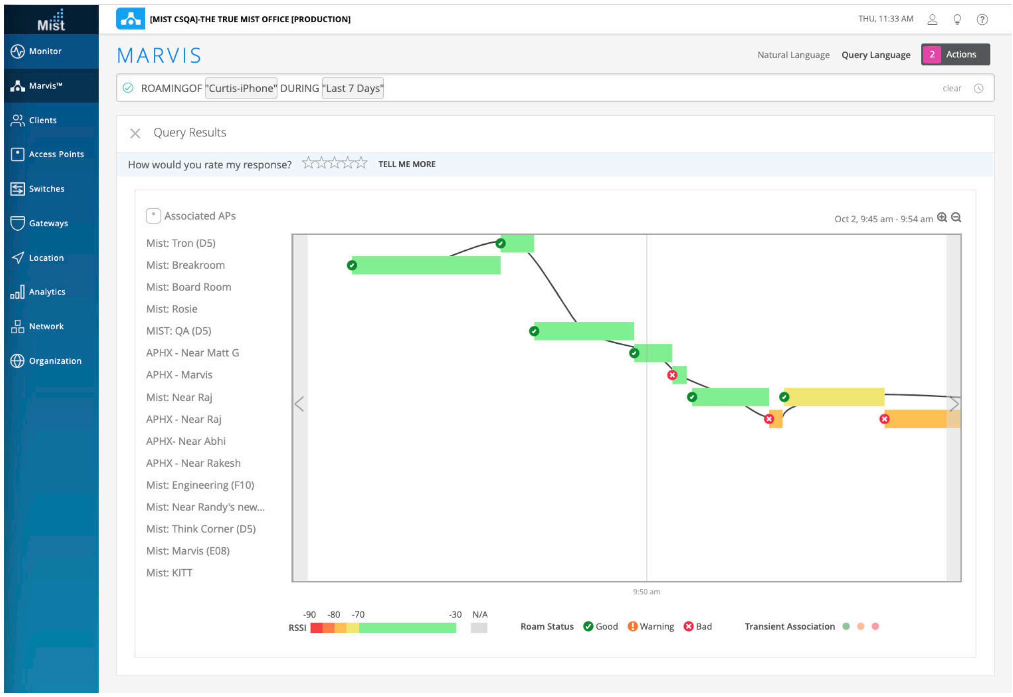
ROAMINGOF "Curtis-iPhone" DURING "Last 7 Days"

Query Results

How would you rate my response? ☆☆☆☆☆ TELL ME MORE

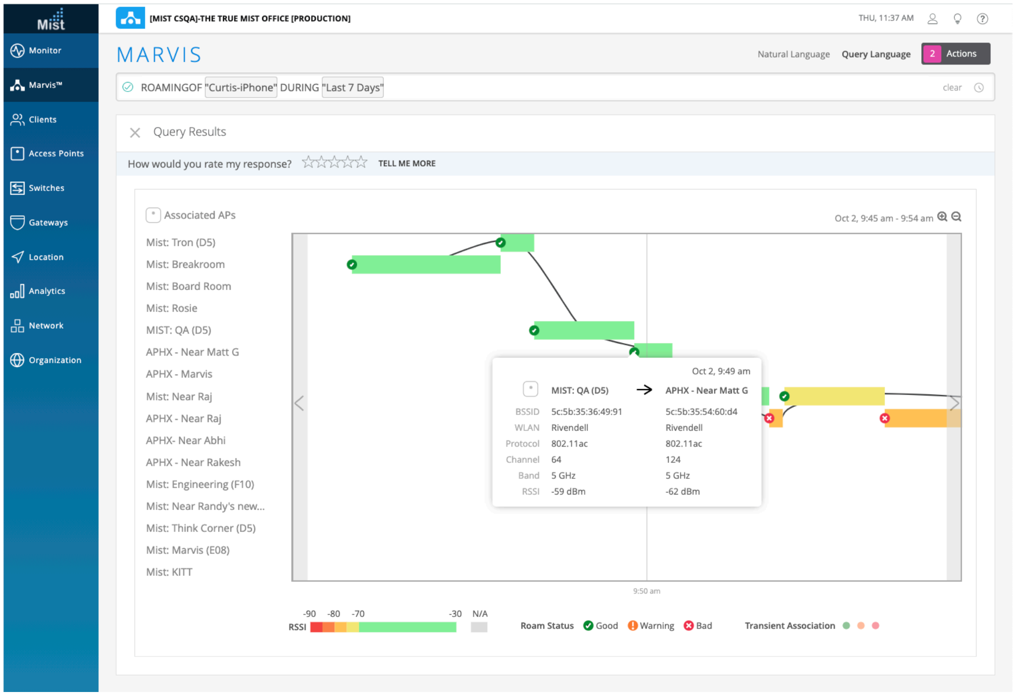
Oct 2, 9:12 am - 2:40 pm

Here is a zoomed-in view of transient associations in the 9:45 a.m. – 9:54 a.m. time interval.



ROAMINGOF "Curtis-iPhone" DURING "Last 7 Days"

You can hover over the roaming status icons on the timeline to view detailed information about the roaming event, such as the WLAN, channel, band, and RSSI. Here you can see that the client experienced a good roaming event between the APs at 9:49 a.m.

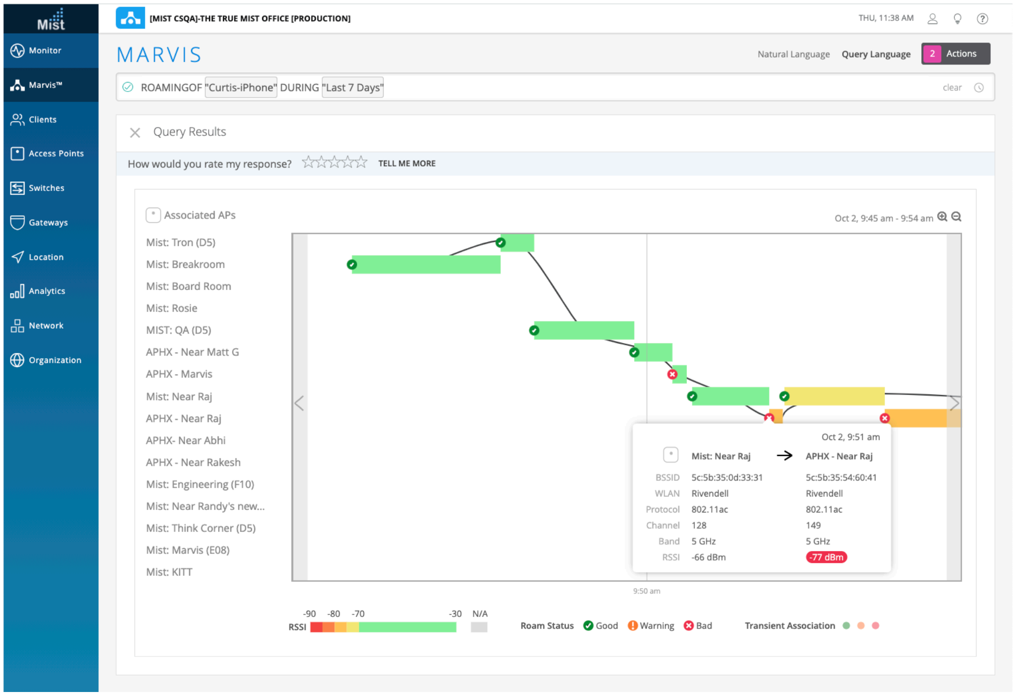


ROAMINGOF "Curtis-iPhone" DURING "Last 7 Days"

Oct 2, 9:49 am

	MIST: QA (D5)	→	APHX - Near Matt G
BSSID	5c:5b:35:36:49:91		5c:5b:35:54:60:d4
WLAN	Rivendell		Rivendell
Protocol	802.11ac		802.11ac
Channel	64		124
Band	5 GHz		5 GHz
RSSI	-59 dBm		-62 dBm

Here's an example of a bad roaming event. Notice that Marvis indicates a low RSSI for this event.

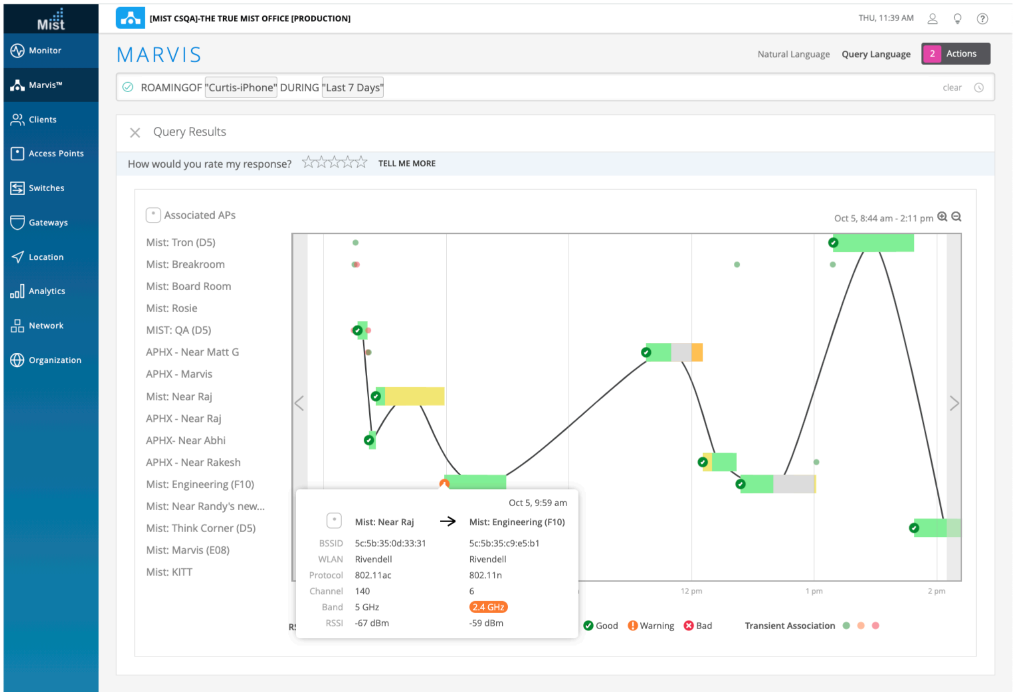


ROAMINGOF "Curtis-iPhone" DURING "Last 7 Days"

Oct 2, 9:51 am

	Mist: Near Raj	→ APHX - Near Raj
BSSID	5c:5b:35:0d:33:31	5c:5b:35:54:60:41
WLAN	Rivendell	Rivendell
Protocol	802.11ac	802.11ac
Channel	128	149
Band	5 GHz	5 GHz
RSSI	-66 dBm	-77 dBm

In the following screenshot, you can see that the client switched from the 5 GHz radio band to the 2.4 GHz band while roaming. Marvis displays the roaming status as Warning.



ROAMINGOF "Curtis-iPhone" DURING "Last 7 Days"

Oct 5, 9:59 am

	Mist: Near Raj	→ Mist: Engineering (F10)
BSSID	5c:5b:35:0d:33:31	5c:5b:35:c9:e5:b1
WLAN	Rivendell	Rivendell
Protocol	802.11ac	802.11n
Channel	140	6
Band	5 GHz	2.4 GHz
RSSI	-67 dBm	-59 dBm

9

CHAPTER

Marvis Android Client

Marvis Android Client Overview

SUMMARY

Get familiar with the benefits of the Marvis Android Client.

You can use the Marvis Android client to view your network from the client's perspective. View detailed data and telemetry about how the client experiences the wireless connection, including insight into client roaming behaviors. The Marvis client recognizes connection types (cellular or wireless) and the corresponding signal strength.

> **NOTE**: To use the Marvis client, you must install it on a compatible device and connect your device to a Juniper Mist AP. You also must have a Marvis subscription. For more information, see "Subscriptions for Marvis" on page 115.

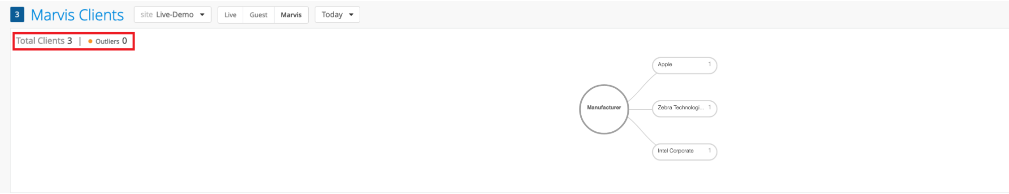
The Marvis client provides an additional layer of detail by displaying device type, manufacturer, and operating system, as follows:

- **Detailed wireless properties**: Mist's device fingerprinting provides the manufacturer, device type, and OS of the device. The Marvis client enhances this visibility by providing the OS version along with the radio hardware (adapter) and firmware (driver) versions. This level of visibility helps you identify:
  - Exceptions in terms of a device with different properties (such as the OS, radio hardware, and firmware) when compared to other devices of the same type.
  - Device-generic issues (for example, issues due to a firmware version).
- **Coverage issues due to asymmetry**: A Mist access point (AP) indicates the received signal strength indicator (RSSI) at which it detects a client. The Marvis client provides the RSSI at which the client detects the AP. This data helps you identify asymmetries in the power level between the client and AP. You can then resolve asymmetries that could result in a poor connection.
- **Connection type**: You can see when the device switches between a wireless and a cellular connection type, along with the corresponding signal strength.
- **Roaming behavior**: Roaming decisions and how a client decides to connect to an AP on a specific band is a client decision. The Marvis client provides visibility into how the client detects the neighboring APs.

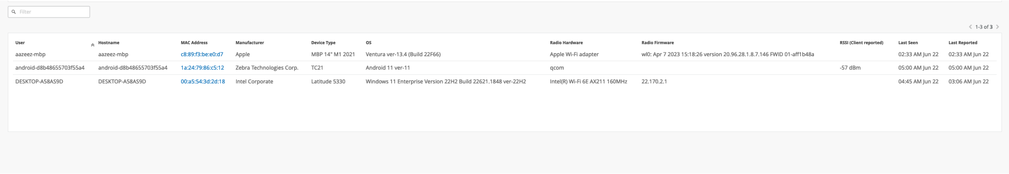
You can view all connected Marvis clients directly on the Mist portal on the WiFi Clients page (**Clients > WiFi Clients > Marvis** tab). You can view a graphical representation of your Marvis clients and their detailed information including manufacturer, device type, OS version, and radio hardware and firmware. You can see the current and historical snapshots of the connected clients in a specific site.

You can select either the Tree or List view to display your Marvis clients, as follows:

- **Tree view**: Groups clients based on their properties. Marvis classifies the clients by manufacturer, device type, OS version, radio hardware, and radio firmware. The tree view displays the total number of Marvis clients for the specified site and time range. It also highlights possible outliers that do not conform to the properties seen for other clients with the same manufacturer or device type.

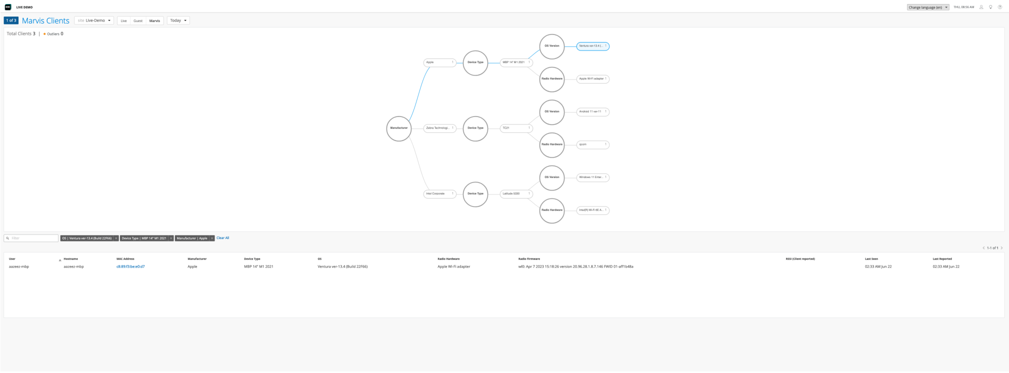


- **List view**: Presents client information in a tabular format. The default columns include user, hostname, MAC address, manufacturer, device type, device OS, radio hardware, radio firmware, and client-reported RSSI value. The list view displays up to 50 clients on a single page. You can navigate between pages by using the arrow buttons located on the top-right corner of the list.



User	Hostname	MAC Address	Manufacturer	Device Type	OS	Radio Hardware	Radio Firmware	RSSI (Client reported)	Last Seen	Last Reported
aazeez-mbp	aazeez-mbp	c8:89:f3:be:e0:d7	Apple	MBP 14" M1 2021	Ventura ver-13.4 (Build 22F66)	Apple Wi-Fi adapter	wl0: Apr 7 2023 15:18:26 version 20.96.28.1.8.7.146 FWID 01-aff1b48a		02:33 AM Jun 22	02:33 AM Jun 22
android-d8b48655703f55a4	android-d8b48655703f55a4	1a:24:79:86:c5:12	Zebra Technologies Corp.	TC21	Android 11 ver-11	qcom		-57 dBm	05:00 AM Jun 22	05:00 AM Jun 22
DESKTOP-A58AS9D	DESKTOP-A58AS9D	00:a5:54:3d:2d:18	Intel Corporate	Latitude 5330	Windows 11 Enterprise Version 22H2 Build 22621.1848 ver-22H2	Intel(R) Wi-Fi 6E AX211 160MHz	22.170.2.1		04:45 AM Jun 22	03:06 AM Jun 22

You can filter the list view by entering keywords in the search filter located at the top-left corner of the list. You can also filter the list view by clicking any client property in the tree view. When you click a property, the selected property and the path from the root property to the selected property are highlighted. You can then see the applied filters above the list view.



User	Hostname	MAC Address	Manufacturer	Device Type	OS	Radio Hardware	Radio Firmware	RSSI (Client reported)	Last Seen	Last Reported
aazeez-mbp	aazeez-mbp	c8:89:f3:be:e0:d7	Apple	MBP 14" M1 2021	Ventura ver-13.4 (Build 22F66)	Apple Wi-Fi adapter	wl0: Apr 7 2023 15:18:26 version 20.96.28.1.8.7.146 FWID 01-aff1b48a		02:33 AM Jun 22	02:33 AM Jun 22

We support the Marvis client on Android handheld devices and smartphones running OS 6.0 and higher versions.

Install the Marvis Client

SUMMARY

Complete the pre-install tasks, and then choose the method that you want to use to install the Marvis Client on your device.

IN THIS SECTION

Before You Begin

Configure your network firewall settings to allow the Marvis client to connect to your Mist organization.

- If your Mist organization resides in Amazon Web Services (AWS) cloud (default), use the following settings:
  - wss://client-terminator.mistsys.net:443/ws or protocol WSS (websocket) port 443 for domain/path
  - https://api.mist.com

    or HTTPS protocol port 443 for domain
- If your Mist organization resides in Google Cloud Platform (GCP) cloud, use the following settings:
  - wss://client-terminator.gc1.mist.com/ws or protocol WSS (websocket) port 443 for domain/path
  - https://api.gc1.mist.com/

or HTTPS protocol port 443 for domain

NOTE: If your Mist organization resides in a cloud other than AWS or GCP, contact the support team for the appropriate URLs to configure the firewall settings.

Get the QR Code (Secret Token)

1. Select **Organization** > **Admin** > **Mobile SDK** from the left menu.
2. Click **Token** at the top of the Mobile SDK page.
3. Create a new token, or use an existing token:
   - For a new token—Click **Create Invitation**. Enter a name for this invitation, and then click **Create**. When the token appears on the page, click **View** to see the QR code.
   - For an existing token—Refer to the token names to find the one that you want to use. Click the **View** link on the right side of the page to see the QR code.

Deploy the Marvis Client Using the SOTI MDM

To deploy the Marvis client using a mobile device management (MDM) solution, you must customize the Android package kit (APK) package deployment. You customize the APK deployment with the Intent action to set the secret software development kit (SDK) token upon installation. When you launch the customized application package, the client will be fully preconfigured and onboarded for operation.

You can onboard the Marvis client using the SOTI MDM.

NOTE: We do not present the overall generic Android application deployment process with SOTI. We present only the information necessary to customize the Android application to complete the client deployment.

Before you begin:

1. Ensure that you have a Windows device or a virtual machine (VM). You will run Package Studio, which runs only on Windows devices.
2. Download SOTI’s MobiControl Package Studio (McStudio.exe).

To deploy the Marvis client using MDM:

1. On your Windows device or VM, launch Package Studio and create a package project with the following settings:

   - Processor—All (unless targeting specific CPU or device types)

   - Platform—Android

   - OS Version—5 to 13 (unless you want to use a specific version)

   - Version String—Set to the same versioning as the APK version

   - Vendor—Mist Systems, Inc.

   - Optional space requirement specifications
2. Add the Marvis client APK.
3. Add the following Script file:

   - Script Engine—Legacy

   - Script Type—Post-Install
4. Import the script file. The script file must have the following content:

   ```
   sendintent -a "intent:#Intent;
   action=android.intent.action.MAIN;component=com.mist.marvisclient/.MainActivity;S.MOBILE_SDK_S
   ECRET=TheSecretValueHere;end;"
   ```

   If you have configured a specific port on a Zebra device for voice calls, then the script file must have the following content:

   ```
   sendintent -a "intent:#Intent;
   action=android.intent.action.MAIN;component=com.mist.marvisclient/.MainActivity;S.MOBILE_SDK_S
   ECRET=TheSecretValueHere;S.MOBILE_VOICE_CALL_PORT=5070;end;"
   ```
5. Build the package.

When you deploy the customized package with SOTI, the Marvis client is preconfigured and onboarded.

Deploy the Marvis Client Using AirWatch or VMWare Workspace ONE

We do not cover the overall generic Android app deployment process with AirWatch. We only cover the specific steps needed to complete the agent deployment.

Use the following intent command to deploy the agent:

```
mode=explicit,broadcast=false,action=android.intent.action.MAIN,package=com.mist.marvisclient,cla
ss=com.mist.marvisclient.MainActivity,extraString=MOBILE_SDK_SECRET=TheSecretValueHere
```

If you have configured a specific port on a Zebra device for voice calls, then use the following content:

```
mode=explicit,broadcast=false,action=android.intent.action.MAIN,package=com.mist.marvisclient,cla
ss=com.mist.marvisclient.MainActivity,extraString=MOBILE_SDK_SECRET=TheSecretValueHere,extraStrin
g=MOBILE_VOICE_CALL_PORT=5070
```

You can use the following references to deploy the intent command:

- Configuring Automatic Launch for Android Mobile Devices if you have already deployed the Marvis client on the device
- RunIntent Action, File-Action Android for new deployments of our APK installer on devices

Deploy Marvis Client Using Other MDMs

If you are using any other MDM, verify that the MDM supports intent execution. If the MDM does not support intent deployment, then you can use the sideloading procedure described in "Install Through Sideloading" on page 215. Here is another example for ADB based (developer/debug) deployment that you can use to adapt to an MDM of your choice:

```
adb shell am start -n "com.mist.marvisclient/com.mist.marvisclient.MainActivity" -a
android.intent.action.MAIN -c android.intent.category.LAUNCHER --es "MOBILE_SDK_SECRET"
"TheSecretValueHere" -t "text/plain"
```

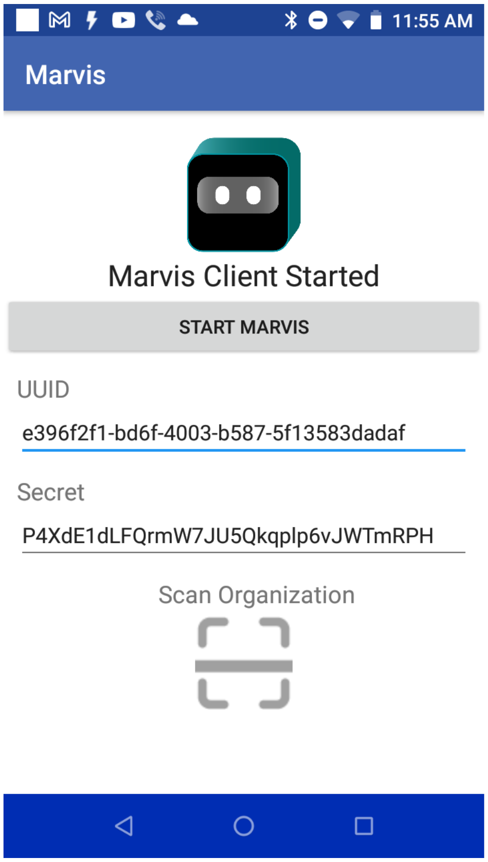
If the MDM solution does not support execution of Android intents, you might need to onboard each deployed client device manually.

Install Through Sideloading

NOTE: Follow this procedure for internal use, development, testing, or debugging. This process is not for official customer deployments. However, you can use this procedure in cases where the MDM solution does not support executing Android Intents to automatically configure the secret token on installation.

This procedure requires manual intervention for each device being onboarded.

1. Install the APK on the device. You can use Android Debug Bridge (ADB), MDM, or file manager (local device storage or an SD card containing the APK).
2. Open the Marvis client application on the device.
3. Tap the Marvis icon 7 times to open a special debug menu.

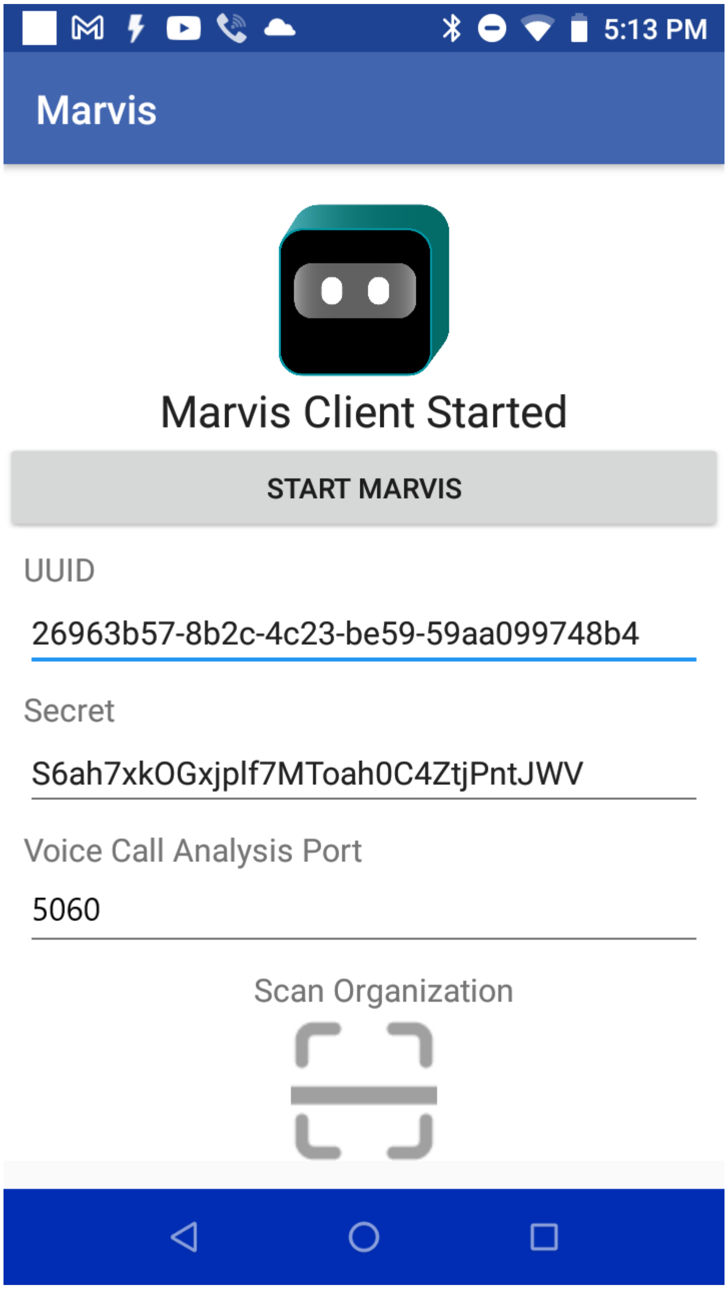


Marvis Client Started

UUID: e396f2f1-bd6f-4003-b587-5f13583dadaf

Secret: P4XdE1dLFQrmW7JU5Qkqplp6vJWTmRPH

For Zebra devices, the debug menu shows the port that is configured for voice calls.



UUID

26963b57-8b2c-4c23-be59-59aa099748b4

Secret

S6ah7xkOGxjplf7MToah0C4ZtjPntJWV

Voice Call Analysis Port

5060

4. Onboard the client using the secret code or scan code:

   To use the QR code:

   a. Tap the **Scan Organization** button to open the camera and scan the invitation QR code. Provide the necessary permissions.

   b. When the QR code is scanned, the matching secret token value is inserted into the Secret field.

      The secret value is applied to the Marvis client automatically. A message appears indicating that the value is applied.

To use the secret code:

a. Type or paste the secret token value in the Secret field. The default value of Secret is empty.

b. Tap the gray **Start Marvis** button to apply the changes.

   A message appears indicating that the value is applied.

You have successfully onboarded the Marvis client.

Verify the Installation

After you install and onboard the Marvis client, verify that those processes have run correctly.

To verify the installation:

- Confirm that the secret token value is added correctly. Close the Marvis client process and then launch it again. Open the debug menu by tapping the Marvis icon 7 times, and verify that the secret token value is still stored in the field.

  If the secret token field is empty and the data does not persist, enter the secret token value manually, as described in "Install Through Sideloading" on page 215. You might also need to configure the application deployment to retain the application data.

- About 15 minutes after you onboard the Marvis client, confirm that the Marvis client data is available on the Mist dashboard. You need to wait for a minimum of 10 minutes after onboarding the Marvis client for the data to propagate to the Mist cloud.

  If the data is not available in the Mist dashboard, a problem occurred in the client workflow of collecting data and sending it to the Mist cloud. Contact the support team. If you are able to use tools such as logcat or Android Debug Bridge (ADB), then you can use them to collect the Marvis client logs and share the logs with the support team.

  For Zebra devices, use the RxLogger tool to collect logs.

  When you contact the support team, you must share the Marvis client UUID. You can find the UUID on the Marvis client debug mode screen. The UUID is used to track the data flow from the Marvis client to the Mist cloud.

Marvis-Zebra Integration

SUMMARY

Explore the benefits of integrating the Marvis Android Client with Zebra Wireless Insights.

IN THIS SECTION

Overview

The Marvis client works with Zebra Wireless Insights to provide enhanced visibility into networking and connectivity. Zebra Wireless Insights is a service built into Zebra Android devices that provides insights into the data, voice, and roaming events of Zebra devices. Zebra devices can directly capture client events on the end-user side without you having to run any additional tests. Combined with the existing event reports captured by the Mist access points (APs) and the Marvis client, these client event reports deliver a holistic view of the network and client activity.

You can view client-reported events by using the **Client-Reported** tab under the **Client Events** section of your Zebra device's **Client Insights Dashboard**. You can switch between AP-reported events and client-reported events by using the tabs. If your Zebra device has no client events to report, the tab is hidden.

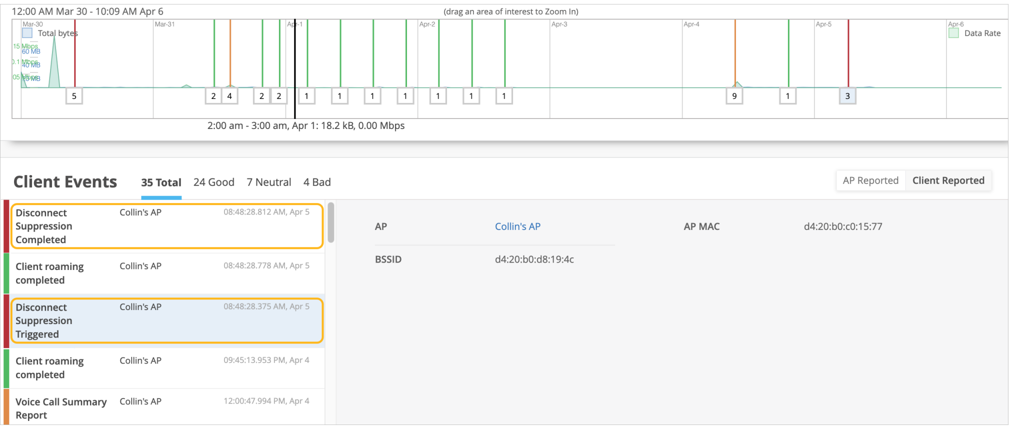
NOTE: To view client events from your Zebra device, the device must have a valid Wireless Insights license and the Marvis Android Client (V33.x or later) installed.

Connection Events

Mist APs provide visibility into user pre-connection and post-connection states. The Marvis client leverages Zebra Wireless Insights to get more information about connection states, including detailed visibility into connection events and their causes. You can view details about client connection and disconnection events. For example, you can decipher what happens when a device tries to connect, roam, or disconnect.

Here is a sample event and the condition that triggered the event:

Disconnect Suppression Triggered: The device-management path is still active with the AP. However, the data path is blocked—the device neither sends nor receives data from the AP. During this period, the data tries to roam to a new AP or reconnect to the same AP. On a successful roam or reconnection to an AP, the data path or connection resumes (indicated by the Disconnect Suppression Completed event).



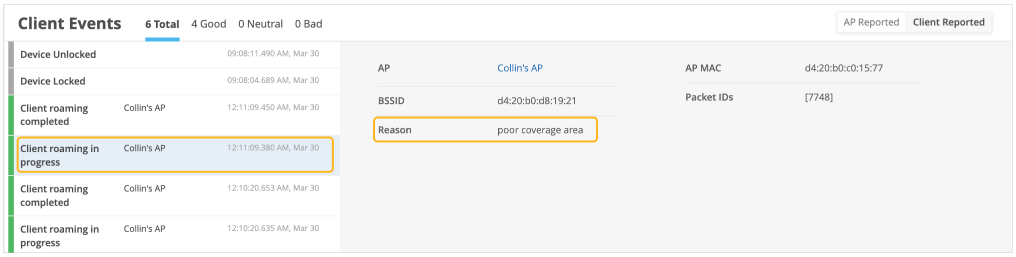
Client Events 35 Total 24 Good 7 Neutral 4 Bad AP Reported Client Reported

Disconnect Suppression Completed	Collin's AP	08:48:28.812 AM, Apr 5
Client roaming completed	Collin's AP	08:48:28.778 AM, Apr 5
Disconnect Suppression Triggered	Collin's AP	08:48:28.375 AM, Apr 5
Client roaming completed	Collin's AP	09:45:13.953 PM, Apr 4
Voice Call Summary Report	Collin's AP	12:00:47.994 PM, Apr 4

AP	Collin's AP	AP MAC	d4:20:b0:c0:15:77
BSSID	d4:20:b0:d8:19:4c		

Roaming Events

The Marvis client provides the roaming journey of every device with the RoamingOf query. With Zebra Wireless Insights, you can get insights into what triggered the roam, such as poor coverage area.



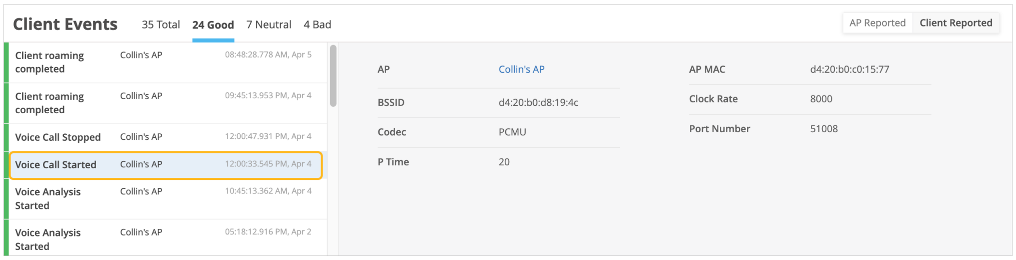
Client Events 6 Total 4 Good 0 Neutral 0 Bad AP Reported Client Reported

Device Unlocked		09:08:11.490 AM, Mar 30
Device Locked		09:08:04.689 AM, Mar 30
Client roaming completed	Collin's AP	12:11:09.450 AM, Mar 30
Client roaming in progress	Collin's AP	12:11:09.380 AM, Mar 30
Client roaming completed	Collin's AP	12:10:20.653 AM, Mar 30
Client roaming in progress	Collin's AP	12:10:20.635 AM, Mar 30

AP	Collin's AP	AP MAC	d4:20:b0:c0:15:77
BSSID	d4:20:b0:d8:19:21	Packet IDs	[7748]
Reason	poor coverage area		

Voice Events

You can view and analyze information about voice calls made using Zebra devices. The Marvis client provides details about when the call began and ended, along with the call performance. You can view a summary of voice events both during the call and after it ends.

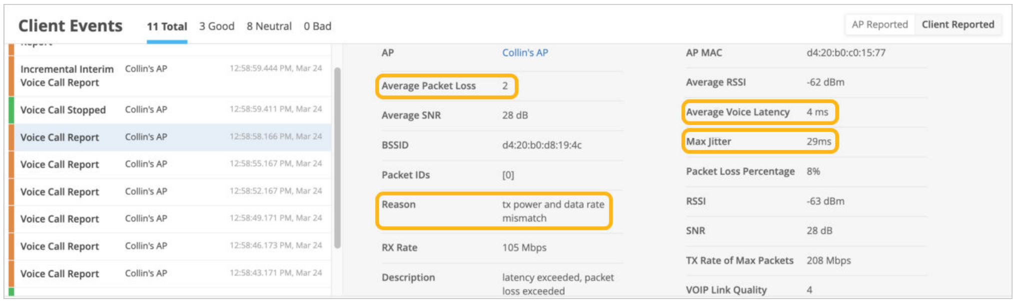


Client Events 35 Total **24 Good** 7 Neutral 4 Bad

Client roaming completed	Collin's AP	08:48:28.778 AM, Apr 5
Client roaming completed	Collin's AP	09:45:13.953 PM, Apr 4
Voice Call Stopped	Collin's AP	12:00:47.931 PM, Apr 4
Voice Call Started	Collin's AP	12:00:33.545 PM, Apr 4
Voice Analysis Started	Collin's AP	10:45:13.362 AM, Apr 4
Voice Analysis Started	Collin's AP	05:18:12.916 PM, Apr 2

AP	Collin's AP	AP MAC	d4:20:b0:c0:15:77
BSSID	d4:20:b0:d8:19:4c	Clock Rate	8000
Codec	PCMU	Port Number	51008
P Time	20		

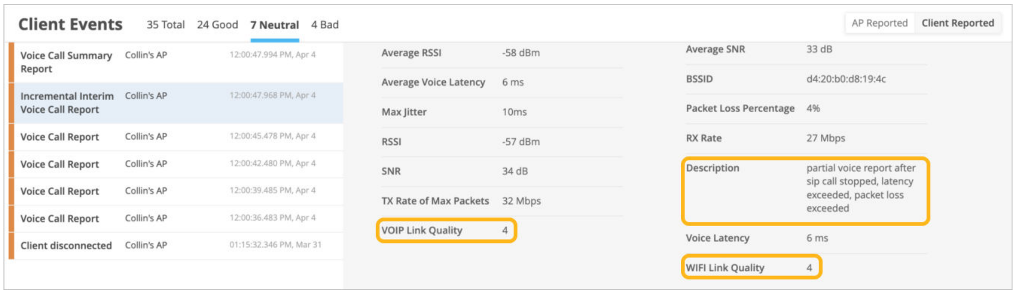
Zebra Wireless Insights measures the performance in terms of packet loss, latency, jitter, VoIP link quality, and Wi-Fi link quality. The Mist cloud receives this data from the Marvis Client and displays the data on the Insights page for a client. You can also see the description and reason for events that occurred during the call, which provides additional insight into the experience from the client's perspective.



Client Events **11 Total** 3 Good 8 Neutral 0 Bad

Incremental Interim Voice Call Report	Collin's AP	12:58:59.444 PM, Mar 24
Voice Call Stopped	Collin's AP	12:58:59.411 PM, Mar 24
Voice Call Report	Collin's AP	12:58:58.166 PM, Mar 24
Voice Call Report	Collin's AP	12:58:55.167 PM, Mar 24
Voice Call Report	Collin's AP	12:58:52.167 PM, Mar 24
Voice Call Report	Collin's AP	12:58:49.171 PM, Mar 24
Voice Call Report	Collin's AP	12:58:46.173 PM, Mar 24
Voice Call Report	Collin's AP	12:58:43.171 PM, Mar 24

AP	Collin's AP	AP MAC	d4:20:b0:c0:15:77
Average Packet Loss	2	Average RSSI	-62 dBm
Average SNR	28 dB	Average Voice Latency	4 ms
BSSID	d4:20:b0:d8:19:4c	Max Jitter	29ms
Packet IDs	[0]	Packet Loss Percentage	8%
Reason	tx power and data rate mismatch	RSSI	-63 dBm
		SNR	28 dB
RX Rate	105 Mbps	TX Rate of Max Packets	208 Mbps
Description	latency exceeded, packet loss exceeded	VOIP Link Quality	4



Client Events 35 Total 24 Good **7 Neutral** 4 Bad

Voice Call Summary Report	Collin's AP	12:00:47.994 PM, Apr 4
Incremental Interim Voice Call Report	Collin's AP	12:00:47.968 PM, Apr 4
Voice Call Report	Collin's AP	12:00:45.478 PM, Apr 4
Voice Call Report	Collin's AP	12:00:42.480 PM, Apr 4
Voice Call Report	Collin's AP	12:00:39.485 PM, Apr 4
Voice Call Report	Collin's AP	12:00:36.483 PM, Apr 4
Client disconnected	Collin's AP	01:15:32.346 PM, Mar 31

Average RSSI	-58 dBm	Average SNR	33 dB
Average Voice Latency	6 ms	BSSID	d4:20:b0:d8:19:4c
Max Jitter	10ms	Packet Loss Percentage	4%
RSSI	-57 dBm	RX Rate	27 Mbps
SNR	34 dB	Description	partial voice report after sip call stopped, latency exceeded, packet loss exceeded
TX Rate of Max Packets	32 Mbps		
VOIP Link Quality	4	Voice Latency	6 ms
		WIFI Link Quality	4

10

CHAPTER

Marvis App for Teams

Overview of the Marvis App for Microsoft Teams

SUMMARY

You can access Marvis from your Teams desktop or web client.

The Marvis Microsoft Teams app makes it easy for you to access Marvis directly from your Teams desktop or web client. The Marvis app is integrated with Microsoft Teams. You can use the app to search for devices, view details, troubleshoot your network and sites, and search for documentation without having to log in to the Juniper Mist™ portal. With the Marvis app, all the information is available on demand, right at your fingertips!

Using the Marvis app, you can log in to your organization and access information similar to how you would access the information in the Mist portal. Network Operation Center (NOC) users can use the app to debug all aspects of support tickets.

You can use the Marvis app as an individual user or as part of a team through a Teams channel.

This short video describes the Teams integration.

Video: Seamless Collaboration & Productivity with Marvis VNA + Microsoft Teams App Enhancement

Enable or Integrate the Marvis App in Microsoft Teams

SUMMARY

Your Microsoft Teams administrator can enable or integrate a third-party application such as Marvis in Teams. This topic provides the procedures to integrate the Marvis app in Teams.

IN THIS SECTION

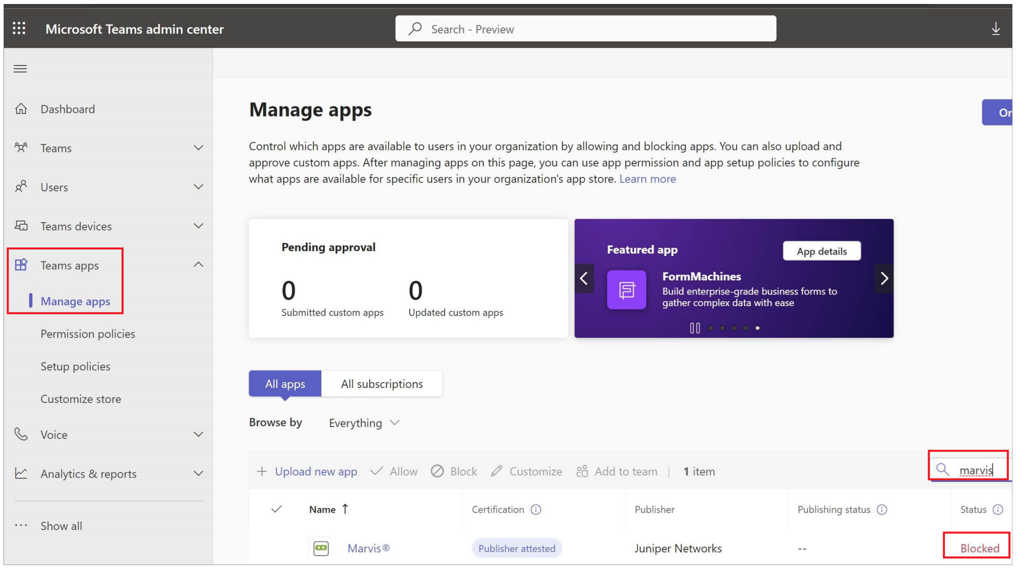
Go through these steps to enable the Marvis app, add the permission policy, and assign the permission to the users.

NOTE: The steps might vary based on updates and changes Microsoft makes to the Teams Admin Center. We recommend that you refer to the Microsoft documentation if the following steps look different from what you expect.

Enable the Marvis App in Your Teams Environment

To enable the Marvis app in your Teams environment:

1. In your web browser, navigate to the Microsoft Teams Admin Center (https://admin.teams.microsoft.com).
2. Log in using your administrator account (Teams admin or Global admin) credentials.
3. From the left menu, select **Teams apps** > **Manage apps**.



Manage apps

Control which apps are available to users in your organization by allowing and blocking apps. You can also upload and approve custom apps. After managing apps on this page, you can use app permission and app setup policies to configure what apps are available for specific users in your organization's app store. Learn more

Name ↑	Certification ⓘ	Publisher	Publishing status ⓘ	Status ⓘ
Marvis®	Publisher attested	Juniper Networks	--	Blocked

4. On the Manage apps page, search for **Marvis**.
   You'll see the Marvis app listed with the status as **Blocked**.
5. Click the Marvis app.

6. On the Marvis details page, change the status to **Allowed**.

The Marvis app is now enabled in your Teams environment.

Add the Permission Policy for the Marvis App

Permission policies allow you to control which users can use the Marvis app. You can control the access by creating and applying the policy to specific users. You can either create a policy or edit the default policy. We recommend that you create a policy.

To add the permission policy for the Marvis app:

1. From the left menu of the Microsoft Teams Admin Center window, select **Teams apps** > **Permission policies**.
2. Click **Add**. Provide a name and description for the policy.
3. Under **Third-party apps**, select an option that suits your organization's requirement. We recommend that you select **Allow specific apps and block all others.** This option enables you to select the apps that you want to allow in your Teams environment.
4. Click **Allow apps**.
5. Search for the Marvis app.
6. Select the Marvis app from the search results and click **Add**.
7. Click **Allow**.
8. Click **Save**.

Assign the Policy to Users

You can assign the policy to specific users or to a group of users.

To assign the policy to users:

1. From the left menu of the Microsoft Teams Admin Center window, navigate to the policy page.
2. To assign the policy to specific users:

   a. Select the policy, click **Manage users**, and then click **Assign users**.

   b. Add the users and then click **Apply**.

> **NOTE**: If you want to assign the policy to all users in your organization, modify the Global policy to allow the Marvis app. However, we do not recommend modifying the Global policy because it affects all users in your organization.

After you assign the policy, the Marvis app will be available to the users or Teams channels based on the assigned permission policy.

Install the Marvis App in Microsoft Teams

SUMMARY

Follow these procedures to install the Marvis app, connect it to your Juniper Mist™ organization, and add the app to a Teams channel.

IN THIS SECTION

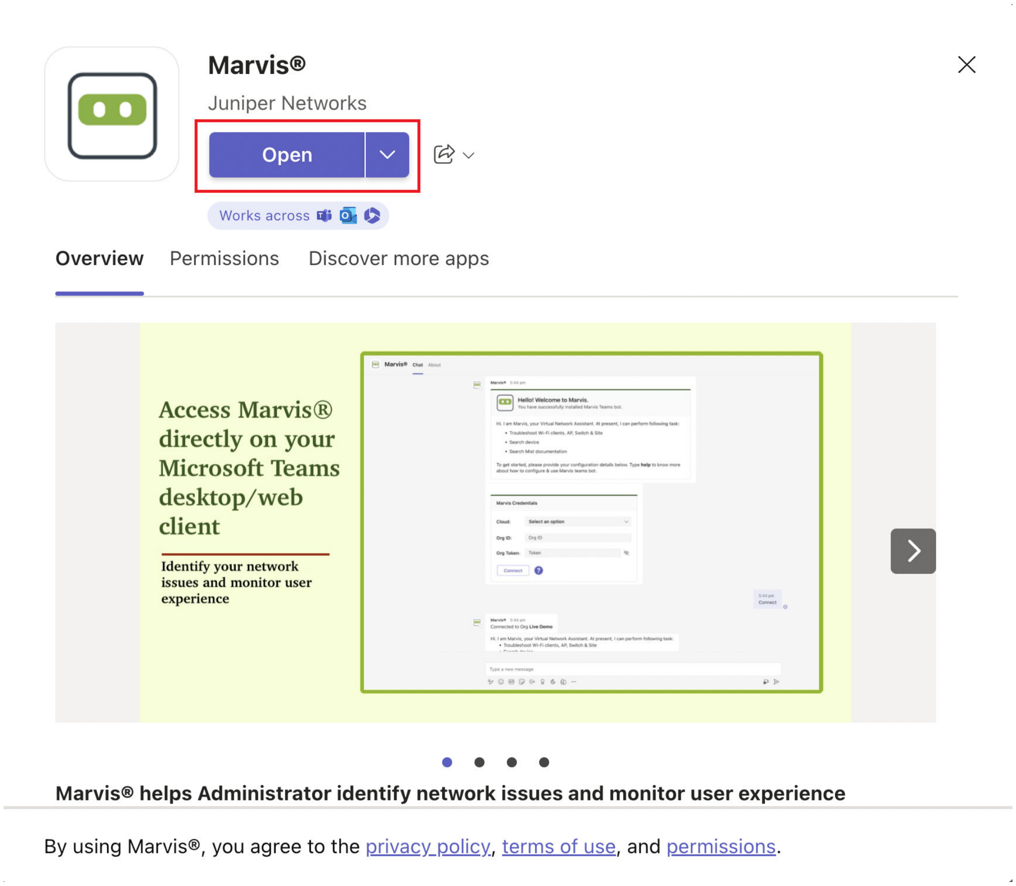
Teams users can install and use the Marvis app only if the administrator allows the app in the Teams environment. Additionally, the administrator must make the app available to users through permission policies. See "Enable or Integrate the Marvis App in Microsoft Teams" on page 222.

Install the Marvis App in Teams

To install the Marvis app in Teams:

1. From the left pane of your Microsoft Teams window, select **Apps**.
2. Enter **Marvis** in the Search box and click the Search icon.

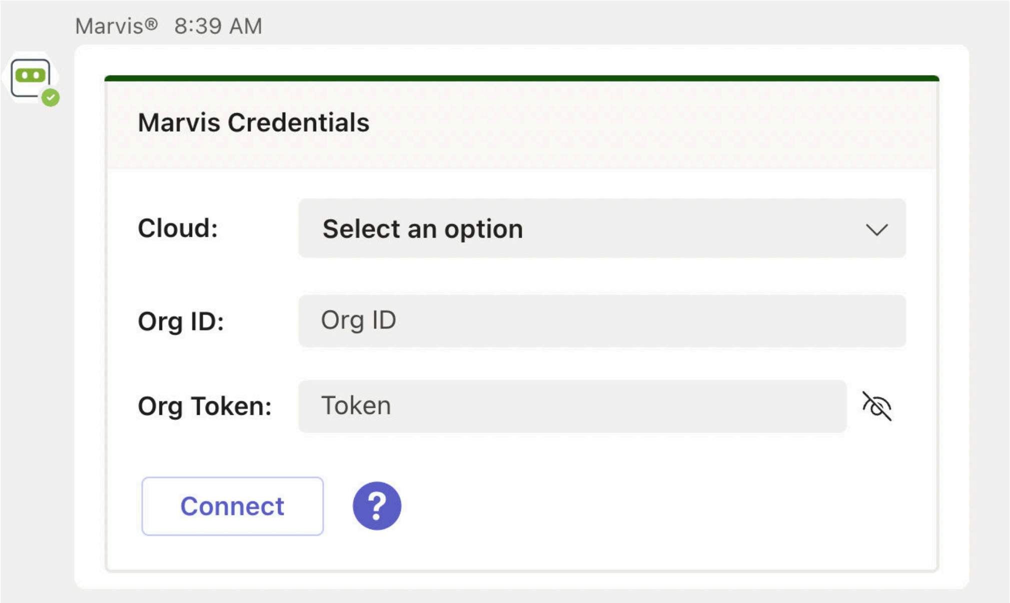
   You'll see the Marvis app listed in the search results.
3. Select the app and click **Open**.


Marvis®
Juniper Networks
Open
Works across
Overview
Permissions
Discover more apps
Access Marvis® directly on your Microsoft Teams desktop/web client
Identify your network issues and monitor user experience

Marvis® helps Administrator identify network issues and monitor user experience

By using Marvis®, you agree to the privacy policy, terms of use, and permissions.

You'll see the following window, which indicates that you have successfully installed the app:



Cloud: Select an option

Org ID: Org ID

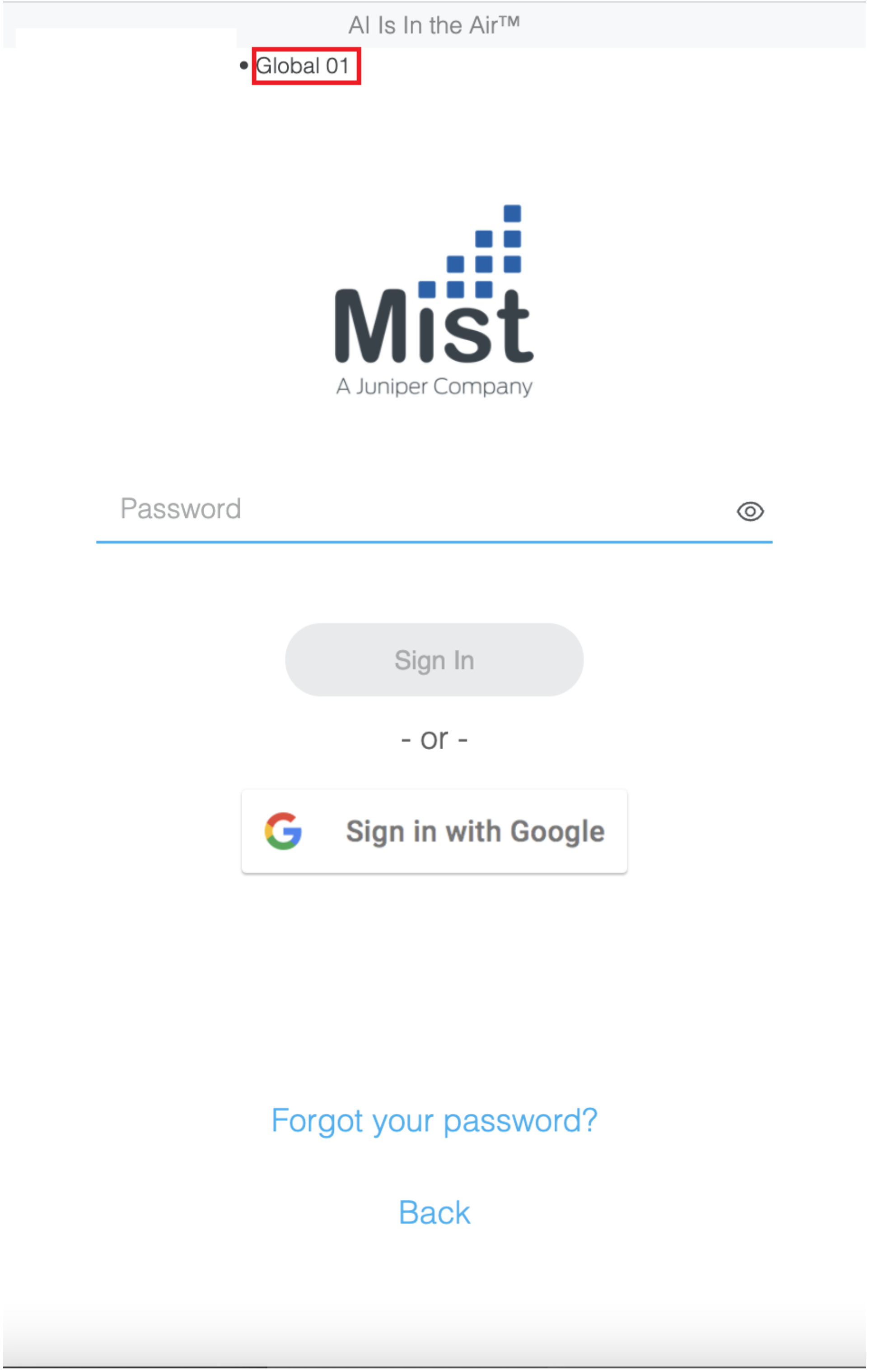
Org Token: Token

4. Next, you'll need to connect to your organization in the Mist portal.

Connect to Your Mist Organization

To connect to your Mist organization:

1. Enter the following details to log in to your organization:
    - Cloud environment name (for example, Global 01, Global 02). You can obtain this information from the Mist portal login screen.



AI Is In the Air™

- Global 01

Password

Sign In

- or -

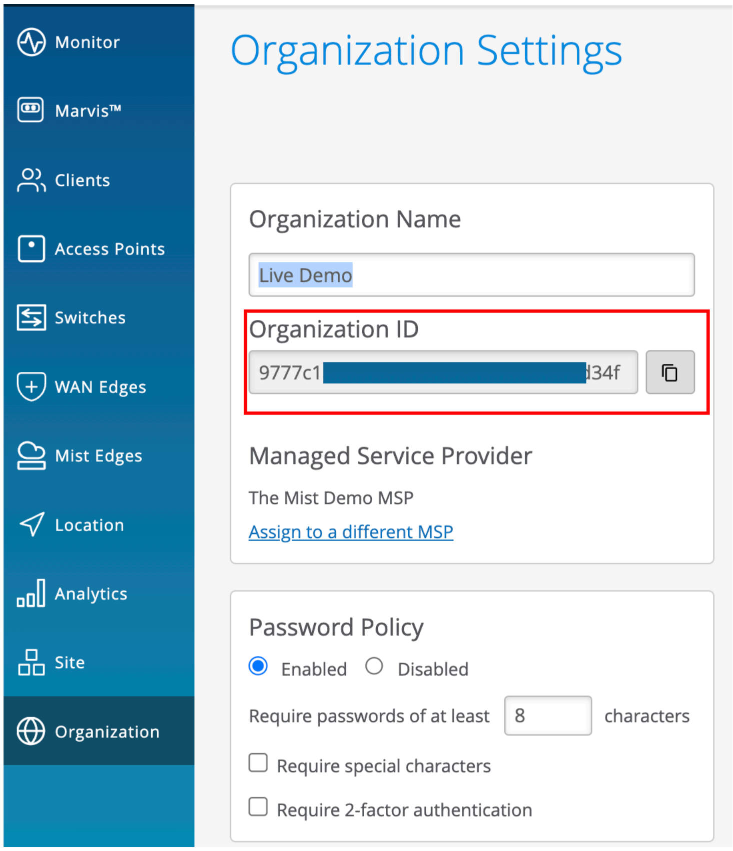
Sign in with Google

Forgot your password?

Back

- Organization ID (Org ID)

  You can find your Org ID on the **Organization** > **Settings** page in the Mist portal.



Organization Settings

Organization Name

Live Demo

Organization ID

9777c1[redacted]34f

Managed Service Provider

The Mist Demo MSP

Assign to a different MSP

Password Policy

● Enabled ○ Disabled

Require passwords of at least 8 characters

□ Require special characters

□ Require 2-factor authentication

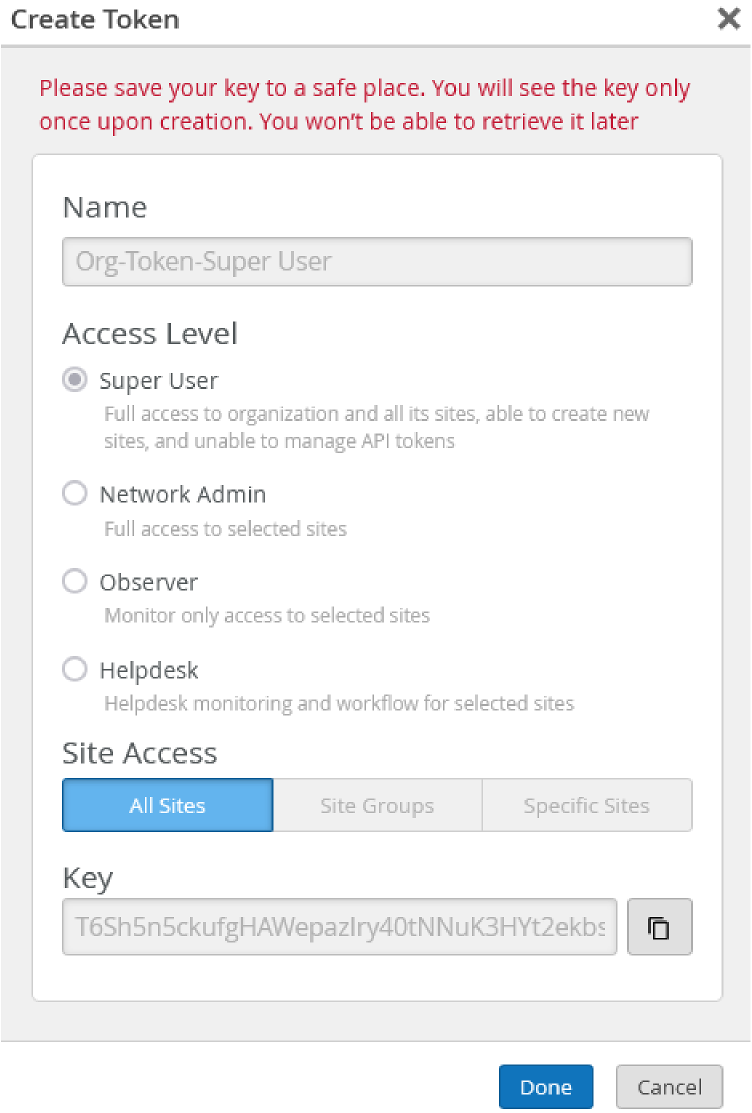
- Org Token

  You can generate the Org token on the **Organization** > **Settings** page in the Mist portal. The Org token operates like the user-based API token, but it is tied to a particular organization. Org token permission is based on the **Access Level** and **Site Access** options you select.

  To create a token:

  a. Click **Create Token** under the **API Token** section on the Settings page.

  b. Enter a name and click **Generate**. The generated key is the Org Token.



Create Token

Please save your key to a safe place. You will see the key only once upon creation. You won't be able to retrieve it later

Name

Org-Token-Super User

Access Level

● Super User

Full access to organization and all its sites, able to create new sites, and unable to manage API tokens

○ Network Admin

Full access to selected sites

○ Observer

Monitor only access to selected sites

○ Helpdesk

Helpdesk monitoring and workflow for selected sites

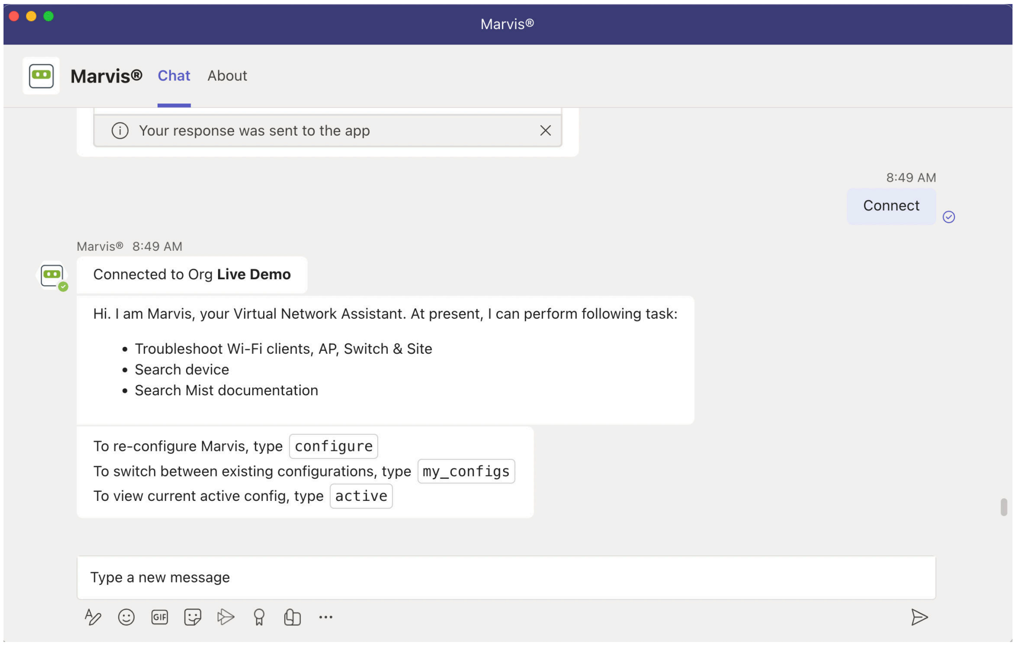
Site Access

[✓ All Sites] Site Groups Specific Sites

Key

T6Sh5n5ckufgHAWepazlry40tNNuK3HYt2ekbs

2. Click **Connect**. A successful connection displays the following window:



Your response was sent to the app

8:49 AM

Connect

Marvis® 8:49 AM

Connected to Org **Live Demo**

Hi. I am Marvis, your Virtual Network Assistant. At present, I can perform following task:

- Troubleshoot Wi-Fi clients, AP, Switch & Site
- Search device
- Search Mist documentation

To re-configure Marvis, type `configure`
To switch between existing configurations, type `my_configs`
To view current active config, type `active`

Type a new message

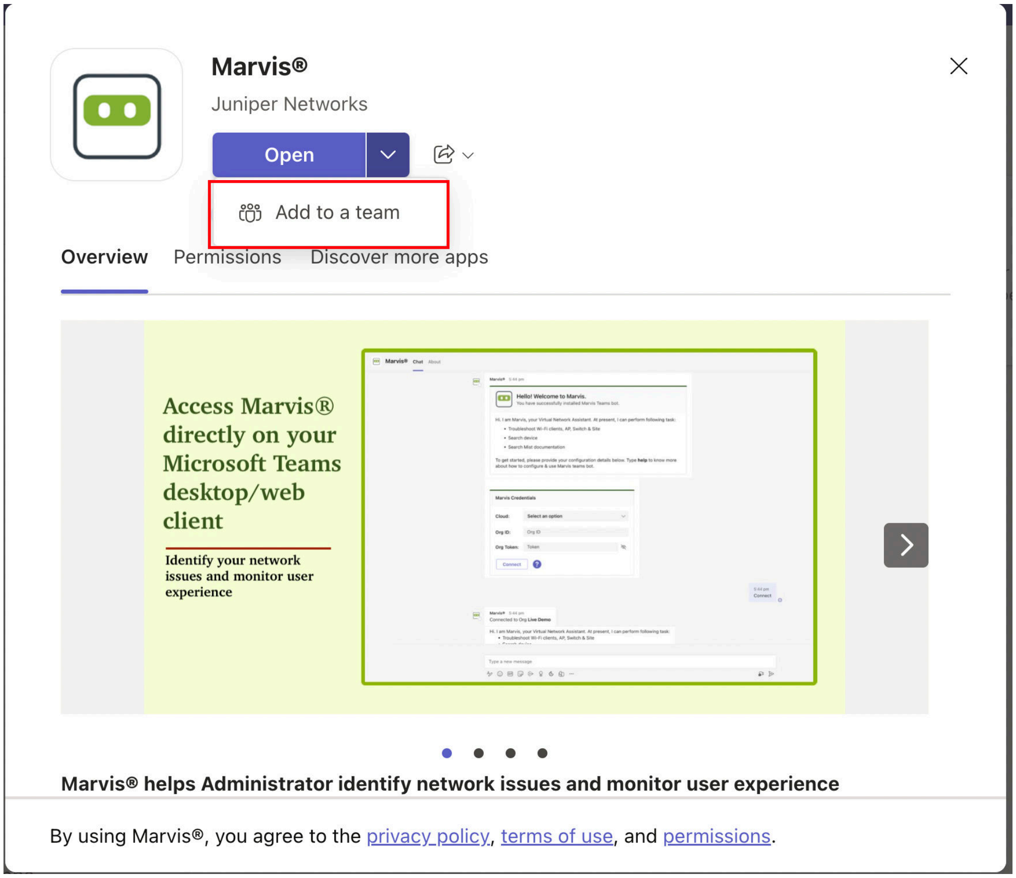
Add the Marvis App to a Microsoft Teams Channel

You can add the Marvis app to a Microsoft Teams channel as a team member. Members of that Teams channel can then query Marvis for information.

Before you add Marvis to a Teams channel, you must install the app in Teams and connect the app to the organization, as described in the previous sections.

To add the Marvis app to a Microsoft Teams channel:

1. In the left pane of your Microsoft Teams window, select **Apps**.
2. Enter **Marvis** in the Search box and click **Search**.
   You'll see the Marvis app listed in the search results.
3. Click the app and select **Add to a Team**.



Access Marvis® directly on your Microsoft Teams desktop/web client

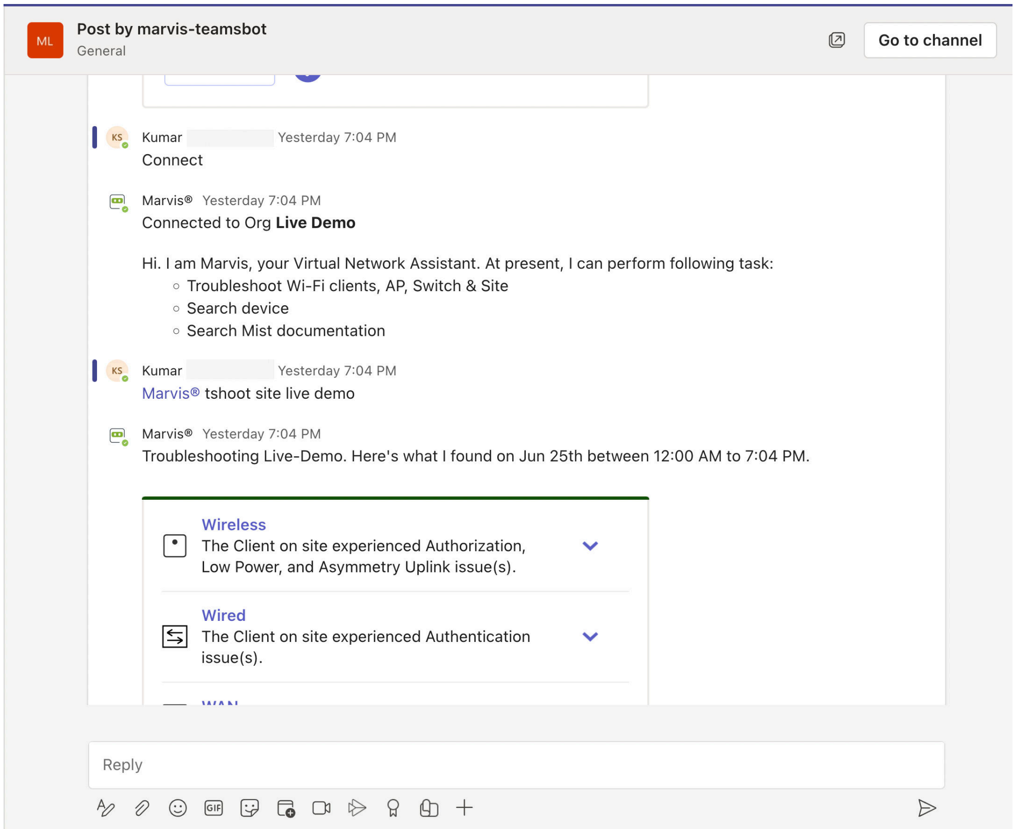
Identify your network issues and monitor user experience

Marvis® helps Administrator identify network issues and monitor user experience

By using Marvis®, you agree to the privacy policy, terms of use, and permissions.

4. Select the Teams channel.

   That's it! You and your team members can start asking Marvis questions.



KS Kumar Yesterday 7:04 PM
Connect

Marvis® Yesterday 7:04 PM
Connected to Org **Live Demo**

Hi. I am Marvis, your Virtual Network Assistant. At present, I can perform following task:

- Troubleshoot Wi-Fi clients, AP, Switch & Site
- Search device
- Search Mist documentation

KS Kumar Yesterday 7:04 PM
Marvis® tshoot site live demo

Marvis® Yesterday 7:04 PM
Troubleshooting Live-Demo. Here's what I found on Jun 25th between 12:00 AM to 7:04 PM.

Wireless
The Client on site experienced Authorization, Low Power, and Asymmetry Uplink issue(s).

Wired
The Client on site experienced Authentication issue(s).

5. Use the @marvis prompt to enter your first question.

Troubleshoot Using the Marvis App

SUMMARY

Follow these procedures to troubleshoot issues with wireless and wired clients, devices, and sites.

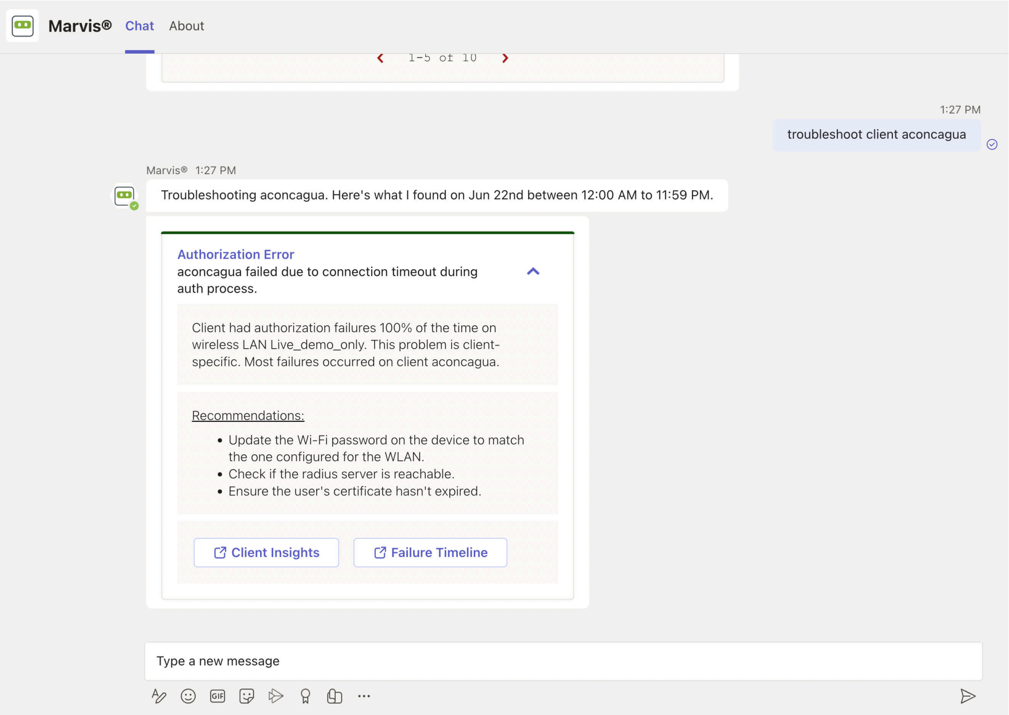
IN THIS SECTION

Troubleshoot a Wireless Client

Using the Marvis app, you can view failures of a wireless client and its associated access point (AP).

To check whether a wireless client is experiencing any issues, enter a phrase such as "Troubleshoot client *name*" in the Teams window.

Here's an example that shows the details Marvis provides for the phrase "troubleshoot client *name*." In this case, Marvis reports that the client is experiencing an authorization error due to a connection timeout.



1:27 PM

troubleshoot client aconcagua

Marvis® 1:27 PM

Troubleshooting aconcagua. Here's what I found on Jun 22nd between 12:00 AM to 11:59 PM.

Authorization Error

aconcagua failed due to connection timeout during auth process.

Client had authorization failures 100% of the time on wireless LAN Live_demo_only. This problem is client-specific. Most failures occurred on client aconcagua.

Recommendations:

- Update the Wi-Fi password on the device to match the one configured for the WLAN.
- Check if the radius server is reachable.
- Ensure the user's certificate hasn't expired.

You can click the issue to view details. You can click the **Client Insights** or **Failure Timeline** option for more details. In some cases, Marvis also provides recommendations to fix the issue, as the screenshot shows.

Here are some sample phrases that you can use to troubleshoot wireless clients:

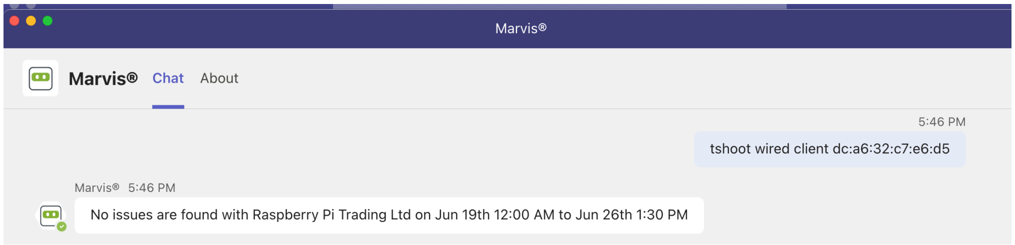
- how was <client name> on June 22nd
- tshoot client <mac or name> on June 21

Troubleshoot a Wired Client

To view wired clients that are experiencing issues, use phrases such as the following:

- tshoot wired client <mac>
- troubleshoot client name

Here's an example that shows the details Marvis provides for the phrase "tshoot wired client <mac>".



5:46 PM

tshoot wired client dc:a6:32:c7:e6:d5

Marvis® 5:46 PM

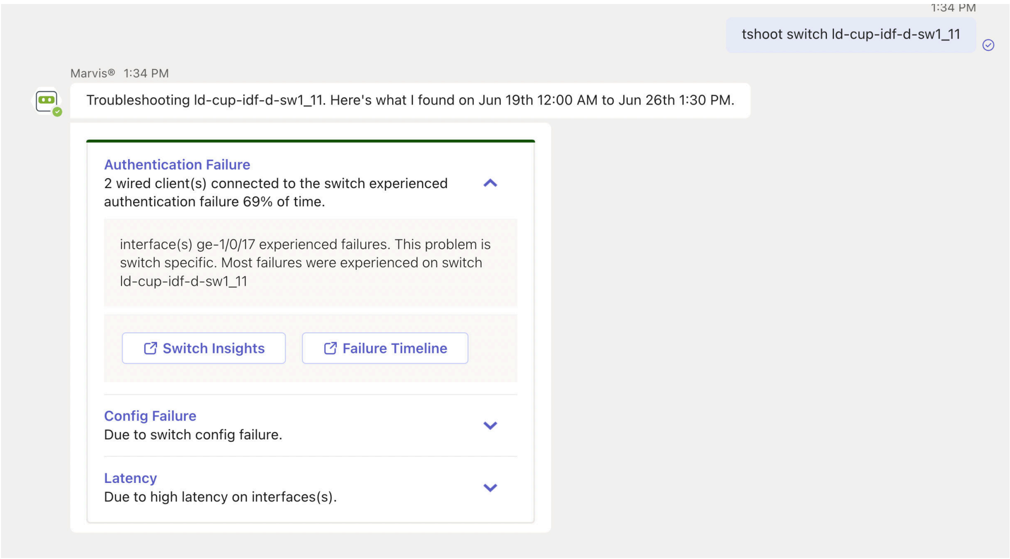
No issues are found with Raspberry Pi Trading Ltd on Jun 19th 12:00 AM to Jun 26th 1:30 PM

Troubleshoot a Device

You can use the Marvis app to check for issues on APs, switches, or WAN edge devices.

To check whether a device is experiencing any issues, enter a phrase such as "tshoot switch *name*" or "tshoot *device name*" in the Teams window.

Here's an example that shows the details Marvis provides for the phrase "tshoot switch *name*." In this case, Marvis reports that two clients connected to the switch experienced an authentication failure.



1:34 PM

tshoot switch ld-cup-idf-d-sw1_11

Marvis® 1:34 PM

Troubleshooting ld-cup-idf-d-sw1_11. Here's what I found on Jun 19th 12:00 AM to Jun 26th 1:30 PM.

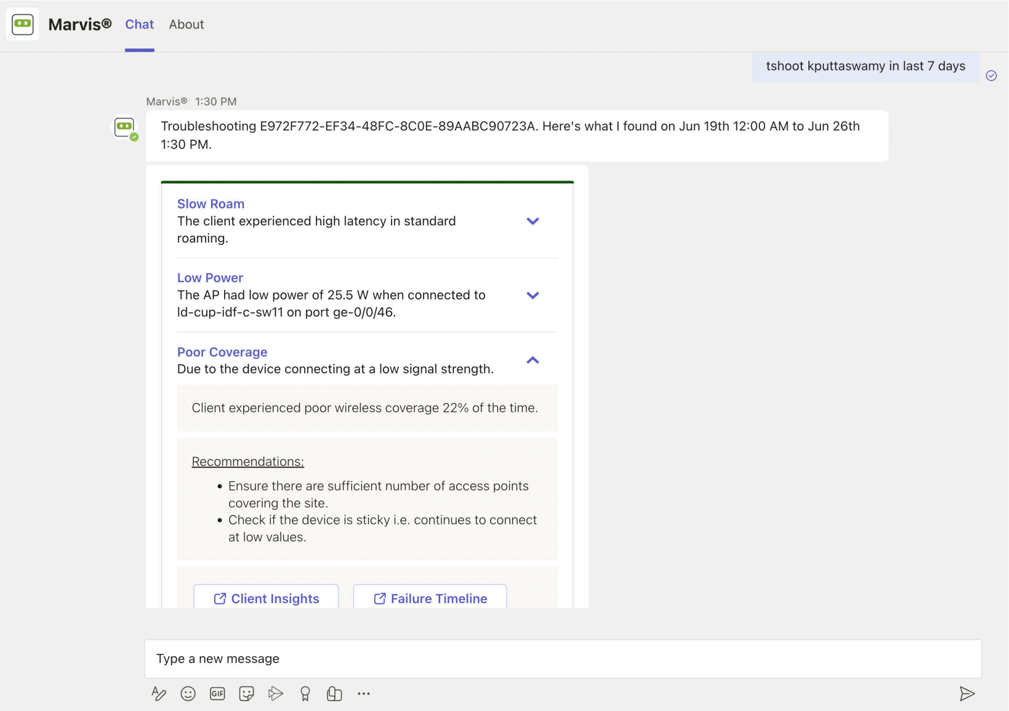
Authentication Failure
2 wired client(s) connected to the switch experienced authentication failure 69% of time.

interface(s) ge-1/0/17 experienced failures. This problem is switch specific. Most failures were experienced on switch ld-cup-idf-d-sw1_11

Config Failure
Due to switch config failure.

Latency
Due to high latency on interfaces(s).

You can click the issue to view details. You can click the **Switch Insights** or **Failure Timeline** option for more details. In some cases, Marvis also provides recommendations to fix the issue, as the following screenshot shows:



tshoot kputtaswamy in last 7 days

Marvis® 1:30 PM

Troubleshooting E972F772-EF34-48FC-8C0E-89AABC90723A. Here's what I found on Jun 19th 12:00 AM to Jun 26th 1:30 PM.

Slow Roam
The client experienced high latency in standard roaming.

Low Power
The AP had low power of 25.5 W when connected to ld-cup-idf-c-sw11 on port ge-0/0/46.

Poor Coverage
Due to the device connecting at a low signal strength.

Client experienced poor wireless coverage 22% of the time.

Recommendations:

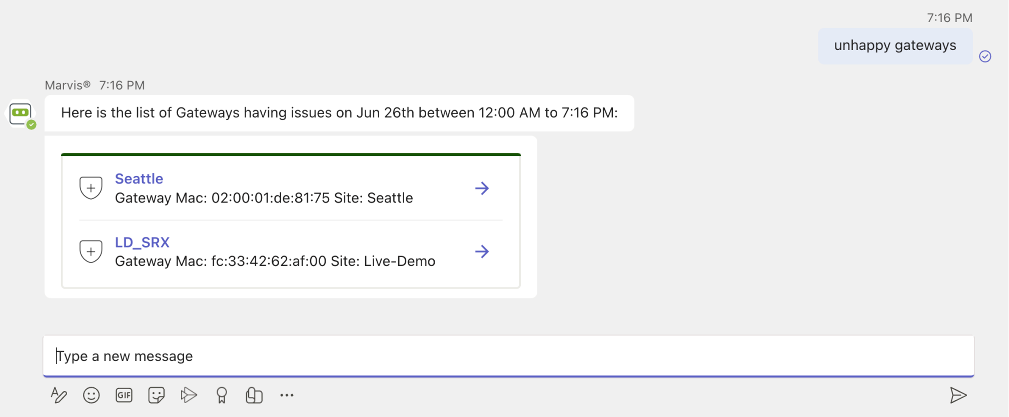
- Ensure there are sufficient number of access points covering the site.
- Check if the device is sticky i.e. continues to connect at low values.

Troubleshoot Unhappy Devices or Clients

To check for devices experiencing issues (unhappy devices), simply enter the phrase "unhappy <device type>" in the Marvis chat window. For example, if you want to view unhappy WAN edge devices, enter "unhappy WAN edges" and Marvis will show all the WAN edges that are experiencing issues.

Here are a few examples. You can click any device to view the issues.

Unhappy WAN edges:


7:16 PM

unhappy gateways

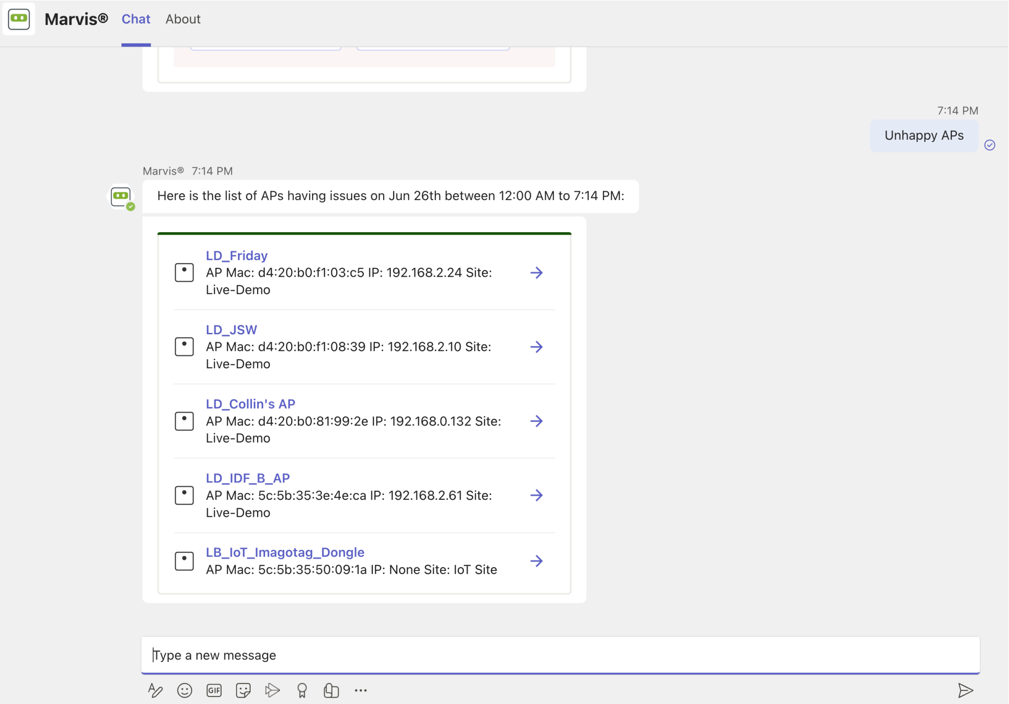
Marvis® 7:16 PM

Here is the list of Gateways having issues on Jun 26th between 12:00 AM to 7:16 PM:

Seattle
Gateway Mac: 02:00:01:de:81:75 Site: Seattle

LD_SRX
Gateway Mac: fc:33:42:62:af:00 Site: Live-Demo

Unhappy APs:



7:14 PM

Unhappy APs

Marvis® 7:14 PM

Here is the list of APs having issues on Jun 26th between 12:00 AM to 7:14 PM:

LD_Friday
AP Mac: d4:20:b0:f1:03:c5 IP: 192.168.2.24 Site: Live-Demo

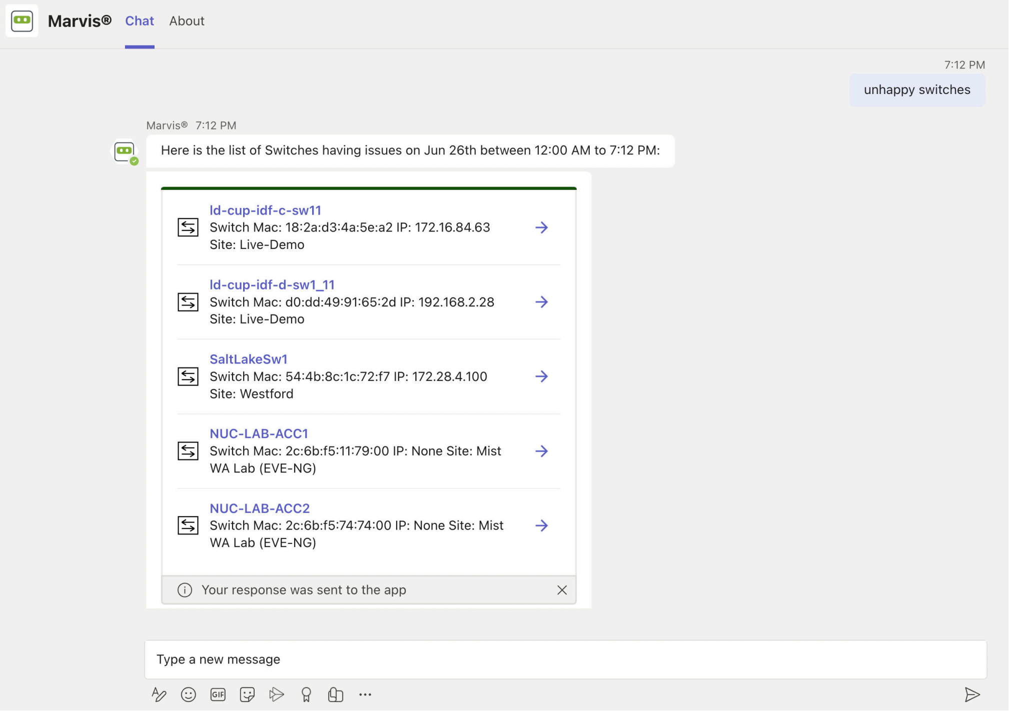
LD_JSW
AP Mac: d4:20:b0:f1:08:39 IP: 192.168.2.10 Site: Live-Demo

LD_Collin's AP
AP Mac: d4:20:b0:81:99:2e IP: 192.168.0.132 Site: Live-Demo

LD_IDF_B_AP
AP Mac: 5c:5b:35:3e:4e:ca IP: 192.168.2.61 Site: Live-Demo

LB_IoT_Imagotag_Dongle
AP Mac: 5c:5b:35:50:09:1a IP: None Site: IoT Site

Unhappy Switches:



7:12 PM

unhappy switches

Marvis® 7:12 PM

Here is the list of Switches having issues on Jun 26th between 12:00 AM to 7:12 PM:

ld-cup-idf-c-sw11
Switch Mac: 18:2a:d3:4a:5e:a2 IP: 172.16.84.63 Site: Live-Demo

ld-cup-idf-d-sw1_11
Switch Mac: d0:dd:49:91:65:2d IP: 192.168.2.28 Site: Live-Demo

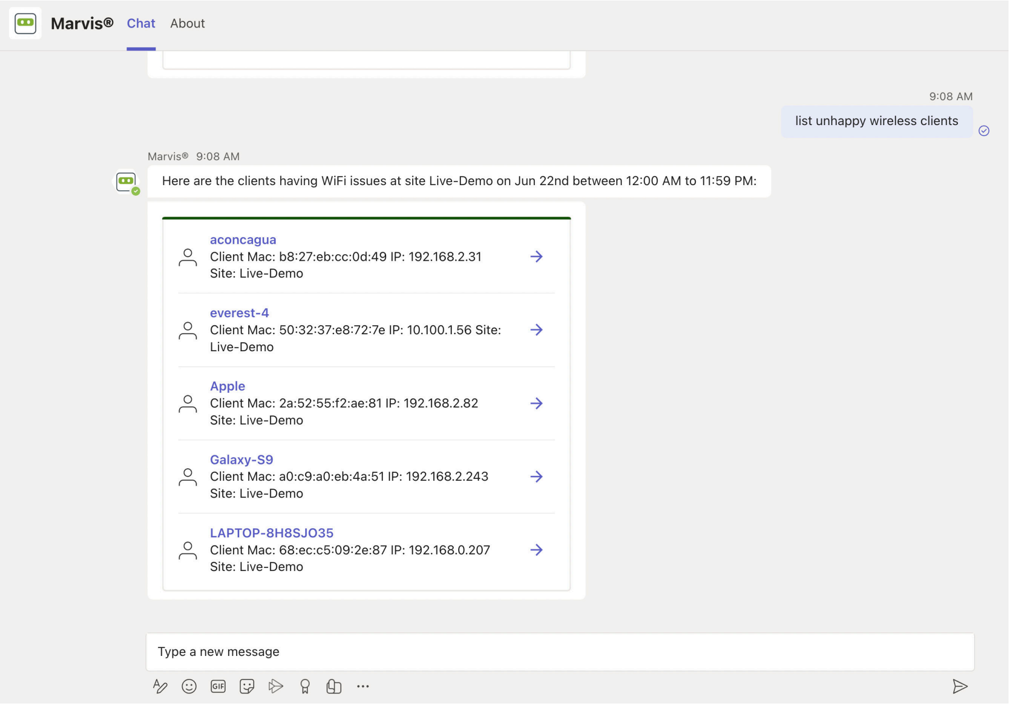
SaltLakeSw1
Switch Mac: 54:4b:8c:1c:72:f7 IP: 172.28.4.100 Site: Westford

NUC-LAB-ACC1
Switch Mac: 2c:6b:f5:11:79:00 IP: None Site: Mist WA Lab (EVE-NG)

NUC-LAB-ACC2
Switch Mac: 2c:6b:f5:74:74:00 IP: None Site: Mist WA Lab (EVE-NG)

Your response was sent to the app

Unhappy Wireless Clients:



9:08 AM

list unhappy wireless clients

Marvis® 9:08 AM

Here are the clients having WiFi issues at site Live-Demo on Jun 22nd between 12:00 AM to 11:59 PM:

aconcagua
Client Mac: b8:27:eb:cc:0d:49 IP: 192.168.2.31 Site: Live-Demo

everest-4
Client Mac: 50:32:37:e8:72:7e IP: 10.100.1.56 Site: Live-Demo

Apple
Client Mac: 2a:52:55:f2:ae:81 IP: 192.168.2.82 Site: Live-Demo

Galaxy-S9
Client Mac: a0:c9:a0:eb:4a:51 IP: 192.168.2.243 Site: Live-Demo

LAPTOP-8H8SJO35
Client Mac: 68:ec:c5:09:2e:87 IP: 192.168.0.207 Site: Live-Demo

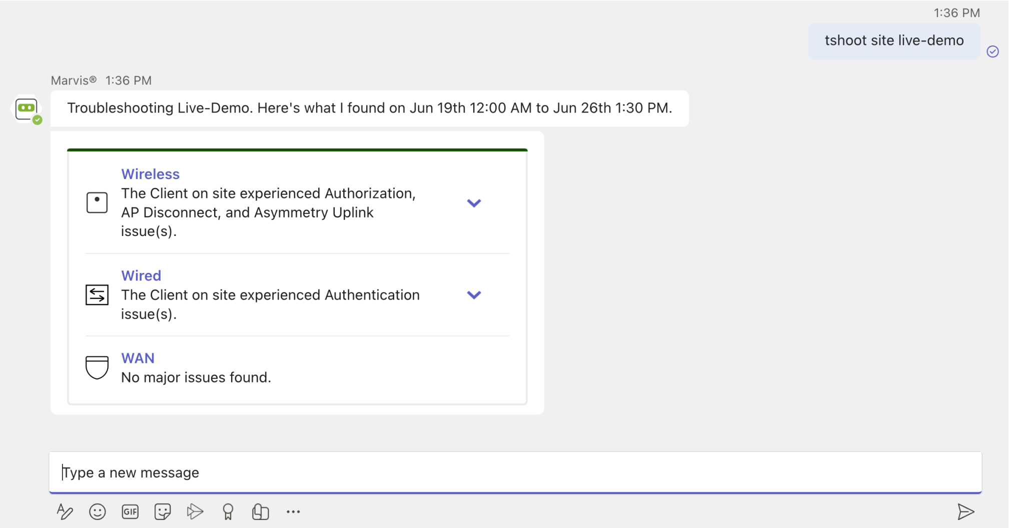
Troubleshoot a Site

You can use the Marvis app to troubleshoot sites to identify site-level failures.

To check whether a device is experiencing any issues, enter a phrase such as "troubleshoot site *name*" in the Teams window.

Here's an example that shows the details Marvis provides for the phrase "troubleshoot site *name*." Marvis shows the troubleshooting results for the site. Marvis classifies these failures under the following categories:

- Wireless
- Wired
- WAN



1:36 PM

tshoot site live-demo

Marvis® 1:36 PM

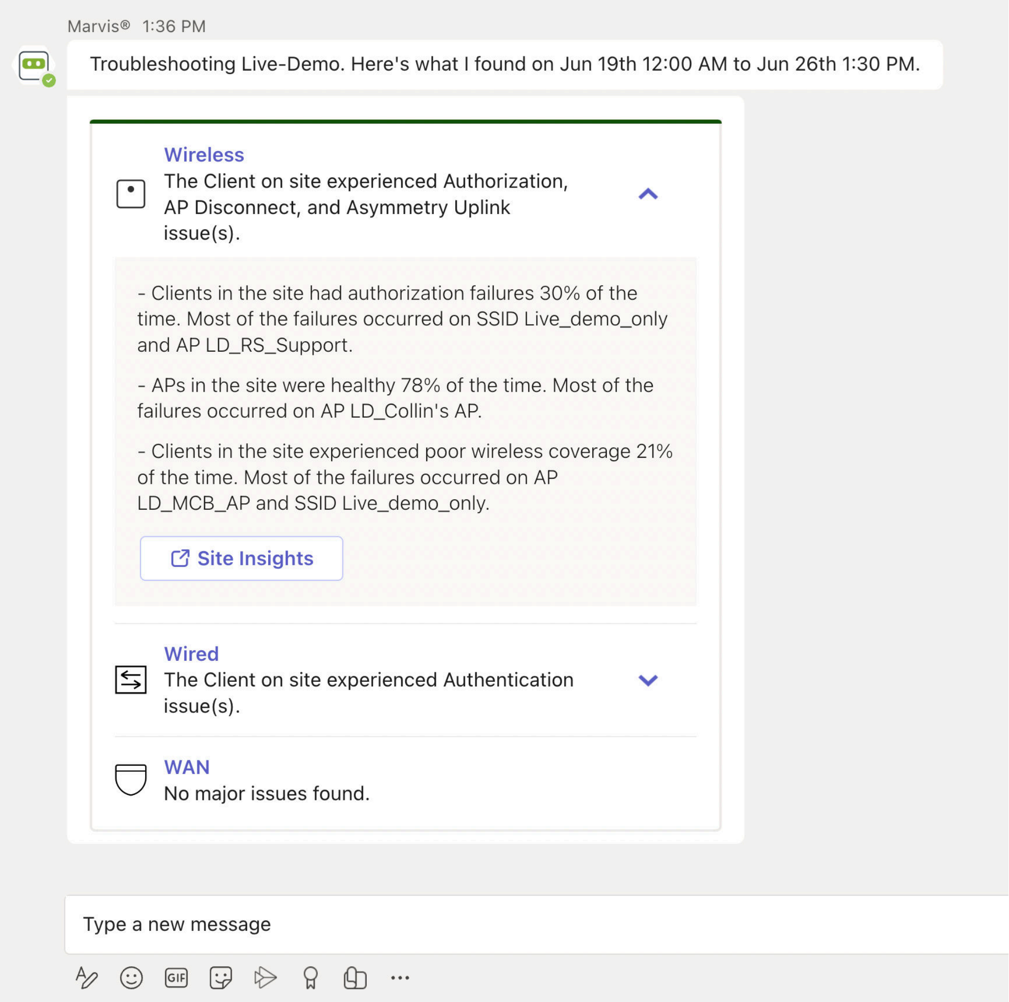
Troubleshooting Live-Demo. Here's what I found on Jun 19th 12:00 AM to Jun 26th 1:30 PM.

Wireless
The Client on site experienced Authorization, AP Disconnect, and Asymmetry Uplink issue(s).

Wired
The Client on site experienced Authentication issue(s).

WAN
No major issues found.

You can click the expand arrow to view more details. You can drill down further to view site-level insights and device-level insights.



Marvis® 1:36 PM

Troubleshooting Live-Demo. Here's what I found on Jun 19th 12:00 AM to Jun 26th 1:30 PM.

Wireless
The Client on site experienced Authorization, AP Disconnect, and Asymmetry Uplink issue(s).

- Clients in the site had authorization failures 30% of the time. Most of the failures occurred on SSID Live_demo_only and AP LD_RS_Support.

- APs in the site were healthy 78% of the time. Most of the failures occurred on AP LD_Collin's AP.

- Clients in the site experienced poor wireless coverage 21% of the time. Most of the failures occurred on AP LD_MCB_AP and SSID Live_demo_only.

Wired
The Client on site experienced Authentication issue(s).

WAN
No major issues found.

Search and List Functions in the Marvis App

SUMMARY

Use the Marvis App to search for devices, sites, and documentation.

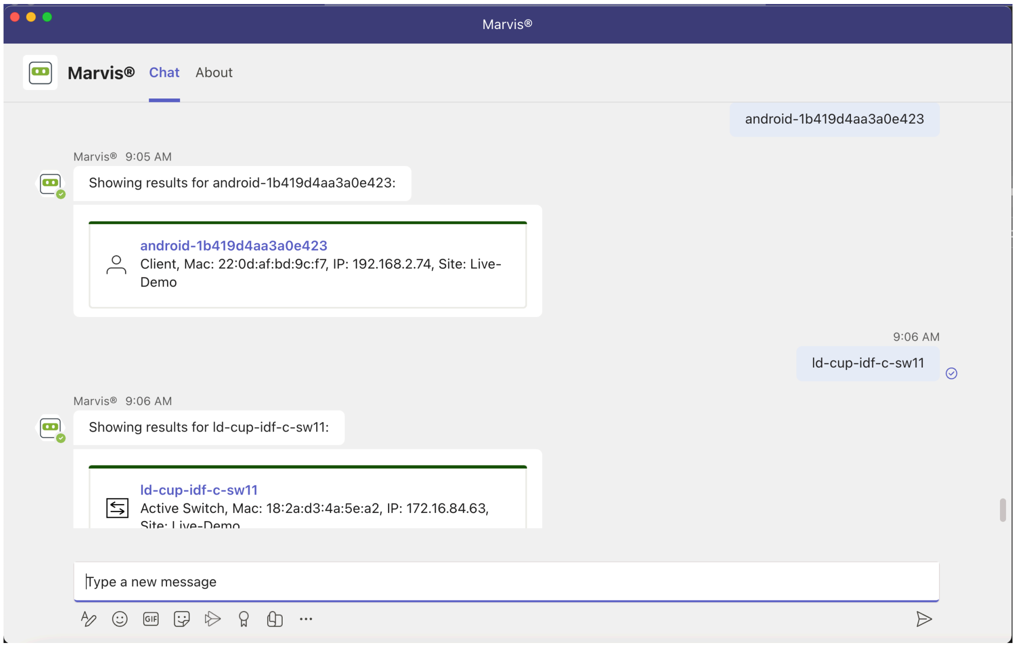
IN THIS SECTION

Search for Devices and Sites

You can use the Marvis app to search for devices such as wireless or wired clients, access points (APs), switches, and WAN edge devices based on the device’s name or MAC address. You can also search for sites by site name. To search for a device or site, simply enter the device or site name in the Marvis chat window.

The search results provide links to the Insights page for the device or site. Note that you can even search using partial names.

Here's an example:



android-1b419d4aa3a0e423

Marvis® 9:05 AM
Showing results for android-1b419d4aa3a0e423:

android-1b419d4aa3a0e423
Client, Mac: 22:0d:af:bd:9c:f7, IP: 192.168.2.74, Site: Live-Demo

9:06 AM
ld-cup-idf-c-sw11

Marvis® 9:06 AM
Showing results for ld-cup-idf-c-sw11:

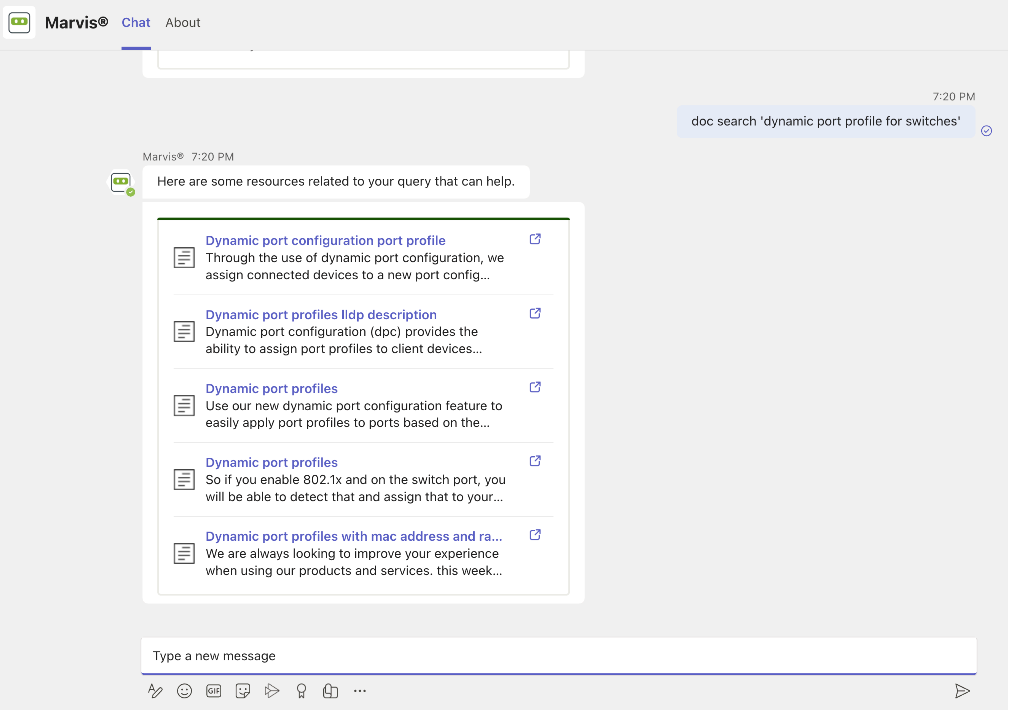
ld-cup-idf-c-sw11
Active Switch, Mac: 18:2a:d3:4a:5e:a2, IP: 172.16.84.63, Site: Live-Demo

Here are some examples of phrases that you can use to search for a device or site:

- <client name>
- Search <ap mac> <switch model>
- Find <WAN edge mac>
- <wired client mac>
- <site partial name>
- Locate <client username>

Search for Documentation

You can search for documentation without having to go to the Juniper Networks documentation portal. To search for documentation, enter a phrase such as "doc search <text>" in the Marvis chat window. It is not necessary to enter the exact name of the topic. You can enter a word or phrase, and Marvis displays all topics containing the text you entered. The following screenshot shows the results of a documentation search using the phrase "doc search <text>".



7:20 PM

doc search 'dynamic port profile for switches'

Marvis® 7:20 PM

Here are some resources related to your query that can help.

Dynamic port configuration port profile
Through the use of dynamic port configuration, we assign connected devices to a new port config...

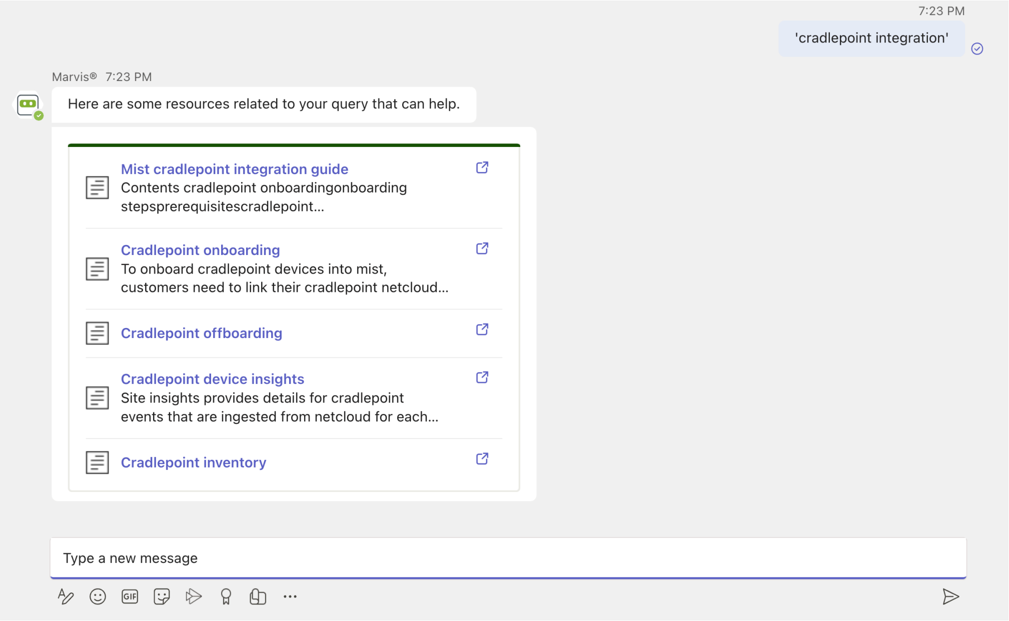
Dynamic port profiles lldp description
Dynamic port configuration (dpc) provides the ability to assign port profiles to client devices...

Dynamic port profiles
Use our new dynamic port configuration feature to easily apply port profiles to ports based on the...

Dynamic port profiles
So if you enable 802.1x and on the switch port, you will be able to detect that and assign that to your...

Dynamic port profiles with mac address and ra...
We are always looking to improve your experience when using our products and services. this week...

In the following screenshot, notice that Marvis displays documentation links even though the phrase does not contain the key words such as "doc" or "search.".



7:23 PM

'cradlepoint integration'

Marvis® 7:23 PM

Here are some resources related to your query that can help.

Mist cradlepoint integration guide
Contents cradlepoint onboardingonboarding stepsprerequisitescradlepoint...

Cradlepoint onboarding
To onboard cradlepoint devices into mist, customers need to link their cradlepoint netcloud...

Cradlepoint offboarding

Cradlepoint device insights
Site insights provides details for cradlepoint events that are ingested from netcloud for each...

Cradlepoint inventory

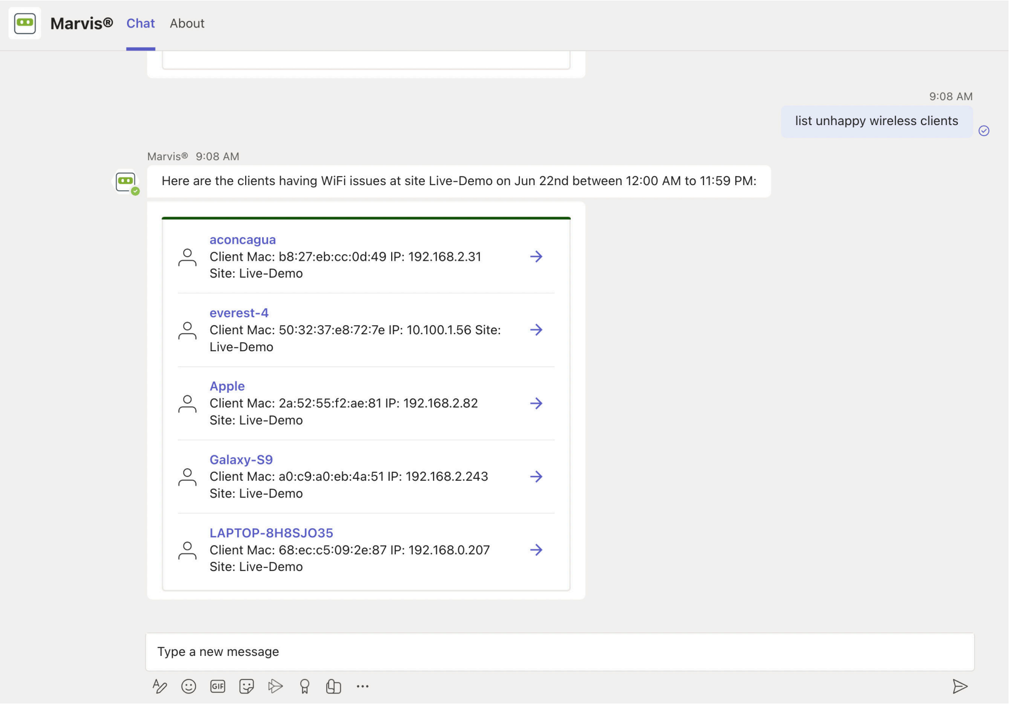
List Function

You can also use the list function to view information such as unhappy clients, access points (APs) running an incorrect firmware version, and switches in a site.

To determine which clients are experiencing connectivity issues (which we also refer to as *unhappy clients*), use phrases such as, "list unhappy wireless clients" or "list unhappy clients" without providing details.

Marvis displays a list of clients that are experiencing issues. You can select any client from the list to view the details.

Here is an example that shows the details that Marvis displays for "unhappy clients."



9:08 AM

list unhappy wireless clients

Marvis® 9:08 AM

Here are the clients having WiFi issues at site Live-Demo on Jun 22nd between 12:00 AM to 11:59 PM:

aconcagua
Client Mac: b8:27:eb:cc:0d:49 IP: 192.168.2.31 Site: Live-Demo

everest-4
Client Mac: 50:32:37:e8:72:7e IP: 10.100.1.56 Site: Live-Demo

Apple
Client Mac: 2a:52:55:f2:ae:81 IP: 192.168.2.82 Site: Live-Demo

Galaxy-S9
Client Mac: a0:c9:a0:eb:4a:51 IP: 192.168.2.243 Site: Live-Demo

LAPTOP-8H8SJO35
Client Mac: 68:ec:c5:09:2e:87 IP: 192.168.0.207 Site: Live-Demo

View or Change the Organization in the Marvis App

SUMMARY

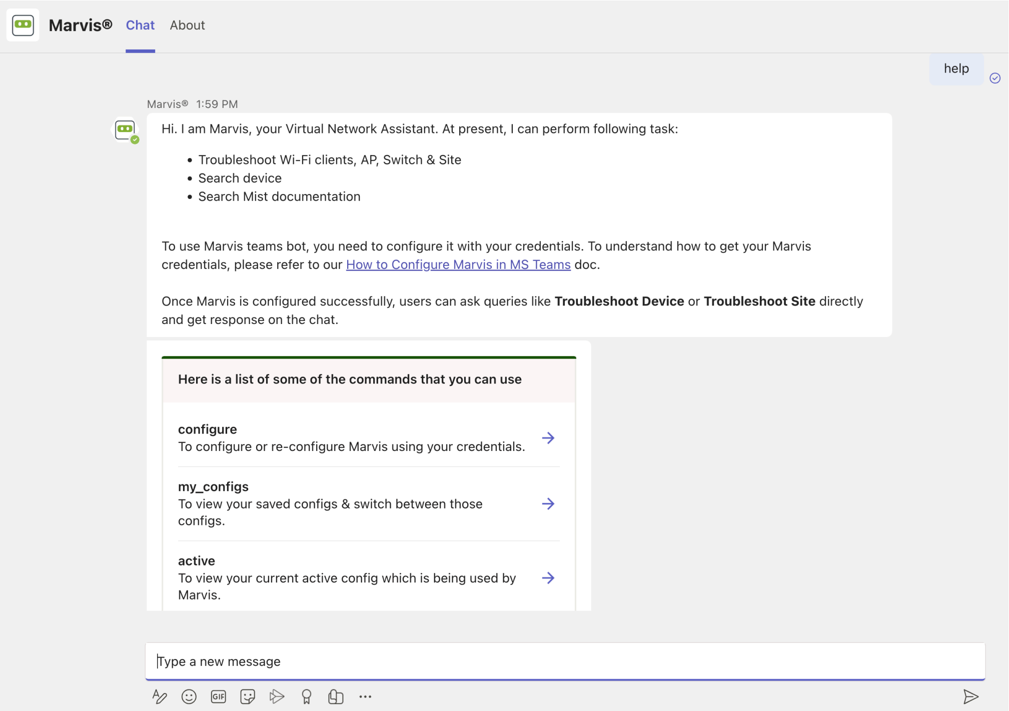
Select the organization that you want to view in the Marvis app.

You can run queries against multiple organizations and also switch between organizations using the Marvis app,

The Marvis app enables you to:

- Switch between organizations.
- View the current active organization (that is, the organization that you're connected to).
- Connect to a new organization or reconnect to the active organization.

Simply type **help** in the Marvis chat window, and you'll see details about the **configure**, **my_configs**, and **active** options:



help

Marvis® 1:59 PM

Hi. I am Marvis, your Virtual Network Assistant. At present, I can perform following task:

- Troubleshoot Wi-Fi clients, AP, Switch & Site
- Search device
- Search Mist documentation

To use Marvis teams bot, you need to configure it with your credentials. To understand how to get your Marvis credentials, please refer to our How to Configure Marvis in MS Teams doc.

Once Marvis is configured successfully, users can ask queries like **Troubleshoot Device** or **Troubleshoot Site** directly and get response on the chat.

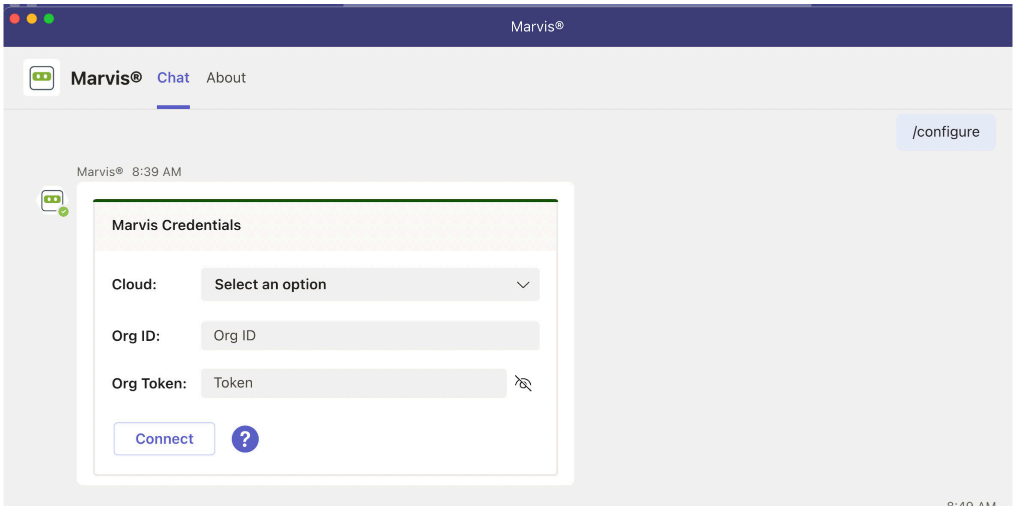
Here is a list of some of the commands that you can use

configure
To configure or re-configure Marvis using your credentials.

my_configs
To view your saved configs & switch between those configs.

active
To view your current active config which is being used by Marvis.

- If you enter **configure**, Marvis displays the login screen. You can either reconnect to the current active organization or connect to a different organization.



/configure

Marvis® 8:39 AM

Marvis Credentials

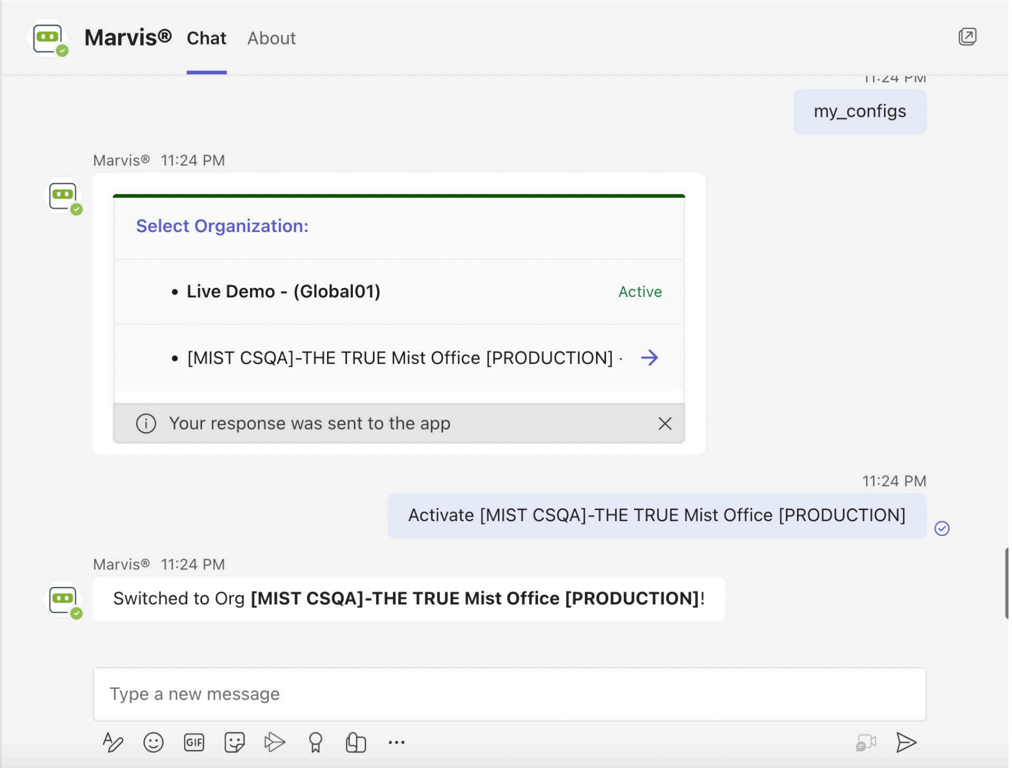
Cloud: Select an option

Org ID: Org ID

Org Token: Token

- If you enter **my_configs**, Marvis displays the following:
  - Organizations that you're connected to
  - The current active organization

  Selecting another organization makes it the active organization. You can query Marvis for information about the devices and sites in that organization.



11:24 PM

my_configs

Marvis® 11:24 PM

Select Organization:

- **Live Demo - (Global01)** Active
- [MIST CSQA]-THE TRUE Mist Office [PRODUCTION] ·

Your response was sent to the app

11:24 PM

Activate [MIST CSQA]-THE TRUE Mist Office [PRODUCTION]

Marvis® 11:24 PM

Switched to Org **[MIST CSQA]-THE TRUE Mist Office [PRODUCTION]**!

- If you enter **active**, Marvis displays the organization that is currently active.

11

CHAPTER

Troubleshooting Examples

Troubleshoot Wireless Connectivity Issues

IN THIS SECTION

To recap the information from the various chapters of this guide, this use case shows how you can use wireless SLEs, the Insights page, Marvis Actions, and the Marvis Conversational Assistant to investigate and troubleshoot connectivity issues.

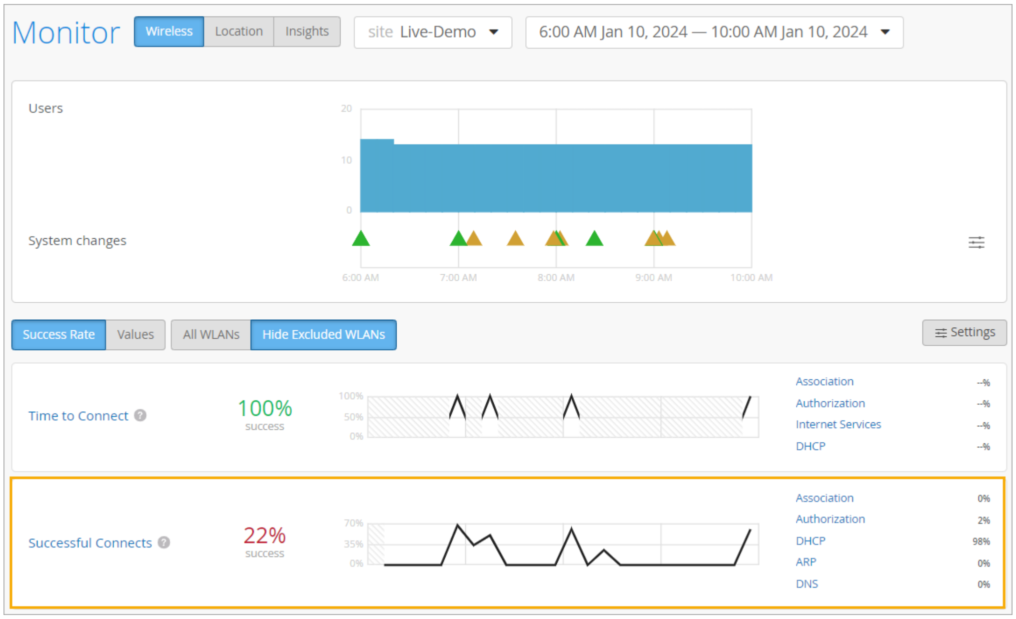
Typically, you wouldn't use *all* these tools, but this use case illustrates the valuable insights that you can gain from these tools. Use whichever options suit your situation and your preferences for working in the Juniper Mist™ portal.

Troubleshoot with the Successful Connects SLE

Let's start on the Wireless SLEs dashboard. SLEs offer insights into current and past issues.

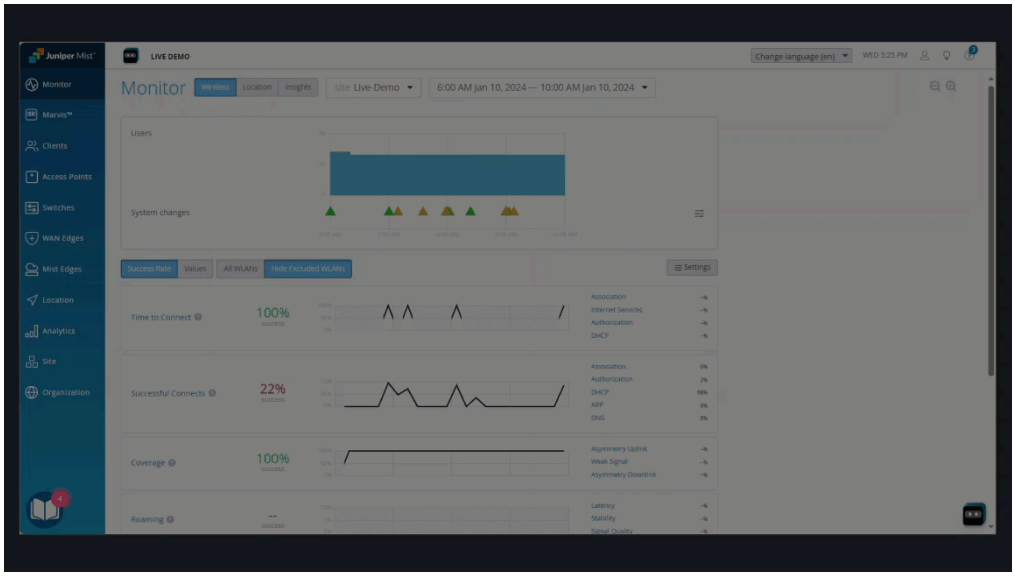
NOTE: To find the Wireless SLEs dashboard, select **Monitor** > **Service Levels** from the left menu, and then click the **Wireless** button.

In this example, you see that only 22 percent of connects were successful. On the right side of the SLE block, you see that 98 percent of the issues involved DHCP errors.



NOTE: Although this example focuses on DHCP errors, you can see that this SLE provides insights into various factors that can affect connectivity, including authorization, ARP, and DNS issues. For more information about this SLE and its classifiers, see "Wireless Successful Connects SLE" on page 67.

As shown in the following animation, you can click the DHCP classifier to view the Root Cause Analysis. There, you can explore the sub-classifiers, statistics, and timeline. You can see which devices were affected, when they were affected, and where they're located.



As you explore the Root Cause Analysis page, you can discover:

- If the failures are being observed across access points (APs) or specific APs.
- If the failures are being observed for specific device types or across all device types.
- If the failures are being observed across all Wireless Lans (WLANs) or a specific WLAN.

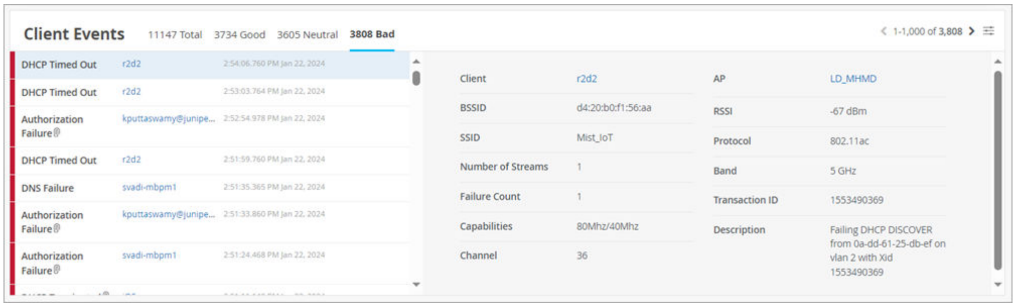
Explore Further on the Insights Dashboard

As you identify the impacted devices, you can get more details on the Insights dashboard. This dashboard offers information about current and past issues.

NOTE: To find the Insights dashboard, select **Monitor** from the left menu of the Juniper Mist portal. Then click the **Insights** button at the top of the Monitor page.

For connectivity issues, it's helpful to look at **AP Events** and **Client Events**.

For this example, let's look at **Client Events**. If you click the **Bad** tab at the top, you can focus on the user-impacting issues. In this example, you see the details that are available for a DCHP timeout. For more information about an incident, you can click the link on the client name or the AP name.



Client Events 11147 Total 3734 Good 3605 Neutral 3808 Bad

1-1,000 of 3,808

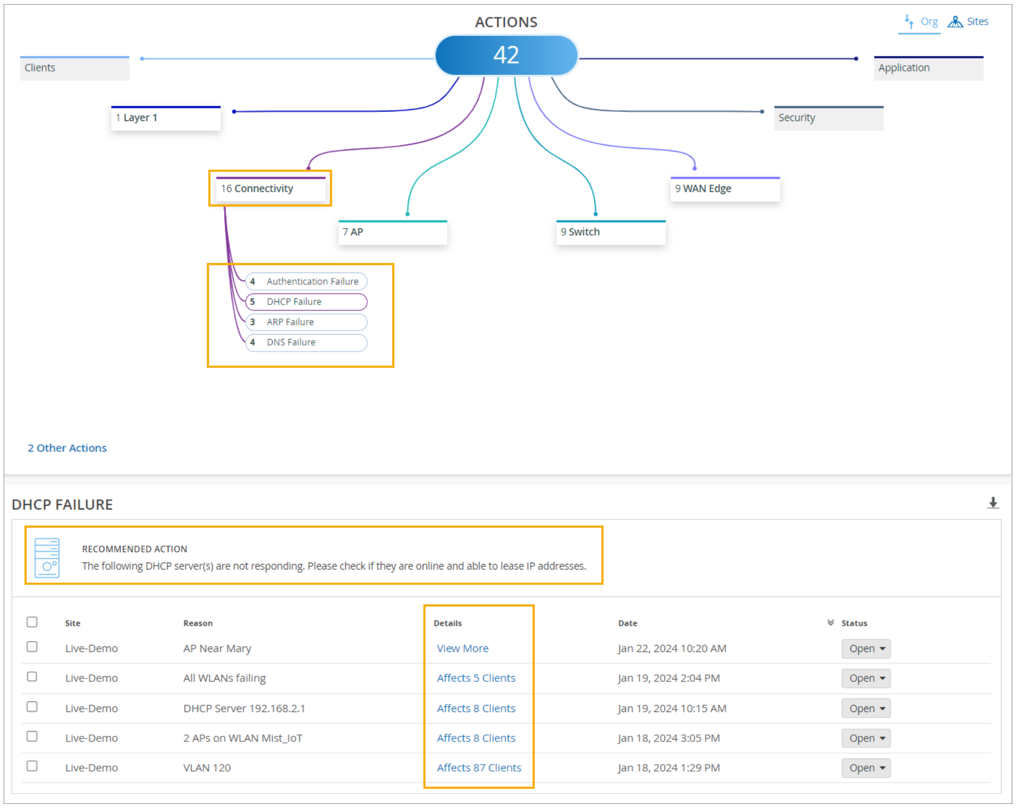
DHCP Timed Out	r2d2	2:54:06.760 PM Jan 22, 2024
DHCP Timed Out	r2d2	2:53:03.764 PM Jan 22, 2024
Authorization Failure	kputtaswamy@junipe...	2:52:54.978 PM Jan 22, 2024
DHCP Timed Out	r2d2	2:51:59.760 PM Jan 22, 2024
DNS Failure	svadi-mbpm1	2:51:35.365 PM Jan 22, 2024
Authorization Failure	kputtaswamy@junipe...	2:51:33.860 PM Jan 22, 2024
Authorization Failure	svadi-mbpm1	2:51:24.468 PM Jan 22, 2024

Client	r2d2	AP	LD_MHMD
BSSID	d4:20:b0:f1:56:aa	RSSI	-67 dBm
SSID	Mist_IoT	Protocol	802.11ac
Number of Streams	1	Band	5 GHz
Failure Count	1	Transaction ID	1553490369
Capabilities	80Mhz/40Mhz	Description	Failing DHCP DISCOVER from 0a-dd-61-25-db-ef on vlan 2 with Xid 1553490369
Channel	36		

Get Quick Recommendations About Ongoing Issues

The Marvis Actions dashboard offers quick recommendations about current and past issues.

In this example, the Actions dashboard shows several connectivity issues. In this example, DCHP Failure has the highest number of issues. When you click DHCP, you see a recommended action. You also see the scope of the issue: which sites were affected, what happened, and when the issues occurred.



DHCP FAILURE

RECOMMENDED ACTION

The following DHCP server(s) are not responding. Please check if they are online and able to lease IP addresses.

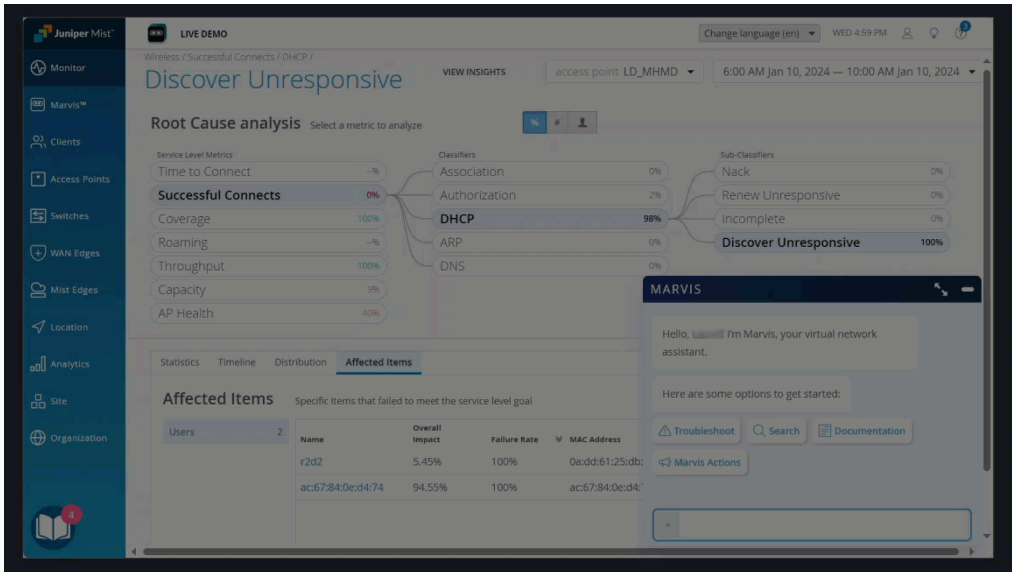
□	Site	Reason	Details	Date	Status
□	Live-Demo	AP Near Mary	View More	Jan 22, 2024 10:20 AM	Open
□	Live-Demo	All WLANs failing	Affects 5 Clients	Jan 19, 2024 2:04 PM	Open
□	Live-Demo	DHCP Server 192.168.2.1	Affects 8 Clients	Jan 19, 2024 10:15 AM	Open
□	Live-Demo	2 APs on WLAN Mist_IoT	Affects 8 Clients	Jan 18, 2024 3:05 PM	Open
□	Live-Demo	VLAN 120	Affects 87 Clients	Jan 18, 2024 1:29 PM	Open

Troubleshoot with Marvis

If you have a Marvis subscription, you get help by clicking the Marvis icon and entering questions.

NOTE: Look for the Marvis icon at the top-left or bottom-right corner of the Juniper Mist portal.

As shown in the animation below, you can enter *troubleshoot* followed by the MAC address or hostname of a device. Then interact with Marvis to get the information that you need.



Name	Overall Impact	Failure Rate	MAC Address
r2d2	5.45%	100%	0a:dd:61:25:db:
ac:67:84:0e:d4:74	94.55%	100%	ac:67:84:0e:d4:

Hello, [redacted] I'm Marvis, your virtual network assistant.

Here are some options to get started:

Troubleshoot Specific Connectivity Issues by Using the Marvis Conversational Assistant

SUMMARY

Understand how you can use the Marvis conversational assistant to troubleshoot specific connectivity issues.

IN THIS SECTION

We cover a few troubleshooting examples so that you get an idea about how you can use the Marvis conversational assistant to troubleshoot connectivity issues.

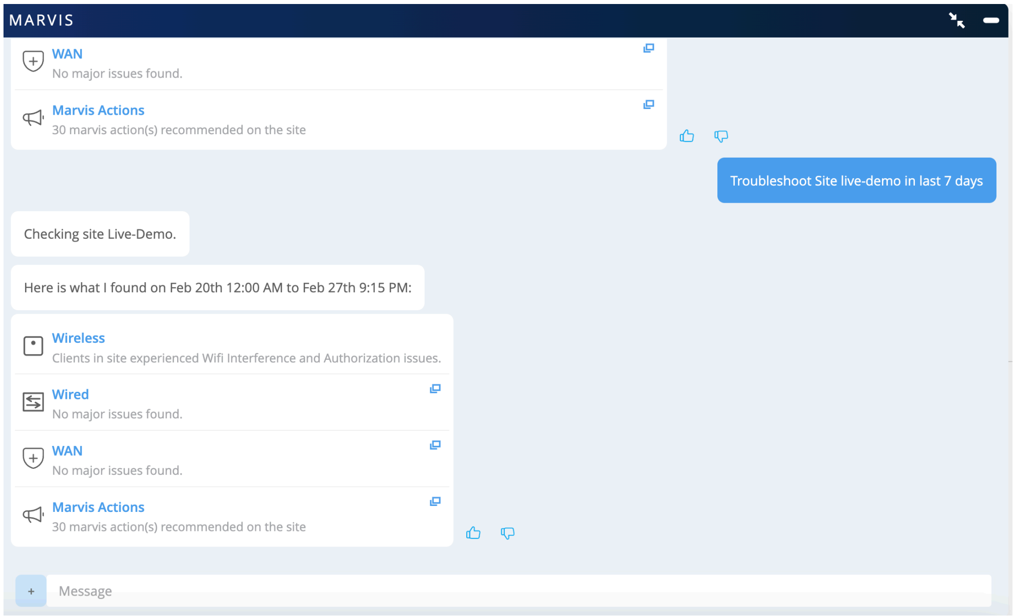
Troubleshoot Authorization Failures

Authorization failures can be due to various reasons such as a RADIUS server not responding and clients failing to complete the authorization process. This example shows how you can use the Marvis conversational assistant to troubleshoot authorization failures both for a site and a client.

To troubleshoot authorization failures at a site:

1. In the Marvis conversational assistant window, enter **troubleshoot** followed by the site name. You can also specify a duration.

   In this example, you'll see that Marvis identifies authorization issues in the wireless network.



WAN
No major issues found.

Marvis Actions
30 marvis action(s) recommended on the site

Troubleshoot Site live-demo in last 7 days

Checking site Live-Demo.

Here is what I found on Feb 20th 12:00 AM to Feb 27th 9:15 PM:

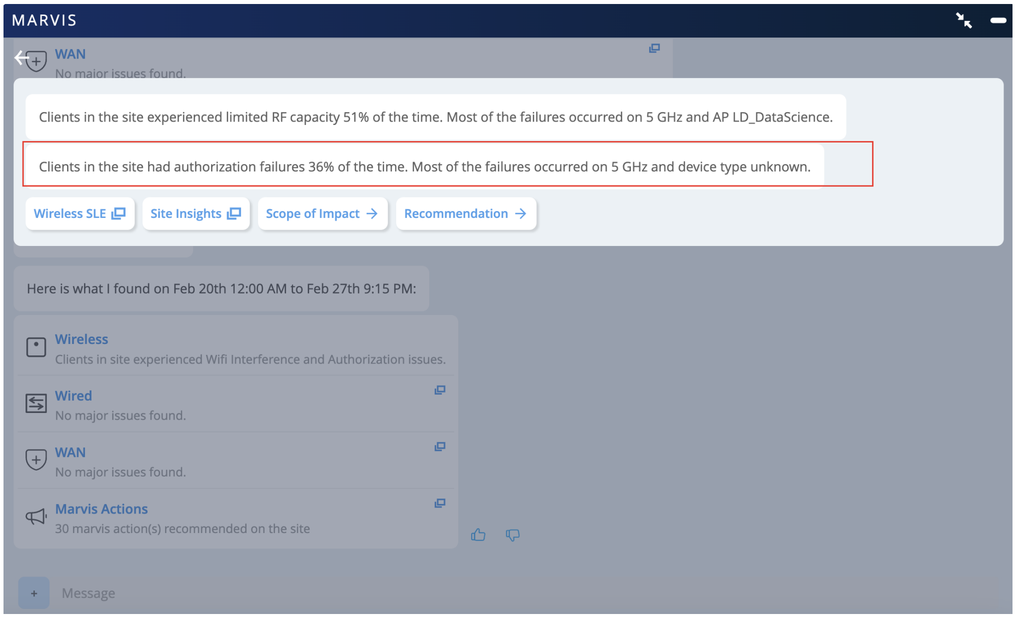
Wireless
Clients in site experienced Wifi Interference and Authorization issues.

Wired
No major issues found.

WAN
No major issues found.

Marvis Actions
30 marvis action(s) recommended on the site

2. Click the **Wireless** category to get some more details about the issue. In this example, you'll see that Marvis reports that the clients at the site faced authorization failures 36% of the time.



WAN
No major issues found.

Clients in the site experienced limited RF capacity 51% of the time. Most of the failures occurred on 5 GHz and AP LD_DataScience.

Clients in the site had authorization failures 36% of the time. Most of the failures occurred on 5 GHz and device type unknown.

Here is what I found on Feb 20th 12:00 AM to Feb 27th 9:15 PM:

Wireless
Clients in site experienced Wifi Interference and Authorization issues.

Wired
No major issues found.

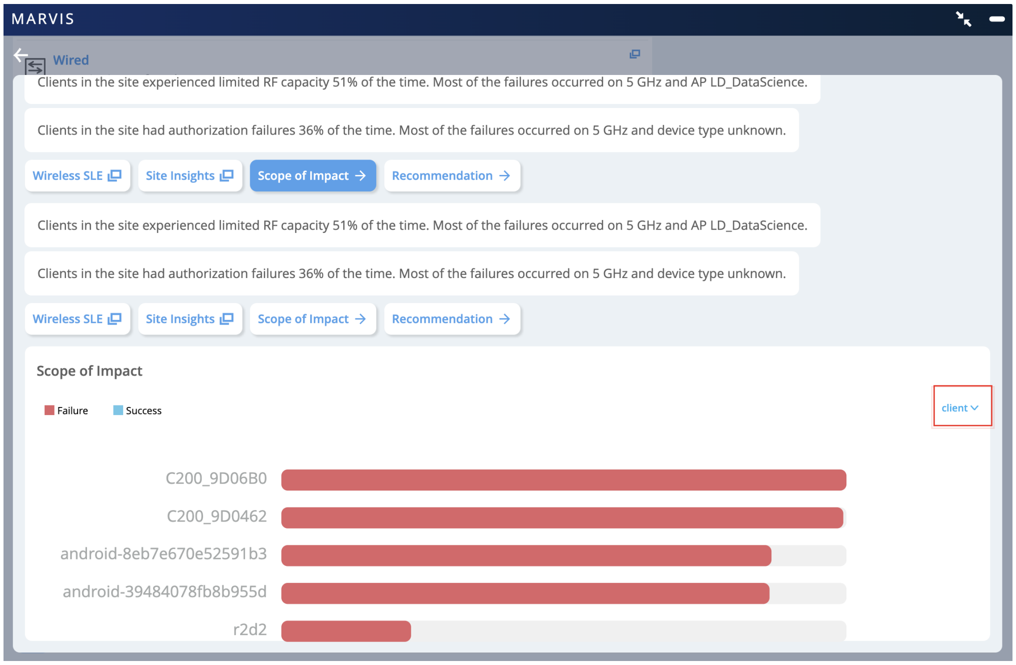
WAN
No major issues found.

Marvis Actions
30 marvis action(s) recommended on the site

You can investigate further by using the options displayed.

Scope of Impact

Scope of Impact provides a graphical representation of all the clients that experienced issues. You can also choose to view the information based on a wireless LAN (WLAN), access point (AP), or radio band by using the drop-down list on the right.



Clients in the site experienced limited RF capacity 51% of the time. Most of the failures occurred on 5 GHz and AP LD_DataScience.

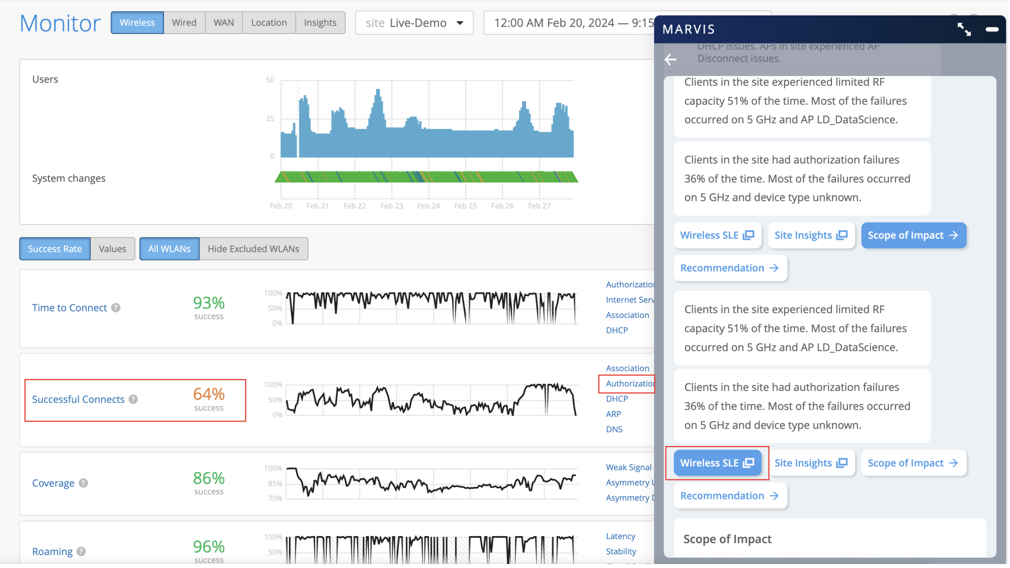
Clients in the site had authorization failures 36% of the time. Most of the failures occurred on 5 GHz and device type unknown.

Clients in the site experienced limited RF capacity 51% of the time. Most of the failures occurred on 5 GHz and AP LD_DataScience.

Clients in the site had authorization failures 36% of the time. Most of the failures occurred on 5 GHz and device type unknown.

Wireless SLE

The Wireless SLEs dashboard provides site-level insights and SLE classifiers. In this example, you'll see that the Successful Connect service-level expectation (SLE) shows that 64 percent of the connects were successful.



DHCP issues. APs in site experienced AP Disconnect issues.

Clients in the site experienced limited RF capacity 51% of the time. Most of the failures occurred on 5 GHz and AP LD_DataScience.

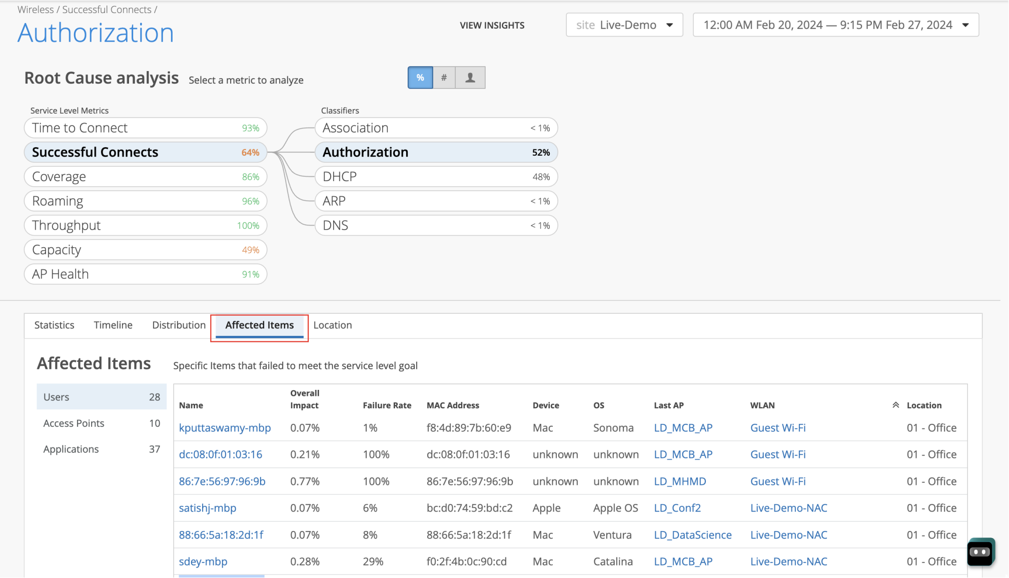
Clients in the site had authorization failures 36% of the time. Most of the failures occurred on 5 GHz and device type unknown.

Clients in the site experienced limited RF capacity 51% of the time. Most of the failures occurred on 5 GHz and AP LD_DataScience.

Clients in the site had authorization failures 36% of the time. Most of the failures occurred on 5 GHz and device type unknown.

Click the **Authorization** classifier on the right to view the Root Cause Analysis page. This page provides detailed information. You can look through each of the tabs on the page. For example, you can use the Distribution tab to determine if the issue is being observed across:

- All APs or specific APs
- All users or specific users
- All WLANs or specific WLANs
- All device types or specific device types



Wireless / Successful Connects /

Authorization

VIEW INSIGHTS site Live-Demo 12:00 AM Feb 20, 2024 — 9:15 PM Feb 27, 2024

Root Cause analysis Select a metric to analyze

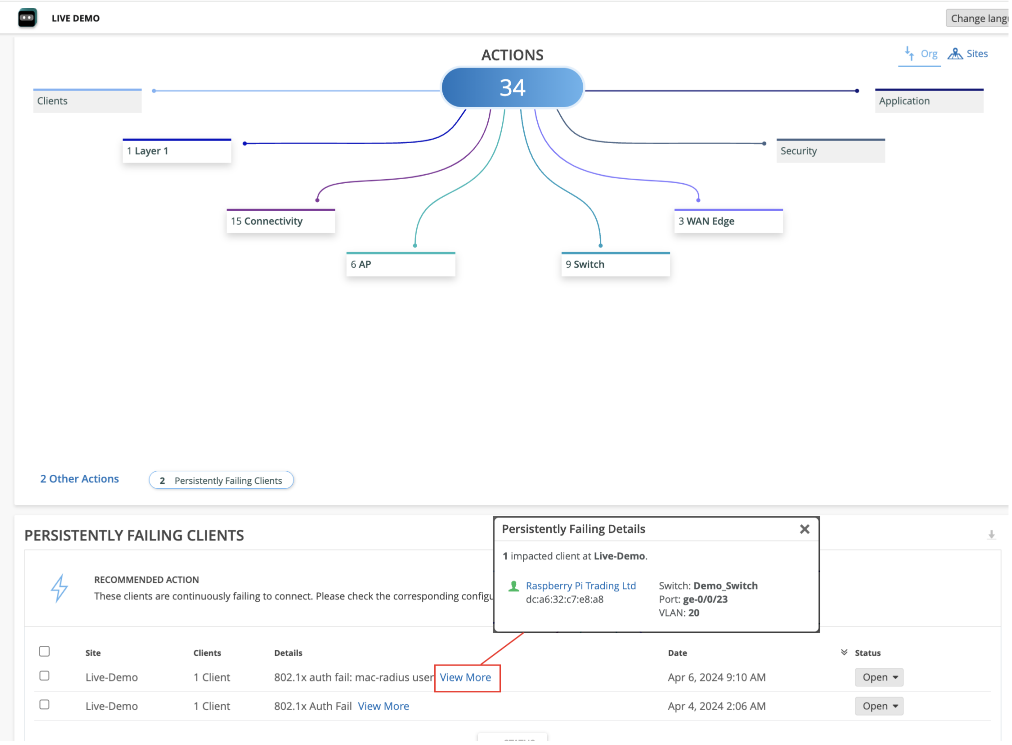
Service Level Metrics		Classifiers	
Time to Connect	93%	Association	< 1%
Successful Connects	64%	Authorization	52%
Coverage	86%	DHCP	48%
Roaming	96%	ARP	< 1%
Throughput	100%	DNS	< 1%
Capacity	49%		
AP Health	91%		

Affected Items Specific Items that failed to meet the service level goal

Users	28
Access Points	10
Applications	37

Name	Overall Impact	Failure Rate	MAC Address	Device	OS	Last AP	WLAN	Location
kputtaswamy-mbp	0.07%	1%	f8:4d:89:7b:60:e9	Mac	Sonoma	LD_MCB_AP	Guest Wi-Fi	01 - Office
dc:08:0f:01:03:16	0.21%	100%	dc:08:0f:01:03:16	unknown	unknown	LD_MCB_AP	Guest Wi-Fi	01 - Office
86:7e:56:97:96:9b	0.77%	100%	86:7e:56:97:96:9b	unknown	unknown	LD_MHMD	Guest Wi-Fi	01 - Office
satishj-mbp	0.07%	6%	bc:d0:74:59:bd:c2	Apple	Apple OS	LD_Conf2	Live-Demo-NAC	01 - Office
88:66:5a:18:2d:1f	0.07%	8%	88:66:5a:18:2d:1f	Mac	Ventura	LD_DataScience	Live-Demo-NAC	01 - Office
sdey-mbp	0.28%	29%	f0:2f:4b:0c:90:cd	Mac	Catalina	LD_MCB_AP	Live-Demo-NAC	01 - Office

The **Affected Items** tab displays the impacted users, APs, and applications. You can drill down further by clicking a user. The **Failure Rate** column indicates whether the user always fails to connect. Users experiencing a 100-percent failure rate over a long period of time are listed under the Persistently Failing Clients category in Marvis Actions as shown in the following example:



2 Other Actions 2 Persistently Failing Clients

PERSISTENTLY FAILING CLIENTS

RECOMMENDED ACTION

These clients are continuously failing to connect. Please check the corresponding configu

Persistently Failing Details

1 impacted client at **Live-Demo**.

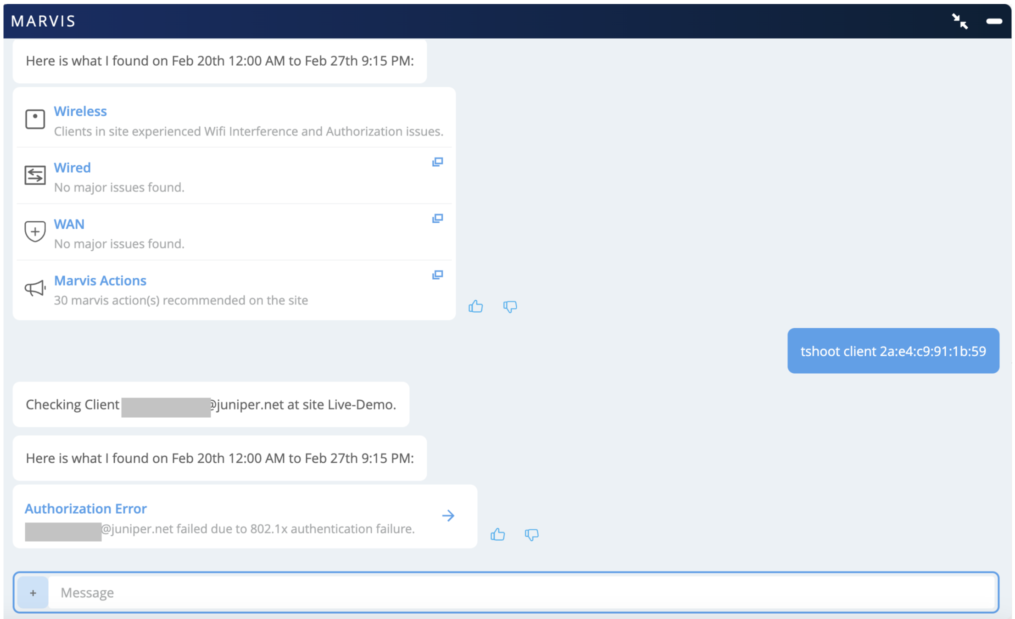
Raspberry Pi Trading Ltd
dc:a6:32:c7:e8:a8

Switch: **Demo_Switch**
Port: **ge-0/0/23**
VLAN: **20**

☐	Site	Clients	Details	Date	Status
☐	Live-Demo	1 Client	802.1x auth fail: mac-radius user View More	Apr 6, 2024 9:10 AM	Open
☐	Live-Demo	1 Client	802.1x Auth Fail View More	Apr 4, 2024 2:06 AM	Open

To troubleshoot authorization failures for a client:

1. In the Marvis conversational assistant window, enter **tshoot client** followed by the MAC address or hostname of the client. In the following example, you'll see that Marvis detects an authorization error for the client.



Here is what I found on Feb 20th 12:00 AM to Feb 27th 9:15 PM:

Wireless
Clients in site experienced Wifi Interference and Authorization issues.

Wired
No major issues found.

WAN
No major issues found.

Marvis Actions
30 marvis action(s) recommended on the site

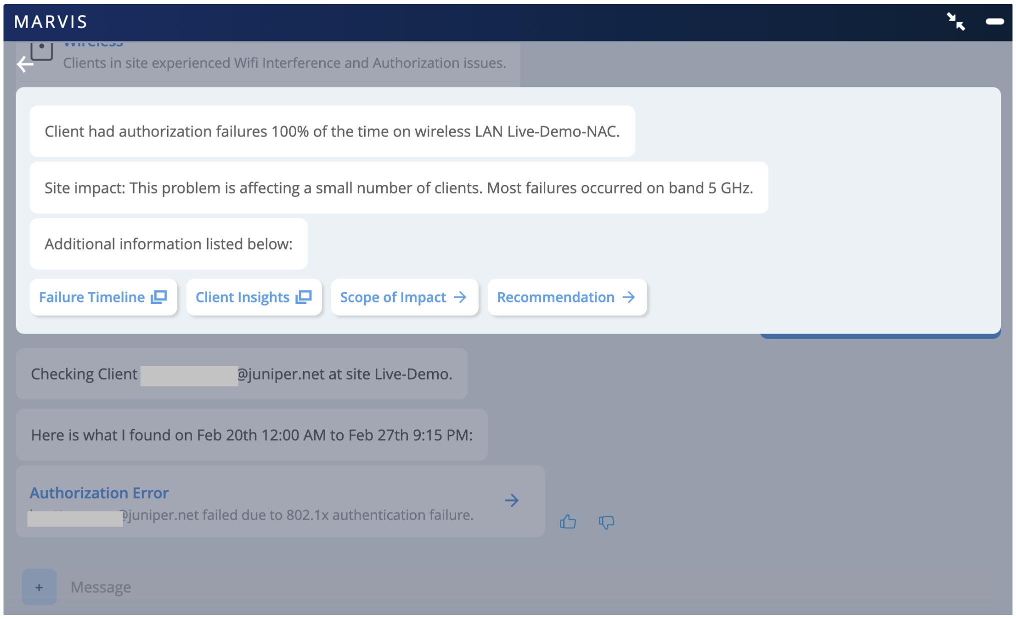
tshoot client 2a:e4:c9:91:1b:59

Checking Client [redacted]@juniper.net at site Live-Demo.

Here is what I found on Feb 20th 12:00 AM to Feb 27th 9:15 PM:

Authorization Error
[redacted]@juniper.net failed due to 802.1x authentication failure.

2. Click **Authorization Error** to view more details. In this example, you'll see that Marvis reports that the client faced authorization failures 100 percent of the time.



Clients in site experienced Wifi Interference and Authorization issues.

Client had authorization failures 100% of the time on wireless LAN Live-Demo-NAC.

Site impact: This problem is affecting a small number of clients. Most failures occurred on band 5 GHz.

Additional information listed below:

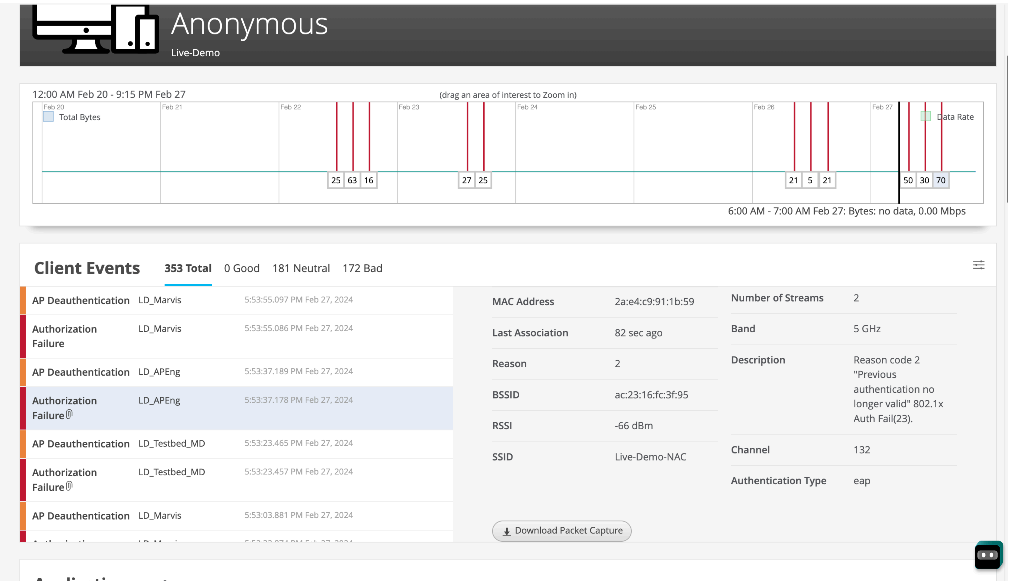
Checking Client [redacted]@juniper.net at site Live-Demo.

Here is what I found on Feb 20th 12:00 AM to Feb 27th 9:15 PM:

Authorization Error
[redacted]@juniper.net failed due to 802.1x authentication failure.

Note that Marvis also reports this issue on the Marvis Actions page, under the Connectivity category.

As we are looking into a client-specific issue, you can click **Client Insights**. The Client Events section lists all the events associated with the clients. You can click the authorization failure event to see the reason for the failure.


Anonymous
Live-Demo
12:00 AM Feb 20 - 9:15 PM Feb 27
(drag an area of interest to Zoom in)
Feb 20
Feb 21
Feb 22
Feb 23
Feb 24
Feb 25
Feb 26
Feb 27
Total Bytes
Data Rate
25
63
16
27
25
21
5
21
50
30
70
6:00 AM - 7:00 AM Feb 27: Bytes: no data, 0.00 Mbps

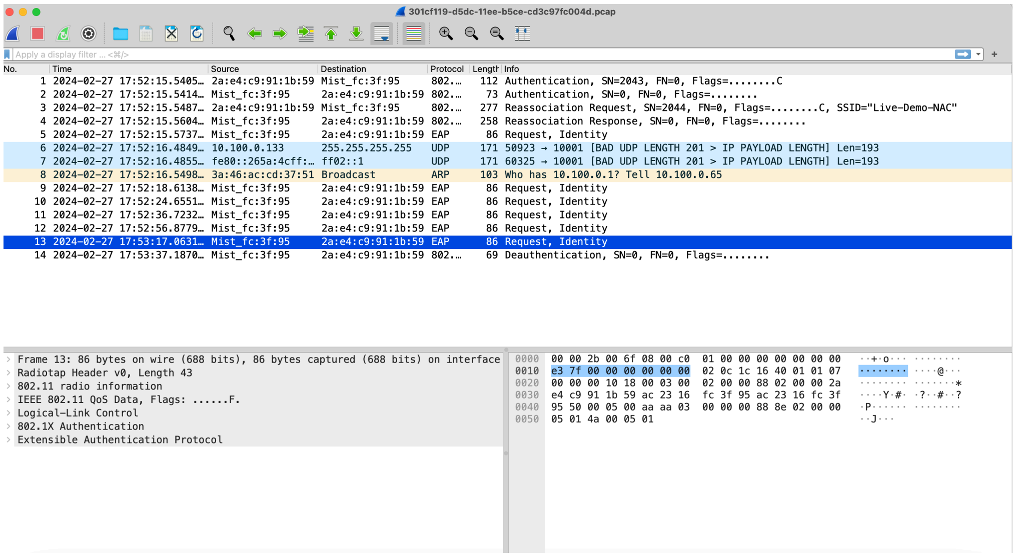
Client Events 353 Total 0 Good 181 Neutral 172 Bad

AP Deauthentication	LD_Marvis	5:53:55.097 PM Feb 27, 2024
Authorization Failure	LD_Marvis	5:53:55.086 PM Feb 27, 2024
AP Deauthentication	LD_APEng	5:53:37.189 PM Feb 27, 2024
Authorization Failure	LD_APEng	5:53:37.178 PM Feb 27, 2024
AP Deauthentication	LD_Testbed_MD	5:53:23.465 PM Feb 27, 2024
Authorization Failure	LD_Testbed_MD	5:53:23.457 PM Feb 27, 2024
AP Deauthentication	LD_Marvis	5:53:03.881 PM Feb 27, 2024

MAC Address	2a:e4:c9:91:1b:59	Number of Streams	2
Last Association	82 sec ago	Band	5 GHz
Reason	2	Description	Reason code 2 "Previous authentication no longer valid" 802.1x Auth Fail(23).
BSSID	ac:23:16:fc:3f:95		
RSSI	-66 dBm	Channel	132
SSID	Live-Demo-NAC	Authentication Type	eap

Download Packet Capture

You can also download the packet capture for the authorization failure. Here is a sample packet capture. You can see that the client does not respond to identity requests and repeatedly tries to connect without providing a client identity response.


301cf119-d5dc-11ee-b5ce-cd3c97fc004d.pcap
Apply a display filter … <⌘/>

```
No.  Time                    Source             Destination        Protocol Length Info
   1 2024-02-27 17:52:15.5405… 2a:e4:c9:91:1b:59 Mist_fc:3f:95     802.…   112 Authentication, SN=2043, FN=0, Flags=........C
   2 2024-02-27 17:52:15.5414… Mist_fc:3f:95     2a:e4:c9:91:1b:59 802.…    73 Authentication, SN=0, FN=0, Flags=........
   3 2024-02-27 17:52:15.5487… 2a:e4:c9:91:1b:59 Mist_fc:3f:95     802.…   277 Reassociation Request, SN=2044, FN=0, Flags=........C, SSID="Live-Demo-NAC"
   4 2024-02-27 17:52:15.5604… Mist_fc:3f:95     2a:e4:c9:91:1b:59 802.…   258 Reassociation Response, SN=0, FN=0, Flags=........
   5 2024-02-27 17:52:15.5737… Mist_fc:3f:95     2a:e4:c9:91:1b:59 EAP      86 Request, Identity
   6 2024-02-27 17:52:16.4849… 10.100.0.133      255.255.255.255   UDP     171 50923 → 10001 [BAD UDP LENGTH 201 > IP PAYLOAD LENGTH] Len=193
   7 2024-02-27 17:52:16.4855… fe80::265a:4cff:… ff02::1           UDP     171 60325 → 10001 [BAD UDP LENGTH 201 > IP PAYLOAD LENGTH] Len=193
   8 2024-02-27 17:52:16.5498… 3a:46:ac:cd:37:51 Broadcast         ARP     103 Who has 10.100.0.1? Tell 10.100.0.65
   9 2024-02-27 17:52:18.6138… Mist_fc:3f:95     2a:e4:c9:91:1b:59 EAP      86 Request, Identity
  10 2024-02-27 17:52:24.6551… Mist_fc:3f:95     2a:e4:c9:91:1b:59 EAP      86 Request, Identity
  11 2024-02-27 17:52:36.7232… Mist_fc:3f:95     2a:e4:c9:91:1b:59 EAP      86 Request, Identity
  12 2024-02-27 17:52:56.8779… Mist_fc:3f:95     2a:e4:c9:91:1b:59 EAP      86 Request, Identity
  13 2024-02-27 17:53:17.0631… Mist_fc:3f:95     2a:e4:c9:91:1b:59 EAP      86 Request, Identity
  14 2024-02-27 17:53:37.1870… Mist_fc:3f:95     2a:e4:c9:91:1b:59 802.…    69 Deauthentication, SN=0, FN=0, Flags=........
```

```
> Frame 13: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface
> Radiotap Header v0, Length 43
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: ......F.
> Logical-Link Control
> 802.1X Authentication
> Extensible Authentication Protocol
```

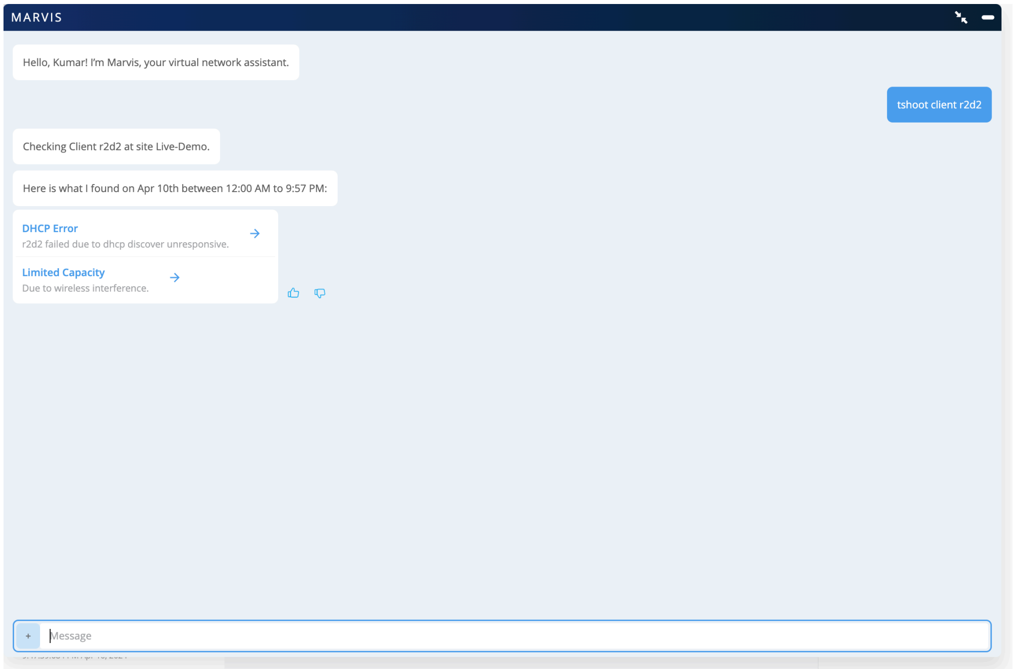
```
0000  00 00 2b 00 6f 08 00 c0  01 00 00 00 00 00 00 00   ··+·o···  ········
0010  e3 7f 00 00 00 00 00 00  02 0c 1c 16 40 01 01 07   ········  ····@···
0020  00 00 00 10 18 00 03 00  02 00 00 88 02 00 00 2a   ········  ·······*
0030  e4 c9 91 1b 59 ac 23 16  fc 3f 95 ac 23 16 fc 3f   ····Y·#·  ·?··#··?
0040  95 50 00 05 00 aa aa 03  00 00 00 88 8e 02 00 00   ·P······  ········
0050  05 01 4a 00 05 01                                  ··J···
```

Troubleshoot DHCP Issues

Clients might face connectivity issues when they fail to obtain an IP address due to a lack of response from the Dynamic Host Configuration Protocol (DHCP) server.

To troubleshoot DHCP issues:

1. In the Marvis conversational assistant window, enter **tshoot client** followed by the MAC address or hostname of the client. In the following example, you'll see that Marvis detects DHCP issues in the network.



Hello, Kumar! I'm Marvis, your virtual network assistant.

tshoot client r2d2

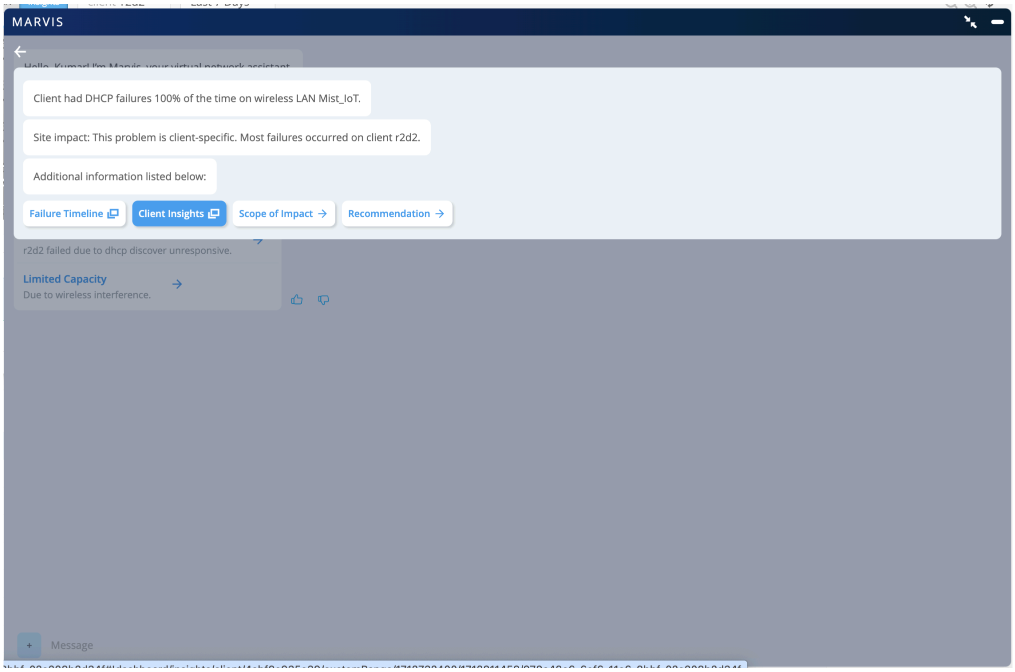
Checking Client r2d2 at site Live-Demo.

Here is what I found on Apr 10th between 12:00 AM to 9:57 PM:

DHCP Error
r2d2 failed due to dhcp discover unresponsive.

Limited Capacity
Due to wireless interference.

2. Click **DHCP Error** to view the details. In the following example, you'll see that Marvis reports that a specific client is facing DHCP failures 100 percent of the time.



Client had DHCP failures 100% of the time on wireless LAN Mist_IoT.

Site impact: This problem is client-specific. Most failures occurred on client r2d2.

Additional information listed below:

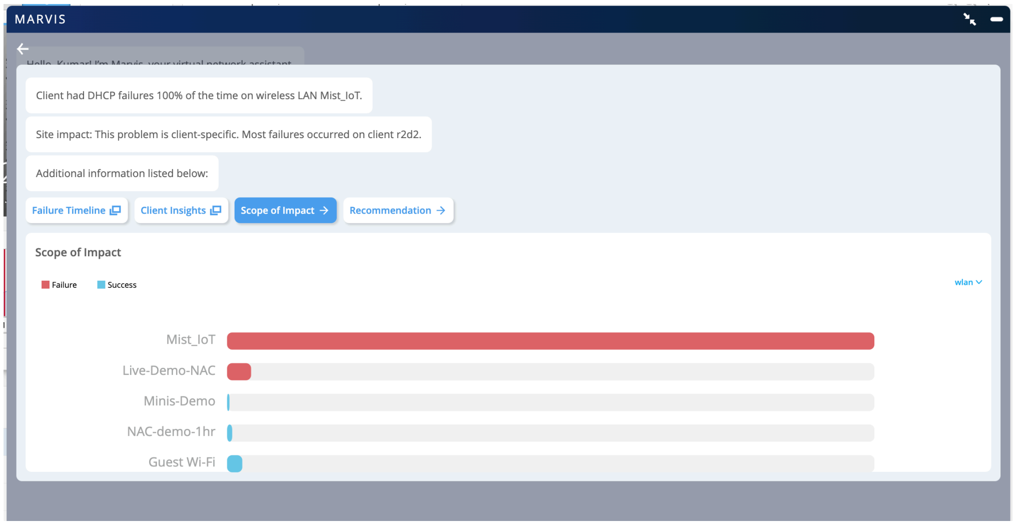
r2d2 failed due to dhcp discover unresponsive.

Limited Capacity
Due to wireless interference.

You can investigate further by using the options displayed.

Scope of Impact

You can start by looking at the Scope of Impact that lists the successful and failed connection attempts. You can use the drop-down list on the right to check whether the client is failing on one WLAN/AP or multiple WLANs/APs.



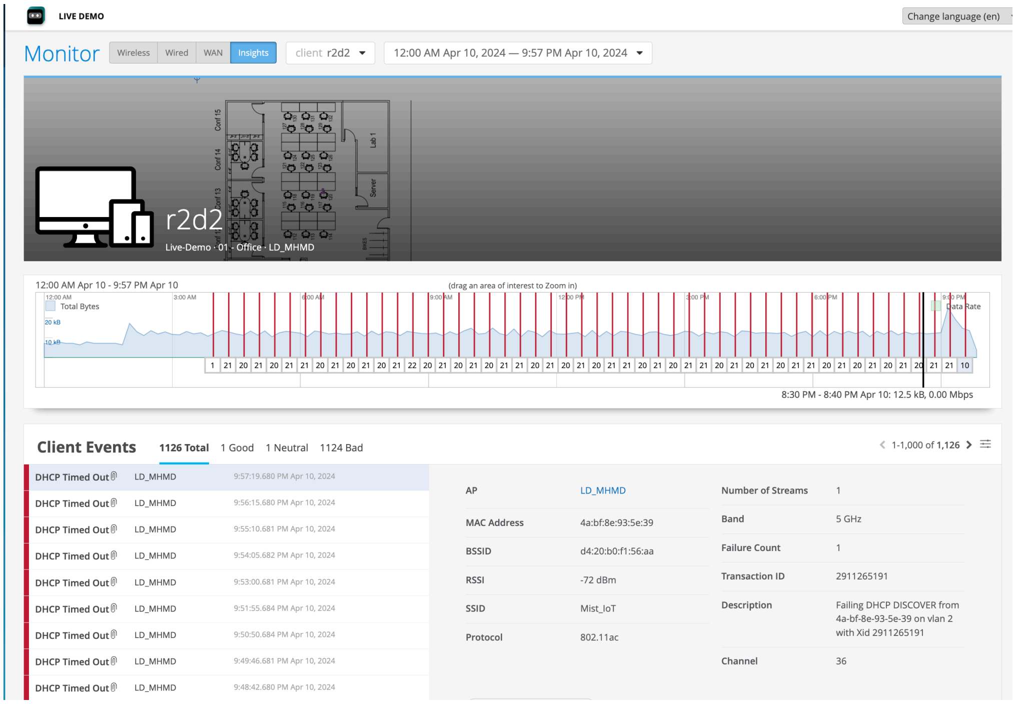
Client had DHCP failures 100% of the time on wireless LAN Mist_IoT.

Site impact: This problem is client-specific. Most failures occurred on client r2d2.

Additional information listed below:

Client Insights

You can also click **Client Insights** to view all the client-related events. You can click the DHCP Timed Out event to view the details of the DHCP server where the DHCP requests are failing.

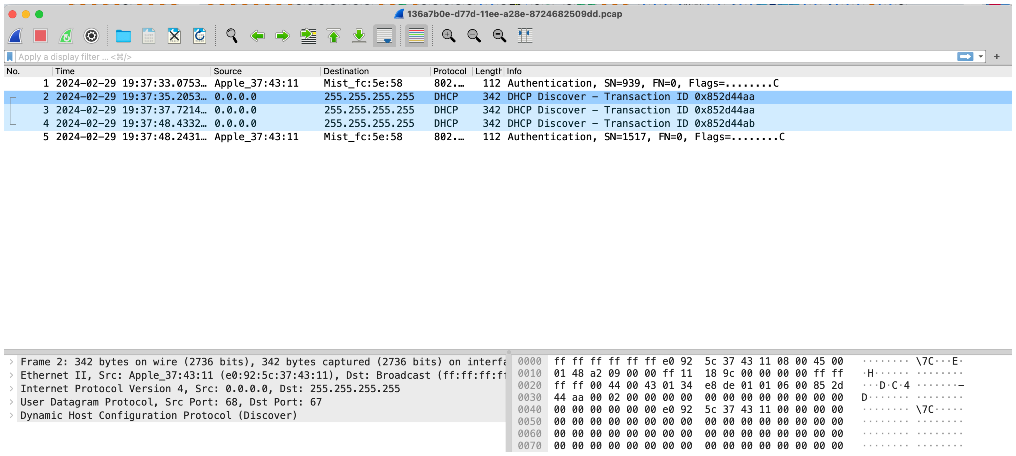

LIVE DEMO
Change language (en)
Monitor
Wireless
Wired
WAN
Insights
client r2d2
12:00 AM Apr 10, 2024 — 9:57 PM Apr 10, 2024
r2d2
Live-Demo · 01 · Office · LD_MHMD
12:00 AM Apr 10 - 9:57 PM Apr 10
(drag an area of interest to Zoom in)
Total Bytes
Data Rate
20 kB
10 kB
8:30 PM - 8:40 PM Apr 10: 12.5 kB, 0.00 Mbps

Client Events 1126 Total 1 Good 1 Neutral 1124 Bad — 1-1,000 of 1,126

DHCP Timed Out	LD_MHMD	9:57:19.680 PM Apr 10, 2024
DHCP Timed Out	LD_MHMD	9:56:15.680 PM Apr 10, 2024
DHCP Timed Out	LD_MHMD	9:55:10.681 PM Apr 10, 2024
DHCP Timed Out	LD_MHMD	9:54:05.682 PM Apr 10, 2024
DHCP Timed Out	LD_MHMD	9:53:00.681 PM Apr 10, 2024
DHCP Timed Out	LD_MHMD	9:51:55.684 PM Apr 10, 2024
DHCP Timed Out	LD_MHMD	9:50:50.684 PM Apr 10, 2024
DHCP Timed Out	LD_MHMD	9:49:46.681 PM Apr 10, 2024
DHCP Timed Out	LD_MHMD	9:48:42.680 PM Apr 10, 2024

AP	LD_MHMD	Number of Streams	1
MAC Address	4a:bf:8e:93:5e:39	Band	5 GHz
BSSID	d4:20:b0:f1:56:aa	Failure Count	1
RSSI	-72 dBm	Transaction ID	2911265191
SSID	Mist_IoT	Description	Failing DHCP DISCOVER from 4a-bf-8e-93-5e-39 on vlan 2 with Xid 2911265191
Protocol	802.11ac	Channel	36

You can download the dynamic packet capture for a specific event. Here's a sample packet capture for a client that experienced a DHCP Timed Out event.


136a7b0e-d77d-11ee-a28e-8724682509dd.pcap
Apply a display filter ... <⌘/>

```
No.  Time                      Source          Destination      Protocol Length Info
   1 2024-02-29 19:37:33.0753… Apple_37:43:11  Mist_fc:5e:58    802.…    112 Authentication, SN=939, FN=0, Flags=........C
   2 2024-02-29 19:37:35.2053… 0.0.0.0         255.255.255.255  DHCP     342 DHCP Discover - Transaction ID 0x852d44aa
   3 2024-02-29 19:37:37.7214… 0.0.0.0         255.255.255.255  DHCP     342 DHCP Discover - Transaction ID 0x852d44aa
   4 2024-02-29 19:37:48.4332… 0.0.0.0         255.255.255.255  DHCP     342 DHCP Discover - Transaction ID 0x852d44ab
   5 2024-02-29 19:37:48.2431… Apple_37:43:11  Mist_fc:5e:58    802.…    112 Authentication, SN=1517, FN=0, Flags=........C
```

```
> Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interfa
> Ethernet II, Src: Apple_37:43:11 (e0:92:5c:37:43:11), Dst: Broadcast (ff:ff:ff:ff
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

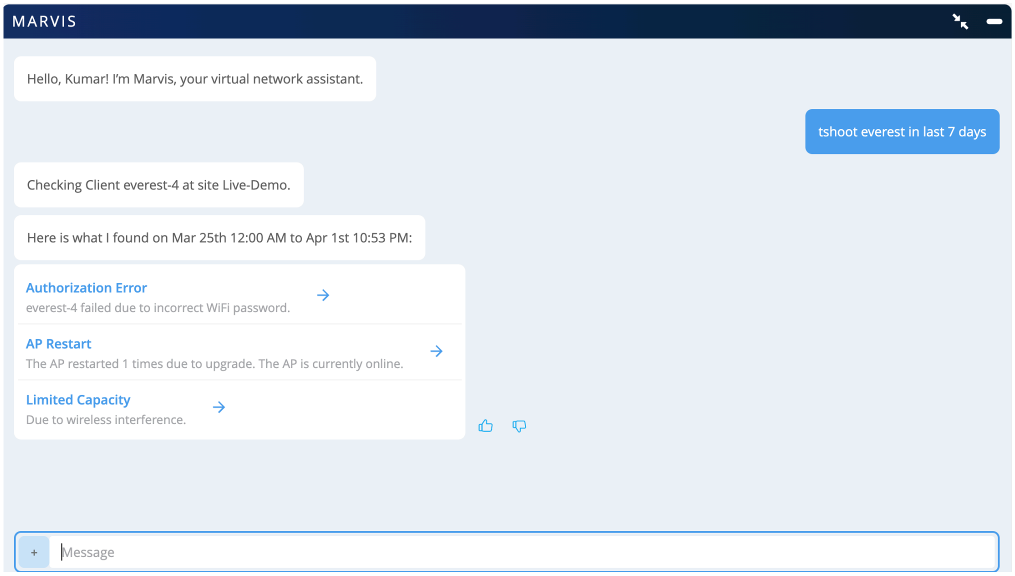
```
0000  ff ff ff ff ff ff e0 92  5c 37 43 11 08 00 45 00   ········ \7C···E·
0010  01 48 a2 09 00 00 ff 11  18 9c 00 00 00 00 ff ff   ·H······ ········
0020  ff ff 00 44 00 43 01 34  e8 de 01 01 06 00 85 2d   ···D·C·4 ·······-
0030  44 aa 00 02 00 00 00 00  00 00 00 00 00 00 00 00   D······· ········
0040  00 00 00 00 00 00 e0 92  5c 37 43 11 00 00 00 00   ········ \7C····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

Troubleshoot PSK Failures

Marvis detects preshared key (PSK) failures when a large number of clients fail to authenticate to a PSK WLAN. A probable cause for this issue could be a recent PSK change that was not communicated to users.

To troubleshoot PSK failures:

1. In the Marvis conversational assistant window, enter **tshoot** followed by the MAC address or hostname of the client. In the following example, you'll see that Marvis reports an authorization issue due to an incorrect wireless password.



Hello, Kumar! I'm Marvis, your virtual network assistant.

tshoot everest in last 7 days

Checking Client everest-4 at site Live-Demo.

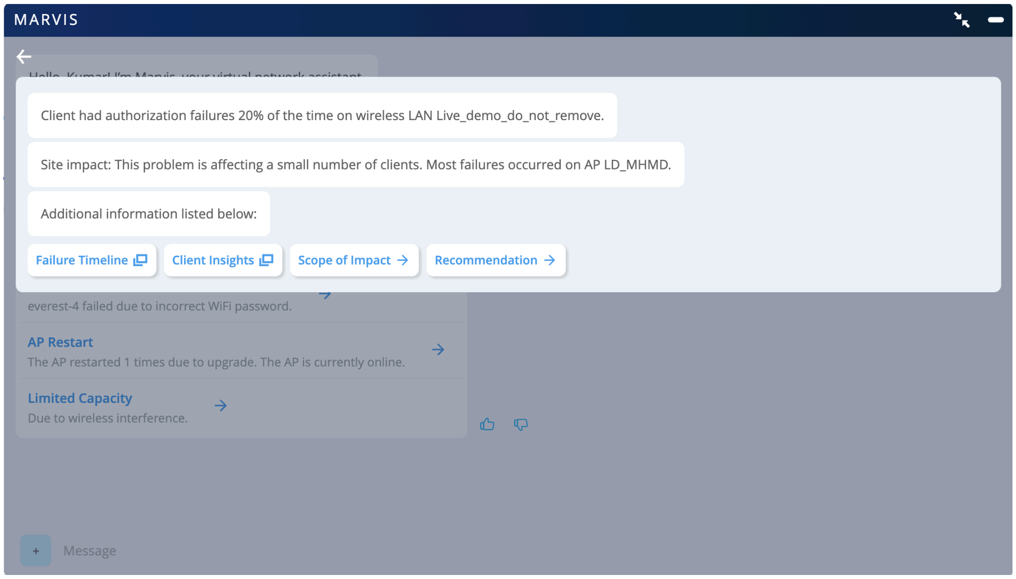
Here is what I found on Mar 25th 12:00 AM to Apr 1st 10:53 PM:

Authorization Error
everest-4 failed due to incorrect WiFi password.

AP Restart
The AP restarted 1 times due to upgrade. The AP is currently online.

Limited Capacity
Due to wireless interference.

2. Click **Authorization Errors** to view the details.



Client had authorization failures 20% of the time on wireless LAN Live_demo_do_not_remove.

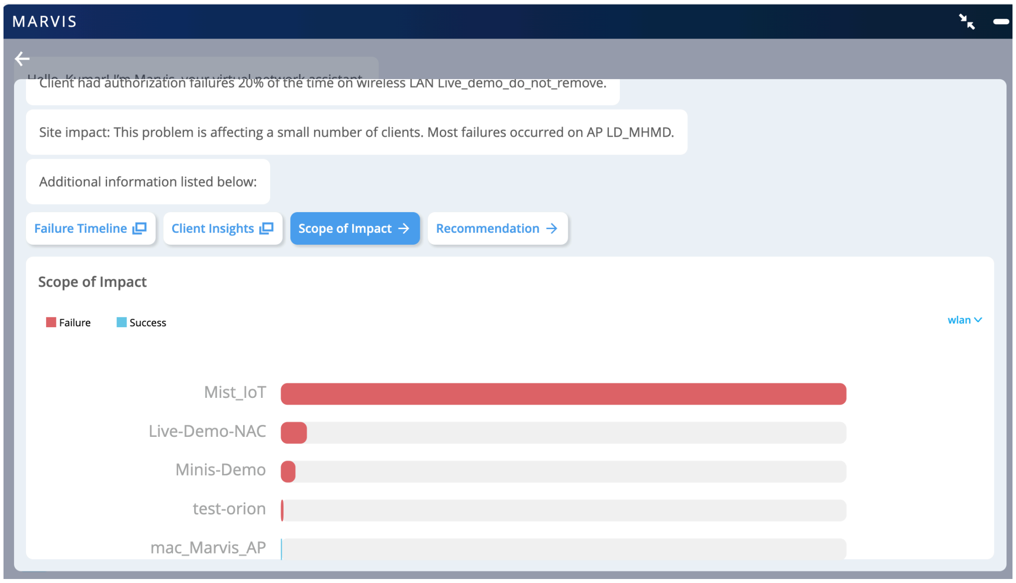
Site impact: This problem is affecting a small number of clients. Most failures occurred on AP LD_MHMD.

Additional information listed below:

Investigate further by using the options displayed.

Scope of Impact

You can start by looking at the Scope of Impact that lists the successful and failed connection attempts. You can check whether the client is failing on one or multiple WLANs.



MARVIS

Client had authorization failures 20% of the time on wireless LAN Live_demo_do_not_remove.

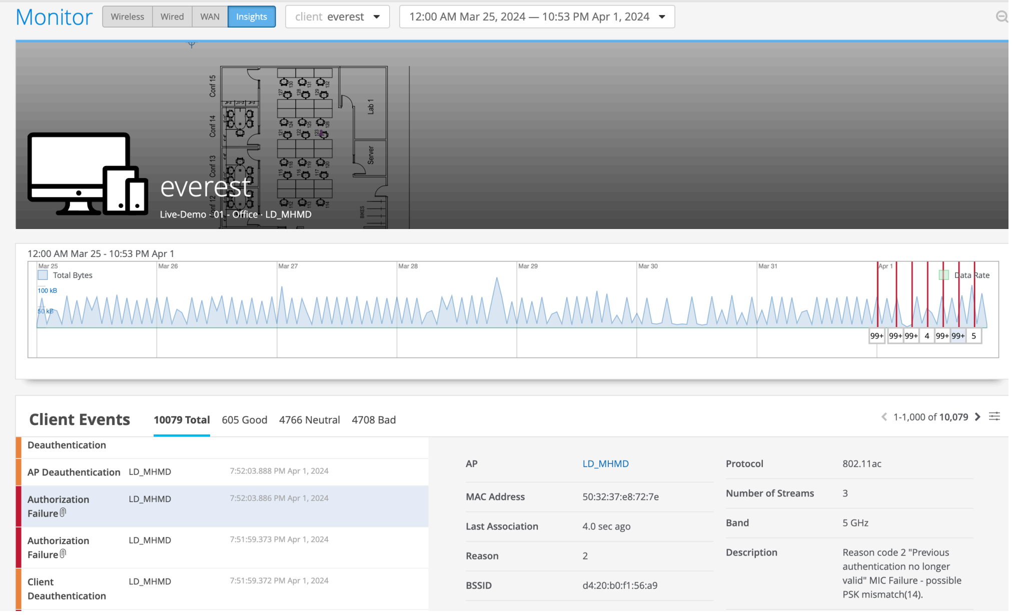
Site impact: This problem is affecting a small number of clients. Most failures occurred on AP LD_MHMD.

Additional information listed below:

Scope of Impact

Client Insights

You can click **Client Insights** to view all the events associated with the client. You can click the authorization failure event to see the reason for the failure as shown in the following example.



Client Events 10079 Total 605 Good 4766 Neutral 4708 Bad

1-1,000 of **10,079**

Deauthentication		
AP Deauthentication	LD_MHMD	7:52:03.888 PM Apr 1, 2024
Authorization Failure	LD_MHMD	7:52:03.886 PM Apr 1, 2024
Authorization Failure	LD_MHMD	7:51:59.373 PM Apr 1, 2024
Client Deauthentication	LD_MHMD	7:51:59.372 PM Apr 1, 2024

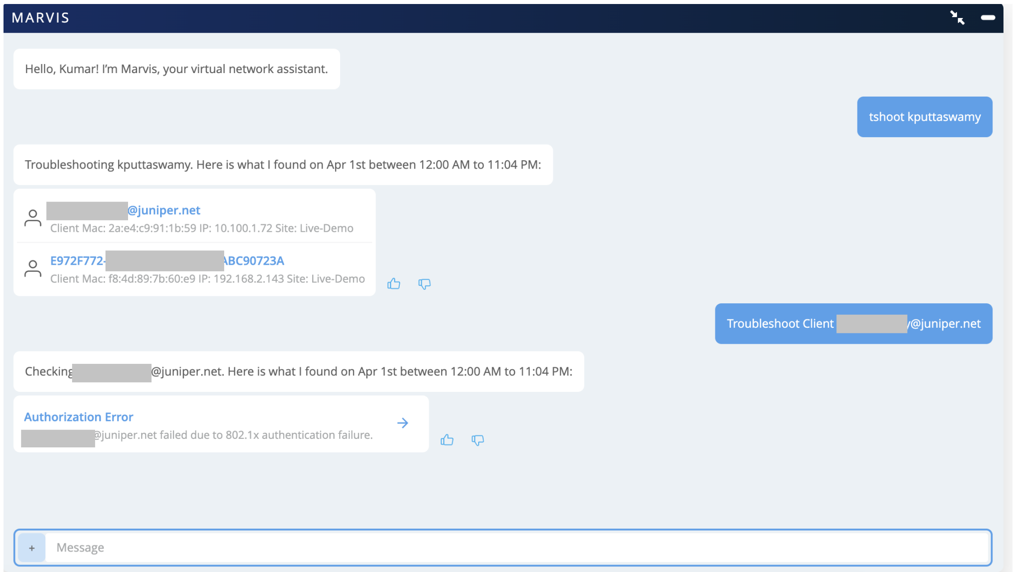
AP	LD_MHMD	Protocol	802.11ac
MAC Address	50:32:37:e8:72:7e	Number of Streams	3
Last Association	4.0 sec ago	Band	5 GHz
Reason	2	Description	Reason code 2 "Previous authentication no longer valid" MIC Failure - possible PSK mismatch(14).
BSSID	d4:20:b0:f1:56:a9		

Troubleshoot RADIUS Authentication Failures

Clients might experience an 802.1x authentication failure when a RADIUS server is down or unreachable.

To troubleshoot RADIUS authentication failures:

1. In the Marvis conversational assistant window, enter **tshoot** followed by the name of the client. In the following example, you'll see that Marvis detects 802.1x authentication failures in the network.



Hello, Kumar! I'm Marvis, your virtual network assistant.

tshoot kputtaswamy

Troubleshooting kputtaswamy. Here is what I found on Apr 1st between 12:00 AM to 11:04 PM:

[redacted]@juniper.net
Client Mac: 2a:e4:c9:91:1b:59 IP: 10.100.1.72 Site: Live-Demo

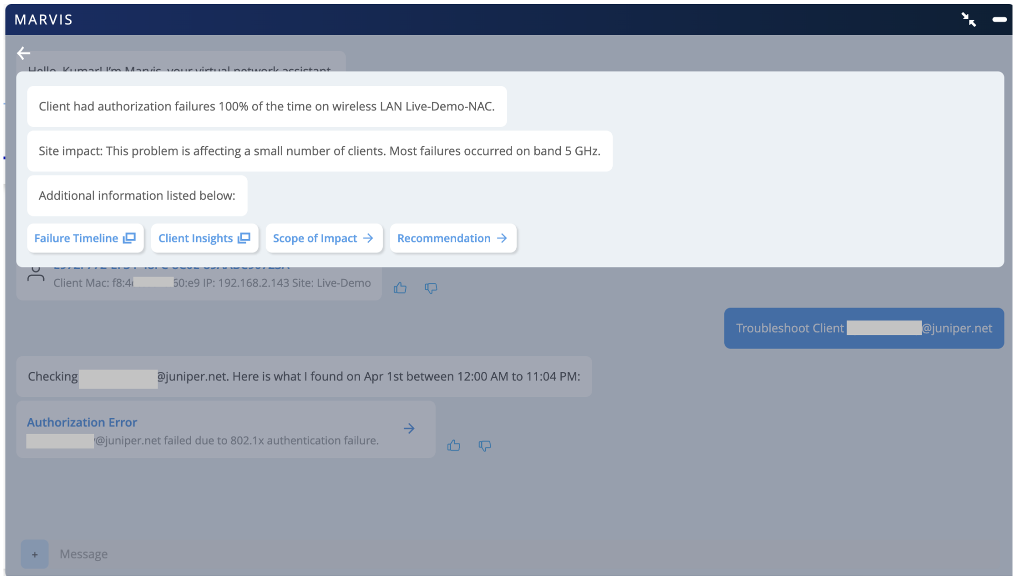
E972F772-[redacted]ABC90723A
Client Mac: f8:4d:89:7b:60:e9 IP: 192.168.2.143 Site: Live-Demo

Troubleshoot Client [redacted]@juniper.net

Checking [redacted]@juniper.net. Here is what I found on Apr 1st between 12:00 AM to 11:04 PM:

Authorization Error
[redacted]@juniper.net failed due to 802.1x authentication failure.

2. Click **Authentication Error** to view the details.



Hello, Kumar! I'm Marvis, your virtual network assistant

Client had authorization failures 100% of the time on wireless LAN Live-Demo-NAC.

Site impact: This problem is affecting a small number of clients. Most failures occurred on band 5 GHz.

Additional information listed below:

Client Mac: f8:4[redacted]60:e9 IP: 192.168.2.143 Site: Live-Demo

Troubleshoot Client [redacted]@juniper.net

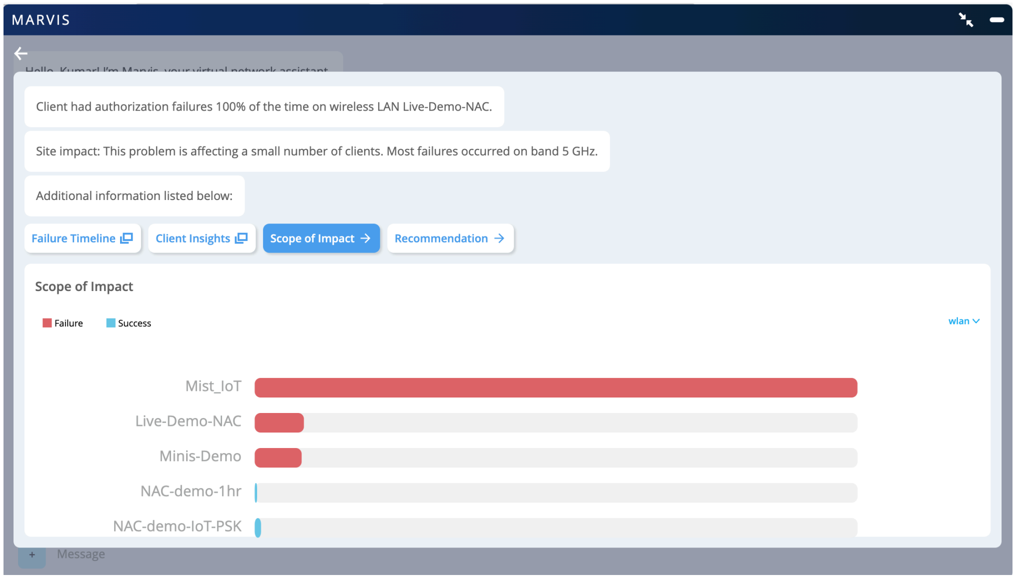
Checking [redacted]@juniper.net. Here is what I found on Apr 1st between 12:00 AM to 11:04 PM:

Authorization Error
[redacted]@juniper.net failed due to 802.1x authentication failure.

You can investigate further by using the options displayed.

Scope of Impact

You can start by looking at the Scope of Impact that lists the successful and failed connection attempts. You can check whether the client is failing on one or multiple WLANs.



Client had authorization failures 100% of the time on wireless LAN Live-Demo-NAC.

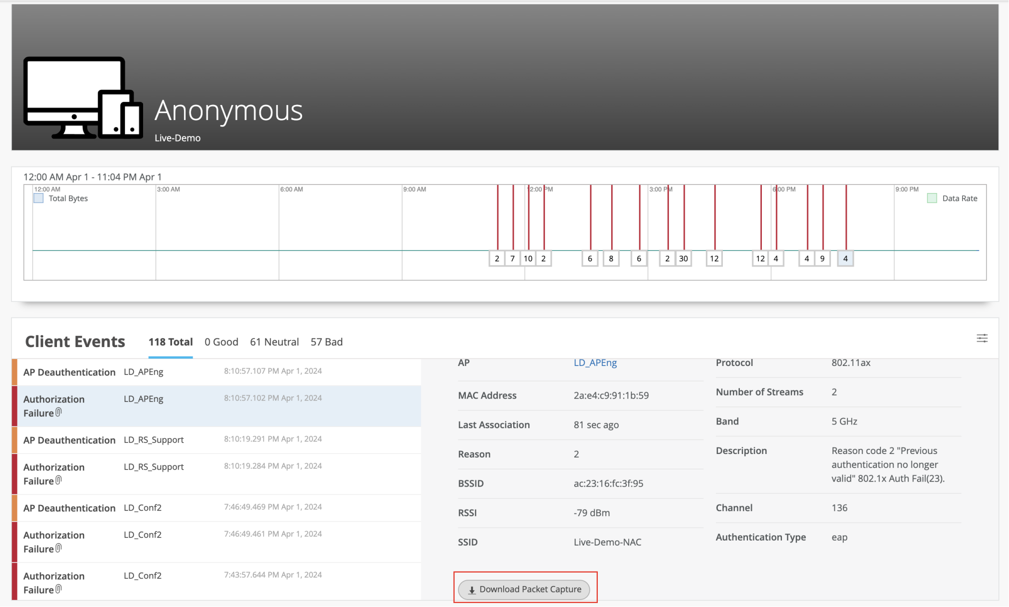
Site impact: This problem is affecting a small number of clients. Most failures occurred on band 5 GHz.

Additional information listed below:

Scope of Impact

Client Insights

You can click **Client Insights** to view all the events associated with the client. You can click the authorization failure event to see the reason for the failure as shown in the following example.

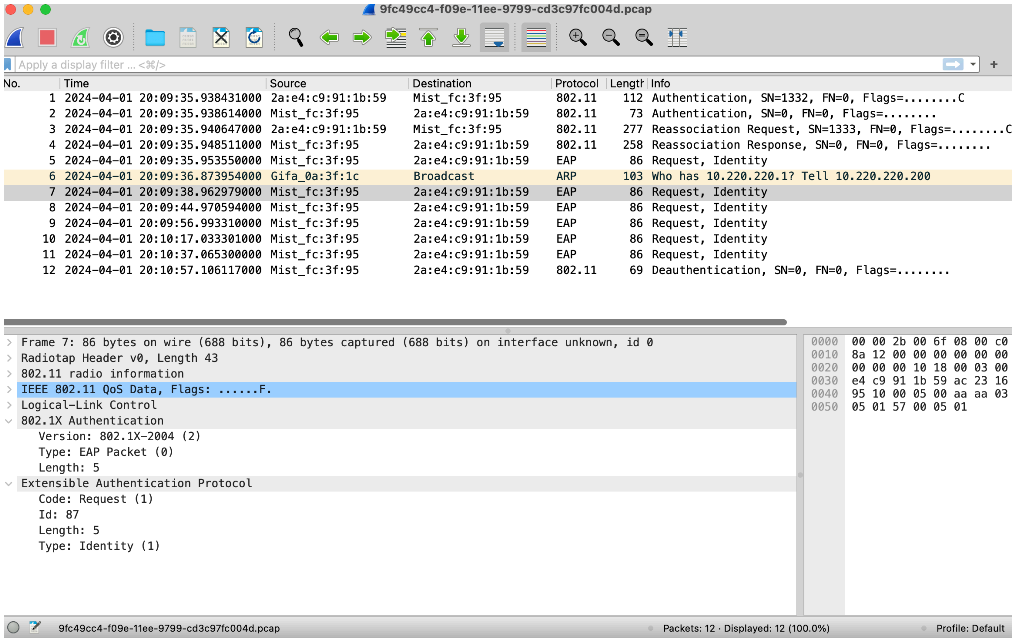


Client Events 118 Total 0 Good 61 Neutral 57 Bad

AP Deauthentication	LD_APEng	8:10:57.107 PM Apr 1, 2024
Authorization Failure	LD_APEng	8:10:57.102 PM Apr 1, 2024
AP Deauthentication	LD_RS_Support	8:10:19.291 PM Apr 1, 2024
Authorization Failure	LD_RS_Support	8:10:19.284 PM Apr 1, 2024
AP Deauthentication	LD_Conf2	7:46:49.469 PM Apr 1, 2024
Authorization Failure	LD_Conf2	7:46:49.461 PM Apr 1, 2024
Authorization Failure	LD_Conf2	7:43:57.644 PM Apr 1, 2024

AP	LD_APEng	Protocol	802.11ax
MAC Address	2a:e4:c9:91:1b:59	Number of Streams	2
Last Association	81 sec ago	Band	5 GHz
Reason	2	Description	Reason code 2 "Previous authentication no longer valid" 802.1x Auth Fail(23).
BSSID	ac:23:16:fc:3f:95	Channel	136
RSSI	-79 dBm	Authentication Type	eap
SSID	Live-Demo-NAC		

You can download the dynamic packet capture for a specific event. Here's a sample packet capture:


9fc49cc4-f09e-11ee-9799-cd3c97fc004d.pcap
Apply a display filter ... <⌘/>
9fc49cc4-f09e-11ee-9799-cd3c97fc004d.pcap
Packets: 12 · Displayed: 12 (100.0%)
Profile: Default

```
No.   Time                          Source             Destination        Protocol  Length Info
    1 2024-04-01 20:09:35.938431000 2a:e4:c9:91:1b:59  Mist_fc:3f:95      802.11    112 Authentication, SN=1332, FN=0, Flags=........C
    2 2024-04-01 20:09:35.938614000 Mist_fc:3f:95      2a:e4:c9:91:1b:59  802.11     73 Authentication, SN=0, FN=0, Flags=........
    3 2024-04-01 20:09:35.940647000 2a:e4:c9:91:1b:59  Mist_fc:3f:95      802.11    277 Reassociation Request, SN=1333, FN=0, Flags=........C
    4 2024-04-01 20:09:35.948511000 Mist_fc:3f:95      2a:e4:c9:91:1b:59  802.11    258 Reassociation Response, SN=0, FN=0, Flags=........
    5 2024-04-01 20:09:35.953550000 Mist_fc:3f:95      2a:e4:c9:91:1b:59  EAP        86 Request, Identity
    6 2024-04-01 20:09:36.873954000 Gifa_0a:3f:1c      Broadcast          ARP       103 Who has 10.220.220.1? Tell 10.220.220.200
    7 2024-04-01 20:09:38.962979000 Mist_fc:3f:95      2a:e4:c9:91:1b:59  EAP        86 Request, Identity
    8 2024-04-01 20:09:44.970594000 Mist_fc:3f:95      2a:e4:c9:91:1b:59  EAP        86 Request, Identity
    9 2024-04-01 20:09:56.993310000 Mist_fc:3f:95      2a:e4:c9:91:1b:59  EAP        86 Request, Identity
   10 2024-04-01 20:10:17.033301000 Mist_fc:3f:95      2a:e4:c9:91:1b:59  EAP        86 Request, Identity
   11 2024-04-01 20:10:37.065300000 Mist_fc:3f:95      2a:e4:c9:91:1b:59  EAP        86 Request, Identity
   12 2024-04-01 20:10:57.106117000 Mist_fc:3f:95      2a:e4:c9:91:1b:59  802.11     69 Deauthentication, SN=0, FN=0, Flags=........
```

```
> Frame 7: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface unknown, id 0
> Radiotap Header v0, Length 43
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: ......F.
> Logical-Link Control
v 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: EAP Packet (0)
    Length: 5
v Extensible Authentication Protocol
    Code: Request (1)
    Id: 87
    Length: 5
    Type: Identity (1)
```

```
0000  00 00 2b 00 6f 08 00 c0
0010  8a 12 00 00 00 00 00 00
0020  00 00 00 10 18 00 03 00
0030  e4 c9 91 1b 59 ac 23 16
0040  95 10 00 05 00 aa aa 03
0050  05 01 57 00 05 01
```

Troubleshoot a Device or Site by Using APIs

You can use the troubleshoot API to troubleshoot devices and sites from an external portal. Devices that you can troubleshoot include clients (wired and wireless), access points (APs), switches, and WAN Edges. You can also use the APIs to troubleshoot sites for wired, wireless, and WAN issues.

To use the Marvis APIs, you must have:

- A valid observer API token.
- Marvis subscription at the organization level.
- MAC address of the device (if you want to troubleshoot a device)
- Site ID or site name (if you want to troubleshoot a site)

Here are the details of the API queries:

- To troubleshoot a device:

  ```
  GET /api/v1/orgs/:org_id/troubleshoot?mac=:device_mac
  ```

  If you know the hostname or username of the device, use the search API (`/clients/search` or `/devices/search`) to get the MAC address.

You can also include the `site_id` option if you want the troubleshoot response to be fetched for a device in a specific site. Include the `start` and `end` options if you want the troubleshoot response for a specific duration.

- To troubleshoot a site:

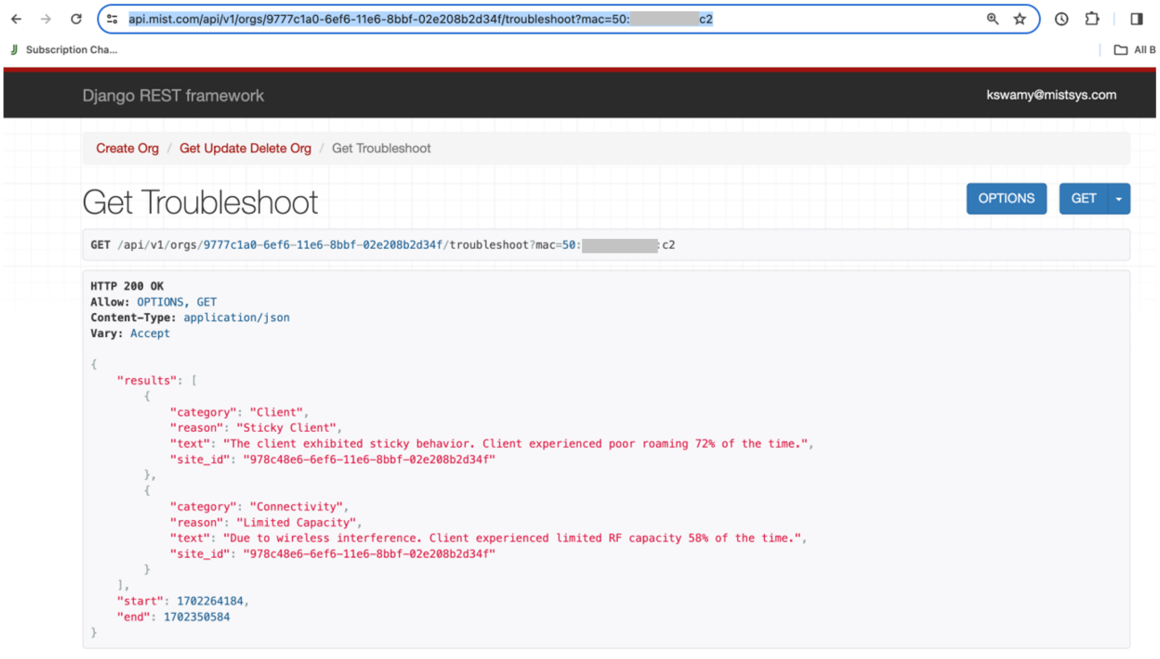
  ```
  GET /api/v1/orgs/:org_id/troubleshoot?site_id=:siteid
  ```

  You can also include the `type` option if you want the troubleshoot response to be fetched for a specific network issue—wired, WAN, or wireless. Note that the default type is wireless. If you have only a WAN or wired deployment, then ensure that you specify the type. Include the `start` and `end` options if you want the troubleshoot response for a specific duration.

The API query fetches a text-based response containing the problem category, reason, description, and recommendation (if applicable). Here are some sample results:

- Troubleshoot a device (wireless client)

  https://api.mist.com/api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?mac=50:xx:xx:xx:xx:c2



api.mist.com/api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?mac=50:[redacted]c2
Subscription Cha...
All B
Django REST framework
kswamy@mistsys.com
Create Org / Get Update Delete Org / Get Troubleshoot
OPTIONS
GET

Get Troubleshoot

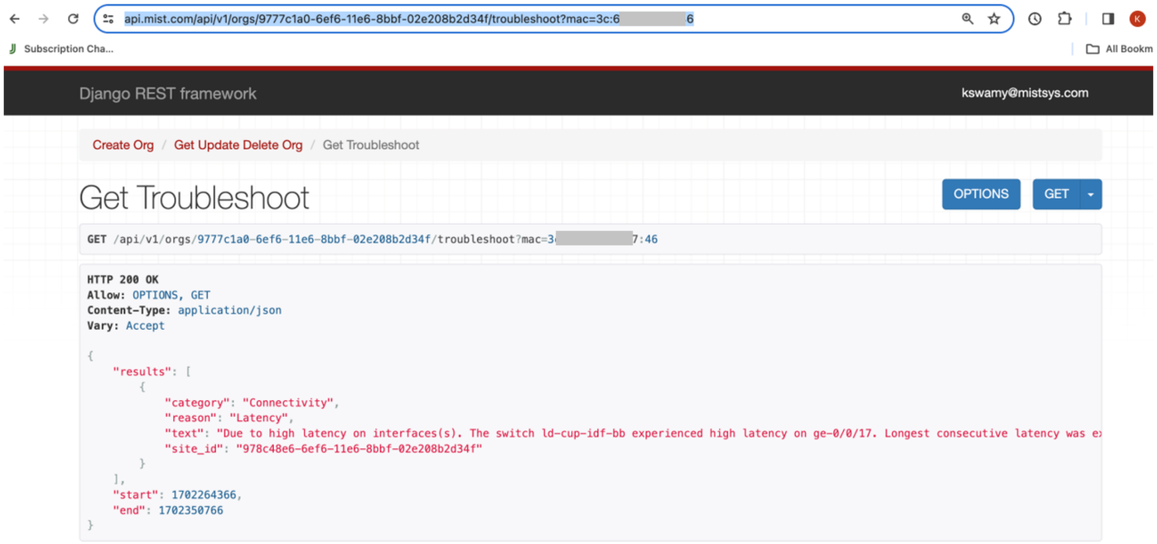
```
GET /api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?mac=50:[redacted]:c2
```

```
HTTP 200 OK
Allow: OPTIONS, GET
Content-Type: application/json
Vary: Accept

{
    "results": [
        {
            "category": "Client",
            "reason": "Sticky Client",
            "text": "The client exhibited sticky behavior. Client experienced poor roaming 72% of the time.",
            "site_id": "978c48e6-6ef6-11e6-8bbf-02e208b2d34f"
        },
        {
            "category": "Connectivity",
            "reason": "Limited Capacity",
            "text": "Due to wireless interference. Client experienced limited RF capacity 58% of the time.",
            "site_id": "978c48e6-6ef6-11e6-8bbf-02e208b2d34f"
        }
    ],
    "start": 1702264184,
    "end": 1702350584
}
```

- Troubleshoot a device (wired client)

  https://api.mist.com/api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?mac=3c:xx:xx:xx:xx:46



```
api.mist.com/api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?mac=3c:6[redacted]6
```

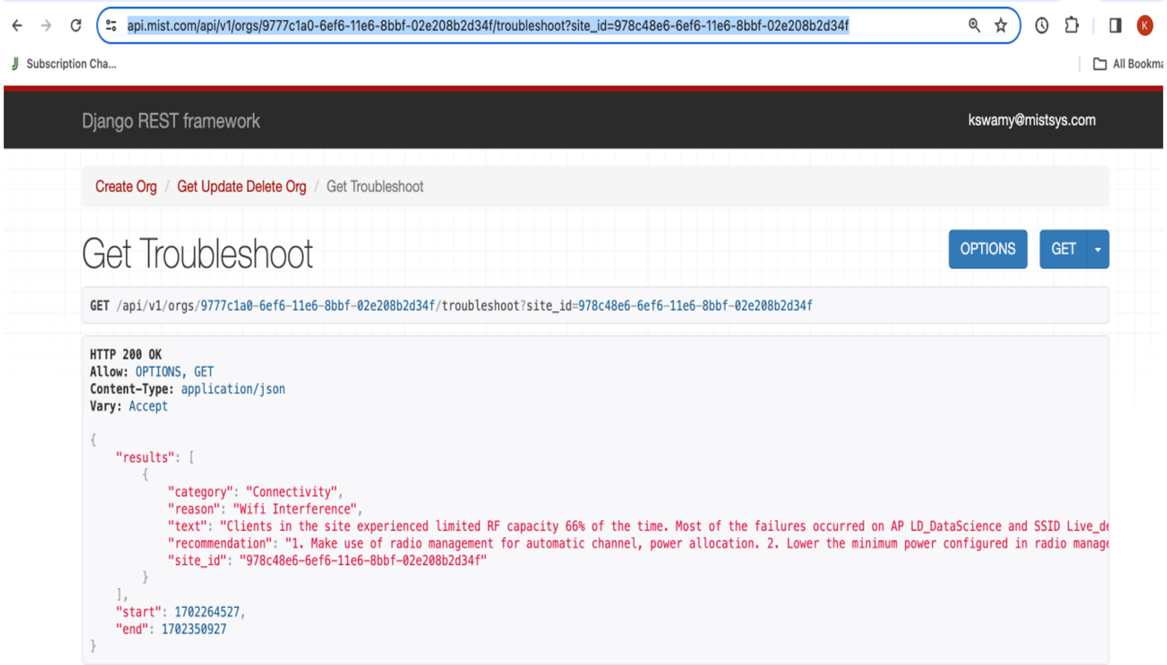
```
GET /api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?mac=3[redacted]7:46
```

```
HTTP 200 OK
Allow: OPTIONS, GET
Content-Type: application/json
Vary: Accept

{
    "results": [
        {
            "category": "Connectivity",
            "reason": "Latency",
            "text": "Due to high latency on interfaces(s). The switch ld-cup-idf-bb experienced high latency on ge-0/0/17. Longest consecutive latency was e
            "site_id": "978c48e6-6ef6-11e6-8bbf-02e208b2d34f"
        }
    ],
    "start": 1702264366,
    "end": 1702350766
}
```

- Troubleshoot a site (wireless)

  https://api.mist.com/api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?site_id=978c48e6-6ef6-11e6-8bbf-02e208b2d34f



```
api.mist.com/api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?site_id=978c48e6-6ef6-11e6-8bbf-02e208b2d34f
```

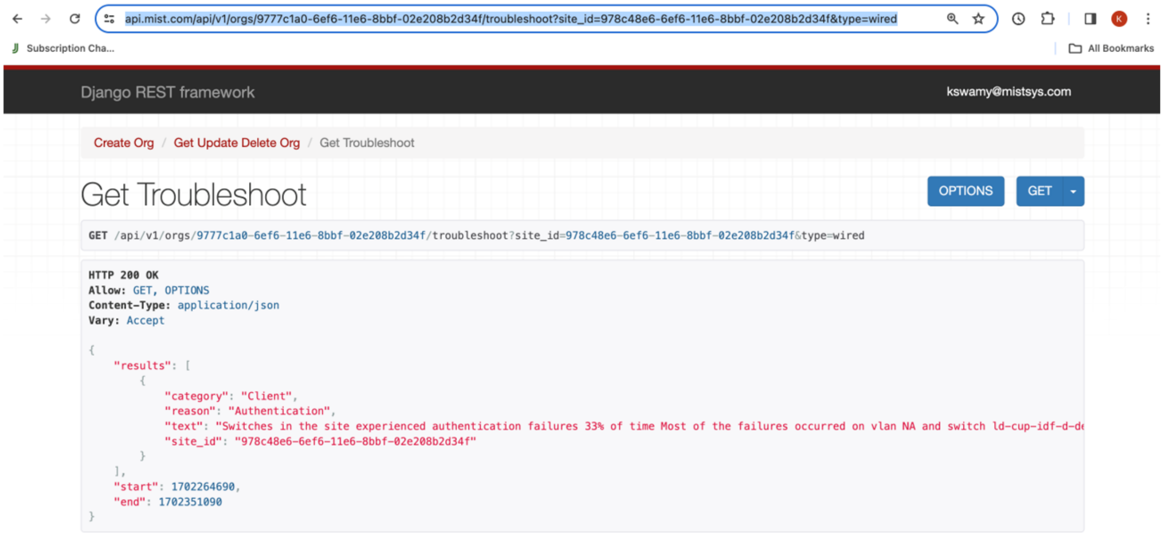
```
GET /api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?site_id=978c48e6-6ef6-11e6-8bbf-02e208b2d34f
```

```
HTTP 200 OK
Allow: OPTIONS, GET
Content-Type: application/json
Vary: Accept

{
    "results": [
        {
            "category": "Connectivity",
            "reason": "Wifi Interference",
            "text": "Clients in the site experienced limited RF capacity 66% of the time. Most of the failures occurred on AP LD_DataScience and SSID Live_d
            "recommendation": "1. Make use of radio management for automatic channel, power allocation. 2. Lower the minimum power configured in radio manag
            "site_id": "978c48e6-6ef6-11e6-8bbf-02e208b2d34f"
        }
    ],
    "start": 1702264527,
    "end": 1702350927
}
```

- Troubleshoot a site (wired)

  https://api.mist.com/api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?site_id=978c48e6-6ef6-11e6-8bbf-02e208b2d34f&type=wired


api.mist.com/api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?site_id=978c48e6-6ef6-11e6-8bbf-02e208b2d34f&type=wired
Subscription Cha...
All Bookmarks
Django REST framework
kswamy@mistsys.com
Create Org / Get Update Delete Org / Get Troubleshoot
OPTIONS
GET

Get Troubleshoot

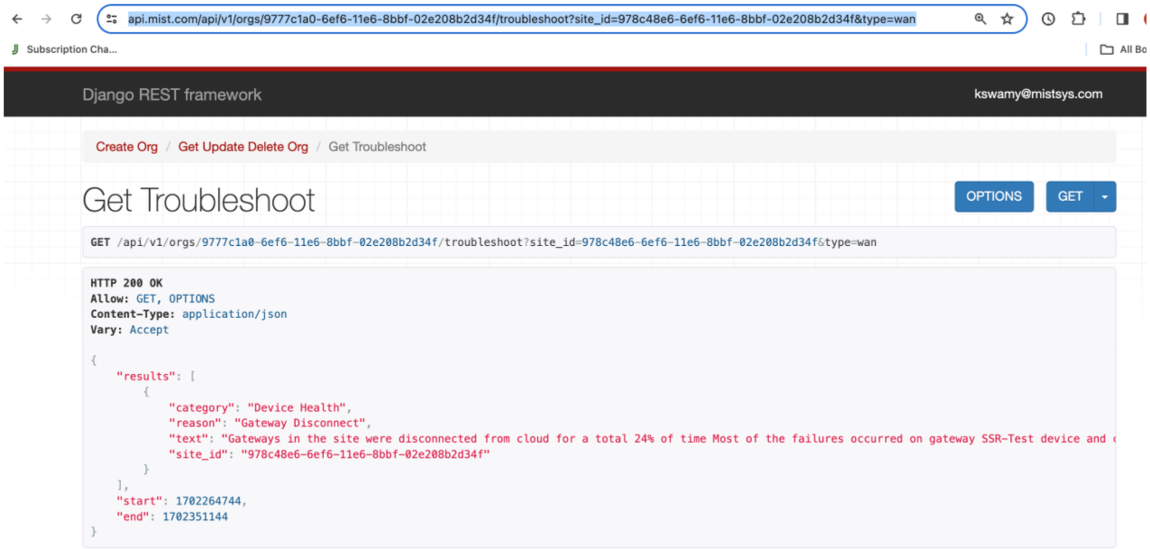
```
GET /api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?site_id=978c48e6-6ef6-11e6-8bbf-02e208b2d34f&type=wired
```

```
HTTP 200 OK
Allow: GET, OPTIONS
Content-Type: application/json
Vary: Accept

{
    "results": [
        {
            "category": "Client",
            "reason": "Authentication",
            "text": "Switches in the site experienced authentication failures 33% of time Most of the failures occurred on vlan NA and switch ld-cup-idf-d-de
            "site_id": "978c48e6-6ef6-11e6-8bbf-02e208b2d34f"
        }
    ],
    "start": 1702264690,
    "end": 1702351090
}
```

- Troubleshoot a site (WAN)

  https://api.mist.com/api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?site_id=978c48e6-6ef6-11e6-8bbf-02e208b2d34f&type=wan


api.mist.com/api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?site_id=978c48e6-6ef6-11e6-8bbf-02e208b2d34f&type=wan
Subscription Cha...
All Bo
Django REST framework
kswamy@mistsys.com
Create Org / Get Update Delete Org / Get Troubleshoot
OPTIONS
GET

Get Troubleshoot

```
GET /api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?site_id=978c48e6-6ef6-11e6-8bbf-02e208b2d34f&type=wan
```

```
HTTP 200 OK
Allow: GET, OPTIONS
Content-Type: application/json
Vary: Accept

{
    "results": [
        {
            "category": "Device Health",
            "reason": "Gateway Disconnect",
            "text": "Gateways in the site were disconnected from cloud for a total 24% of time Most of the failures occurred on gateway SSR-Test device and 
            "site_id": "978c48e6-6ef6-11e6-8bbf-02e208b2d34f"
        }
    ],
    "start": 1702264744,
    "end": 1702351144
}
```

You can view the API documentation at https://api.mist.com/api/v1/docs/Org#troubleshoot.