Juniper Networks | Engineering Simplicity

Juniper Mist AI-Native Operations Guide

Published
2026-01-29

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

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

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

10 **Marvis Client**

1

CHAPTER

Get Started with AI Ops

IN THIS CHAPTER

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.

Use these features to shorten your troubleshooting time and identify proactive actions to improve 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 create an impact. Use the Service Level Expectations (SLE) dashboards to quickly spot 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) supports your human language engagements with Marvis (the AI engine). It helps Marvis understand you when you're asking about network health, troubleshooting, or 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 helps identify network features with the most impact on your Service Level Expectations (SLEs).

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 optimizes RF (Radio Frequency) intelligently and dynamically in real time. As a result, you'll get the best possible Wi-Fi coverage, capacity, and connectivity. This approach far surpasses the performance you'd see from manual settings or traditional fixed algorithms. Even better, it's totally customized for each site.

Video: Explainable AI Whiteboard Technical Series: Reinforcement Learning

Key concepts:

- Reinforcement Learning

- Value Function
- Future Rewards

Decision Trees and Issue Detection

Decision Trees are a form of supervised learning. They pinpoint common network issues like faulty cables, access point and switch health issues, and wireless coverage.

Video: Explainable AI Whiteboard Technical Series: Decision Trees

Key concepts:

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

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, Zoom, and more.

RELATED DOCUMENTATION

Requirements | 6

AIOps in Action

SUMMARY

Watch an ops engineer troubleshoot issues by using the Marvis conversational assistant and Service Level Expectations (SLEs). View technical details, audit logs, and 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.

- 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 68
- Alerts—To get started with Alerts, see: "Alerts Overview" on page 126
- Marvis—To get started with Marvis, see: "Marvis Virtual Network Assistant Overview" on page 155

2
CHAPTER

Insights

IN THIS CHAPTER

Insights Overview

SUMMARY

Get familiar with the major features of the Insights page.

IN THIS SECTION

The Mist Insights page provides a quick overview into your clients' network experience for anywhere in the stack, be it the Wireless, Wired, or WAN network. From there, double-click whatever parameters or events that interest you to get statistical insights into the health of your network or to identify and troubleshoot issues.

To open the page, select **Monitor** > **Service Levels** from the left menu and then click the **Insights** button at the top of the Monitor page. (Click **Classic View** if you don't want the Full Stack design, or if you experience any numerical discrepancies in the data as presented.)

Figure 1: Mist Insights for the Full Stack

You can view data for a given site using the map view, by device using a floorplan, or by time using the timeline. For example, under AP Insights you can get details about network traffic, client session and connection trends, post client connection metrics, as well as traffic volume and type transiting all or selected APs.

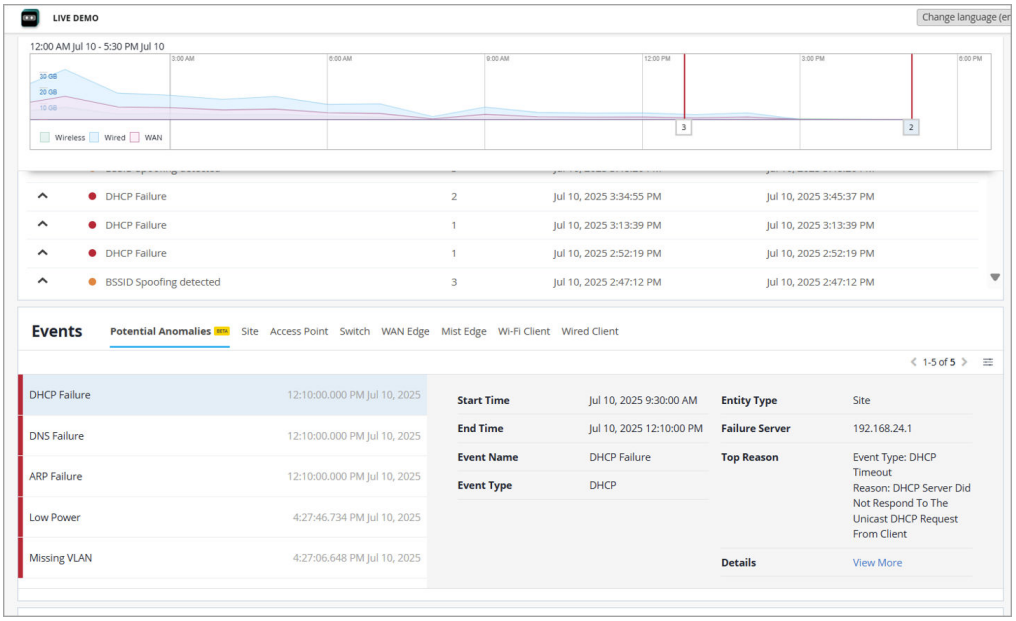
The time-based analysis is especially useful. You can view Insights telemetry aggregated by the past 60 minutes, all the way up to the past seven days. Analysis includes overall connection status, client connection trends, and network traffic patterns. If you need an even longer time-view, Premium

Analytics provides up to three years' data and analysis with a subscription (select **Analytics** > **Premium Analytics** from the Mist menu).

Insights Telemetry and Events

The Insights summary shows the connection status of devices such as access points (APs), switches, WAN edges, and Wi-Fi clients. It also includes event details for all devices and sites.

Figure 2: Network Events



The Applications view shows the number of clients and the bytes sent and received on the both WAN and Wireless networks.

Telemetry sources include the following:

- 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

For information about the various sections of the page, see the other topics in this chapter.

Site Insights

SUMMARY

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

IN THIS SECTION

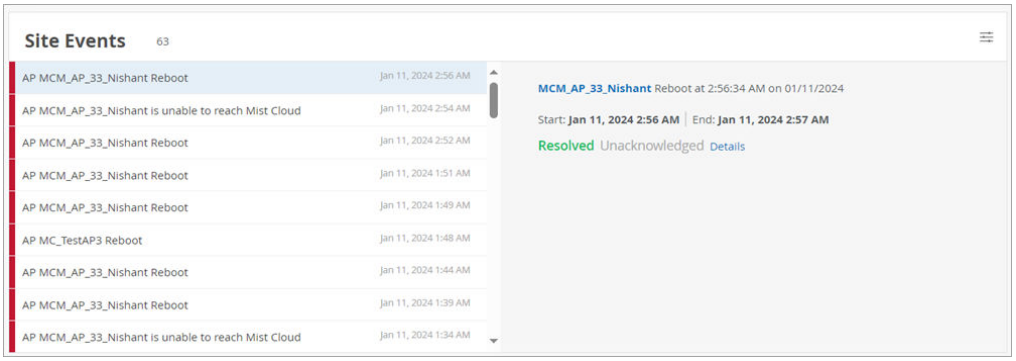
Finding the Site Insights

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

Site Events

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

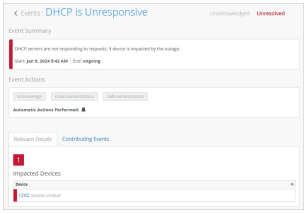
Click an event to see a summary on the right side of the page.



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 15.
- 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.

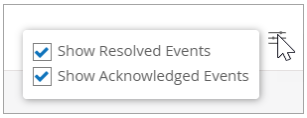
  Here's an example of the event details page for a DHCP server event.



Site Event Types

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

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.



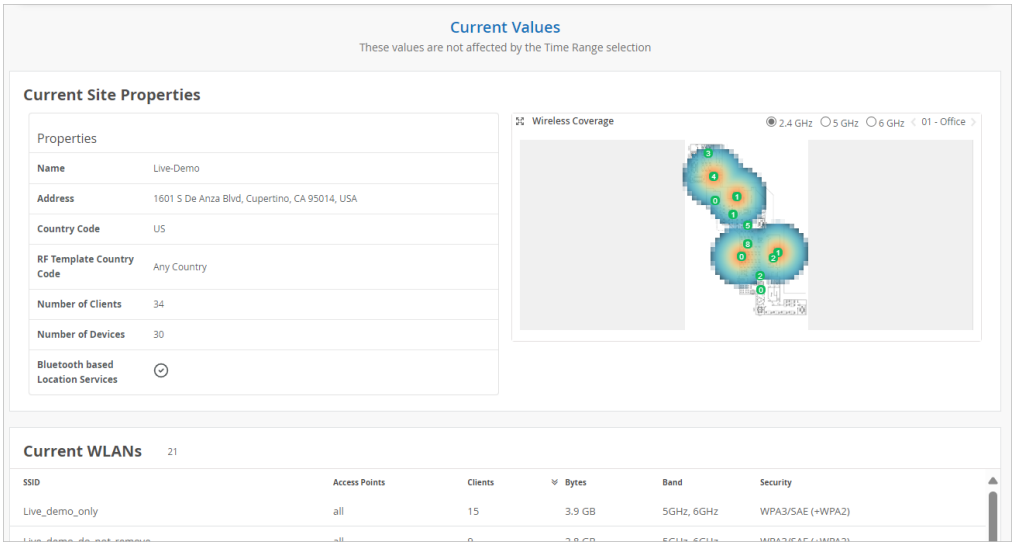
Related Events and Information for Sites

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 27
- "Applications" on page 60
- "Meeting Insights Chart" on page 61
- "Network Servers" on page 64
- "Pre-Connection and Post-Connection Charts" on page 65

Current Values for Sites

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



NOTE: The values in this section don't change when you adjust the time range selection at the top of the page.

When you select a site 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.

AP Insights

SUMMARY

Investigate issues affecting access points (APs).

IN THIS SECTION

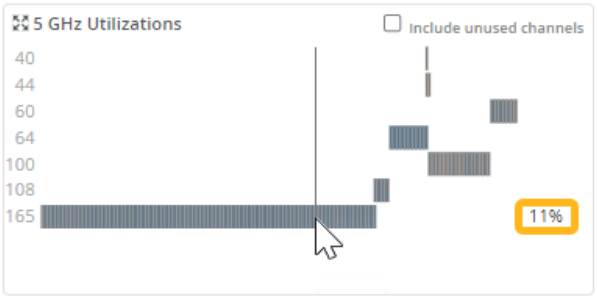
Finding the AP Insights

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 graphs for the 2.4 GHz, 5 GHz, and 6 GHz frequency bands to view interference sources and to assess overall channel health.

- 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.



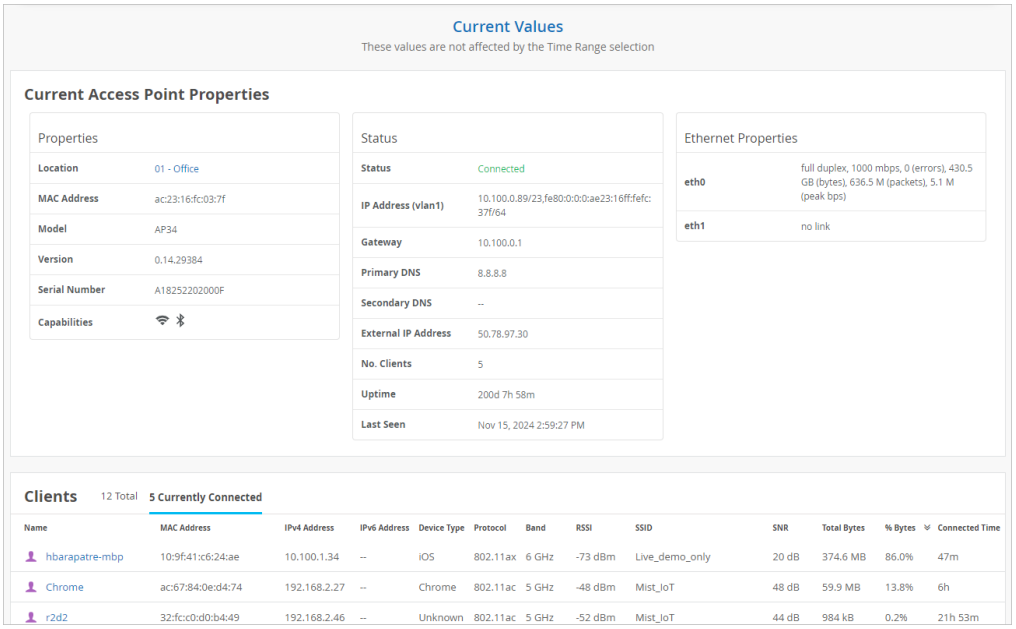
Related Events and Information for APs

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 27
- "Site Events" on page 14
- "Applications" on page 60
- "Post-Connection Charts" on page 66

Current Values for APs

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



NOTE: The values in this section don't change when you adjust the time range selection at the top of the page.

When you select an AP 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.

Organization Insights (BETA)

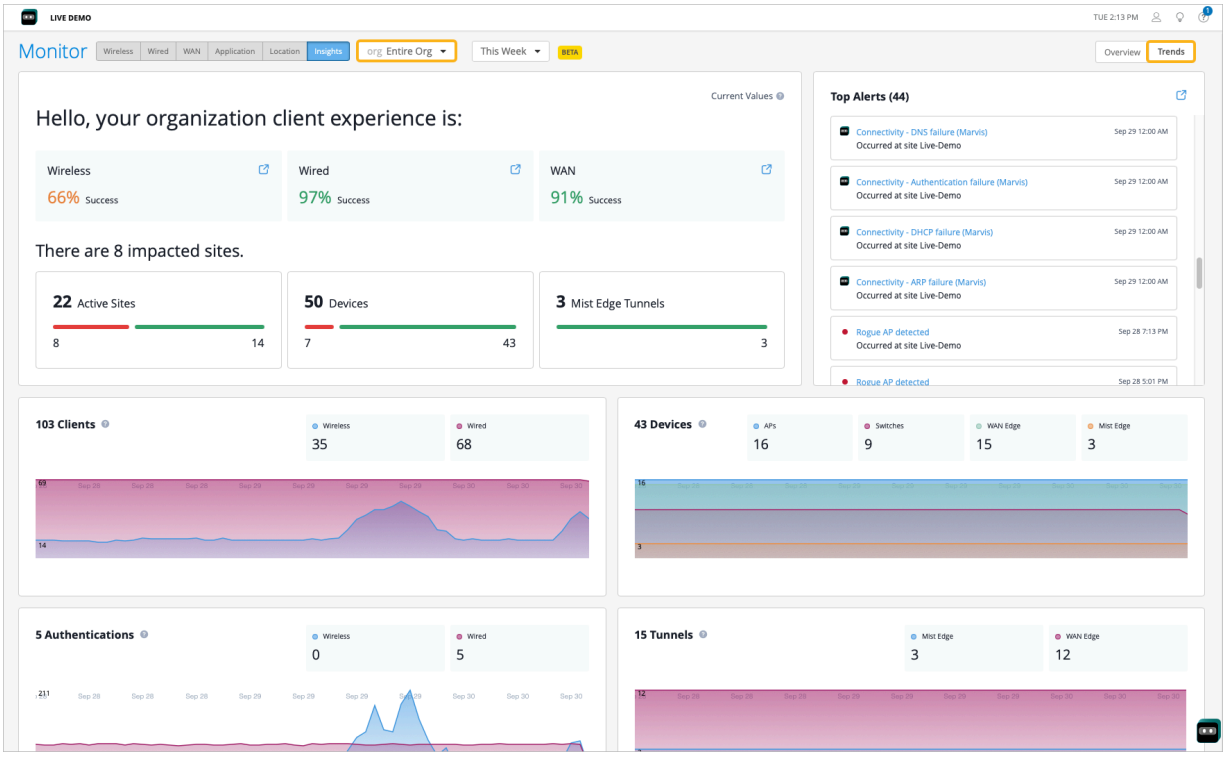
SUMMARY

Investigate issues affecting sites, devices, clients, tunnels, alerts, events, and firmware for your Mist organization.

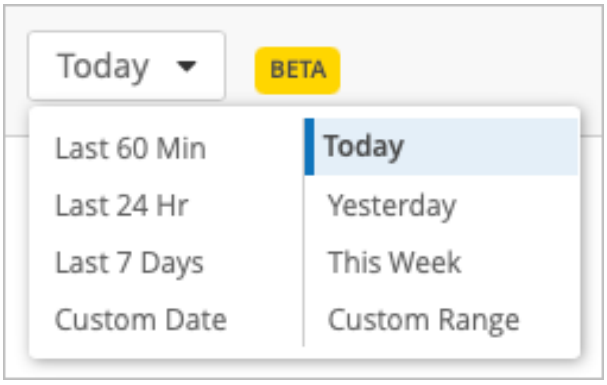
IN THIS SECTION

Find the Org Insights

Go to the "Insights page" on page 12. By default, the **Site** Insights page displays. Select the drop-down menu and select **Entire Org**. In the top right corner of the page, select **Trends**.

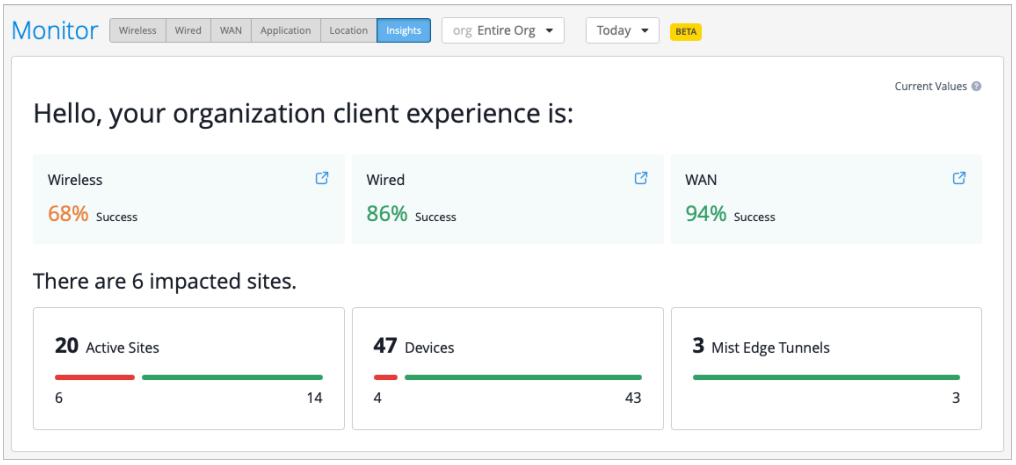


You can select a time frame for which you want to view the data. To do so, select the drop-down menu at the top of the page and select the desired time frame.



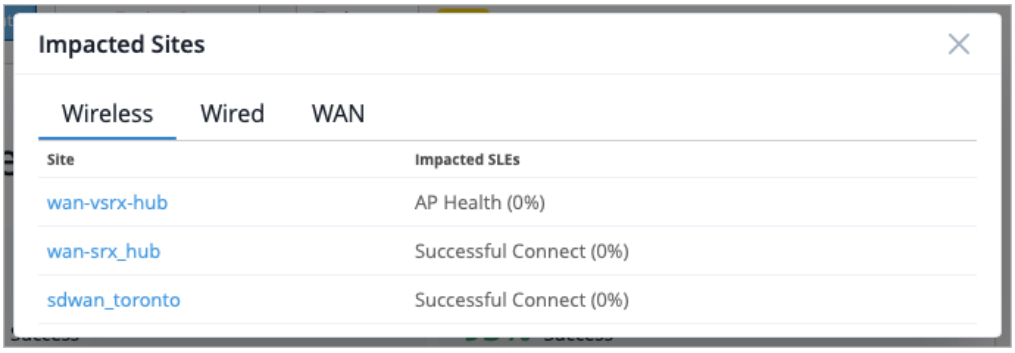
Organization Client Experience

This section displays real-time statistics outlining client experience and impacted sites.



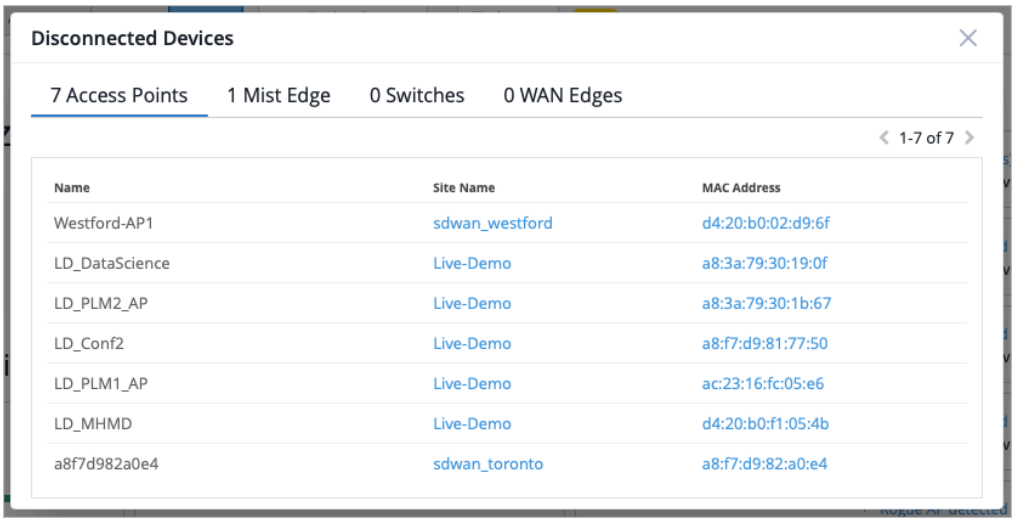
- **Overall SLE Health**—This displays the overall SLE health across Wireless, Wired, and WAN clients. The SLE health score is calculated by considering a subset of the most actionable SLEs within each. There is also a shortcut in each widget you can use to jump to those Insights pages.
- **Active Sites**—The Active Sites count inidicates the number of sites in service and lists the sites that have had client activity in the past 7 days. This count also tells you the number of sites in your org that had client activity in the past 7 days. The breakdown provides you with the number of sites with optimal (represented in green) or sub-optimal (in red) SLEs for the subset of SLEs in each domain. This is refreshed every minute minute.

  Select the red portion of the bar to bring up the list of Impacted Sites with sub-optimal SLEs. This displays the impacted SLE and the success percentage.



- **Devices**—The Devices count provides insight into the total number of active devices (active in the last 14 days) and a further breakdown of connected and disconnected devices at an organization level.

  Click the red portion of the bar to open the list of disconnected devices per device category.

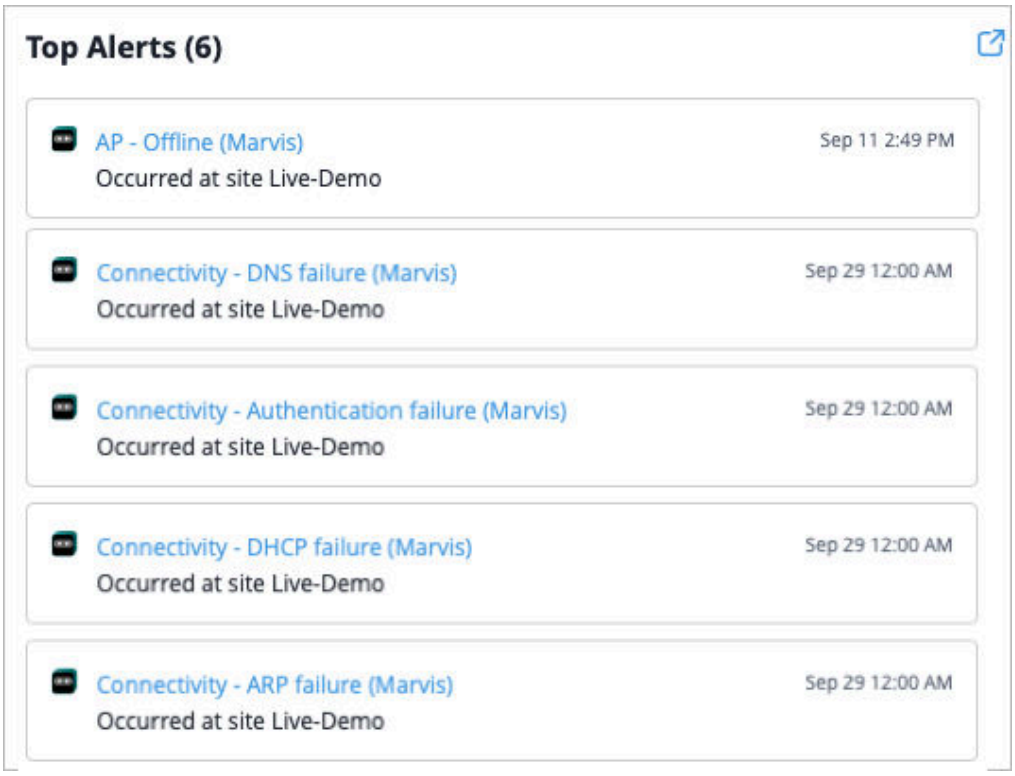


- **Mist Edge Tunnels**—This count provides insight into the total number of tunnels configured for Mist Edges. If you click the red portion of the bar, the breakdown provides insight into the tunnels that are configured but currently disconnected.

- **Top Alerts**—This section displays the alerts with the highest impact, effectively reducing alert fatigue. The following alert types can be displayed in this list:

  - Marvis Action
  - AP Loop Detected event
  - WAN Edge/Switch DHCP Pool Exhausted
  - Critical Switch Port Up/Down
  - Critical WAN Edge Port Up/Down

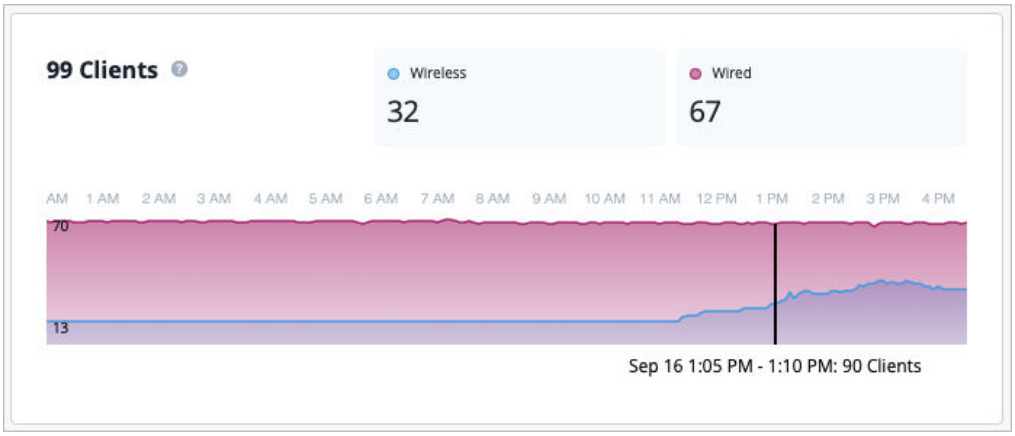
- EVPN Detected Duplicate MAC Address



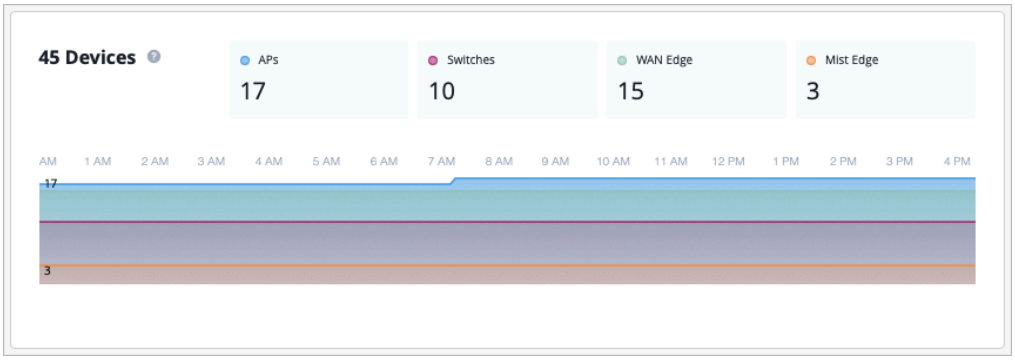
Network Activity Overview

These graphs provide high-level insights into network activity. The data visualizations reflect system status and usage patterns over a selected time period. The graphs are updated via the API and WebSockets.

- **Clients**—This graph reflects the most up to date number of clients per wired and wireless assurance. The numbers are updated every minute via WebSockets. The graph itself displays client connectivity for wireless and wired users and automatically refreshes every 10 minutes. It may take up to 5 minutes for the graph to indicate a major drop in trends.

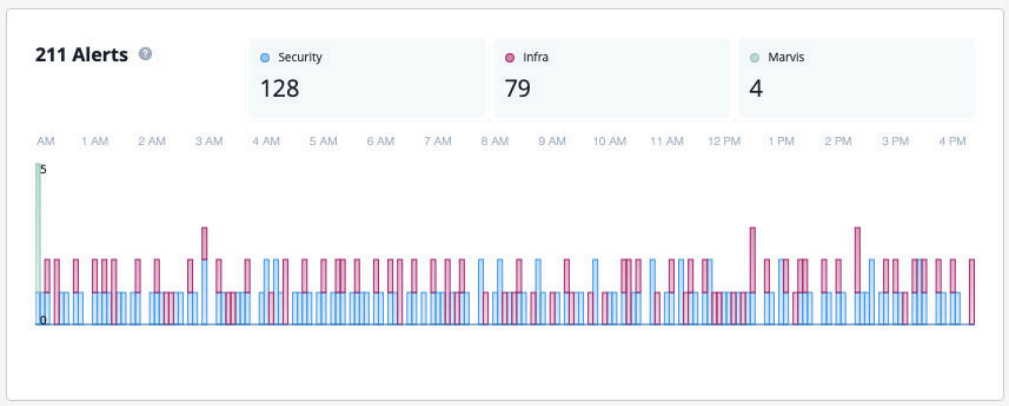


- **Devices**—The most up to date number of cloud connected wired, wireless, and WAN devices are displayed. These numbers are updated every minute through WebSocket, and can take up to 5 minutes before indicating a major drop in trends. The graph itself shows device cloud connectivity for access points, switches, WAN Edges and Mist Edges. It automatically refreshes every 10 minutes.



- **Authentications**—The current rate of successful authentication events across wired and wireless clients are shown. These numbers are updated every minute through WebSockets. The graph itself shows trends of successful authentication events across wired and wireless clients per 5 minutes per hour based on the selected time. It automatically refreshes every 10 minutes.

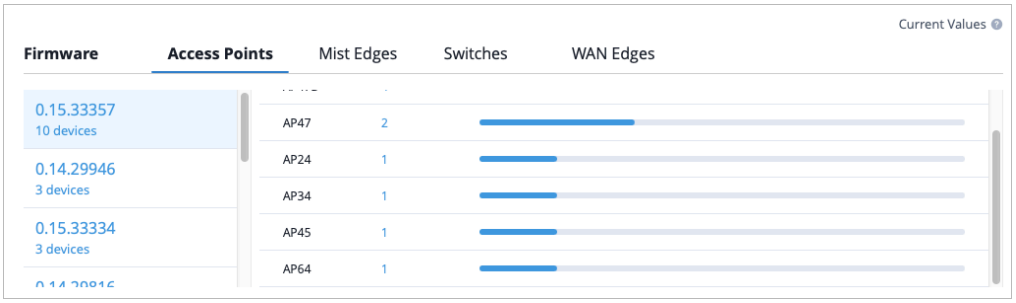
- **Alerts**—This displays the total number of alerts for the selected time period, including the most up to date number of Security, Infrastructure, and Marvis alerts. In the graph, you can see what types of alerts occurred at a specific point in time.



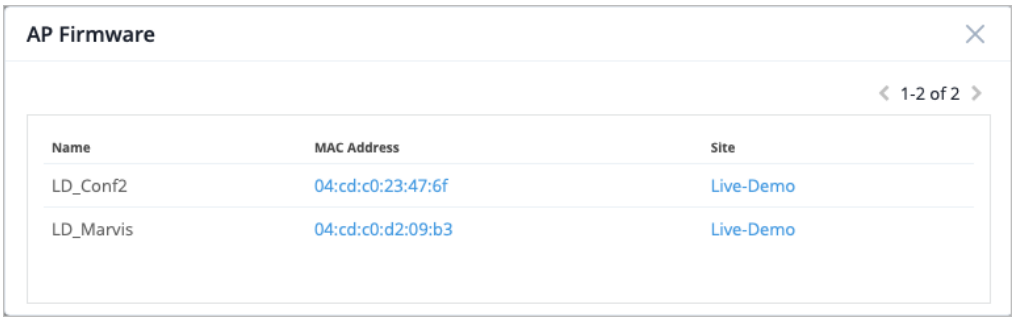
- **Events**—This displays the total number of current infrastructure and client events for the selected time period. The graph is updated via API and the UI refreshes every 10 minutes.

Firmware Overview

The firmware section provides a detailed breakdown of device firmware deployments segmented by device type, firmware version, and hardware model. Network engineers and IT administrators can use the firmware section to monitor firmware consistency, identify upgrade opportunities, and ensure optimal performance across wireless infrastructure.



You can also click on the number in the Device Count column to see a pop-up window which includes device information such as device name, MAC address, and the Site that the device belongs to.



RELATED DOCUMENTATION

Site Insights | 14

Wireless Client Insights

SUMMARY

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

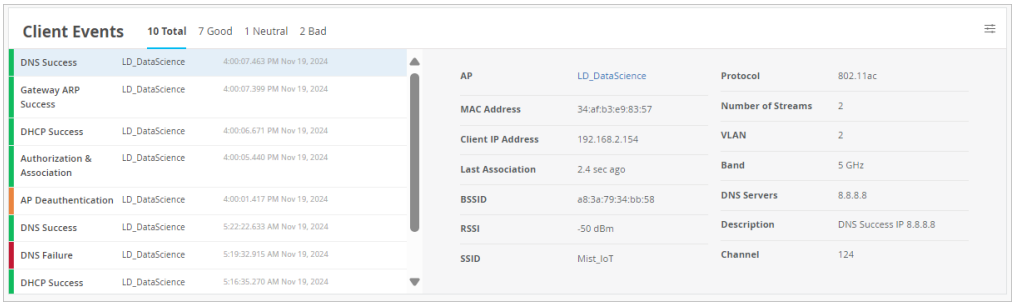
IN THIS SECTION

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.



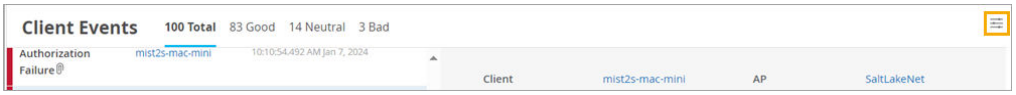
NOTE: Client Events appear on the Insights page when you select a site, AP, or client as the context.

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 28.
- 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 capture 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.



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.

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

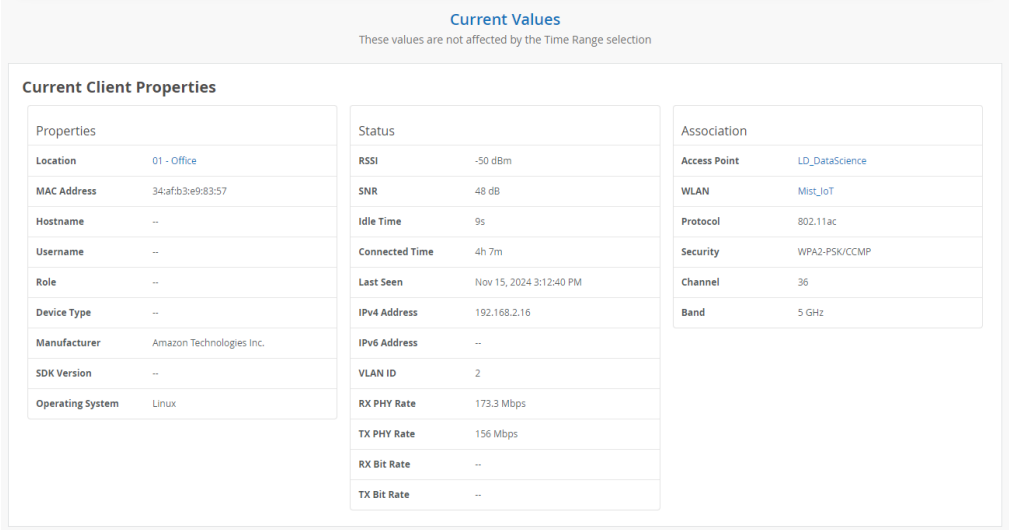
Related Events and Information for Wireless Clients

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 60
- "Meeting Insights Charts" on page 61 (including Meeting Details)
- "Pre-Connection and Post-Connection Charts" on page 66

Current Values for Wireless Clients

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



NOTE: The values in this section don't change when you adjust the time range selection at the top of the page.

When you select a wireless client 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.

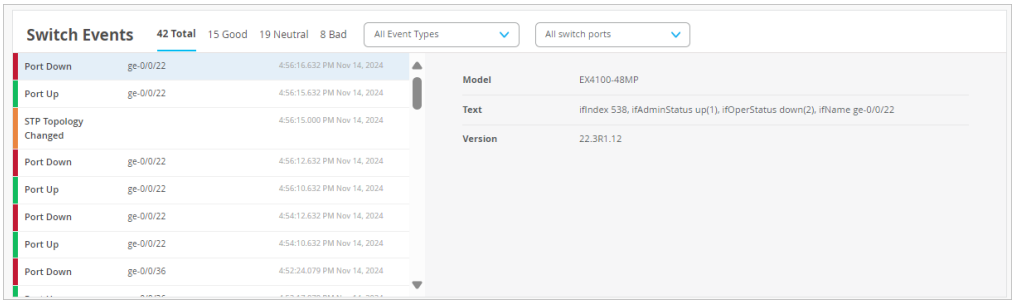
IN THIS SECTION

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.



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. You can add multiple types, clicking them one by one. For more information, see "Switch Event Types" on page 33.
- Use the **Switch Ports** menu to show all ports or select a port.

Switch Event Types

The Event Types options include:

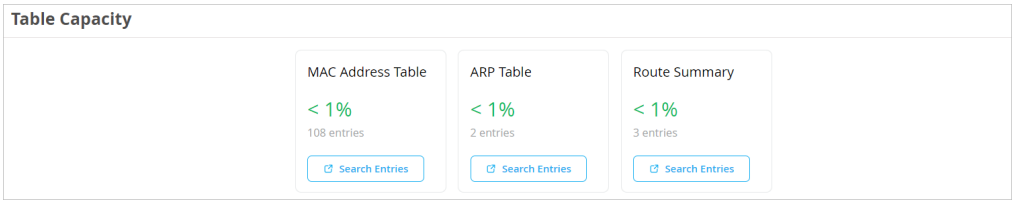
- Alarm Chassis FAN
- Alarm Chassis Hot
- Alarm Chassis Partition
- Alarm Chassis PEM
- Alarm Chassis POE
- Alarm Chassis PSU
- Alarm POE Controller Upgrade Available
- Assigned
- Auth Session Deleted
- BFD Session Disconnected
- BFD Session Established
- BGP Neighbor Down
- BGP Neighbor Up
- Bounce 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

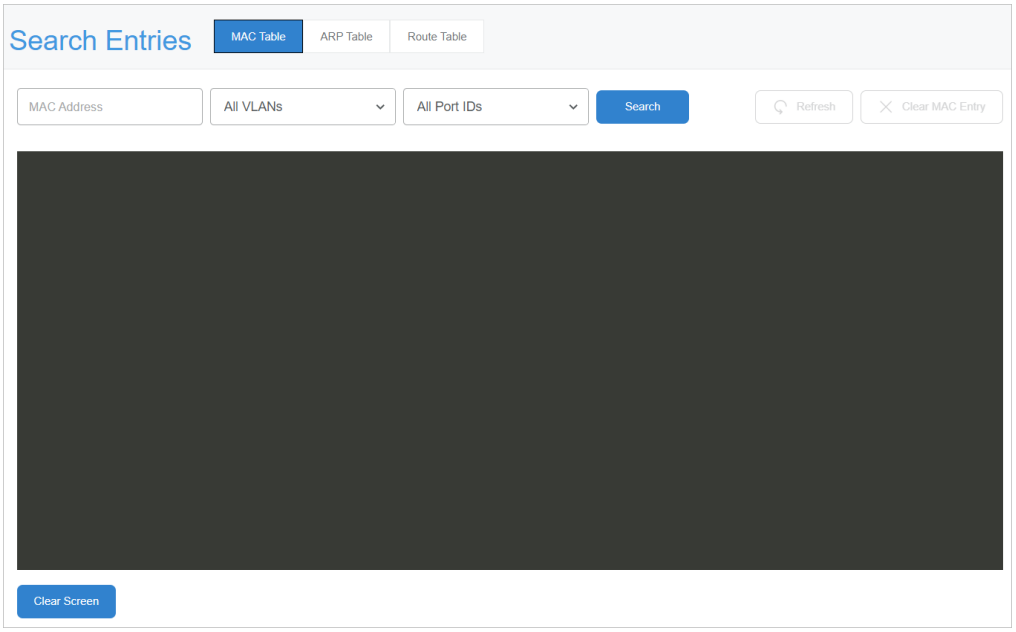


This section shows the utilization and the number of entries for these tables:

- 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 your search term (such as MAC address, IP address, prefix, or port ID, 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.

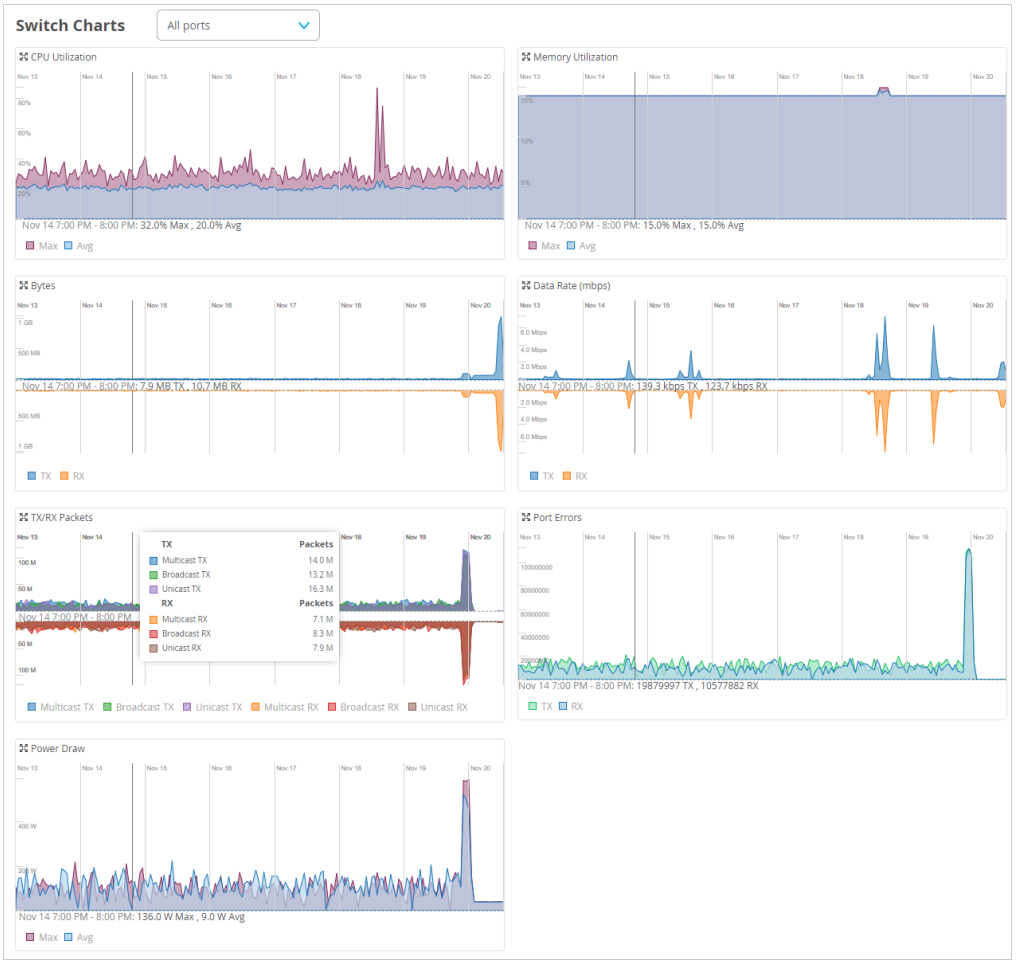


Switch Charts

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.

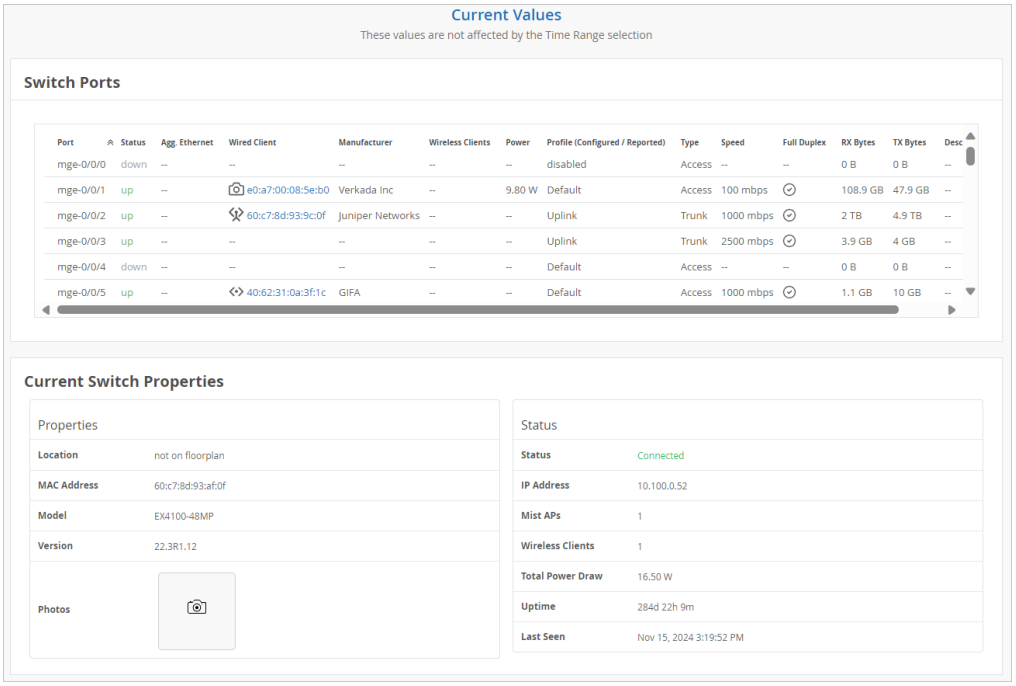


The charts include:

- 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.



NOTE: The values in this section don't change when you adjust the time range selection at the top of the page.

When you select a switch 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.

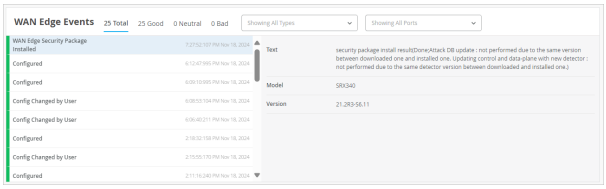
IN THIS SECTION

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.



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. You can add multiple types, clicking them one by one. For more information, see "WAN Edge Event Types" on page 42.

- 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

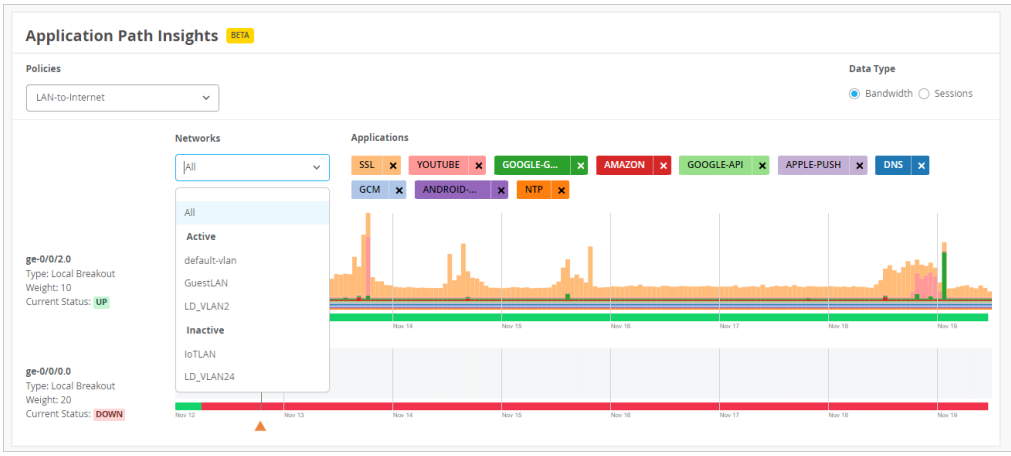
- Port Up
- Reassigned
- Restarted by User
- RG State Change
- Unassigned
- Unclaimed
- WAN Edge Alarm
- WAN Edge App package Install Failed
- WAN Edge ARP Failure
- WAN Edge ARP Success
- WAN Edge BGP Neighbor Down
- WAN Edge BGP Neighbor Up
- WAN Edge Certificate Regenerated
- WAN Edge Chassis Hot
- 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 Start
- 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.

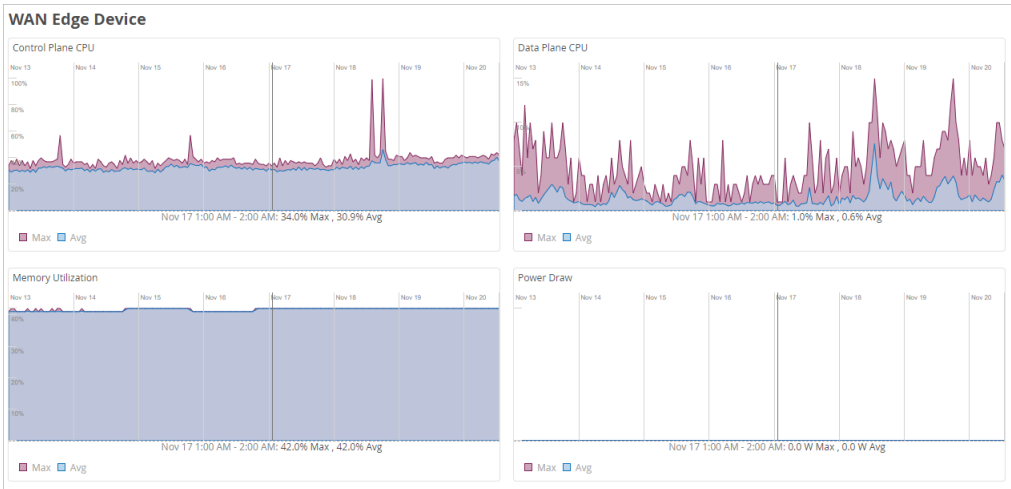


You can select the information to show the chart:

- **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.



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.

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—Displays bandwidth utilization metrics in megabits per second (Mbps) for that particular interface.
- Max Bandwidth—Displays insights into the highest point of link utilization recorded for received power signal (RX) and transmitted power signal (TX) packets in megabits per second (Mbps) on each port during the day.

- Applications TX + RX Bytes—Displays transmit and receive data information at application-level. You can click the application name at the bottom of the chart to see clients, MAC address, IP address, device type, and bytes for bandwidth utilization.
- Port Errors—The **Port Errors** graph displays port errors detected on the WAN Edge device over a period of time. It includes all possible ethernet errors reported by the port device driver. Exact types of errors vary by device driver, and the total may include but is not limited to CRC errors, collisions, etc. Errors are counted in both the transmit (TX) and receive (RX) direction. The graph displays the total for all ports, or for a particular port based on the WAN Edge Ports selection.
- IPSec Traffic—Displays the IPsec traffic for transmit and receive packets during the day in kilobytes or megabytes.

Peer Path Stats

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

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

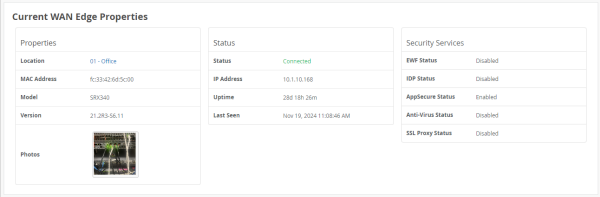
In each chart, hover your mouse pointer over any data point to see the details in a pop-up box.

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.



NOTE: The values in this section don't change when you adjust the time range selection at the top of the page.

When you select a WAN Edge 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.

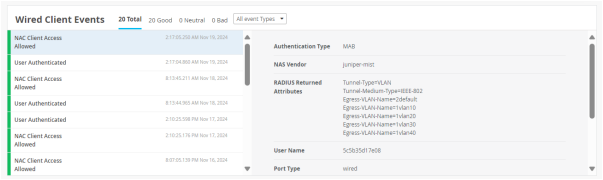
IN THIS SECTION

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.



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 50
- 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 33
- "Meeting Insights" on page 61 (including Meeting Details)

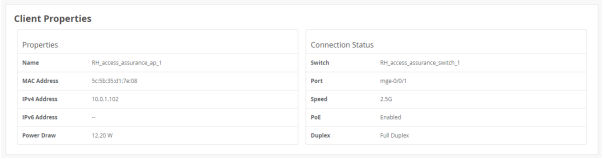
Wired Client Charts

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.



NOTE: The values in this section don't change when you adjust 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

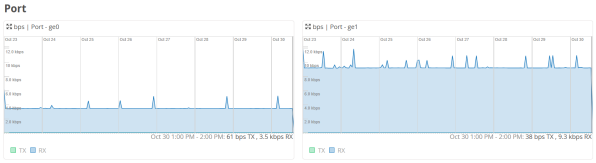
Events include:

- AP Tunnel Bounce Success
- All Tunnel Interface Dropped from LACP
- All Tunnels Disconnected
- AP Auto Preemption Skipped
- AP Tunnel Bounce by User
- AP Tunnel Bounce Failed
- AP Tunnel Bounce Success
- Configuration Failed
- Configuration Modified

- Configuration Modified by User
- Connected to Mist
- Disconnected from Mist
- Distro Upgrade Completed
- Distro Upgrade Failed
- Fan Connected
- Fan Disconnected
- First Tunnel Connected
- First Tunnel Interface Joined LACP
- Inactive Upstream VLAN Detected
- Last Tunnel Interface dropped from LACP
- Primary Radius Server Changed
- Primary Radius Server Unresponsive
- PSU Inserted
- PSU Withdrawn
- Restarted
- Restarted by User
- Secondary Power Connected
- Secondary Power Disconnected
- Service Failed to Start
- Service Install Failed
- Service Installed
- Service Restarted
- Service Started
- Service Uninstalled
- Service Update Failed

- Service Version Updated
- Tunnel Interface Blocked
- Tunnel Interface Bounce Failed
- Tunnel Interface Bounce Success
- Tunnel Interface Bounced by User
- Tunnel Interface Dropped from LACP
- Tunnel Interface Forwarding
- Tunnel Interface Joined LACP
- Tunnel Interface Link DOWN
- Tunnel Interface Link UP
- Tunnel Interface Upstream Monitored Resource Reachable
- Tunnel Interface Upstream Monitored Resource Unreachable

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 don't change when you adjust the time range selection at the top of the page.

When you select a Mist Edge as the context, the Current Values section includes:

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

Cellular Edge Insights

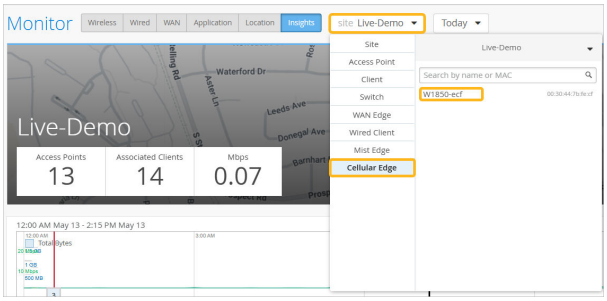
SUMMARY

Investigate issues affecting Cellular Edges.

IN THIS SECTION

Finding the Insights for Cellular Edges

Go to the "Insights page" on page 12. In the **site** menu at the top of the page, click **Cellular Edge**. Then click the device that you want to view.

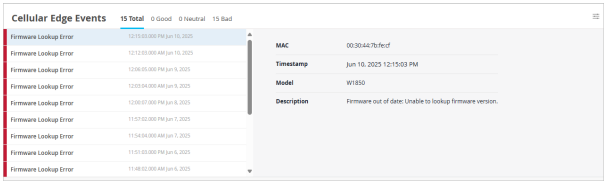


Cellular Edge Events

The Cellular Edge Events section provides a list of events.

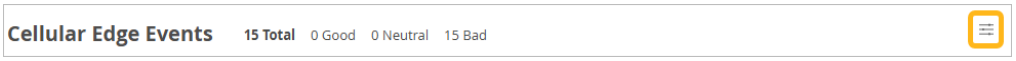
Use the tabs at the top of this section to show all, good, neutral, or bad events.

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



Cellular Edge Event Types

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



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.

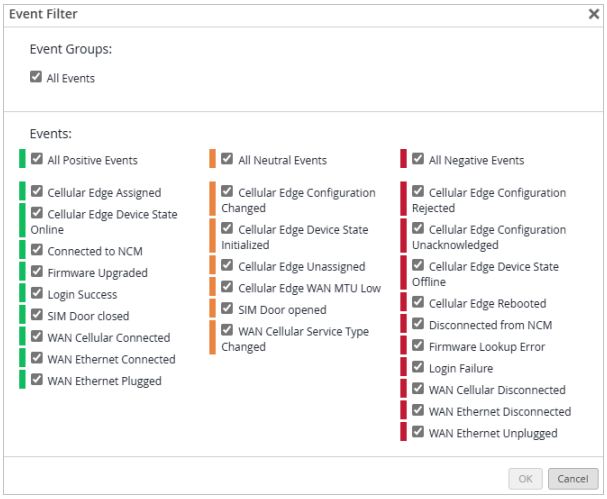
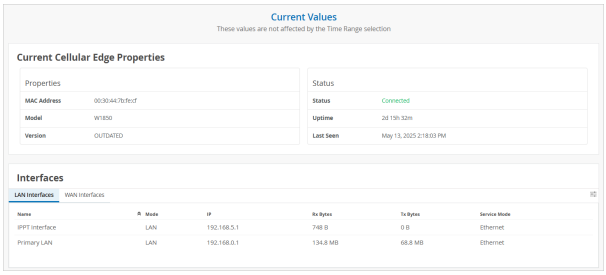


Table 2: Cellular Edge Event Types

Positive Client Events	Neutral Client Events	Negative Client Events
Cellular Edge Assigned	Cellular Edge Configuration Changed	Cellular Edge Configuration Rejected
Cellular Edge Device State Online	Cellular Edge Device State Initialized	Cellular Edge Configuration Unacknowledged
Connected to NCM	Cellular Edge Unassigned	Cellular Edge Device State Offline
Firmware Upgraded	Cellular Edge WAN MTU Low	Cellular Edge Rebooted
Login Success	SIM Door opened	Disconnected from NCM
SIM Door closed	WAN Cellular Service Type Changed	Firmware Lookup Error
WAN Cellular Connected		Login Failure
WAN Ethernet Connected		WAN Cellular Disconnected
WAN Ethernet Plugged		WAN Ethernet Disconnected
		WAN Ethernet Unplugged

Current Values for Cellular Edges

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



NOTE: The values in this section don't change when you adjust the time range selection at the top of the page.

When you select a Cellular Edge 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 the applications for your site, WAN edge, AP, or client.

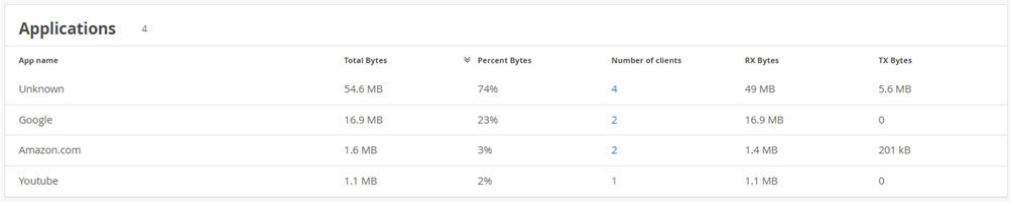
IN THIS SECTION

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 you select a **site, client, or wired client** as the context at the top of the Insights page.

The **Meeting Details** section appears when you select a **client or wired client** as the context.

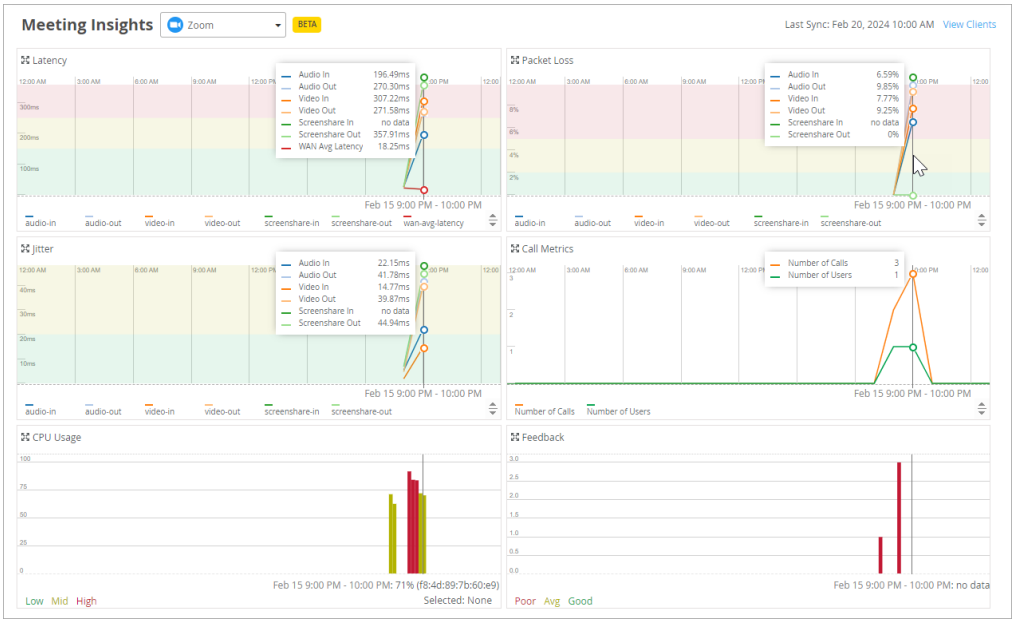
NOTE: This feature is in Beta release.

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 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 all synchronized to 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.



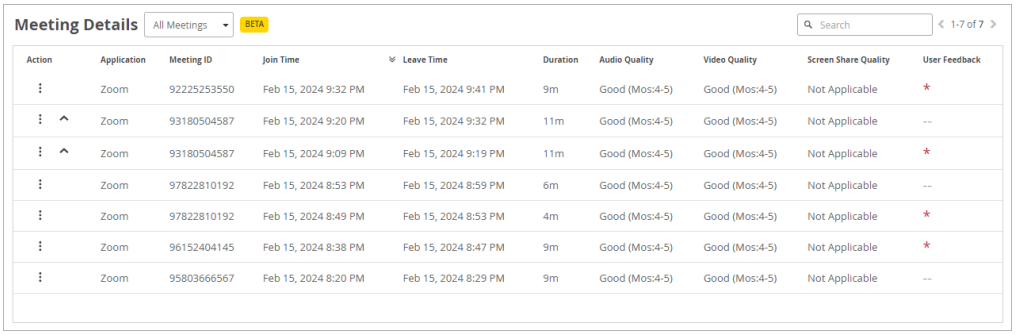
Meeting Details Table

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, the join and leave time, and the quality ratings for audio, video, and screenshare.

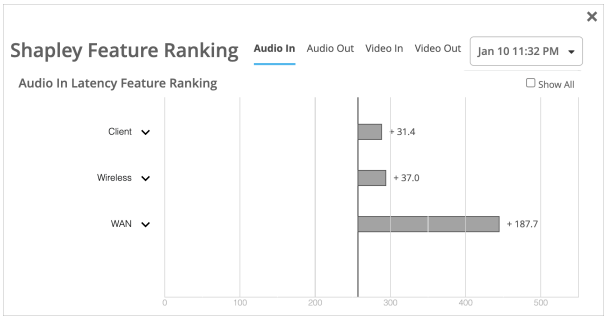


In the Actions column, you can:

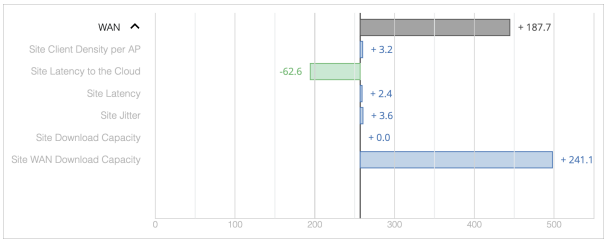
- Troubleshoot—If you have a Marvis subscription, you can click the ellipsis button to get troubleshooting help from the Marvis Conversational Assistant.
- View the Shapley Feature Ranking—A carat ^ icon appears if a user reports a bad experience. Click the ^ icon to view the Shapley Feature Ranking.

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 with 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 shortcut 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.

Pre-Connection and Post-Connection Charts

SUMMARY

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

IN THIS SECTION

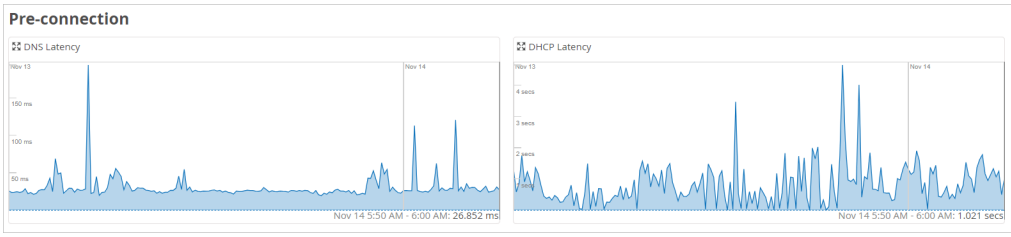
Finding the Pre- and Post-Connection Information

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 shortcut menu.

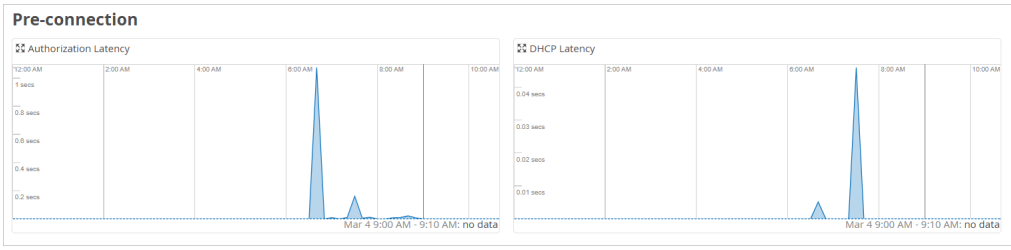
Only the Post-Connection Charts appear when you select an AP or a Cellular Edge.

Pre-Connection Charts

For sites, the Pre-Connection charts include **DNS Latency** and **DHCP Latency**.



For clients, the Pre-Connection charts include **Authorization Latency** and **DHCP Latency**



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

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 don't change when you adjust the time range selection at the top of the page.

For more information, go to these topics:

- "Current Values for Sites" on page 16
- "Current Values for Access Points" on page 19
- "Current Values for Wireless Clients" on page 31
- "Current Values for Switches" on page 40
- "Current Values for WAN Edges" on page 49
- "Current Values for Wired Clients" on page 53
- "Current Values for Mist Edges" on page 56
- "Current Values for Cellular Edge" on page 59

CHAPTER 3

Service-Level Expectations (SLE)

SUMMARY

Get familiar with the Service-Level Expectations (SLEs) and the SLE dashboard.

IN THIS CHAPTER

What Are Service-Level Expectations (SLEs)?

The following video gives you a quick, high-level introduction to SLEs.

Video: Mike and Marvis Episode 2: Understanding Service Level Expectations

Juniper Mist™ captures, analyzes, correlates, and classifies event and performance data from your network and devices. It then provides you with an assessment of users' experiences on your network.

Many factors contribute to positive or negative user experiences. Juniper Mist organizes these factors into SLEs. You can set the SLE thresholds to define exactly what "success" means for SLEs such as throughput, capacity, AP health, switch health, and more (as relevant to your network).

When user experiences fail to meet your SLE success thresholds, Juniper Mist identifies the root cause of each poor experience and provides complete details so that you can address the issues.

By skimming the SLE dashboard, you can see at a glance which service levels are low and what types of issues are occurring.

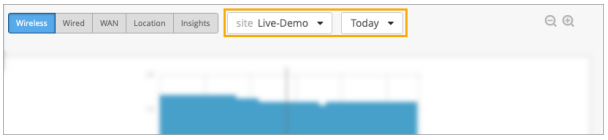
Finding the SLE Dashboard

To access the SLE dashboard, select **Monitor** > **Service Levels** from the left menu. Then use the buttons at the top of the page to select the dashboard that you want to view (such as Wireless, Wired, WAN, Location, and Insights).

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

Selecting the Context and Time Period

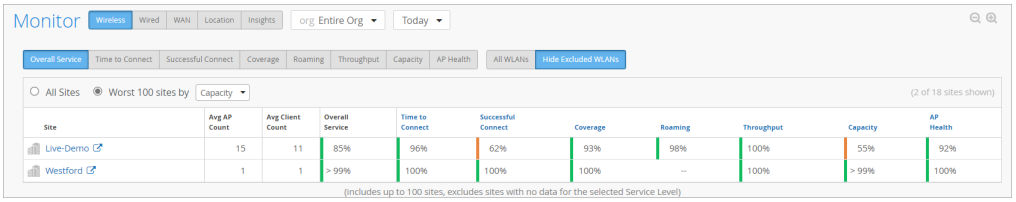
At the top of the Monitor page, select the context, which can be an entire organization, an AP, or a client. In addition, select a time period.



NOTE: The Monitor 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 of the portal.

Context Example: Organization

To compare the performance of all sites in your organization, select **Entire Org** as the context.



Use the filter buttons above the table to change the view:

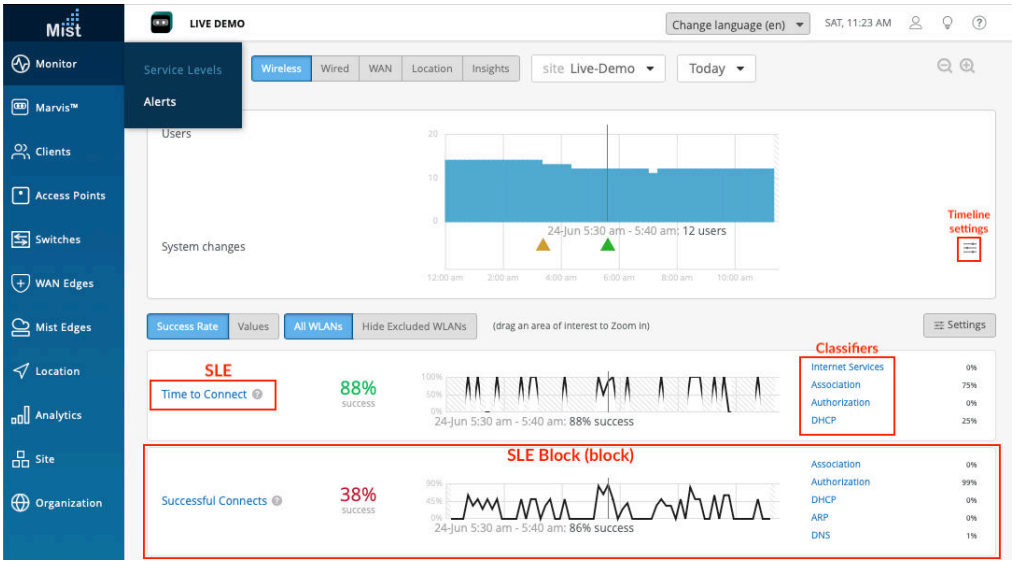
- Overall Service—This is the default view when you select Entire Org as the context. You can compare the overall user experience at each site.
- SLE filter buttons—Zoom in on a single SLE by using the SLE buttons above the table. The button options vary, depending on which page you're on (Wireless, WAN, and so on).

You also have the option to view **All Sites** or the **Worst 100 Sites**. For the Worst 100 option, also use the drop-down list to select the SLE that you're concerned about. For example, if you're troubleshooting an issue with capacity, you'd select that option from the drop-down list to see which sites are having the most issues with this SLE.

NOTE: The available SLEs for the filter buttons and the Worst 100 drop-down list vary, depending on whether you're looking at Wireless, Wired, or WAN SLEs.

Context Example: Site

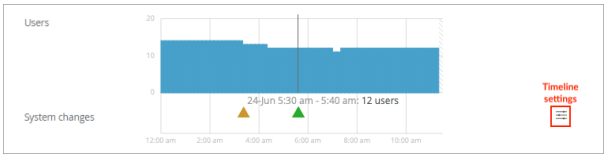
To compare all SLEs for one site, select the site as the context.



NOTE: This image shows a Wireless example, but the SLE blocks are set up the same way for Wired, WAN, and so on.

Using the System Changes Timeline

When investigating issues, your first question might be, "Did anything change on the network?" With this timeline, you can see at a glance if any system changes occurred and how many users or clients were active at the time.

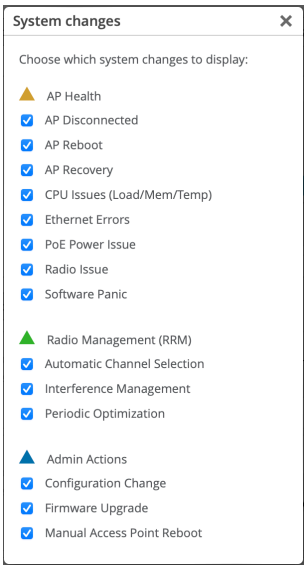


The triangles below the timeline represent various types of system changes:

- Yellow triangle—AP Health
- Green triangle—Radio Management (RRM)
- Blue triangle—Admin Actions

You can adjust the timeline settings to specify the types of changes to include. To get started, click the timeline settings button: 

In the System Changes window, select or clear the check boxes the events to include or exclude.

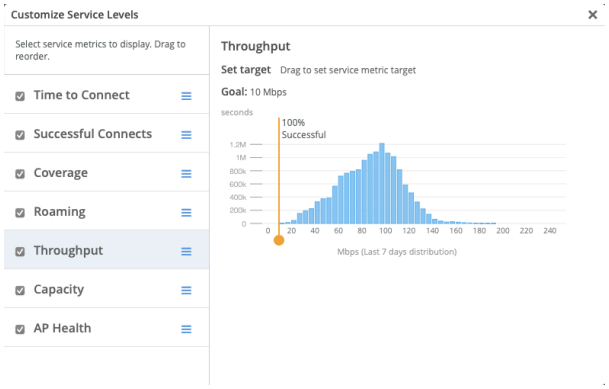


Setting the SLE Thresholds

Each SLE has a success threshold. For the Time to Connect SLE, for example, you might set a threshold of 2 seconds. This means that you consider your network successful when users can send and receive data over the Internet within 2 seconds of attempting to associate with an AP.

To view or modify the SLE thresholds, you can click the **Settings** button on the right side of the SLE dashboard.

In the Customize Service Levels window, you can modify the thresholds as needed to ensure that the SLE settings meet your goals for your network.



NOTE: This example shows the wireless SLEs. Depending on the dashboard that you're viewing, you'll see different SLEs in this window.

Understanding the SLE Blocks

Each SLE appears in a separate block (sub-section) on the dashboard.

In each block, you'll see:

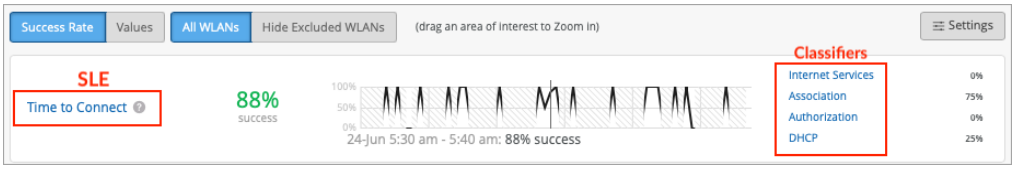
- **Overall Service Level.** On the left side of each SLE block, you'll see the overall service level for the selected site and time period.
  - Click **Success Rate** to see the *percentage* of user experiences that met the SLE success threshold.
  - Click **Values** to see the *number* of user experiences that met the SLE success threshold.
- **Timeline.** In the middle of each SLE block, you can explore the timeline. As your mouse moves across the timeline, information appears under it.
  - Click **Success Rate** to see the *percentage* of successful user experiences at the selected point in time.
  - Click **Values** to see the *number* of successful user experiences at the selected point in time.
- **Classifiers.** On the right side of each SLE block, you see the *classifiers* for the user experiences that didn't meet the SLE success threshold. Juniper Mist attributes each unsuccessful user experience to one classifier. Together, the classifiers give you a high-level root cause analysis of the unsuccessful user experiences.
  - Click **Success Rate** to see the *percentage* of unsuccessful user experiences associated with each classifier.

> **NOTE**: Together, these individual percentages total 100 percent of the unsuccessful user experiences.

- Click **Values** to see the *number* of unsuccessful user experiences that were caused by each classifier.

> **NOTE**: Together, these individual values represent the total number of unsuccessful user experiences.

Sample SLE Block



In this example, the Success Rate button is selected, so you see percentages instead of values.

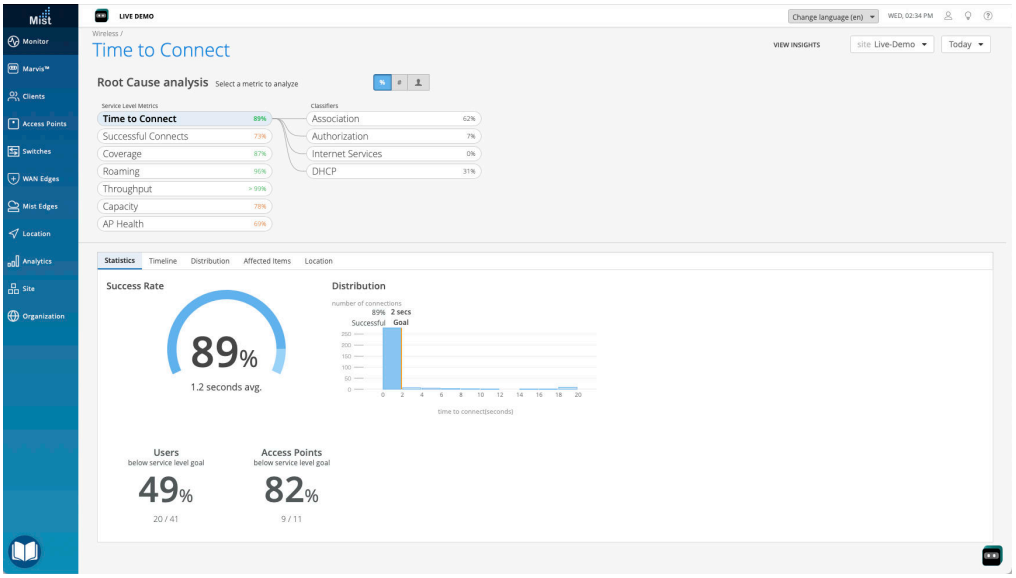
- On the left, you see that the overall success rate for the selected site and time period was 88 percent.
- In the middle, the timeline caption shows that the mouse is hovering over 24-Jun 5:30 am - 5:40 am. At that point, the success rate was 88 percent.

  On the right, you see that 75 percent of the SLE-lowering issues occurred in the Association process and 25 percent occurred in the DHCP process. Together, these classifiers account for 100 percent of the user experiences that failed to meet the threshold. The other classifiers show 0 percent, meaning that they had no impact on this SLE.

Viewing the Root Cause Analysis Page

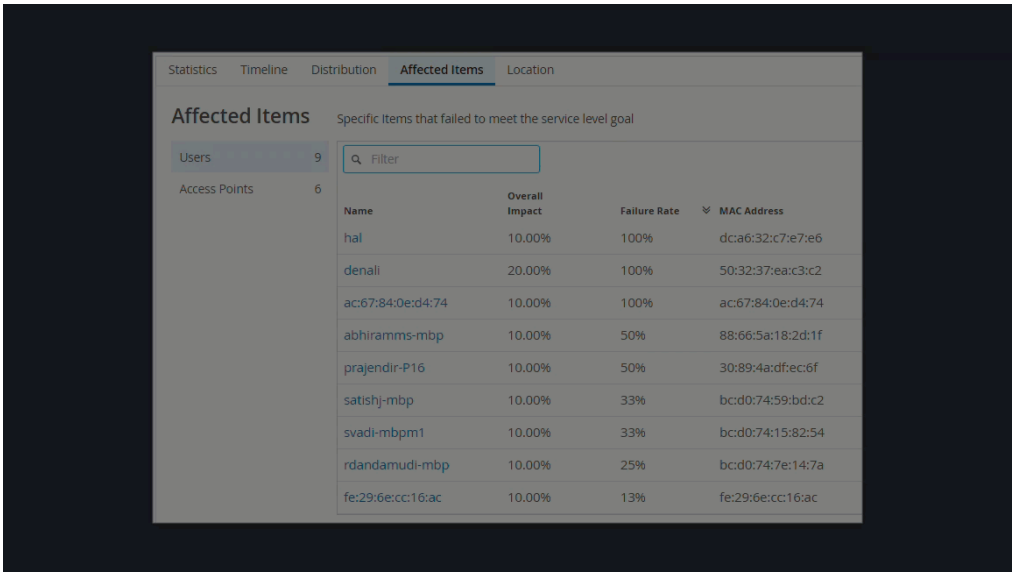
From the dashboard, you can click any SLE or classifier to go to the Root Cause Analysis page.

This example shows the Root Cause Analysis page for the wireless Time to Connect SLE.



Tips:

- At the top of the page, you see the data for all classifiers and their sub-classifiers (if applicable).
- In the lower part of the page, you see additional details about the selected item. Depending on the classifier, you might see signal strength information, a list of affected devices and clients, or other information. These details help you to understand the scope of the issues.
- On the Affected Items page, you can use the Filter box to search for an item. As shown in the animation below, simply start typing in the box, and matching items will appear in a drop-down list. Then click the item that you want to view.



Wireless SLEs

SUMMARY

Use the wireless service-level experiences (SLEs) to assess user-impacting factors such as throughput, signal strength, roaming, and more.

IN THIS SECTION

Overview

IN THIS SECTION

Wireless SLEs Video Overview

Watch this short video to get a quick overview of Wireless SLEs.

Video: Wireless Service Level Expectations

Finding the Wireless SLEs

Select **Monitor** > **Service Levels** from the left menu, and then click the **Wireless** button. The wireless SLEs appear below the Users and System Changes timeline.

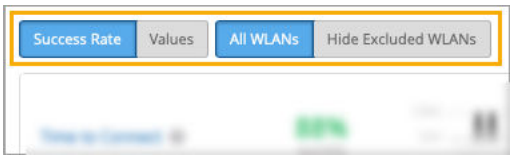
NOTE:

- Your subscriptions determine which buttons appear.
- At the top of the page, use the drop-down menus to set the time period and context (organization, site, or device).

SLE Filter Buttons

Filter buttons appear above the SLE blocks.

- Use the buttons on the left to show **Success Rate** or **Values**.
- Use the buttons on the right to show **All WLANs** or **Hide Excluded WLANs**. The "excluded" WLANs are those that you've excluded by using the Wi-Fi SLE option in your WLAN configuration.



Success Threshold Settings

You can adjust the thresholds that determine success or failure. To do so, click the **Settings** button at the right top corner of the wireless SLEs section. In the settings window, follow the on-screen instructions to set the threshold.

NOTE: Most SLEs allow you to increase or decrease the threshold. Certain SLEs are not adjustable.

Wireless SLEs Video Deep Dive

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

Video: SLE v2

Wireless SLE Blocks

As shown in the following example, each SLE block provides valuable information.

- At the left, you see that this SLE has a 51 percent success rate. If you select the Value filter button, you'll see a number instead.
- At the center, the timeline shows variations across the time period. You can hover your mouse pointer over any point to see the exact time and SLE outcome.

  At the right, the classifiers show the percentage of the issues that were attributed to each root cause. In this example, 86 percent of the issues were attributed to Association and 14 percent to DHCP.

- If you click a classifier, you'll see more information on the Root Cause Analysis page. Most classifiers have sub-classifiers for greater insight into the exact causes. The Root Cause Analysis page also provides additional details about the scope and impact of the issues.

See the following table for more information about the wireless SLEs and classifiers.

Table 3: Wireless SLE Descriptions

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
Time to Connect	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 to set the number of seconds to use as the threshold for this SLE.	Authorization	Connection attempts that took significantly longer than the average to pass the authentication state.
		Association	Connection attempts that took significantly longer than the average to pass the association state.
		Internet Services	Connection attempts that took significantly longer than the average to access Internet resources.

Table 3: Wireless SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
		DHCP	Connection attempts that were affected by DHCP timeouts. Sub-Classifiers: • Stuck • Nack • Unresponsive
Successful Connects	Juniper Mist tracks the success or failure of all connection attempts, including initially connecting to the network, roaming from one AP to another, and ongoing connectivity. The threshold for this SLE is not configurable. It's assumed that you want 100 percent successful connects.	Association	Connections that failed during the association process.
		Authorization	Connections that failed during the authorization process.
		DHCP	Connections that failed during the DHCP process (DHCP timeouts). Sub-classifiers: • Renew Unresponsive • Nack • Incomplete • Discover Unresponsive

Table 3: Wireless SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
		ARP	Connections that failed due to one of these problems: • ARP failure for the default gateway during the initial connection • ARP gateway failures after the initial connection or roam
		DNS	Connections that failed due to DNS failures during or after the connection process.
Coverage	Juniper Mist tracks active clients' Received Signal Strength Indicator (RSSI), as measured by the AP. Use this SLE to determine if you have enough APs. You can click the **Settings** button to set the RSSI to use as the threshold for this SLE.	Weak Signal	RSSI weakness due to low signal strength.
		Asymmetry Downlink	User minutes when the AP's signal was weaker than the client's.
		Asymmetry Uplink	User minutes when the client's signal was weaker than the AP's.

Table 3: Wireless SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
Roaming	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 set to 2 and cannot be changed.	Latency	Excessive roaming time due to latency. Sub-Classifiers: • **Slow 11r Roams**—Fast (802.11r) roaming time exceeding 400 ms • **Slow Standard Roams**—Standard roaming time exceeding 2 seconds • **Slow OKC Roams**—Opportunistic Key Caching (OKC) roaming time exceeding 2 seconds
		Stability	User minutes affected by instability of fast roaming (802.11r). This classifier applies when both the client and the SSID are capable of fast roaming but the client experiences slow roaming for more than 2 seconds. This classifier contains one sub-classifier: **Failed to fast Roam**.

Table 3: Wireless SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions

		Signal Quality	Roaming events affected by weak signal strength
			
			Sub-Classifiers:
			
			• **Interband Roam**—Weak RSSI when clients roam between bands
			
			• **Suboptimal Roam**—Weak RSSI 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**—Weak RSSI when client remains connected to an AP even when more roaming options are available to improve the RSSI by more than 6 dBm.

Table 3: Wireless SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
Throughput	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 number of Mbps to use as the success threshold for this SLE.	Network Issues	Low throughput due to the capacity of the wired network
		Coverage	Low throughput due to weak signal strength
		Device Capability	Low throughput 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 due to either excessive load on the AP or interference on the channel. Sub-Classifiers: • High Bandwidth Utilization • Non Wi-Fi Interference • Excessive Client Load • Wi-Fi Interference
Capacity	Juniper Mist monitors the percentage of the total RF channel capacity that is available to clients.	Non-Wi-Fi Interference	Low capacity due to interference from non-Wi-Fi sources
		Client Usage	Low capacity due to a high client load

Table 3: Wireless SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
	You can click the **Settings** button to set the percentage of the RF channel capacity (bandwidth) that must be available to clients at any time.	Wi-Fi interference	Low capacity due to wireless interference
		Client Count	Low capacity due to a high number of attached clients
AP Health	Juniper Mist tracks the percentage of time the APs are operational without rebooting or losing connectivity to the cloud.	Low Power	Insufficient power received from the PoE connection
		AP Disconnected	Disconnection due to one of these issues: • 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.

Table 3: Wireless SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
		Ethernet	Ethernet connectivity issues due to one of these issues: • 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	Network-related issues due to round-trip time, packet loss, and Mist Edge tunnel unreachability. Sub-Classifiers: • Latency • Jitter • Tunnel Down

Wired SLEs

SUMMARY

Use 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

Overview

IN THIS SECTION

Juniper Mist™ cloud continuously collects network telemetry data and uses machine learning (ML) to analyze the end-user experience. This service efficiently collects and analyzes data your entire network, whether you have hundreds or thousands of ports.

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. It's not merely a matter of devices or links being up or down—it's the quality of the client experience.

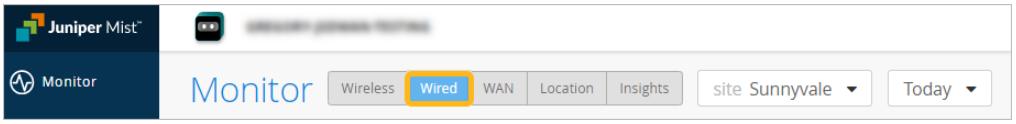
For the wired network, the two burning questions are:

- Are clients able to connect?
- Are clients able to pass traffic after connecting?

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.

Root Cause Analysis for the Wired Successful Connect SLE

After you click a classifier in the SLE block, you'll see the Root Cause Analysis page. Click classifiers and sub-classifiers to view timeline and scope information in the lower half of the screen.

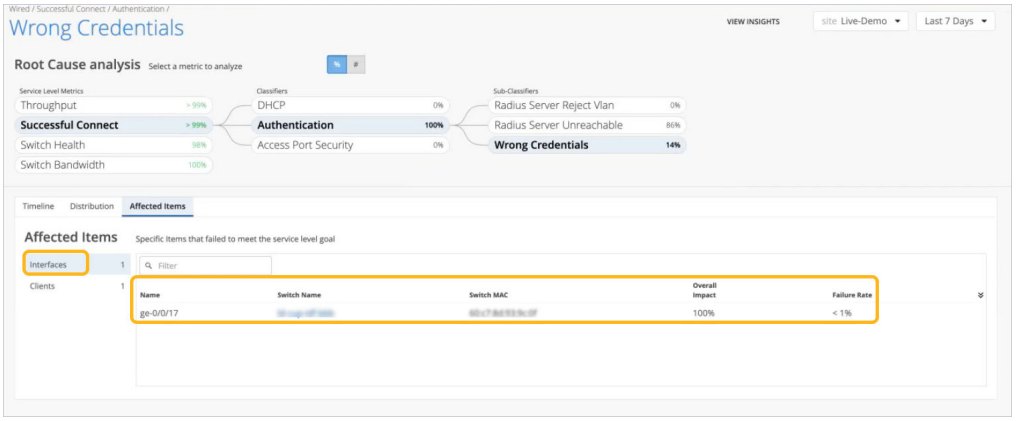
NOTE: The information in the lower half of the screen depends on what you've selected at the top.

Useful tabs in the lower half of the screen are:

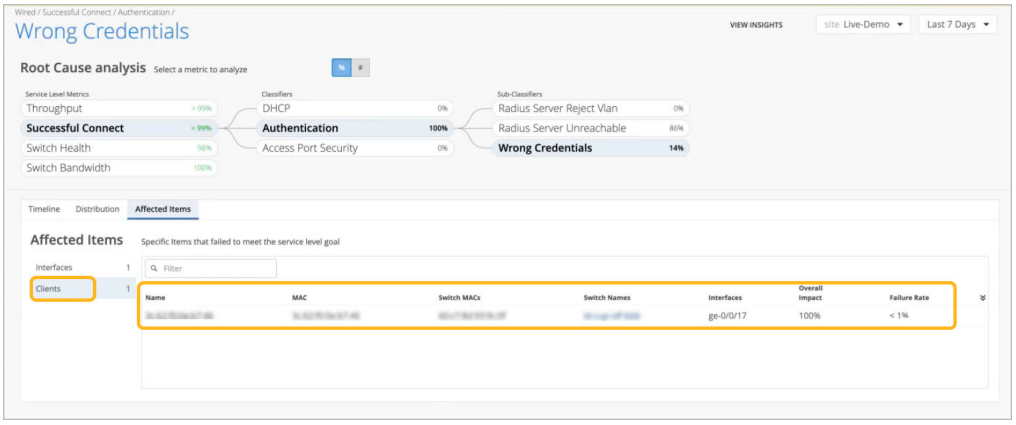
- Timeline—See exactly when the issues occurred.
- Distribution—See which VLANs were affected.
- Affected Items—See which interfaces and clients were affected and how much each one contributed to the overall impact. Also see the individual failure rate for each interface or client.

Let's look at an example for the Successful Connect SLE. By clicking options at the top of the page, you can drill down from the SLE to classifiers and sub-classifiers. The lower half of the page shows information relevant to these selections.

By selecting the **Affected Items** tab and then clicking the **Interfaces** option on the left, we see the interfaces that were unable to connect due to incorrect credentials.



By clicking the **Clients** tab on the left, we now see the affected clients.



TIP:

- **Overall Impact** is the percentage that a client or interface contributed to *all* issues for the selected sub-classifier. For example, it can show if a client account for 20 percent or 90 percent of the issues.
- **Failure Rate** is the impact of this issue on this interface or client. For example, it can show if an interface was unsuccessful on 20 percent or 90 percent of connection attempts.
- To see more details, click the hyperlinks in the table to go to the Insights page, where you can see all client and switch events.

Wired Assurance: Day 2 - Wired SLEs Video Overview

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

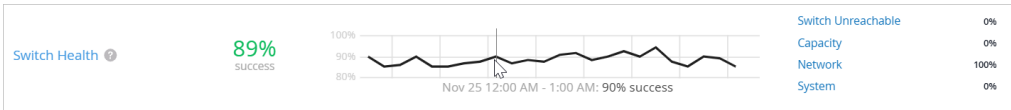
Wired SLE Blocks

As shown in the following example, each SLE block provides valuable information.

- At the left, you see that this SLE has an 89 percent success rate.

  At the center, the timeline shows variations across the time period. You can hover your mouse pointer over any point to see the exact time and SLE outcome.

  At the right, the classifiers show what percentage of issues were attributable to each root cause. In this example, 100 percent of the issues were attributed to Network.



If you click a classifier, you'll see more information on the Root Cause Analysis page. Most classifiers have sub-classifiers for greater insight into the exact causes of issues.

The following table provides more information about the wired SLEs and classifiers.

Table 4: Wired SLE Descriptions

SLE	SLE Description	Classifier	Classifier Description
Successful Connect	Juniper Mist monitors client connection attempts and identifies failures. The source of data is 802.1X events on the switch. This SLE helps you to assess the impact of these failures and to identify the root causes to address. This SLE is available if you use 802.1X on the wired network to authenticate clients or if you have DHCP snooping configured. You cannot set the threshold for this SLE. It's assumed that you want 100 percent successful	DHCP	Client connections that fail to reach the bound state within a minute. This classifier is available only when DHCP snooping is enabled in the port profile. DHCP snooping might not always work well with endpoints that have static IPs.

Table 4: Wired SLE Descriptions *(Continued)*

SLE	SLE Description	Classifier	Classifier Description
	connects and consider any unsuccessful connect as a critical issue to track.	Authentication	Events when a client failed to authenticate. Sub-Classifiers: • RADIUS Server Reject VLAN—Couldn't authenticate to the specified VLAN. • Wrong Credentials—The credentials weren't valid. • RADIUS Server Unreachable—The RADIUS server was down.

Table 4: Wired SLE Descriptions *(Continued)*

SLE	SLE Description	Classifier	Classifier Description
		Access Port Security	Client connection failures caused by access port security issues. Based on the security features configured in your port profiles, this classifier is triggered as security events occur. Sub-Classifiers: • BPDU-Guard—Detects connection failures because of the BPDU guard configuration on the switch port. This feature is important to prevent looping, as when a switch is connected to a switch. To enable this feature, go to the port profile, and enable STP Edge. • MAC Limit—Detects connection failures reported when a client exceeds the MAC limit configured on the switch port. For example, you might configure your port profile with a MAC limit of 2 if you have an outdoor security camera or public address system and want to prevent other devices from connecting to that

Table 4: Wired SLE Descriptions *(Continued)*

SLE	SLE Description	Classifier	Classifier Description
			port. If someone unplugs your camera and attempts to connect their own device, the MAC limit would be reached, and this event would be reflected by the MAC limit classifier. • Dynamic ARP Inspection—Identifies client connection failures when a port drops invalid Dynamic ARP Inspection packets. This security feature prevents people from snooping for someone else's ARP address to gain access. Requires enabling ARP Inspection in the DHCP Snooping section of the port profile. • Rogue DHCP Server—Identifies client connection failures caused by a rogue DHCP server event. This could be an event where an untrusted port drops traffic from DHCP servers to block unauthorized servers. Enabling this feature can prevent rogue devices from

Table 4: Wired SLE Descriptions *(Continued)*

SLE	SLE Description	Classifier	Classifier Description
			connecting. This classifier shows any such attempts that occur. Requires enabling DHCP snooping in the port profile.
Throughput	This SLE represents the ability of wired users to pass traffic without impedance. You cannot set the threshold for this SLE. It's assumed that you want 100 percent of traffic to pass without impedance and consider any impedance as a critical issue to track.	Storm Control	Events when storm control level was exceeded and packets were dropped. Available only if you've enabled Storm Control in the port profile (recommended).

Table 4: Wired SLE Descriptions *(Continued)*

SLE	SLE Description	Classifier	Classifier Description
		Interface Anomalies	Events when devices were powered up but could not pass traffic. Sub-Classifiers: • **Cable Issues**—This sub-classifier shows the user minutes affected by faulty cables in the network. Cable issues can cause a high failure rate on an interface or client device. • **Negotiation Failed**—This sub-classifier identifies bad user minutes caused by issues such as incomplete negotiation, duplex conflict, and latency. • **MTU Mismatch**—This sub-classifier identifies issues where MTU size is mismatched somewhere along the packet's path (any MTU mismatch along the path will result in discarded or fragmented packets). The information for this SLE comes from the switch; each input error or MTU error contributes to a bad

Table 4: Wired SLE Descriptions *(Continued)*

SLE	SLE Description	Classifier	Classifier Description
			user minute under this sub-classifier.
Switch Bandwidth	Juniper Mist™ measures the available bandwidth on your network based on the queued packets and dropped packets for each configured queue. A pattern of low success rates can indicate a need for more wired bandwidth. You can click the **Settings** button to set the percentage to use as the success threshold for this SLE. This percentage represents the total_DropppedPackets as a portion of total_QueuedPackets.	Congestion	Heavy congestion causing dropped packets (TxDrops) when the input queue (buffer) fills up. Triggered by considering these ratios: • 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.

Table 4: Wired SLE Descriptions *(Continued)*

SLE	SLE Description	Classifier	Classifier Description
		Congestion Uplink	High congestion on uplinks with these uplink port characteristics: • Has a switch or a router as an LLDP neighbor • Is a Spanning Tree Protocol (STP) root port • Has a higher number of transmitted and received packets compared to the other ports • Experiencing congestion due to aggregated Ethernet links and module ports
		Bandwidth Headroom	High bandwidth usage.
Switch Health	Juniper Mist™ monitors your switches' operating temperature, power consumption, CPU, and memory usage. Monitoring switch health is crucial because issues such as high CPU usage can directly impact connected clients. For example, if CPU utilization spikes to 100 percent, the connected APs might lose	Switch Unreachable	Poor switch-to-cloud connectivity. The switch might be down, or the connection might be severed.

Table 4: Wired SLE Descriptions *(Continued)*

SLE	SLE Description	Classifier	Classifier Description
	connectivity, affecting the clients' experience.	Capacity	Usage exceeding 80 percent. High usage can indicate that the switch is dealing with more requests that it can optimally handle. Sub-Classifiers indicate usages exceeding 90 percent of the relevant table capacity: • ARP Table • Route Table • MAC Table
		Network	Lower than expected throughput due to uplink capacity limitations. Based on the round-trip time (RTT) value of packets sent from the switch to the Mist cloud. Sub-Classifiers: • **WAN Latency**—Based on the average value of RTT over a period of time. • **WAN Jitter**—Calculated by comparing the standard deviation of RTT within a small period with the overall deviation of RTT over a longer period.

Table 4: Wired SLE Descriptions *(Continued)*

SLE	SLE Description	Classifier	Classifier Description
		System	Issues on the switch that can impact user experiences Sub-Classifiers: • **CPU**—Utilization above 90 percent • **Memory**—Utilization above 80 percent • **Temp**—Temperature above or below the specified operating range • **Power**—Consumption above 90 percent of the available power

WAN SLEs

SUMMARY

Use the WAN Service-Level Experiences (SLEs) to assess user-impacting factors such as WAN Edge health, WAN link health, and application health.

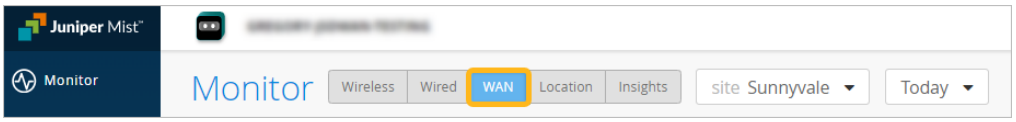
IN THIS SECTION

Overview

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.

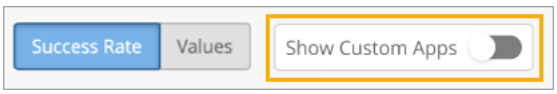


NOTE: The buttons appear only if you have the required subscriptions. See Requirements.

SLE Filter Buttons

- Use the buttons on the left to show **Success Rate** or **Values**.
- Use the **Show Custom Apps**button to show or hide your custom applications.

  In the example below, the button is in the Off position, so all applications are included. If you drag the button to the **On** position, you'll see only your custom applications.



Video: WAN Assurance Overview

Video: WAN Assurance Video Overview

Video: Troubleshoot WAN Issues with SLEs

Video: SLE Example

WAN SLE Blocks

As shown in the following example, each SLE block provides valuable information.

- At the left, you see that this SLE has an 85 percent success rate. If you select the Value filter button, you'll see a number instead.
- At the center, the timeline shows variations across the time period. You can hover your mouse pointer over any point to see the exact time and SLE outcome.

  At the right, the classifiers show the percentage of the issues that were attributed to each root cause. In this example, 100 percent of the issues were attributed to Jitter.

- If you click a classifier, you'll see more information on the Root Cause Analysis page. Most classifiers have sub-classifiers for greater insight into the exact causes. The Root Cause Analysis page also provides additional details about the scope and impact of the issues.

See the following table for more information about the WAN SLEs and classifiers.

Table 5: WAN SLE Descriptions

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
WAN Edge Health	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, directly affecting any clients connected to the device.	WAN Edge Disconnected	Lost connectivity to the Juniper Mist cloud

Table 5: WAN SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
		System	High system usage relative to capacity Sub-Classifiers: • Memory—Memory utilization above 80 percent • Power—Power consumption above 90 percent • Temp CPU—CPU temperature outside the prescribed threshold range • Temp Chassis—Chassis temperature outside the prescribed threshold range • **CPU Data Plane**—CPU Data Plane utilization above 90 percent • CPU Control Plane—CPU control plane utilization above 90 percent

Table 5: WAN SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
		Table Capacity	High number of table entries relative to capacity Sub-Classifiers: • Flow—Session flow table utilization • FIB—Forwarding Information Base (FIB) table utilization
		DHCP Pool	High DHCP utilization relative to pool size Sub-Classifiers: • DHCP Denied • DHCP Headroom

Table 5: WAN SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
WAN Link Health	Juniper Mist monitors the user minutes when the WAN link's 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.	Network	Network issues Sub-Classifiers: • 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 • 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. • Loss—Lost packets

Table 5: WAN SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
		Interface	Interface issues Sub-Classifiers: • Congestion—High 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 • VPN • Port Down • Negotiation Incomplete (SRX only)
WAN Application Health	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.	Jitter	Inconsistent packet transmit times
		Latency	Slow response time (lag)
		Loss	Packet loss

Table 5: WAN SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
	Performance metrics vary by device: • SSR—Values come from the Session Smart bidirectional forward detection between peers • SRX—Values come from variation detection against RTT, lost packets, and latency above the RTT For fine-tuning, you can click the **Settings** button to select individual applications to include or exclude.	Application Services (SSR only)	Issues such as slow responses to application requests, recurring disconnects, and insufficient bandwidth Sub-Classifiers: • Slow Application • Application Bandwidth • Application Disconnects

Table 5: WAN SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
Gateway Bandwidth	Juniper Mist evaluates the IPsec overlay that constitutes the SD-WAN. Use this SLE to determine if you need more WAN bandwidth on your site.	Bandwidth Headroom	Current usage exceeding the baseline, which is determined by the highest usage over the past 14 days If you've enabled automatic speed tests, these results also are incorporated into the Bandwidth Headroom classifier. In this case, the headroom threshold is based on maximum usage and the speed test results, if available. Speed tests occur if configured in your organization settings and if enabled in the WAN settings for the WAN Edge template, hub profile, or WAN Edge device.
		Congestion Uplink (SRX Only)	High ratio of total transmitted bytes dropped (TX drops) to total packets transmitted (TX packets).

Location SLEs

SUMMARY

Use the Location Service Level Experiences (SLE) dashboard to assess the service levels for user-impacting factors such as SDK connection issues, latency, dropped requests, access point health, and more.

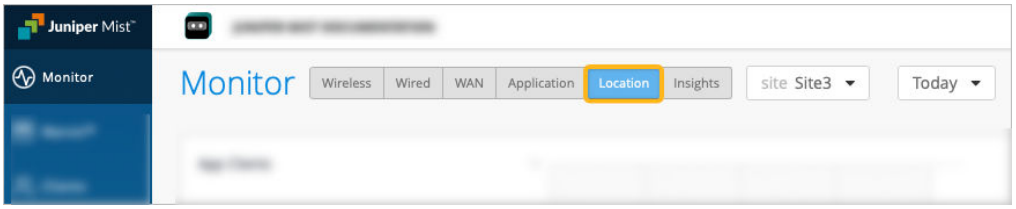
IN THIS SECTION

Overview

IN THIS SECTION

Finding the Location SLEs Dashboard

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



NOTE: Your subscriptions determine which buttons appear.

Success Threshold Settings

You can adjust the thresholds that determine success or failure. To do so, click the **Settings** button at the right top corner of the location SLEs section. In the settings window, follow the on-screen instructions to set each threshold.

NOTE: Most SLEs allow you to increase or decrease the threshold. Certain SLEs are not adjustable.

Location SLE Blocks

As shown in the following example, each SLE block provides valuable information.

- At the left, you see that this SLE has a 77 percent success rate. If you select the Value filter button, you'll see a number instead.
- At the center, the timeline shows variations across the time period. You can hover your mouse pointer over any point to see the exact time and SLE outcome.

  At the right, the classifiers show the percentage of the issues that were attributed to each root cause. In this example, the issues were almost evenly distributed among Beam Density (33 percent of the issues), Beacon Density (33 percent), and Weak RSSI (32 percent). Another 2 percent of issues were attributed to Machine Learning.

- If you click a classifier, you'll see more information on the Root Cause Analysis page. Most classifiers have sub-classifiers for greater insight into the exact causes. The Root Cause Analysis page also provides additional details about the scope and impact of the issues. For all location SLEs, the Root Cause Analysis page includes a Location tab, where you can see exactly where the issues occurred on your floor plans.

See the following table for more information about the location SLEs and classifiers.

Table 6: Location SLE Descriptions

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
SDK Connect Time	Juniper Mist measures the time when your SDK-enabled app clients are connected to location services at your site.	User Usage	Incidents when the client connection time was below the threshold. For example, if you set the threshold to 60 seconds (by clicking the **Settings** button), then this classifier is triggered when a client is connected for less than a minute.
Latency	Juniper Mist measures the latency of location responses and estimates to app clients.	Cellular	Latency on a cellular data connection
		WiFi	Latency on a wireless connection
		No Reported Connection Type	Latency with unknown connection type
Teleports	Juniper Mist identifies instances when the app client's estimated location veers away (or "teleports") from the actual location. For example, if you set 3 meters as the service target, this SLE is triggered when the actual location is more than 3 meters from the estimated location.	Beacon Density	The app client detected a low number of beacons from the access points (APs).
		Beam Density	The app client detected a low number of beams.
		Machine Learning	—Changes in machine learning affected location accuracy.

Table 6: Location SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
		vBLE Placement	The placement of the APs affected location accuracy. Sub-Classifiers: • Device Sensor—Sensor issues in the device affected location accuracy with respect to motion, acceleration, etc. • Weak RSSI—The app client received a weak signal (low Received Signal Strength Indicator).
Dropped Requests	Juniper Mist monitors the instances when dropped location requests reduced location accuracy. The Pending Requests classifier uses the threshold that you set with the **Settings** button. The other classifiers act on a pass/fail basing, counting any incidents that result in dropped requests.	Reconnects	Reconnection attempts made after losing Internet connectivity
		Offline	App offline due to issues such as Wi-Fi reception, poor cellular reception, connectivity problems, or user actions (for example, switching to airplane mode)
		Not Uniform Requests	Inconsistent speeds when sending location requests The app relies on uniform requests for location accuracy.

Table 6: Location SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
		Dropped by Network	Network issues causing dropped requests
		Client Request Timeout	Client timeouts causing dropped requests
		Cellular	Dropped requests while using a cellular data connection
		WiFi	Dropped requests while using a Wi-Fi connection
		Pending Requests	Excess requests above the configured SLE threshold A high number of pending requests is used as an indicator that future requests are likely to be dropped.
AP Health	Juniper Mist counts the incidents when APs rebooted or lost connectivity to the cloud.	Low Power	Insufficient power for location features
		AP Disconnected	Disconnected from cloud due to issues such as site down, switch down, AP reboot, or AP unreachable
		Ethernet	Ethernet errors or speed mismatch
		Network	Issues such as tunnel down, latency, or jitter

Application SLEs

SUMMARY

Use the application experience and service-level expectations (SLE) dashboard to assess the service levels for user-impacting factors such as signal strength, RF channel capacity, client CPU utilization, and more.

IN THIS SECTION

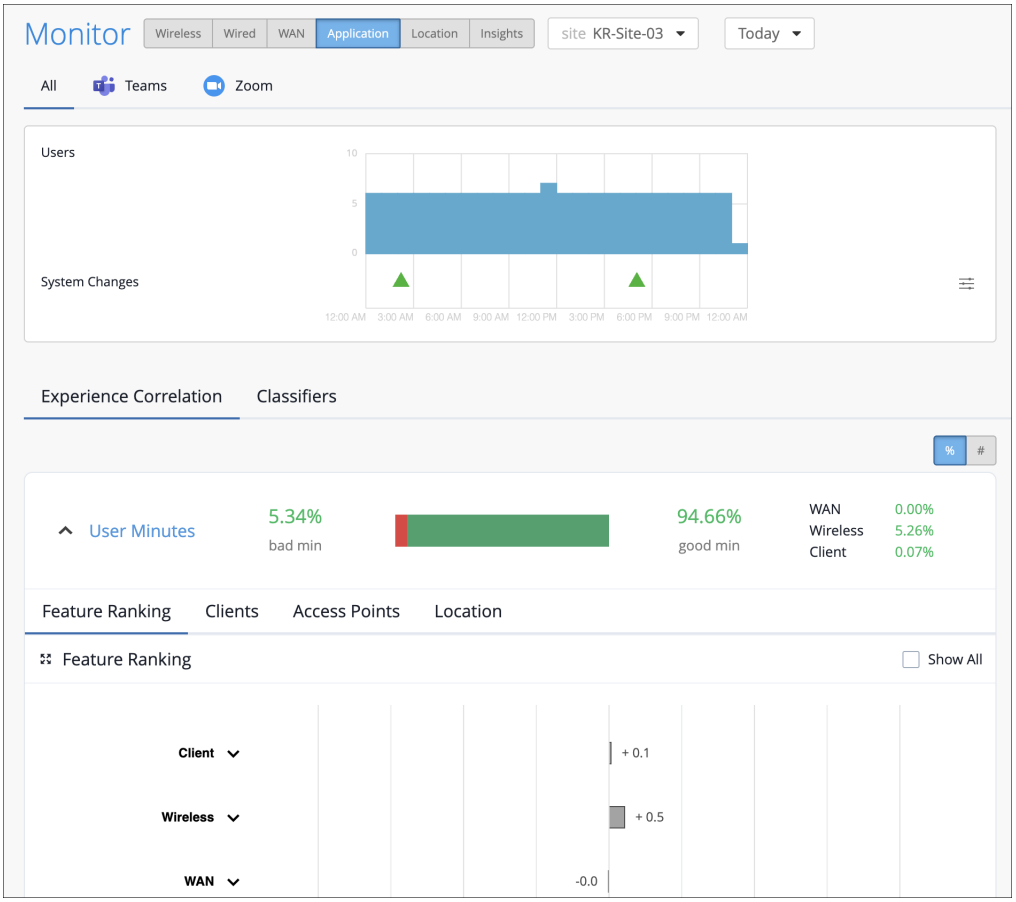
Overview

IN THIS SECTION

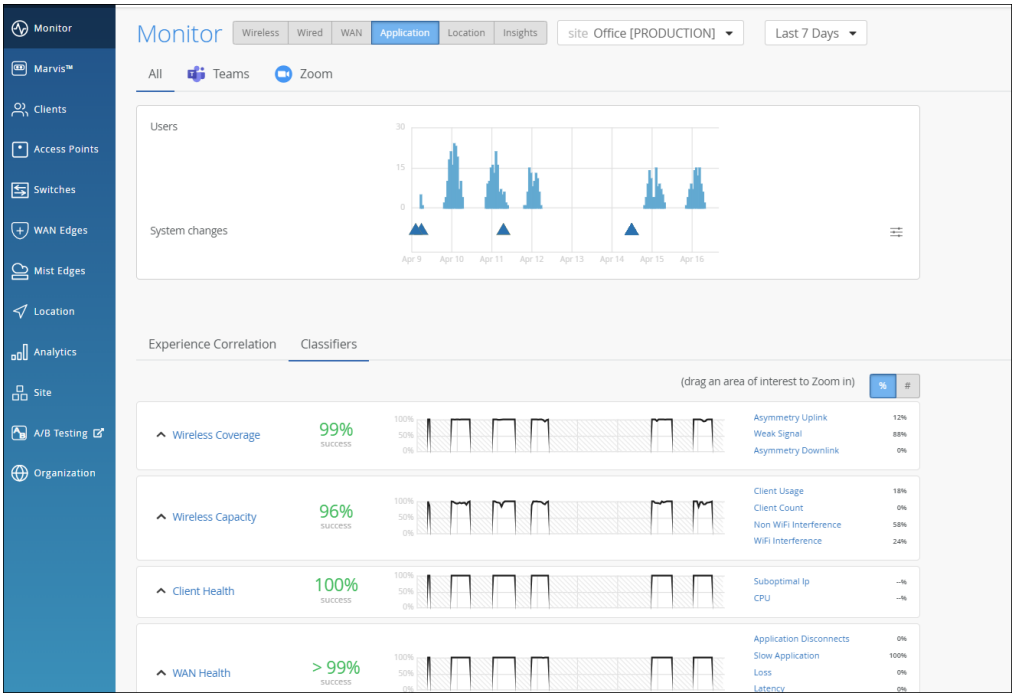
Monitoring network performance is crucial for any organization as a healthy network is key to the performance of applications. Monitoring the network performance requires you to assess multiple network aspects using reliable performance indicators. However, efficient assessment and reporting of network performance at an organization level continues to be a challenge.

Juniper Mist™ provides a cloud-to-cloud integration with Zoom and Microsoft Teams to analyze, correlate, and classify collaboration user experience based on correlation of network parameters both at the site level and organization level. Using this information, Juniper Mist provides an assessment of the quality of user experience on your network. Zoom and Microsoft Teams applications are sensitive to any network changes and play a key role in determining the user experience. A measure of how well these application user minutes are performing acts as a third-party report card for your network. The absence of any Zoom and Teams issues on a network indicates that all other user applications are probably performing well.

Juniper Mist identifies various factors contributing to a bad user experience and provides a site-level or organization-level experience correlation of the bad user minutes experienced by all users. The Application Experience dashboard provides a Shapley feature ranking that helps determine the contribution of network parameters towards a negative user experience.

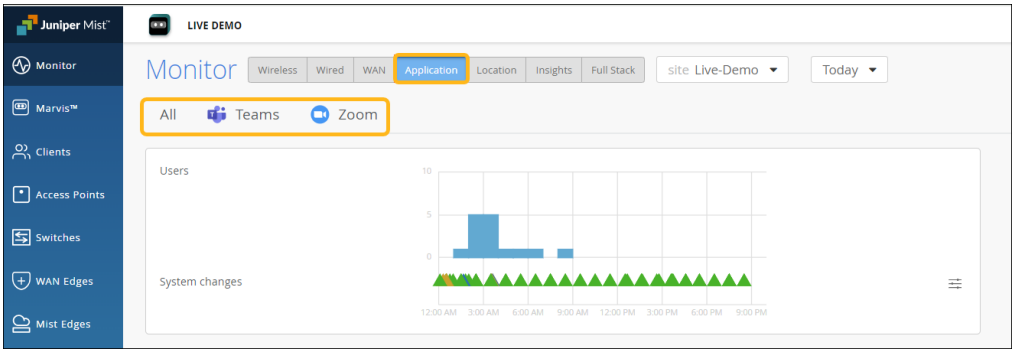


In addition, service level metrics provide visibility into how the users are experiencing the network and help you to proactively address issues.



Finding the Application Experience Correlation and Classifiers View

To find the Application Experience Correlation and Classifiers view, select **Monitor** > **Service Levels** from the left menu of the Juniper Mist portal, and then select the **Application** button.



NOTE: Your subscriptions determine which SLE buttons appear. The **Application** button is available when you have a Marvis for Wireless subscription. In addition, you'll also need to integrate your Zoom or Teams account with Juniper Mist. See Zoom Integration Overview and Microsoft Teams Integration Overview.

Application Experience Correlation

IN THIS SECTION

Juniper Mist collects information such as latency, packet loss, and jitter experienced by every user during a Teams or Zoom session. It correlates this information against the network parameters to identify the root cause for a bad user experience. Juniper Mist then aggregates this individual user information to provide insights into the quality of Teams or Zoom application user experiences at a site or an organization level.

Experience Correlation

Experience correlation provides visibility into the performance of Teams and Zoom applications at a site or an organization level. With detailed insights into the factors impacting the application quality, the correlation data helps network administrators to quickly identify issues causing bad user experiences across a site or an entire organization.

Use the feature ranking graph to identify which features contributed the most to an issue, Also view the insights for the impacted clients and the APs that they're connected to. If clients experience degraded Zoom or Teams call quality, use the experience correlation at the site level to easily identify which APs are involved.

As Juniper Mist provides the correlation based on the latency, loss, and jitter data it fetches from the third-party applications (Zoom and Teams), fewer bad user minutes also serve as a third-party validation of your network.

The feature ranking (Shapley) helps you to troubleshoot Zoom or Teams sessions by ranking the impact of each network feature on the sessions. You can read more about the Shapley feature ranking in Troubleshoot Zoom Sessions Using Shapley Feature Ranking.

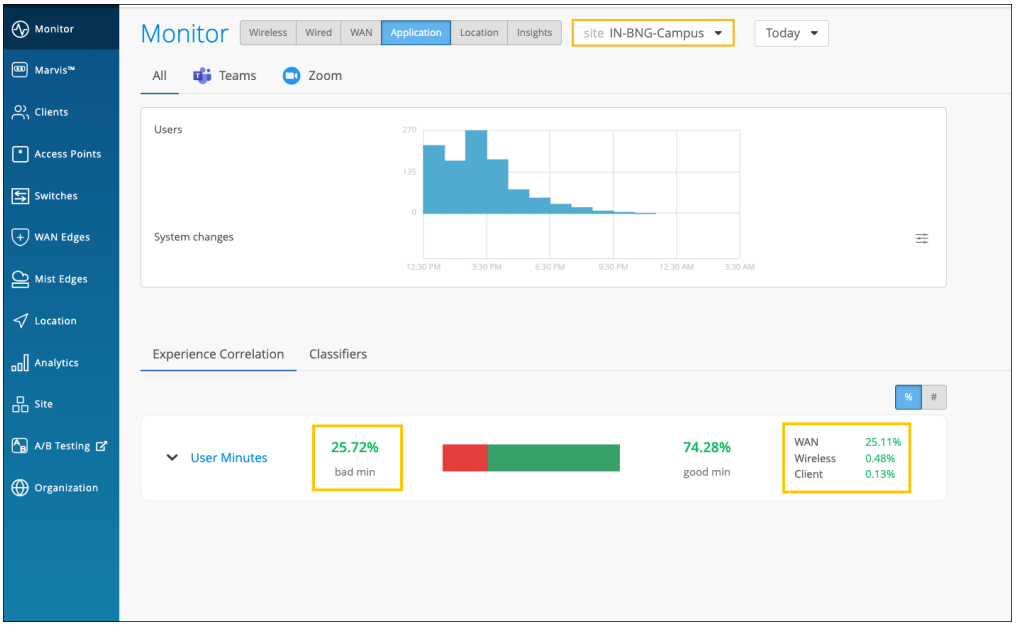
To understand how you can integrate the Teams and Zoom applications with Juniper Mist, see:

- Integrate Your Microsoft Teams Account with Mist
- Integrate Your Zoom Account with Mist

Site-Level Application Experience Correlation

The Experience Correlation section provides an aggregate of the total good and bad user minutes experienced by all users in a site for a specific duration. It also provides granularity by providing a breakup of the bad user minutes based on the factors that contributed to it—WAN, wireless, or client.

To view the site-level application correlation, select the site and the duration. Here's an example. You can see the good and bad user minutes listed for the site. You can also see the distribution of the bad user minutes across the WAN, Wireless, and Client categories, with WAN contributing the most.

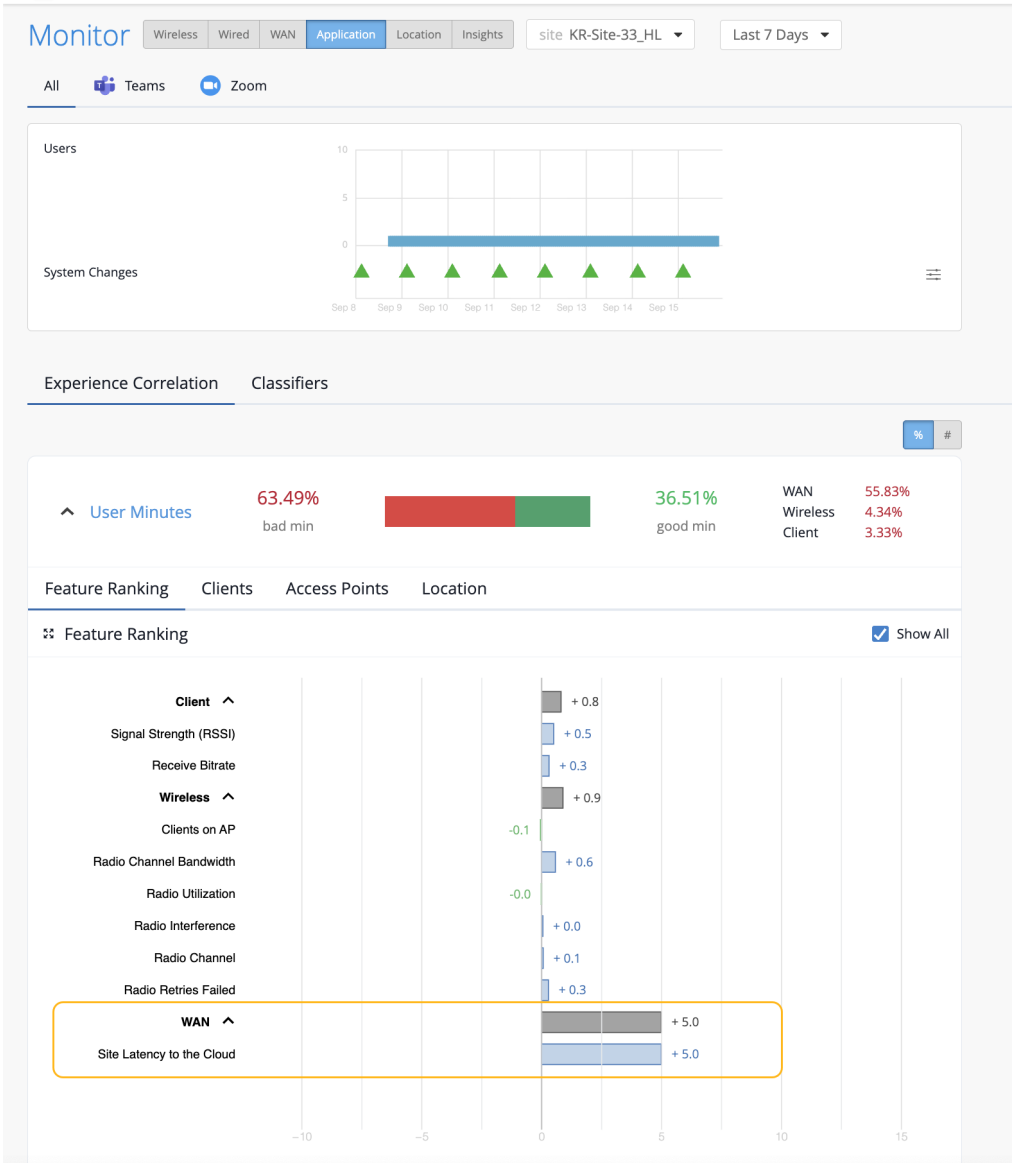


You can further expand **User Minutes** to view the following information:

- **Feature ranking**—Provides a Shapley feature ranking graph computed based on the latency, packet loss, and jitter for every user minute. As shown in the following example, you can expand the Client, Wireless, and WAN categories to drill down to the network feature that is contributing the most to the issue.

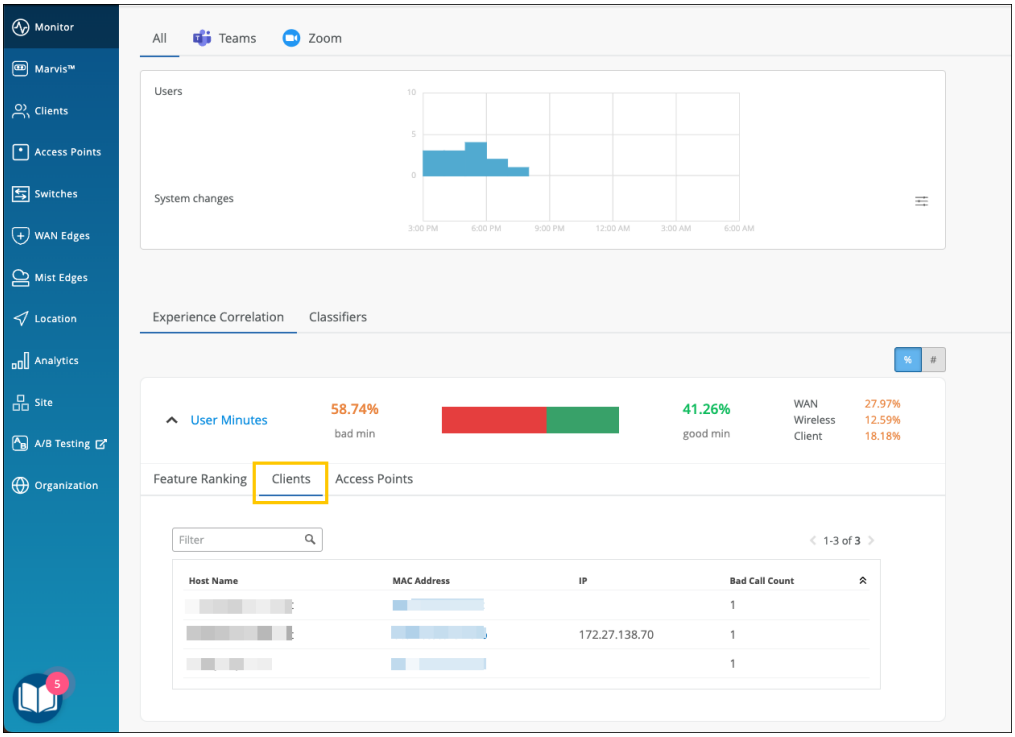
  Each contributing feature for bad user minutes is ranked in terms of the additional latency that it adds to the Zoom or Teams call. The increase in latency for each contributing feature is measured against the site average latency.

  In the following example, you'll notice that WAN is contributing the most to the issue.

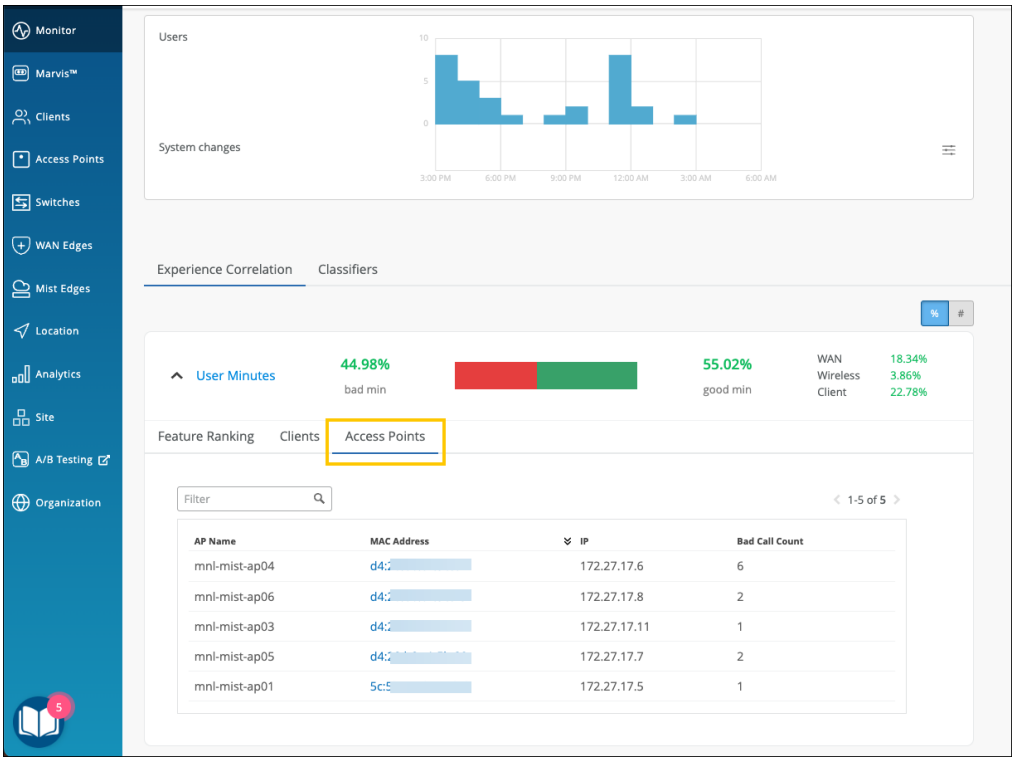


When you expand the categories, you see that the site latency is the major contributing factor to the increased call latency. Based on this information, you can look at the site WAN uplink metrics to confirm the issue and take necessary action.

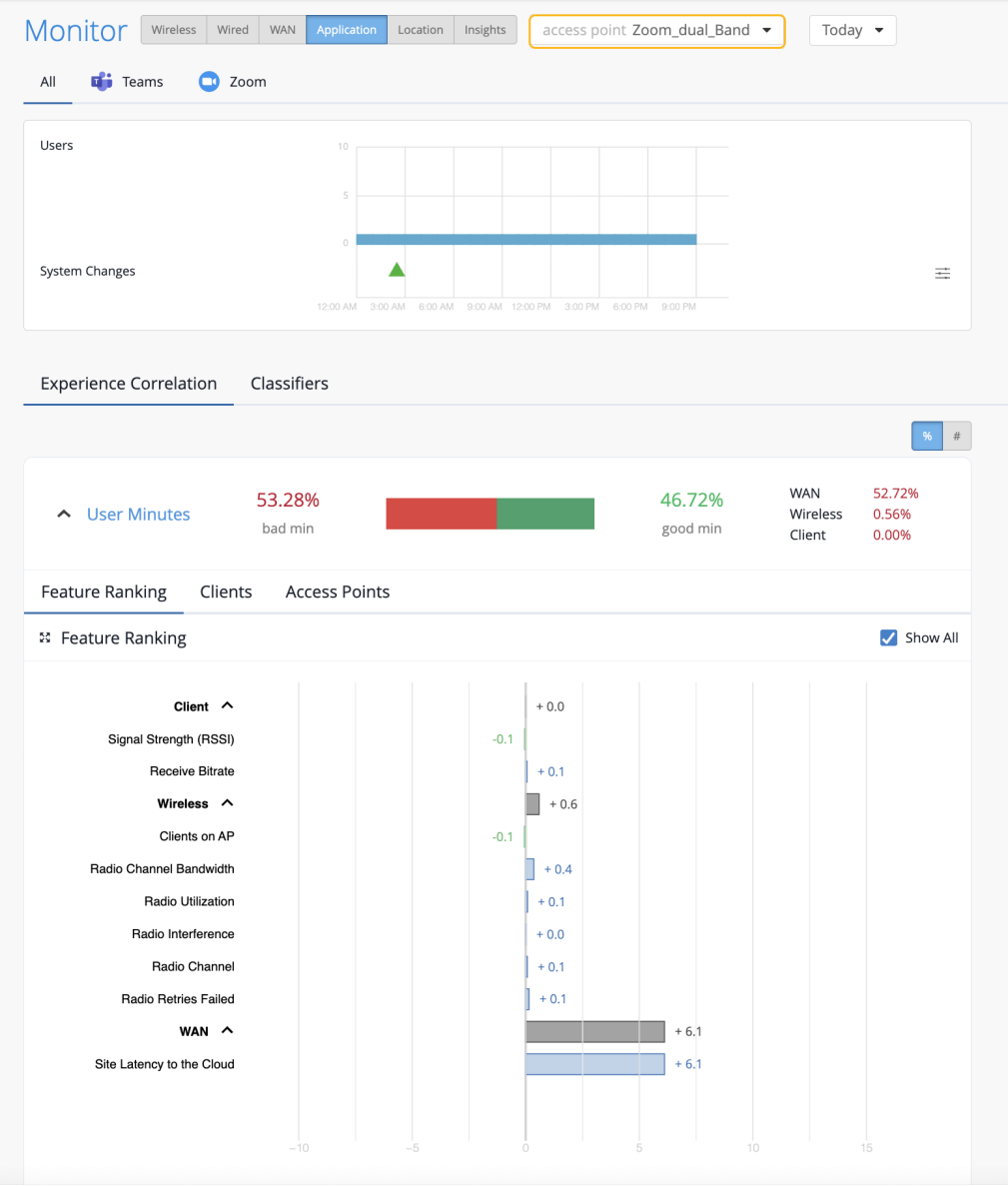
- **Clients**—The Clients tab displays the users that experienced bad user minutes and lists the number of bad call occurrences. Click the MAC address to go into the individual client insights page to view the meeting details, Shapley feature ranking, and pre and post connection metrics for the client. If you look through the list of affected clients for a specific duration (for example, last 24 hours, yesterday, 7 days), you can identify clients that faced a bad user experience consistently. You can also obtain information by entering 'list bad zoom calls for last 7 days' or 'list bad Teams calls for last 7 days' in the Marvis conversational assistant. You can also view the details for a site or a specific user—for example, 'list bad zoom calls for host-abc for last 7 days'.



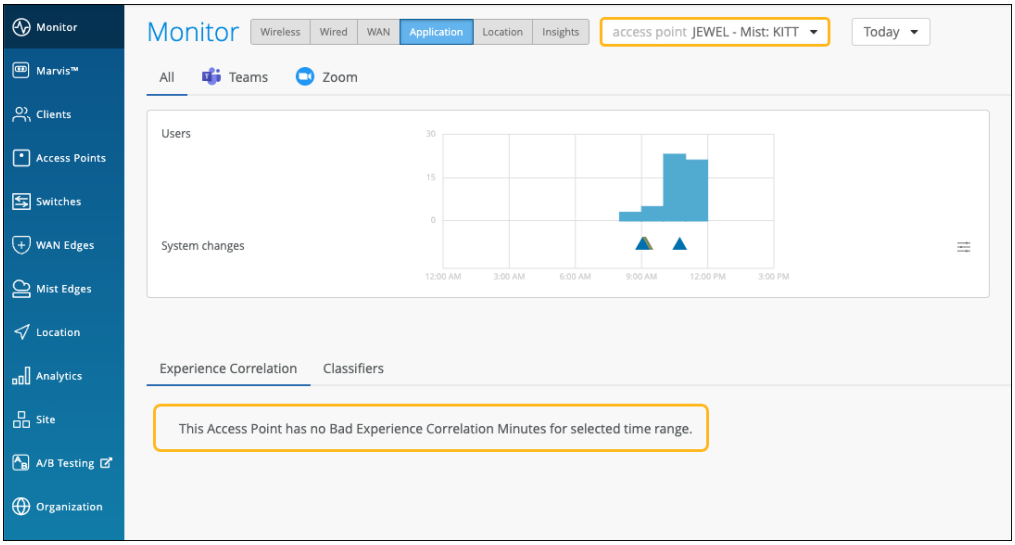
- **Access Points**—Shows the APs that the users were connected to when issues occurred. You can click the MAC address of an individual AP to view the insights.



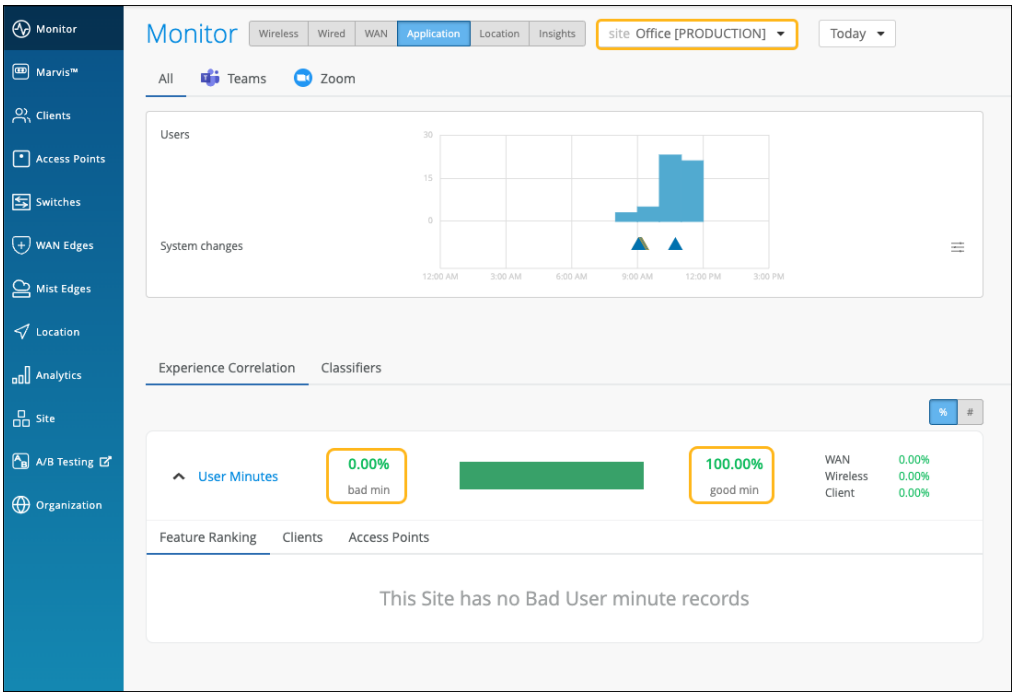
You can also select the individual AP from the drop-down list on the top. Juniper Mist will list the feature ranking specific to the selected AP and its connected clients that experienced the issue.



In the following example, the users connected to the selected AP did not experience any bad user minutes.



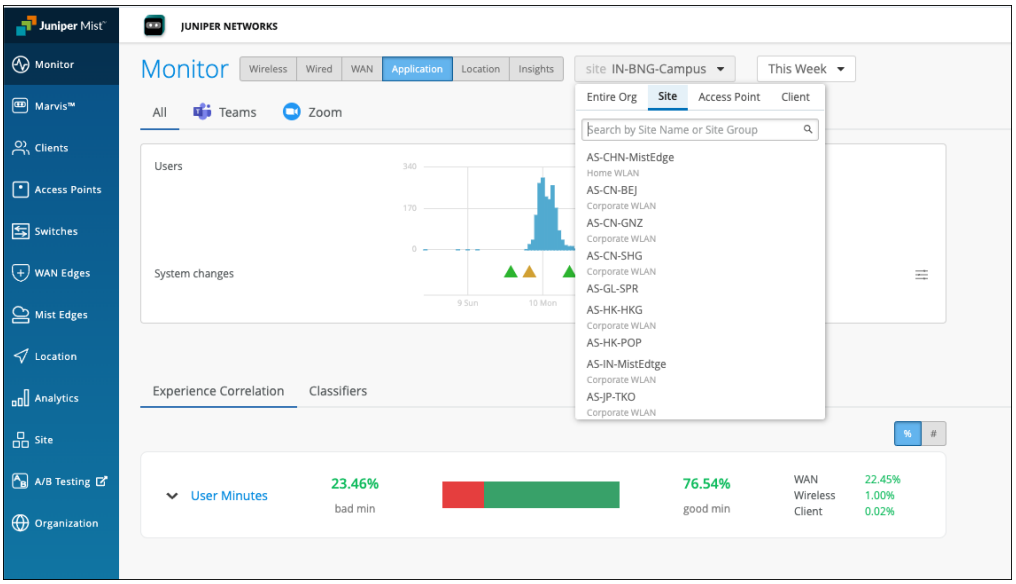
If all users connected to an AP do not experience any bad user minutes, then you'll see the page like the following example.



Organization-Level Application Experience Correlation

Juniper Mist also provides an aggregated view of all affected sites at an organization level. Using this data, you can identify sites where users are facing issues consistently for a specific duration. You can also determine the dominant feature for the bad experience along with the total number of clients and APs involved.

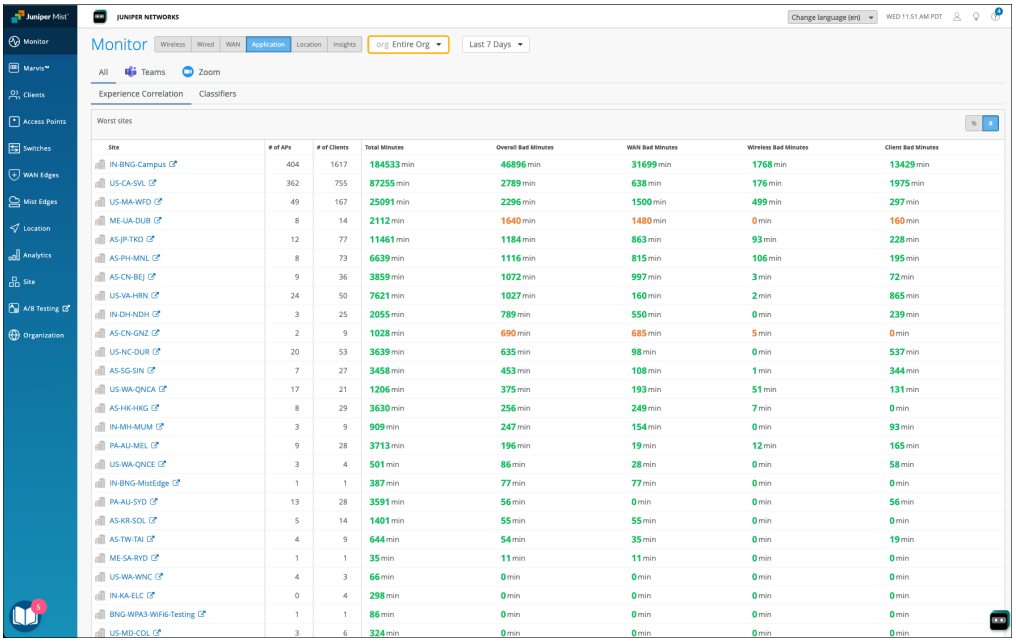
In the Application Experience Correlation page, select the organization and time duration for which you want to view the data.



You'll see a list of all sites that experienced bad user minutes. You can click a site to view the details.

In the following example, you see the sites with bad user experience and the total bad minutes for the WAN, Wireless, and Client categories. At an organization level, this type of data helps the networking teams to enhance and optimize the network, WAN links and any increased client CPU or memory utilization that could be causing the problem.

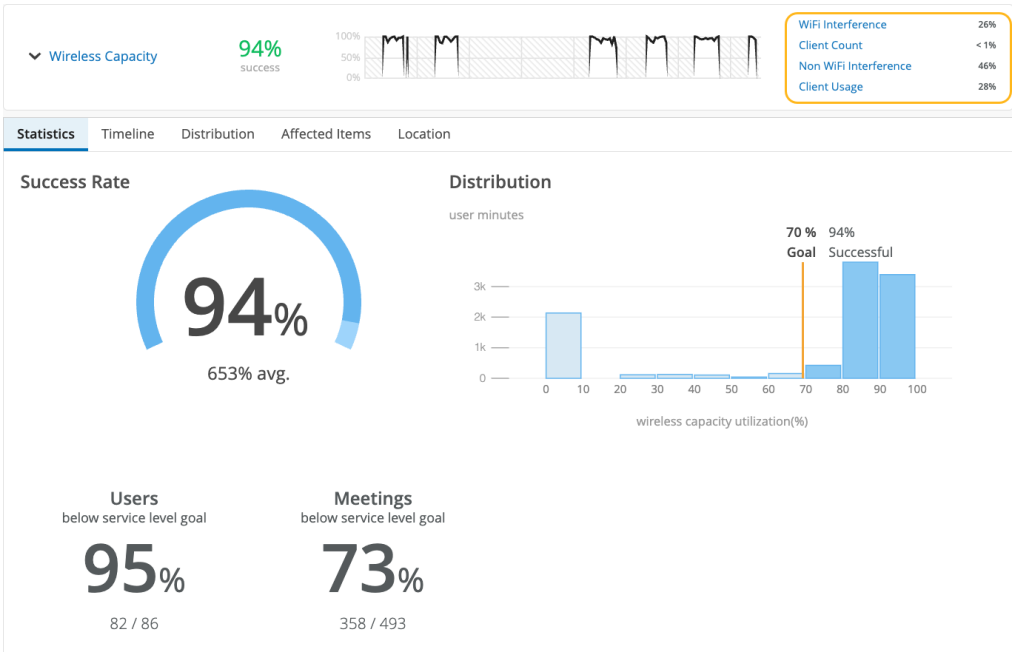
Zoom and Teams applications are sensitive to any network changes. Viewing application performance at an organization level is essential for assessing and improving the user experience.



Application SLE Blocks

As shown in the following example, each SLE block provides valuable information.

- At the left, you see that this SLE has a 94 percent success rate. If you select the Value filter button, you'll see a number instead.
- At the center, the timeline shows variations across the time period. You can hover your mouse pointer over any point to see the exact time and SLE outcome.
- At the right, the classifiers show the percentage of the issues that were attributed to each root cause. In this example, 46 percent of issues were attributed to non-Wi-Fi interference. The remaining issues were due to Wi-Fi Interference and Client Usage.



- By clicking the down arrow next to the SLE name, you can see additional information, such as the timeline, distribution, affected items, and the client locations on your floorplan.

See the following table for more information about the application SLEs and classifiers.

Table 7: Application SLEs and Classifiers

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
Wireless Coverage (for Applications)	Juniper Mist tracks active clients' Received Signal Strength Indicator (RSSI),	Weak Signal	Unknown causes of weak signal

Table 7: Application SLEs and Classifiers *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
	as measured by the access point for the duration of the Zoom or Teams call. A low RSSI impacts the quality of the audio or video during a Zoom or Teams call. You can use this SLE to determine if you have sufficient access points.	Asymmetry Downlink	Weak signal due to asymmetric transmission strength from the AP to the client
		Asymmetry Uplink	Weak signal due to asymmetric transmission strength from the client to the AP Asymmetry can occur for various reasons, such as clients being too far from the AP.
Wireless Capacity (for Applications)	Juniper Mist monitors the percentage of the total RF channel capacity that is available to clients for the duration of the Zoom or Teams call. When the capacity threshold for a Zoom or Teams user minute is less than MOS 3.0, Juniper Mist sorts the issues into classifiers.	Non-Wi-Fi interference	Low capacity due to interference from non-Wi-Fi sources
		Wi-Fi interference	Low capacity due to wireless interference
		Client Count	Low capacity due to a high number of clients
Client Health (for Applications)	Juniper Mist monitors the CPU utilization and routing paths to identify issues affecting application performance.	Suboptimal IP	Latency and call quality issues due to a suboptimal network path, as might happen when the client is directed to a geographically distant server
		CPU	Low resource availability due to high CPU utilization

Table 7: Application SLEs and Classifiers *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
WAN Health (for Applications)	Juniper Mist monitors the network performance of the Zoom or Teams application to determine if there is any performance degradation. This SLE can help you understand the end users' experiences when accessing the applications.	Application Disconnects	Disconnects due to network issues, ISP-related issues, or device-specific issues
		Loss	Issues due to packet loss
		Slow Application	Issues involving slow responses to application requests
		Latency	Lag interrupting video and audio streams
		Jitter	Inconsistent packet transmit times
Partner Link	Juniper Mist assesses performance from network co-participants that can contribute to issues.	Co Participant	• Issues on a co-participant's side of a video or audio call For example, one of your users might report a bad application experience if a co-participant has issues when sharing their screen.

4

CHAPTER

Alerts

IN THIS CHAPTER

Alerts Overview

SUMMARY

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

IN THIS SECTION

What Are Alerts?

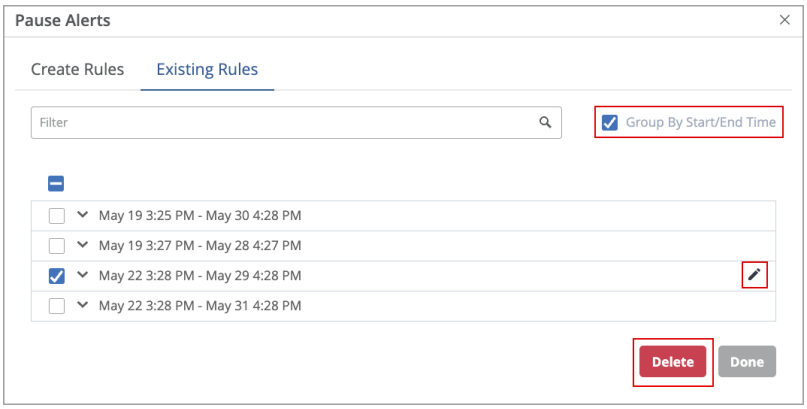
Alerts represent network and device issues that are ongoing. Juniper Mist™ categorizes them as follows:

- Infrastructure Alerts—Repeated events involving servers and protocols 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—Repeated events that Marvis tracks on the Marvis Actions dashboard. For example, if an access point (AP) regularly fails health checks, you'll see a Marvis alert for it.
- Security Alerts—Repeated events that could dramatically affect network security. For example, these alerts appear if a rogue AP is detected and clients start connecting to it.
- Certificate Alerts—Notification for expired, and soon-to-expire, user-added digital certificates. These include RadSec (configured at **Organization > Settings > RadSec Certificates and AP RadSec certificate**), SSO (configured at **Organization > Settings > Single Sign-On**), and PSK Portal IDP certificates (configured at **Organization > Client Onboarding**). Certificate alerts appear on the Alerts page and begin 30 days before the certificate's expiry date, then the notification repeats 15, 7, 3, and 1 day before expiration unless the certificate is renewed. .

You can pause alerts for the organization, selected sites, and site groups:

- In the main menu, select **Monitor** > **Alerts**, then click **Alerts Configuration** and **Pause Alerts**. From the **Existing Rules** tab of the **Pause Alerts** window, you can view the schedule of current rules, and make new rules at the **Create Rules** tab.

Figure 3: Schedule Alert Pauses



NOTE:

- For information about alerts, see "Juniper Mist Alert Types" on page 130.
- To enable the alerts that you want to include on the Alerts dashboard, see "Juniper Mist Alert Types" on page 130.
- Junos, the network operating system used in Juniper switching, routing, and security devices, provides another system for alerts and notifications that you can use to monitor switch ports. For more information, see https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/topic-map/overview-port-security.html.

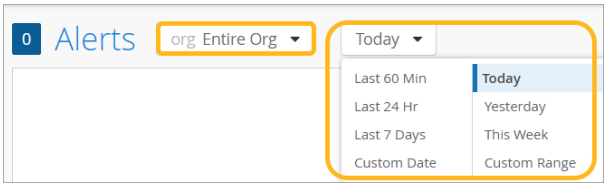
Finding the Alerts Dashboard

The Alerts dashboard lists all alerts that you've enabled on the Alerts Configuration page. To view the Alerts dashboard, select **Monitor** > **Alerts** from the left menu.

NOTE: For help configuring alerts, see "Configure Alerts and Email Notifications" on page 145.

Selecting the Context and Time Period

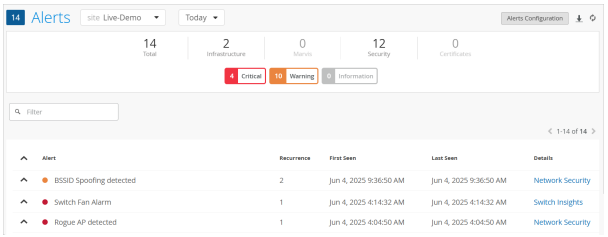
At the top of the Alerts page, select the context, which can be an entire organization or a single site. Also select the time period to view.



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.

Page Overview

Get familiar with the major elements of the Alerts dashboard.



At the top, the current alerts are summarized by type and severity level. All these summary blocks are buttons that you can use to filter the alerts list.

The alerts list includes this information:

- 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 129 table later in this topic.
- Site—The name of the site where this issue occurred. Appears only if you've selected Entire Org as the context at the top of the page.
- Recurrence—The number of times that this issue occurred.
- First Seen and Last Seen—The time period when this issue occurred.

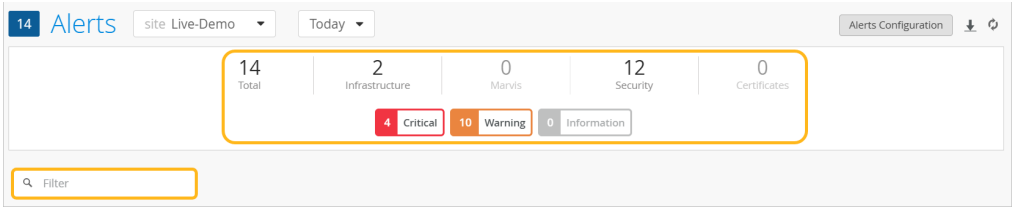
- Details—The affected component (as listed below), with a link that you can click for more details.

  The displayed link corresponds to the alert type. The 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.

Filters

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



Alert Type Filters

Juniper Mist categorizes alerts by type. The alert type buttons at the top of the Alerts page show the current number of issues for each type. Click a button to show only the alerts of that type.

NOTE: For more information about alert types, see "Juniper Mist Alert Types" on page 130.

Severity Filters

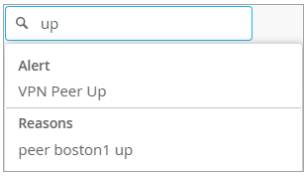
Juniper Mist ranks alerts by severity. The severity buttons at the top of the Alerts page show the current number of issues for each severity level. Click a button to show only the alerts for that severity level.

Table 8: 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 narrow down the alerts to view. Start typing the name of an alert, and then click a matching alert in the drop-down list.



Juniper Mist Alert Types

SUMMARY

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

IN THIS SECTION

Certificate Alerts

NOTE: Certificate alerts are available when you select **Entire Org** as the scope at the top of the Alerts Configuration page.

Table 9: Certificate Alerts by Severity

Severity	Alert Name
Critical (red icon)	Mist Access Assurance CA Certificate Expired
	Mist Access Assurance Server Certificate Expired
	NAC Portal IdP Certificate Expired
	PSK Portal IdP Certificate Expired
	RadSec CA Certificate Expired
	RadSec Device Certificate Expired
	SSO IdP Certificate Expired
	SSO LDAP CA Certificate Expired
	SSO LDAP Client Certificate Expired
	WLAN SSO IdP Certificate Expired
Warning (orange icon)	Mist Access Assurance CA Certificate Expiring
	Mist Access Assurance Server Certificate Expiring
	NAC Portal IdP Certificate Expiring
	PSK Portal IdP Certificate Expiring
	RadSec CA Certificate Expiring
	RadSec Device Certificate Expiring
	SSO IdP Certificate Expiring
	SSO LDAP CA Certificate Expiring
	SSO LDAP Client Certificate Expiring
	WLAN SSO IdP Certificate Expiring

Infrastructure Alerts

Infrastructure alerts are for events that involve servers and protocols that can 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 10: 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
	Mist Edge service failed to start
	Mist Edge unplugged from power
	Switch Fan Alarm
	Switch IP Conflict Detected
	Switch MAC Limit Exceeded
	Switch OSPF Neighbor Down
	Switch POE Controller Device Failure

Table 10: Infrastructure Alerts by Severity *(Continued)*

Severity	Alert Name
	Virtual Chassis - Backup Member Elected
	Virtual Chassis - New device elected for Active Role
	Virtual Chassis Member Deleted
	Virtual Chassis Port Down
	WAN Edge Chassis Hot
Informational (blue icon)	AP restarted
	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
	Cellular Edge WAN Ethernet Connected

Table 10: Infrastructure Alerts by Severity *(Continued)*

Severity	Alert Name
	Cellular Edge WAN Ethernet Plugged
	Cellular Edge WAN MTU Low
	Cradlepoint incident identified
	Cradlepoint incident investigation started
	Cradlepoint incident resolved
	Cradlepoint maintenance completed
	Cradlepoint maintenance scheduled
	Cradlepoint maintenance started
	Critical Switch Port Up **NOTE**: If you enable this alert, also identify the critical ports in the switch configuration. In your switch template, go to **Select Switches Configuration**, select the rule to edit, select the port range, and then select **Enable critical alerts**. For help, see Juniper Mist Wired Assurance Configuration Guide.
	Critical WAN Edge Port Up **NOTE**: If you enable this alert, also update the WAN or LAN configuration to identify the critical ports. In your WAN Edge template, select the WAN or LAN configuration, go to **Interface**, enter the ports, and then select **Enable critical alerts**. For help, see Juniper Mist WAN Assurance Configuration Guide.
	Fpc Management Ethernet Link Down Clear
	Inactive vlan(s) detected on tunnel port
	Mist Edge connected to cloud
	Mist Edge cpu usage normal
	Mist Edge disk usage normal

Table 10: Infrastructure Alerts by Severity *(Continued)*

Severity	Alert Name
	Mist Edge memory usage normal
	Mist Edge plugged to power
	Mist Edge power input connected
	Mist Edge upgrade completed
	New tunnel(s) formed
	Switch Fan Alarm Clear
	Switch High Humidity Clear
	Switch High Temperature Clear
	Switch OSPF Neighbor Up
	Switch PEM Alarm CLEAR
	Switch PoE Alarm Clear
	Switch Power Supply Alarm Clear
	Switch Radius Server Unresponsive
	Switch Storage Partition Alarm Clear
	Switch restarted
	Tunnel Monitored resource reachability restored
	Virtual Chassis Member Added
	Virtual Chassis Port Up
	WAN Edge Chassis Hot Cleared

Table 10: Infrastructure Alerts by Severity *(Continued)*

Severity	Alert Name
	WAN Edge Chassis Warm Clear
	WAN Edge Flow Count Returned to Normal
	WAN Edge Forwarding Information Base Count Returned to Normal
Warning (orange icon)	Mist Edge Fan Plugged
	AP offline (alert immediately when AP offline)
	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
	Critical Switch Port Down **NOTE**: If you enable this alert, also identify the critical ports in the switch configuration. In your switch template, go to **Select Switches Configuration**, select the rule to edit, select the port range, and then select **Enable critical alerts**. For help, see Juniper Mist Wired Assurance Configuration Guide.
	Critical WAN Edge Port Down **NOTE**: If you enable this alert, also update the WAN or LAN configuration to identify the critical ports. In your WAN Edge template, select the WAN or LAN configuration, go to **Interface**, enter the ports, and then select **Enable critical alerts**. For help, see Juniper Mist WAN Assurance Configuration Guide.
	EVPN detected a duplicate MAC address
	Failed to sync cradlepoint devices

Table 10: Infrastructure Alerts by Severity *(Continued)*

Severity	Alert Name
	Fpc Management Ethernet Link Down
	HA Control Link Down
	Last data port dropped from LACP
	Loop detected (by AP)
	Mist Edge configuration apply failed
	Mist Edge primary radius server unresponsive
	Mist Edge service crashed
	Mist Edge upgrade failed
	Mist Edge was restarted
	Rogue DHCP SErver Detected
	Storm Control in Effect on Switch port
	Switch BPDU Error
	Switch Bad Optics
	Switch DHCP Pool Exhausted
	Switch High Humidity
	Switch High Temperature
	Switch OSPF Neighbor Adjacency Failed
	Switch PEM Alarm
	Switch PoE Alarm

Table 10: Infrastructure Alerts by Severity *(Continued)*

Severity	Alert Name
	Switch Power Supply Alarm
	Switch Storage Partition Alarm
	Switch offline
	Tunnel Monitored resource is unresponsive
	Tunnel down
	VPN Peer Down
	Virtual Chassis Member Restarted
	WAN Edge BGP Neighbor Down
	WAN Edge Chassis Warm
	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 **NOTE**: This alert will trigger immediately when the gateway goes offline (the default behavior) unless you configure a delay threshold, for example, to prevent repeated alerts in the case of connectivity flaps. The time range is from 0 to 240 minutes. When you set a delay threshold, it applies to the entire organization. Click the pencil icon next to the alert to open the **Edit WAN Edge Offline Threshold** config page.

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 11: Marvis Alerts by Device/Service Type and Severity

Applies To	Severity	Alert Name
AP	Critical (red)	AP health check failed
		AP insufficient capacity
		AP insufficient coverage
		Bad cable
		Non-compliant
		Offline (Marvis)
		Site Offline (ISP)
	Warning (orange)	AP Loop due to Switch Port Flap
		AP Loop due to Tunnels paths
		AP Loop due to duplicated WLAN paths
Data Center/Application	Critical (red icon)	Application Reachability Failure (Marvis-Minis)
Connectivity	Critical (red icon)	ARP failure (Marvis)
		ARP failure (Marvis-Minis)
		Authentication failure (Marvis)
		DHCP failure (Marvis)
		DHCP failure (Marvis-Minis)

Table 11: Marvis Alerts by Device/Service Type and Severity *(Continued)*

Applies To	Severity	Alert Name
		DNS failure (Marvis)
		DNS failure (Marvis-Minis)
WAN	Critical (red icon)	Bad WAN Uplink
		Bad cable
		Device Problem
		Intermittent WAN Connectivity
		MTU mismatch
		Negotiation mismatch
		Non-compliant
		VPN Path Down
Wired	Critical (red icon)	Bad cable
		MTU Mismatch
		Missing VLAN
		Negotiation incomplete
		Port Stuck
		Switch Offline
		Switch STP Loop
	Warning (orange icon)	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 12: Security Alerts by Severity

Severity	Alert Name
Critical (red icon)	Client Connection to rogue AP detected
	Rogue AP detected
Informational (blue icon)	Air Magnet Scan detected
	EAP Handshake Flood detected
	Switch DDoS Protocol Violation Clear
Warning (orange icon)	Active Watched Station detected
	Adhoc Network detected
	BSSID Spoofing detected
	Client MAC Spoofing
	Disassociation Attack detected
	EAP Dictionary Attack detected
	EAP Failure Injection detected
	EAP Spoofed Success detected

Table 12: Security Alerts by Severity *(Continued)*

Severity	Alert Name
	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
	Out of Sequence detected
	Repeated Client Authentication Failures
	Replay Injection detected - KRACK Attack
	SSID Injection detected
	Security Policy Violation
	Switch DDoS Protocol Violation Set
	TKIP ICV Attack
	URL blocked
	Vendor IE Missing

Table 12: Security Alerts by Severity *(Continued)*

Severity	Alert Name
	Zero SSID Association Request detected

Recommended Alerts

SUMMARY

As a best practice, enable these recommended alerts.

We recommend certain alerts for all deployments. Also consider additional alerts as appropriate for your organization.

NOTE: To help you to find these alerts easily on the Alert Configuration page, the Recommended Alerts column is sorted by the alert category and the alert color.

Table 13: Recommendations

Devices/Deployments	Recommended Alerts
All *We recommend these alerts for all Juniper Mist organizations.*	Enable these alerts in the Infrastructure category: • Mist Edge Fan Unplugged (red) • Switch Fan Alarm (red) • Switch PoE Controller Failure (red) • Virtual Chassis Member Deleted (red) • Virtual Chassis Port Down (red) • Switch Restarted (blue) • Switch Offline (blue) • Switch Bad Optics (orange) • Switch High Temperature (orange) • Switch PEM Alarm (orange) • Switch PoE Alarm (orange) • Switch Power Supply Alarm (orange) • Switch Storage Partition Alarm (orange)
Campus Fabric *For campus fabric deployments, we recommend these additional alerts.*	Enable these alerts in the Infrastructure category: • BGP Neighbor State Changed (blue) • BGP Neighbor Up (blue) • EVPN Duplicate MAC Address (orange) Enable these alerts in the Security category: • Switch DDOS Protocol Violation Clear (blue) • Switch DDOS Protocol Violation Set (orange)

Table 13: Recommendations *(Continued)*

Devices/Deployments	Recommended Alerts
Critical Switch Ports *If you've configured any ports as critical ports, also enable these alerts.*	• Critical Switch Port Up (blue) • Critical Switch Port Down (orange) • Switch Offline (orange)

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.

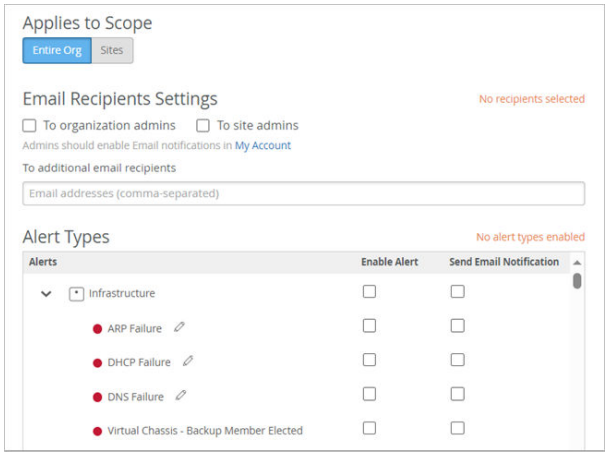
Video: Alert Configuration Overview

Configuration

To configure alerts:

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

The configuration page is divided into sections, where you'll set the scope, identify recipients for alert notifications (optional), and enabling the alerts that you want to monitor.



3. Under **Applies to Scope**, select one of these options:

   - **Entire Org**—Configure alerts for the entire organization.
   - **Sites**—Configure alerts for sites that you want to monitor differently than the rest of your organization. Click the plus sign to select a site.

4. (Optional) Under **Email Recipient Settings**, set up an email distribution list for any email notifications that you enable.

   NOTE: Here, you're identifying the *recipients*. In the Alert Types section, you'll enable the *notifications* for the alerts that you want to monitor via email.

   Options include:

   - **To organization admins**—Select this option to include all admins whose permissions allow access to the entire organization.
   - **To site admins**—Select this option to include only admins with access to the sites specified in the scope section.
   - **To additional email recipients**—Select this option to specify personnel who do not have Juniper Mist admin accounts but need to monitor alerts. To enter multiple email addresses, separate them with commas.

5. In the **Alert Types** section, enable dashboard alerts and email notifications for the events that you want to monitor.

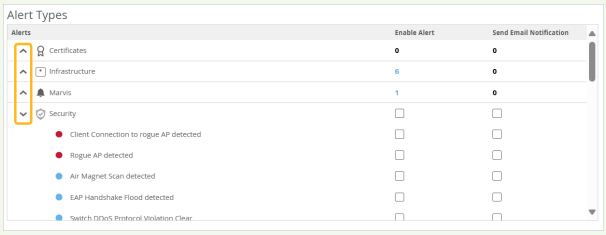
   For information about the various alerts, see "Juniper Mist Alert Types" on page 130.

   For each type of alert, you have these options:

   - **Enable Alert**—Include this alert on the Alerts dashboard. (You can view the dashboard by selecting **Montior** > **Alerts** from the left menu of the Juniper Mist portal.)

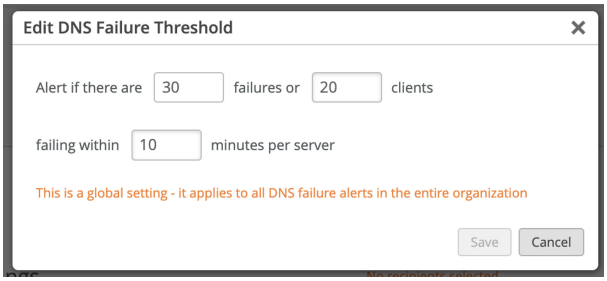
- **Enable Email Notification**—Send alert notifications to the personnel that you specified in the Email Recipients section.

TIP: Use the expand/collapse buttons on the left side of the alert Types section to focus on one type of alert at a time. For example, expand only Security and collapse the other alert types, as shown below.



6. If you enabled an alert that has a pencil icon, click the icon to configure the settings.

   For example, when you click the pencil icon for DNS Failure, you can set the threshold based on the number of failures, the impacted clients, and the duration.



7. Click **Save** at the top-right corner of the Alerts Configuration page.

Temporarily Pause Your Alerts

SUMMARY

During certain periods, such as initial installation or site maintenance, you might want to pause your alerts. This way, you won't get unnecessary communications about the system changes that you're making.

You'll specify the time period and the scope. For example:

- Pause alerts for all devices across your entire organization.
- Pause alerts only for your organization-level devices like Mist Edge.
- Pause alerts for specific sites.
- Pause alerts for one site only.

During the specified time period, all alerts are paused for the specified devices and sites. You'll continue to get the normal alerts for any out-of-scope devices and sites. When the time period elapses, all enabled alerts resume as usual.

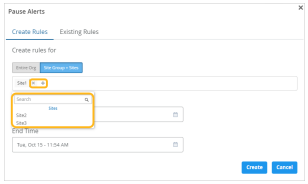
To temporarily pause your alerts:

1. From the left menu, select **Monitor** > **Alerts**.
2. Click the **Alerts Configuration** button at the top-right corner of the Alerts page.
3. Click the **Pause Alerts** button near the top-right corner of the Alerts: Configuration page.
4. In the Pause Alerts window, use the **Create Rules** tab and the **Existing Rules** tab to create and manage your pause rules.

Table 14: Create a New Pause Rule

Scope of New Rule	Instructions
Pause all alerts across your entire organization.	This approach covers your entire organization, though you can specify the types of devices to include. **a.** Click the **Create Rules** tab. **b.** Click **Entire Org**. **c.** Select one or both check boxes to specify the types of devices to include: • Organization—Check this box to include devices like Mist Edge that are assigned to an organization, not to a specific site. If the box is unchecked, you'll receive the normal alerts for organization-level devices. • Site—Check this box to include devices that are assigned to specific sites. This option includes most devices in your Mist organization, since onboarding typically involves assigning devices to sites. If this box is unchecked, you'll receive the normal alerts for site-assigned devices. **d.** Select the **Start Time** and **End Time**. **e.** Click **Create** to save your rule. The Existing Rules tab appears. If you selected organization devices only, you'll see one new rule. If you selected site devices, you'll see a separate rule for each site in your organization.

Table 14: Create a New Pause Rule *(Continued)*

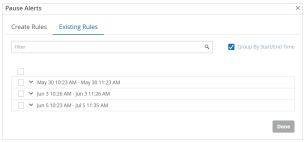
Scope of New Rule	Instructions
Pause alerts for specific sites.	This approach covers only the sites that you specify. You'll continue to get alerts for other sites as you normally do. **a.** Click the **Create Rules** tab. **b.** Click **Site Group + Sites**. **c.** Click the **+** button, and then select a group or site.  **d.** Repeat as needed to add all applicable sites. **NOTE**: If you add an site by mistake, click **X** to remove it. **e.** Select the **Start Time** and **End Time**. **f.** Click **Create** to save your rule. The Existing Rules tab appears. You'll see one rule for each site that you selected.

NOTE: A site can have only one active pause rule. If your new rule includes a site that already has a pause enabled, a message pops up. Follow the on-screen instructions to override the old rule or to remove the specified site from the new rule.

Table 15: Manage Existing Rules

Task	Options
View the status of a pause.	On the **Existing Rules** tab, look in the **Active** column. Green indicates an active rule.

Table 15: Manage Existing Rules *(Continued)*

Task	Options
Cancel a pause.	On the **Existing Rules** tab, select the check box for each rule to delete. Then click **Delete**.
Filter the list of pause rules.	On the **Existing Rules** tab, start typing in the **Filter** box. Matching rules appear.
Organize the pause rules by date.	On the **Existing Rules** tab, select **Group by Start/End Times**. You can expand or collapse each dated section to show or hide the rules. 

5. To close the Pause Alerts window, click **Done**.

Alerts FAQ

IN THIS SECTION

When I receive a "Certificate Expiring" alert, what is the timeframe for the expiration?

"Certificate Expiring" alerts, such as RadSec CA Certificate Expiring or SSO IdP Certificate Expiring, first appear at 30 days before expiry. If don't take action, you'll see additional alerts at 15 days, 7 days, 3 days, and 1 day.

When I receive a "Certificate Expired" alert, what is the timeframe for the expiration?

"Certificate Expired" alerts, such as Mist Access Assurance CA Certificate Expired or PSK Portal IdP Certificate Expired, first appear on the first day after expiry. If don't take action, you'll see additional alerts at 30-day intervals until the certificate is removed or replaced.

On the Alerts Configuration page, why do some alert types have pencil icons?

On the Alerts Configuration page, you can use the pencil icons to review and change the threshold values that trigger an alert.

For example, in the Infrastructure section, you'll see a pencil icon next to the ARP Failure alert type. You can define various numbers to use in the alert trigger: "Alert if there are <number> failures or <number> clients failing within <number> minutes per server."

Where you see a pencil icon, click it, review or change the parameters, and then click **Save**.

CHAPTER 5

Get Started with Marvis

SUMMARY

Use the information in this chapter to start using Marvis to improve user experiences on your network.

IN THIS CHAPTER

Meet Marvis

Video: Journey Into AI With Marvis, Our Virtual Network Assistant

What Do You Want to Do?

Table 16: Top Tasks

If you want to...	Use these resources:
Explore Marvis' recommended actions for current network issues *Get a dashboard view of high-impact network issues. Drill down to discover the scope of impact and the recommended actions.*	"Marvis Actions Overview" on page 159
Interact with Marvis to get real-time information and troubleshooting help *Have an interactive conversation with Marvis by entering natural-language questions or structured queries.*	"Marvis Conversations and Queries Overview" on page 273
Use Marvis on your Android device *View your network from the client's perspective. Get detailed data and telemetry about how clients experience the wireless connection, including insight into client roaming behaviors.*	"Marvis Client Overview" on page 291
Access Marvis from Microsoft Teams *Search for devices, view details, troubleshoot, and search for documentation from the Marvis App for Microsoft Teams.*	"Overview of the Marvis App for Microsoft Teams" on page 357

Table 16: Top Tasks *(Continued)*

If you want to...	Use these resources:
Use Marvis Minis to proactively assess network connectivity and service reachability *By proactively simulating user connections through an access point (AP), Marvis Minis can help detect and resolve issues before they impact users.*	"Marvis Minis Overview" on page 237

Marvis Virtual Network Assistant Overview

SUMMARY

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

Marvis® Virtual Network Assistant 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 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 parameters that help represent a client's network view. The Marvis Android client works with the Zebra wireless insights to provide enhanced telemetry and visibility into the Zebra client experience.
- **Marvis Query Language**—A structured format to request data or troubleshoot issues.

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

Subscriptions for Marvis

In addition to your base Assurance subscriptions (Wireless Assurance, WAN Assurance, or Wired Assurance), you also need Marvis subscriptions for each device.

- Marvis for Wired
- Marvis for WAN
- Marvis for Wireless

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

CHAPTER 6

Marvis Actions

IN THIS CHAPTER

Marvis Actions Overview

SUMMARY

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.

As you add new sites and devices to your network, Marvis Actions scales with ease without any additional configuration.

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.

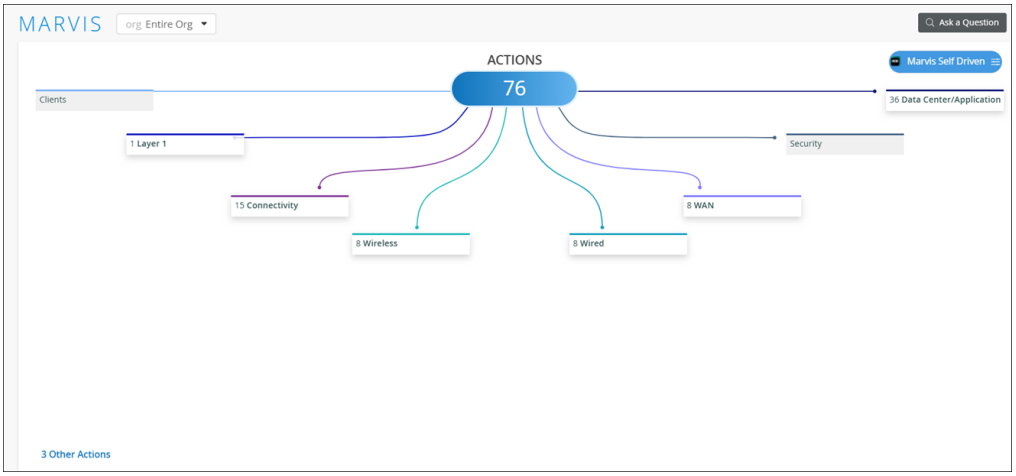
Video: Marvis Actions

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.

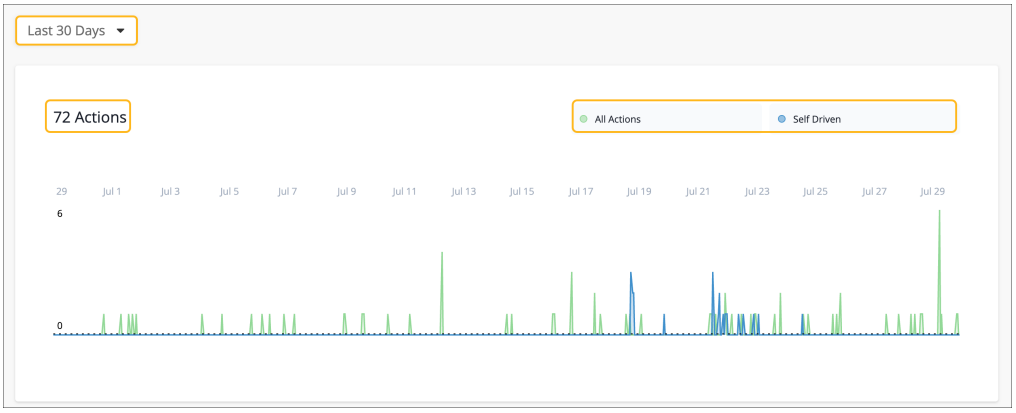
To view the Marvis Actions dashboard, select **Marvis > Marvis Actions** from the left menu of the Juniper Mist™ portal.

Here's what the Marvis Actions page looks like. You'll notice that the page displays the information under three sections. The first section displays different categories. Marvis indicates the number of issues detected for a category. Note that the categories list only the issues that are currently open at the organization or site level, irrespective of the time. For example, in the following screenshot, you'll notice that Marvis lists 15 issues for the Connectivity category.



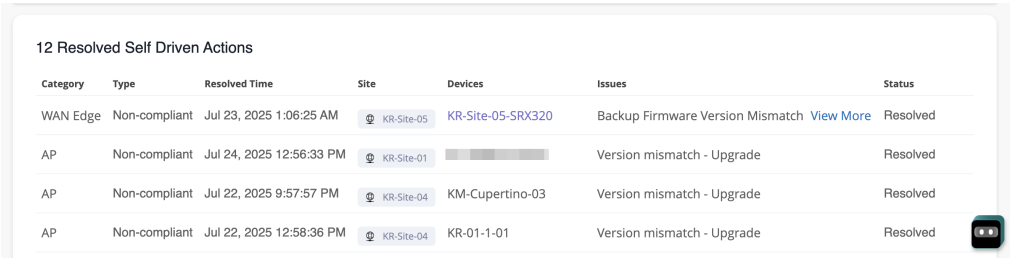
You can also view the issues for a site.

The second section displays a time series graph of the number of actions created over a specific time duration, the default being 30 days. You can view either all the actions or only the self-driven actions (if enabled). All actions include the self-driven actions. Here is an example of how the graph is displayed when you click **All Actions**. Note that the total number of actions created in the last 30 days is 72, which includes the self-driven actions.



The last section displays the list of issues that were automatically resolved by self-driving actions (if enabled) for the selected time duration, the default being 30 days. If you select an action under a category, then you will see the list of recommended actions instead.

For information about self-driving actions, see "Self-Driving Marvis Actions" on page 166.



NOTE: The Time Series graph and the Recommended Actions sections display issues for all possible statuses for a selected action and time duration at the organization or site level, unlike the categories section that lists only the currently open issues.

Self-Driving Marvis Actions

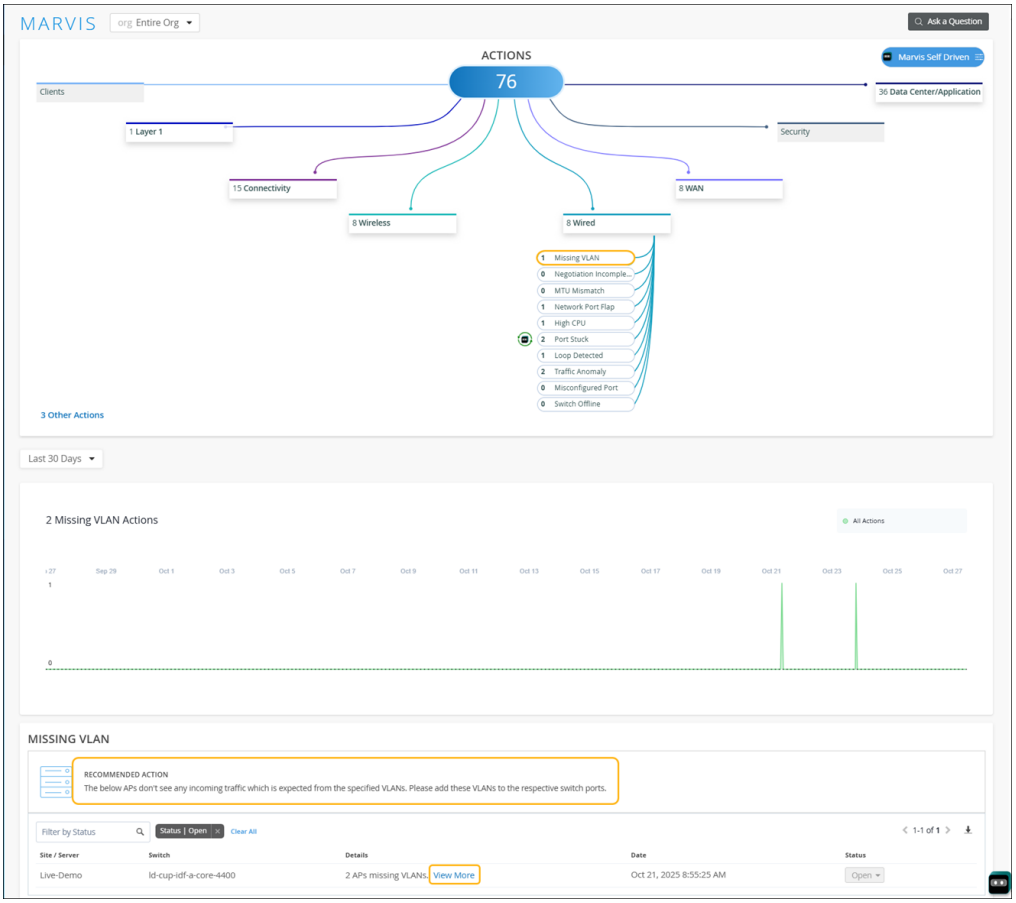
You can enable self-driving capability for certain Marvis actions by granting permissions to Marvis. Marvis performs remediation automatically to resolve any issues flagged under that action. For information about the self-driving capability, see "Self-Driving Marvis Actions" on page 166.

Detailed View of Issues and Marvis Recommended Actions

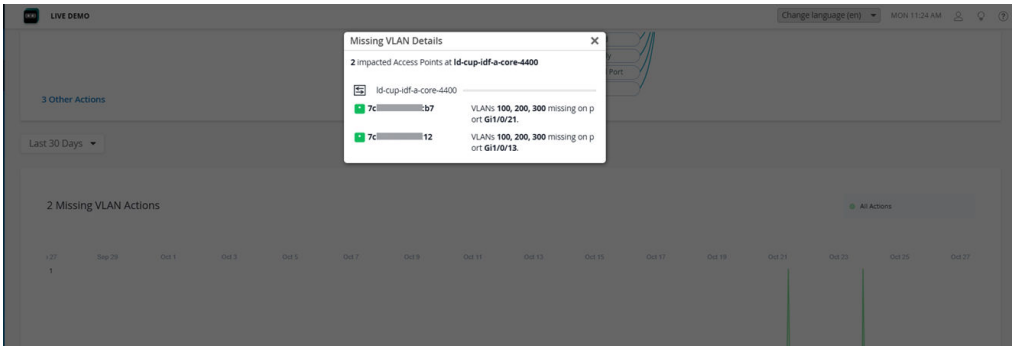
Each category has a group of actions under it. Each action can have one or multiple issues associated with it. If Marvis does not detect any anomalies associated with an action, the action appears dimmed but you can still click the action to view the previous list of AI Validated issues for the action. You can view details of Marvis Actions that were created in the last two months for an action or a category.

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.



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.



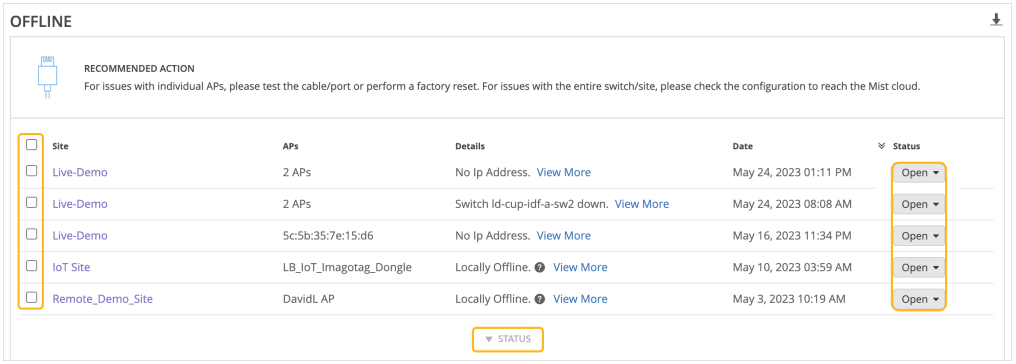
Downloadable List of Issues

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.

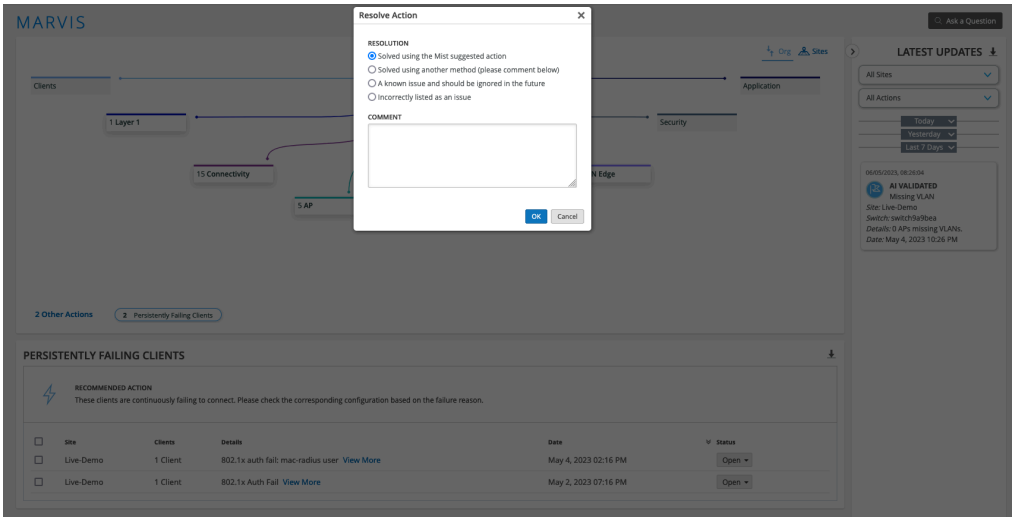
Issue Resolution

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.

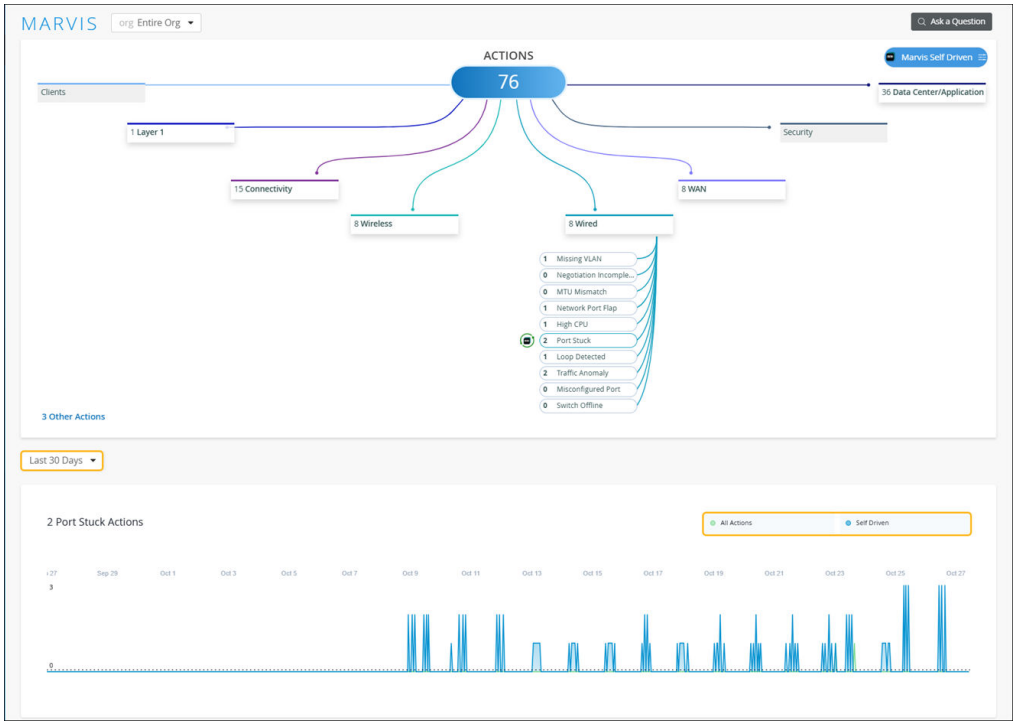


Marvis prompts you for feedback, which Mist uses internally to determine the efficacy of the action.



View the Marvis Actions Time Series Graph

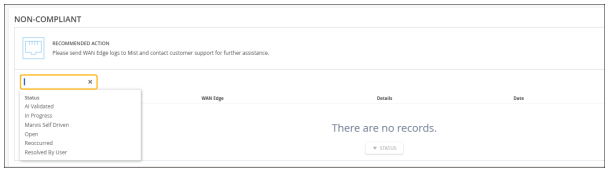
The Marvis Actions page displays the creation date and time for each action. The data is presented on a time series graph, providing a clear and quick overview of the number of actions generated over specific periods. You can see the trends for both driver-assisted and self-driven actions at the site or organizational level for the selected duration.



If you click **All Actions**, you can view all the actions generated by Marvis for the selected duration. Click **Self-Driven** to view the automatically resolved issues. Note that the **Self-Driven** option is hidden for actions without the self-driving capability.

Filter Marvis Recommended Actions by Status

The RECOMMENDED ACTION section on the Marvis Actions page provides filters to list issues based on the status. By default, all issues in the Open status for the selected Marvis Action and duration are displayed. Click **Clear All** and press the **Spacebar** in the filter text box to select a filter criteria. You can also manually enter the filter criteria directly into the filter text box.



Marvis classifies the issues under one of the following states:

- All (no filter option selected)—Lists all the issues for the selected Marvis action.
- AI Validated—Lists all the resolved issues that have been validated as fixed by Marvis.

  If you fix an issue and update the status to Resolved by User, 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 changes the status to AI Validated.

If the issue is fixed by a self-driving action, Marvis validates that the issue no longer exists and changes the status to AI Validated.

- In progress —Lists issues being fixed manually by users. Marvis continuously monitors in-progress issues and marks them as **AI Validated** if it does not observe these issues during the validation time. The validation time is the time taken for Marvis to mark an open Marvis action as AI validated.
- Marvis Self Driven—Lists issues resolved by the Marvis self-driving feature. After the issue is fixed, Marvis performs checks to ensure that the issue is indeed resolved. If the issue is not observed during the validation time, Marvis changes the status to **AI Validated**. The validation time is the time taken for Marvis to mark an open Marvis action as AI validated.
- Open—Lists the unresolved issues for the selected Marvis action.
- Resolved by User (applicable to driver-assist actions only)—Lists the issues resolved by users manually.

For any self-driving action with permissions enabled, Marvis identifies and automatically rectifies the issue by taking necessary actions. After the issue is resolved, the status of the issue changes to **Marvis Self Driven**. Marvis changes the status to **AI Validated** only after validating that the issue has not reoccurred.

You can view issues resolved through a self-driven action by selecting the **Marvis Self Driven** or **AI Validated** filter. If you do not select a filter, all issues are listed including any **Marvis Self Driven**, **AI Validated**, and **Open** issues.

If an issue resolved by a self-driving action reoccurs, then Marvis changes the status of the issue to **Open**.

You can click the download (down arrow) icon next to the toggle button to download the list of issues for your organization or site in CSV format.

Video: Troubleshooting Bad Signal Strength

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

Video: Marvis Actions Example

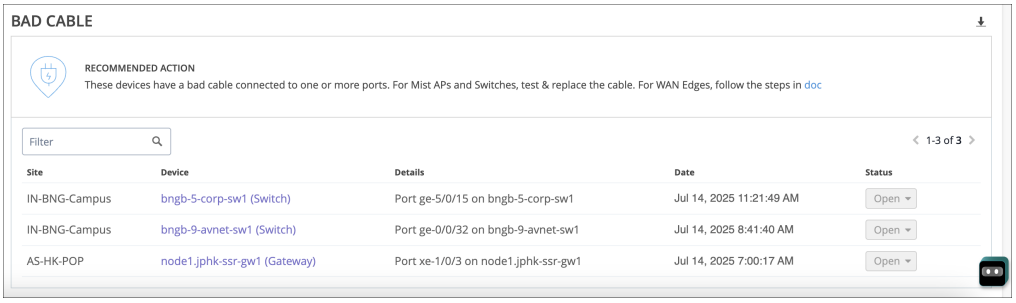
Self-Driving Marvis Actions

SUMMARY

Use self-driving Marvis Actions to simplify and automate troubleshooting.

IN THIS SECTION

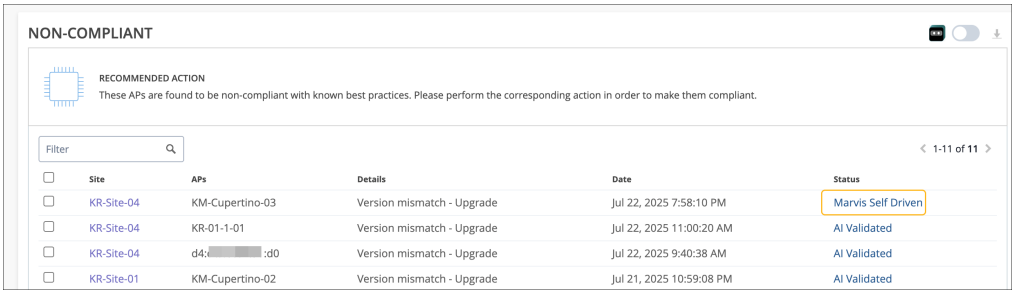
Marvis actions provide both driver-assist and self-driving actions. Driver-assist actions require user intervention based on the details and recommendations provided by Marvis. Here's an example of a driver-assist action. Marvis provides the necessary details that enable you to address the issue.



In contrast, when you grant permissions to Marvis, it autonomously initiates self-driving actions to execute corrective measures without any user involvement. This effectively automates the process of identifying and resolving issues. For example, a driver-assist action involves a network administrator having to manually upgrade the firmware on an AP. Conversely, a self-driving action automatically initiates the firmware upgrade when Marvis detects a firmware non-compliance on an AP.

By utilizing the self-driving capabilities, you can automate simple repetitive tasks, streamline troubleshooting processes, minimize downtime, and enhance overall network efficiency.

When an issue is fixed by a self-driving action, the status of the issue changes to **Marvis Self Driven** as shown in the following example. After the issue is fixed, Marvis performs checks to ensure that the issue is indeed resolved. If the issue is not observed during the validation time, Marvis changes the status to **AI Validated**. The validation time is the time taken for Marvis to mark an open Marvis action as AI validated.



The self-driving capability is available for the following actions:

Table 17: Self-Driving Marvis Actions

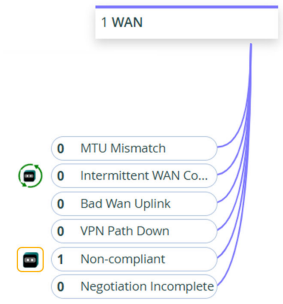
Category	Actions With Self-Driving Capability
AP	Non-compliant
Switch	Port Stuck (self-driving capability enabled by default)
WAN Edge	Non-compliant
	Intermittent WAN Connectivity (self-driving capability enabled by default)

How to Enable Self-Driving Actions

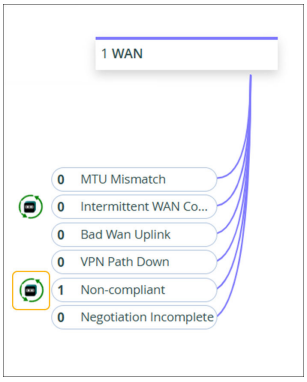
To enable self-driving actions, you must grant Marvis the necessary permissions by using the **Marvis Self Driven** button on the Marvis Actions page. You can grant permissions at the organization or site level. Permissions granted at the organization level are applicable to all sites in the organization. You can change the permissions at the site level to override the permissions granted at the organization level.

The self-drive permission is disabled by default. If the self-drive permission is disabled for a Marvis action, Marvis will not attempt to automatically resolve the issue; instead, it provides an option for you to manually initiate the corrective action.

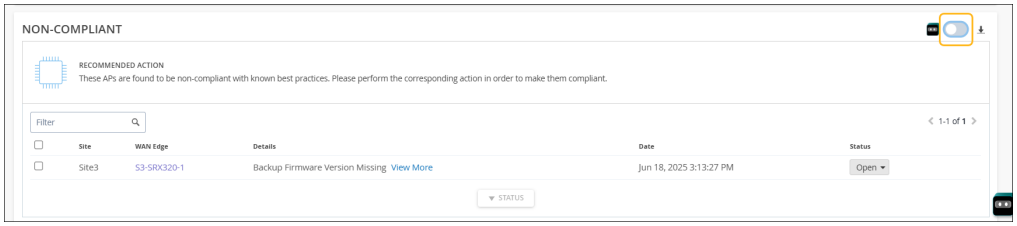
Actions with self-driving capabilities are tagged with the Marvis icon, allowing you to easily identify self-driving actions.



When you enable the self-driving feature for an action, the Marvis icon will change as shown in the following example:



You can also enable the self-driving capability for a specific action by using the toggle button in the Recommended Actions section.

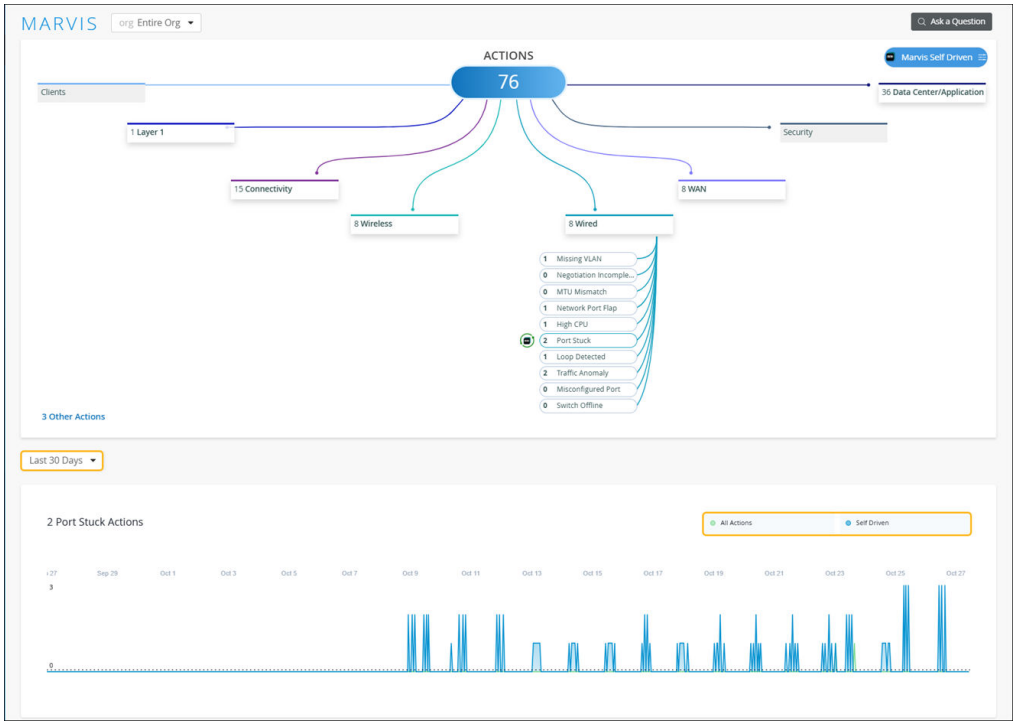


NOTE: You can disable the self-driving capability for an action at any point in time. If you disable the capability, ongoing self-driving tasks will complete, but subsequent tasks will not be self-driven.

Once a self-driven action is completed, you can view it by selecting either the All or self-driven filter options.

Self-Driven Actions Time Series Graph

You can use the time series graph on the Marvis Actions page to view historical patterns or trends for self-driven actions at the site or organization level, The graph displays the number of self-driven actions generated for a site or organization for the selected time range.



Click **Self-Driven** to view the automatically resolved issues. Note that the **Self-Driven** option is hidden for actions without the self-driving capability.

Self-Driving Switch Actions

For switches, the self-driving capability is available for the Port Stuck action and is enabled by default. Marvis automatically bounces the port to fix the issue. Marvis will attempt to bounce the port three times and if the issue remains unresolved, then Marvis will set the issue status as Open and provide details of the automatic remediation steps taken. Stopping the automatic bounce after three attempts prevents continuous port bounce cycles. You can then check whether the port stuck issue is due to a hardware issue with the device connected to the switch port.

Self-Driving AP Actions

For APs, the self-driving capability is available for the Non-Compliant action. If you enabled the self-driving capability for this action, Marvis automatically initiates the firmware upgrade on the APs.

Automatic upgrade involves upgrading one AP at a time during periods of low network usage at a site to minimize network downtime and impact to users. Consequently, if multiple APs need to be upgraded, the process might take a few days as Marvis upgrades one AP in a 24-hour window during periods of low site usage to avoid creating any network coverage issues.

Self-Driving WAN Edge Actions

For WAN Edges, the self-driving capability is available for the following actions:

- Non-Compliant—If you enabled the self-driving capability for this action, Marvis automatically initiates the Snapshot Device feature to update the Junos OS version on the backup partition of an SRX Series device so that it matches the version that is currently running on the primary partition.

  Automatic upgrade involves upgrading one device at a time during periods of low network usage at a site to minimize network downtime and impact to users. Consequently, if multiple devices need to be upgraded, the process might take a few days as Marvis upgrades one device in a 24-hour window during periods of low site usage to avoid creating any network disruption.

- Intermittent WAN Connectivity—The self-driving capability for this action is enabled by default. When Marvis detects an uplink port on a WAN Edge device that is unable to pass traffic due to one of the following reasons, it automatically bounces the port to fix the issue:

- ARP resolution for the gateway fails for the ISP server provided IP address.
- Uplink port does not receive an IP address from the ISP.

Marvis will attempt to bounce the port three times and if the issue remains unresolved, then Marvis will set the issue status as Open.

Find Self-Driven Actions Using Filters

The RECOMMENDED ACTION section on the Marvis Actions page provides filters to list issues based on the status. For information about the filter options, see "Filter Marvis Recommended Actions by Status" on page 164.

For any self-driving action with permissions enabled, Marvis identifies and automatically remediates the issue by taking the necessary action. After the issue is resolved, the status of the issue changes to **Marvis Self Driven**. Marvis then validates that the issue has not reoccurred and then changes the status to **AI Validated**.

You can view issues resolved through a self-driven action by selecting the **Marvis Self Driven** or **AI Validated** filter. If you do not select a filter, all issues are listed including any **Marvis Self Driven**, **AI Validated**, and **Open** issues.

If an issue resolved by a self-driving action reoccurs, then Marvis changes the status of the issue to **Open**.

You can click the download (down arrow) icon next to the toggle button to download the list of issues for your organization or site in CSV format.

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

The Actions shown on the dashboard differ according to your Marvis subscriptions. If an Action is not included in your subscription, you won't be able to drill down to the scope, details, and root-level analysis. For trial subscription, you can access all Actions for the duration of the trial.

Subscriptions and Actions

The following tables show the available actions for each subscription type.

Table 18: Subscription Type: Marvis for Wired Actions

Category	Available Actions
Connectivity	Authentication Failure
	DHCP Failure
Wired	Negotiation Incomplete
	MTU Mismatch
	Loop Detected
	Network Port Flap
	High CPU
	Port Stuck
	Traffic Anomaly
	Switch Offline
Other Actions	Persistently Failing Clients
	Access Port Flap

Table 19: Subscription Type: Marvis for WAN Actions

Category	Available Actions
WAN	MTU Mismatch
	Bad WAN Uplink
	Intermittent WAN Connectivity
	VPN Path Down
	Non-Compliant

Table 20: Subscription Type: Marvis for Wireless Actions

Category	Available Actions
Layer 1	Bad Cable
Connectivity	Authentication Failure
	DHCP Failure
	ARP Failure
	DNS Failure
Wireless	Offline
	Health Check Failed
	Non-compliant
	Coverage Hole
	Insufficient Capacity
	AP Loop Detected
Wired	Missing VLAN

Table 20: Subscription Type: Marvis for Wireless Actions *(Continued)*

Category	Available Actions
Other Actions	Persistently Failing Clients

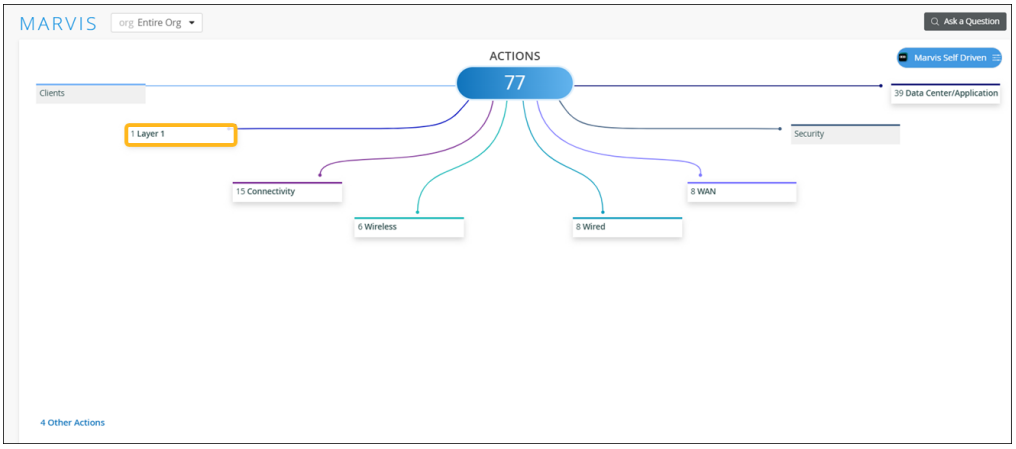
Layer 1 Actions

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. This category currently contains two actions: Bad Cable and Bad Fiber Optics.



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 171.

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.

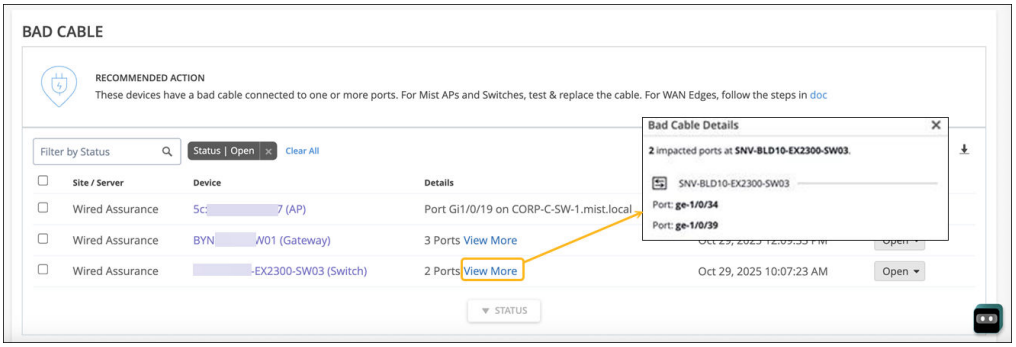
A bad cable action indicates cable issues that APs, Switches, and WAN edge devices detect at a site. The details section indicates if a switch, an AP, or a WAN edge device detected the issue.

Marvis monitors APs that reboot frequently to determine if the cause for the reboot is a bad cable. For example, if one AP reboots frequently while other APs connected to the same switch do not reboot, then it might indicate a faulty cable.

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:



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.

Video: Bad Cable

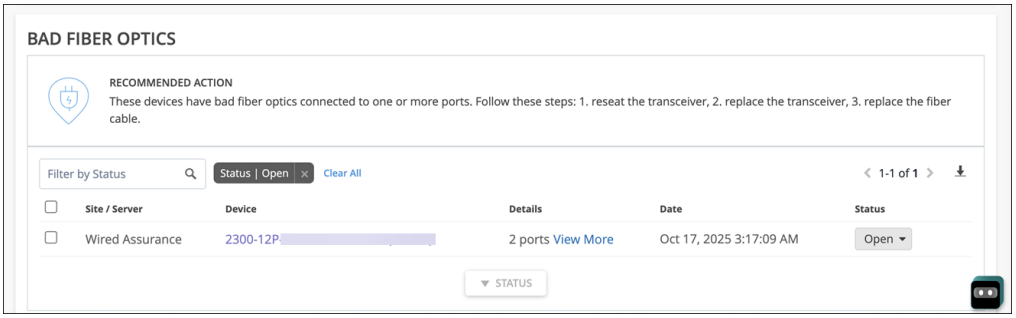
Bad Fiber Optics

Fiber optic cables and transceivers that are damaged, degraded, or not functioning properly can significantly affect the network performance, speed, and scalability. Issues such as physical damage, wear and tear, using the wrong transceiver, or improper installation can lead to fiber optic failures. Regular inspections are crucial to detect and fix faulty fiber optics promptly. By utilizing switch reported events and network statistics, Marvis can help in the early detection of faulty fiber optics, enabling quick resolution and minimizing network disruptions.

Marvis identifies the following two types of issues:

- Cable related issues, which include CRC errors, link flaps, and packet mismatches
- Fiber optics hardware issues indicated by low-light alarms

The Bad Fiber Optics Marvis action is generated only when both the above issues occur on the same switch port within a 2-hour window.



The **View More** link provides more details about the issue:

When you see a bad fiber optics Marvis action listed, follow these steps:

- Reseat the transceiver—This procedure involves physically removing the transceiver from its port and then reinserting it. It's a quick and effective diagnostic step to address connection problems caused by an improperly seated transceiver.
- Replace the transceiver—If reseating does not resolve the issue, then evaluate whether the transceiver needs to be replaced.
- Replace the fiber cable—Sometimes the issue might stem from a damaged fiber cable warranting its replacement.

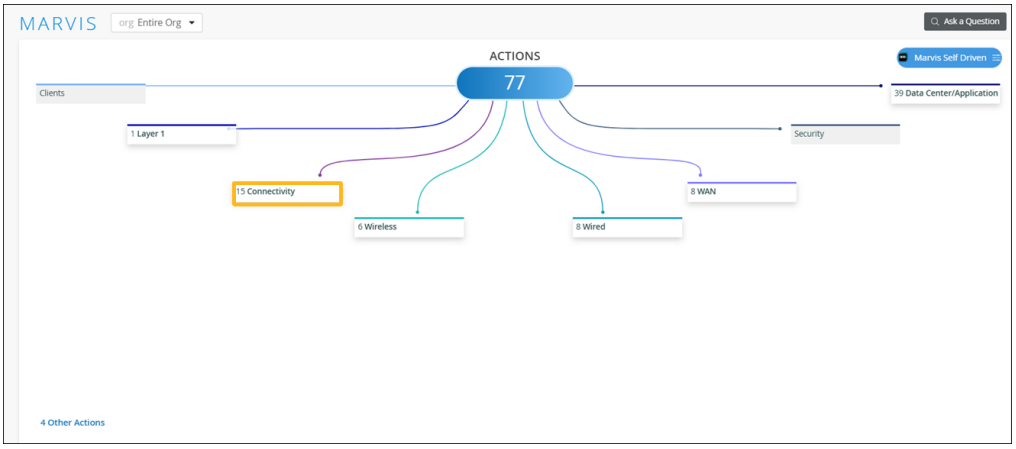
Connectivity Actions

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.



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 171.

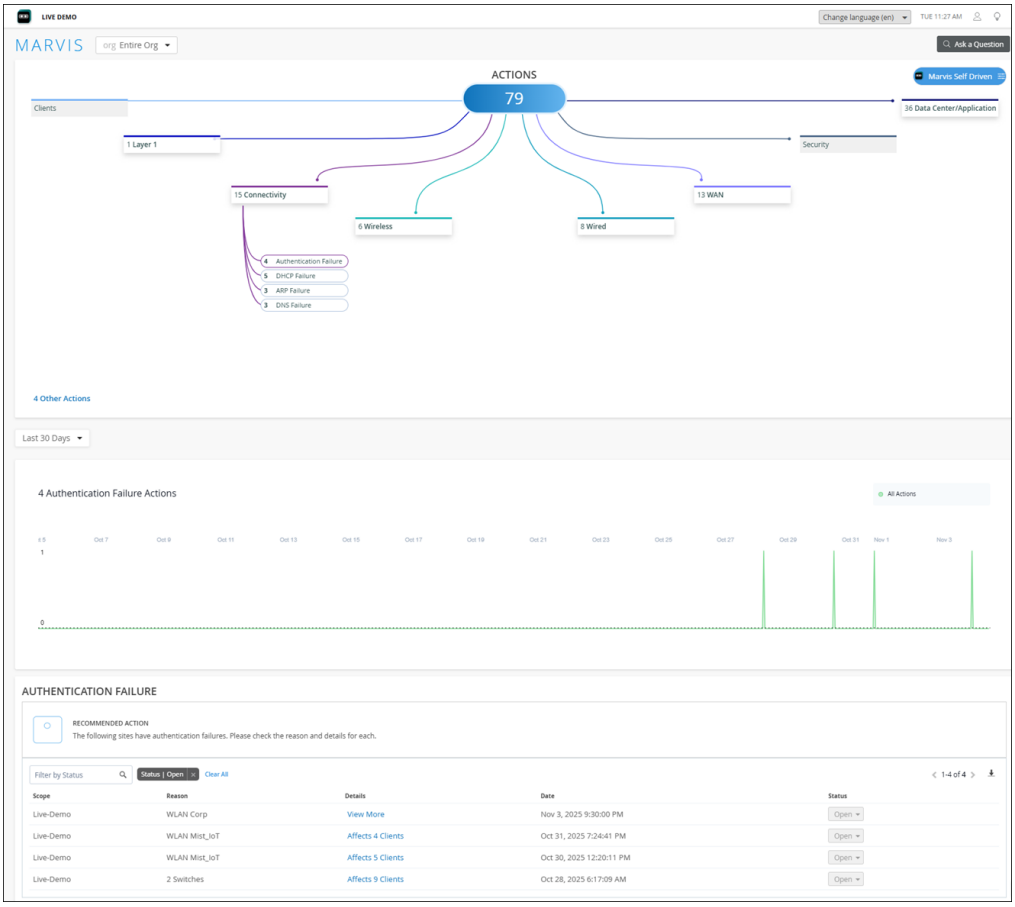
How Are Connectivity Failures Detected?

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 224.

  After you fix the issue, the action automatically resolves 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:



After you fix the issue, the action automatically resolves 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.

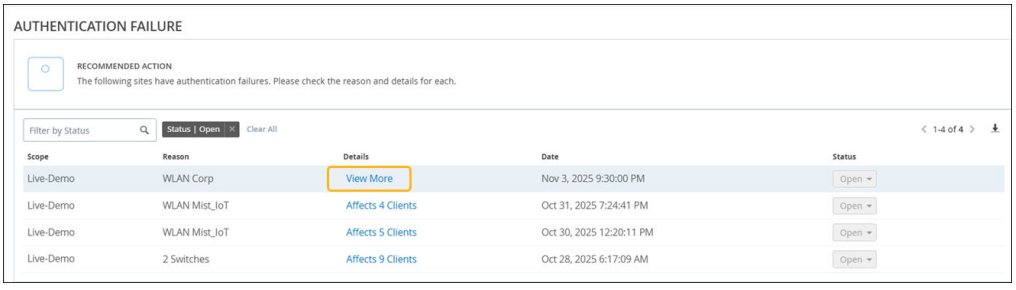
> **NOTE**: If you see a **View More** link in the Authentication Failure table, click the link to open the Event Card. For more information, see "Anomaly Detection Event Card" on page 224.

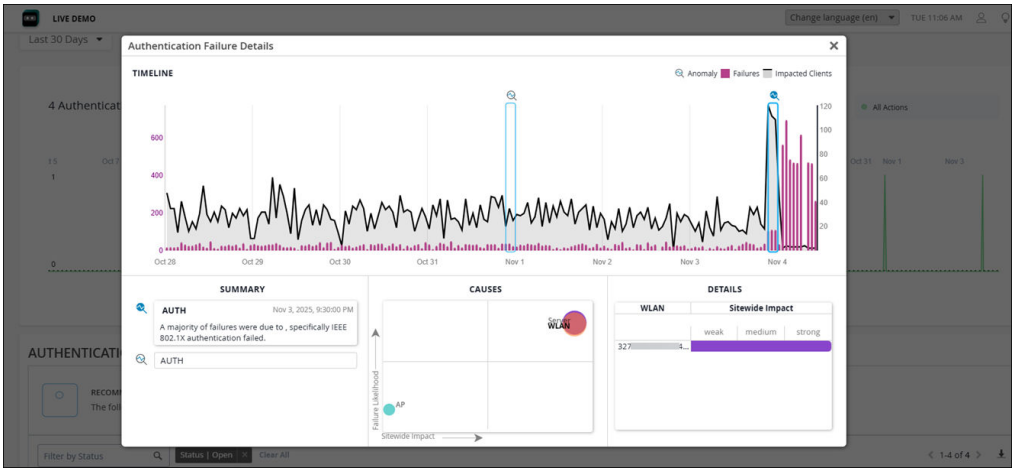
802.1x Failures

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:





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.

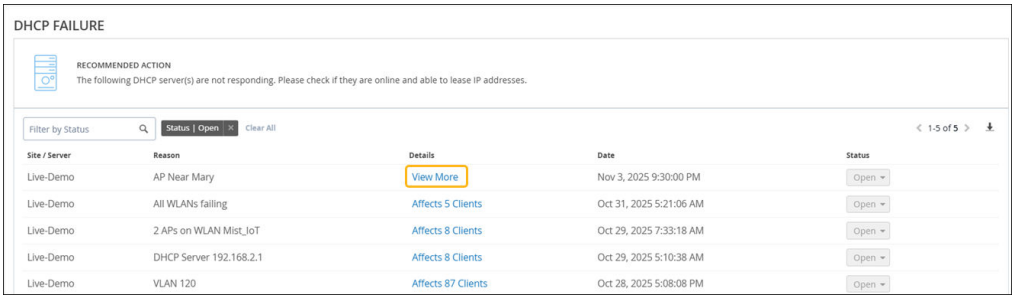
DHCP Failure

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.

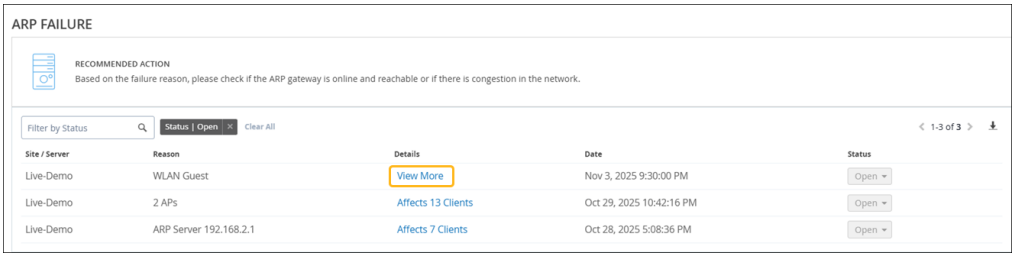
NOTE: For wired-only deployments, you must enable DHCP snooping for Marvis to detect DHCP failures.

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 224.



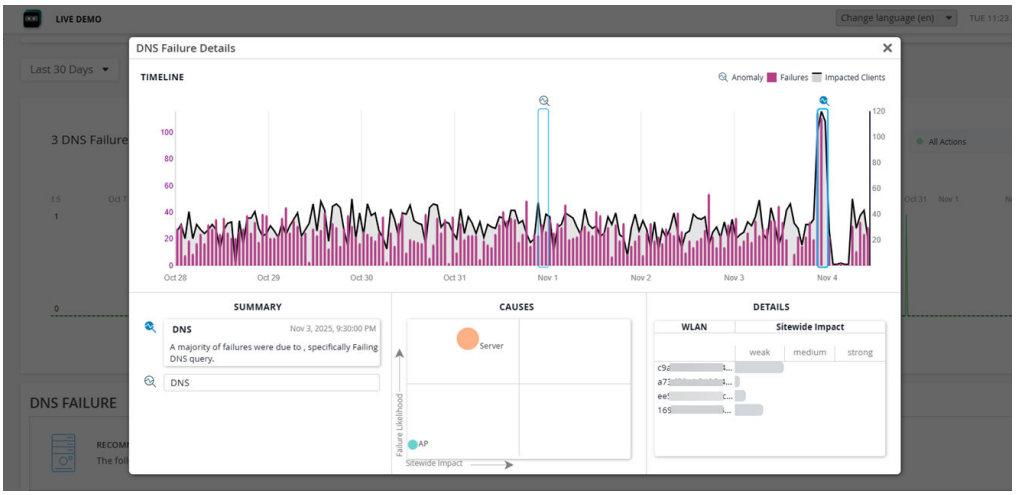
ARP Failure

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.



DNS Failure

Marvis detects 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.



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 224.

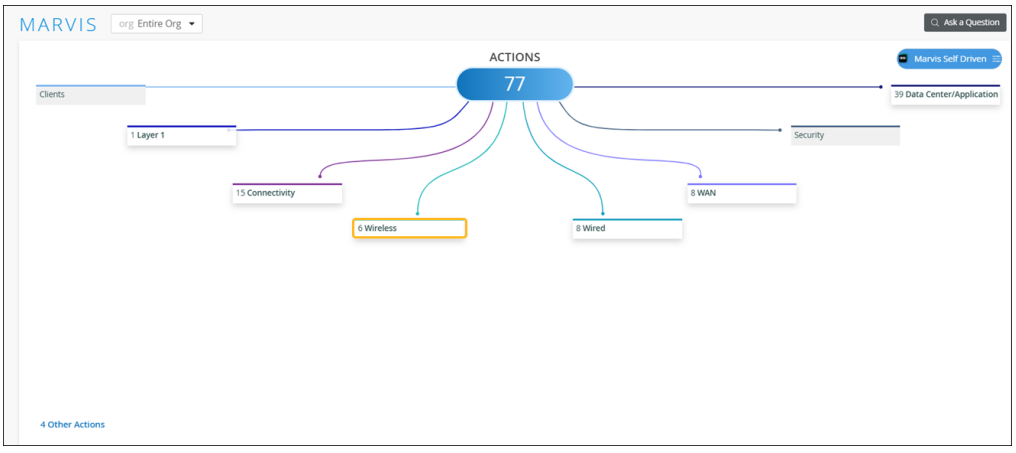
Wireless Actions

SUMMARY

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

IN THIS SECTION

When you click the Wireless 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.



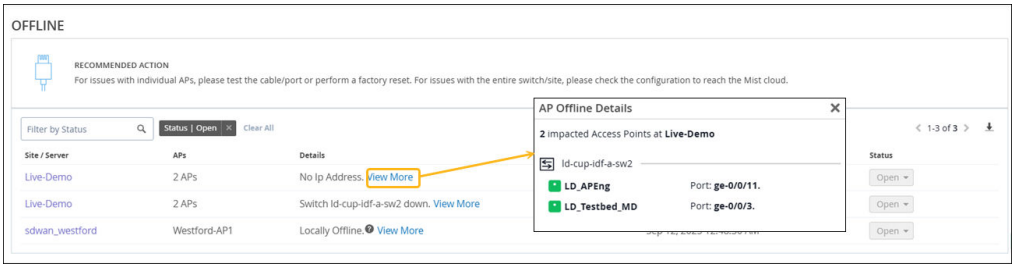
NOTE: Your subscriptions determine the actions that you can see on the Actions dashboard. For more information, see "Subscription Requirements for Marvis Actions " on page 171.

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 (heard locally but not connected to the cloud).
- An AP is locally offline (not heard locally and not connected to the cloud).

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



Health Check Failed

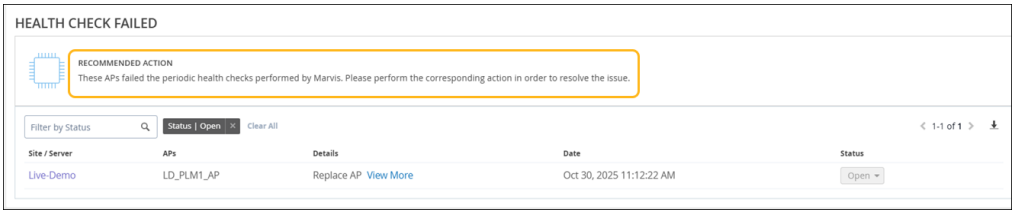
Marvis reports health check failures when it detects potential hardware or software issues.

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 to ensure 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.



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 within 30 minutes.

NOTE: The Non-Compliant Marvis action is a self driving action. By default, the self-driving capability for the Non-Compliant action is disabled. For information about the self-driving capability and how you can enable it, see "Self-Driving Marvis Actions" on page 166.

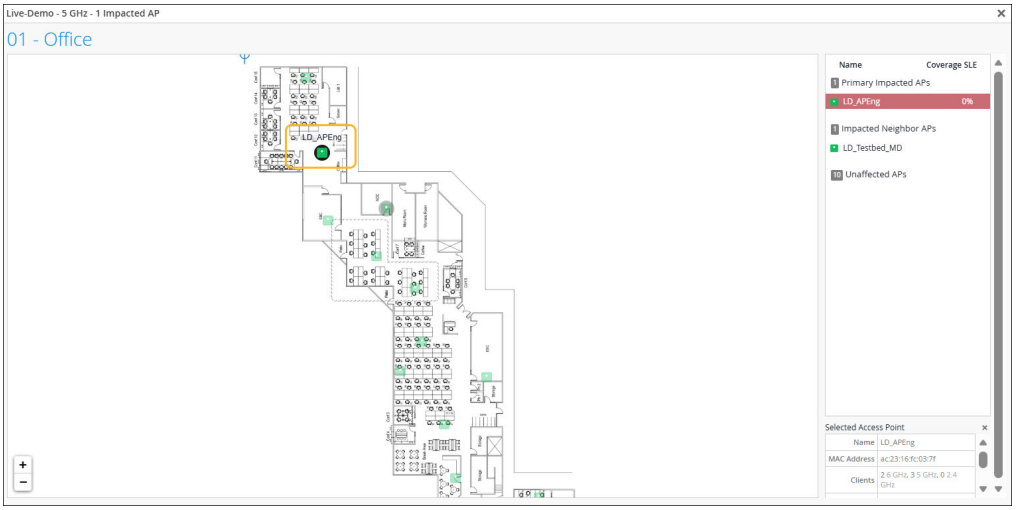
Coverage Hole

The Coverage Hole action detects coverage issues at your site and provides a floor plan indicating the APs with the issues. Use this visual to locate areas with low coverage. Then make necessary improvements, such as adding APs, upgrading firmware, changing AP placement, 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:

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

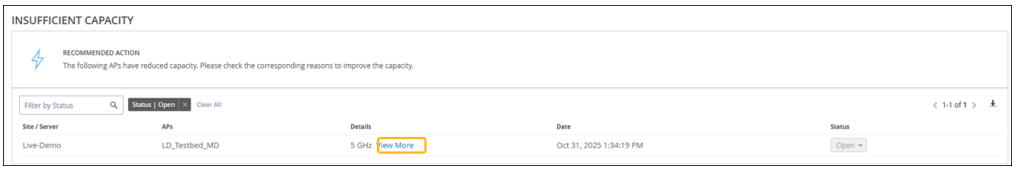


After you fix the issue in your network, Mist AI monitors the network for a certain period to ensure that the coverage is sufficient for the network. Hence, it might take up to 24 hours for the Coverage Hole action to automatically resolve.

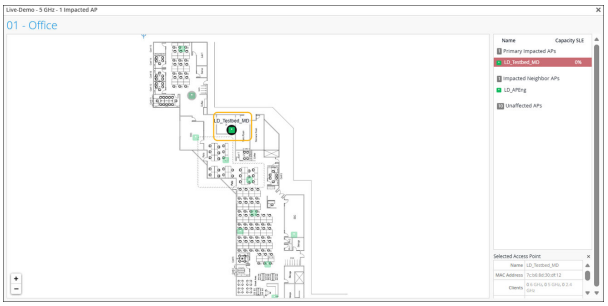
Insufficient Capacity

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.



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

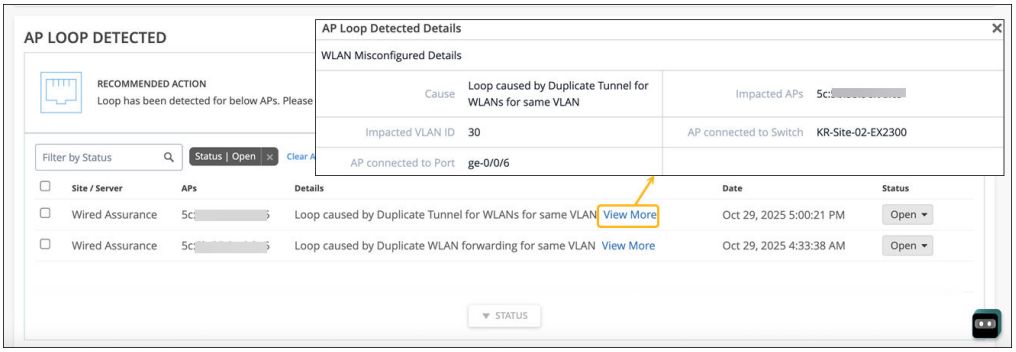


AP Loop Detected

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 datapaths 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,

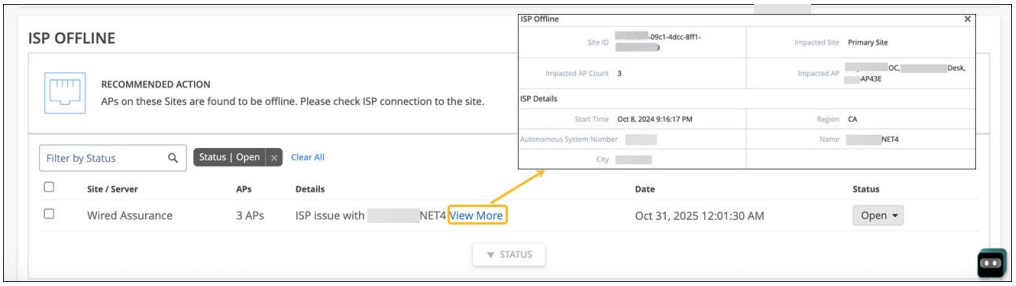


ISP Offline

While the AP Offline Marvis action flags APs that are offline due to a local network or cloud connectivity issue, the ISP Offline action focuses on APs that are offline due to ISP-related issues. Marvis detects APs that are offline due to, for example, issues with routing, DNS, incorrect network settings, or ISP regional outages.

Marvis can assess the scope of the issue, that is, it determines whether the issue is limited to APs in a specific site or APs across multiple sites. In addition, Marvis can also pinpoint the ISPs through which the impacted APs were connected, which makes the troubleshooting process easier.

Here's an example that shows an ISP Offline action. You can see that Marvis provides the details of the ISP such as name, ISP's Autonomous System Number (ASN), and region. It also lists the date and time from when the APs are offline. Marvis lists each impacted site separately with the list of offline APs and ISP details.



If you see an ISP Offline action, here are some of the steps that you can take:

- Check the ISP's portal to find out if there is any outage reported.
- Check the router or modem configuration for any changes.
- Contact the ISP support team.

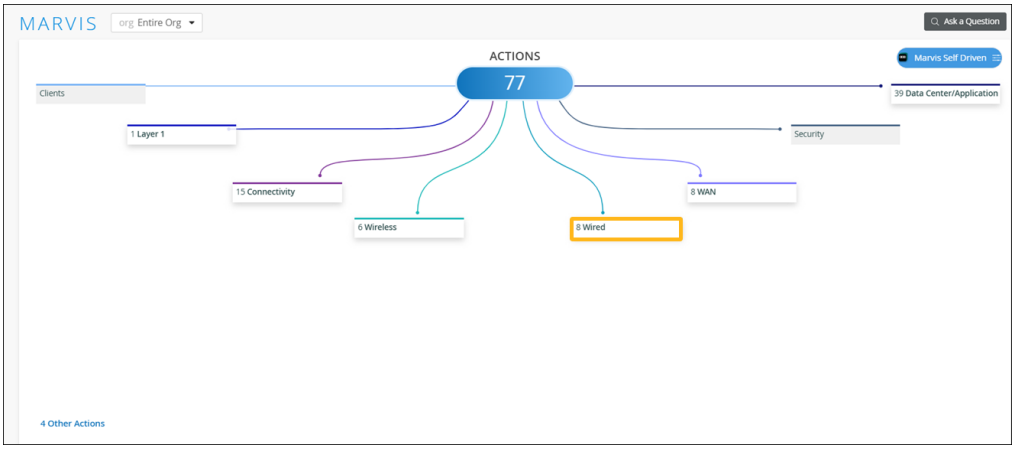
Wired Actions

SUMMARY

Use the Actions dashboard to resolve issues affecting your switches.

IN THIS SECTION

When you click the Wired 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.



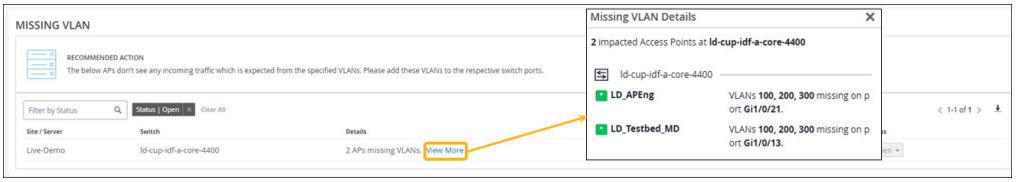
NOTE: Your subscriptions determine the actions that you can see on the Actions dashboard. For more information, see "Subscription Requirements for Marvis Actions " on page 171.

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.

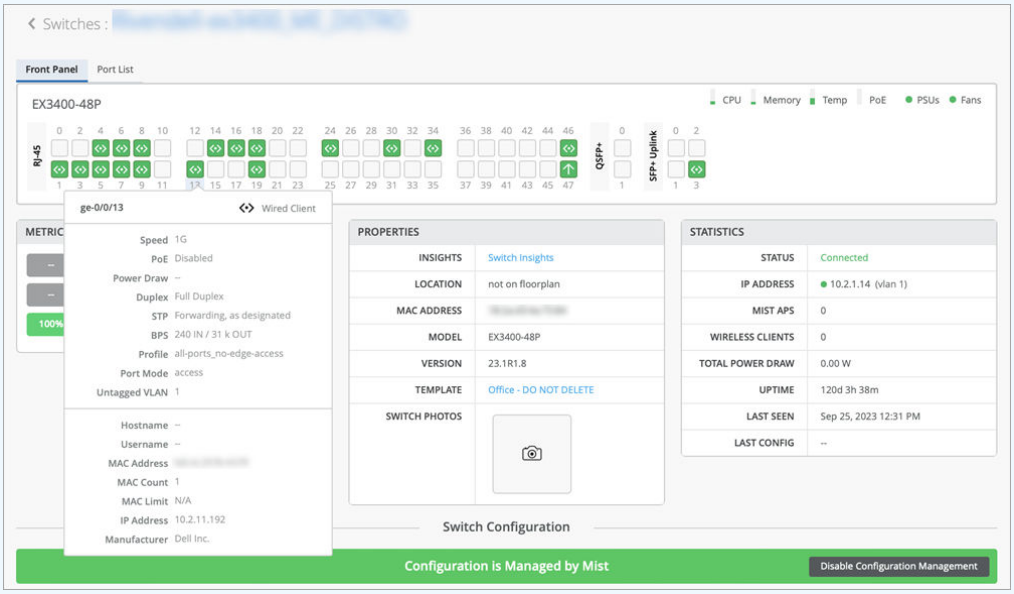
The switch can either be a Juniper EX Series or QFX series switch, or a third-party switch.

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.



When you see a Missing VLAN action, you can go to the Client Events section on the AP Insights page and check for failures on the VLAN that is reported in the Missing VLAN action. You can verify whether all the clients connecting on that VLAN are experiencing DHCP failures.

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.



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.

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.

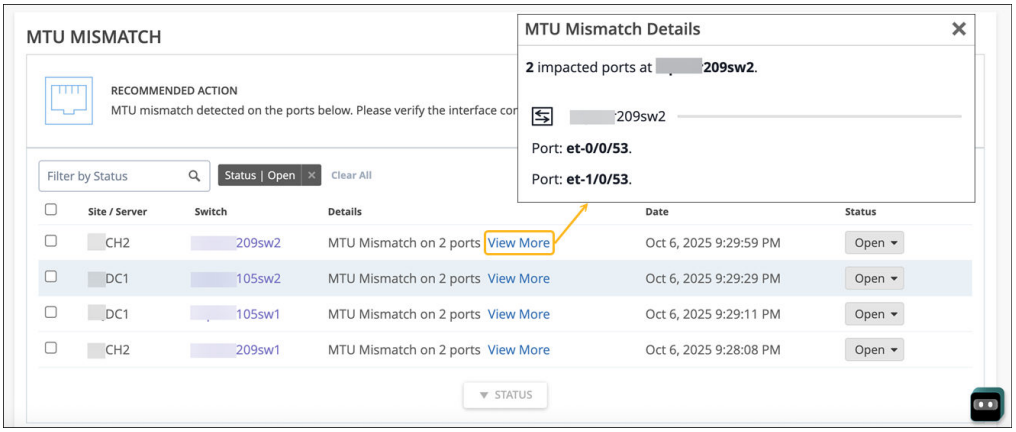
The following example shows the details for the Negotiation Incomplete action. Notice that Marvis lists the switch and the port on which the autonegotiation failed.

After you fix the issue in your network, the Negotiation Incomplete action automatically resolves 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.

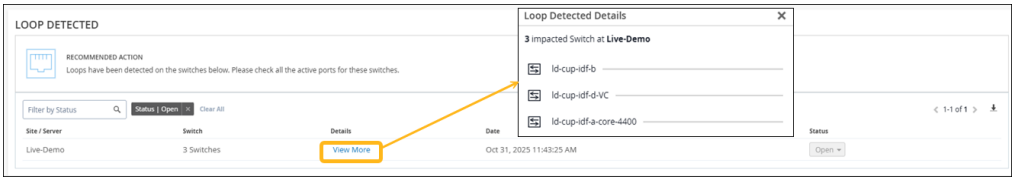
You'll need to review the port configuration on the switch and the connected device to resolve the issue. Here's an example of an MTU mismatch identified by Marvis. The **Details** column lists the port on which the mismatch occurs.



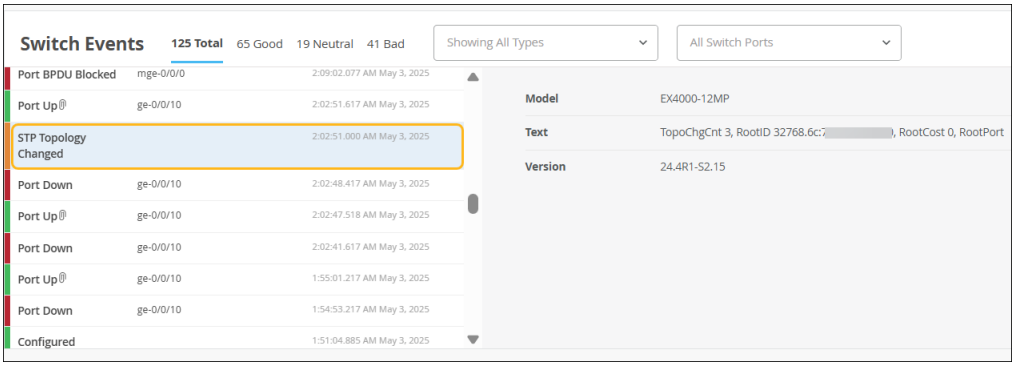
Loop Detected

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:

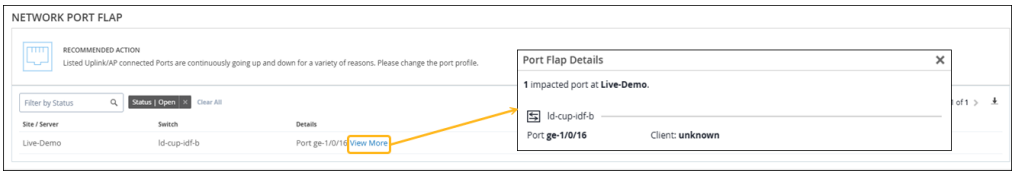


Switching loops are listed under Switch Events on the Switch Insights page. In the following example, you can see the STP topology change listed.



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:



You can view the port up and port down events under Switch Events on the Switch Insights page. Marvis does not list slow port flaps as an action unless the flapping frequency increases. Marvis continues to monitor the slow port flapping to determine the severity of the issue. If the flapping becomes excessive, Marvis lists it as an action after considering the frequency and severity. You can use the conversational assistant to view details about slow port flaps.

For details about access port flaps, see "Access Port Flap" on page 208,

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.

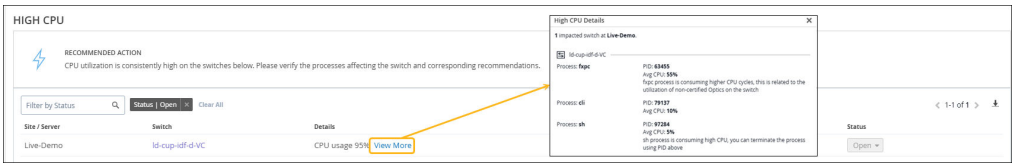
After you fix the issue in your network, the Port Flap action automatically resolves within an hour.

Video: Port Flap

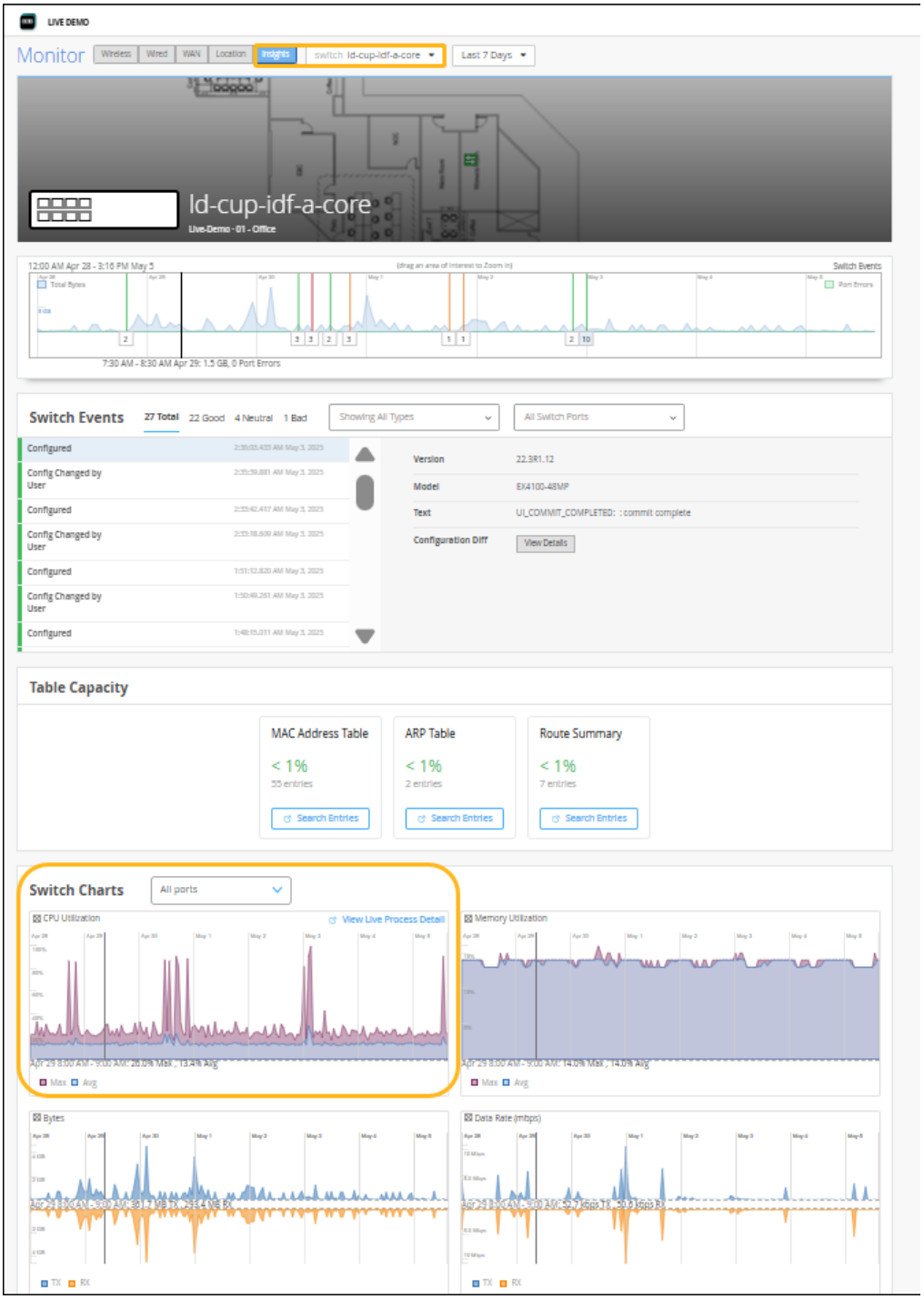
High CPU

Marvis detects switches that constantly have high CPU utilization (> 90%). 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:



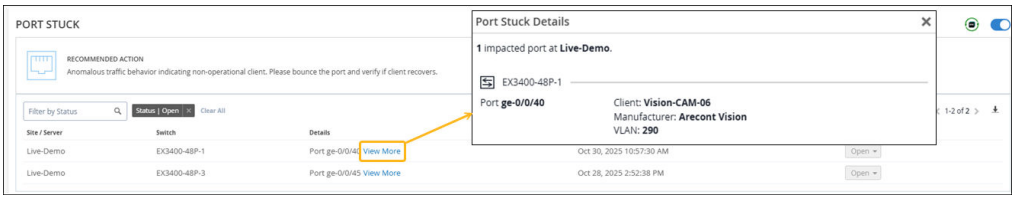
If you see a High CPU action, you can go to the Insights page for the switch and analyze the CPU Utilization chart under Switch Charts. Here's an example:



Port Stuck

The Port Stuck action detects a difference in traffic pattern on an access port of a switch, 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.

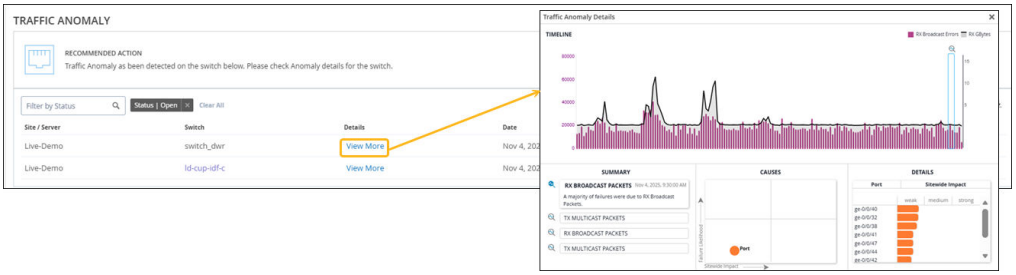


When Marvis detects a port stuck issue, it initiates an automatic port bounce to fix the issue. If the automatic port bounce fails to resolve the issue, Marvis lists it as an action. You can view the automatic bounce action under Switch Events on the Switch Insights page as shown in the following example. The graph on the right shows the traffic before and after the port bounce. You'll see that before the port bounce only the Tx traffic is seen (indicated in green). After the port bounce, you'll see that the Rx traffic is also seen.

NOTE: The self-driving capability for the Port Stuck action is enabled by default. For information about the self-driving capability, see "Self-Driving Marvis Actions" on page 166.

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.



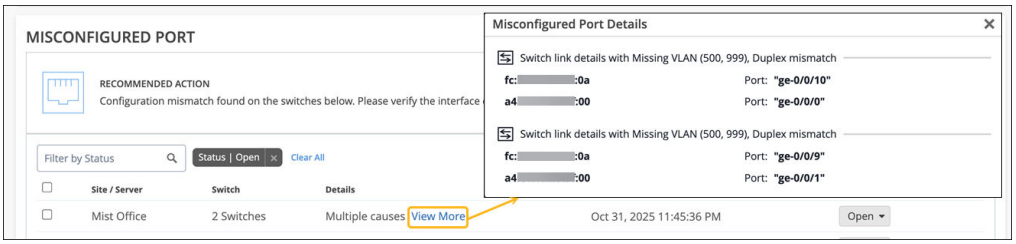
Video: Marvis Can Detect Switch Traffic Anomalies

Misconfigured Port

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

- 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.



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

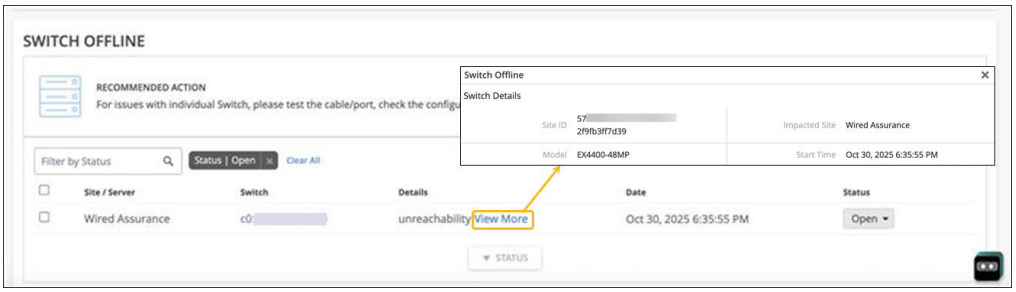
Switch Offline

Marvis detects switches that are disconnected from the Juniper Mist cloud. Switches can go offline due to many reasons including the following:

- Power issues
- Faulty cable
- Required firewall ports are not open
- Incorrect configuration

When a switch goes offline, Marvis monitors the switch to check the duration of the offline status. If the switch is offline for more than three minutes, Marvis generates the Switch Offline action. Note that the Switch Offline infrastructure alerts and events on the Switch Insights page show up as soon as a switch goes offline.

Here's an example that shows the the Switch Offline Marvis action. Click the **View More** link to view details of the switch that is offline. If you click the switch name, then you can view the Insights page where you can view the event listed under Switch Events.



To troubleshoot a switch that is offline, see Troubleshoot Your Switch Connectivity.

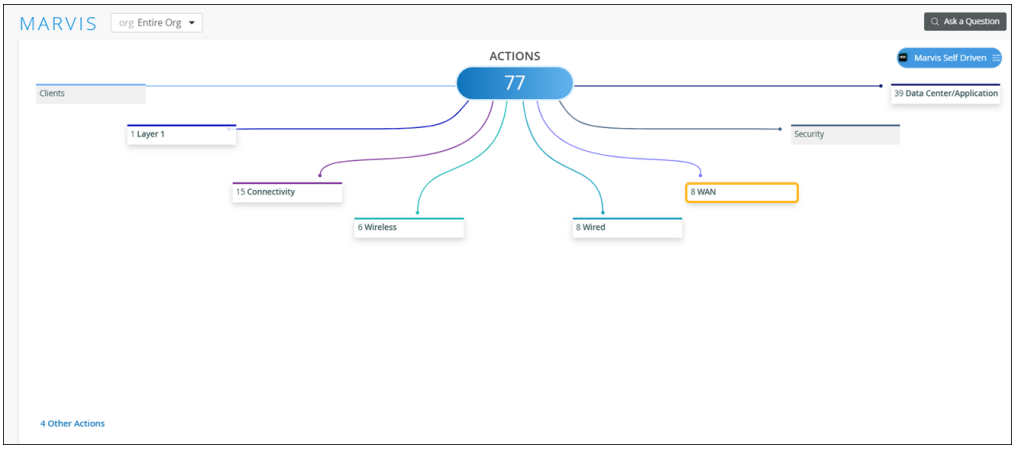
WAN Actions

SUMMARY

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

IN THIS SECTION

When you click the WAN 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 171.

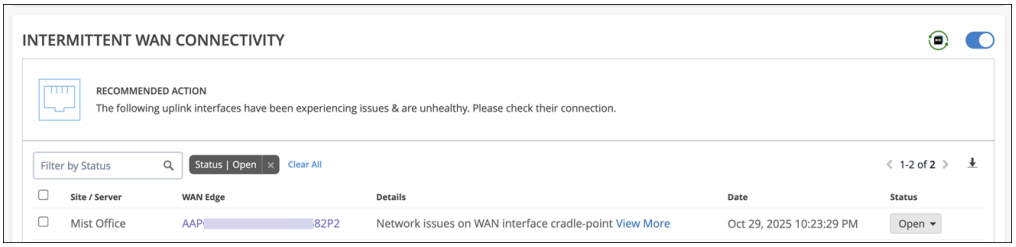
MTU Mismatch

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.

Intermittent WAN Connectivity

The Intermittent WAN Connectivity action identifies interface-related issues on WAN Edge devices such as uplink interface not receiving an IP address or the gateway ARP not being resolved for the uplink. These issues can cause poor user experience and result in an unhealthy WAN link. You might see errors in forming the overlay.

When you see an Intermittent WAN Connectivity 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:



An Intermittent WAN Connectivity action can be triggered when the ARP resolution for the ISP server's gateway IP address fails. The ISP ARP failure occurs when the WAN Edge device is unable to resolve the gateway's IP address to its corresponding MAC address. This issue can lead to network connectivity issues, as traffic cannot pass through the gateway, preventing the WAN Edge device from accessing external networks or Internet services.

Failure to obtain an IP address from the ISP can also trigger this action. In this case, the WAN Edge device is unable to connect to the Internet as it is unable to obtain an IP address from the ISP DHCP server.

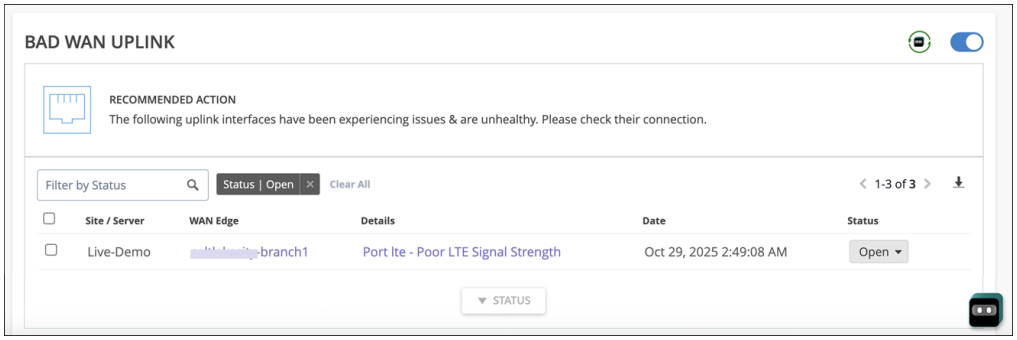
NOTE: The self-driving capability is enabled for the Intermittent WAN Connectivity action by default. When Marvis detects an ISP ARP or ISP DHCP failure, it initiates an automatic port bounce in an attempt to fix the issue. If the automatic port bounce fails to resolve the issue, Marvis lists it as an open action. For information about the self-driving capability, see "Self-Driving Marvis Actions" on page 166.

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 due to poor LTE connectivity. For a bad LTE WAN link, Marvis shows a timeline of 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:

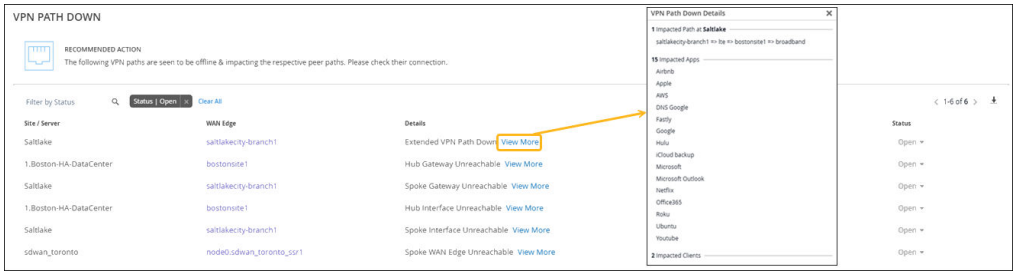
- Received signal strength indicator (RSSI)
- Reference Signal Received Power (RSRP)
- Signal-to-noise ratio (SNR)



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.

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 VPN tunnels or peer paths toward 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.



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.

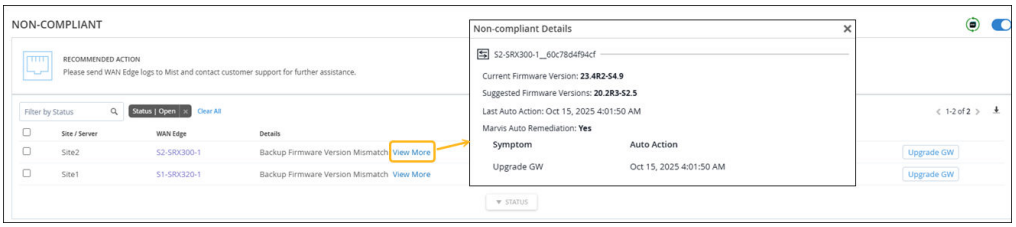
- Spoke Gateway Unreachable—All the paths originating from a spoke are experiencing a peer path down issue.
- Hub Gateway Unreachable—All the paths terminating at a hub are experiencing a peer path down issue.
- Hub Interface Down—All the paths to a hub interface are down as the hub interface is down.

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.

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.



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

NOTE: The Non-Compliant Marvis action is a self driving action. By default, the self-driving capability for the Non-Compliant action is disabled. For information about the self-driving capability and how you can enable it, see "Self-Driving Marvis Actions" on page 166.

Negotiation Incomplete

The Negotiation Incomplete action for WAN Edges detects instances on the WAN Edge ports where autonegotiation failures occur. This issue can occur due to a duplex mismatch between the WAN Edge

and the connected device 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.

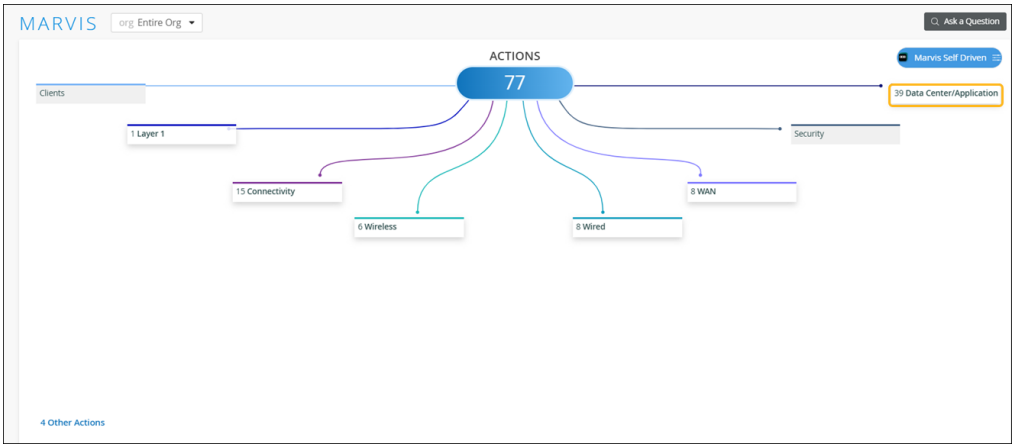
Data Center/Application Actions

SUMMARY

Use the Actions dashboard to resolve issues affecting your data centers or applications.

IN THIS SECTION

When you click the **Data Center/Application** button on the Actions dashboard, you'll see a list of all available actions. You can then click an action to investigate further.



Data Center Actions

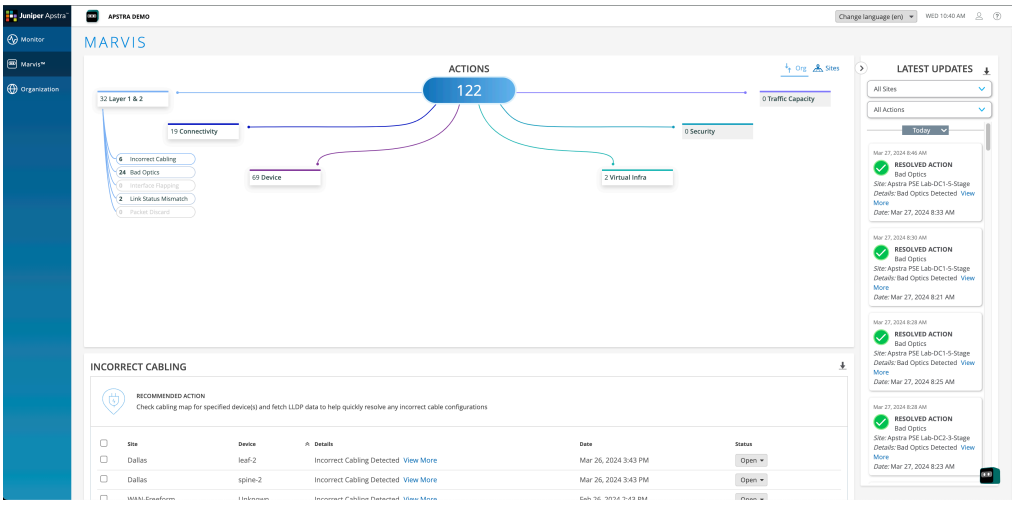
If you manage your enterprise network with Juniper Mist and your data centers with Juniper Apstra, you can click **Data Center Actions** to quickly view what the Marvis Virtual Network Assistant for Data Center has collected.

> **NOTE**: For **Data Center Actions** to be visible, you must perform some configuration in both your Juniper Mist portal and your Juniper Apstra Cloud Services portal. See Access Apstra Cloud Services.

When you click **Data Center Actions**, a new browser window or tab displays the Marvis Actions page in your Juniper Apstra Cloud Services portal. See Figure 1 on page 205.

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

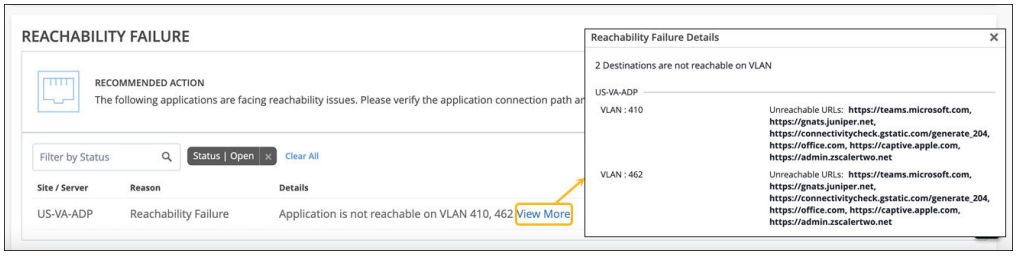
Figure 4: Marvis Actions Page on Juniper Apstra Cloud Services Portal



Reachability Failure

Marvis highlights application reachability failures detected by Marvis Minis as an action. Marvis Minis validates application reachability as part of its validation.

While the Marvis Minis page provides the details of validations run for DHCP, ARP, DNS, and application reachability, the Reachability Failure action focuses on the application reachability failures identified by Marvis Minis. Application reachability is key to user experience and this action provides you early visibility into the issue and enables you to address the issue before it impacts users.



RELATED DOCUMENTATION

- Access Juniper®Data Center Assurance
- Juniper Data Center Assurance Overview

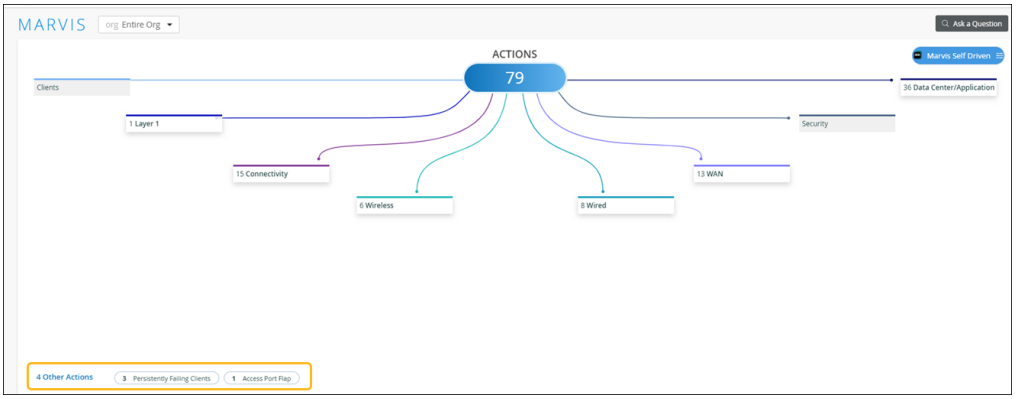
Other Marvis Actions

SUMMARY

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

IN THIS SECTION

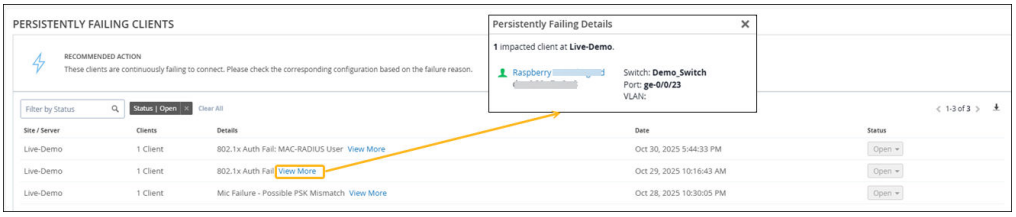
When you click the Other Actions link on the Action dashboard, all available actions appear. Currently this category includes only two types of actions: Persistently Failing Clients and Access Port Flap.



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 171.

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.



NOTE: After you fix this issue, the Persistently Failing Clients action automatically resolves within an hour.

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:

Marvis Actions: An Insight into Back-End Operations

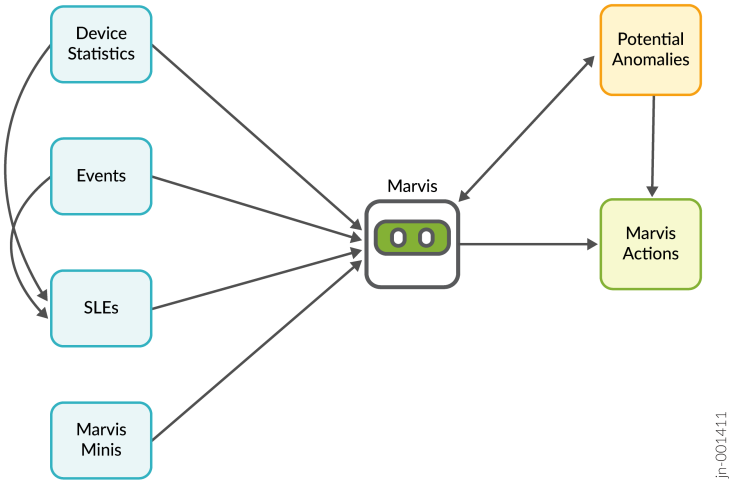
SUMMARY

Take a closer look at the factors that Marvis uses to identify key issues and to categorize them as Marvis actions.

IN THIS SECTION

Marvis proactively scans your network for events and actionable insights. Using data from statistics and events, Marvis identifies user-impacting issues pertaining to wired, WAN, and wireless connectivity for both pre-connection and post-connection experiences. By highlighting high efficacy actions and automating root cause analysis, Marvis helps reduce mean time to resolution/innocence (MTTR/MTTI).

Note that Marvis Actions does not replace alerts. Alerts are triggered in real-time as and when events occur, for example a port up or down event. For information about alerts, see Alerts Overview.



Glossary of Terms

Term	Definition
Model input feature	The inputs or features that the model consumes to determine whether the condition for generating the specific action is met.
Trigger conditions	The conditions that trigger the model to create Marvis actions.
Validation time	The time taken for Marvis to mark an open Marvis action as resolved. A user might have fixed the issue. Or the symptoms might not beobserved anymore.

Layer 1 Actions

Marvis Action	Model Input Feature	Trigger Conditions	Validation Time
Bad Cable	AP, switch, or WAN Edge statistics, events	Speed changes, errors reported on ports, switch port link active but not passing traffic, and frequent disconnections and restarts (only APs) over the monitored period.	7 days

Connectivity Actions

Marvis Action	Model Input Feature	Trigger Conditions	Validation Time
Authentication Failure	Wired and Wireless clients	Deviations from the predicted baseline. The LSTM-based model baselines authentication success or failure events across the site. The model considers the severity of the issue to generate this Marvis action. The higher the severity and deviation from the baseline, the higher the confidence of the model to generate this action within the observed time duration.	1 day
DHCP Failure	Wired and Wireless clients	Deviations from the predicted baseline. The LSTM-based model baselines Dynamic Host Configuration Protocol (DHCP) success or failure events across the site. The model considers the severity of the issue to generate this Marvis action. The higher the severity and deviation from the baseline, the higher the confidence of the model to generate this action within the observed time duration.	1 day

(Continued)

Marvis Action	Model Input Feature	Trigger Conditions	Validation Time
ARP Failure	Wired and Wireless clients	Deviations from the predicted baseline. The LSTM-based model baselines Address Resolution Protocol (ARP) success or failure events across the site. The model considers the severity of the issue to generate this Marvis action. The higher the severity and deviation from the baseline, the higher the confidence of the model to generate this action within the observed time duration.	1 day
DNS Failure	Wired and Wireless clients	Deviations from the predicted baseline. The LSTM-based model baselines Domain Name System (DNS) success or failure events across the site. The model considers the severity of the issue to generate this Marvis action. The higher the severity and deviation from the baseline, the higher the confidence of the model to generate this action within the observed time duration.	1 day

Wireless Actions

Marvis Action	Model Input Feature	Trigger Conditions	Validation Time
Offline	AP statistics	One AP or multiple APs are locally up or down (loss of cloud connectivity only). The model correlates to identify the cause for the AP being down—that is, if the issue is due to a switch, site, region, or ISP outage. If you want to be notified when devices go offline, configure infrastructure alerts for device up or down events and specify a threshold.	15 minutes

(Continued)

Marvis Action	Model Input Feature	Trigger Conditions	Validation Time
Health Check Failed	AP statistics	AP or radios remain repeatedly inoperable after autorecovery.	30 days
Non-Compliant	AP statistics	Difference in firmware version on an AP or multiple APs from that in the version compliance settings configured under site settings.	30 minutes
Coverage Hole	AP and client statistics	Anomaly in the SLE baseline caused due to repeated low RSSI reported by all clients associated with an AP or multiple APs in a high-impact area. The model considers the recurrence of the issue and fringe pattern awareness in the case of outdoor APs or APs located at the building entry or exit. The model considers the strength of the anomaly to generate the Marvis action to indicate a user-impacting coverage-hole issue. If the anomaly index is strong, the model generates the action faster than when the anomaly index is weak. The model examines multiple batches of data to identify APs for coverage-hole issues.	7 days
Insufficient Capacity	AP and client statistics	Anomaly in the baseline caused by APs with repeated and prolonged capacity constraints that are not seasonal in nature. The model factors the anomaly strength to generate the Marvis action to indicate a user-impacting capacity issue. If the anomaly index is strong, the model generates the action faster than when the anomaly index is weak. The model examines multiple batches of data to identify APs for capacity issues.	7 days

(Continued)

Marvis Action	Model Input Feature	Trigger Conditions	Validation Time
AP Loop Detected	AP events	Reflection events on an AP triggered by network loops caused due to misconfiguration or incorrect configuration. Reflection events occur when an AP receives the packet it sent on the same or different VLAN. Reflection events are generated almost immediately under site events, enabling you to monitor these events for raw statistics-based tracking.	30 minutes

Wired Actions

Marvis Action	Model Input Feature	Trigger Conditions	Validation Time
Missing VLAN	AP port statistics	Uplink port statistics reported by an AP missing a VLAN. This action correlates data from two or more APs to determine whether an active VLAN used by clients is missing on the AP port. This correlation helps prevent generation of the **Missing VLAN** action if a VLAN is unused by any client across the entire site.	30 minutes
Negotiation Incomplete	Individual switch port statistics	Autonegotiation failure reported on the switch ports.	Up to 60 minutes

(Continued)

Marvis Action	Model Input Feature	Trigger Conditions	Validation Time
MTU Mismatch	Individual switch port statistics	MTU mismatch between any switch port and connected devices. The reported statistics indicate errors on the port. The model considers the severity and time to generate the Marvis action. The greater the MTU mismatch, the greater the severity, resulting in faster generation of the Marvis action.	1 day
Loop Detected	Switch port events	An intentionally or unintentionally introduced loop in the topology resulting in rapid and repeated Spanning Tree Protocol (STP) topology changes. The model uses the STP topology changes event as an input feature and considers the severity and time. The higher the frequency of STP topology changes in each period, the faster the detection. Alternatively, a loop causing events at a slower pace for a longer duration also triggers the Marvis action.	30 minutes
Network Port Flap	Switch ports events (trunk port only)	Consistent port bounce on a port configured as a trunk port. The model considers the frequency and time. The higher the frequency of port flaps, the higher the severity of the issue. For slow port flaps that occur for a longer duration, the model detects the port flaps within a couple of hours or a few days.	30 minutes
High CPU	Switch chassis statistics	Average CPU utilization consistently greater than 90% for the monitored duration. The model considers the frequency and duration of the issue. Statistics that show high average CPU utilization for every sample in the monitored dataset indicate a severe user-impacting issue. The model generates the Marvis action quickly for such an issue.	30 minutes

(Continued)

Marvis Action	Model Input Feature	Trigger Conditions	Validation Time
Port Stuck	Switch port statistics	Sudden deviation in traffic patterns for end devices on access ports. The model does not generate false positives for recurring seasonal traffic patterns. It also considers traffic patterns across similar endpoints for inference. . This Marvis action is self-driving. When a *port stuck* issue is detected, the port is automatically bounced to operationalize the endpoint again. The model generates the action only if the endpoint fails to come back into operation after an automatic port bounce or if the port stuck issue recurs multiple times. .	30 minutes
Traffic Anomaly	Switch port statistics	Any deviation in broadcast and multicast frame counters from the predicted traffic patterns. The model baselines traffic patterns on each switch or switch port every couple of days. This action uses the *long short-term memory* (LSTM)-based model. The model generates this Marvis action based on the severity of the issue. For strong deviations that last for the entire monitored duration, the model generates the action quickly. The model might take longer to generate actions for minor, longer-lasting deviations.	1 day
Misconfigured Port	Uplink switch port statistics	MTU, VLAN, mode, or duplex mismatches between identified uplink ports. The model identifies discrepancies on the switch-switch connections at the edge.	60 minutes

WAN Actions

Marvis Action	Model Input Feature	Trigger Conditions	Validation Time
MTU Mismatch	WAN Edge statistics	MTU mismatch between a WAN Edge port and connected devices. The model examines the reported statistics that indicate certain errors on the port. The model considers the severity and time to generate this Marvis action. The greater the MTU mismatch, the greater the severity, and the action is generated within a specific time duration.	30 minutes
Bad WAN Uplink	Uplink ports on WAN Edges	High latency, packet drops, congestion, and network service failures such as ARP or DHCP reported in the WAN port statistics, indicating a change in the baseline behavior. Issues determined as high-severity issues are listed sooner than the low-severity issues.	1 day
VPN Path Down	VPN tunnels or peer paths	Peer-path down issue in either of the following paths: • Paths originating from a spoke toward a specific hub • Paths terminating at a hub Subscribe to the critical port monitoring alert for raw alerting if your requirement is to get alerts on every port up or port down scenario. Issues determined as high-severity issues are listed sooner than the low-severity issues.	1 hour
Non-Compliant	SRX Series Firewall	Difference in Junos OS version on the primary and backup partitions.	30 minutes

Other Marvis Actions

Marvis Action	Model Input Feature	Trigger Conditions	Validation Time
Persistently Failing Clients	Wired and Wireless clients	Clients continuously failing to authenticate and connect to the network. Persistent failures are observed continuously during the monitored time frame. The trigger time is dependent on the site—that is, the number of clients and correlated simultaneous failures.	60 minutes
Access Port Flap	Access ports on a switch	Consistent port up or port down events for a port configured as an access port. The model considers the frequency and duration of the issue. The higher the frequency of port flaps, the higher the severity of the issue. For slow port flaps that occur for a longer duration, the model detects the port flaps within a couple of hours or a few days.	30 minutes

Potential Anomalies Detected by Marvis

SUMMARY

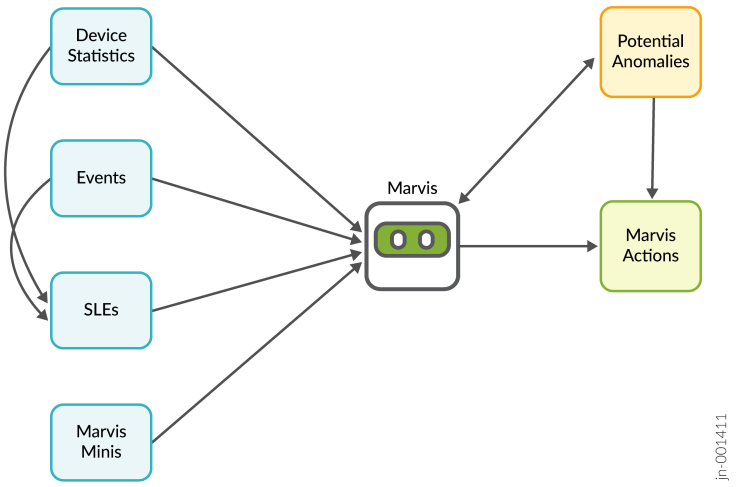
Potential anomalies help identify user-impacting site-level and device-level operational issues.

IN THIS SECTION

View Potential Anomalies on the Insights Page | 223

Marvis continuously monitors and analyzes data and events generated by APs, switches, and WAN Edges in real time. Marvis leverages information from device telemetry, system logs, and performance metrics to intelligently surface events that signal user-impacting issues across your network. These events are flagged as potential anomalies and are displayed on the Insights page in the Juniper Mist portal. For every potential anomaly detected, Marvis also provides a recommended remediation step that you can follow to resolve the issue.

Covering a wide range of issues ranging from hardware and connectivity issues to configuration inconsistencies and performance degradations,these anomalies can be at the site level (for example, DHCP failure) or device level (for example, device health). Marvis-highlighted anomalies are an indicator of issues that might translate into Marvis Actions.



The potential anomalies serve as early warning signals enabling administrators to take action before minor issues escalate into major disruptions. Network administrators gain precise, real-time visibility into where and why issues occur, resulting in a significant improvement in operational efficiency and reduction in troubleshooting effort and time.

Subscription Requirements

Similar to Marvis Actions, you can view the list of potential anomalies based on your subscription type—Marvis for Wired, Marvis for Wireless, and Marvis for WAN. For example, if you have a Marvis for Wired subscription, you can view only the switch-related anomalies.

However, you can view site-level potential anomalies such as DHCP, DNS, and ARP-related events even if you do not have a Marvis subscription.

List of Potential Anomalies for APs

You can view the anomalies detected for APs if you have a Marvis for Wireless subscription.

Table 21: List of Potential Anomalies for APs

Anomaly	Factors Triggering the Anomaly
Bad Cable	Speed transistions, port errors, or frequent device restarts.
Missing VLAN	AP unable to detect or operate on its assigned VLAN. This issue can be attributed mostly to one of the following: • Switch port misconfiguration • Incorrect VLAN settings (allowed VLANs or native VLAN) on the switch uplink trunk port or the port to which the AP is connected • Upstream filtering
Ethernet Error	Ethernet interfaces on the AP report generic errors such as CRC errors and input-output errors.

Table 21: List of Potential Anomalies for APs *(Continued)*

Anomaly	Factors Triggering the Anomaly
AP Loop Detected	AP detects a potential loop in the network topology. A loop can be caused due to an incorrect configuration. Some common issues that can cause loops are: • 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. • Loop on the wired network where the AP receives the packet that it sends out.
Low Power	AP receiving less PoE from the switch port. A common cause for this issue can be one of the following: • PoE negotiation issue • Insufficient PoE budget on the switch • Switch unable to support the required AP power in PoE+ or PoE++ mode
Low Ethernet Speed	The Ethernet port on the AP negotiates at a speed lower than expected (for example, 100 Mbps instead of 1 Gbps). The low speed can be due to one of the following: • Potential bad cable An Ethernet cable with missing pairs can result in intermittent or no connectivity, and possibly slow speeds. • Hardware capability mismatches • Negotiation failures

List of Potential Anomalies for Switches

You can view the potential anomalies for switches if you have a Marvis for Wired subscription.

Table 22: List of Potential Anomalies for Switches

Anomaly	Factors Triggering the Anomaly
Bad Cable	Physical layer issues such as speed changes, errors reported on ports, and active switch port links not passing traffic.
Switch Health	Switch health impacted by one of the following: • High CPU usage • Excessive temperature • Port misconfiguration (role/VLAN/STP mismatch) • High memory usage • Power draw exceeding safe limits
Negotiation Mismatch	Ethernet links with inconsistent settings across peers, such as MTU mismatches causing packet fragmentation or auto-negotiation failures leading to duplex mismatches.
Switch STP Loop	The Spanning Tree Protocol (STP) identifies a loop in the Layer 2 network, which might cause broadcast storms or connectivity issues.
DHCP Pool Exhausted	The DHCP server associated with the switch runs out of IP addresses, preventing devices from obtaining IP addresses for network connectivity.

List of Potential Anomalies for WAN Edges

You can view potential anomalies for WAN Edges if you have a Marvis for WAN subscription.

Table 23: List of Potential Anomalies for WAN Edges

Anomaly	Factors Triggering the Anomaly
Backup Firmware Invalid	Missing backup firmware, difference in the active and backup firmware versions, or outdated firmware version.
Gateway Health	A major WAN Edge subsystem experiences high load due to control plane CPU overload, high memory usage, or data plane CPU overload, potentially impacting routing, management, and packet forwarding.
Path Flap	Network paths between the WAN Edge and upstream peers change frequently enough to be considered as instable rather than a failure.
Port Flap	An interface repeatedly switches to the Up or Down state over a monitored window, indicating cable issues, loose connections, or negotiation errors.
Bad Cable	Physical layer issues such as speed changes and errors reported on ports.
Negotiation Mismatch	An MTU configuration mismatch between the WAN Edge and peer devices. MTU mismatches can cause packet fragmentation or packet drops.
Network Issue	The WAN Edge detects excessive packet loss, latency, jitter, or IPsec errors that might indicate tunnel instability.
HA Control Link Down	The High Availability control link between redundant WAN Edges is lost, preventing failover synchronization or role transitions.

Table 23: List of Potential Anomalies for WAN Edges *(Continued)*

Anomaly	Factors Triggering the Anomaly
LTE Signal	The LTE modem reports low signal quality, impacting cellular failover or primary transport.
ISP Reachability	The WAN Edge is unable to reach the ISP due to upstream service failures such as ARP resolution issues or DHCP IP configuration failures.
Congestion	High queue occupancy or output drops that indicate congestion on a WAN Edge interface.

List of Potential Anomalies for Sites

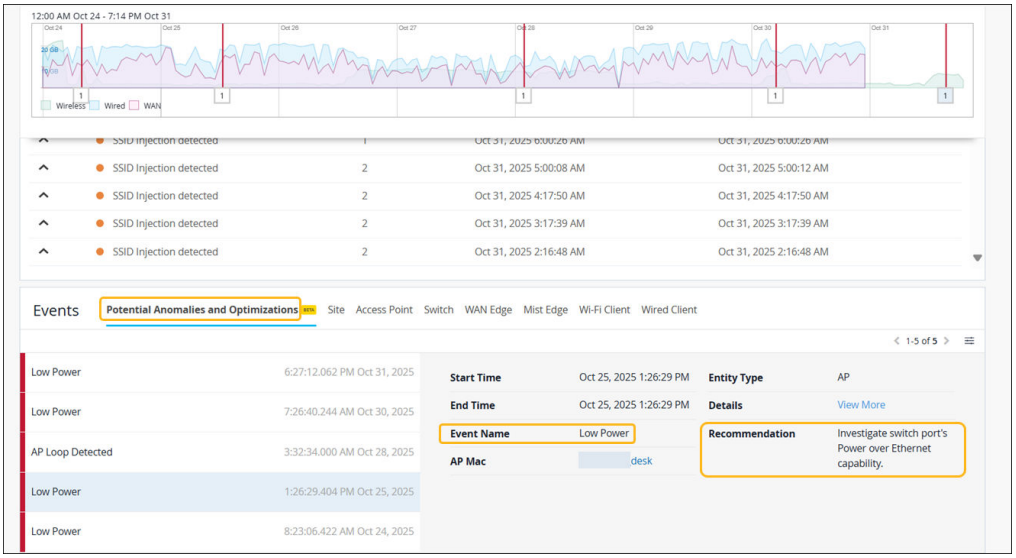
You can view site-level pre-connect (DHCP, DNS, and ARP) anomalies even if you do not have a Marvis subscription.

Table 24: List of Potential Anomalies for Sites

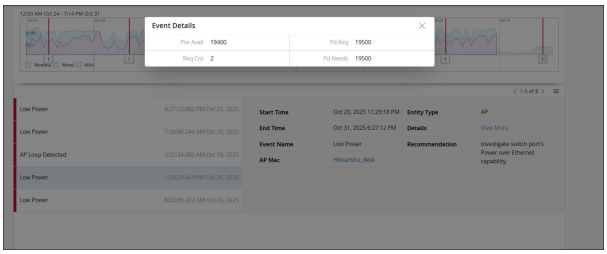
Anomaly	Factors Triggering the Anomaly
Failed Scope DNS/DHCP/ARP	Site-level client connectivity failure due to DHCP, ARP, or DNS issues.
DNS/DHCP/ARP failures	A sudden increase in DNS, DHCP, or ARP failure events, indicating potential user-impacting issues.

View Potential Anomalies on the Insights Page

You can view the potential anomalies detected by Marvis under the Events section on the Potential Anomalies and Optimizations tab on the **Monitor** > **Service Levels** > **Insights** page.



To view more details of an anomaly, you can click the View More link.



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:

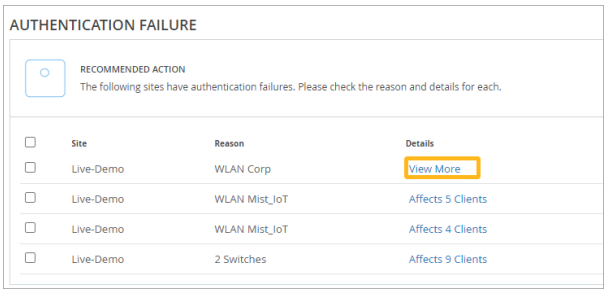
- Authentication Failures
- Domain Name System (DNS) Failures

- 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.



When you click **View More**, the card appears in a pop-up window. Here's a sample event card for an authentication failure.

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.

AP Deployment Assessment

SUMMARY

Do you have enough access points (APs) at your site? Assess your deployment by using Marvis Actions, Wireless Service Level Expectations (SLEs), and the RF Health and Utilization dashboard in Premium Analytics.

IN THIS SECTION

Overview

Determine if you need more APs for optimal connectivity and user experience. Consider our recommendations as you optimize your deployment.

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 AP 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 APs 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.

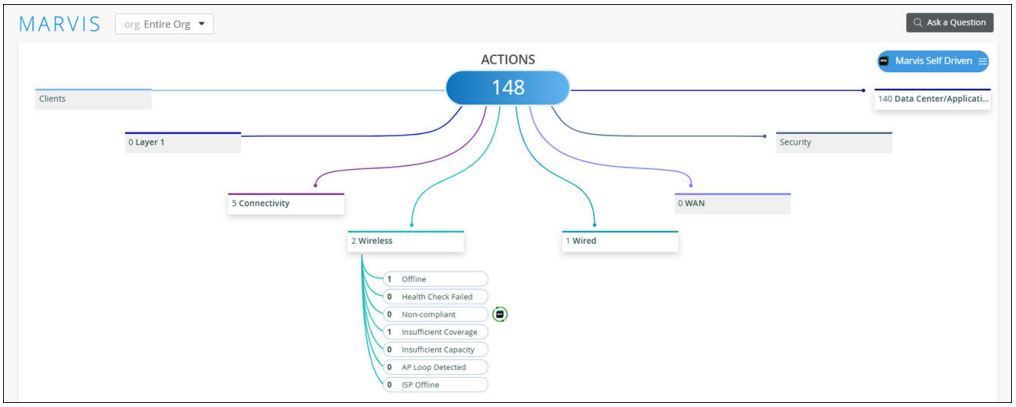
Marvis Actions

In order to ensure optimal network performance and coverage, it is essential to regularly assess the sufficiency of the APs in 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 **Wireless** button on the Actions dashboard, you'll see a list of all available actions. You can then click an action to investigate further.

Figure 5: 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 might 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 with other APs of the same model at the site. Updating firmware is crucial to ensure security, stability, and performance improvements.

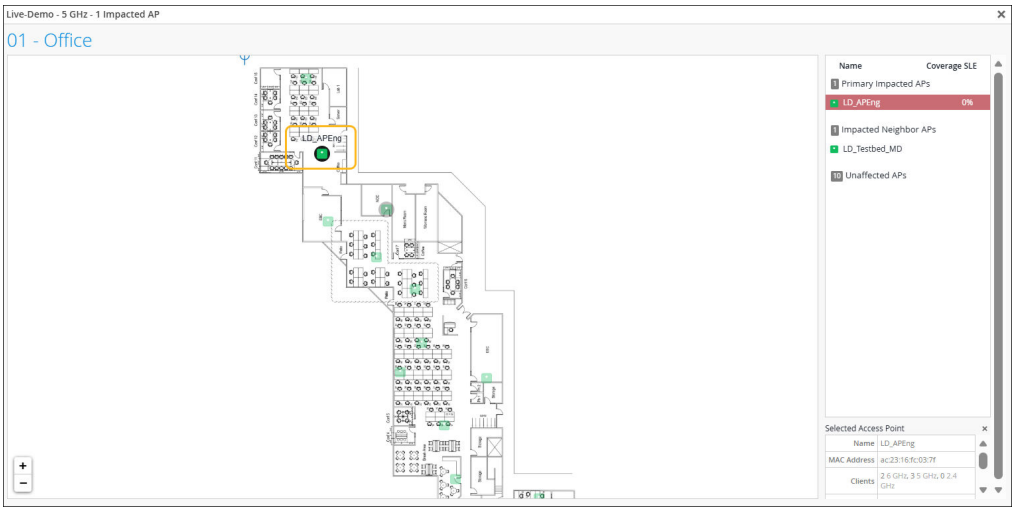
Upgrade the firmware of Non-Compliant APs from the Marvis Actions page to align with the latest version. This step helps in maintaining consistency across APs and mitigating potential vulnerabilities.

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.

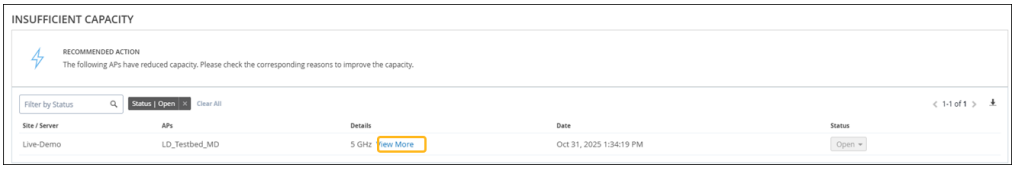
Utilize the floor plan visual provided by Marvis to pinpoint areas with coverage issues and take necessary steps such as adding APs, adjusting placements, or increasing power output to address the coverage gaps.



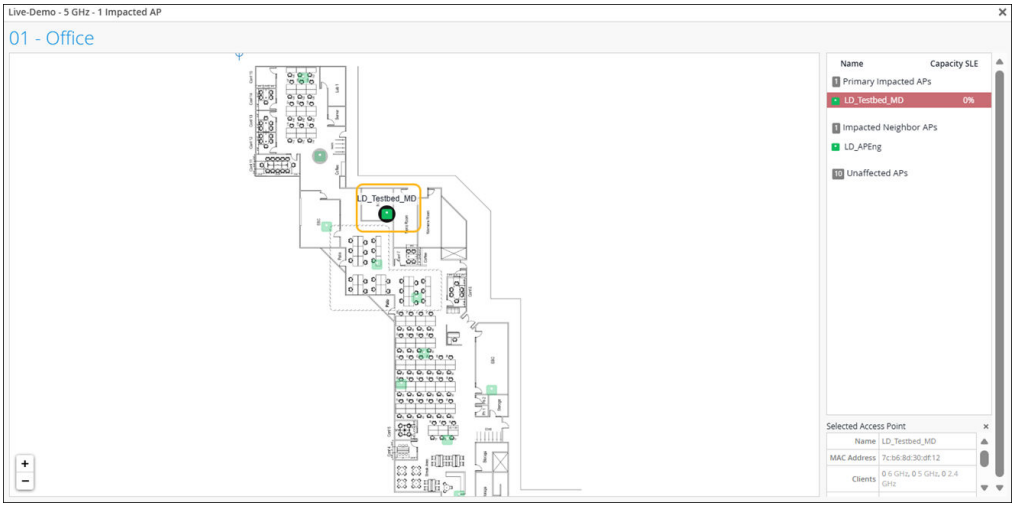
By identifying and resolving coverage holes promptly, you can enhance network connectivity and user experience, ensuring seamless communication across all areas.

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.



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.

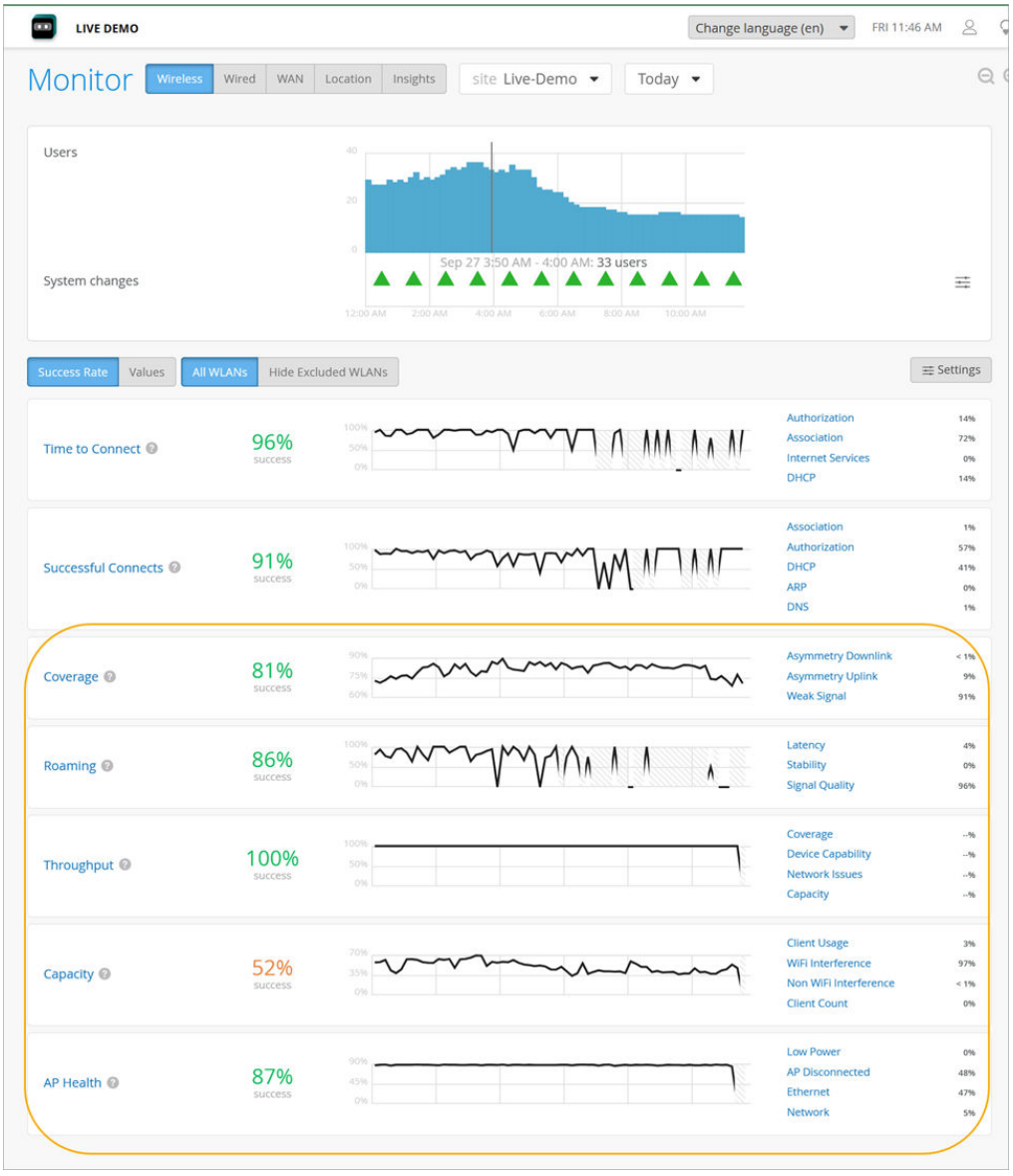


Wireless SLE Analysis

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 for more information.

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



Use the following SLE to assess your users' experiences with signal strength, throughput, RF channel capacity, roaming between APs, and APs availability.

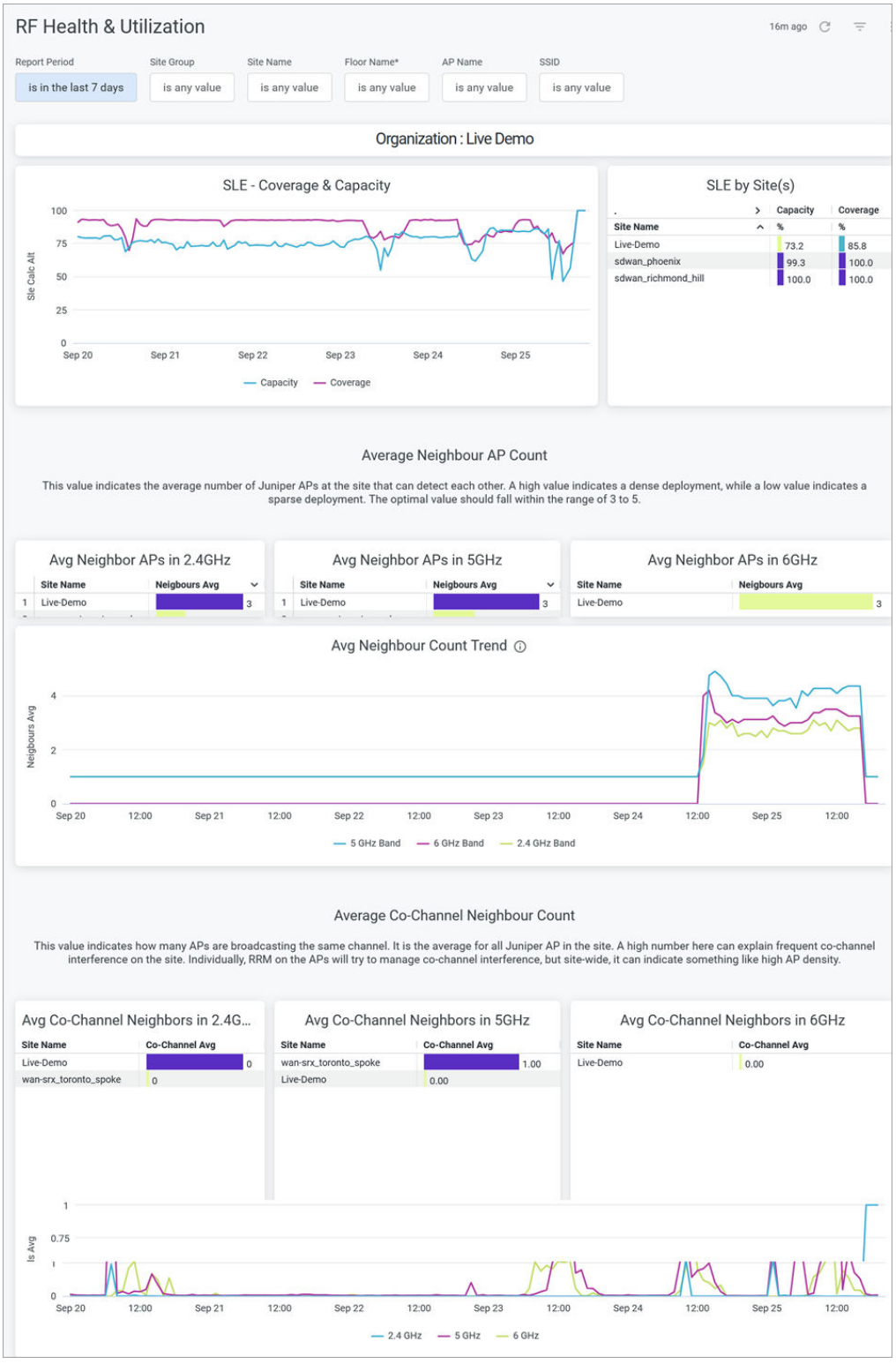
1. **Signal Coverage:** Analyze the Received Signal Strength Indicator (RSSI) and signal quality data to identify areas with weak coverage or potential signal asymmetry.
2. **Roaming Performance:** Evaluate the success rate of client device roams between APs and identify any issues related to latency 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 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**.



Here you can analyze channel utilization trends for different 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 APs to improve signal coverage and address any identified dead zones. For help placing APs for location services, see the Juniper Mist Location Service Guide.
- Implement recommended actions provided by Marvis to address ongoing network issues and enhance overall network performance.
- Consider the deployment of additional APs 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. For help with radio management, see the Juniper Mist Wireless Assurance Guide.

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

Wireless Actions

CHAPTER 7

Marvis Minis

IN THIS CHAPTER

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 to other APs and switches. By doing so, Marvis Minis can determine if an issue affects your entire site or a specific switch, WLAN, VLAN, server, or AP. Marvis Minis automatically scopes and validates changes such as new device additions, configuration changes, and so on.

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 0.14.29313 or a later version for Marvis Minis to run validations. If you add an AP running a firmware version earlier than 0.14.29313 to a site, Marvis Minis validations might be interrupted until the AP firmware is upgraded to the minimum required version.

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. As you add devices, Marvis Minis builds and updates its testing scope.

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:

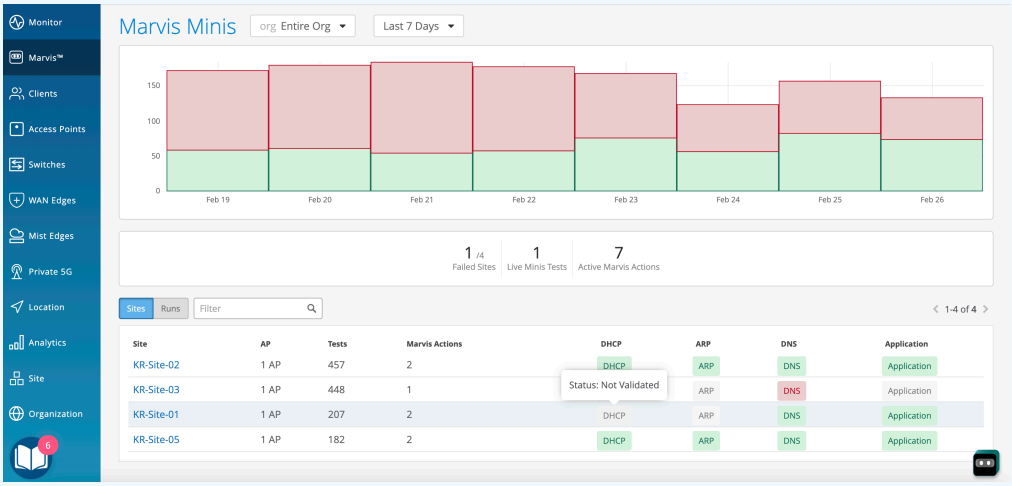
- Dynamic Host Configuration Protocol (DHCP)
- Address Resolution Protocol (ARP)
- Domain Name System (DNS)
- Application reachability

Marvis Minis simulates a user connection on active user VLANs and validates the connectivity process using the following steps:

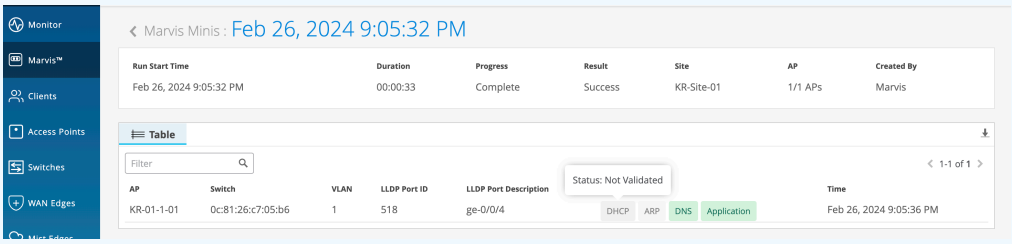
1. Sends a DHCP request for a client VLAN and reports whether the VLAN obtains an IP address. The AP sends both broadcast discovers and unicast renews.
2. Generates an ARP request for the gateway.
3. Resolves DNS queries against all the DNS server IP addresses received in the DHCP offer.
4. Verifies 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 over DHCP and ARP, you'll see the status as **Not Validated**.



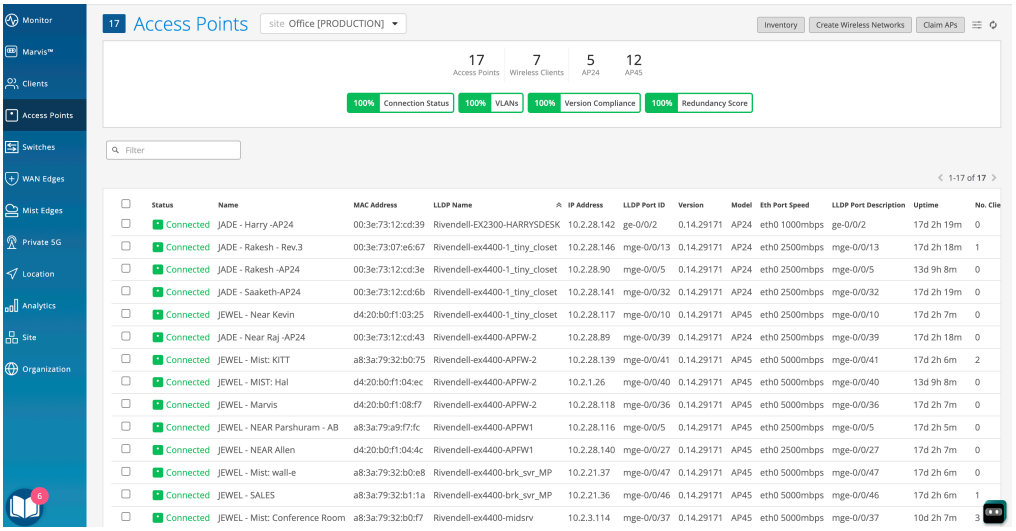
Here's the detailed view when you click the site.



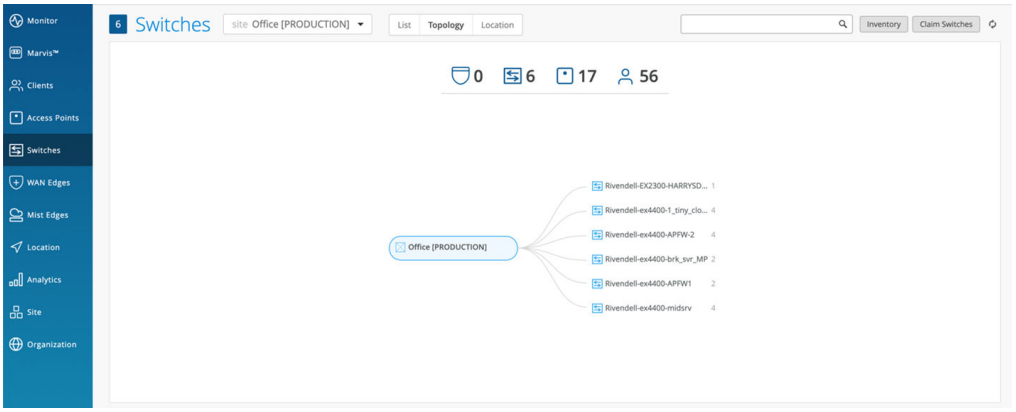
If Marvis Minis detects any failure in reachability, it performs the following checks to understand the scope of failure:

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.

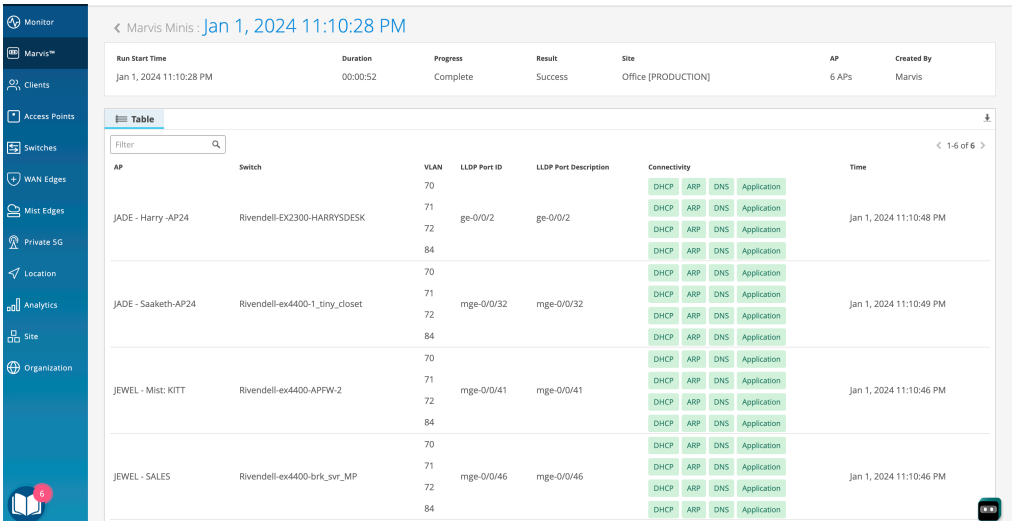
In the following example, a site has 17 APs connected across 6 switches. The validation scope includes 6 APs - one AP connected to each switch and the relevant VLANs.



The **Switches > Topology** page shows the six switches to which the APs are connected.



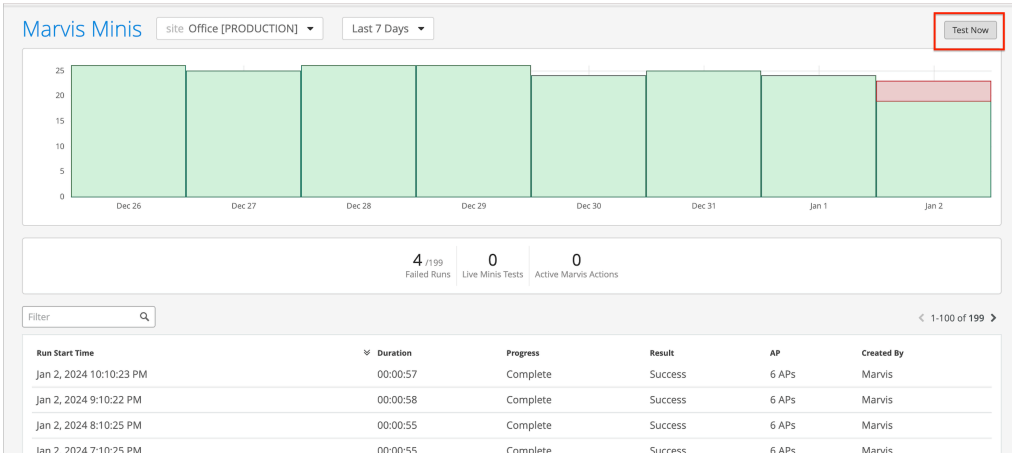
Here is the Marvis Minis page that shows the validation results:



Marvis Minis Validation Frequency

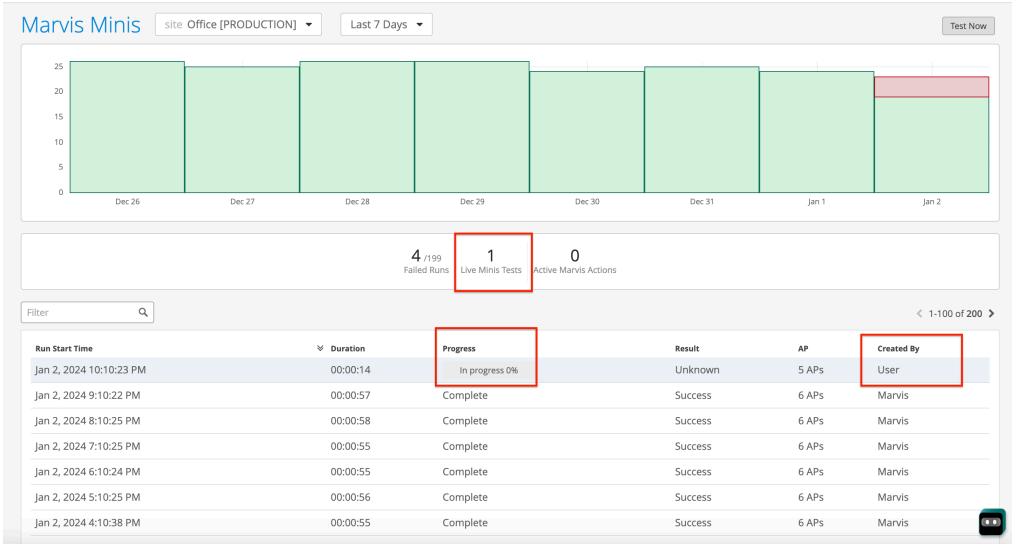
Marvis Minis validations can be triggered either automatically or manually.

- 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.



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.

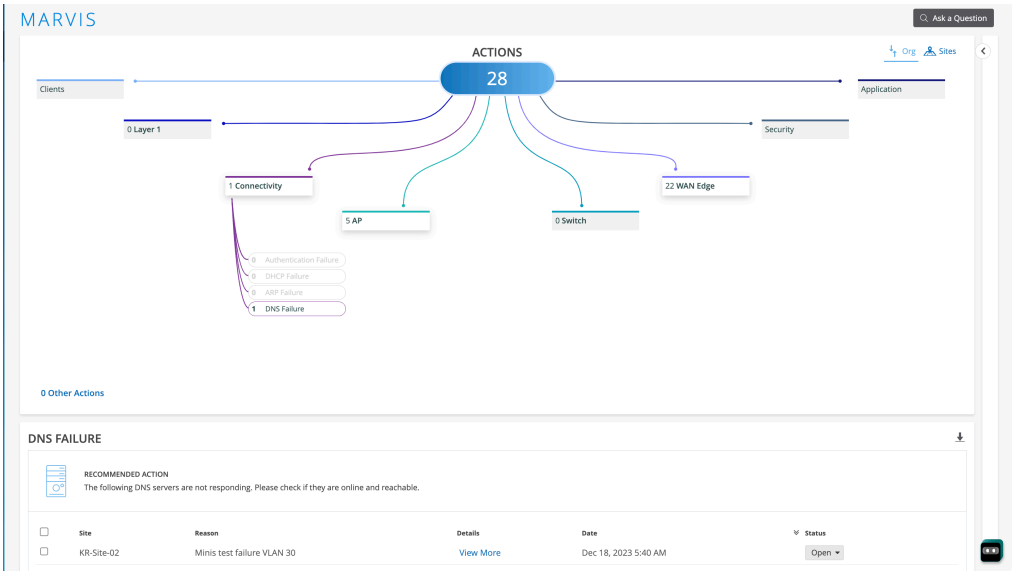


Marvis Actions for Marvis Minis

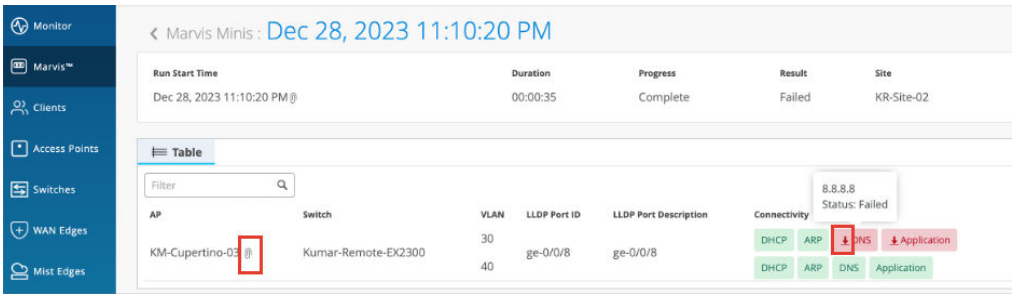
Marvis Actions provides visibility into all the ongoing issues that impact user experience in an organization. Marvis constantly receives data observed by Marvis Minis. Marvis ingests this additional data and lists Marvis Minis-detected failures under the **Connectivity** category on the Marvis Actions page.

When Marvis Minis detects a DHCP or ARP or DNS failure for a given VLAN ID on all APs (including APs in the expanded validation scope), the failure is listed under the **Connectivity** category immediately.

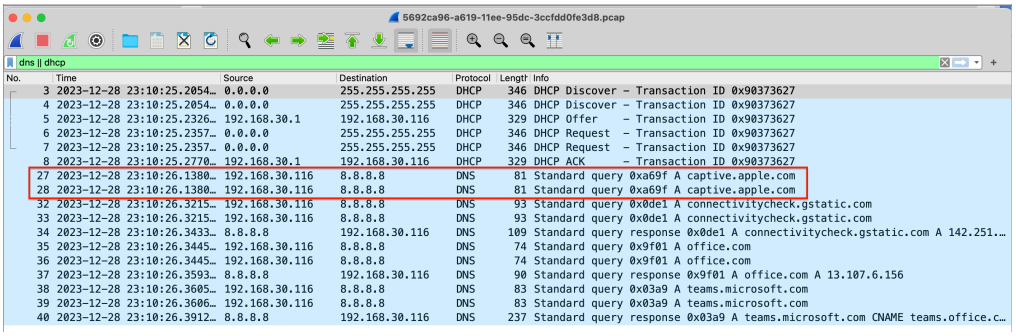
Here is an example that shows how a Marvis Minis-detected failure is listed as an action. Notice that Marvis attributes the failure reason to Marvis Minis validation.



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.



Here is a sample of a downloaded packet capture:



NOTE: After you fix an issue, it might take up to 24 hours for the Marvis action to disappear from the Marvis Actions page. 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

SUMMARY

Get familiar with the major features of the Marvis Minis Dashboard and the details that you can view in the validation results. See how to use filters and

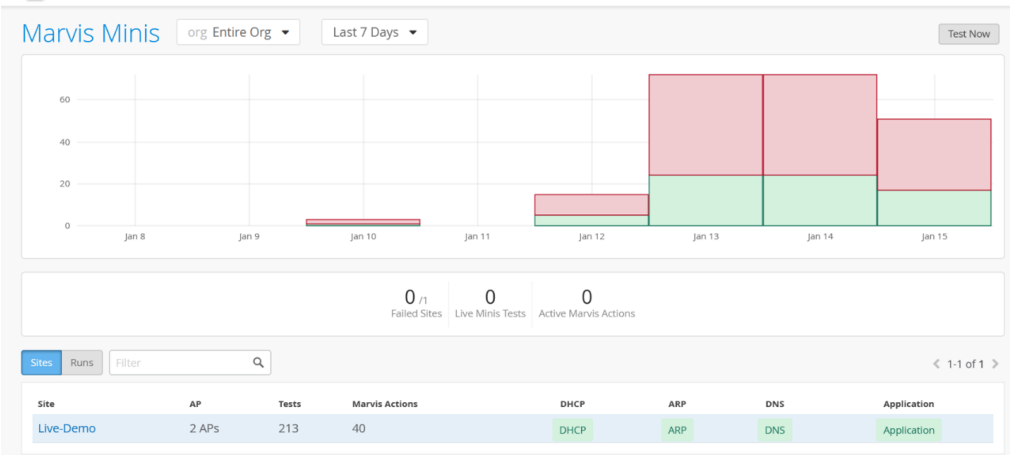
IN THIS SECTION

other options to find exactly the information that you need.

Site-Level Dashboard | 248

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:



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.

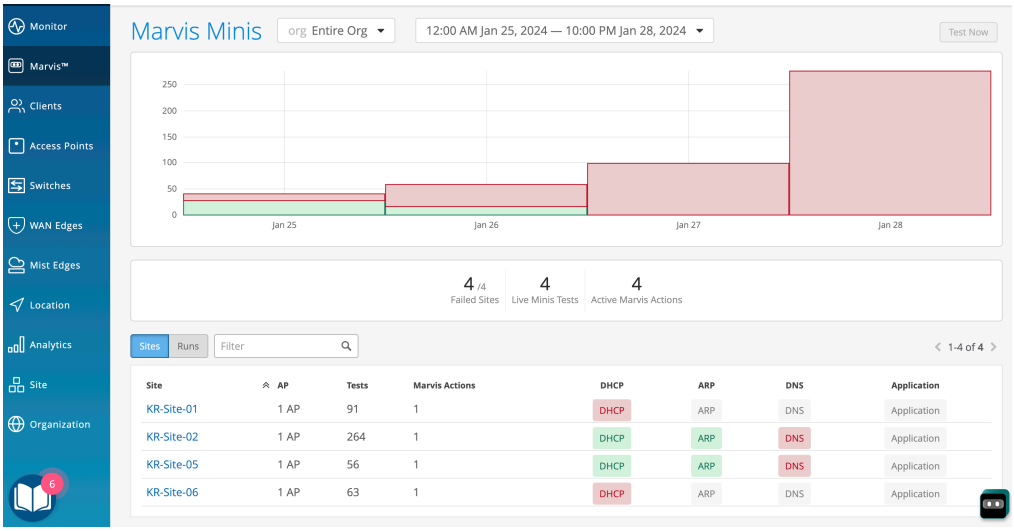
Directly below the graph, you'll see the following statistics for the organization:

- 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

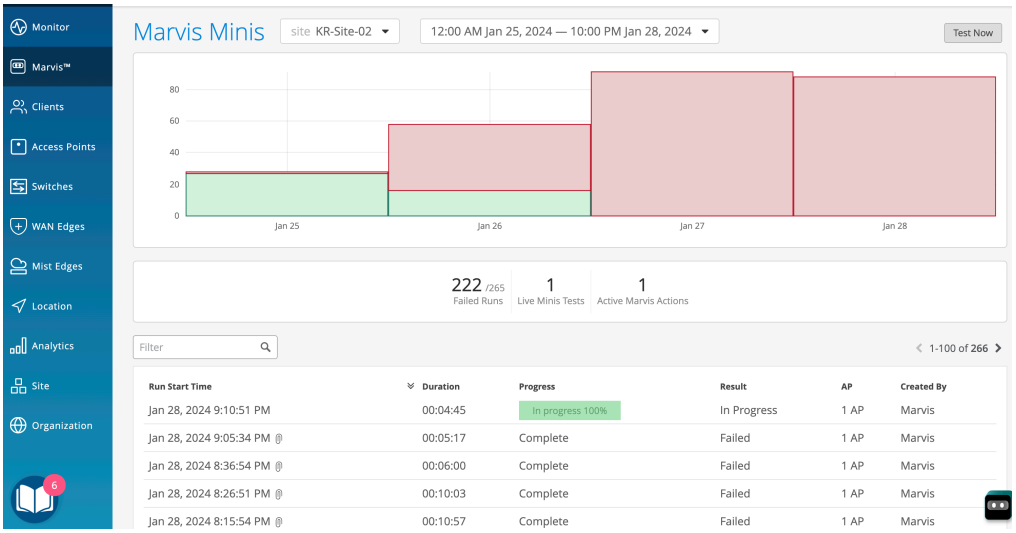
Here is an example of the Marvis Minis dashboard view for an organization:



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

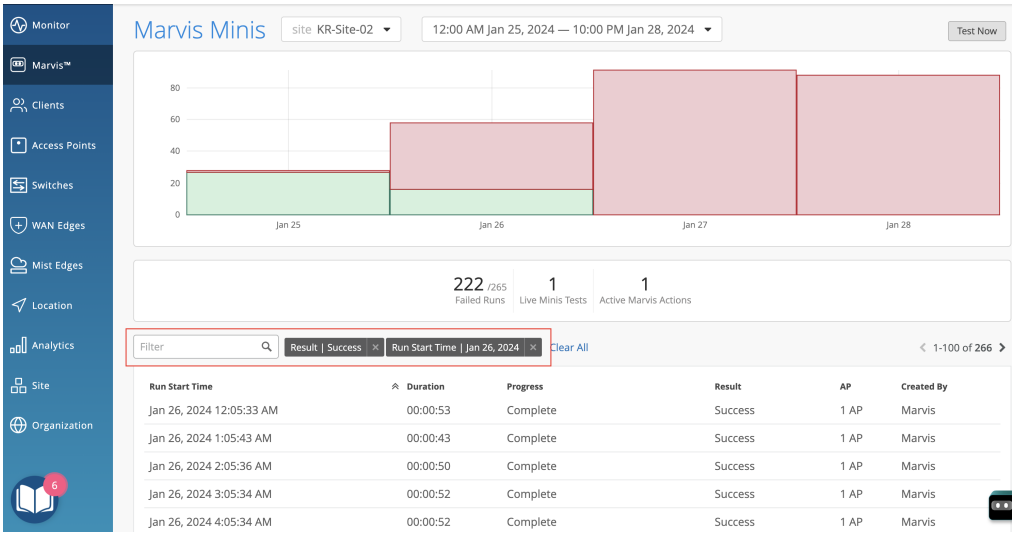
You can view the details of each validation run on a site by clicking the site name. In this example, you can see the validations run on a site.



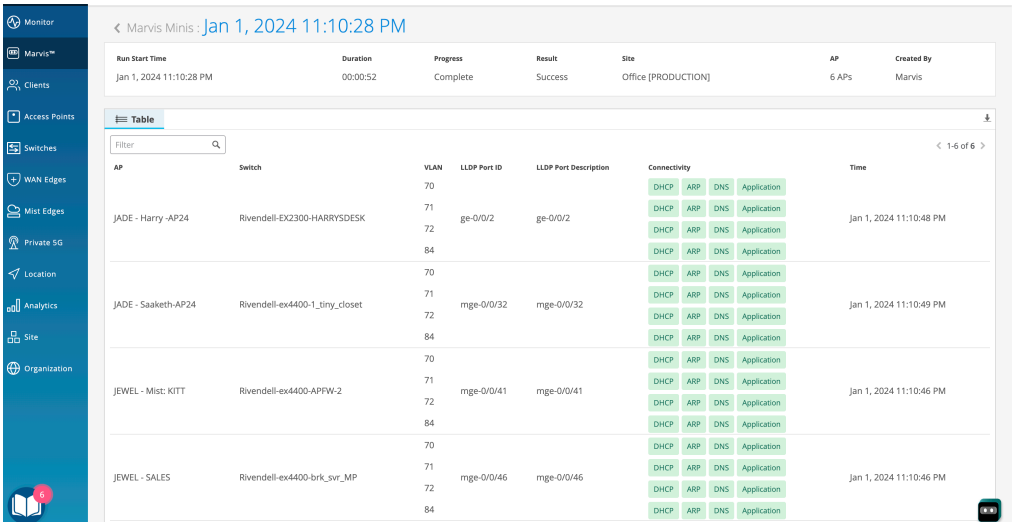
The **Created By** column indicates who initiated the validation:

- 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.

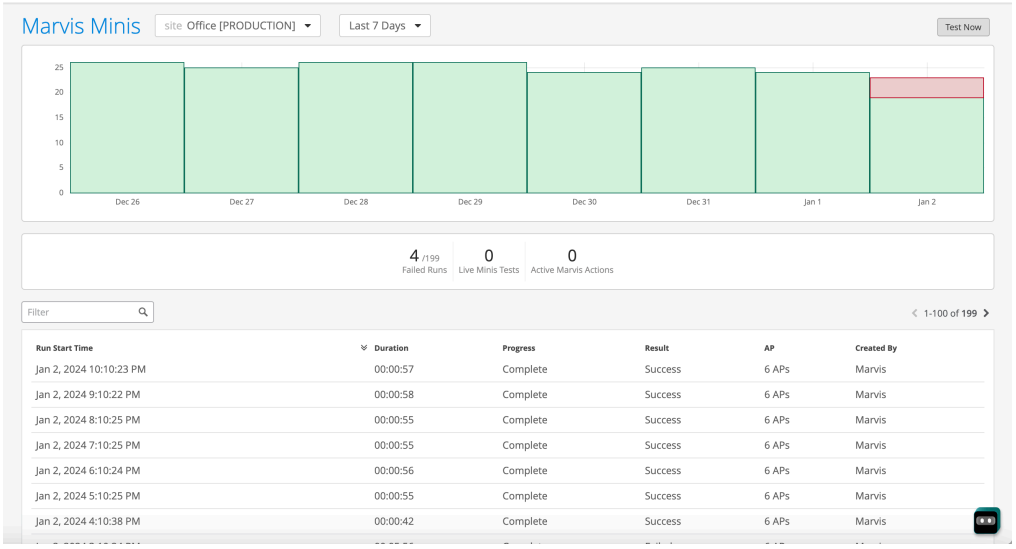


To view more information about each validation, click each row. You'll see the details for a validation. The table lists all the APs at the site, the switch to which each AP is connected, VLANs, LLDP port information, and the status for DHCP, ARP, DNS, and application connectivity.

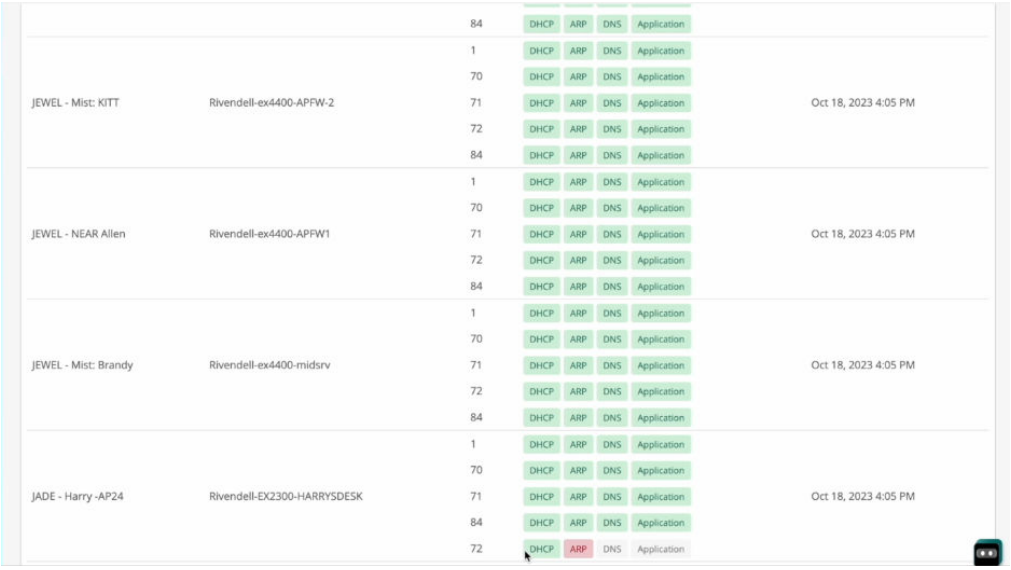


Site-Level Dashboard

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.



Here's an example of a validation that detected an ARP failure on one of the APs.



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.

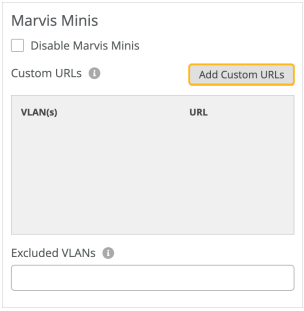
Add Custom URLs for Marvis Minis Validation

SUMMARY

To expand Marvis Minis validations to include additional URLs outside your site, add the URLs that you want to validate. For example, add Amazon Web Services and Microsoft Azure workload application URLs to verify service reachability.

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**.



4. Enter the URL or fully qualified domain name (FQDN) of the site and the VLANs that you want Marvis Minis to validate.

   When adding a URL for validation, note that

   - If you include https://, Marvis Minis will use HTTPS.
   - If you don't specify a protocol, Marvis Minis will consider HTTP.

   Marvis Minis considers an application as reachable if the response status code is either 200 (OK) or 408 (for default apps).

   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 250.

5. Click **Add**.
6. Click **Save** in the top-right corner of the Organization Settings page.

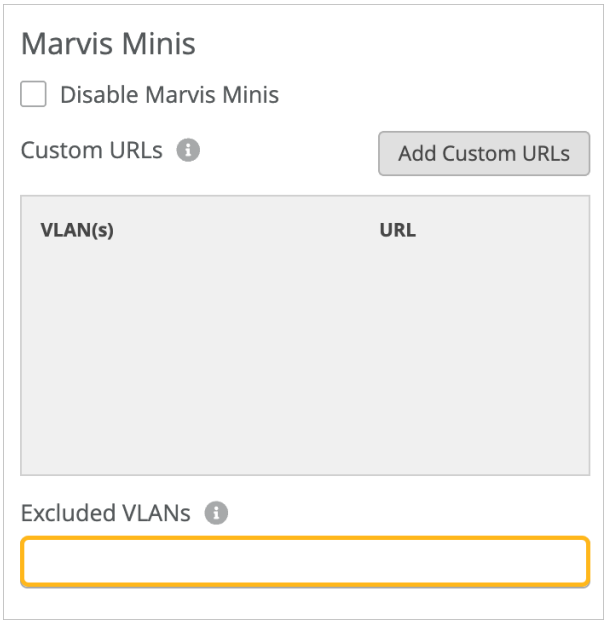
Exclude VLANs from Marvis Minis Validation

SUMMARY

Follow these steps if you want to exclude some of your VLANs from the validation tests.

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

SUMMARY

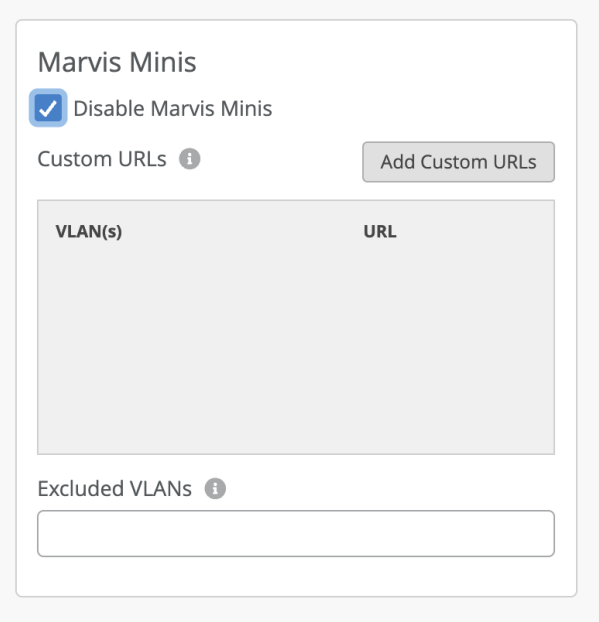
If you don't want to run Marvis Minis validations, you can disable them at any time.

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.



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

SUMMARY

To gain insights into network performance, view the connections timeline, site insights, and system events for Marvis Minis.

IN THIS SECTION

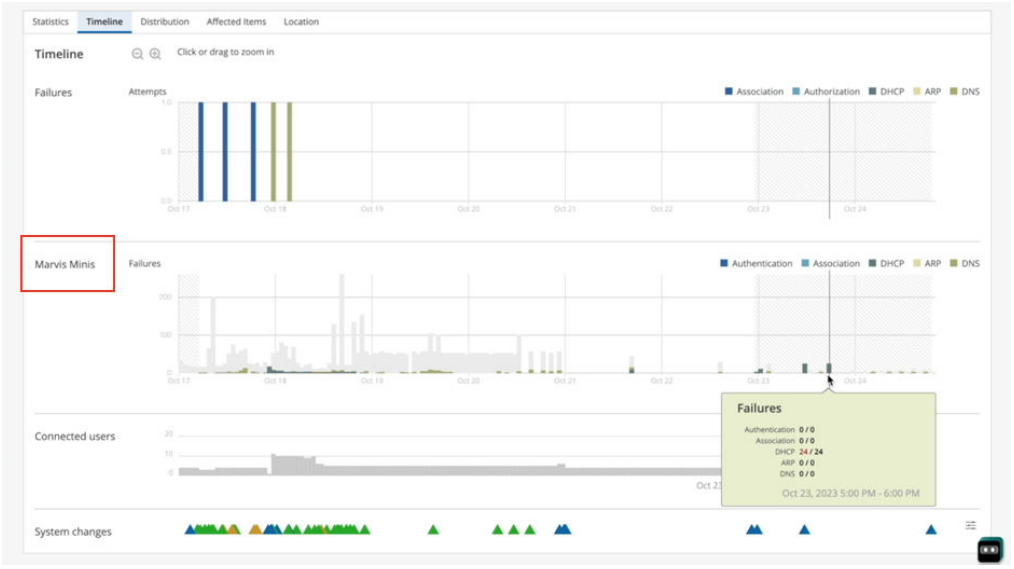
Juniper Mist™ uses data from Marvis Minis to analyze the end-user experience and provides the overlay of Marvis Minis runs in the wireless service-level expectation (SLE) dashboards. You can use the information to analyze connectivity failure trends and manage your network proactively by identifying issues before they become larger issues 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.

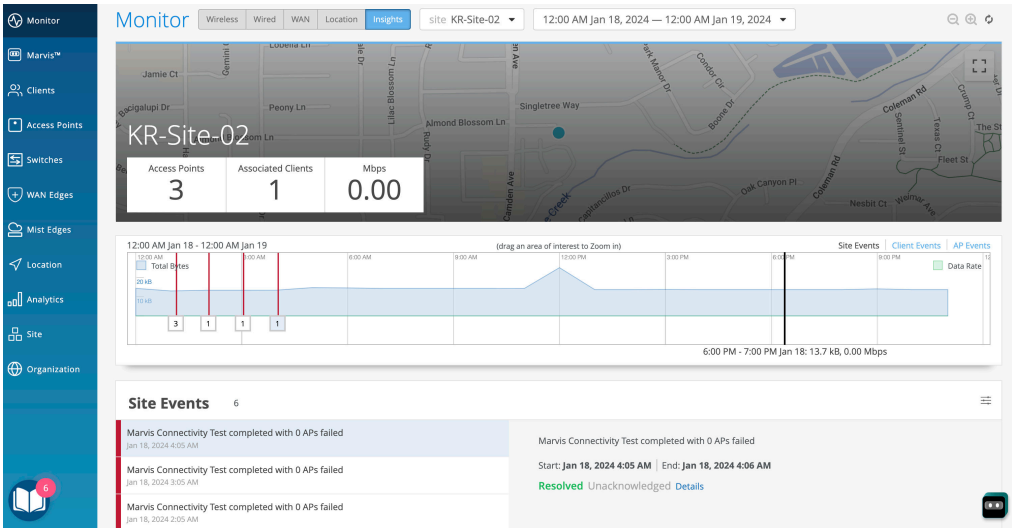


View Site Insights for Marvis Minis

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.

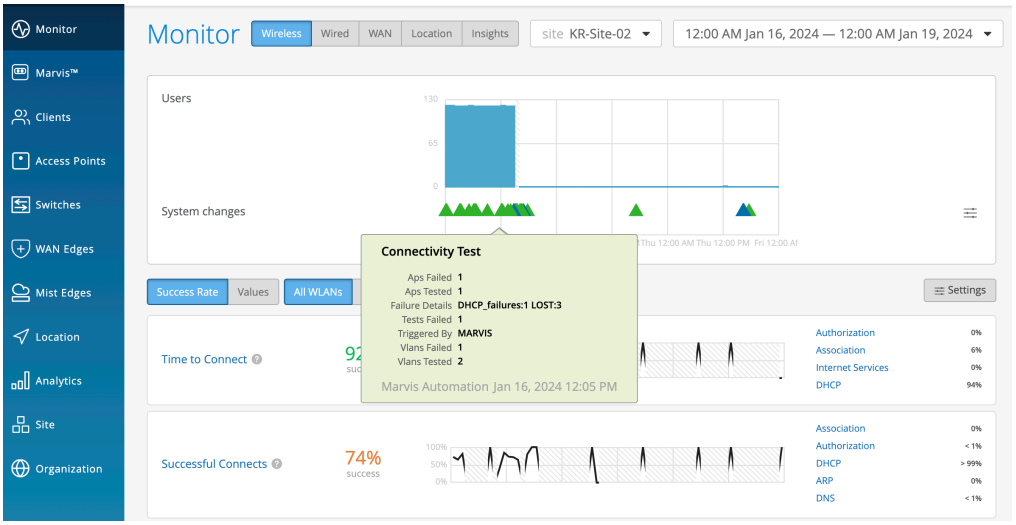


View System Events for Marvis Minis

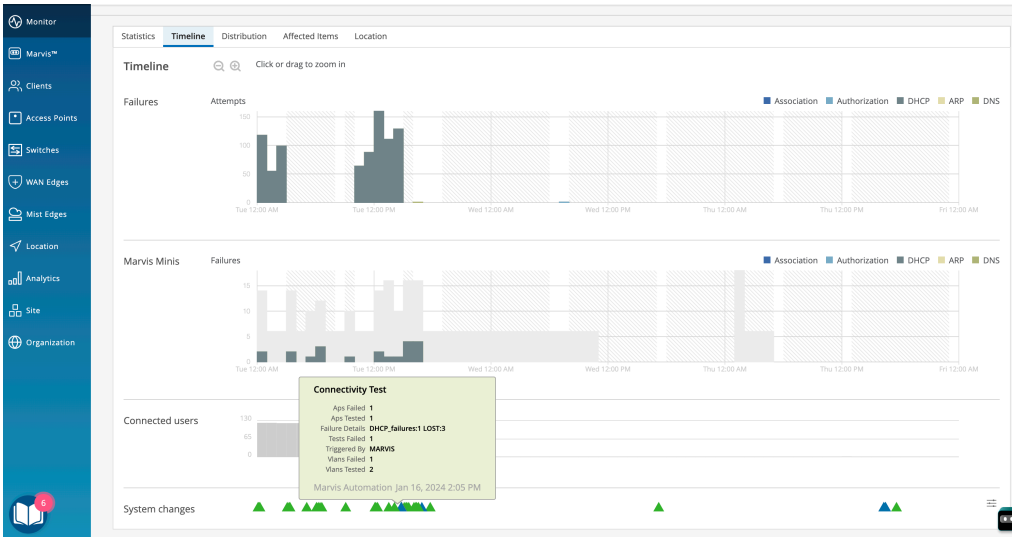
Mist displays all Marvis Minis connectivity validations executed on a site as part of the system events. With this information, you can keep track of the connectivity validations from the Wireless SLE page.

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.



You can also access the System Changes information from the Successful Connect Timeline view.



Troubleshoot Marvis Minis

SUMMARY

Follow these guidelines to resolve issues with Marvis Minis.

If you notice that Marvis Minis is not running any validations, then check whether:

- An AP or multiple APs in the site are running a firmware version earlier than 0.14. All APs in the site must run firmware version 0.14 or later for Marvis Minis to run validations. Marvis Minis does not run validations even if one AP in the site is running a firmware version earlier than 0.14.
- All WLANs are disabled in the site. There must be at least one active WLAN with untagged or tagged VLANs.
- Marvis Minis is disabled at the organization level (**Organization**> **Settings**) or site level (**Organization** > **Site Configuration**).
- The organization has an active Marvis for Wireless subscription or a trial subscription. You will not see the Marvis Minis option in the UI after the subscription expires.

8
CHAPTER

Marvis Minis SLE

IN THIS CHAPTER

Marvis Minis SLE Dashboard (Beta)

SUMMARY

Get started using the Marvis Minis service-level experience (SLE) dashboard to get end-to-end visibility of the client to cloud user experience.

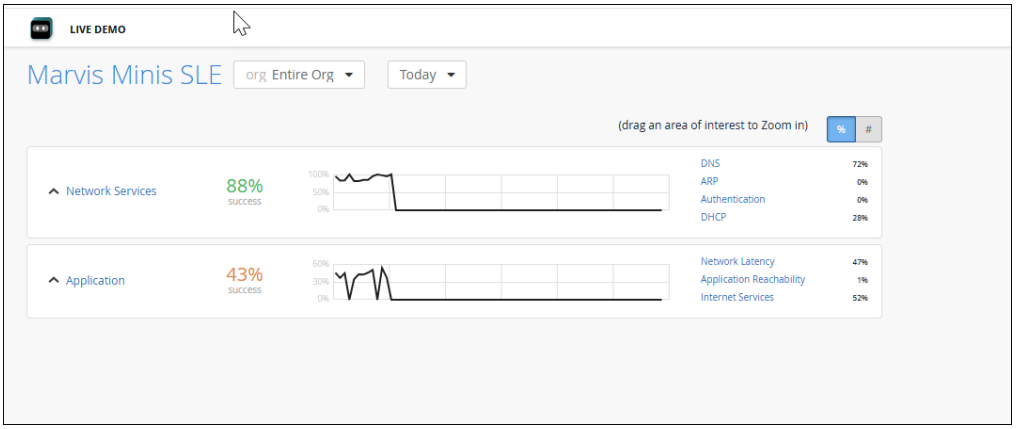
IN THIS SECTION

Marvis Minis is a digital user twin that emulates network users and evaluates the network and application performance of your network by proactively simulating user connections through an access point (AP). Marvis Minis runs periodic validations on active VLANs within a site to assess network connectivity and application reachability for users. A key functionality of Marvis Minis is its ability to detect network or application issues even in the absence of actual users. This proactive approach enables the identification and resolution of potential issues before they affect users. To know more, see Marvis Minis.

The Marvis Minis SLE measures the network and application performance based on the validations run by Marvis Minis. Marvis Minis SLEs delve deeper into factors affecting the client-to-cloud user experience helping you understand the impact and scope of issues. These factors are categorized under two types of SLEs—Network Services and Application.

- The Network Services SLE provides insights into the failures that occurred when Marvis Minis initiated DHCP, DNS, ARP, or authentication tests.
- The Application SLE provides insights into failures that occur after Marvis Minis initiated the application reachability and connectivity tests. This SLE provides a comprehensive view of application performance across the entire organization and localized performance data specific to individual sites, enabling detailed analysis of how particular applications are functioning in different contexts.

The SLEs provide a time series view that helps you to quickly narrow down the type of failure and the failure start time. With detailed visibility into site-level and organization-level performance, these SLEs enable early detection and resolution of issues.



Finding the Marvis Minis SLE Dashboard

Select **Monitor** > **Service Levels** > **Marvis Minis SLE** from the left menu to view the Marvis Minis SLE dashboard. You can click each SLE to view the Root Cause Analysis page that provides details such as the timeline of failure occurrences. impacted applications and sites.

Subscription Requirements for Marvis Minis SLEs

You do not require a separate subscription to view the Marvis Minis SLEs. Any organization with an active Marvis for Wireless subscription is automatically entitled for Marvis Minis SLEs. Note that Marvis Minis is supported only on APs and switches (authentication) currently.

Network Services SLE (Marvis Minis)

SUMMARY

Use the Network Services SLE to gain insights into user connectivity experience at an organization or site level.

IN THIS SECTION

The Network Services SLE provides insights into the number of failed DNS, ARP, DHCP, or authentication attempts at an organization or site level based on the Marvis Minis validations. Marvis Minis simulates and validates user connectivity on active VLANs to ensure that users can reliably connect to the Internet and access necessary applications. Active VLANs refer to VLANs that are currently being used by clients to pass traffic.

For the validation on APs, Marvis Minis

- Sends a DHCP request on a client VLAN to check if an IP address is successfully obtained.
- Generates an ARP request to verify if the gateway is responsive, which is crucial for network communication.
- Resolves DNS queries using all DNS server IP addresses provided in the DHCP offer. This step confirms that DNS is reachable and can resolve the application URLs, which is vital for translating domain names into IP addresses.
- Checks application reachability by validating the accessibility of specific applications. You can define applications that need to be tested by Marvis Minis. You can define custom URLs/FQDNs in the organization or site settings. See Add Custom URLs for Marvis Minis Validation .

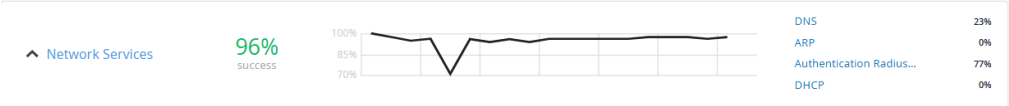
  Marvis Minis considers an application as reachable if the response status code is either 200 (OK) or 408 (for default apps).

  However, if you do not define any applications, then Marvis Minis validates accessibility to application by using default URLs such as captive.apple.com, connectivitycheck.gstatic.com, office.com, and teams.microsoft.com, along with verifying the reachability of Office365 services.

The final step in the connectivity validation process is explicitly releasing the DHCP lease on the tested VLAN. This ensures that resources are freed and available for other requests.

Classifiers

Marvis categorizes the results from the validations under the following classifiers to provide insights into failures detected during the connectivity phase.



- **DHCP**—DHCP request initiated by Marvis Minis for a client VLAN times out. This issue occurs when the DHCP server fails to respond within the expected timeframe, potentially due to network congestion, server misconfiguration, or connectivity issues.

- **Nack (Negative Acknowledgment)**—The requested IP address could not be provided to theMarvis Minis. This could happen if the IP address is already in use by another device, if the request does not comply with the server's policy.
- **Renew Unresponsive**—No response to a DHCP renew request When Marvis Minis attempts to renew its DHCP lease to maintain its IP address, it might not receive a response from the DHCP server. This can lead to connectivity interruptions, especially if the lease expires without renewal. Potential causes for unresponsiveness could include server outages or configuration errors on the server.
- **Incomplete**—DHCP process did not complete. Marvis Minis could not obtain an IP address. This could be due to incomplete or incorrect DHCP configuration settings, network issues, or server-side errors that prevent the full exchange of DHCP messages required to establish a lease.
- **Unresponsive**—No response to a DHCP Discover request which might result in Marvis Minis being unable to connect to the network. This can be caused due to server unavailability, or incorrect VLAN configurations that prevent the discover request from reaching the DHCP server.

- **ARP**—Marvis Minis experienced problems related to ARP during the connectivity process.

  Marvis Minis experienced issues with ARP resolution. The ARP process failed to resolve the IP address to the MAC address of the default gateway. This prevented Marvis Minis from successfully communicating with external networks, as the default gateway acts as a crucial point for routing traffic outside the local network.

- **DNS**—DNS servers are not reachable, which indicates that attempts to resolve domain names to their corresponding IP addresses are failing. As a result, internet services relying on domain name resolution might be disrupted. This issue could be due to network configuration errors, server outages, or issues with the DNS settings on your device or network.

- **Authentication**—Marvis Minis automatically learns all the RADIUS authentication servers configured for your network and validates server reachability. Using preset credentials, Marvis Minis initiates an authentication request to a RADIUS server. If the server rejects the authentication request, then it indicates that the server is available and reachable. This is currently supported only for switches.

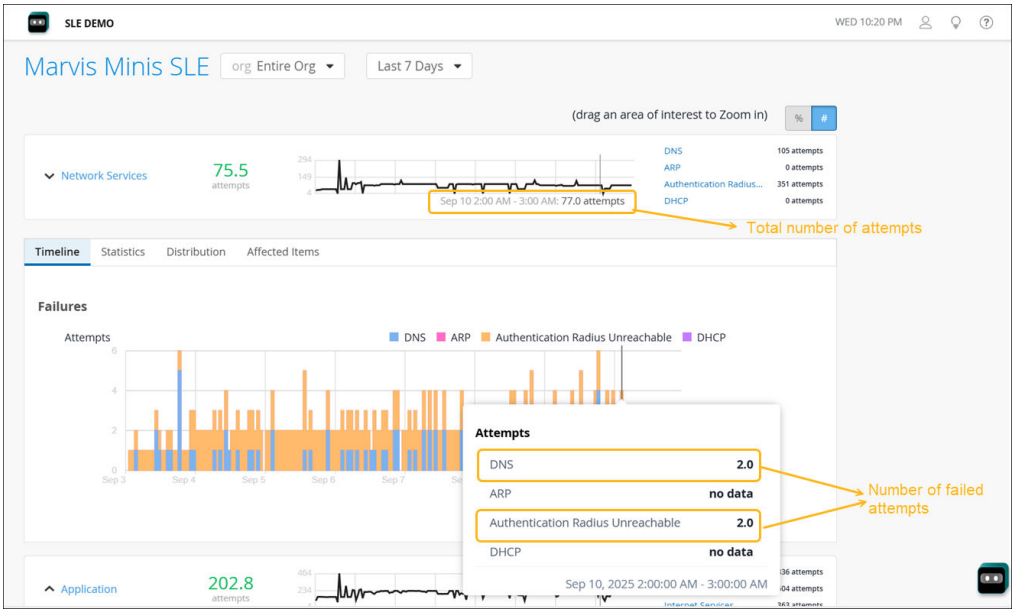
Root Cause Analysis for the Network Services SLE

You can use the information across the following tabs that display when you click **∨** beside Network Services.

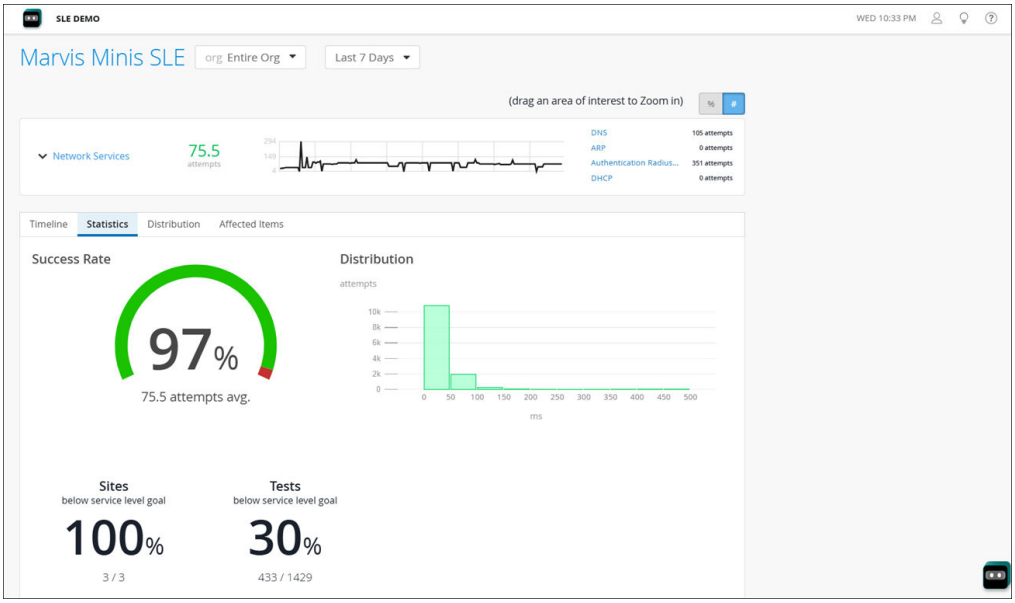
NOTE: The same information displays when you click a classifier in the SLE block. You'll see the tabs displayed in the Root Cause Analysis page. Click classifiers and sub-classifiers to view the timeline and scope information on the lower half of the page.

- **Timeline**—See exactly when the issues occurred.

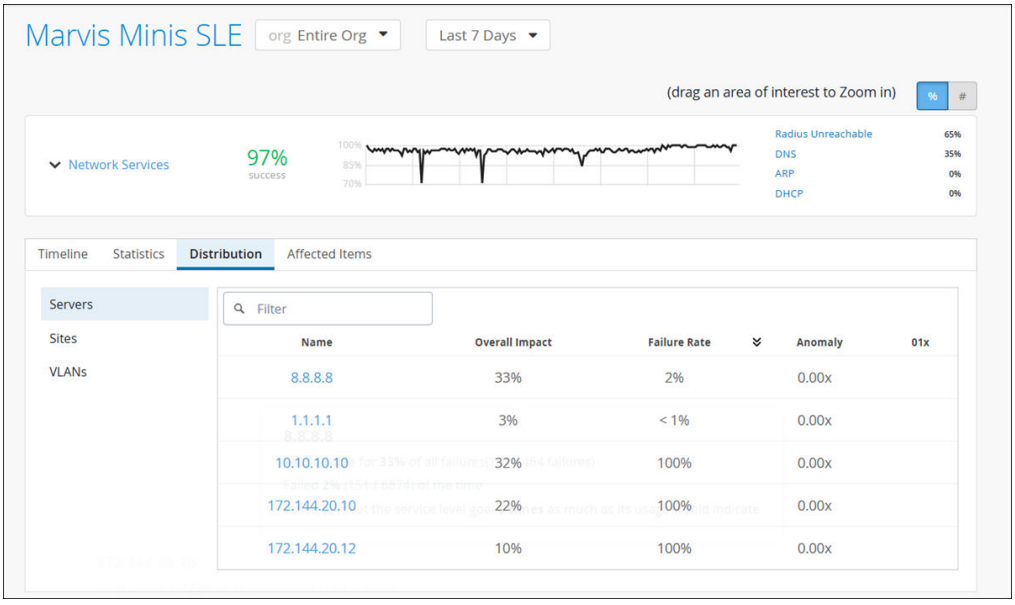
  Here is an example of how Marvis displays the timeline for the Network Services SLE. You can view the total number of attempts and the number of failed attempts for a specific date and time by hovering your mouse over the graph. In this example you can see that a total of 77 attempts were made to connect to the network on September 10 between 2 AM and 3 AM of which 2 DNS attempts and 2 attempts to reach the authentication server failed.



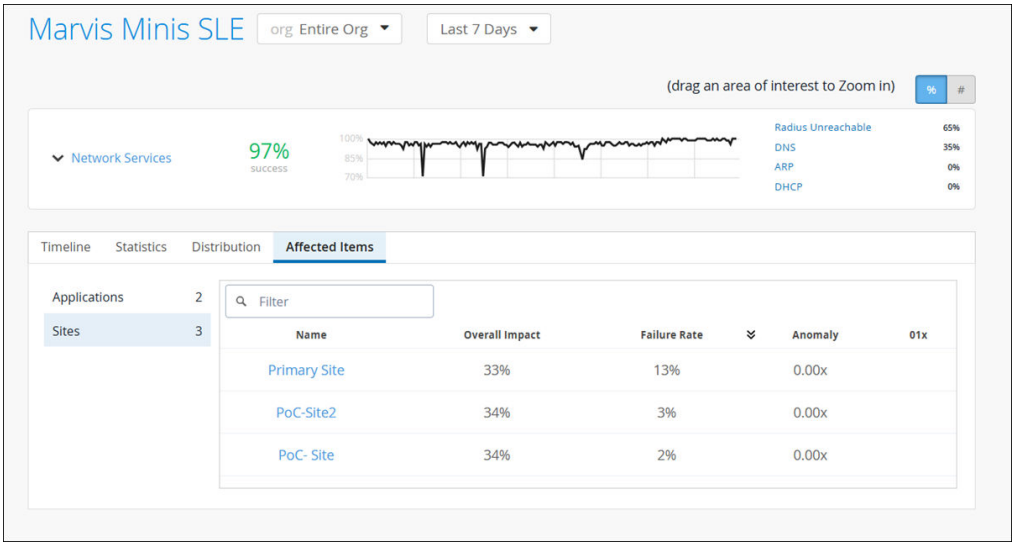
- **Statistics**—See the success rate, number of sites experiencing failures and the latency information. The Distribution graph indicates the latency. In this example, you can see that 10000 connection attempts experienced a latency of 50 ms.



- **Distribution**—See which sites and VLANs were affected.



- **Affected Items**—See which applications and sites were affected and how much each one contributed to the overall impact. Also see the individual failure rate for each application or site.



Application SLE (Marvis Minis)

SUMMARY

Use the Application SLE to assess the performance of applications in your network.

IN THIS SECTION

Marvis Minis runs validations using curl tests to assess application reachability and network connectivity issues. These tests help determine if an application server is responsive and accessible. Applications are constantly monitored, with classifiers being triggered at the first sign of latency or reachability issues.

The Application SLE provides insights into the reachability of applications based on the Marvis Minis validations. If an application is down or unreachable, the SLE can provide insights into potential network connectivity issues or server downtime. The Application SLE can also help determine if network latency is affecting application performance.

Classifiers

The Application SLE classifiers help distinguish whether an application is reachable or whether the application performance is degraded due to network latency.

The Application SLE classifiers help differentiate between two critical conditions affecting applications—reachability and performance degradation caused by network latency.

- **Application Reachability**—This classifier indicates unsuccessful HTTP requests based on the validation data. Marvis Minis verifies application reachability by using default Internet connectivity URLs. You can also define custom URLs/FQDNs in the organization or site settings. See Add Custom URLs for Marvis Minis Validation .

  Marvis Minis considers an application as reachable if the response status code is either 200 (OK) or 408 (for default apps).

- **Network Latency**—This classifier lists the number of attempts when the application response is slow due to latency. The latency can be caused due to a network issue or an issue with the application. The latency is computed based on curl tests and comparison with a rolling baseline over the past 14 days. .

- **Internet Services**—This classifier lists failures experienced by users when accessing application due to:

  - **Latency**—Application slowness due to DNS latency. A high DNS latency can result in slower application page load times as the browser must wait longer to receive the IP address before it can start loading the page.

  - **DNS**—Application failures due to DNS resolution issues.

Root Cause Analysis for the Application SLE

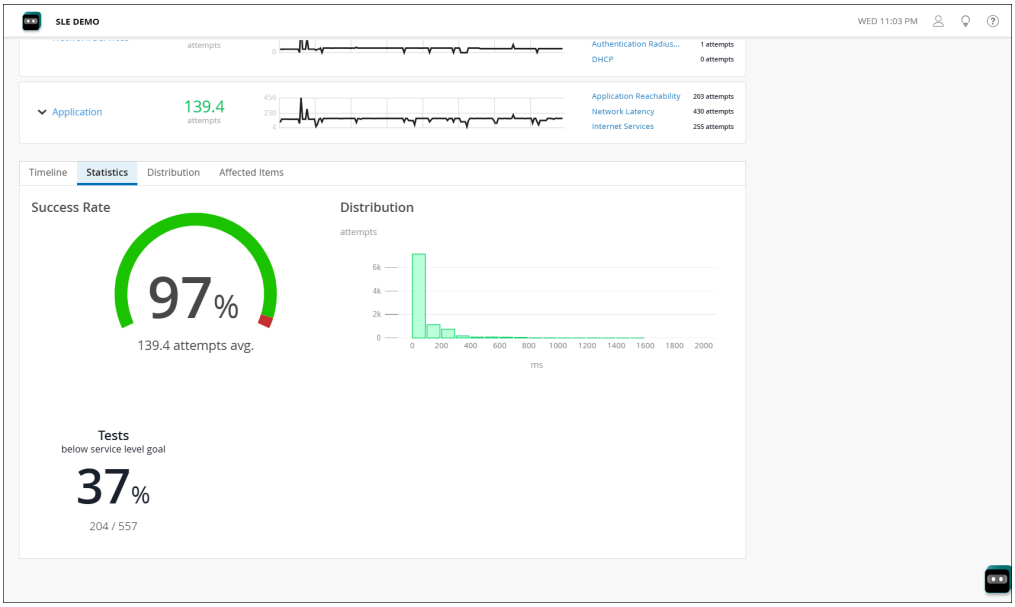
You can use the information across the following tabs that display when you click ˅ beside Application.

NOTE: The same information displays when you click a classifier in the SLE block. You'll see the tabs displayed in the Root Cause Analysis page. Click classifiers and sub-classifiers to view the timeline and scope information on the lower half of the page.

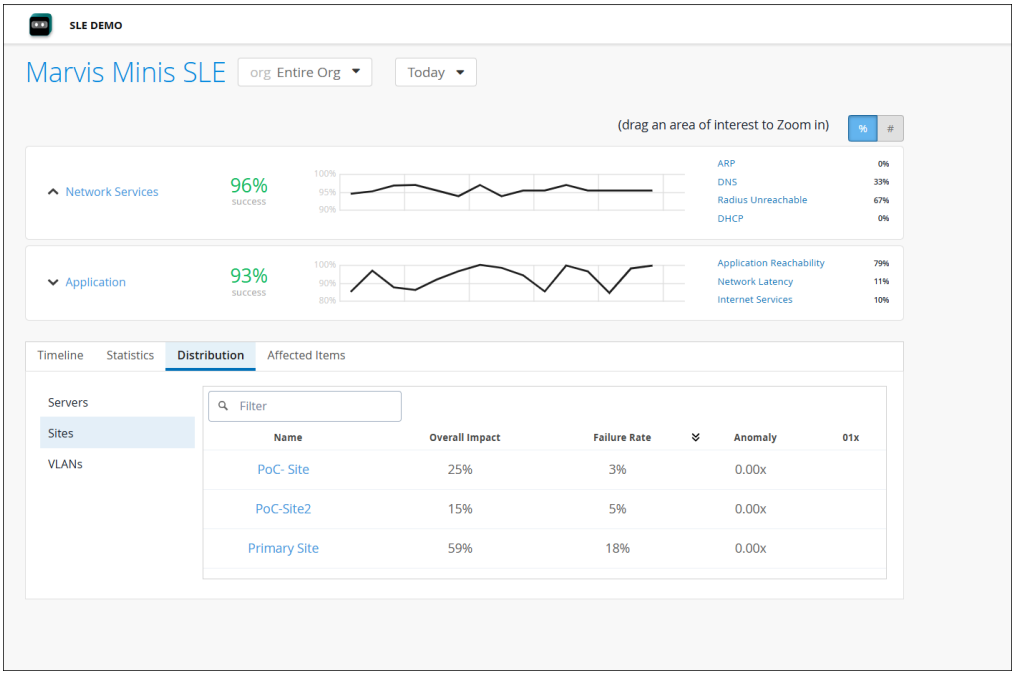
- **Timeline**—See exactly when the issues occurred.

Here is an example of how Marvis displays the timeline for the Application SLE. You can view the total number of attempts and the number of failed attempts for a specific date and time by hovering your mouse over the graph. In this example you can see that a total of 148 attempts were made to connect to the network on September 9 of which 2 attempts failed due to network latency and 2 attempts failed due to issues with the Internet services.

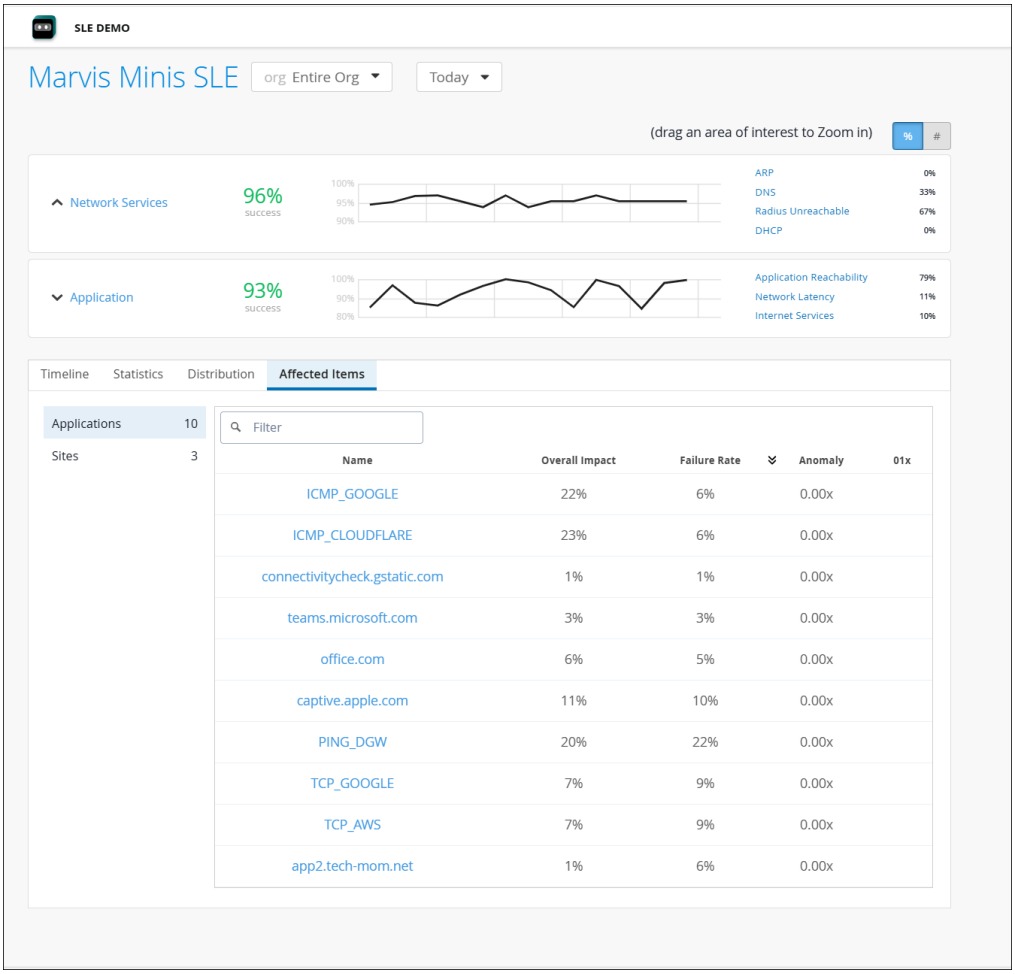
- **Statistics**—See the success rate, number of sites experiencing failures and the latency information. The Distribution graph indicates the latency. In this example, you can see that ~1000 connection attempts experienced a latency of up to 200 ms.



- **Distribution**—See which switches, APs, and VLANs were affected.



- **Affected Items**—See which applications were affected and how much each one contributed to the overall impact. Also see the individual failure rate for each application.



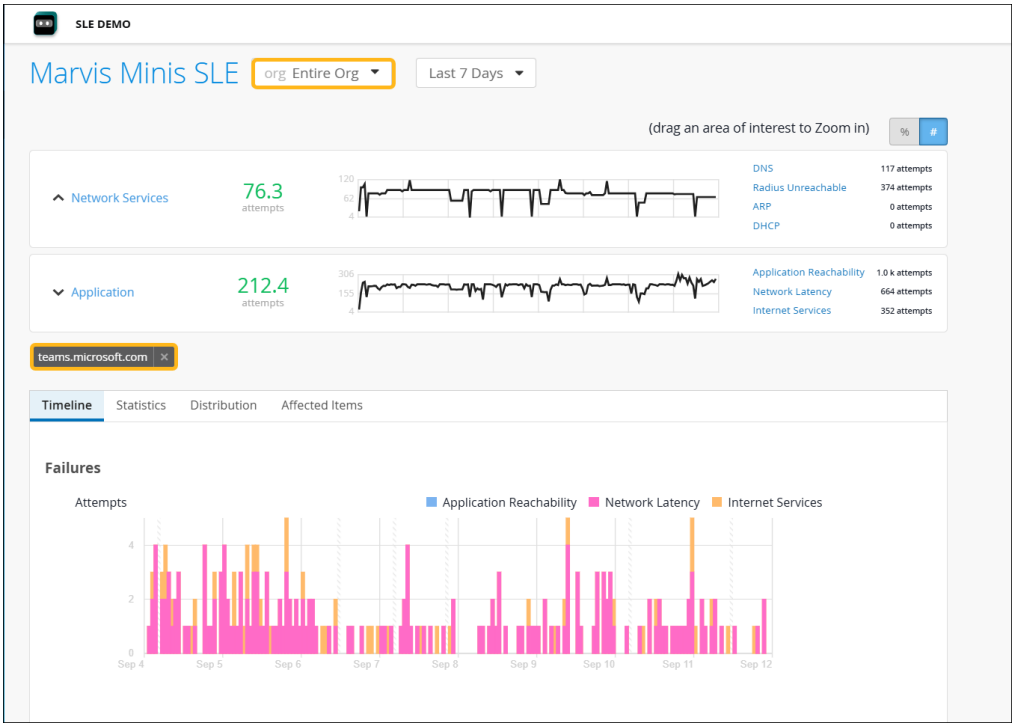
You can view in-depth information for applications at an organization or site-level. Here are the different options to view data:

- **All applications in an organization**

  This view is the default view as shown in the above example.

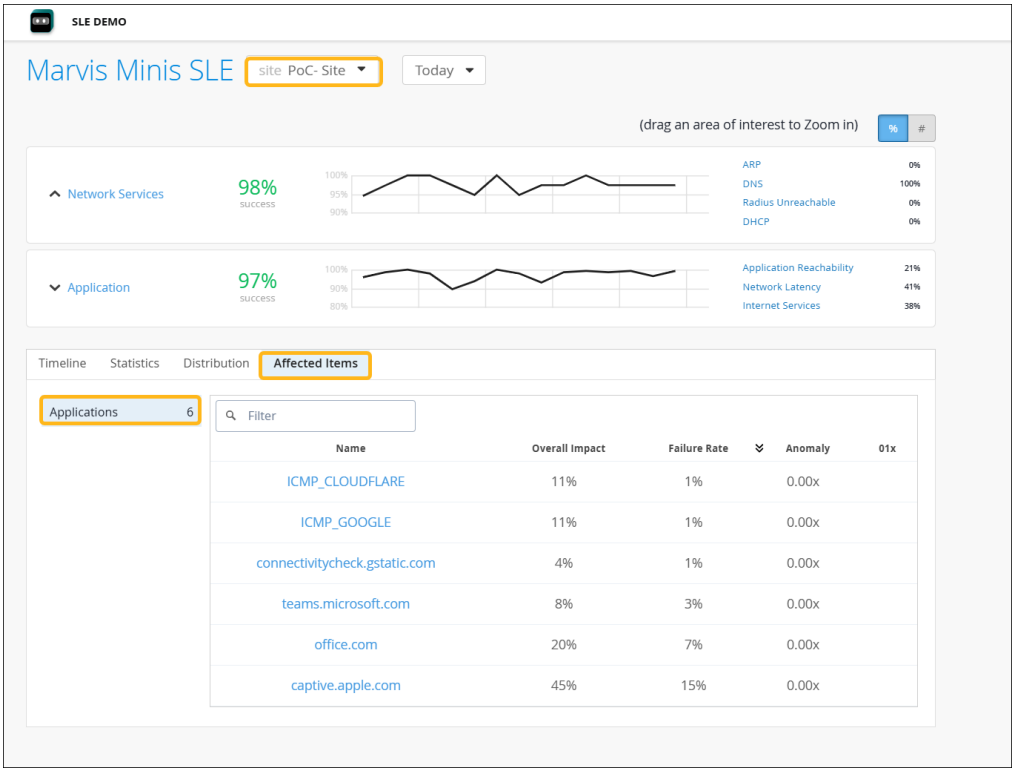
- **A specific application at an organization level**

  Click the specific application listed in the Affected Items tab (which is the default view shown above). You can view the details as shown in the following example.



- **All applications in a site**

  Select a site from the drop-down list on the top of the page, and navigate to the Affected Items tab. You can see the data for all the applications that experienced issues within the selected site.



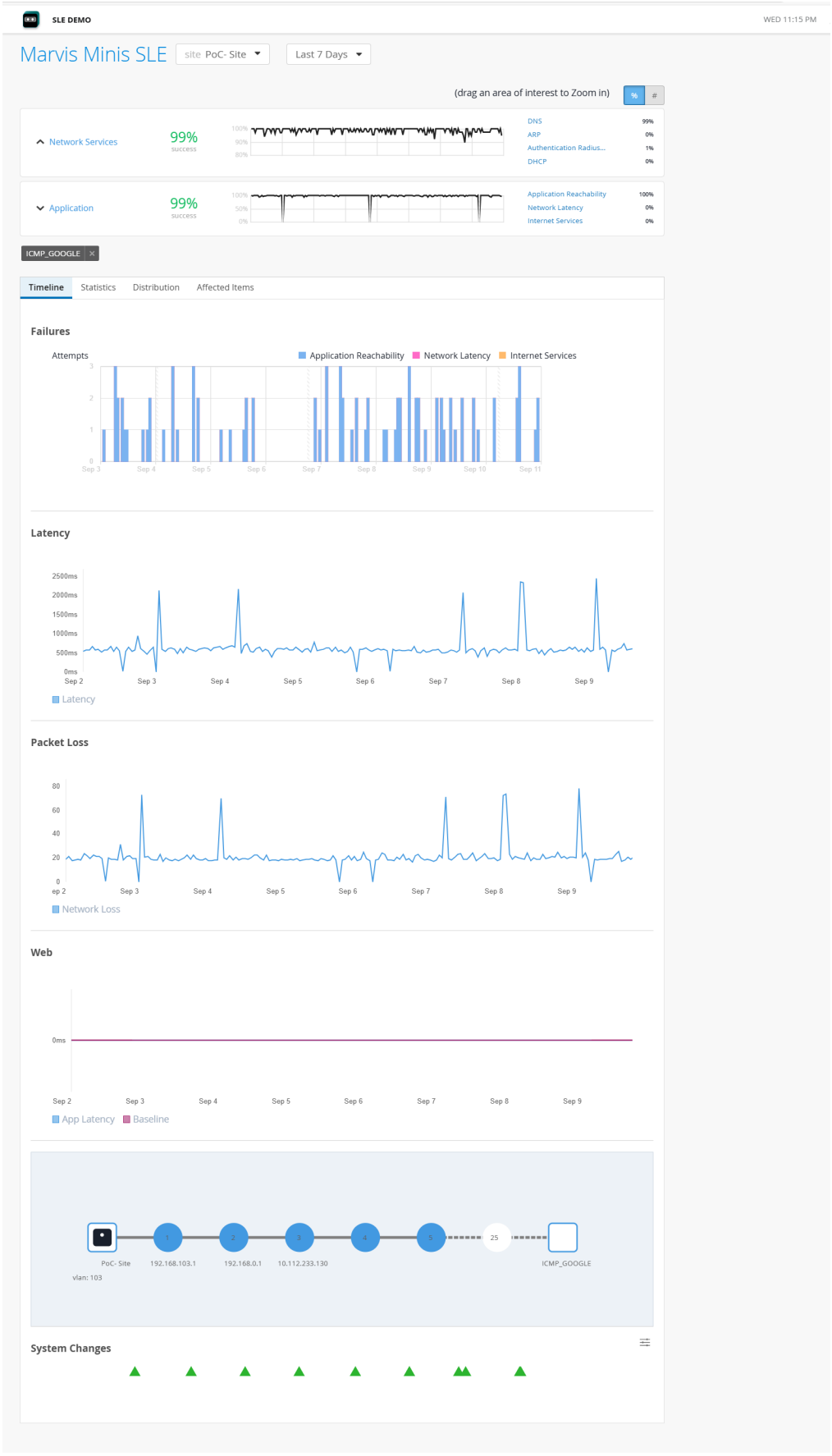
- **A specific application at a site level**

  Select a site from the drop-down list on the top of the page and navigate to the Affected Items tab. Click an application to view the details. The site-level application view offers additional insights for the selected application, providing a more granular understanding of its performance and issues:

  - Network Latency
  - Packet Loss
  - Curl Latency
  - Traceroute

  NOTE: The Latency, Jitter, and Traceroute statistics are currently available as part of the Beta program for the enhanced Marvis Minis. Contact your account team to participate in the Beta program. Also, note that these sections are displayed only for an application at the site level.


SLE DEMO
WED 11:15 PM
Marvis Minis SLE
site PoC- Site
Last 7 Days
(drag an area of interest to Zoom in)
%
#
Network Services
99%
success
DNS 99%
ARP 0%
Authentication Radius... 1%
DHCP 0%
Application
99%
success
Application Reachability 100%
Network Latency 0%
Internet Services 0%
ICMP_GOOGLE
Timeline
Statistics
Distribution
Affected Items
Failures
Attempts
Application Reachability
Network Latency
Internet Services
Sep 3
Sep 4
Sep 5
Sep 6
Sep 7
Sep 8
Sep 9
Sep 10
Sep 11
Latency
2500ms
2000ms
1500ms
1000ms
500ms
0ms
Sep 2
Sep 3
Sep 4
Sep 5
Sep 6
Sep 7
Sep 8
Sep 9
Latency
Packet Loss
80
60
40
20
0
Sep 3
Sep 4
Sep 5
Sep 6
Sep 7
Sep 8
Sep 9
Network Loss
Web
0ms
Sep 2
Sep 3
Sep 4
Sep 5
Sep 6
Sep 7
Sep 8
Sep 9
App Latency
Baseline
PoC- Site
vlan: 103
192.168.103.1
192.168.0.1
10.112.233.130
25
ICMP_GOOGLE
System Changes

CHAPTER 9

Conversations and Queries

IN THIS CHAPTER

Marvis Conversations and Queries Overview

SUMMARY

Watch a video demo to see how easy troubleshooting is with help from the Marvis Conversational Assistant and Marvis Query Language.

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 277.

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 274.

- 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 277.

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:

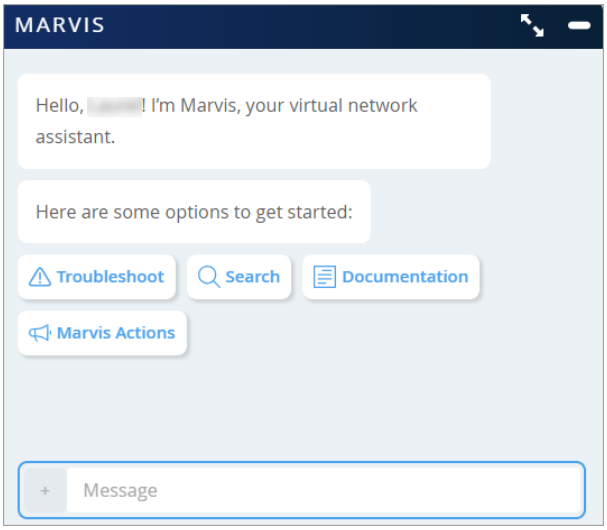
- Meet the subscription requirements. For more information, see "Subscriptions for Marvis" on page 156.
- Have a user account with permission to access all sites in your organization.

Finding the Conversational Assistant

Click the Marvis icon at the top-left corner or bottom-right corner of the Juniper Mist portal.

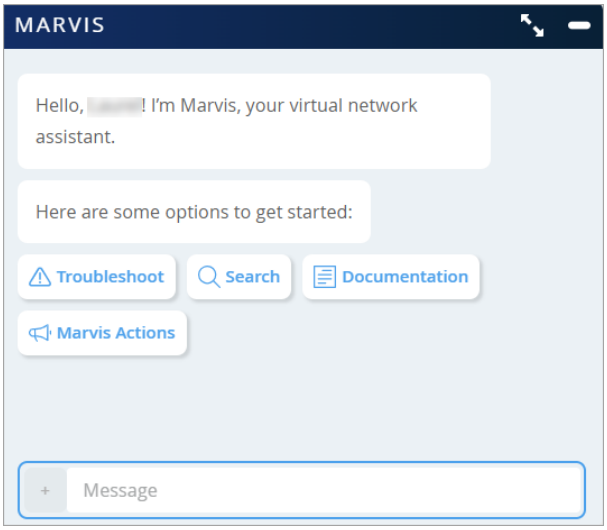
Using Natural Language

Click the Marvis icon, and then enter your question or concern in the **Message** box at the bottom of the Marvis window.



Following Prompts

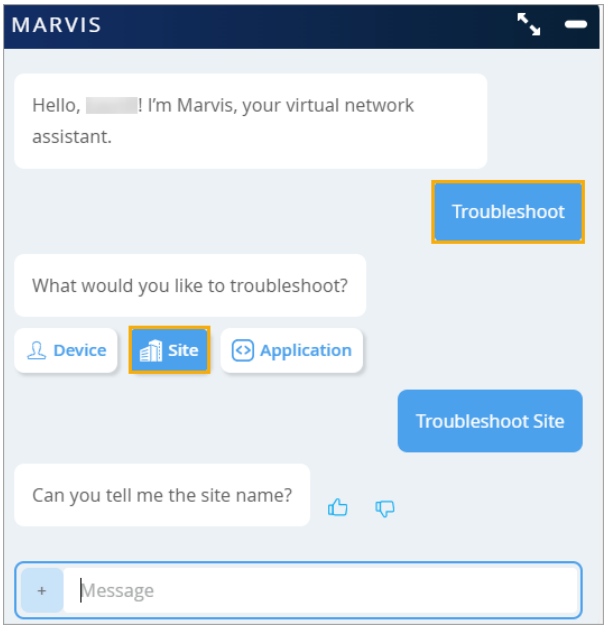
Click the Marvis icon, and then click one of the buttons that Marvis displays.



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.



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 elements listed below. Use your space bar after selecting each element to see the next available options.

- 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, and download the results in CSV format, along with the query string.

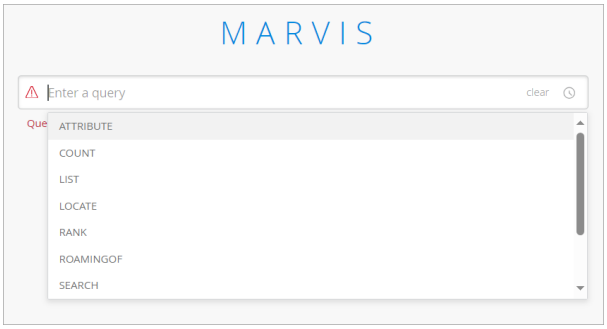
Finding the Marvis Query Page

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

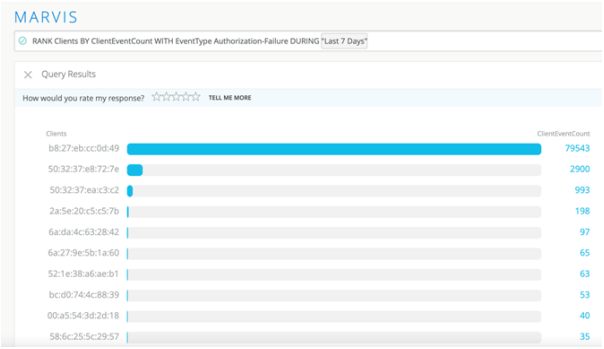
Marvis guides you step by step to enter the required elements in the query.

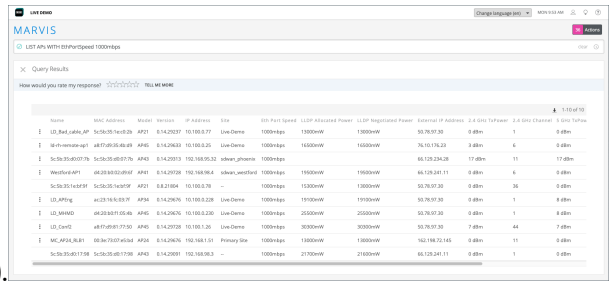
To get started, click in the **Enter a query** text box. Then click one of the options in the drop-down menu.



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:



Here's an example of a LIST query that lists APs with an Ethernet Port Speed of 1000 megabits per second (Mbps). 

NOTE: AP-specific queries have been updated so that you can now LIST, COUNT, and RANK APs based on the following parameters: Eth Port Speed, LLDP Allocated Power, LLDP Negotiated Power, External IP Address, 2.4GHz TxPower, 2.4GHz Channel, 5GHz TxPower, 5GHz Channel, 6GHz TxPower, and 6GHz Channel.

For more information about useful queries, see "Troubleshoot Using Marvis Query Language" on page 279.

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 Channel Utilization of an AP | 286

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 25 on page 280 and Table 26 on page 282 provide a few LIST queries that you can use as a reference to build queries based on your requirements.

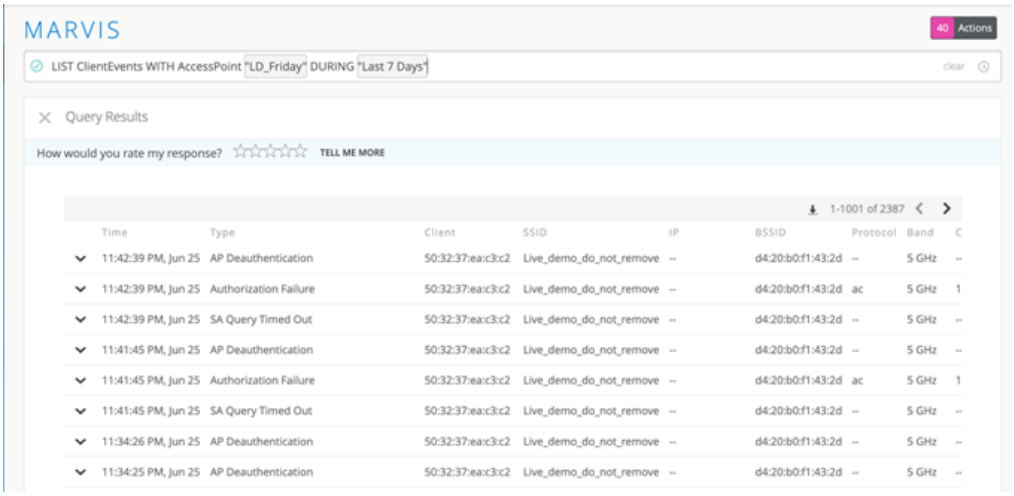
Table 25: Key LIST Queries to View Events

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>*

Table 25: Key LIST Queries to View Events *(Continued)*

If you want to view	Use
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.



This example shows the list for a specific event type:

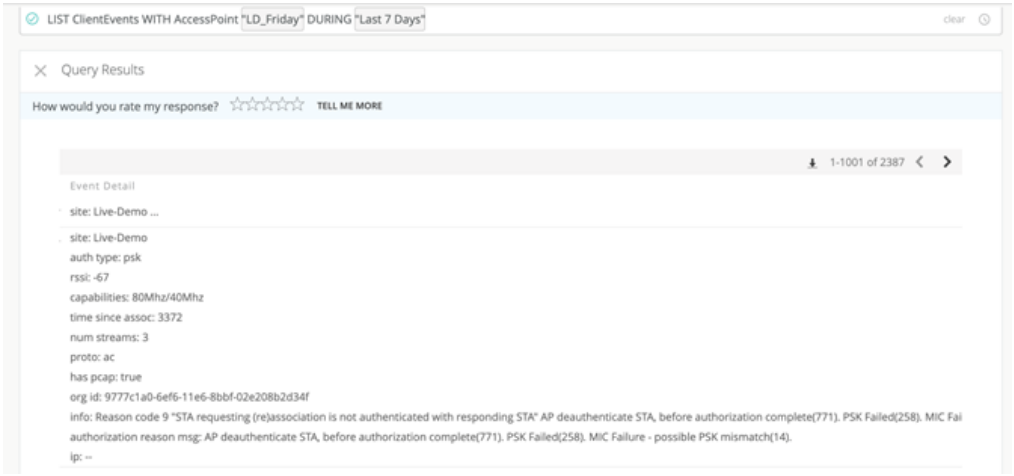
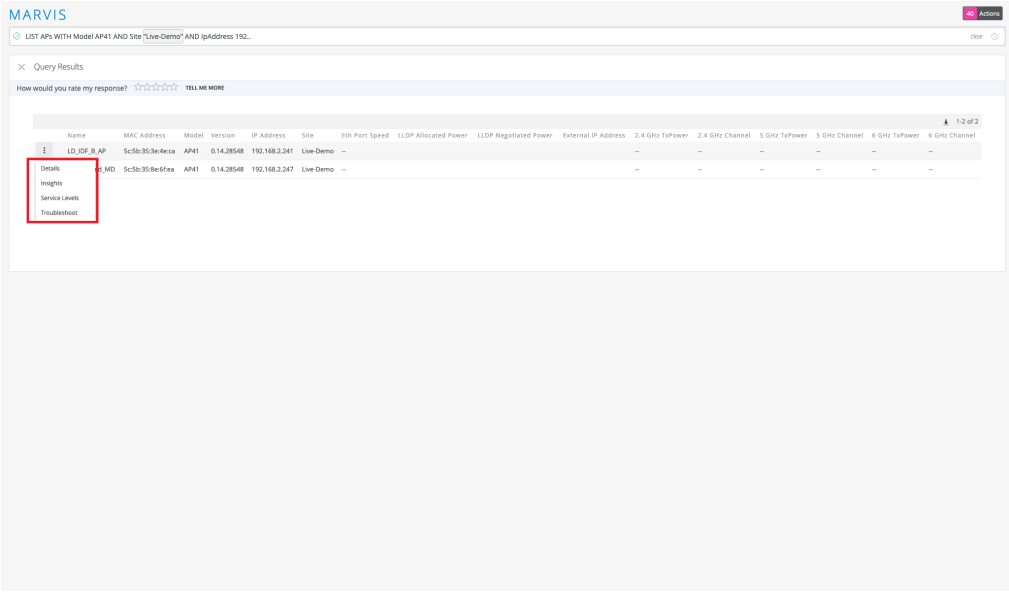


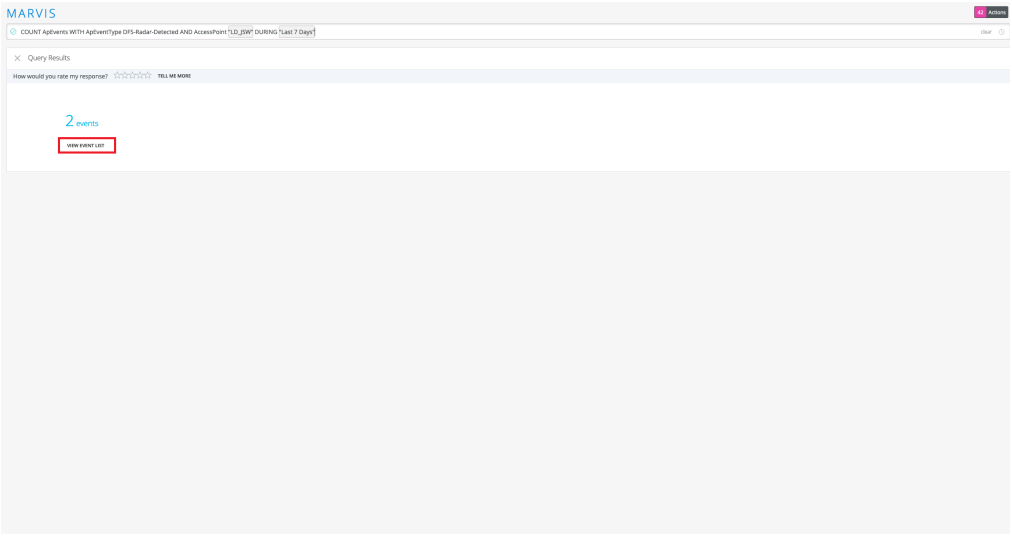
Table 26: Key LIST Queries to View Devices

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>***
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.



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.



View Roaming Details of a Client

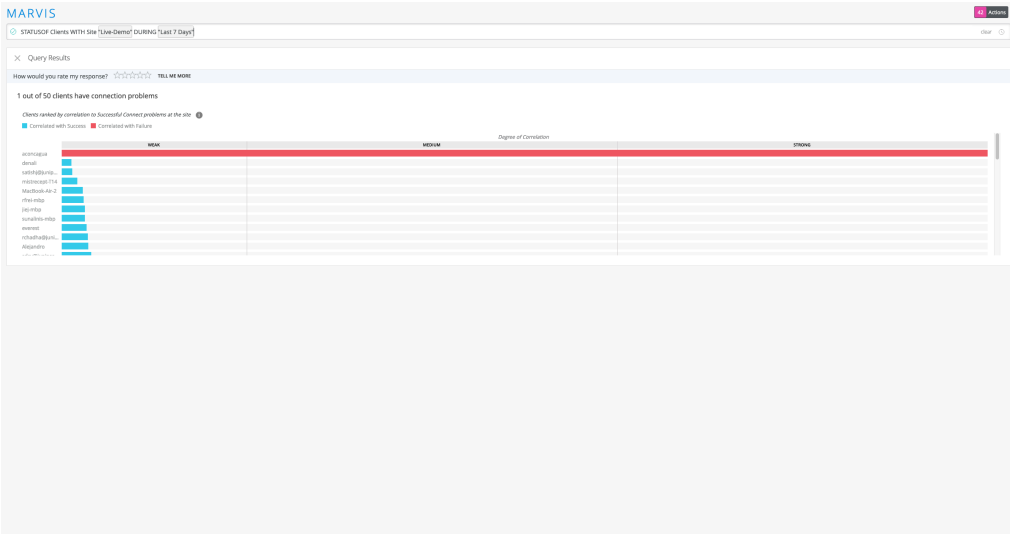
You can use the ROAMINGOF query to see a graphical view of a client roaming between different APs.

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>***



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.

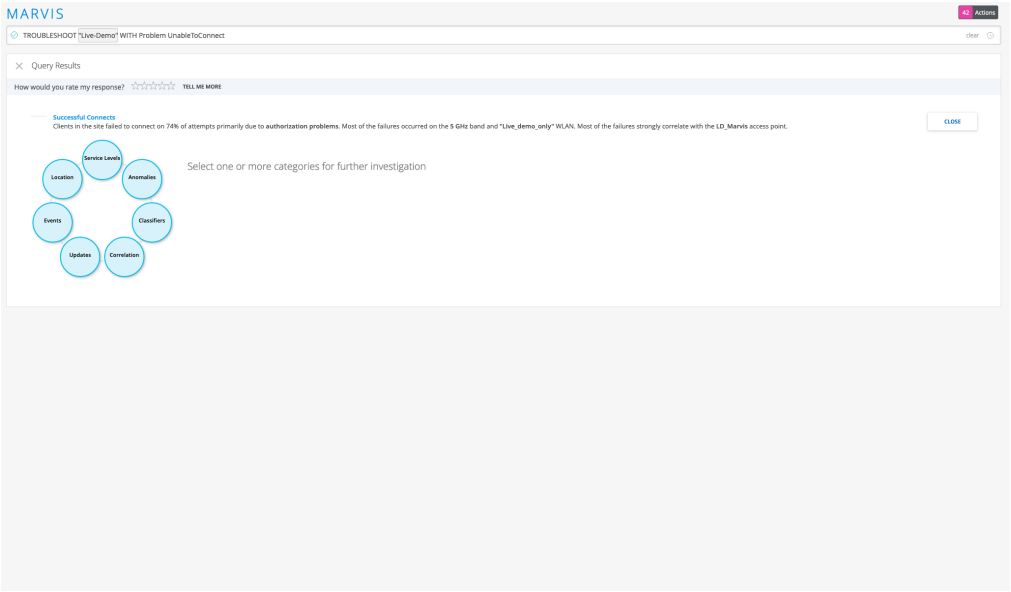
Troubleshoot APs, Sites, or Clients

Table 27 on page 284 lists a few TROUBLEHOOT queries that you can use to troubleshoot a site, a client, or an AP.

Table 27: 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>***

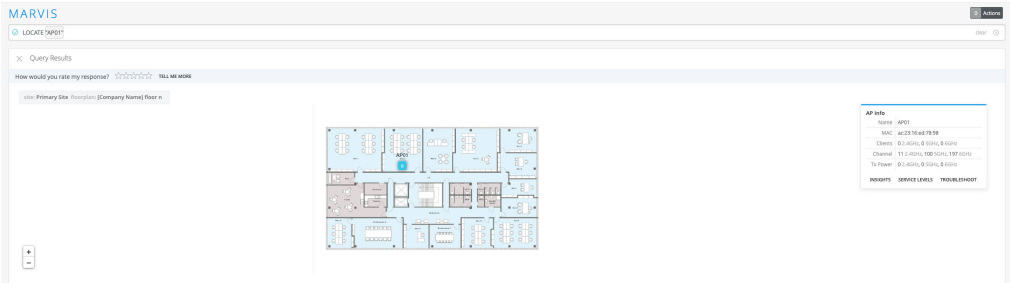
The following screenshot shows the output for the **TROUBLESHOOT <site name> WITH Problem UnableToConnect** query. You'll see that Marvis provides data such as the cause of the issue, the band, and the WLAN on which the issue occurred.



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:

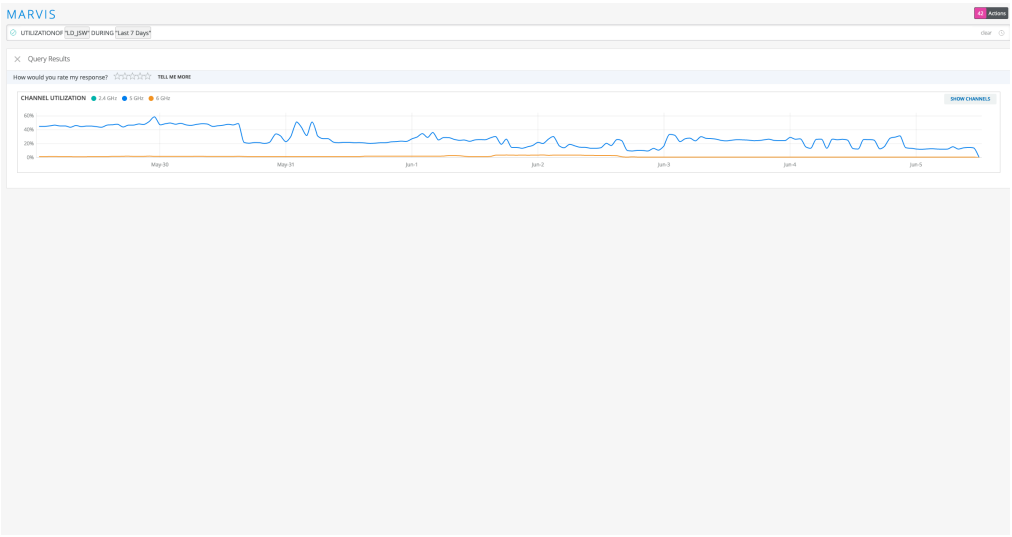
Locate APs, Sites, or Clients

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.



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.



Client Roaming Visualization

SUMMARY

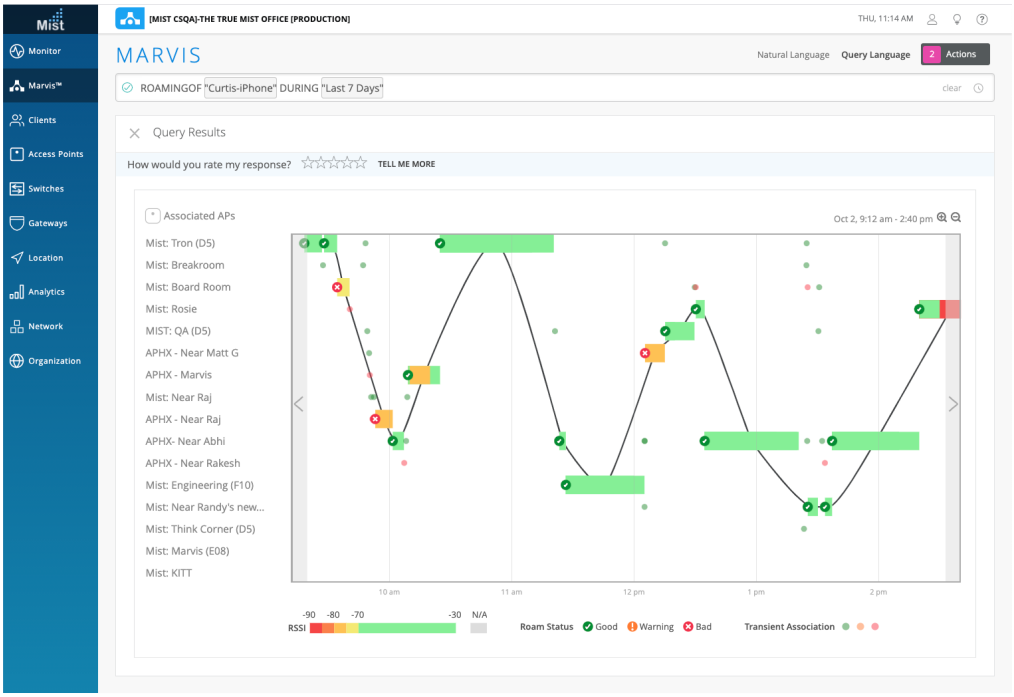
Gain additional insights by using the ROAMINGOF query to view the client roaming status.

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

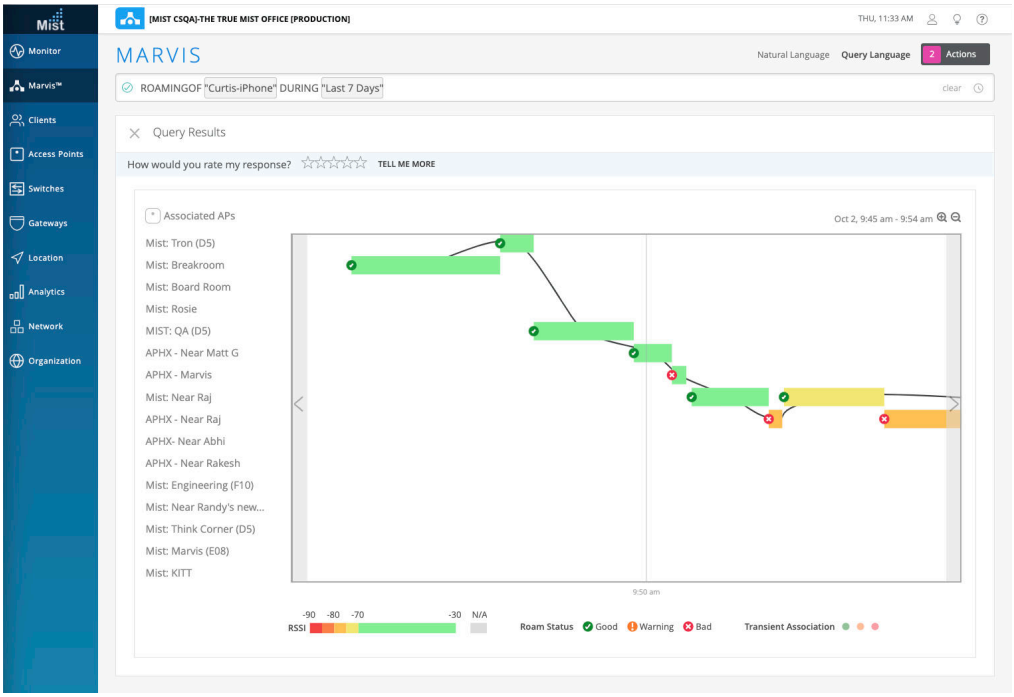
indicator (RSSI) values of the connection. Marvis uses the data from **Client Events** to provide a visual of the path your device takes and its transitions between various APs. Marvis indicates a Bad roaming status when the RSSI is low and a warning roaming status when the client switches to a different 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.

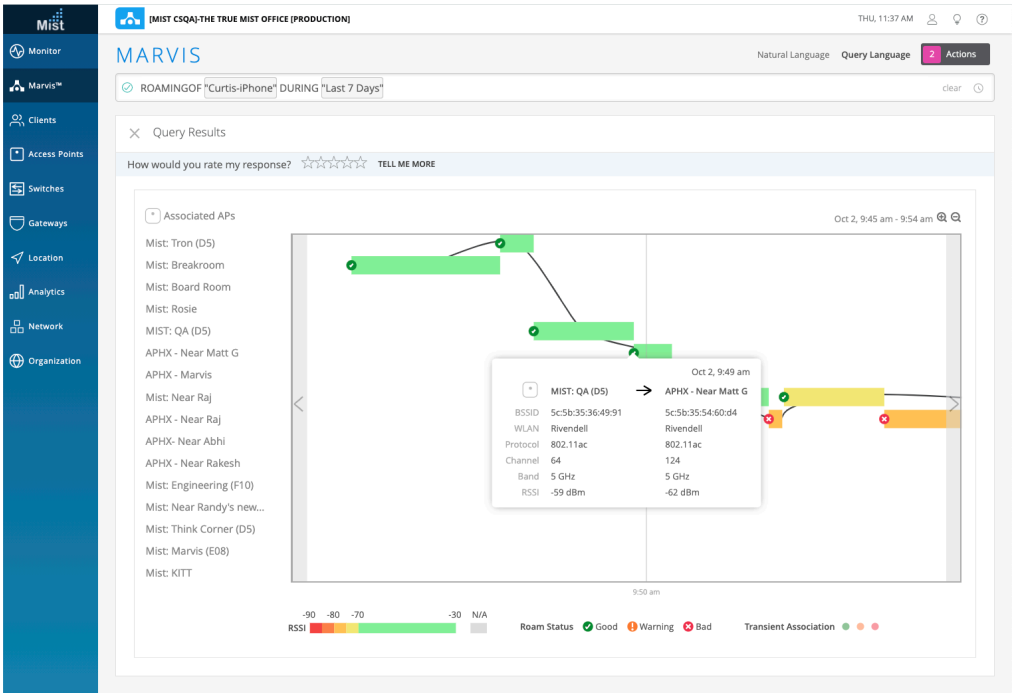
Marvis highlights information such as the roaming status, RSSI value, and transitions, to improve troubleshooting. The dots you see in this screenshot indicate Transient Associations, which means that the device was associated with the AP for a very short time.



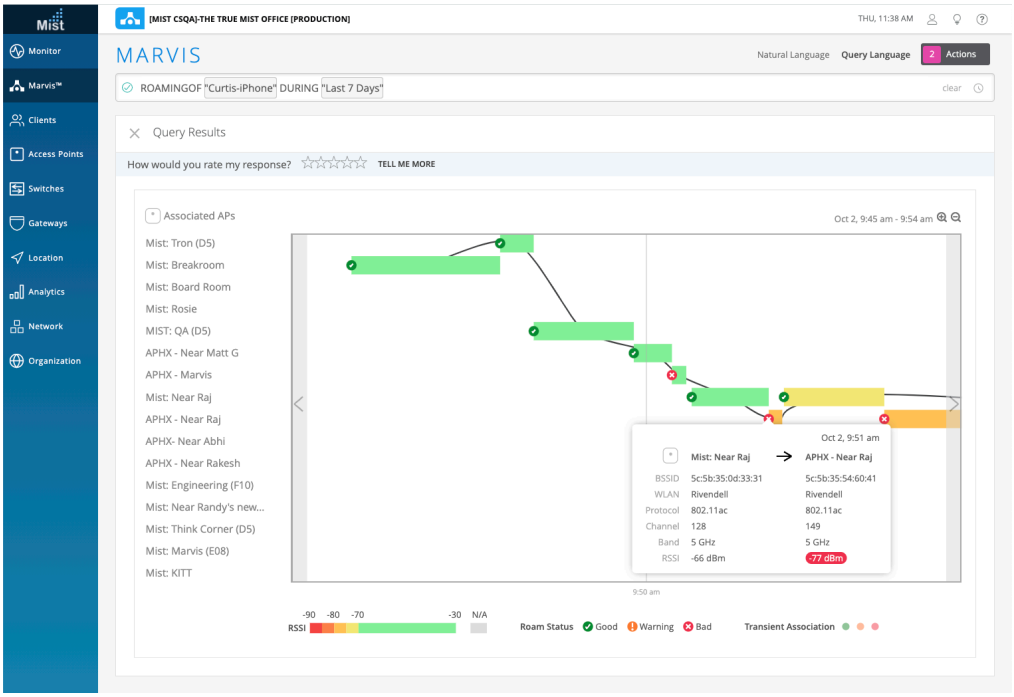
Here is a zoomed-in view of transient associations in the 9:45 a.m. – 9:54 a.m. time interval.



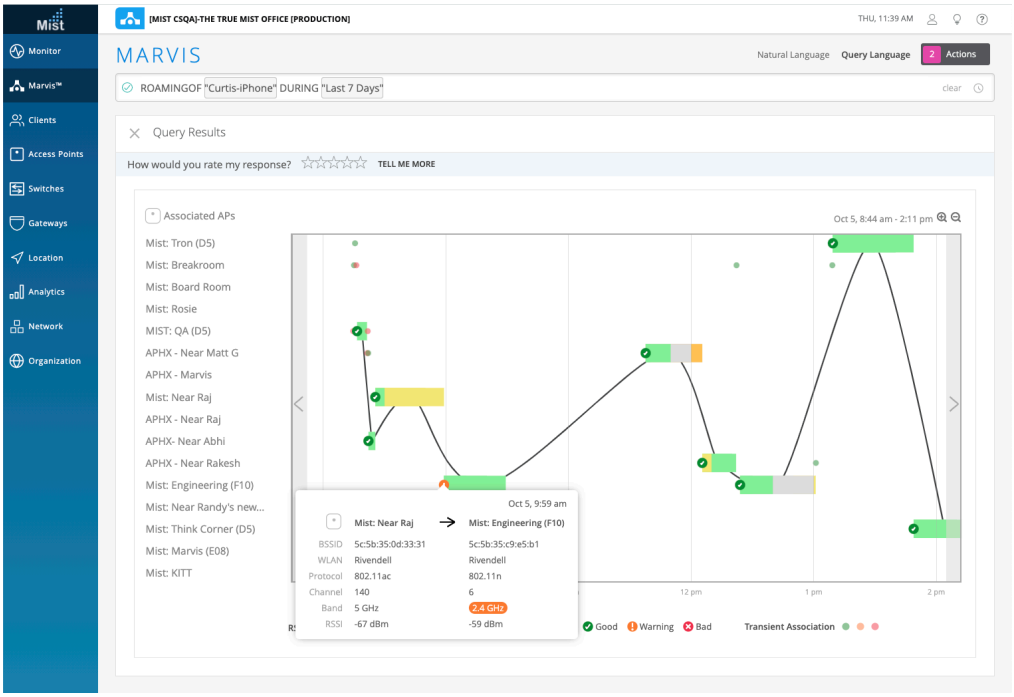
You can hover over the roaming status icons on the timeline to view detailed information about the roaming event, such as the WLAN, channel, band, and RSSI. Here you can see that the client experienced a good roaming event between the APs at 9:49 a.m.



Here's an example of a bad roaming event. Notice that Marvis indicates a low RSSI for this event.



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.



10
CHAPTER

Marvis Client

IN THIS CHAPTER

Marvis Client Overview

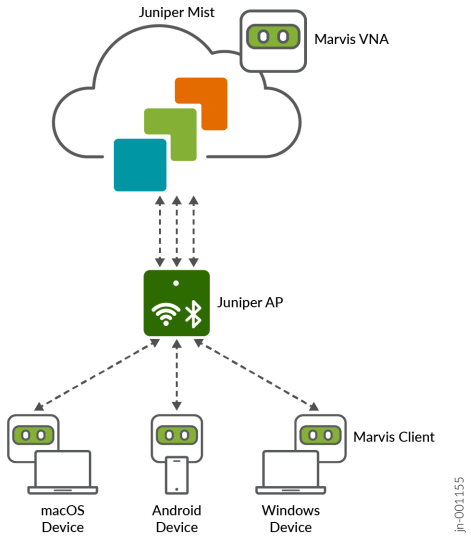
SUMMARY

Get familiar with the Marvis Client. Understand how you can use Marvis Client to get visibility into how your device interacts with the wireless network.

IN THIS SECTION

Marvis client is a software agent in the form of an app or headless service that is installed on end-user devices to view the network from the client's perspective. You can view detailed data and telemetry about how the client experiences the wireless connection, including insight into client roaming behaviors. The Marvis client recognizes the wireless connection and the corresponding signal strength.

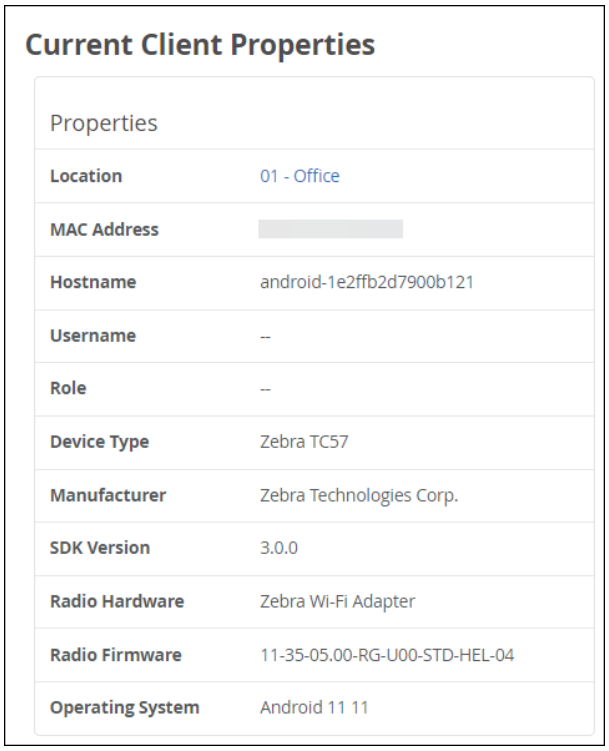
The Marvis client collects data on your device's Wi-Fi interactions, including signal strength, connection quality, and other network metrics. Juniper Mist uses this data to provide a comprehensive view of the device's network experience. You can use this data to identify potential issues or areas for improvement.



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 156.

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. The Marvis client also enhances the Mist device fingerprinting of the device type and OS version in cases where the other Mist fingerprinting data sources—such as user agent and DHCP fingerprinting—lack accuracy. 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 Juniper 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.

The following video provides a high-level overview of the Marvis client.

Video: NOW in 60: Marvis Client

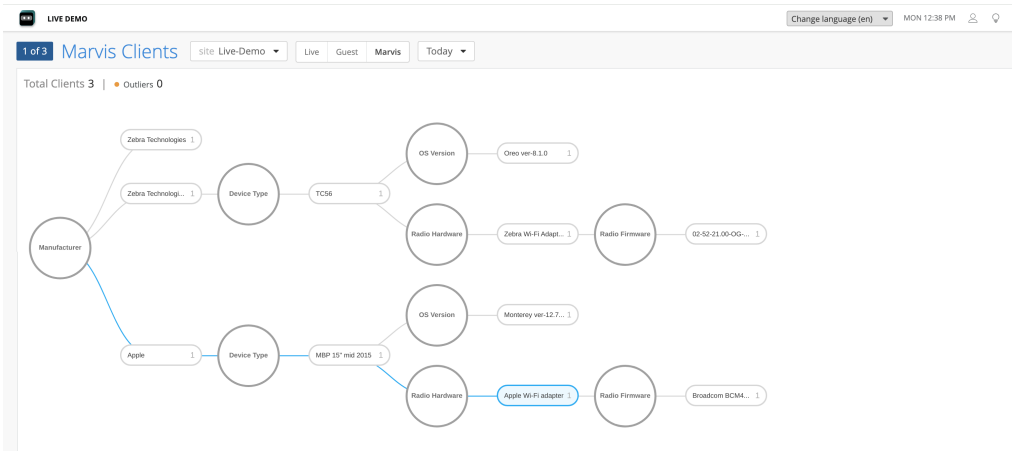
Marvis Clients View in the Juniper Mist Portal

You can view all connected Marvis clients directly on the Juniper 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.

The Marvis clients page also highlights possible outliers that do not conform to the properties (for example, radio firmware version) seen for other clients with the same manufacturer or device type.

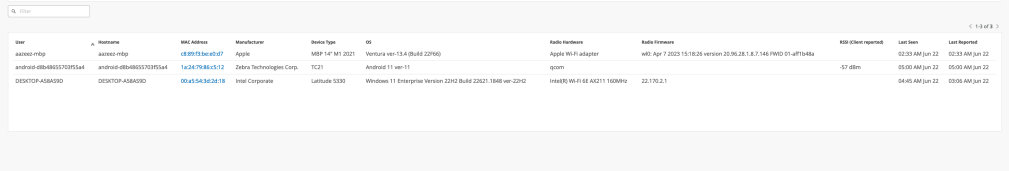
You can select either the Tree or List view to display your Marvis clients, as follows:

- **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.

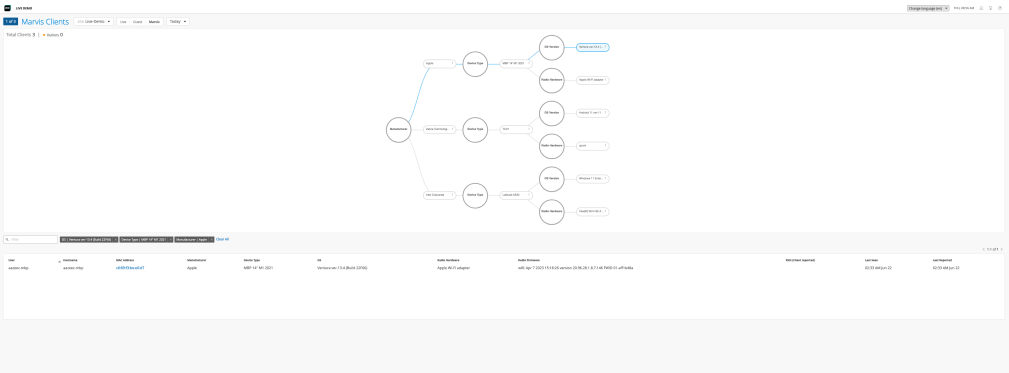


- **List view**: Presents client information in a tabular format. The default columns include user, hostname, MAC address, manufacturer, device type, device OS, radio hardware, radio firmware, and

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.



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.



Subscription Requirements for Marvis Client

You'll need a Marvis Client (S-VNACLIENT) subscription per client.

Supported Devices

The Marvis client is supported on the following devices:

- Android—Oreo 8.0 and later releases
- Windows—10 or later releases
- macOS—macOS 12 or later releases

Marvis Android Client

SUMMARY

Complete the preinstallation tasks, and then choose the method that you want to use to install the Marvis Client on your device.

IN THIS SECTION

The Marvis client for Android provides detailed visibility into how your Android device interacts with the wireless network. It helps optimize network performance, streamline troubleshooting, and enhance overall user experience by providing insights into device connectivity and performance.

The Marvis Android client is supported on the following devices:

- Android handheld devices and smartphones that run Android 11.0 and later versions
- Zebra devices that run Android 11.0 and later versions

Marvis Android Client Installation Overview

IN THIS SECTION

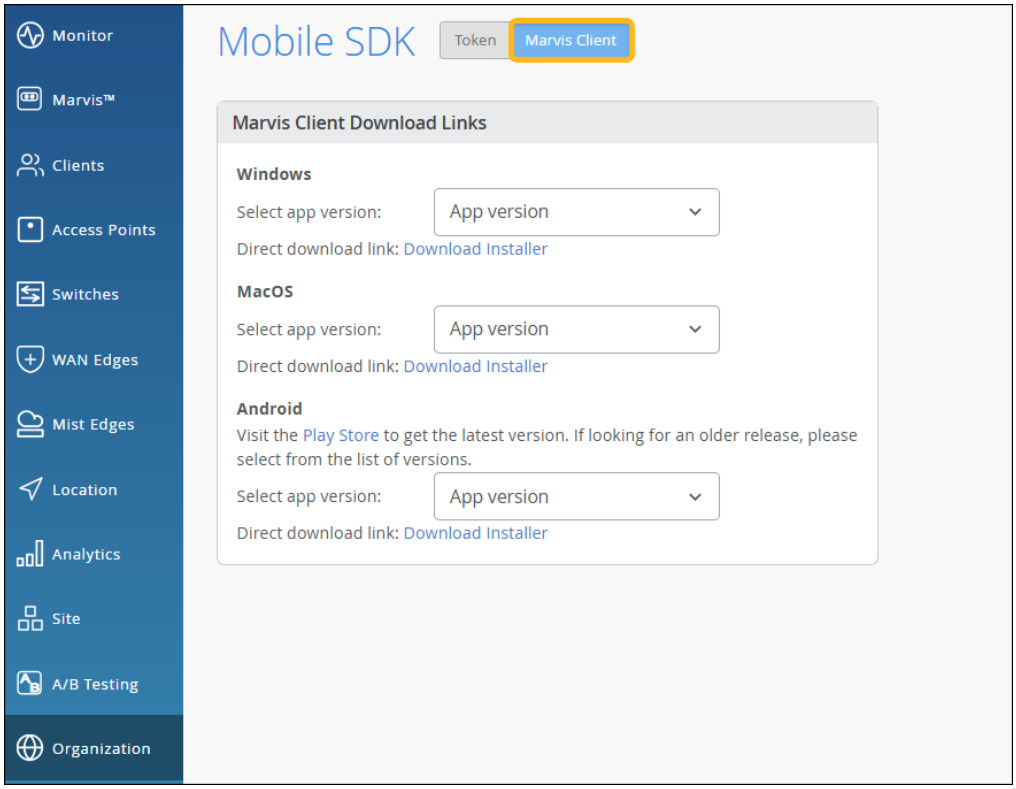
Connection States | 301

You can use any one of the following methods to install the app:

- Manual—Download and install the Marvis client app directly from the Google Play Store or the Juniper Mist portal.

  To download the client from the Juniper Mist portal:

  1. Select **Organization** > **Admin** > **Mobile SDK** from the left menu.
  2. Click **Marvis Client** at the top of the Mobile SDK page.
  3. Select the app version under Android, and then click **Download Installer**.



- Android Debug Bridge (ADB)—Install the app using ADB, a command-line tool that developers can use to communicate with Android devices to debug issues and install/uninstall apps.
- Mobile device management (MDM)—Use any of the following MDM solutions to install the app:
  - AirWatch or VMware Workspace ONE

- SOTI

NOTE: We've tested interoperability only with the MDMs listed above.

Requirements

Before you start the installation:

- Enable the mandatory permissions listed in Table 28 on page 297 for the app.

  Table 28: Permissions Required for the Marvis Client App for Android

Permission	Description	Mandatory or Optional
Location—Set as **Allow all the time**	Enables the Marvis client app to obtain the Wi-Fi roam data and function as expected.	Mandatory
Bluetooth	Allows the app to obtain the x and y coordinates of the location.	Mandatory
Nearby devices	Enables the app to determine the relative location of nearby devices. Android 12 needs this permission enabled to run the location service on mobile devices.	Mandatory
Notifications	Enables notifications if you want to be notified when the Marvis client is running actively in the background.	Optional
Camera—Set as **Allow Once**	Enables you to scan the QR code during enrollment. You need not enable this permission if you are installing the app through ADB or MDM.	Optional

- Configure your network firewall settings to allow the Marvis client to connect to your organization.

If your organization resides in the 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 the HTTPS protocol port 443 for domain

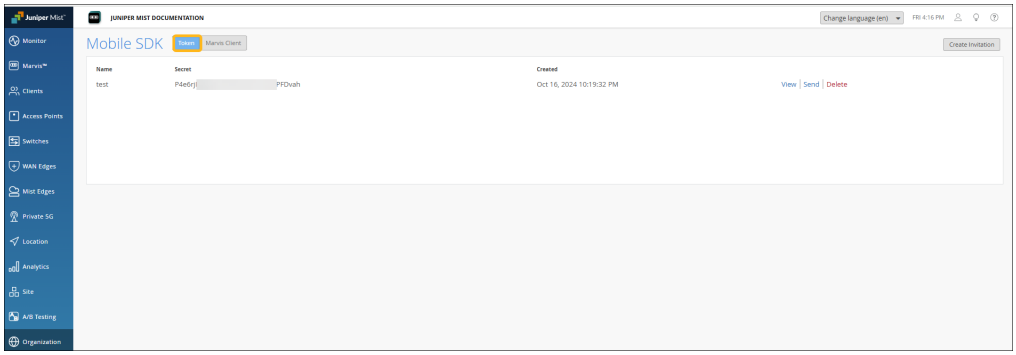
If your organization resides in the Google Cloud Platform (GCP) cloud, use the following settings:

- wss://client-terminator.gc1.mist.com/ws or protocol WSS (websocket) port 443 for domain/path
- https://api.gc1.mist.com/ or the HTTPS protocol port 443 for domain

NOTE: If your organization resides in a cloud other than AWS or GCP, contact the support team for the appropriate URLs to configure the firewall settings.

- Obtain your secret token or QR code to onboard the Marvis client.

  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.

NOTE: To obtain the secret token using API, see Create SDK Invite.

As a best practice, we recommend that you disable the random MAC address. This avoids the need to re-register your device every time it connects to the network. To disable the random MAC address:

1. Navigate to the Settings page on your device.
2. Tap **Network & Internet** or **Connections** and then tap **Wi-Fi**.
3. Tap the gear (settings) icon next to the wireless connection.
4. Tap **MAC Address Type** and then tap **Phone MAC**.

Operational Modes

The Marvis client operates in the following modes:

- Onboarding mode—Default mode when you install the Marvis client app using the GUI method. In this mode, you can onboard devices through a NAC portal.
- Telemetry mode—Mode when you install the Marvis client app using the CLI method. This mode is the standard operational mode for live environments.

Configure Marvis Android Client for Onboarding

You can use the Marvis Client app to onboard devices to the Juniper Mist Access Assurance network through a custom Network Access Control (NAC) portal. For more information, see Client Onboarding Through a NAC Portal Using the Marvis Client App.

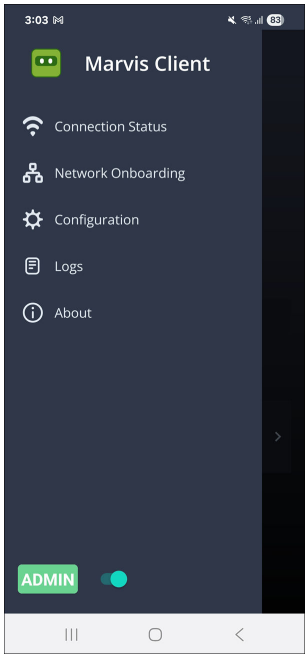
Configure Marvis Android Client to Operate in Telemetry Mode

To enable the Marvis client to operate in Telemetry mode, install the Marvis client using an MDM ("Deploy the Marvis Client Using the SOTI MDM)" on page 301 or **adb** command ("Deploy Marvis Android Client Using Other MDMs" on page 305).

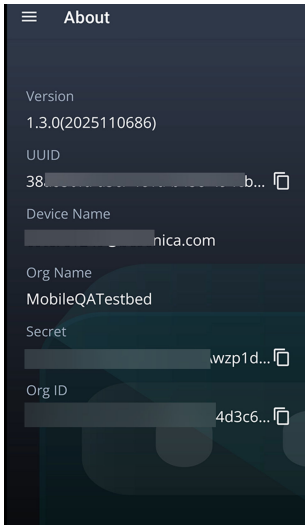
Admin Mode on the Marvis Android Client

When you open the Marvis client in onboarding or Telemetry mode, you'll see only the **Network Onboarding** and **About** options. To view other menu options, you'll need to switch to the Admin mode:

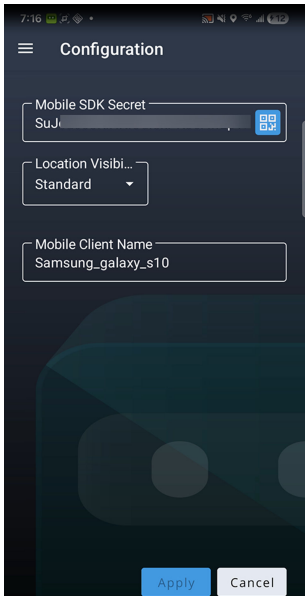
1. Tap the hamburger icon, and then tap the Marvis client icon 7 times.
2. Enter the password as AIDriven. Now you can see that you are in the Admin mode and can view additional menu options.



In Admin mode, the About page displays the UUID, Device Name, Org ID and Org Name.

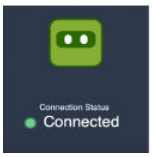


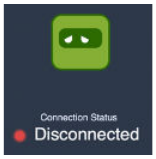
You can use the Configuration option to update or verify the client name, location access, and mobile SDK token.

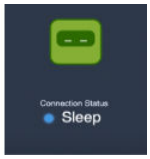


Connection States

The Marvis client status is indicated by the following visual indicators and connection states. Note that you can view these states only if the Marvis client is in Telemetry mode.





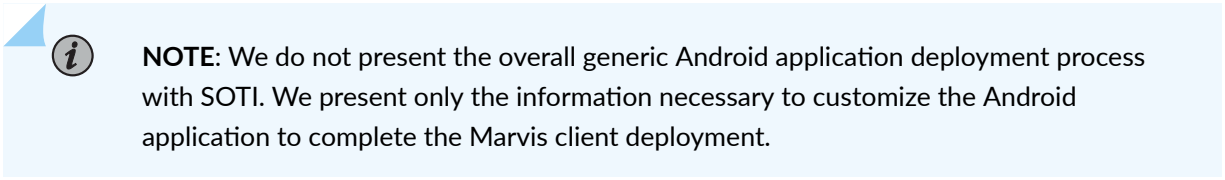


- Disconnected—Client is not connected to the Juniper Mist cloud.
- Connected—Client is connected to the Juniper Mist cloud.
- Sleep —Client is connected to the Juniper Mist cloud through a non-Juniper AP.

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 is 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 Marvis 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 the SOTI MDM:

1. On your Windows device or VM, launch Package Studio and create a package project with the following settings:
   - **Processor**—**All** (unless you're targeting specific CPU or device types)
   - **Platform**—**Android**
   - **OS Version**—11 or later
   - **Version String**—Same as the APK version
   - **Vendor**—Juniper Networks
   - 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(string);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(string);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 cover only the specific steps needed to complete the Marvis client deployment.

Use the following intent command to deploy the client:

```
mode=explicit,broadcast=false,action=android.intent.action.MAIN,package=com.mist.marvisclient,cla
ss=com.mist.marvisclient.MainActivity,extraString=MOBILE_SDK_SECRET=TheSecretValueHere(string)
```

If you have configured a specific port on a Zebra device for voice calls, then use the following intent command:

```
mode=explicit,broadcast=false,action=android.intent.action.MAIN,package=com.mist.marvisclient,cla
ss=com.mist.marvisclient.MainActivity,extraString=MOBILE_SDK_SECRET=TheSecretValueHere(string),ex
traString=MOBILE_VOICE_CALL_PORT=5070
```

You can use the following references to deploy the intent command:

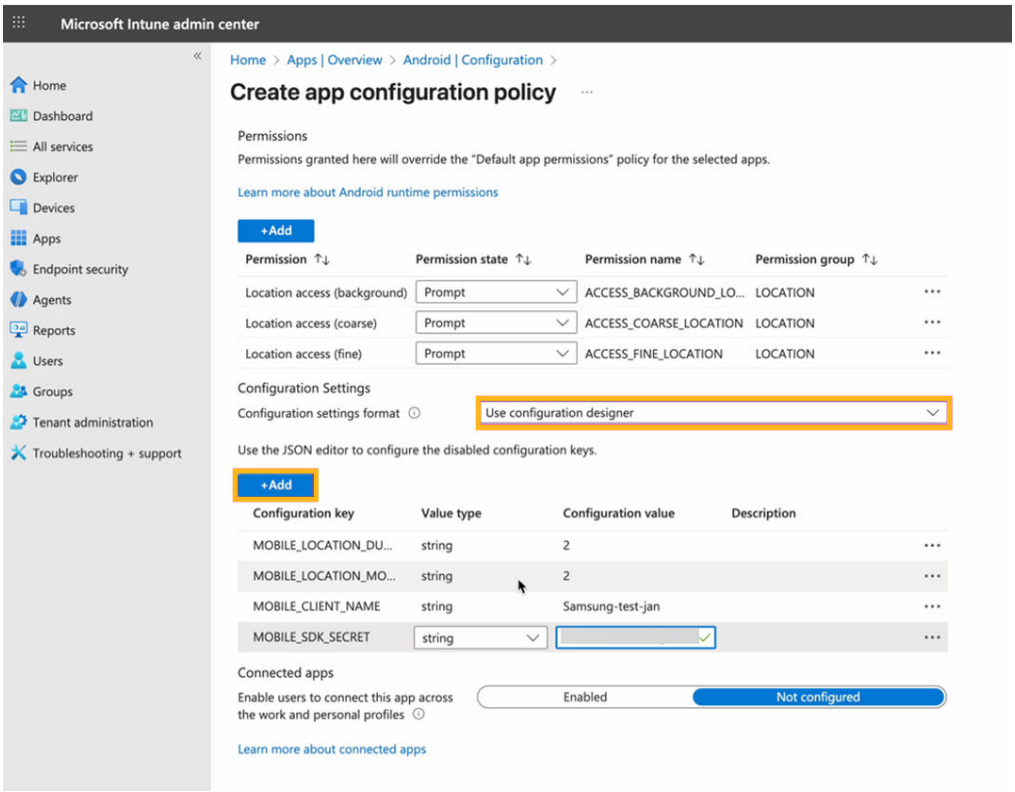
- Configuring Automatic Launch for Android Mobile Devices if you have already deployed the Marvis client on the device
- RunIntent Action, File-Action Android for new deployments of our APK installer on devices

Deploy Marvis Android Client Using Intune

Follow the procedure in Add Managed Google Play Apps to Android Enterprise Devices With Intune to deploy the Marvis Android client using Intune.

Once the Marvis client is installed successfully, add the configuration details such as secret token, location mode, device name:

1. On the Intune portal, navigate to **Apps>Manage Apps**.
2. Select **Configuration>Create>Managed devices**.
3. Add Basic details such as the name, platform, and profile type. Select Marvis Client as the Targeted app.
4. Add the location access permissions and configuration settings such as MOBILE_LOCATION_DURATION, MOBILE_LOCATION_MODE, MOBILE_CLIENT_NAME, AND MOBILE_SDK_SECRET.



5. Add groups.
6. Click **Create**.

Deploy Marvis Android Client Using Other MDMs

If you're using any other MDM, verify that the MDM supports intent execution. Here is a sample for Android Debug Bridge (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(string)" -t "text/plain"
```

Enable the location mode and update the client name:

```
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(string)" -t "text/plain" --es "MOBILE_CLIENT_NAME" "TheClientName(String)" -
t "text/plain" --es "MOBILE_LOCATION_DURATION" "2" -t "text/plain" --es "MOBILE_LOCATION_MODE"
"2" -t "text/plain"
```

If the MDM solution does not support execution of Android intents, you might need to onboard each deployed client device manually.

Verify the Installation

After you install and onboard the Marvis client, verify that those processes have run correctly. Ensure that your device is connected to the Mist Wi-Fi network.

To verify the installation:

- Confirm that the secret token value is applied correctly. Navigate to the About or Configuration (if you're in the non-production mode) page on the Marvis client app and verify that the secret token value is still stored in the field.

  If the data does not persist and the secret token field is empty, enter the secret token value manually. You might need to also configure the application deployment to retain the application data.

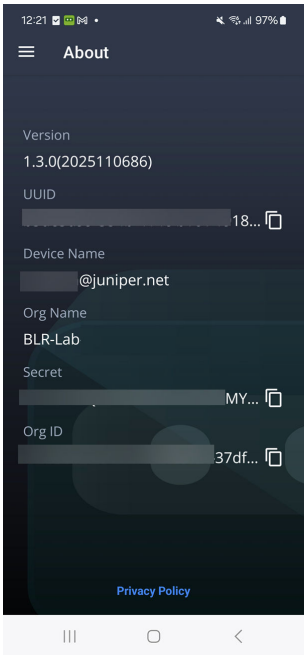
- About 15 minutes after you onboard the Marvis client, confirm that the Marvis client data is available on the Juniper Mist portal. You need to wait for a minimum of 10 to 15 minutes after onboarding the Marvis client for the data to propagate to the Juniper Mist cloud.

  The client data is not available on the Juniper Mist portal when a problem occurs in the client workflow of collecting and sending data to the Juniper Mist cloud. Contact the support team. You

can access the logs in the Marvis client app. See "View Logs in the Marvis Android Client " on page 306. Alternatively, you can also use tools such as Logcat or Android Debug Bridge (ADB) to collect the Marvis client logs and share the logs with the support team.

For Zebra devices, you can use the RxLogger tool as an alternative method to collect logs.

When you contact the support team, you must share the Marvis client UUID. You can find the UUID on the **About** page of the Marvis client app. The UUID is used to track the data flow from the Marvis client to the Juniper Mist cloud.



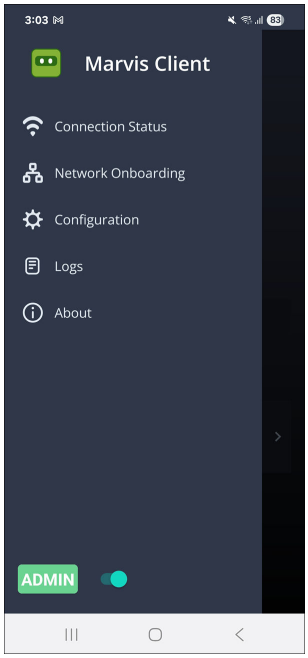
View Logs in the Marvis Android Client

The Marvis client classifies the logs as:

- Info—General information
- Error—Critical issues
- Debug—Detailed data that you can use to debug issues

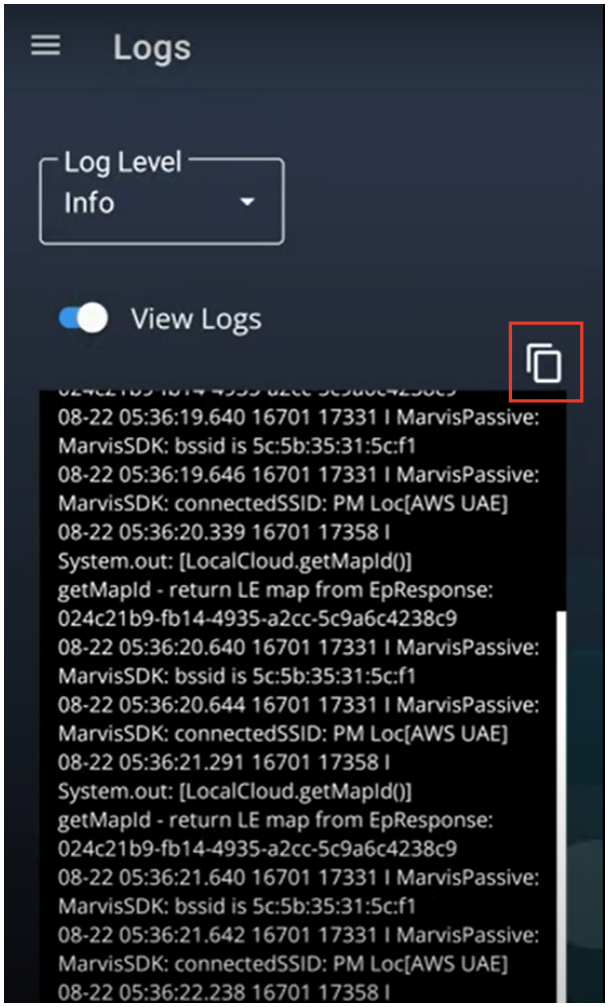
To view the logs in the app, you'll need to enable debug mode on the app:

1. Tap the hamburger icon and then tap the **Marvis Client** icon 7 times.
   You'll be prompted for a password.
2. Enter the password as **AIDriven**.
   You'll see the Logs option listed in the menu.



3. Tap **Logs**.
4. Enable **View Logs** to view the logs captured by the Marvis client. You can select the type of information you want to view from the **Log Level** drop-down list.

   You can click the **Copy** button to copy and send the log details to the support team for troubleshooting.



NOTE: If you contact the Juniper Mist support team to resolve any issue, you might be asked to provide details such as the organization ID, UUID, and organization name. You can find these details listed in the About page. Note that you'll need to access this page in Admin mode to view the information. See "Admin Mode on the Marvis Android Client" on page 299.

Marvis Windows Client

SUMMARY

Complete the preinstallation tasks, and then choose the method that you want to use to install the Marvis client on your Windows device.

IN THIS SECTION

The Marvis client for Windows provides detailed visibility into how your Windows device interacts with the wireless network. The Marvis client helps optimize network performance, streamline troubleshooting, and enhance overall user experience by offering insights into device connectivity and performance.

Marvis Windows Client Installation Overview

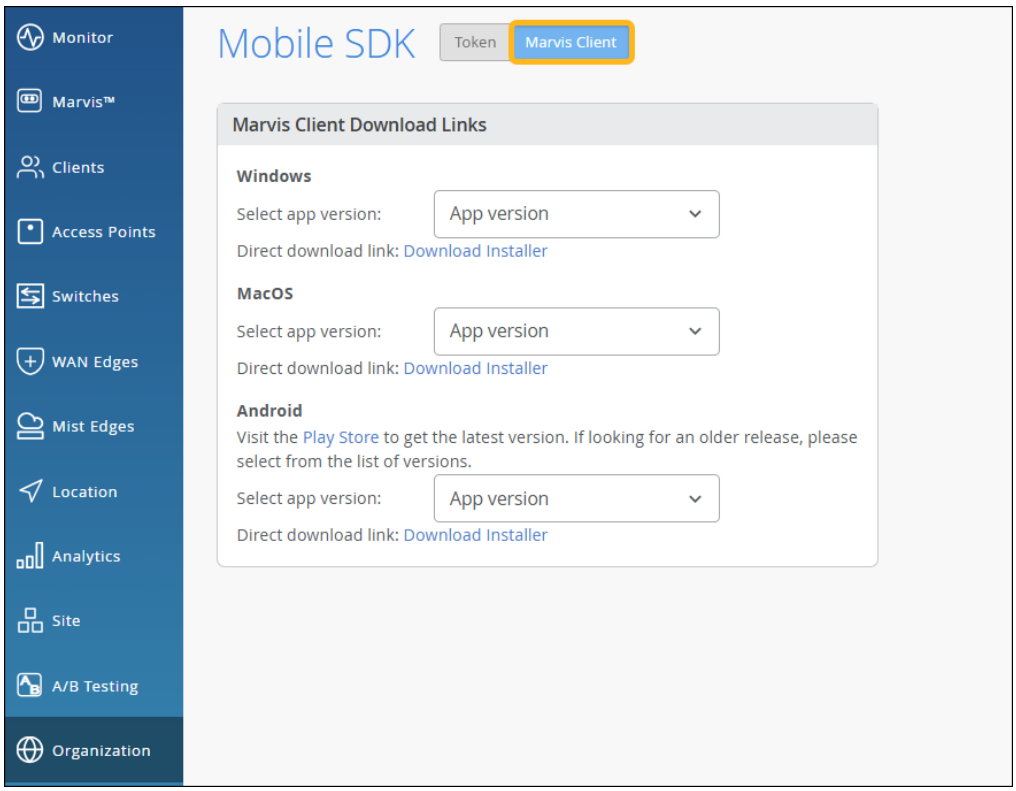
IN THIS SECTION

Operational Modes | 312

You can download the Marvis client for Windows (marvisclient-installer.msi file) from the Juniper Mist portal.

To download the .msi file from the Juniper Mist portal:

1. Select **Organization** > **Admin** > **Mobile SDK** from the left menu.
2. Click **Marvis Client** at the top of the Mobile SDK page.
3. Under **Windows**, select the app version, and then click **Download Installer**.



4. Extract the marvisclient-installer.msi file from marvisclient-installer.zip.

Save the .msi file in a folder on your device.

Installation Options for the Marvis Windows Client

You can use any of the following installation options:

- "Install the Marvis Windows Client (GUI Method)" on page 313
- "Install the Marvis Windows Client (CLI Method)" on page 313
- "Install the Marvis Windows Client (Configuration File Method)" on page 315
- "Deploy the Marvis Client on Windows Devices Using an MDM" on page 316

Prerequisites

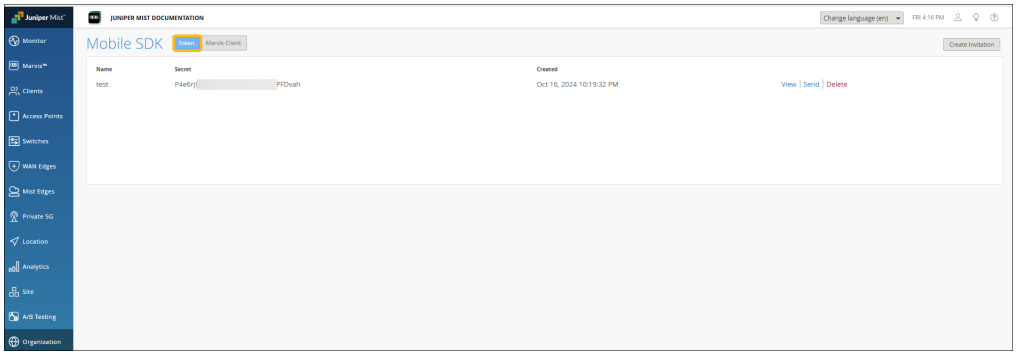
Before you begin, you'll need to have:

- **.Net Framework Runtime (4.6.2 or above)** installed on your device.

  NOTE: You can opt to install these applications later after installing the Marvis Windows client. However, installing the application later requires you to restart the device.

- The secret token or QR code to onboard the Marvis client.

  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.

> **NOTE**: To obtain the secret token using API, see https://api.mist.com/api/v1/docs/Org#sdk-invite.

- Windows 10 or a later release running on the devices
- Location services enabled to allow Marvis client to collect Wi-Fi telemetry from the client device

  Location services in this context refer to the device-level location settings available on Windows. Note that client real-time location services are not supported on Windows devices.

> **NOTE**: On devices running Windows 11, version 24H2 and later, the Marvis client can obtain the BSSID of the wireless network only if location services are enabled. Disabling location services causes the Marvis client to switch to the Sleeping state.
>
> This behavior is different In Windows 11 versions earlier than 24H2. In those versions, the status of the location services does not impact the state of the Marvis client. The Marvis client fetches the BSSID of the wireless network irrespective of the location services being enabled or disabled. The Marvis client remains in the Connected state when location services are enabled or disabled.

Operational Modes

The Marvis client operates in the following modes:

- Onboarding mode—Default mode when you install the Marvis client app using the GUI method. In this mode, you can onboard devices through a NAC portal.
- Telemetry mode—Mode when you install the Marvis client app using the CLI method. This mode is the standard operational mode for live environments.

Configure Marvis Client for Onboarding

You can use the Marvis Client app to onboard devices to the Juniper Mist Access Assurance network through a custom Network Access Control (NAC) portal. For more information, see Client Onboarding Through a NAC Portal Using the Marvis Client App.

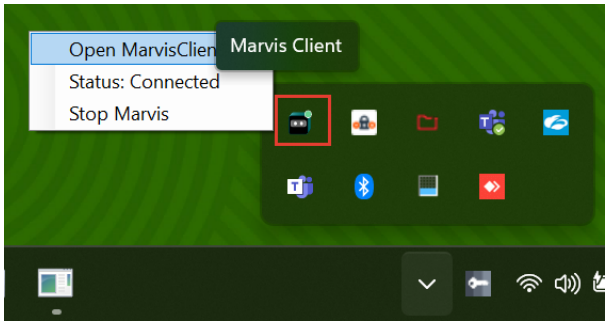
Configure Marvis Windows Client to Operate in Telemetry Mode

To enable the Marvis client to operate in Telemetry mode, you must install the Marvis Windows client using the CLI method.

Install the Marvis Windows Client (GUI Method)

When you install the Marvis Windows client using the GUI method, the Marvis client is installed in the Onboarding mode. To install the Marvis Windows client:

1. Double-click the marvisclient-installer.msi file that you downloaded from the Juniper Mist portal.
2. Click **Yes** to proceed with the installation.
3. Verify that the installation is successful. After the installation is complete, you'll see the Marvis icon in the system tray.
4. Click the Marvis icon in the system tray to open the Marvis client app. To see the menu, right-click the icon.



You can now onboard your device through a NAC portal using the Marvis client app. See Client Onboarding Through a NAC Portal Using the Marvis Client App.

Install the Marvis Windows Client (CLI Method)

You can use the CLI method to install the Marvis client app if you want to make some advanced customization during installation.

1. Open a command prompt window as an administrator or as a user with administrator privileges.
2. Navigate to the folder where you saved the marvisclient-installer.msi file.
3. Use one of the following options to install the client using your secret SDK token:

> **NOTE**: You must install the Marvis client in quiet mode using administrator privileges. For Windows 11, ensure to enter the quiet mode parameter `/qn` at the end of the `msiexec` installation command. For Windows 10, there is no restriction on the placement of the `/qn` parameter.

- Default configuration:

```
msiexec /i MarvisInstaller.msi MOBILE_SDK_SECRET="customer-sdk-token" /l*v
InstallLog.log /qn
```

- Custom configuration:

  You can customize the installation by configuring additional parameters listed in Table 29 on page 314. Here's an example:

```
msiexec /i MarvisInstaller.msi MOBILE_SDK_SECRET="customer-sdk-token"
MIST_BATTERY_SAVING="standard" /l*v InstallLog.log /qn
```

Table 29: Custom Configuration Parameters for Marvis Client Installation

Parameter	Description
MOBILE_SDK_SECRET	The SDK invite code or secret for your organization
MIST_BATTERY_SAVING	Determines the frequency at which the client sends the payloads. You can use one of the following Battery Saving modes: • **High**: With reduced frequency of data transmission, this mode helps conserve battery power. This mode is suitable for scenarios that require less frequent updates. • **Standard**: This mode provides a balance between data and battery consumption, offering more frequent updates without significantly impacting battery life. • **Low**: With the highest frequency of data transmission, this mode provides the most detailed insights into network performance. However, this mode requires more battery power compared to the other modes.

Table 29: Custom Configuration Parameters for Marvis Client Installation *(Continued)*

Parameter	Description
MIST_LOG_LEVEL	Defines the log level for the Marvis client.
MIST_UI_ENABLED	Hides (value=True) or shows (value=False) the Marvis client UI during installation. The default value is **true**.
Proxy Server Settings	
MIST_PROXY_URL	Complete URL of the proxy server including the port.
MIST_PROXY_BYPASS_LIST	List of hosts on which you don't want to apply the proxy settings.
MIST_PROXY_USERNAME	Username (required if the proxy server requires authentication).
MIST_PROXY_PWD	Password (required if the proxy server requires authentication).

4. Verify that the installation was successful. See "Verify the Marvis Client Installation for Windows" on page 320.

Install the Marvis Windows Client (Configuration File Method)

You can install the Marvis client using a transform file, which enables customized or bulk installations.

1. Set up a transform file. The transform file (*.mst) provides the .msi file with the configuration parameters to customize the default installation. You can use the configuration parameters listed in Table 29 on page 314.

   For information about setting up a transform file, see How to Edit an MSI File using [ORCA Editor (plus alternative tool)].

2. Open a command prompt window and enter the following command:

```
msiexec /i MarvisInstaller.msi TRANSFORMS=<path-to-mst-file> /l*v InstallLog.log /qn
```

Deploy the Marvis Client on Windows Devices Using an MDM

IN THIS SECTION

You can deploy the Marvis client on Windows devices by using the SOTI or Intune mobile device management (MDM) solution. Before you begin, verify that all devices have the appropriate MDM profiles and permissions assigned.

You can refer to the following topics for information about enrolling and managing devices using MDMs:

- SOTI
  - Enrolling Windows Modern Desktop Devices
  - Installing an App Using SOTI
  - Managing App Policies for Windows Devices Using SOTI
- Intune
  - Enrolling Windows Devices to the Intune Portal
  - Managing Windows Devices Using the Intune Portal

Deploy the Marvis Windows Client Using the Intune MDM

To deploy the Marvis client using the Intune MDM:

1. Enroll the target device in Intune.
2. Add the .msi installer as a Windows LOB (Line of Business) app in the Intune portal.

3. Configure the necessary policies and include the following post-installation script:

```
MOBILE_SDK_SECRET="<ADD_YOUR_SECRET_TOKEN_HERE>" MIST_BATTERY_SAVING="<standard/low/high>"
MIST_UI_ENABLED="<false/true>"
```

   Refer to Table 29 on page 314 for details about the parameters.

   Depending on your policy type (mandatory or suggested), the Marvis client app is either directly installed or appears in the company portal as an optional app that you can install.

4. Verify the installation status on the MDM portal to confirm that the deployment is successful.

Upgrade the Marvis Windows Client in Intune

To upgrade to a newer version of the Marvis client, replace the existing .msi file with the latest version in the Intune portal. The post-installation script does not require any changes. It might take some time for the updates to reflect on the Intune portal.

Update the Marvis Windows Client Configuration in Intune

To update the Marvis client configuration parameters, you can change the registry values on the target devices and restart the system. This method enables you to update configurations without reinstallation. Make configuration script updates and registry adjustments cautiously to customize app functionality and user experience.

1. Update the Marvis client configuration values under the following registry path:

   Path: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Juniper\Marvis\Config

   Values: MOBILE_SDK_SECRET, MIST_BATTERY_SAVING

   Refer Table 29 on page 314 for details about the parameters.

   NOTE: You cannot update the MIST_UI_ENABLED parameter through the registry after the Marvis client is installed.

2. Create a registry update script. Use PowerShell to update the registry values as shown:

```powershell
Set-ItemProperty -Path "HKLM:\SOFTWARE\WOW6432Node\Juniper\Marvis\Config" -
Name "MOBILE_SDK_SECRET" -Value "<Your_New_Secret_Token>"

Set-ItemProperty -Path "HKLM:\SOFTWARE\WOW6432Node\Juniper\Marvis\Config" -
Name "MIST_BATTERY_SAVING" -Value "standard"
```

Some configuration changes might require restarting the device. If needed, include the restart command at the end of the script:

```
Restart-Service -Name "MarvisClient" -Force
```

3. Deploy the registry update script.

   Navigate to **Device Configuration** > **Scripts** to assign the script to the device group.

Uninstall the Marvis Windows Client Using the Intune MDM

To uninstall the Marvis client:

1. Revoke the application assignment in Intune. Remove the policy that enforces Marvis client installation for the target devices.
2. Create a script using the CLEAN=true parameter to remove the Marvis client completely:

```
msiexec /x marvis-installer.msi CLEAN=true /quiet /norestart
```

3. Deploy the uninstallation script. Use **Device Configuration** > **Scripts** and assign the PowerShell script to the device group.

> **NOTE**: After the uninstallation is complete, ensure to remove the devices from the **Uninstall** rule to avoid conflicts during future installations.

Deploy the Marvis Windows Client Using the SOTI MDM

To deploy the Marvis client using the SOTI MDM:

1. Ensure that the target Windows device is enrolled in SOTI MobiControl and is connected to the management console.
2. Upload the .msi installer for the Marvis client:

a. Navigate to **Add Applications** in SOTI MobiControl and select **Enterprise Apps** > **Windows**.

b. Select and upload the .msi installer for the Marvis client to the SOTI server.

3. Assign the Marvis client app to the appropriate devices or device groups within SOTI. Based on the deployment settings, the application is automatically installed or is available on demand.

4. Create a separate Script Job in SOTI with the required environment variables for configuration.

Upgrade the Marvis Windows Client in SOTI

To upgrade the Marvis client in SOTI:

1. Replace the current .msi installer for the Marvis client with the updated installer in SOTI.

2. Reassign the application.

   The policy will push the updated installer to devices according to the assignment.

Update the Marvis Windows Client Configuration in SOTI

You can apply configuration updates directly through registry edits:

1. Update the Marvis client configuration values under the following registry path:

   Path: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Juniper\Marvis\Config

   Values: MOBILE_SDK_SECRET, MIST_BATTERY_SAVING, MIST_UI_ENABLED

2. Create a registry update script. Use PowerShell to update the registry values as shown:

   PowerShell

   ```
   Set-ItemProperty -Path "HKLM:\SOFTWARE\WOW6432Node\Juniper\Marvis\Config" -
   Name "MOBILE_SDK_SECRET" -Value "<Your_New_Secret_Token>"

   Set-ItemProperty -Path "HKLM:\SOFTWARE\WOW6432Node\Juniper\Marvis\Config" -
   Name "MIST_BATTERY_SAVING" -Value "standard"
   ```

   Some configuration changes might require a system restart. If needed, include the restart command at the end of the script:

   ```
   Restart-Service -Name "MarvisClient" -Force
   ```

3. Deploy the registry update script. Use the Jobs feature to deploy this PowerShell script to the target devices.

Uninstall the Marvis Windows Client Using the SOTI MDM

To uninstall the Marvis client:

1. Revoke the application assignment in SOTI. Remove the policy that enforces Marvis client installation for the target devices.
2. Create a script using the **CLEAN=true** parameter to remove the Marvis client completely:

```
msiexec /x marvis-installer.msi CLEAN=true /quiet /norestart
```

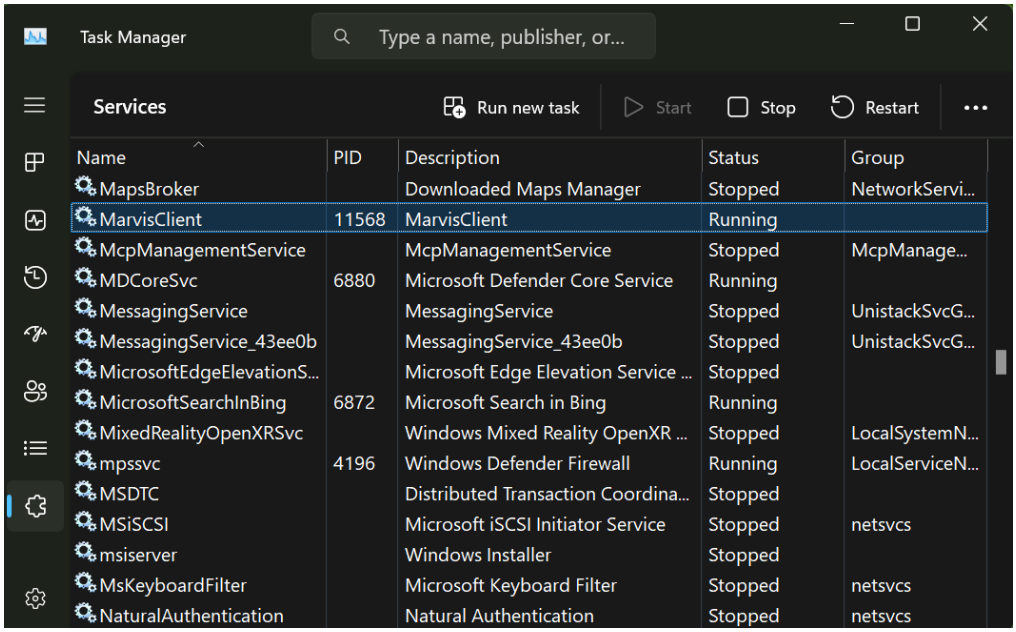
3. Deploy the uninstallation script. Use the Jobs feature to deploy this PowerShell script to the target devices.

> **NOTE**: After you've uninstalled the client, ensure to remove the devices from the **Uninstall** rule to avoid conflicts during future installations.

Verify the Marvis Client Installation for Windows

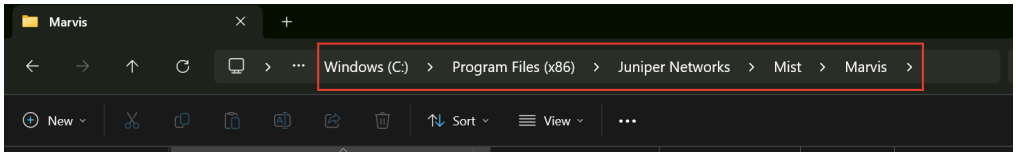
Use any of the following options to verify that the Marvis client was installed successfully:

- Verify services:
  1. Open Task Manager and navigate to the **Services** tab. Alternatively, you can use the Windows Service Manager (compmgmt.msc).
  2. Verify that the MarvisClient service is running.

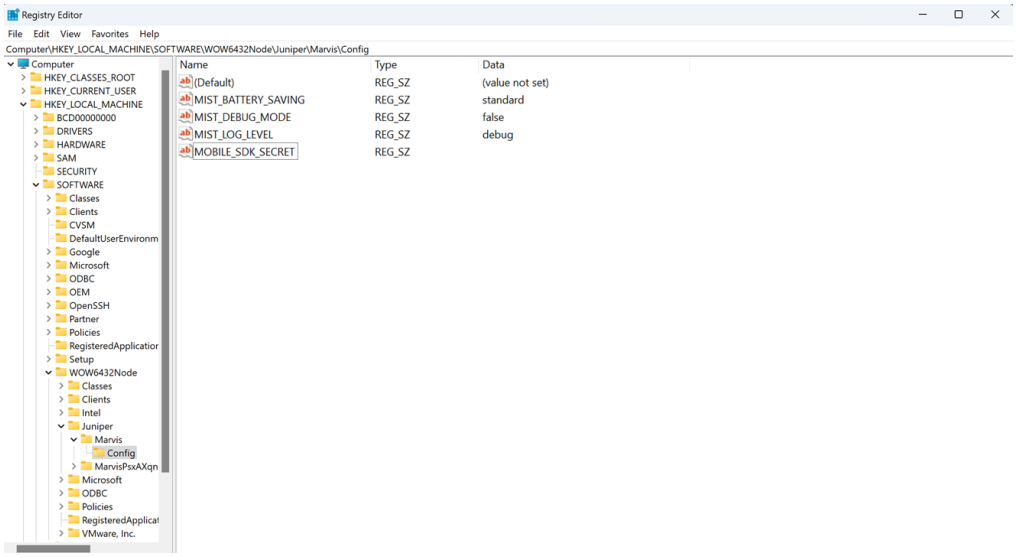


- Verify files and system registry:

1. Verify that the files are located in the **C:/Program Files(x86)/Juniper Networks/Mist/Marvis** folder.



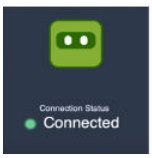
2. Navigate to the system registry and verify that the configuration variables are listed under **HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Juniper\Marvis\Config**.

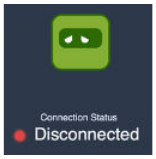


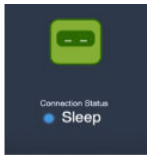
- Verify that the Marvis client icon is displayed in the startup folder **C:\ProgramData\Microsoft \Windows\Start Menu\Programs\StartUp**.

Connection States

The Marvis client status is indicated by the following visual indicators and connection states. Note that you can view these states only if the Marvis client is in Telemetry mode.







- Disconnected—Client is not connected to the Juniper Mist cloud.
- Connected—Client is connected to the Juniper Mist cloud.
- Sleep —Client is connected to the Juniper Mist cloud through a non-Juniper AP.

NOTE: On devices running Windows 11, version 24H2 and later, the Marvis client can obtain the BSSID of the wireless network only if location services are enabled. Disabling location services causes the Marvis Client to switch to the Sleeping state.

View Logs in the Marvis Windows Client

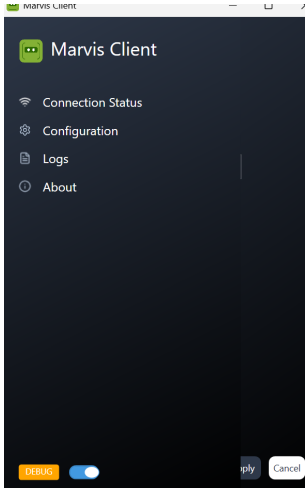
The Marvis Windows client classifies the logs as:

- Info—General information
- Error—Critical issues
- Debug—Detailed data that you can use to debug issues

To view the logs in the Marvis Windows client app, you'll need to enable debug mode on the app:

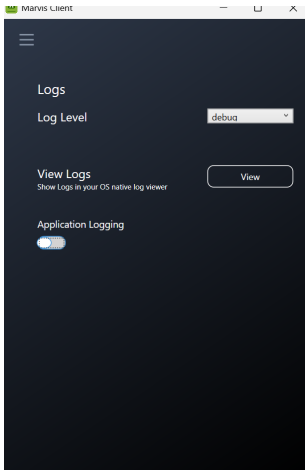
1. Click the hamburger icon, select About, and then tap the version number 7 times.

   You'll see the Logs option listed in the menu.



2. Select **Logs**. You can select the type of information you want to view by selecting an option from the **Log Level** drop-down list.

   You'll see recent logs based on the selected log level.



   You can click the **Copy** button to copy the log details and send the data to the support team for troubleshooting.

3. Click **View** to view the logs captured by the Marvis client in your OS-specific log viewer.

> **NOTE**: If you contact the Juniper Mist support team to resolve any issue, you might be asked to provide details such as the organization ID, UUID, and organization name. You can find these details listed in the About page, which you can access from the hamburger menu.
>
> The information in the About page varies based on the operational mode of the Marvis client:

- Onboarding mode—Application version and UUID, user information, organization name
- Telemetry mode—Application version and UUID, user information, organization name
- Debug mode- Application version and UUID, user information, organization name, organization ID

Uninstall the Marvis Windows Client

You uninstall the Marvis client only when you make major changes, such as name changes or file path location changes. Minor updates or change in organization do not require that you uninstall the Marvis client.

To uninstall the Marvis client:

1. Navigate to **Settings** > **Apps** on your device.
2. Search for **MarvisClient** from the list of applications.
3. Click **...** and select **Uninstall**.

The Marvis client will be uninstalled from your device.

NOTE: Uninstalling the client might not remove all log files and folders. You can choose to delete the files manually if required. To completely remove Marvis client along with all the logs and configuration files, use the following command:

```
msiexec.exe /x marvisclient-installer.msi /quiet /L*v uninstall.log CLEAN=true"`
```

Marvis macOS Client

SUMMARY

Complete the preinstallation tasks, and then choose the method that you want to use to install the Marvis client on your macOS device.

IN THIS SECTION

The Marvis client for macOS provides detailed visibility into how your macOS device interacts with the wireless network. With insights into device connectivity and performance, the Marvis client helps optimize network performance, streamline troubleshooting, and enhance overall user experience.

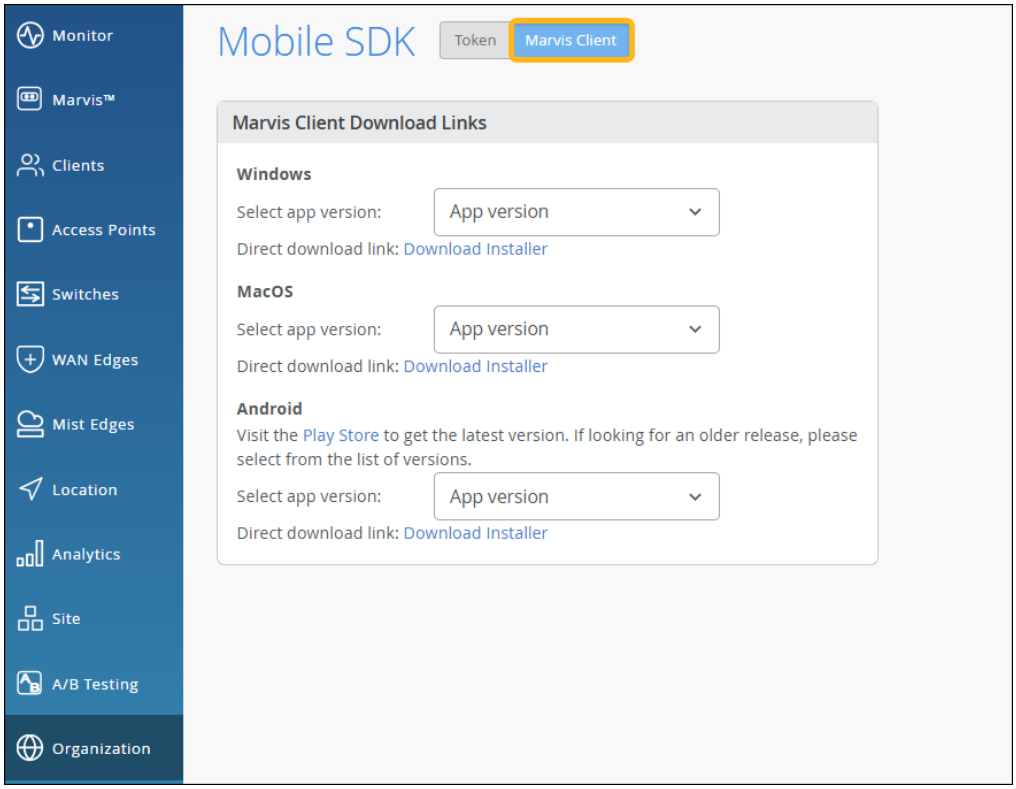
Marvis macOS Client Installation Overview

IN THIS SECTION

You can download the installer file from the Juniper Mist portal. To download the installer file from the Juniper Mist portal:

1. Select **Organization** > **Admin** > **Mobile SDK** from the left menu.
2. Click **Marvis Client** at the top of the Mobile SDK page.
3. Under MacOS, select the app version, and then click **Download Installer**.

   You'll need to save the *.dmg installer file in a folder on your device.



Prerequisites

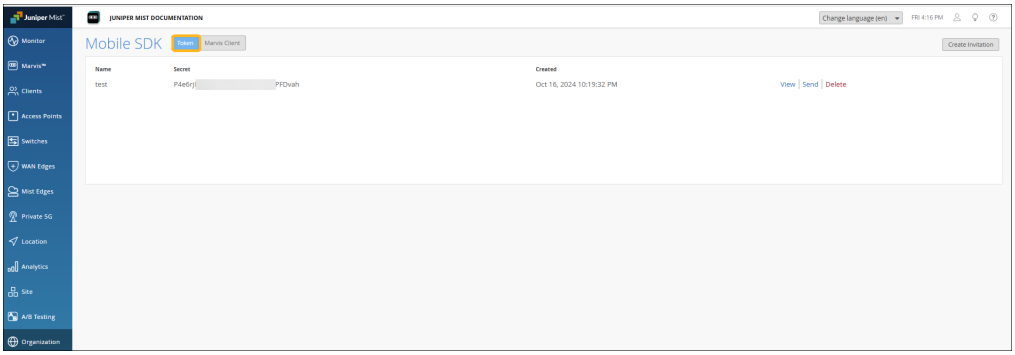
Before you begin, you'll need:

- The secret token to onboard your Marvis client

  To obtain the secret code:

  1. Select **Organization** > **Admin** > **Mobile SDK** from the left menu on the Juniper Mist portal.
  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.



NOTE: To obtain the secret token using API, see https://api.mist.com/api/v1/docs/Org#sdk-invite.

- macOS 14.6 or a later release running on your device
- Administrator rights required for installation

Installation Options for the Marvis Client (macOS)

You can install the Marvis client for macOS by using any of the following methods:

- "Install the Marvis Client for macOS (CLI Method)" on page 328
- "Install the Marvis Client for macOS (GUI Method)" on page 329
- "Deploy the Marvis Client on macOS Devices Using an MDM" on page 332

Operational Modes

The Marvis client operates in the following modes:

- Onboarding mode—Default mode. See "Configure Marvis Client for Onboarding" on page 331.
- Telemetry mode—Standard operational mode for live environments that you can set using command-line parameters during installation. See "Configure Marvis Client to Operate in Telemetry Mode" on page 331.

Install the Marvis Client for macOS (CLI Method)

When you install the Marvis macOS client using the CLI method, the Marvis client is installed in Telemetry mode. To install the Marvis client for macOS using the CLI:

1. Extract the .pkg file from the .dmg file.
2. Press the **Command** + **Space** keys to open the Spotlight search window.
3. Type **Terminal**. The Terminal app is displayed in the search results.
4. Double-click the Terminal app.
5. Execute the following command:

   ```
   sudo installer -pkg <path_to_pkg> -target / && marvis-cli start --token-value <token> [--auto-upgrade-allowed <true|false> ] [--ui-mode-enabled <true|false>] [--force]
   ```

   Set the values for the following parameters:

   Mandatory parameter:

   - `token-value`—Provide the secret token.

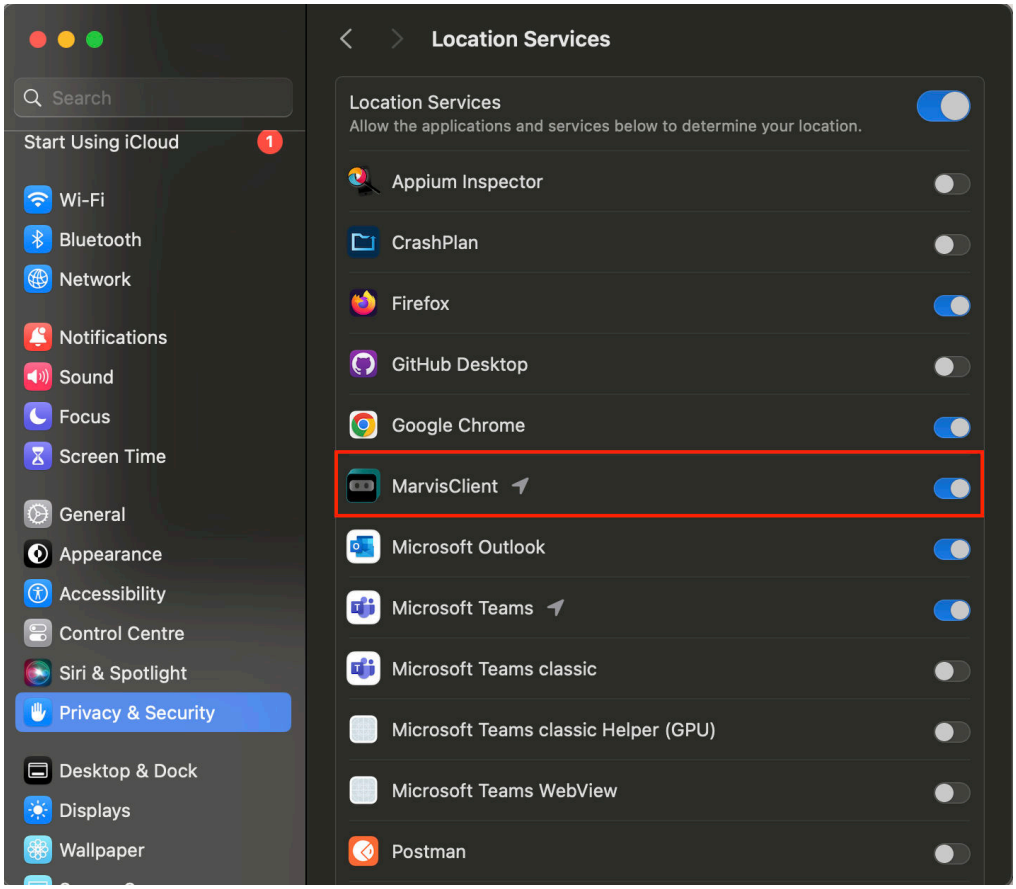
   Optional parameters:

   - `--ui-mode-enabled <true|false> or -ui <true|false>`—Enable or disable UI mode. By default, the UI mode is enabled.
   - `--auto-upgrade-allowed <true|false`—Enable or disable automatic upgrades. By default, this option is disabled.
   - `--force or -f`—Force restart irrespective of the current configuration
6. Enter the administrator password when prompted.
7. Verify that the installation is successful. See "Verify the Installation" on page 334.
   After the installation is completed successfully, the Marvis client app opens. You can also see the Marvis client icon listed in the status bar. You will be prompted to enable Location Services for the Marvis client. Note that Location Services in this context refer to the device-level location settings available on macOS. Client real-time location services are not supported on macOS devices.
8. Select **Allow**. Location permission is needed for the Marvis client to collect Wi-Fi telemetry from the client device.

   If Location Services is not enabled automatically after you install the Marvis Client, follow these steps:

   a. Navigate to **System Settings** > **Privacy** > **Location Services**.

   b. Enable location services for the Marvis Client.



Install the Marvis Client for macOS (GUI Method)

When you install the Marvis macOS client using the GUI method, the Marvis client is installed in the Onboarding mode. To install the Marvis client for macOS:

1. Double-click the .dmg file and then double-click the .pkg file to start the installation process.
2. Click **Continue**.
3. Click **Agree** to accept the license agreement.
4. Click **Install**.

   The Marvis client is installed in the Onboarding mode. If you want to switch to Telemetry mode, proceed with the following steps.
5. Press the **Command** + **Space** keys to open the Spotlight search window.
6. Type **Terminal**.
   The Terminal app is displayed in the search results.
7. Double-click the Terminal app.

8. Execute the following command:

```
marvis-cli start --token-value <token> [--auto-upgrade-allowed <true|false> ] [--ui-mode-enabled <true|false>] [--force] [--yes]
```

Set the values for the following parameters:

Mandatory parameter:

- `token-value`—Provide the secret token.

Optional parameters:

- `--ui-mode-enabled <true|false> or -ui <true|false>`—Enable or disable UI mode. By default, the UI mode is enabled.
- `--auto-upgrade-allowed <true|false`—Enable or disable automatic upgrades. By default, this option is disabled.
- `--force or -f`—Force restart irrespective of the current configuration
- `--yes` or `-y`—Skip the confirmation prompt for a forced restart. This is useful during silent or MDM installation.

9. Verify that the installation is successful. See "Verify the Installation" on page 334.

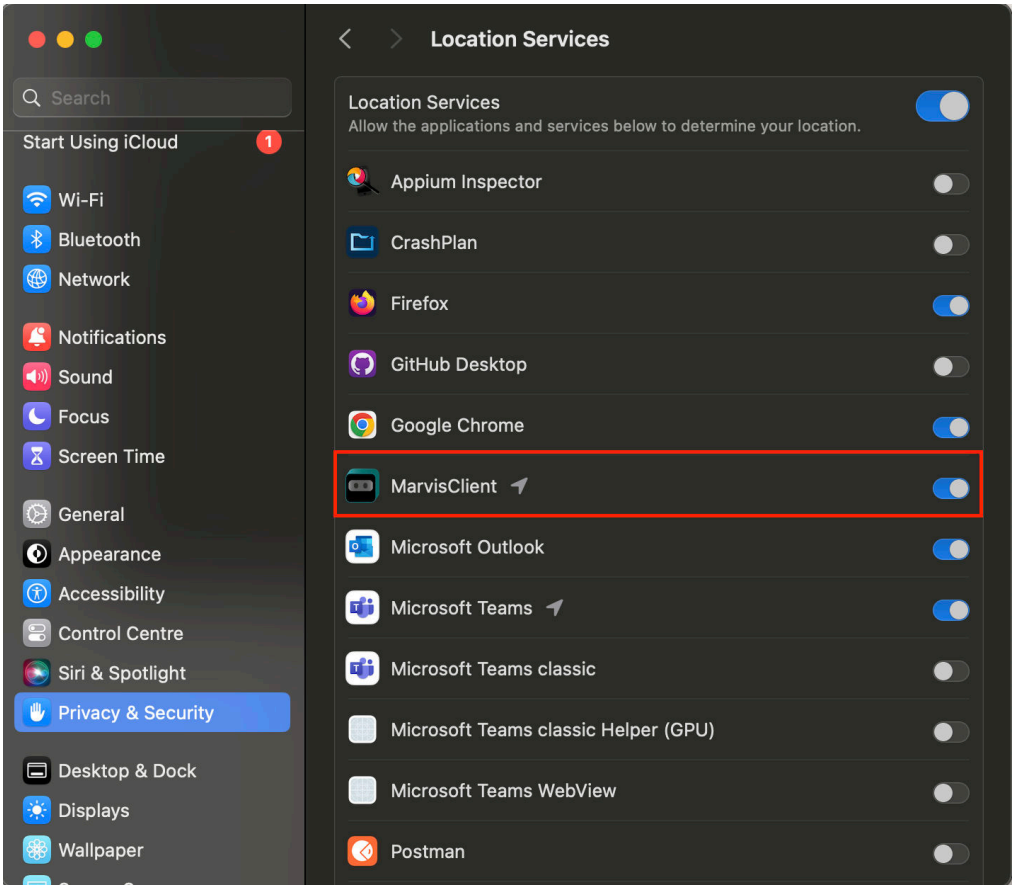
After the installation is completed successfully, the Marvis client app opens. You can also see the Marvis client icon listed in the status bar. You will be prompted to enable Location Services for the Marvis client.

10. Select **Allow**. Location services must be enabled for the Marvis client to function correctly.

If Location Services is not enabled automatically after you install the Marvis Client, follow these steps:

a. Navigate to **System Settings** > **Privacy** > **Location Services**.

b. Enable location services for the Marvis Client.



Configure Marvis Client for Onboarding

You can use the Marvis Client app to onboard devices to the Juniper Mist Access Assurance network through a custom Network Access Control (NAC) portal. For more information, see Client Onboarding Through a NAC Portal Using the Marvis Client App.

Configure Marvis Client to Operate in Telemetry Mode

The Marvis client is configured to operate in Onboarding mode by default. To enable the Marvis client to operate in Telemetry mode, use the following command:

```
marvis-cli --token-value <token>
```

Deploy the Marvis Client on macOS Devices Using an MDM

IN THIS SECTION

You can deploy the Marvis client on macOS devices by using the SOTI, Intune, or Jamf mobile device management (MDM) solution. You can refer to the following topics for information about enrolling and managing devices using MDMs:

- SOTI
  - Enrolling macOS Devices Using a SOTI MobiControl Certificate
  - Enrolling macOS Devices Using a Third-Party Certificate
  - Installing an App Using SOTI
- Intune
  - Enrolling macOS Devices to the Intune Portal
  - Managing macOS Devices Using the Intune Portal
- Jamf
  - Enrolling macOS Devices Using JAMF
  - Deploying an App using Jamf

To deploy the Marvis client:

1. Enroll the target devices or device groups with the appropriate MDM profile.
2. Configure the necessary profiles or application policies within your MDM portal.
3. Upload the Marvis client .pkg installer file to your MDM portal and assign the file to the target devices or device groups.

4. After the installation is complete, send a configuration script to the devices through the MDM portal:

```
#!/bin/bash
/usr/local/bin/marvis-cli --token-value <token> [options]
```

Upgrade the Marvis Client for macOS Using MDM

To upgrade to a newer version of the Marvis client, upload the updated .pkg file to the MDM portal and reassign the application policies to the target devices or device groups. You need not resend the configuration script.

Update the Marvis Client Configuration for macOS Using MDM

To update the Marvis client configuration parameters, resend the configuration script with the updated parameters:

```
#!/bin/bash
/usr/local/bin/ marvis-cli start --token-value <token> [--auto-upgrade-allowed <true|false> ] [--
ui-mode-enabled <true|false>] [--force]
```

Uninstall Marvis Client for macOS Using an MDM

To uninstall the Marvis using an MDM:

1. Remove the application policy assignment if it enforces mandatory app installation.
2. Send the uninstallation script to the devices:

```
#!/bin/bash
 /usr/local/bin/marvis-cli uninstall
```

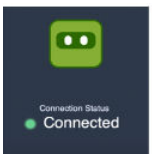
You might still see the app as **Installed** on some MDM portals. After you remove the policy, wait for a while, and then check the app status.

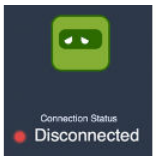
NOTE: The uninstall process might not remove all log files and folders. You can choose to delete the files manually if required. To completely remove Marvis client along with all the logs and configuration files, use the following command:

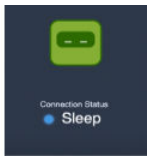
```
#!/bin/bash
/usr/local/bin/marvis-cli uninstall --clean
```

Connection States

The Marvis client status is indicated by the following visual indicators and connection states. Note that you can view thesestates only if the Marvis client is in Telemetry mode.





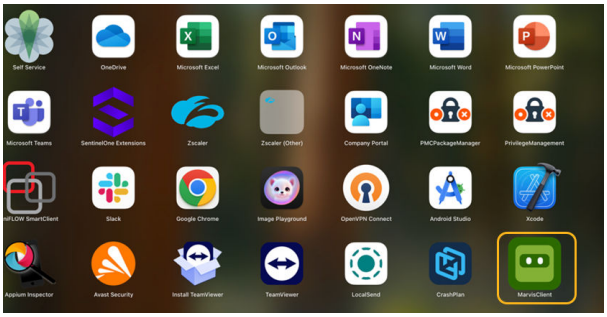


- Disconnected—Client is not connected to the Juniper Mist cloud.
- Connected—Client is connected to the Juniper Mist cloud.
- Sleep —Client is connected to the Juniper Mist cloud through a non-Juniper AP.

Verify the Installation

Use any of the following options to verify that the Marvis client was installed successfully:

- Verify that the Marvis client is present in your Applications directory.

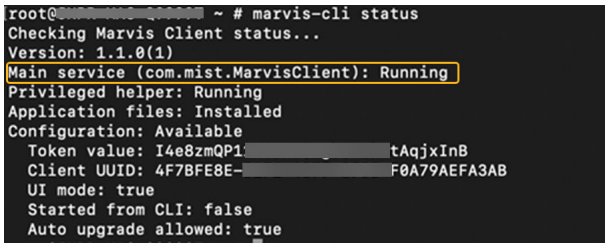


- Verify the background services:

1. Open the Terminal app and execute the following command:

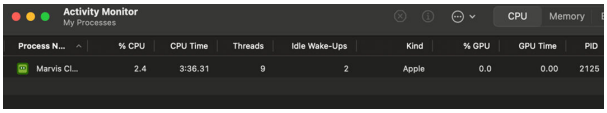
```
sudo -i

marvis-cli status
```

2. Provide your administrator password when prompted.
3. Verify that a service entry is present.



- Verify that Marvis Client is listed in the Services tab in Activity Monitor.

  If you do not see Marvis Client listed, reinstall the Marvis client. If that does not resolve the issue, contact the support team.



After the installation, you'll see the Marvis icon in your system tray or menu bar. You can click the icon to open the Marvis client and view the connection status.

Manage Services

Here are the commands that you can use to manage the following main Marvis client system services:

- Main Service: com.mist.MarvisClient
- Privileged Helper: com.mist.MarvisClient.MarvisPrivilegedHelper
- Start services:

```
marvis-cli start --token-value <token> [options]
```

- Restart services:

```
marvis-cli restart
```

- Logs services:

```
marvis-cli logs
```

- Version services:

```
marvis-cli --version
```

View Logs in the Marvis macOS Client

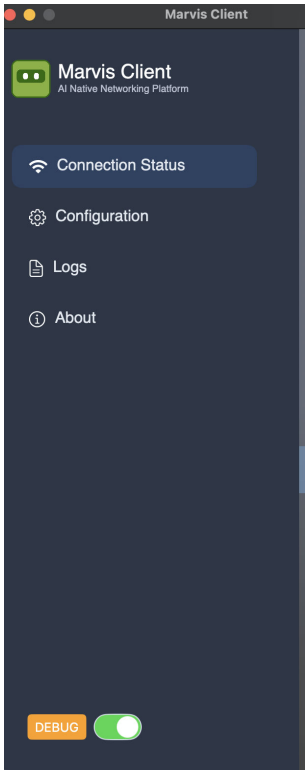
The Marvis macOS client classifies the logs as:

- Info—General information
- Error—Critical issues
- Debug—Detailed data that you can use to debug issues

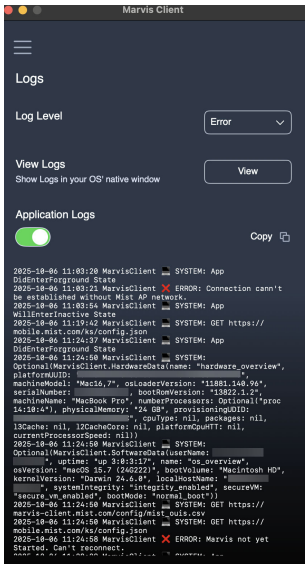
To view the logs in the Marvis macOS client, you'll need to enable debug mode:

1. Click the hamburger icon, select About, and then tap the version number 7 times.

   You'll see the Logs option listed in the menu.



2. Select **Logs**. Select the log category from the **Log Level** drop-down list.
   You'll see recent logs based on the selected log level. You can click the **Copy** button to copy the log details and send the information to the support team for troubleshooting.



3. Click **View** to see the logs captured by the Marvis client in your OS native window.

NOTE: If you contact the Juniper Mist support team to resolve any issue, you might be asked to provide details such as the organization ID, UUID, and organization name. You can find these details listed in the **About** page, which you can access from the hamburger menu.

The information in the **About** page varies based on the operational mode:

- Onboarding mode—Application version and UUID, user information, organization name
- Telemetry mode—Application version and UUID, user information, organization name
- Debug mode- Application version and UUID, user information, organization name, organization ID

Uninstall the Marvis macOS Client

IN THIS SECTION

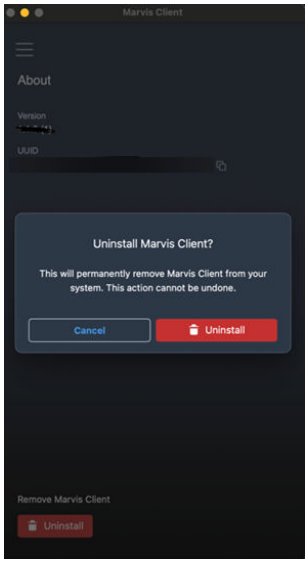
You can uninstall the Marvis macOS client by using the Finder (GUI) or the CLI. The CLI method offers a clean uninstall option to remove residual files and configurations.

Uninstall the Marvis macOS Client (GUI)

The GUI method provides a user-friendly way to uninstall the Marvis client.

1. Open the **Marvis Client** application.
2. Navigate to the **About** page.
3. Tap **Uninstall** to uninstall the Marvis client.

NOTE: The **Uninstall** option is available in Marvis macOS client version 1.1.0 and later.



Uninstall the Marvis macOS Client Using the CLI

The CLI method provides flexibility for advanced users with the provision of both standard and clean uninstallation of the Marvis client. You'll need administrative privileges for this procedure. Enter your admin password when prompted.

Standard Uninstall

To remove the application only (without configuration files):

1. Open **Terminal**.
2. Run the following command:
   - For standard uninstall:

```
sudo -i
marvis-cli uninstall
```

- For clean uninstall:

```
sudo -i
marvis-cli uninstall --clean
```

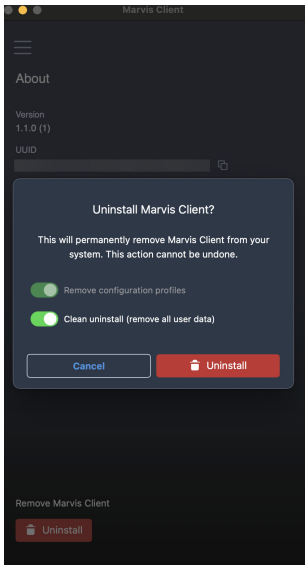
Clean Uninstall

To completely remove the Marvis client, including all residual files and configurations:

1. Enable Debug mode by tapping the version number 7 times on the About page.
2. Tap **Uninstall**.

> **NOTE**: The **Uninstall** option is available in Marvis macOS client version 1.1.0 and later.

3. Enable both these options and tap **Uninstall** to proceed.
   - **Remove Configuration Profile**
   - **Clean Uninstall**



Marvis iOS Client

SUMMARY

Understand how you can set up the Marvis client on your iOS device.

IN THIS SECTION

The Marvis client for iOS is a secure, lightweight mobile app that helps simplify and secure the process of connecting iOS devices to enterprise networks. With Juniper Mist Access Assurance, Marvis client facilitates zero-touch onboarding through certificate-based authentication, eliminating the need for passwords. The Marvis client allows employees, guests, and contractors to access the organization's wireless network securely and with ease.

Key features of the Marvis client for iOS include:

- Certificate-based authentication (no passwords required)
- Automatic installation of wireless profiles and certificates
- One-tap provisioning
- Auto-renewal of credentials before expiry
- Support for BYOD, guest, and corporate devices
- AI-driven visibility and troubleshooting through the Juniper Mist portal

Requirements

- Device running iOS 12.0 or later
- Juniper Mist Access Assurance subscription
- A valid provisioning link from your organization

Privacy and Security

Juniper Mist adheres to the following guidelines:

- Marvis client installs the wireless and certificate profiles only after authentication.
- Juniper Mist does not share personal data with third parties.
- Device identity is managed securely within the Juniper Mist cloud.

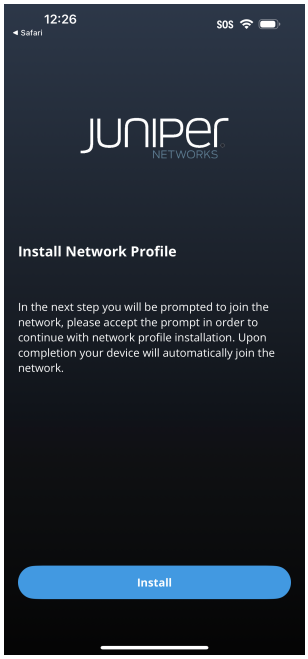
Marvis iOS Client Setup Overview

The Marvis iOS client setup involves a simple process:

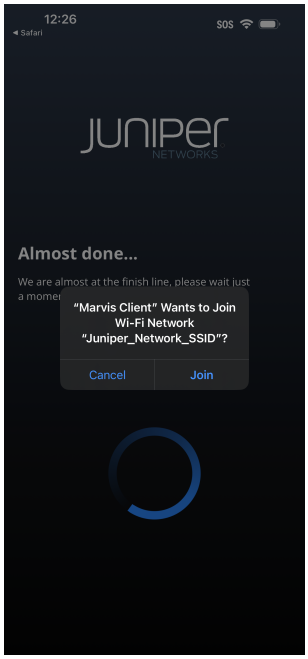
1. Install the Marvis iOS client app from App Store on your device.
2. Click the onboarding link that you received from your organization through an e-mail, a QR code, or an onboarding portal.
3. Authenticate using your organization credentials through SSO such as Okta.

   The Marvis client app is launched.
4. Click **Install** to install the network and Wi-Fi profiles.

   The onboarding process starts automatically. A secure certificate is issued and the wireless profile is installed on your device.



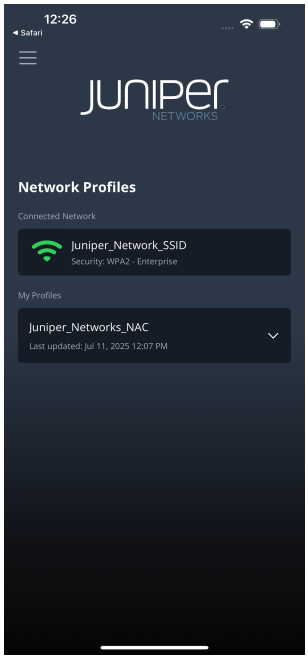
5. Click **Join** when prompted.



Your device connects to the Wi-Fi network and uses certificate-based access for seamless and secure connectivity.

You might see an error message stating that the SSID or Wi-Fi is not available. This might occur if the SSID is not within the range. You can try to reconnect when the SSID is within the range.

You'll see the Network Profiles page once the device is onboarded.



If the device onboarding fails or if you're unable to connect to the network, contact your support team.

For more information about Mist Access Assurance and Marvis Client, see https://www.juniper.net/us/en/products/cloud-services/marvis-ai-assistant/marvis-client.html

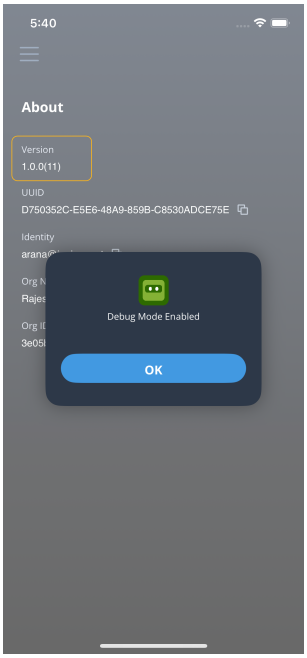
View Logs in the Marvis iOS Client

The Marvis iOS client classifies the logs as:

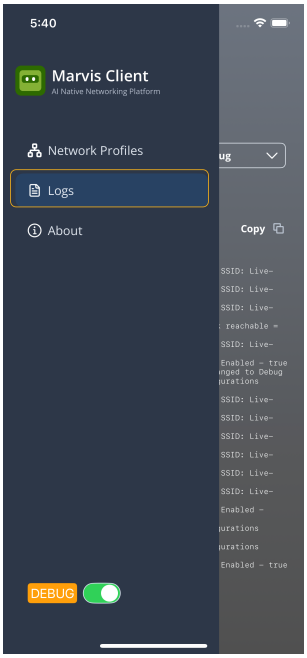
- Info—General information
- Error—Critical issues
- Debug—Detailed data that you can use to debug issues

To view the logs in the Marvis macOS client, you'll need to enable debug mode:

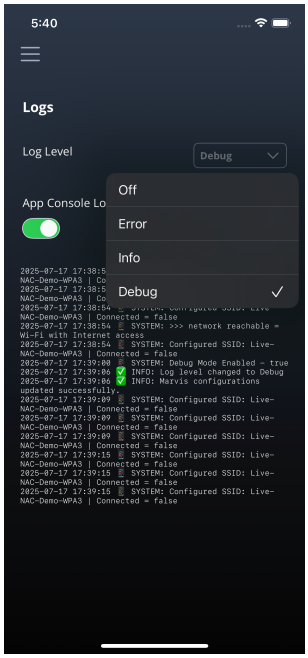
1. Tap the version number in the **About** page 7 times to enable debug mode.



You'll see the Logs option listed in the menu after the debug mode is enabled.



2. Select **Logs**. Select the log category from the **Log Level** drop-down list.



You'll see recent logs based on the selected log level. You can click the **Copy** button to copy the log details and send the information to the support team for troubleshooting.

3. Click **View** to see the logs captured by the Marvis client in your OS native window.

> **NOTE**: If you contact the Juniper Mist support team to resolve any issue, you might be asked to provide details such as the version, UUID, and organization name. You can find these details listed in the **About** page, which you can access from the hamburger menu.

Enable NAC Client Onboarding Through the Marvis Client

SUMMARY

Onboard your device to the Juniper Mist Access Assurance network securely through the Marvis client app.

You can onboard devices to the Juniper Mist Access Assurance network through a custom Network Access Control (NAC) portal, using the Marvis Client app. Users can automatically provision their devices with the appropriate Wi-Fi profile and personal certificate after a successful SSO authentication to the NAC portal. Device onboarding through the NAC portal using Marvis Client ensures a secure, seamless, and password-less access to your organization's Wi-Fi network.

After you configure the NAC portal and associate it with your SAML SSO, users can access the portal through a designated URL to initiate the onboarding process. If the Marvis Client app is not already installed on the client device, you will need to manually download and install it using the download link on the NAC portal. The NAC portal then facilitates the installation of the appropriate network profile with the client certificate through the Marvis client app on the device.

You can onboard the following types of devices:

- Windows
- macOS
- iOS
- Android

You'll need an active Access Assurance Advanced subscription to onboard devices using a NAC portal.

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.

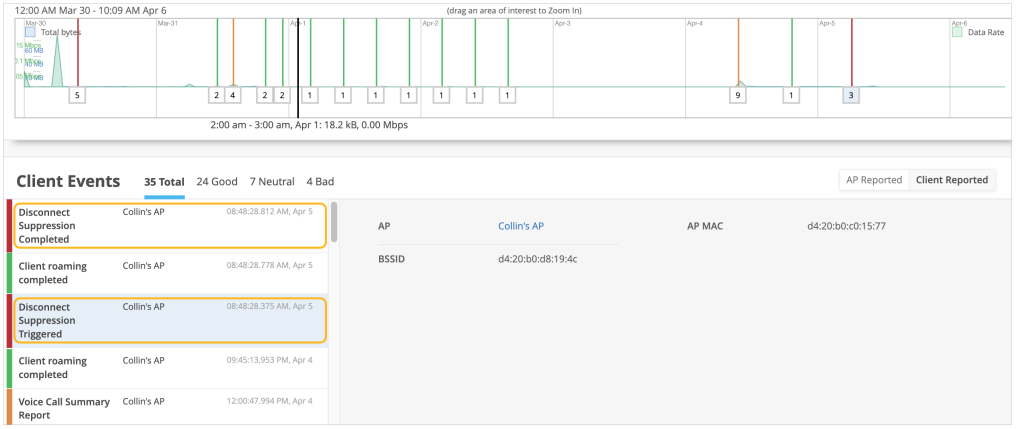
NOTE: To view client events from your Zebra device, the device must have a valid Wireless Insights license and the Marvis Android Client (V33.x or later) installed.

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.

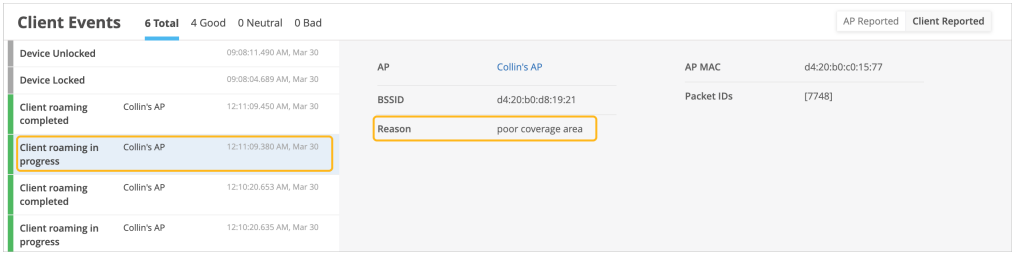
Here is a sample event and the condition that triggered the event:

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).



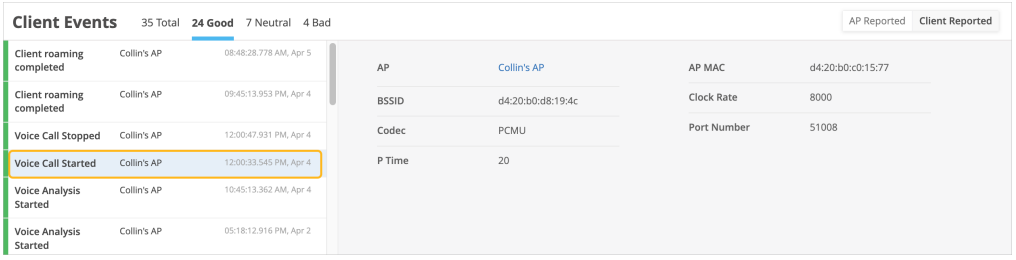
Roaming Events

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.

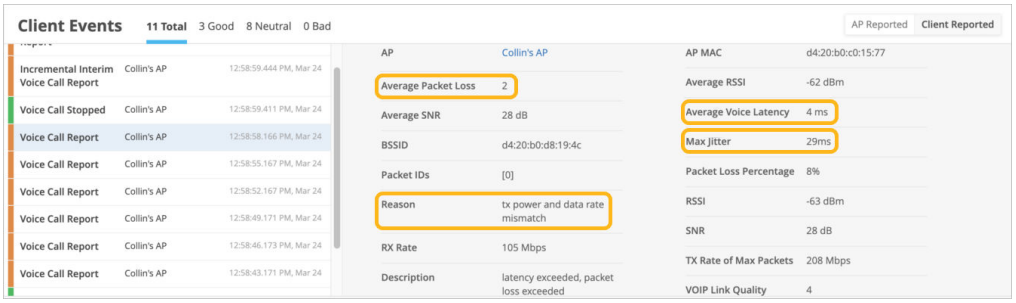


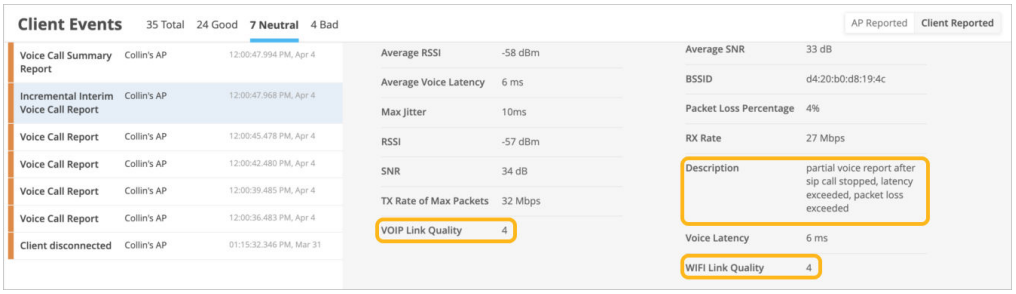
Voice Events

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.



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.





Marvis Client FAQ

SUMMARY

Get answers to common questions about subscription requirements, status messages, logs, and troubleshooting for the Marvis Client.

IN THIS SECTION

What should I do if I do not have a secret token?

You can request for a secret token from your network administrator through the Juniper Mist portal.

Which subscription do I need to purchase to use Marvis client?

You'll need a Marvis Client (S-VNACLIENT) subscription per client.

Why should I disable random MAC address for my Android device?

Disabling the random MAC address enables the Marvis client app to maintain a single MAC address for a device and associate all the device data with that MAC address.

Why does the connection status show as Disconnected on my Marvis client app?

When you download and install the app for the first time, the connection status shows as Disconnected. After you configure the secret key, enable the required permissions, and connect the device to the Mist SSID, the connection status changes to Connected.

Why does the connection status show as Sleeping on the Marvis client app?

Your device might be on a non-Mist AP network. If you are connected to the Juniper Mist network and if the Marvis client still shows the status as Sleeping, contact Juniper Mist support.

Why does the Marvis client app request for location permission even though I set the Location Visibility as OFF?

It is mandatory to set the location permission as **Allow all the time** for the app to function. According to the Android OS requirements, an app needs this permission to access the Wi-Fi information.

Why doesn't any data appear on the Marvis tab (Clients > WiFi Clients > Marvis tab) even though the app connection status shows as Connected?

This could happen due to one of the following reasons:

- If you installed the Marvis client app for the first time, the Juniper Mist cloud might take up to 15 minutes to appear on the Marvis page.
- Your device is not connected to the Juniper Mist access point (AP) network.
- You have not enabled the required location permission.
- Your device is not enrolled in the correct organization.

Why do I see only device locked and unlocked events in the client reported events? How can I obtain additional data on client events?

Juniper Mist displays additional client events such as client roams, sticky clients, good roams, bad roams, and optimal and sub-optimal roams when:

- The site has sufficient APs (at least three).
- The device is always connected to the Mist SSID.

If the device moves across the site (within the Juniper Mist network), the app can collect adequate data for client roam events.

Why do client events not display voice call events data for Zebra devices?

Voice call might not be supported on your Zebra device. Zebra voice call is supported only on specific device models and OS versions. For more information, see https://www.zebra.com/us/en/support-downloads/software/mobile-computer-software/wireless-insights.html#Ta-item-014a3a6ca9-tab.

What is the battery consumption of the Marvis client app?

The battery consumption is ~2% to 3% per hour. Note that this value can vary based on the device model, device OS version, other apps running on the device, or device settings.

How do I switch from POC mode to Production mode?

Reinstall the Marvis client using the appropriate command line parameters to set the mode.

Where are the logs stored?

Logs are stored in a location specific to your OS and configuration. You can access the logs in the following locations:

- **C:\Windows\Temp\Marvis** on Windows devices

- **/Users/Shared/MarvisClient/Data/Documents** on macOS devices

Are there any additional requirements to run the Marvis client on Windows?

Unlike on Android, apps don't require specific permissions on Windows. However, you must ensure that you've exposed the physical MAC address of your Wi-Fi adapter. Ensure that you have the necessary administrator rights for installation and that your system meets the prerequisites, such as having the .NET Framework installed. For security settings, make sure that the Marvis client is configured according to your organization's policies.

I do not see my device listed on the Clients > WiFi Clients > Marvis page. What should I do?

You'll need to perform the following checks:

1. Verify that your device is connected to a Juniper Mist AP. Ensure that the AP is enrolled to the same organization with which the SDK secret is associated.
2. Ensure that you have enabled location and BLE permissions (applicable only for Android devices).
3. Check your firewall settings. Ensure to configure your firewall to allow traffic to/from the client to the Juniper Mist cloud. See https://www.juniper.net/documentation/us/en/software/mist/mist-management/topics/ref/firewall-ports-to-open.html.
4. Check if you have any cloud security tools (such as Zscaler or Netskope) that prevent the client from connecting to the Juniper Mist cloud.
5. Check the platform-specific app logs for any errors.

My Marvis client seems to be stuck, and I can't use it. I might need an app reset. How can I fix this issue?

To fix this issue, completely uninstall and reinstall the application. Marvis client for macOS and Windows supports clean uninstall (with additional parameters).

For uninstallation instructions for Windows, see

- "Uninstall the Marvis Windows Client" on page 324
- "Uninstall the Marvis Windows Client Using the SOTI MDM" on page 320
- "Uninstall the Marvis Windows Client Using the Intune MDM" on page 318

For uninstallation instructions for macOS, see

- "Uninstall Marvis Client for macOS Using an MDM" on page 333

My Marvis client shows the status as Connecting or the connection request shows timed out. What should I do?

Make sure you have added the client-terminator URL for your cloud environment to the allowlist on your network firewall settings. See Juniper Mist Firewall Ports and IP Addresses for Firewall Configuration.

CHAPTER 11

Marvis App for Teams

IN THIS CHAPTER

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

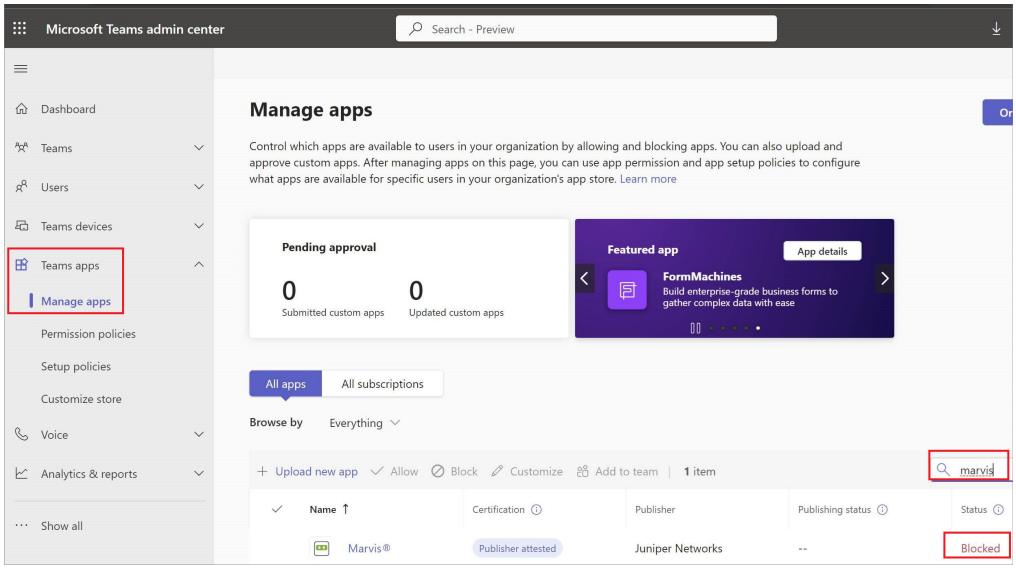
Go through these steps to enable the Marvis app, add the permission policy, and assign the permission to the users.

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**.



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.

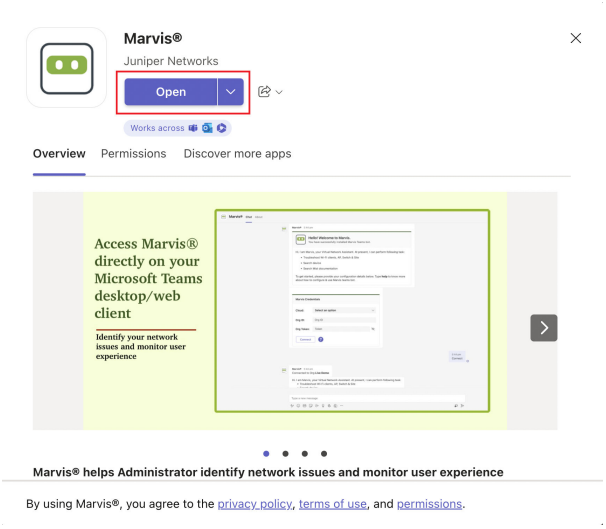
IN THIS SECTION

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 357.

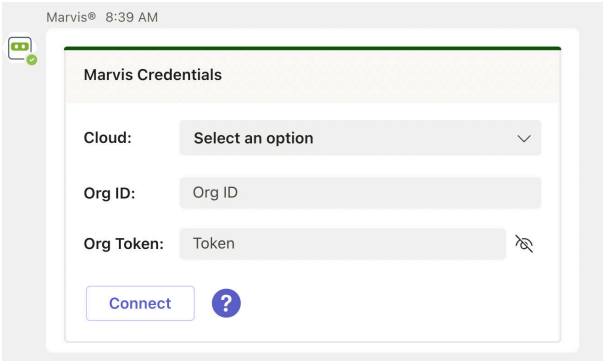
Install the Marvis App in Teams

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**.



You'll see the following window, which indicates that you have successfully installed the app:

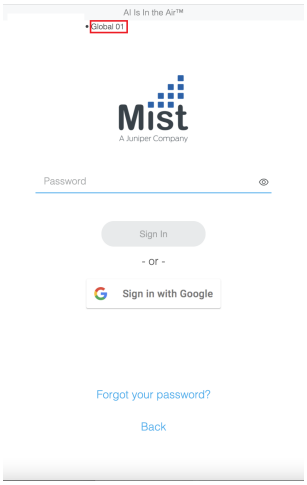


4. Next, you'll need to connect to your organization in the Mist portal.

Connect to Your Mist Organization

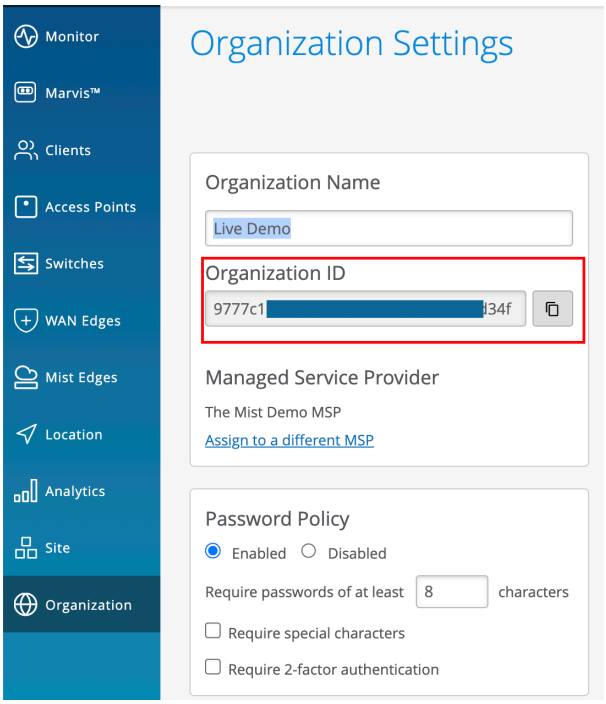
To connect to your Mist organization:

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.



- Organization ID (Org ID)

  You can find your Org ID on the **Organization > Settings** page in the Mist portal.



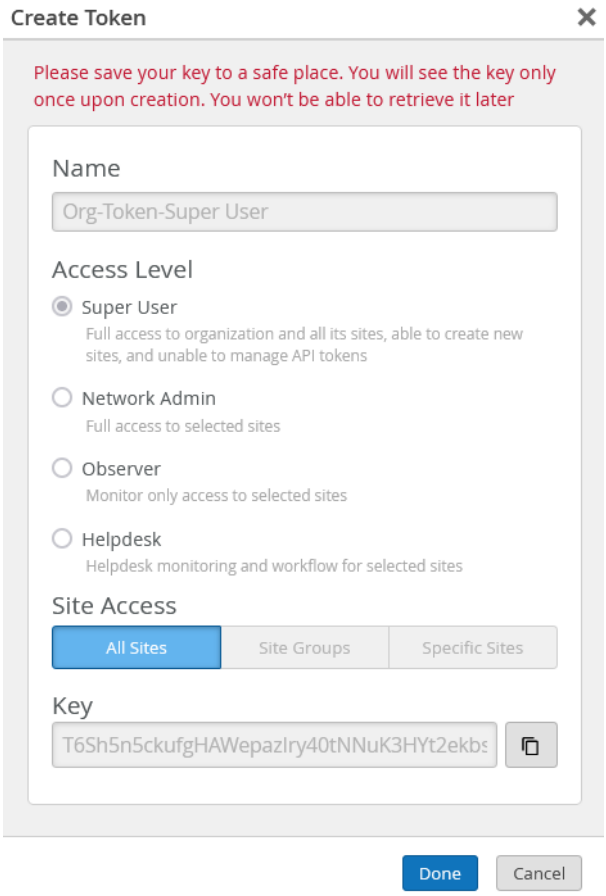
- Org Token

  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.

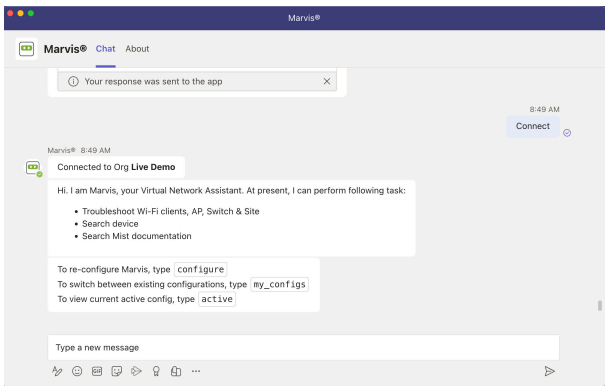
  To create a token:

  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.



2. Click **Connect**. A successful connection displays the following window:



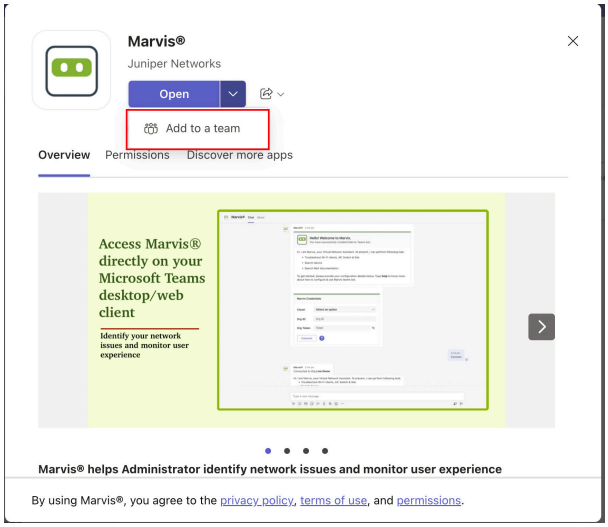
Add the Marvis App to a Microsoft Teams Channel

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.

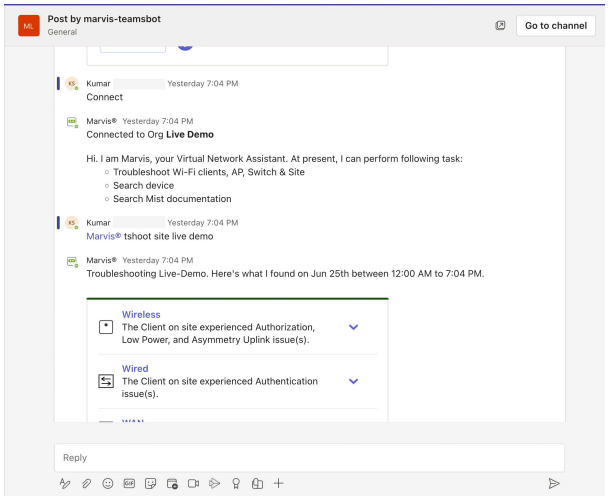
Before you add Marvis to a Teams channel, you must install the app in Teams and connect the app to the organization, as described in the previous sections.

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**.



4. Select the Teams channel.
   That's it! You and your team members can start asking Marvis questions.



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.

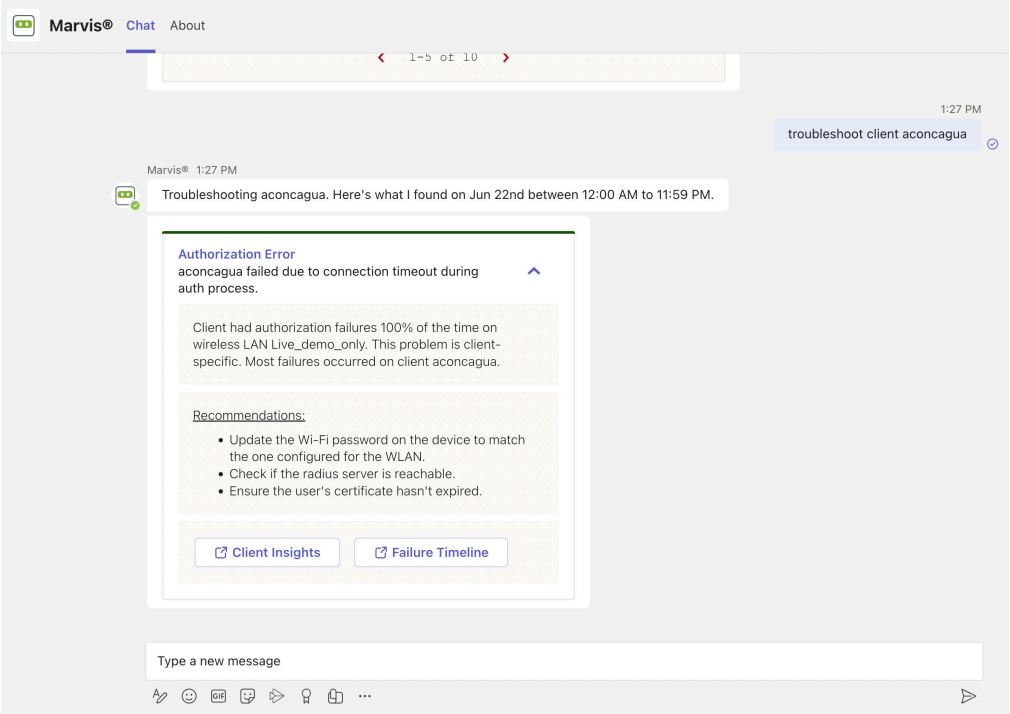
IN THIS SECTION

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.



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:

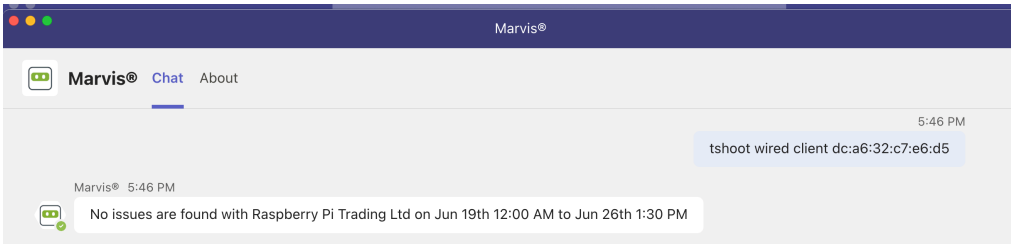
- how was <client name> on June 22nd
- tshoot client <mac or name> on June 21

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>".

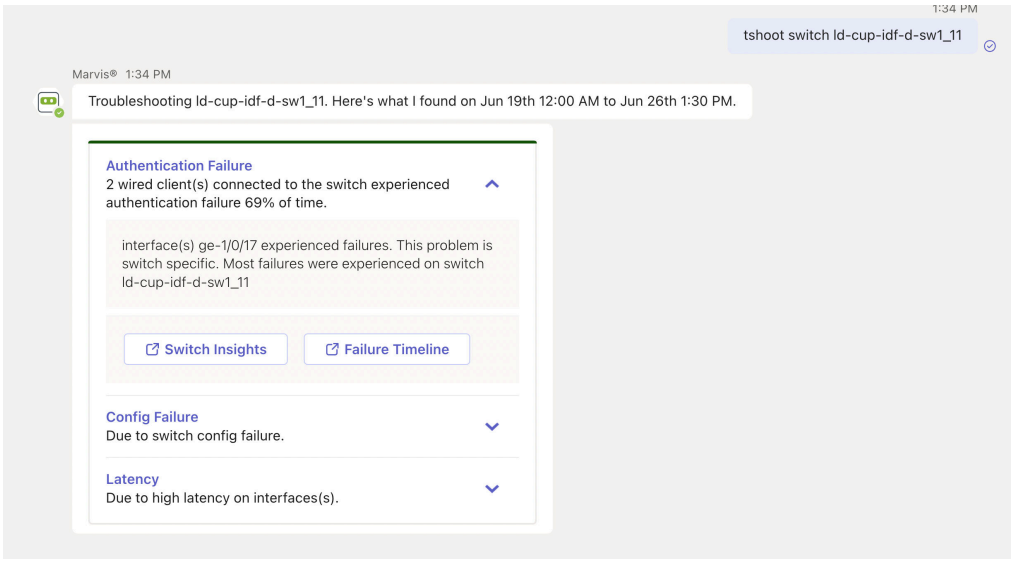


Troubleshoot a Device

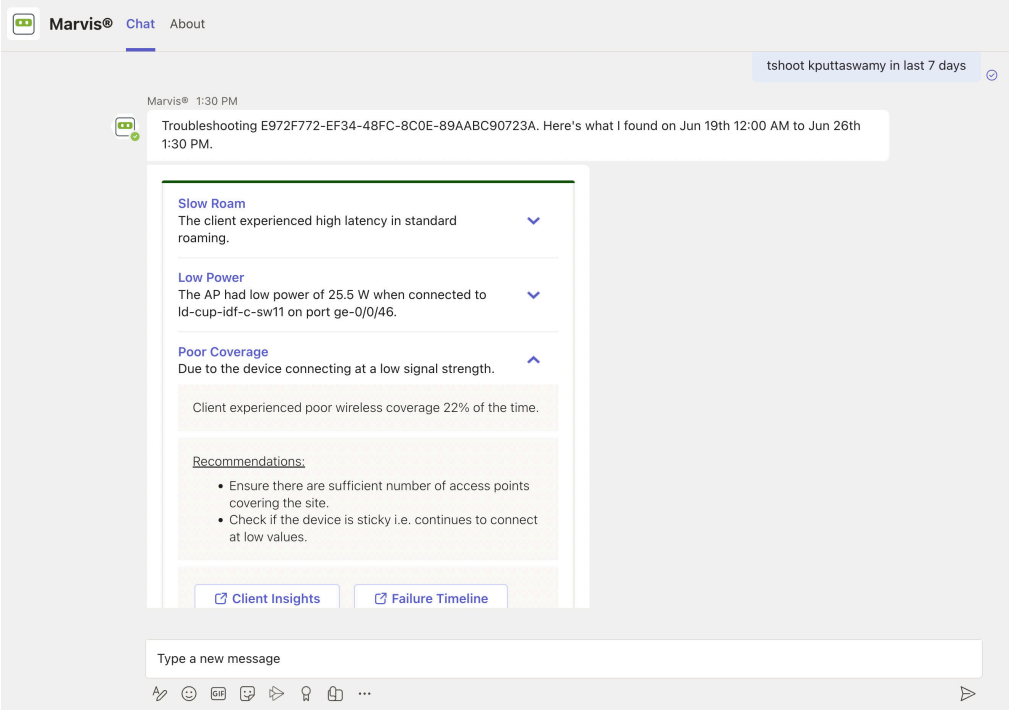
You can use the Marvis app to check for issues on APs, switches, or WAN edge devices.

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.



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:

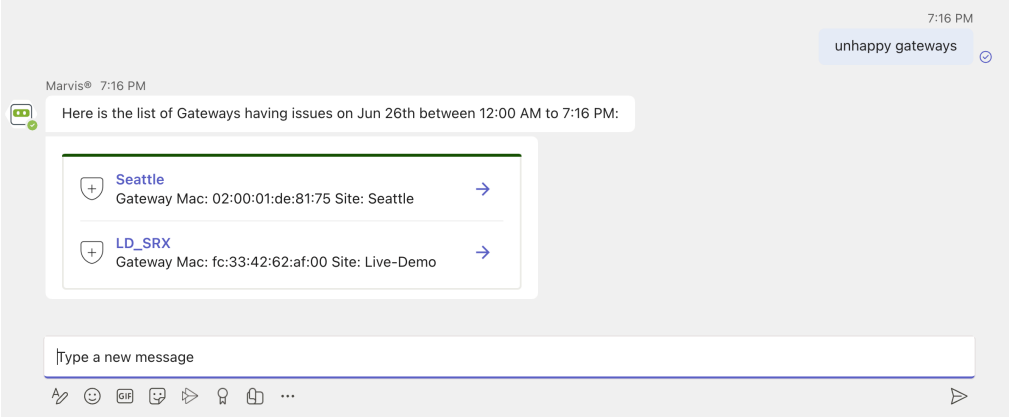


Troubleshoot Unhappy Devices or Clients

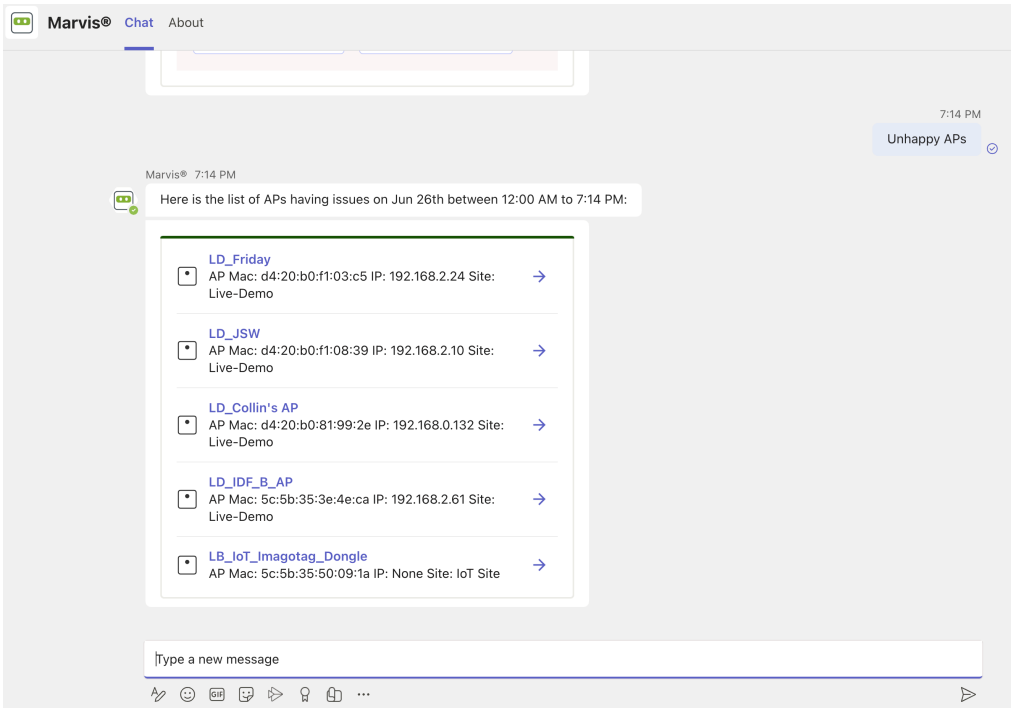
To check for devices experiencing issues (unhappy devices), simply enter the phrase "unhappy <device type>" in the Marvis chat window. For example, if you want to view unhappy WAN edge devices, enter "unhappy WAN edges" and Marvis will show all the WAN edges that are experiencing issues.

Here are a few examples. You can click any device to view the issues.

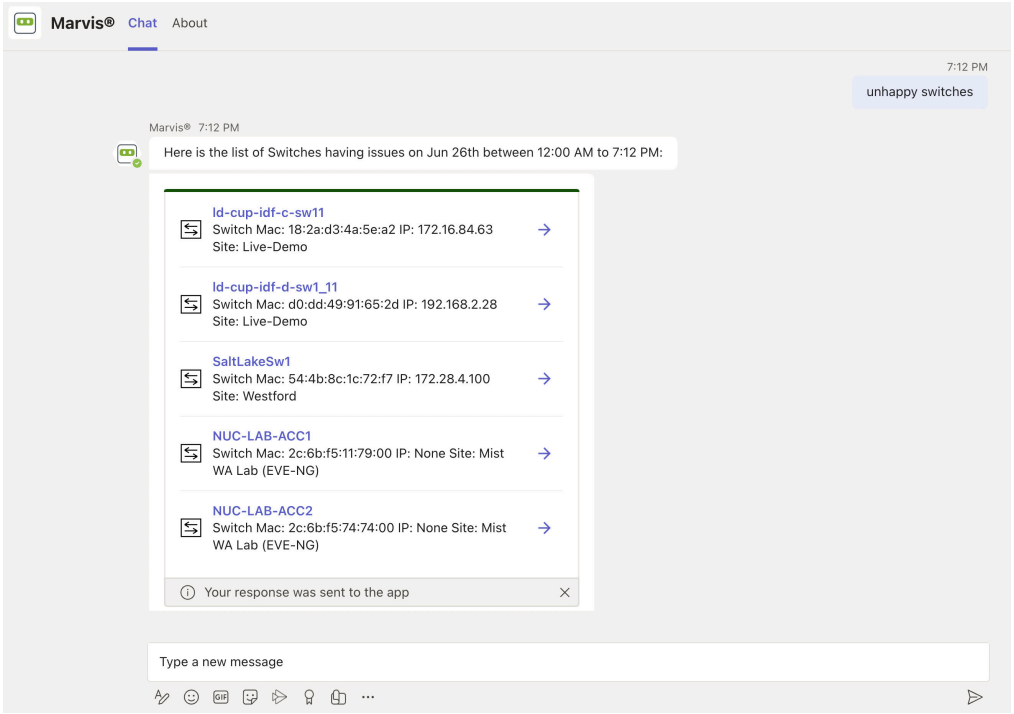
Unhappy WAN edges:



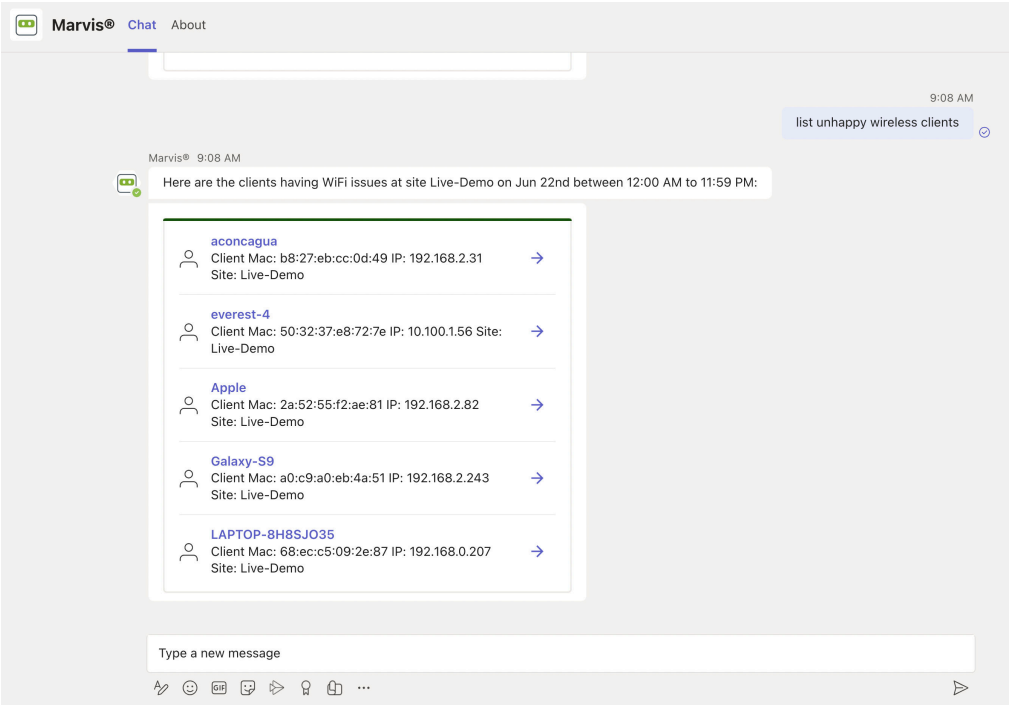
Unhappy APs:



Unhappy Switches:



Unhappy Wireless Clients:



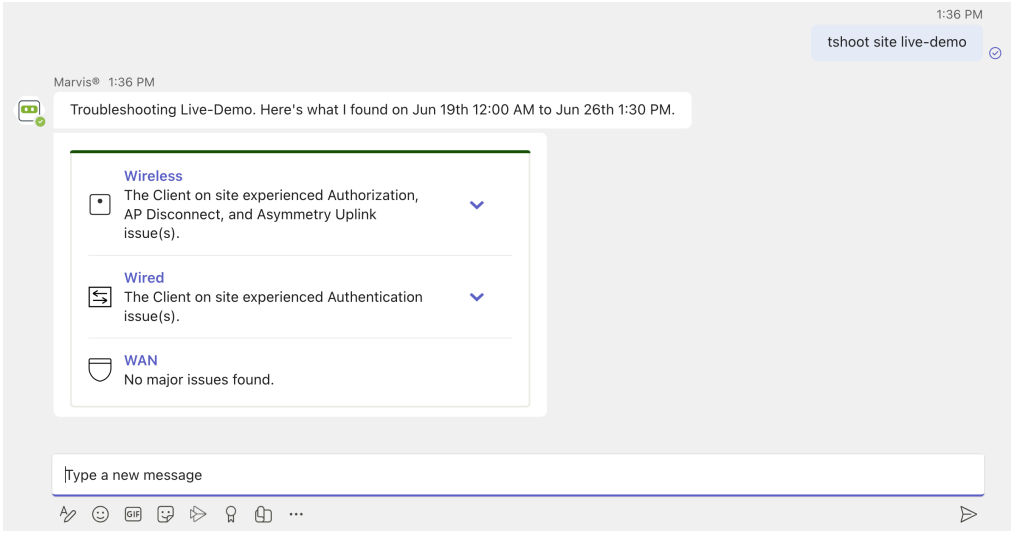
Troubleshoot a Site

You can use the Marvis app to troubleshoot sites to identify site-level failures.

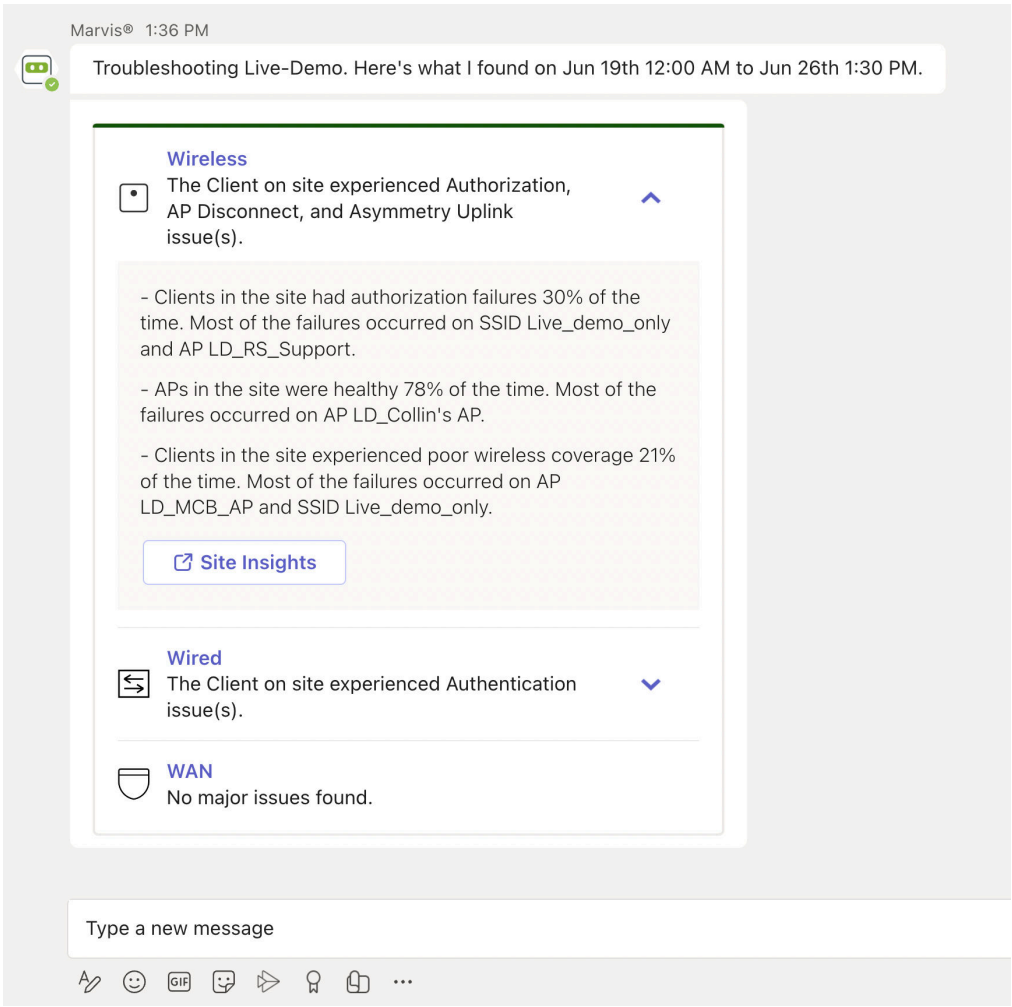
To check whether a device is experiencing any issues, enter a phrase such as "troubleshoot site *name*" in the Teams window.

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



You can click the expand arrow to view more details. You can drill down further to view site-level insights and device-level insights.



Search and List Functions in the Marvis App

SUMMARY

Use the Marvis App to search for devices, sites, and documentation.

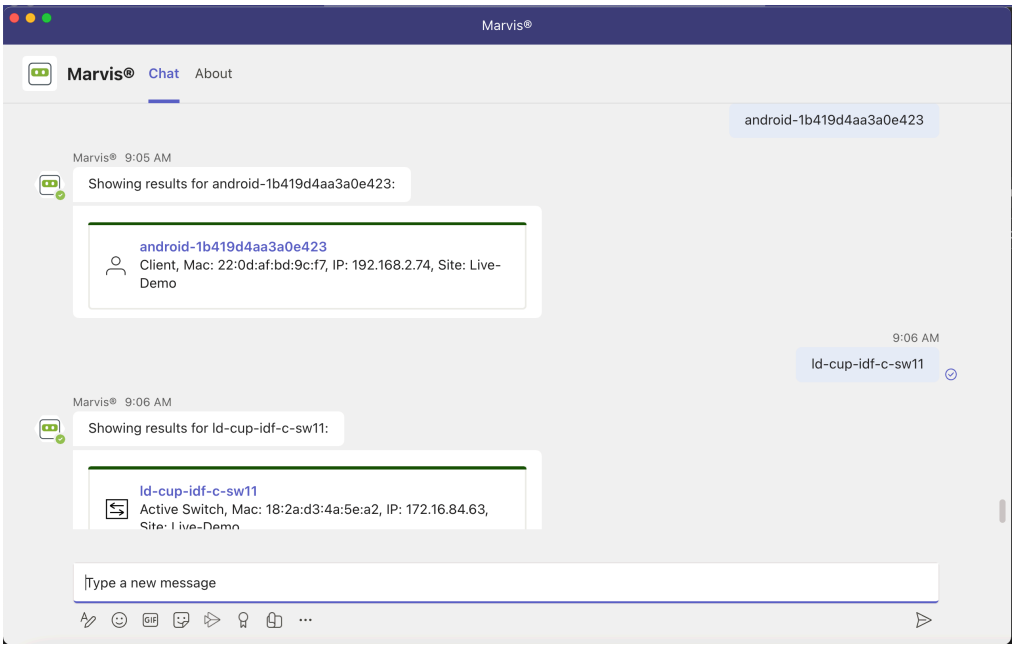
IN THIS SECTION

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:

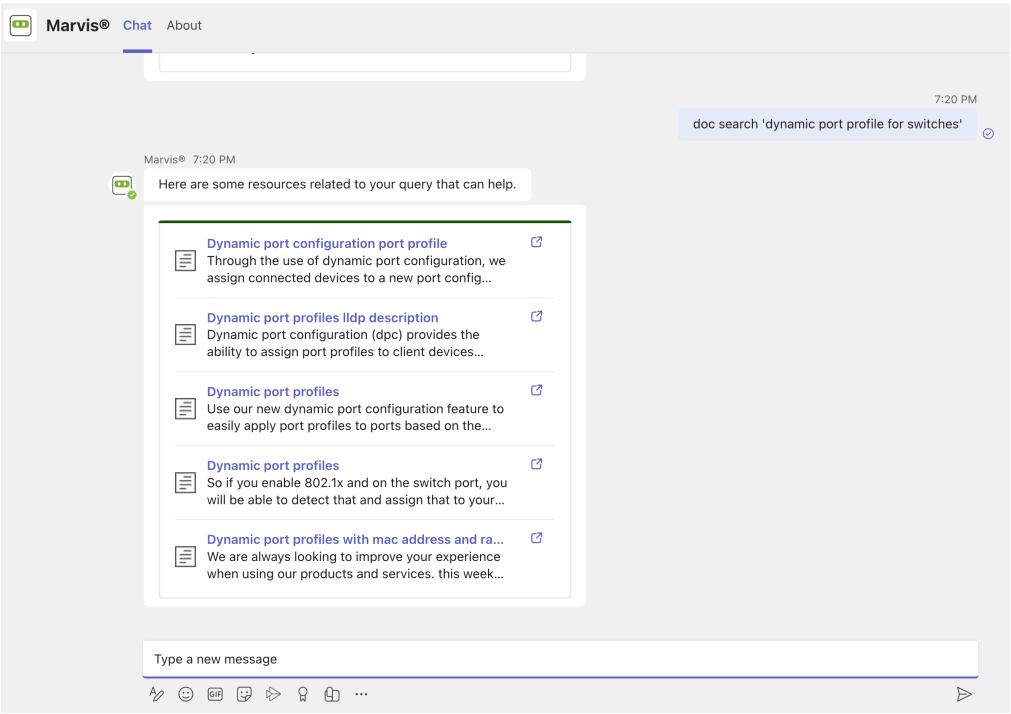


Here are some examples of phrases that you can use to search for a device or site:

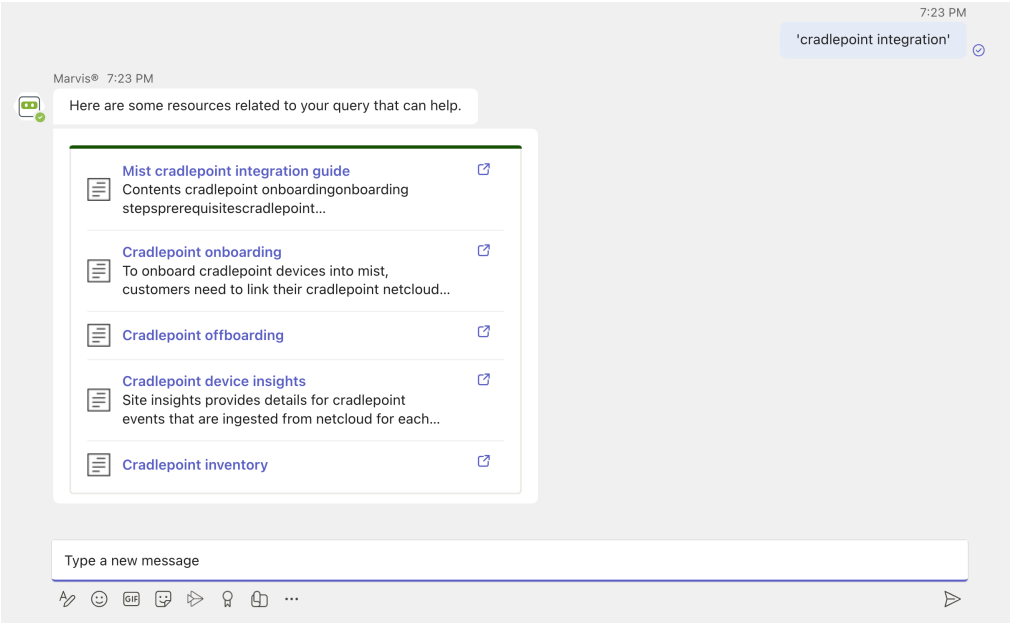
- <client name>
- Search <ap mac> <switch model>
- Find <WAN edge mac>
- <wired client mac>
- <site partial name>
- Locate <client username>

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>".



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.".



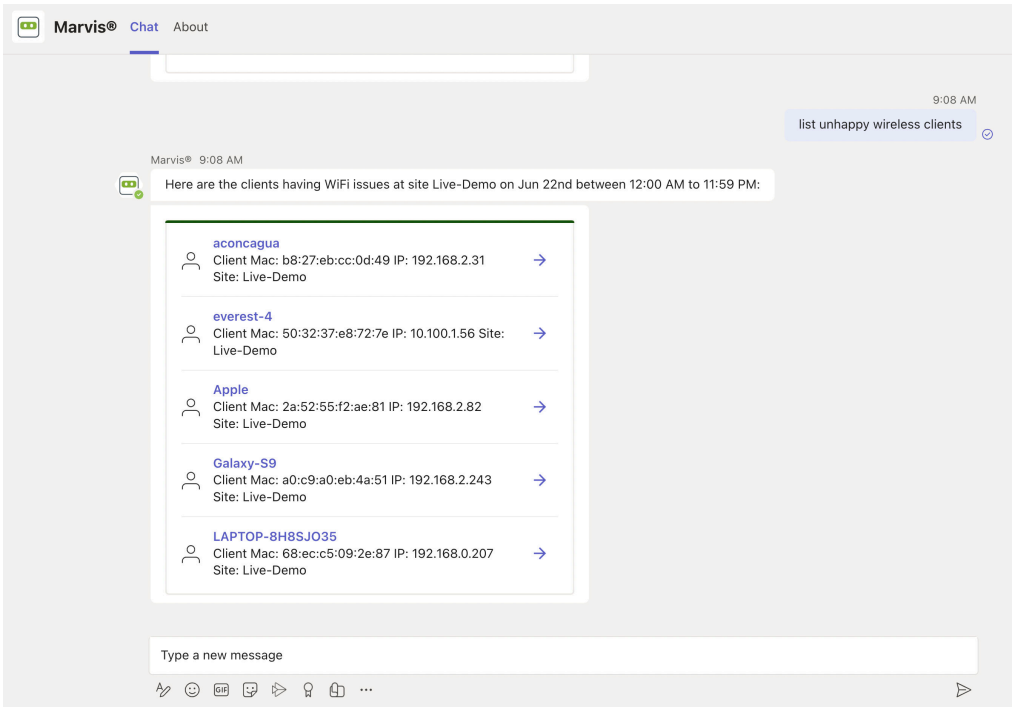
List Function

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."



View or Change the Organization in the Marvis App

SUMMARY

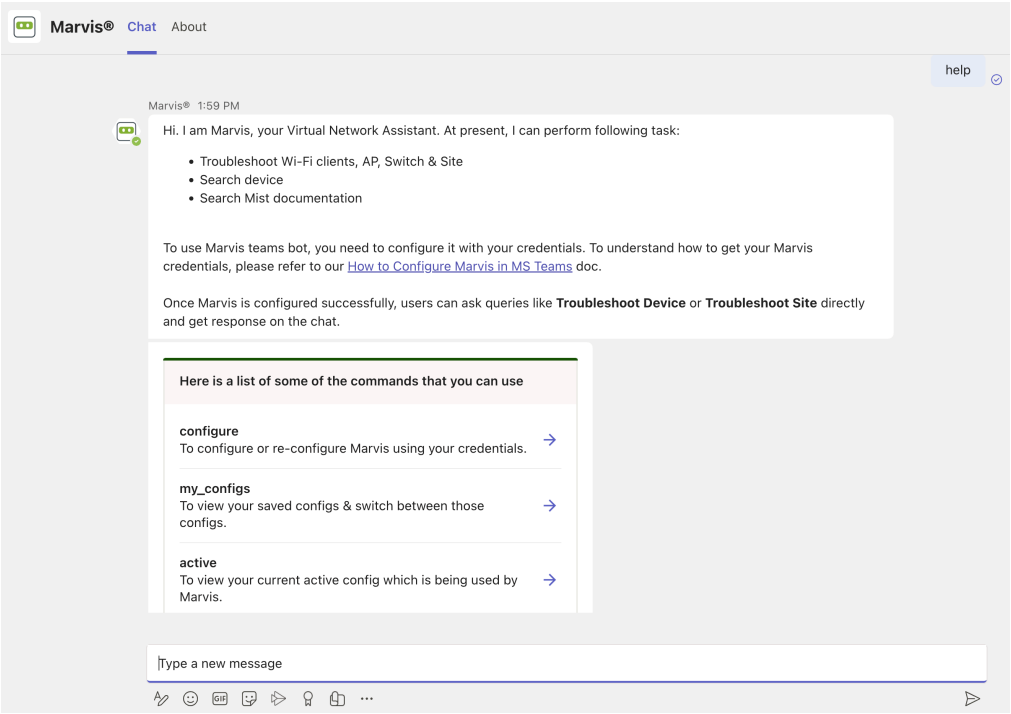
Select the organization that you want to view in the Marvis app.

You can run queries against multiple organizations and also switch between organizations using the Marvis app,

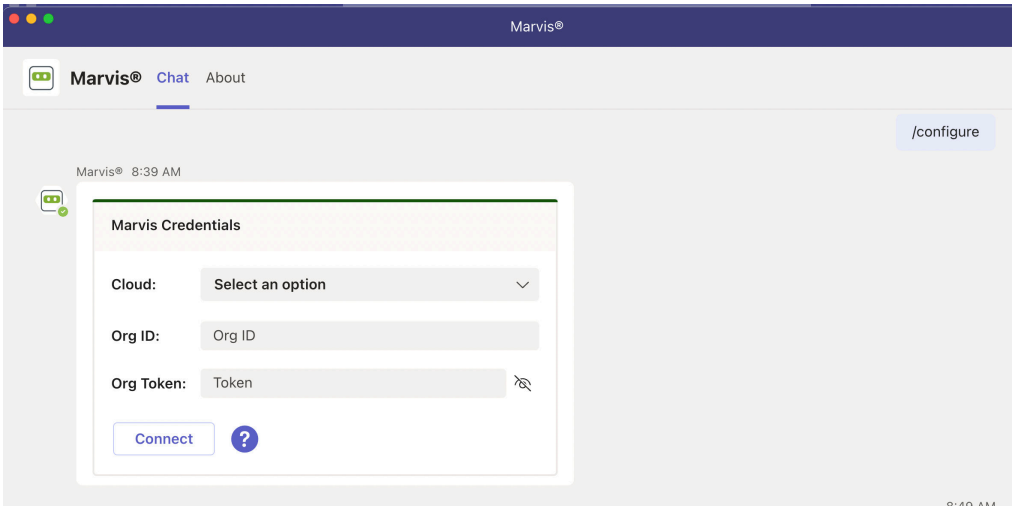
The Marvis app enables you to:

- 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:

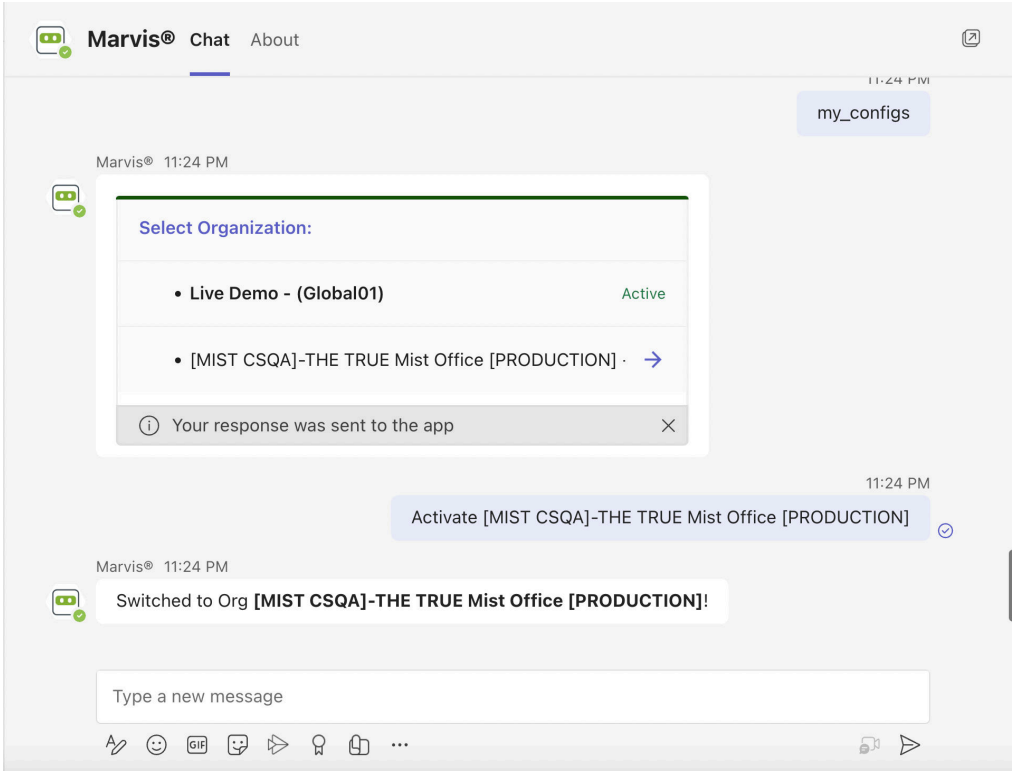


- If you enter **configure**, Marvis displays the login screen. You can either reconnect to the current active organization or connect to a different organization.



- 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.



- If you enter **active**, Marvis displays the organization that is currently active.

12

CHAPTER

Troubleshooting Examples

IN THIS CHAPTER

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.

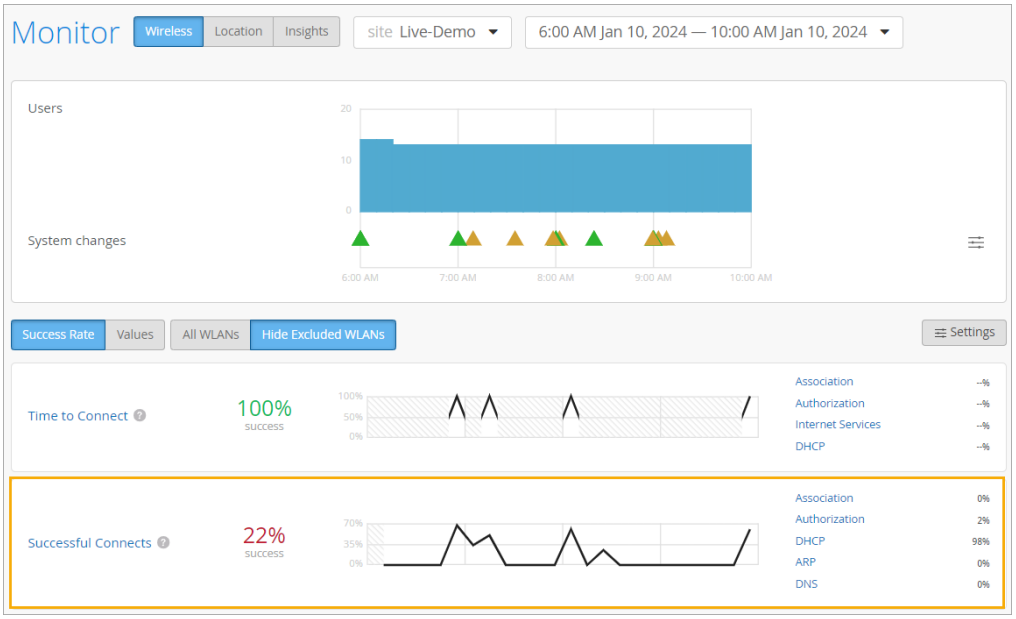
Typically, you wouldn't use *all* these tools, but this use case illustrates the valuable insights that you can gain from these tools. Use whichever options suit your situation and your preferences for working in the Juniper Mist™ portal.

Troubleshoot with the Successful Connects SLE

Let's start on the Wireless SLEs dashboard. SLEs offer insights into current and past issues.

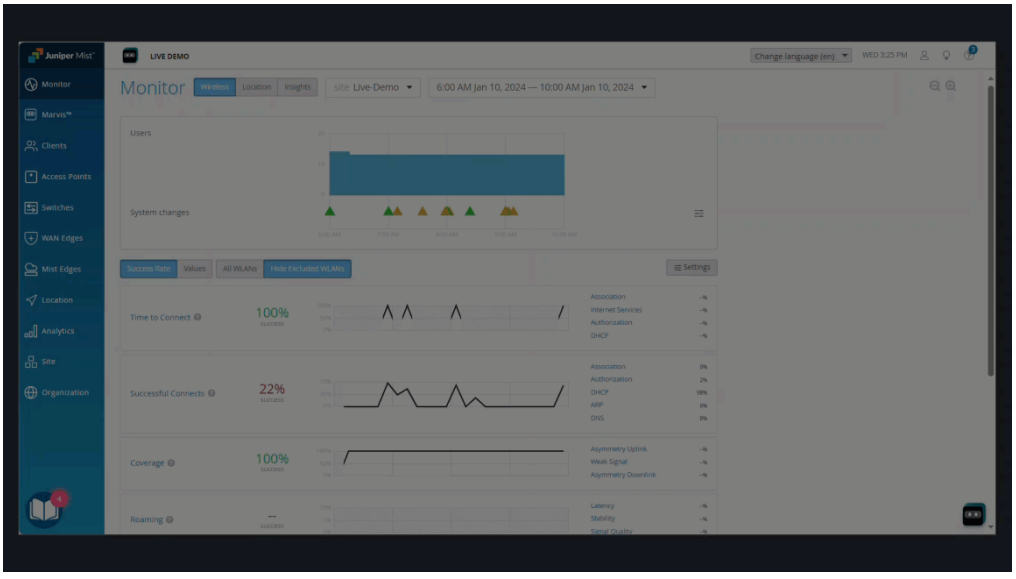
NOTE: To find the Wireless SLEs dashboard, select **Monitor** > **Service Levels** from the left menu, and then click the **Wireless** button.

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 SLEs" on page 76.

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.

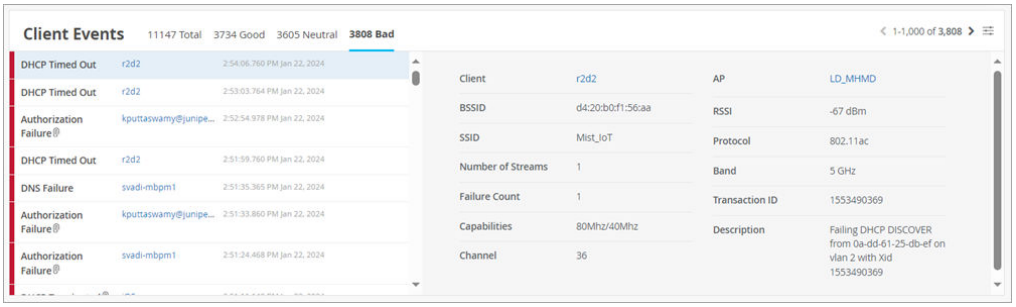
Explore Further on the Insights Dashboard

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**.

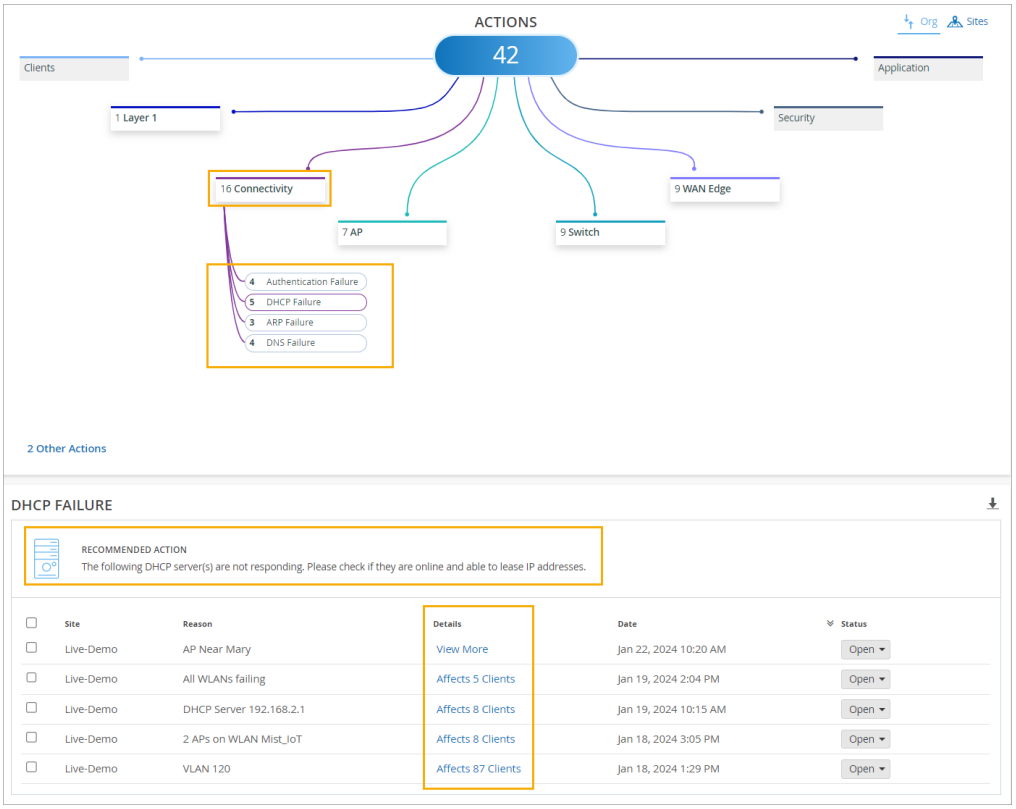
For this example, let's look at **Client Events**. If you click the **Bad** tab at the top, you can focus on the user-impacting issues. In this example, you see the details that are available for a DCHP timeout. For more information about an incident, you can click the link on the client name or the AP name.



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.

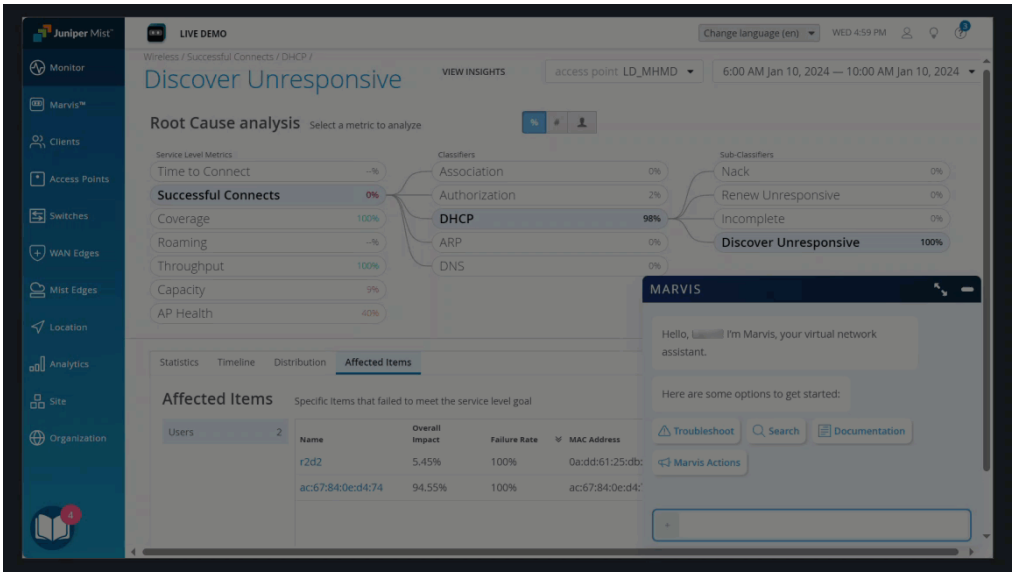


Troubleshoot with Marvis

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.



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.

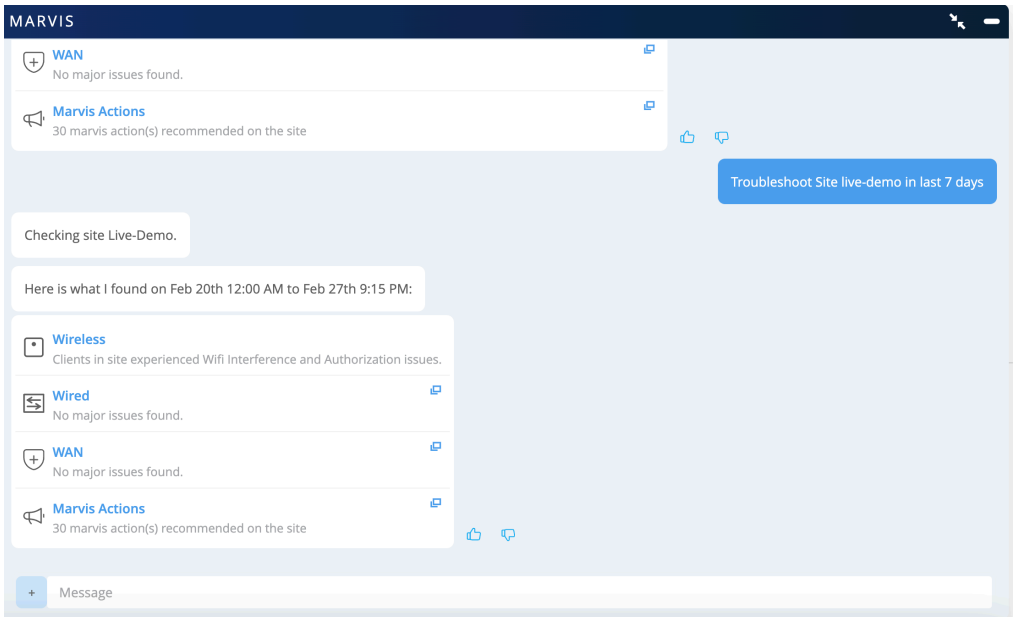
Troubleshoot Authorization Failures

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.

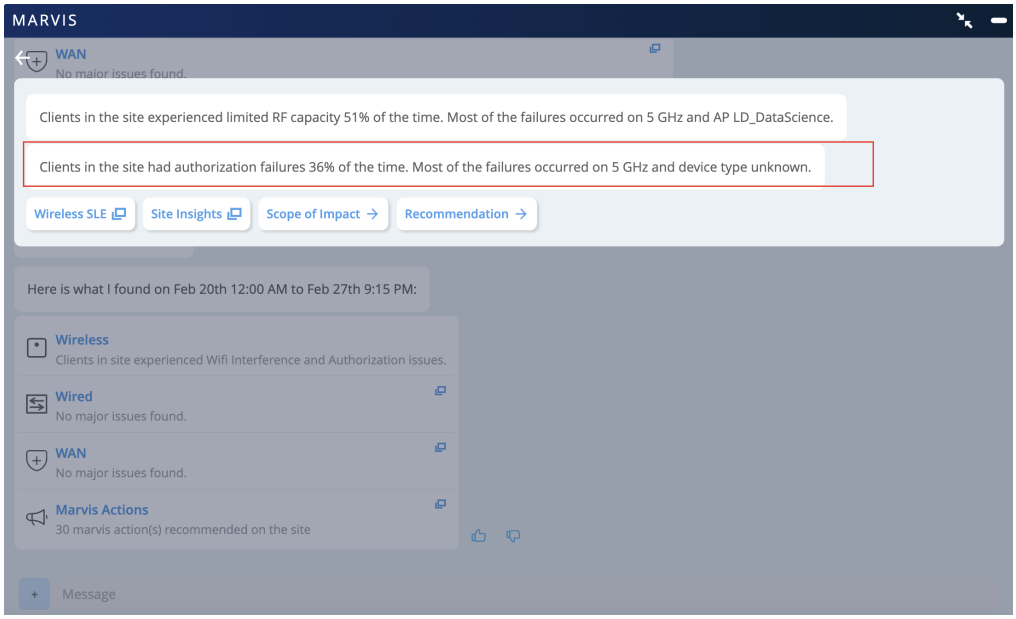
To troubleshoot authorization failures at a site:

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.



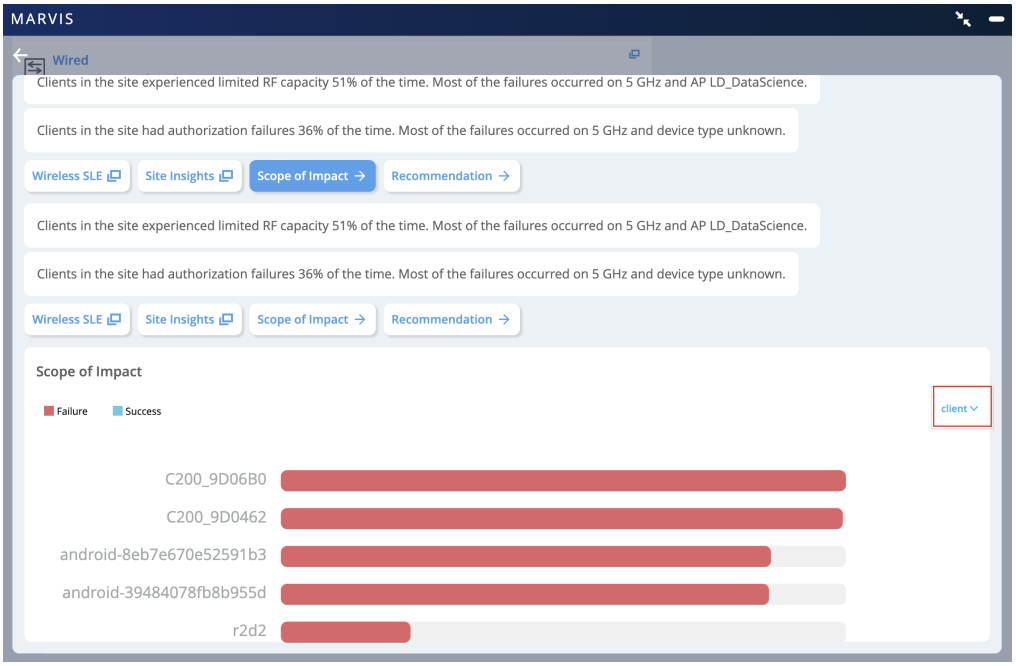
2. Click the **Wireless** category to get some more details about the issue. In this example, you'll see that Marvis reports that the clients at the site faced authorization failures 36% of the time.



You can investigate further by using the options displayed.

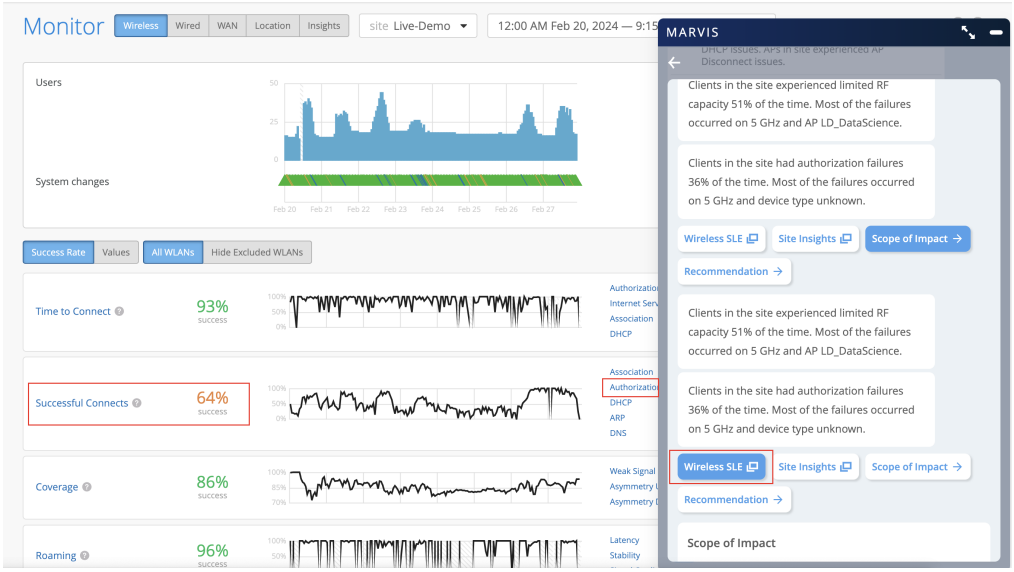
Scope of Impact

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.



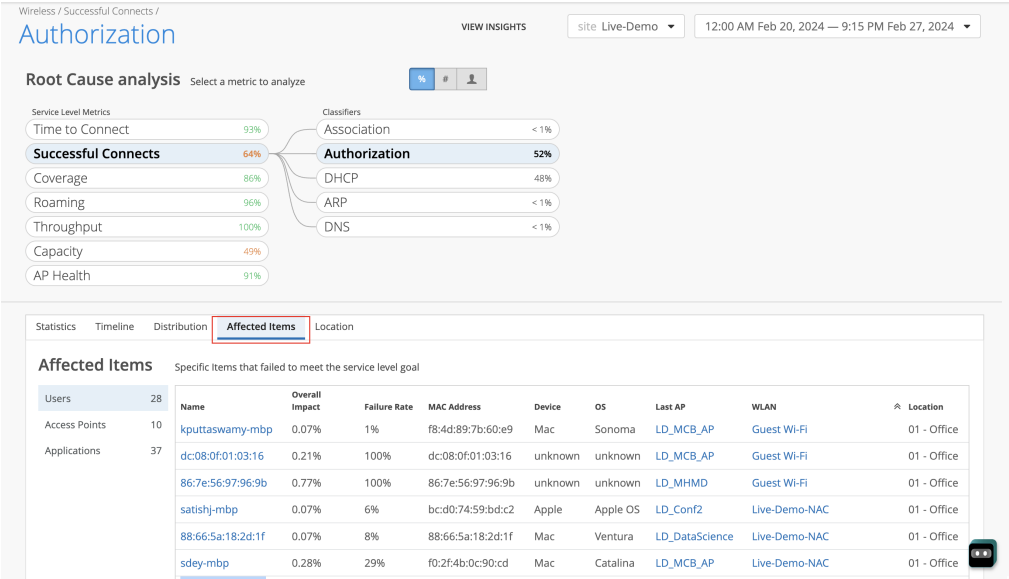
Wireless SLE

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.

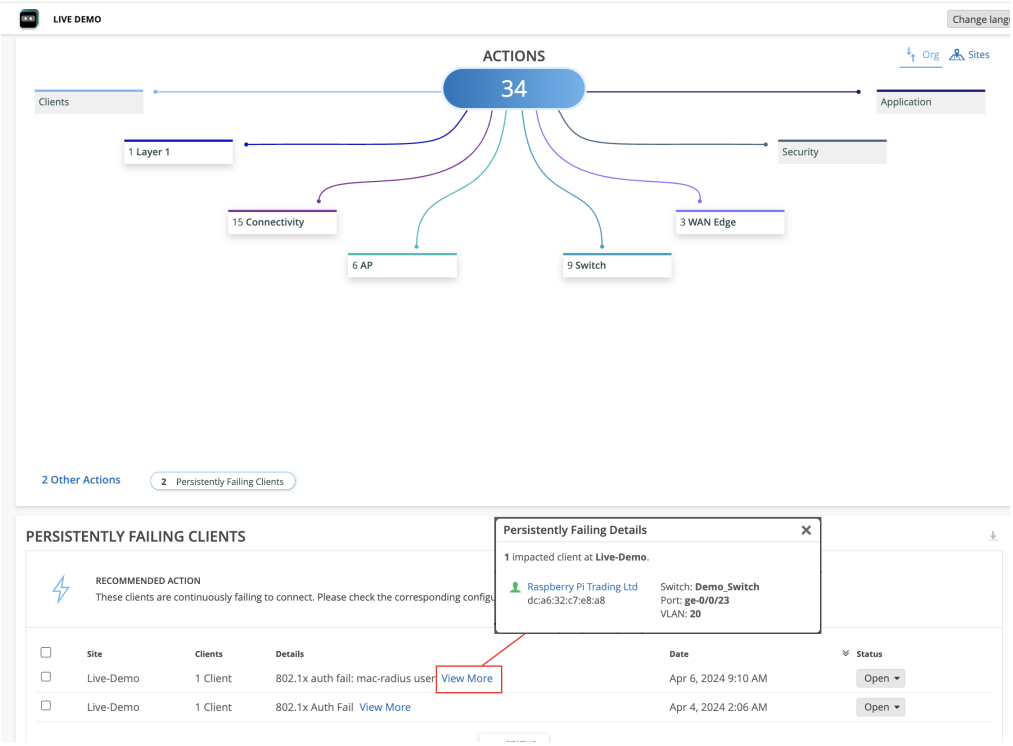


Click the **Authorization** classifier on the right to view the Root Cause Analysis page. This page provides detailed information. You can look through each of the tabs on the page. For example, you can use the Distribution tab to determine if the issue is being observed across:

- All APs or specific APs
- All users or specific users
- All WLANs or specific WLANs
- All device types or specific device types

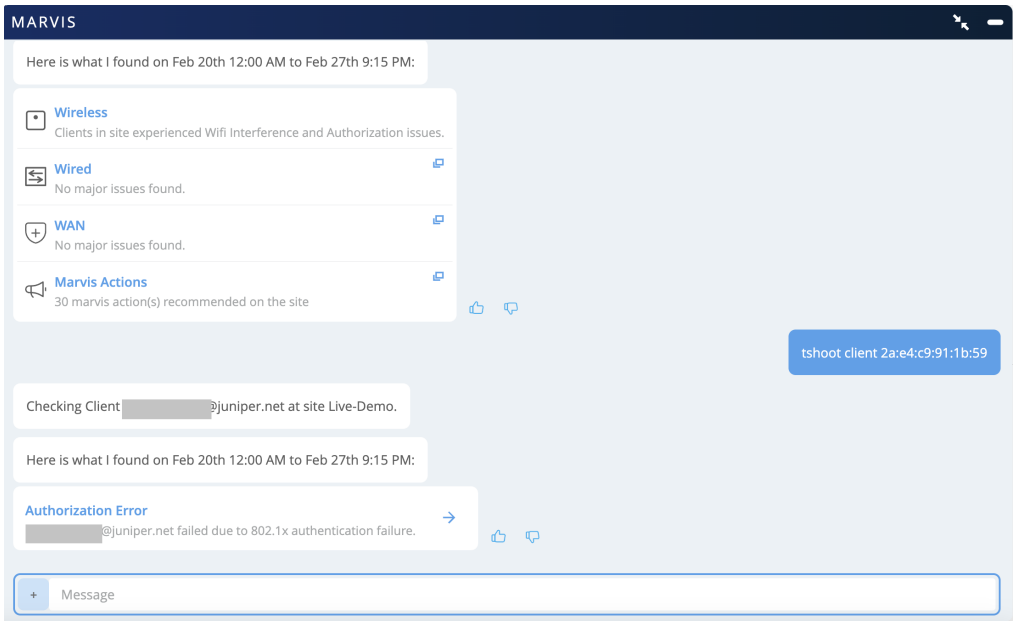


The **Affected Items** tab displays the impacted users, APs, and applications. You can drill down further by clicking a user. The **Failure Rate** column indicates whether the user always fails to connect. Users experiencing a 100-percent failure rate over a long period of time are listed under the Persistently Failing Clients category in Marvis Actions as shown in the following example:

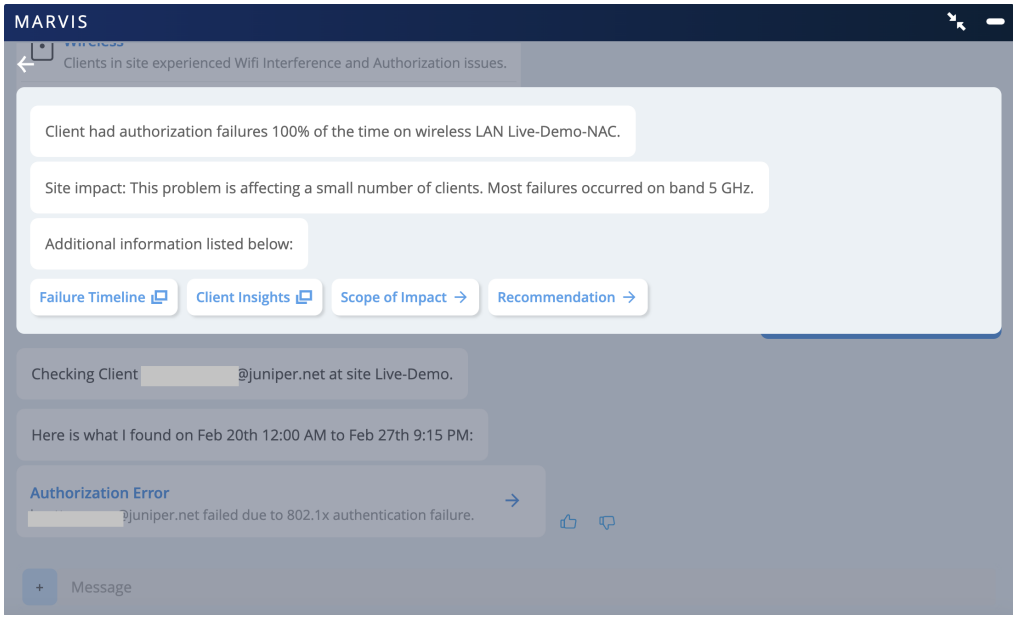


To troubleshoot authorization failures for a client:

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.

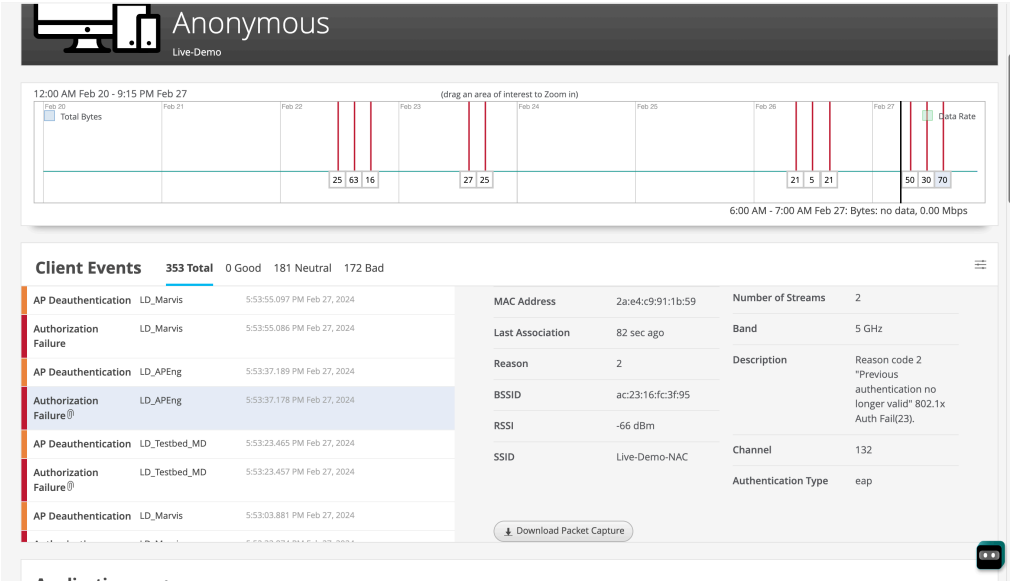


2. Click **Authorization Error** to view more details. In this example, you'll see that Marvis reports that the client faced authorization failures 100 percent of the time.

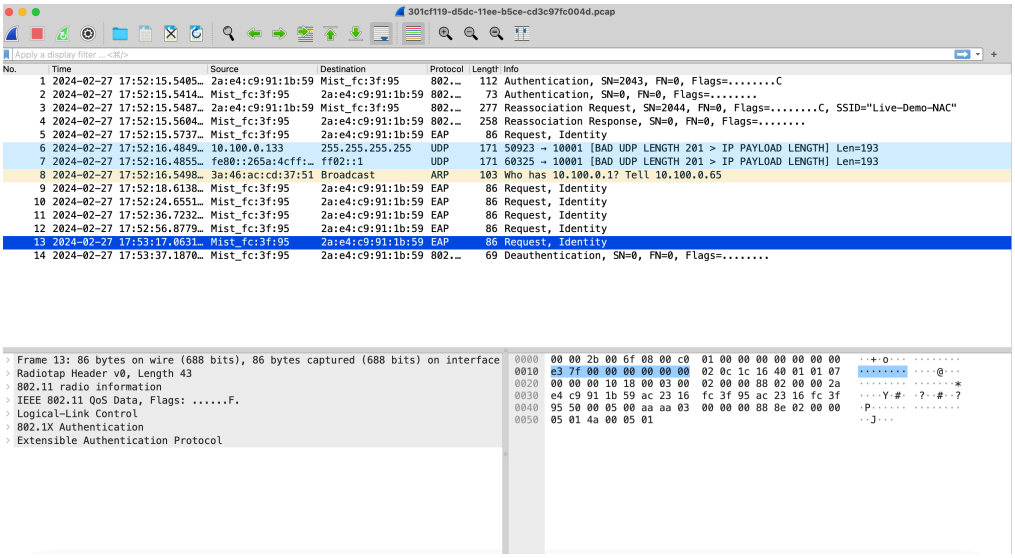


Note that Marvis also reports this issue on the Marvis Actions page, under the Connectivity category.

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.



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.

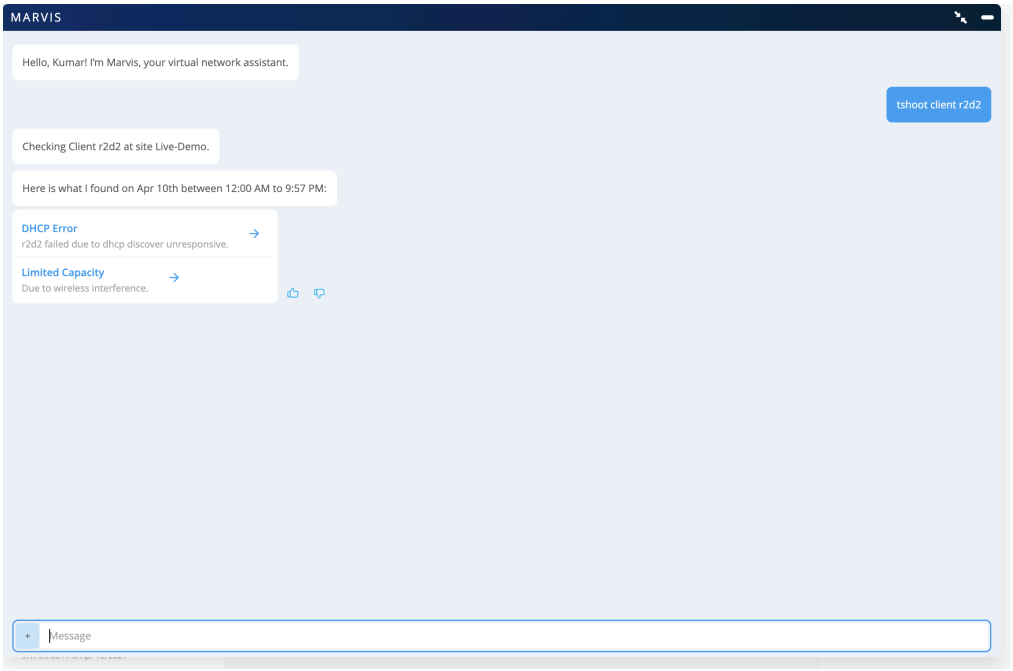


Troubleshoot DHCP Issues

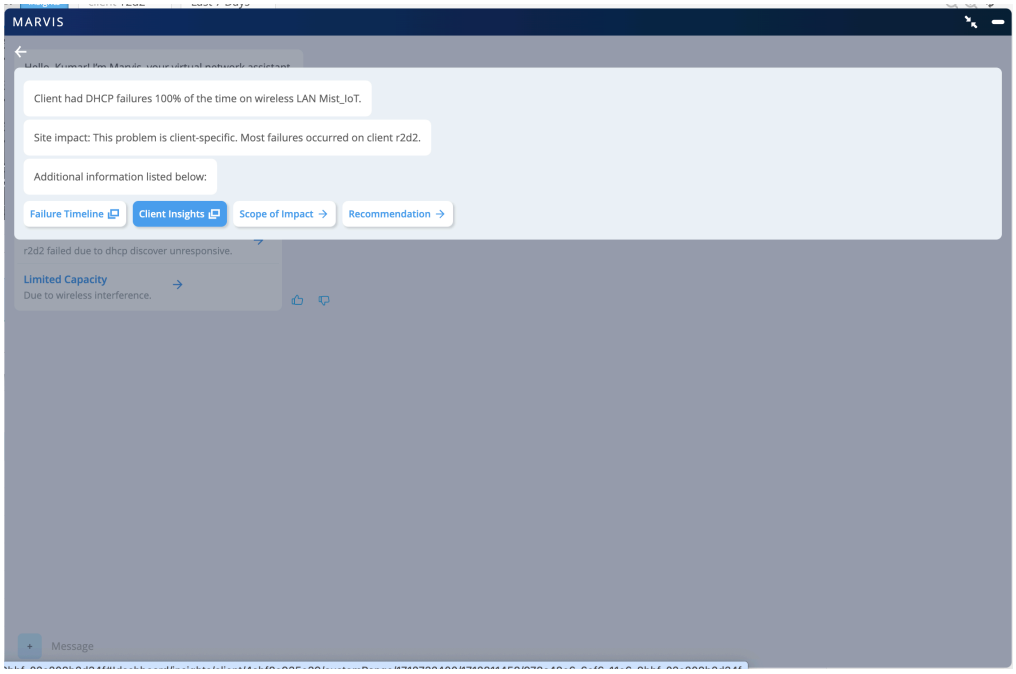
Clients might face connectivity issues when they fail to obtain an IP address due to a lack of response from the Dynamic Host Configuration Protocol (DHCP) server.

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.



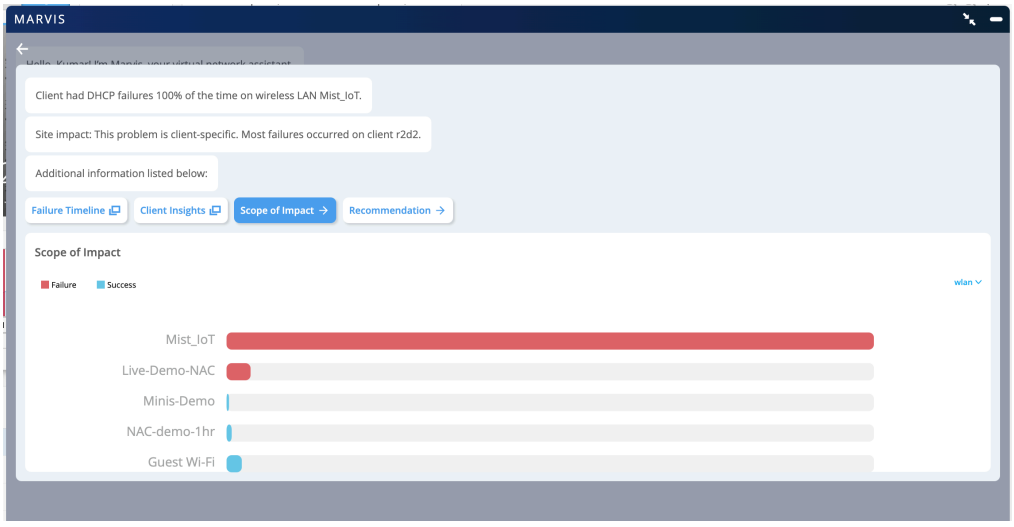
2. Click **DHCP Error** to view the details. In the following example, you'll see that Marvis reports that a specific client is facing DHCP failures 100 percent of the time.



You can investigate further by using the options displayed.

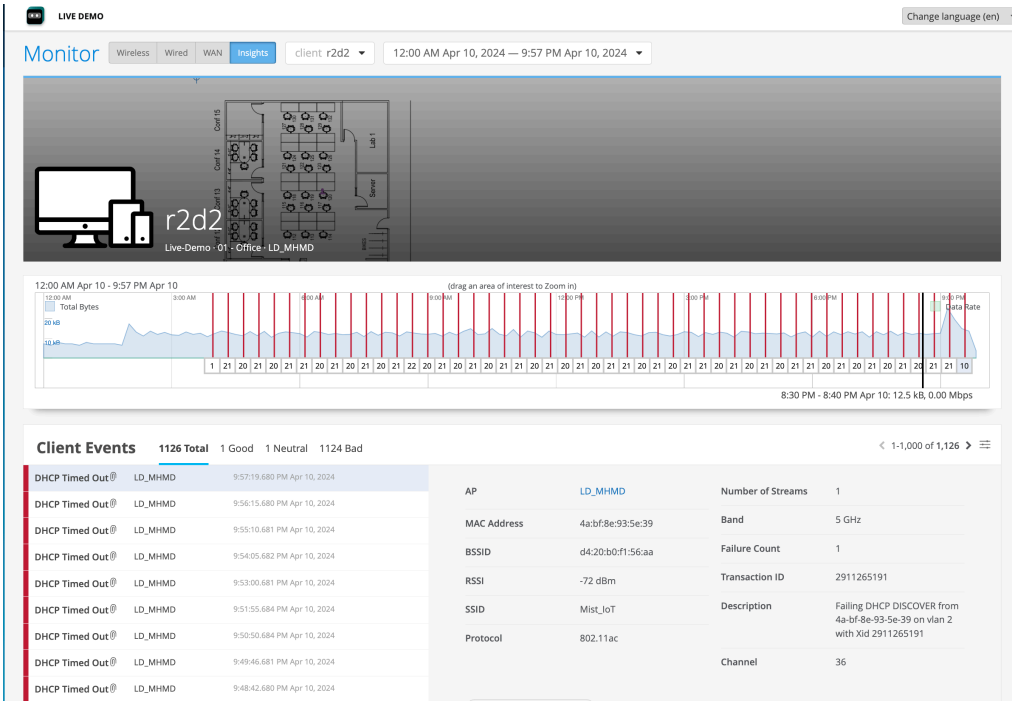
Scope of Impact

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.

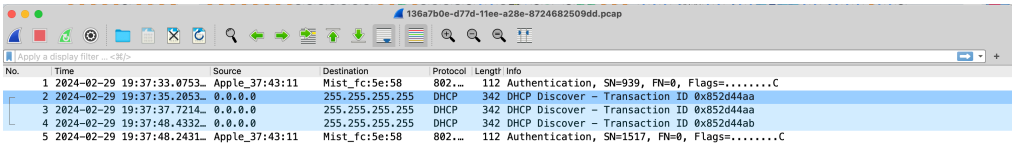


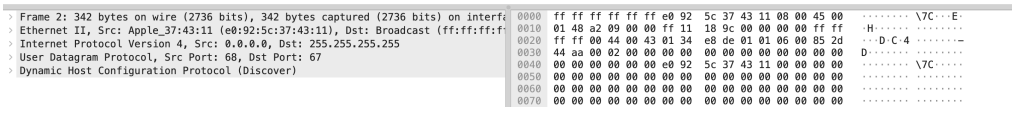
Client Insights

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.



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.



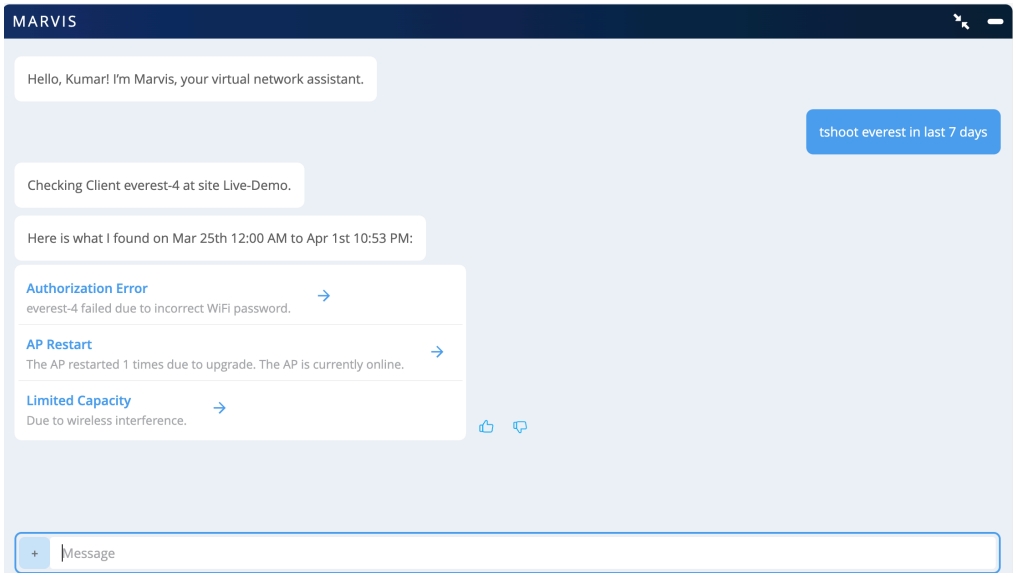


Troubleshoot PSK Failures

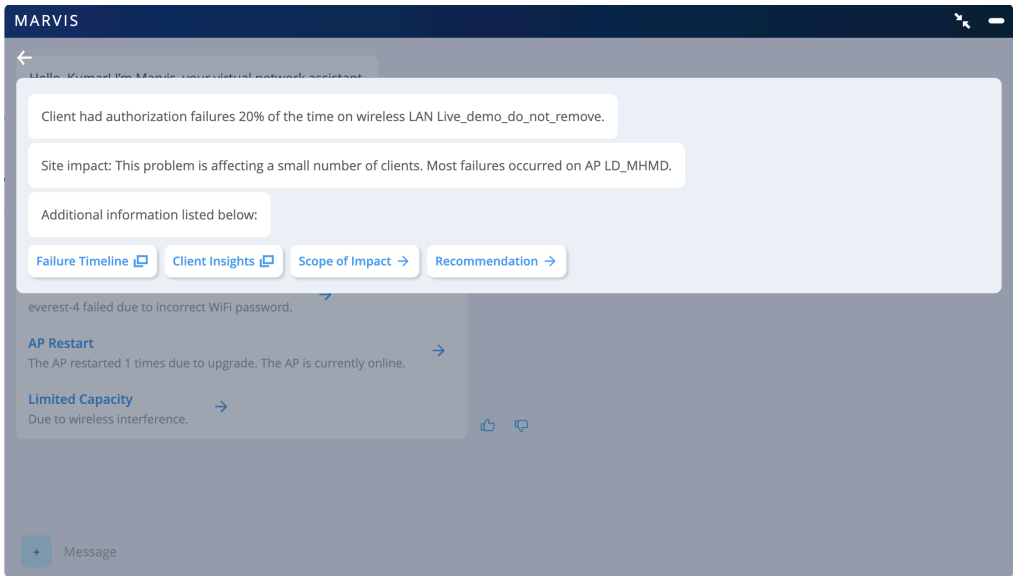
Marvis detects preshared key (PSK) failures when a large number of clients fail to authenticate to a PSK WLAN. A probable cause for this issue could be a recent PSK change that was not communicated to users.

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.



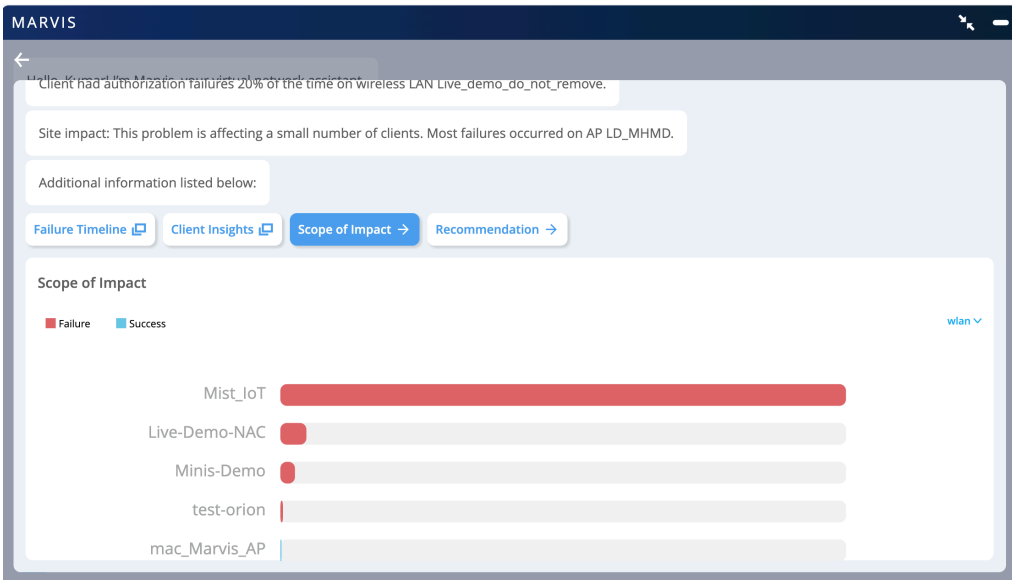
2. Click **Authorization Errors** to view the details.



Investigate further by using the options displayed.

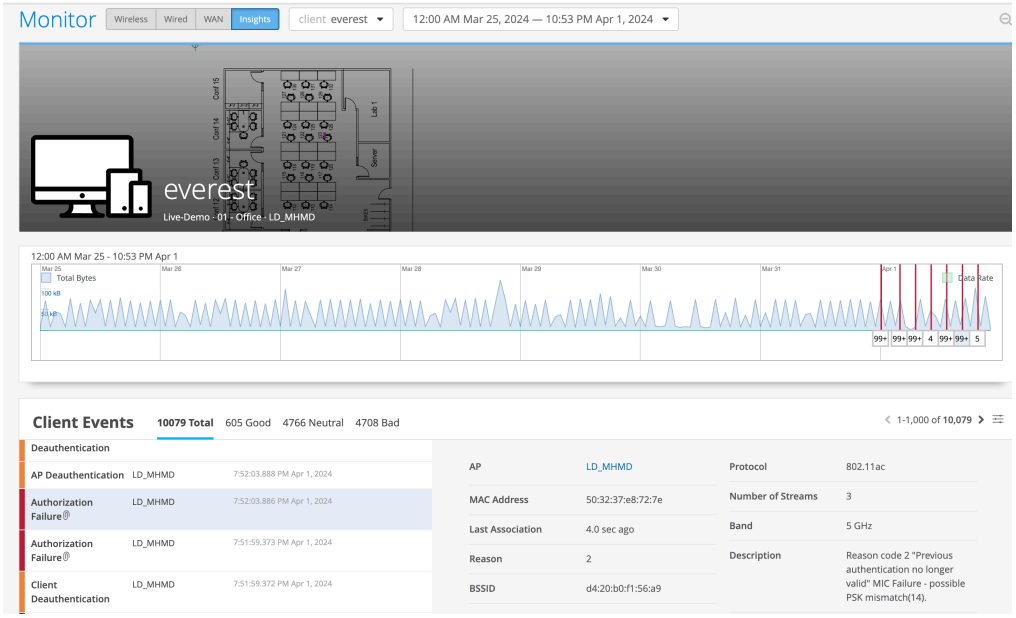
Scope of Impact

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 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.

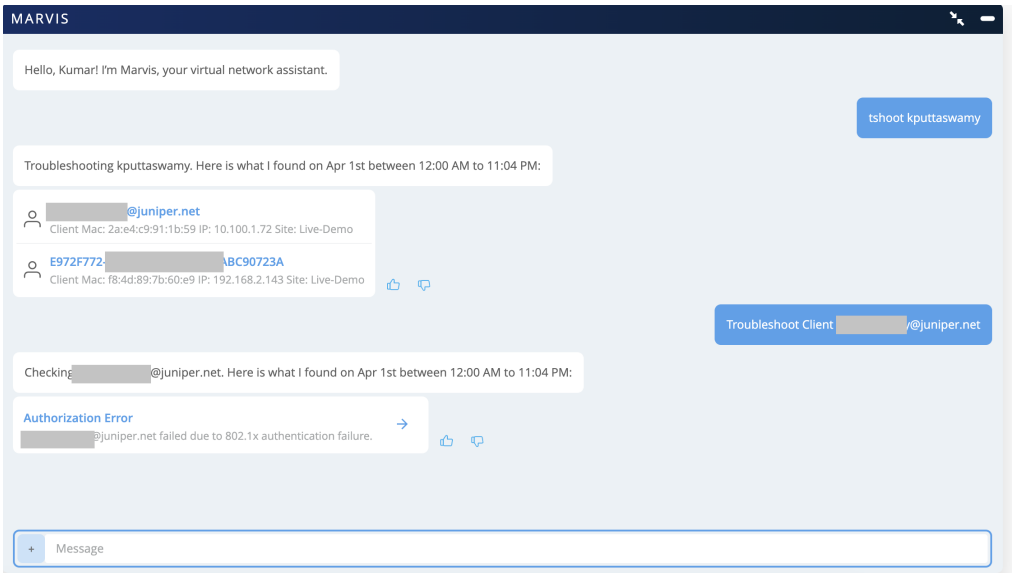


Troubleshoot RADIUS Authentication Failures

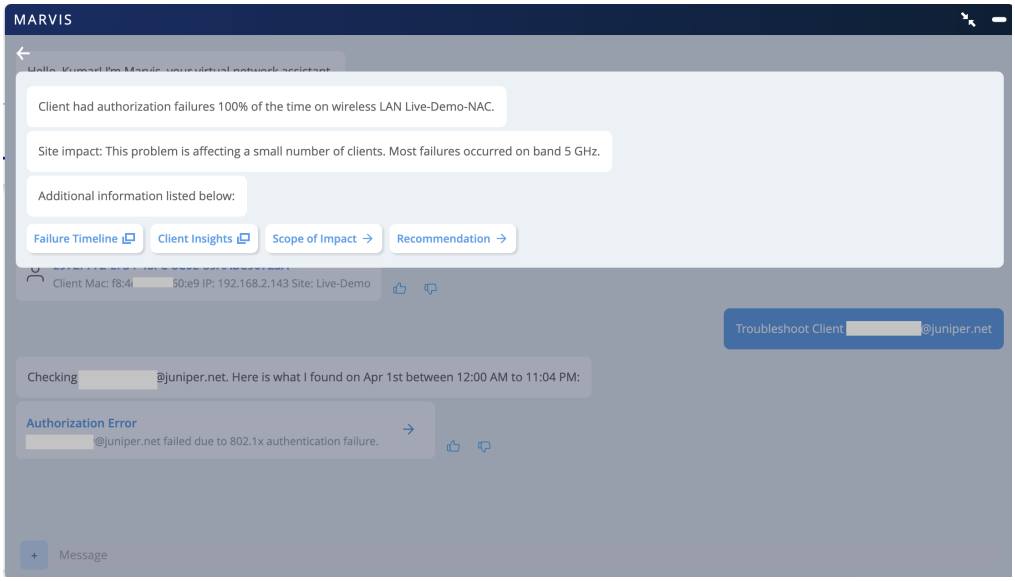
Clients might experience an 802.1x authentication failure when a RADIUS server is down or unreachable.

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.



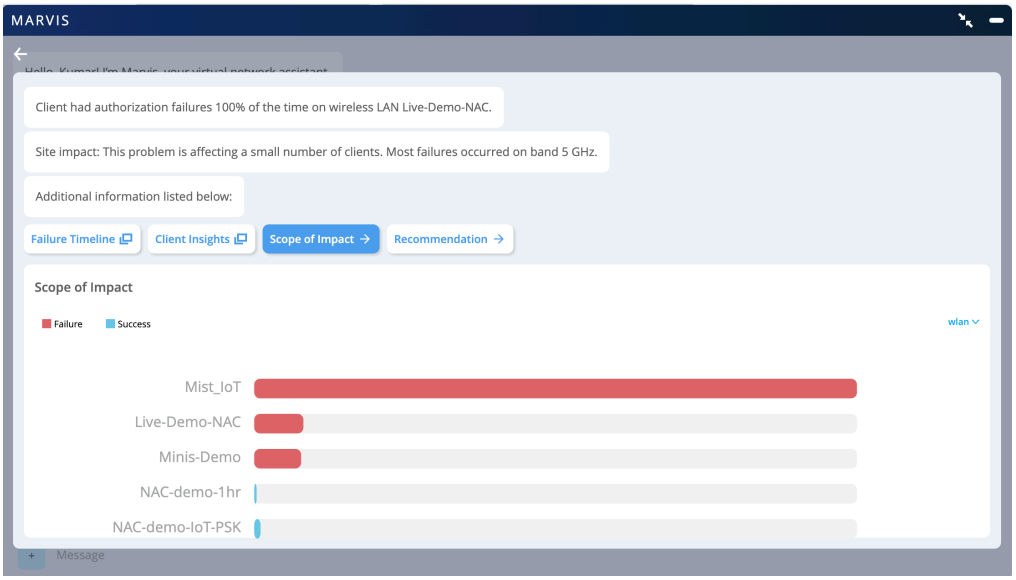
2. Click **Authentication Error** to view the details.



You can investigate further by using the options displayed.

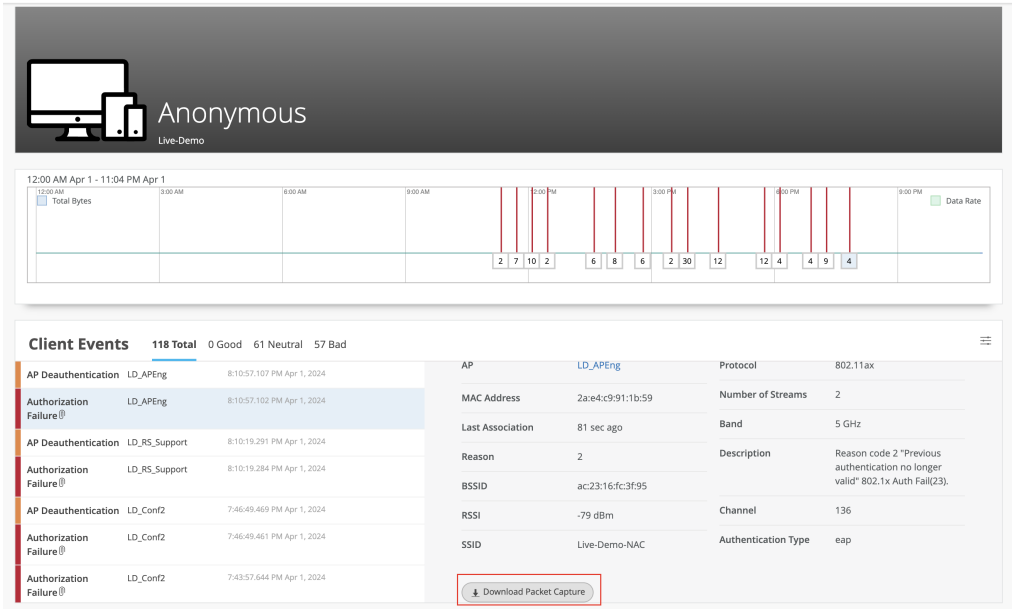
Scope of Impact

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.

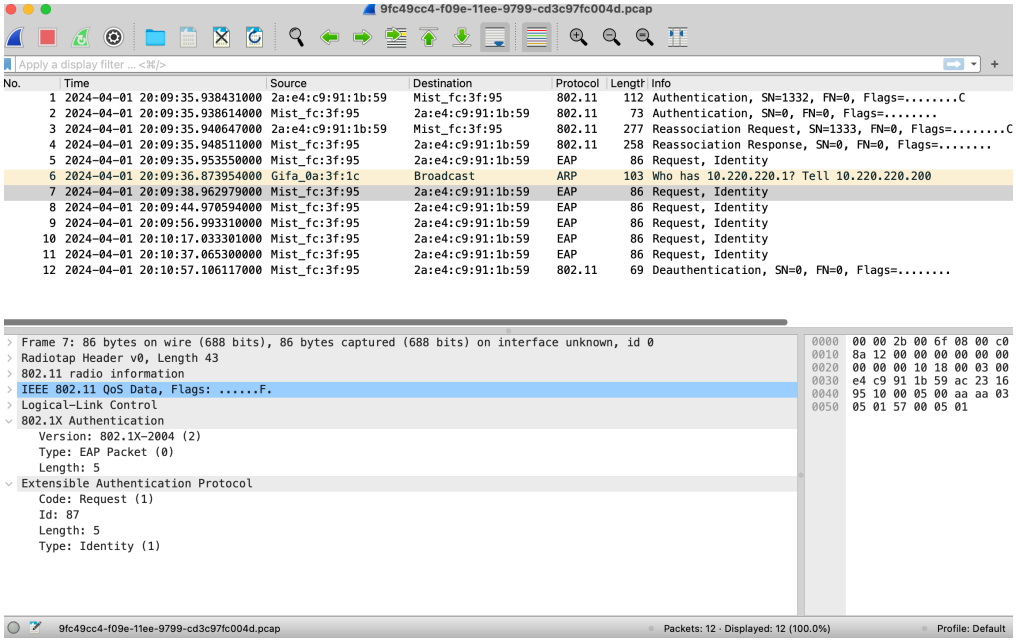


Client Insights

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.



You can download the dynamic packet capture for a specific event. Here's a sample packet capture:



Troubleshoot a Device or Site by Using APIs

SUMMARY

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:

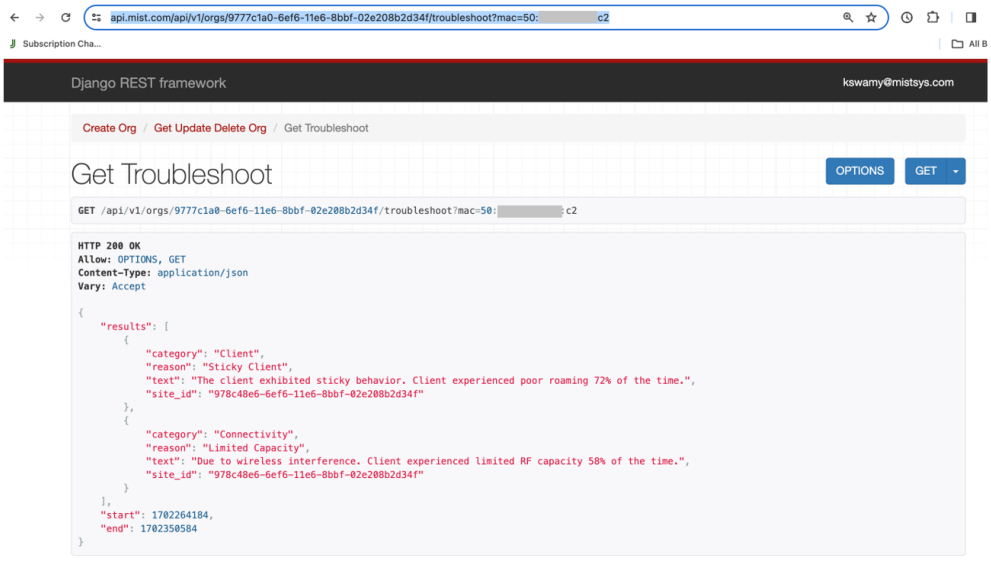
  `GET /api/v1/orgs/:org_id/troubleshoot?site_id=:siteid`

  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:

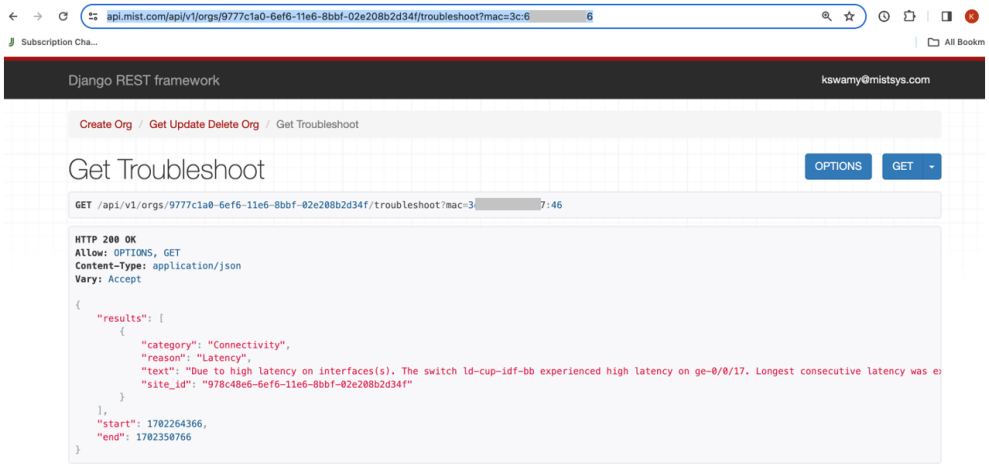
- Troubleshoot a device (wireless client)

  https://api.mist.com/api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?mac=50:xx:xx:xx:xx:c2



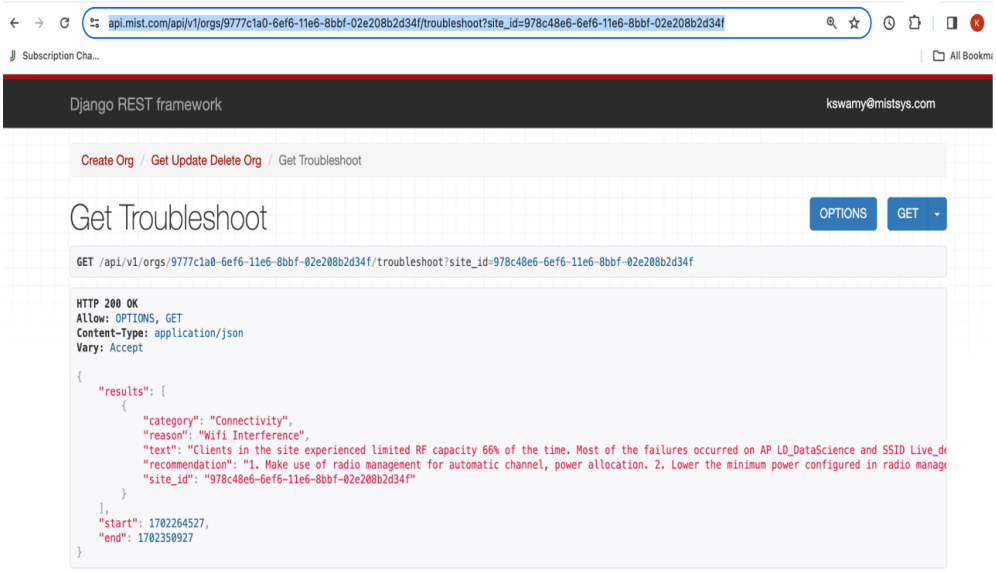
- Troubleshoot a device (wired client)

https://api.mist.com/api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?mac=3c:xx:xx:xx:xx:46



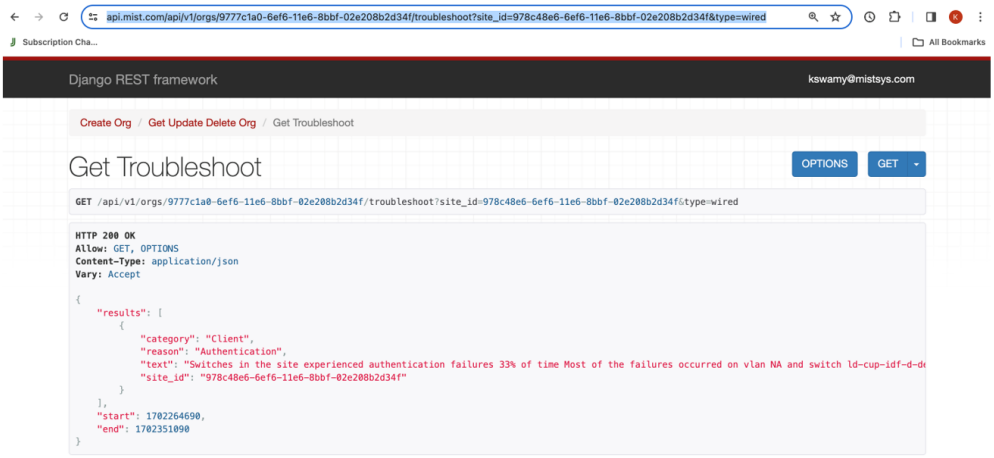
- Troubleshoot a site (wireless)

  https://api.mist.com/api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?site_id=978c48e6-6ef6-11e6-8bbf-02e208b2d34f



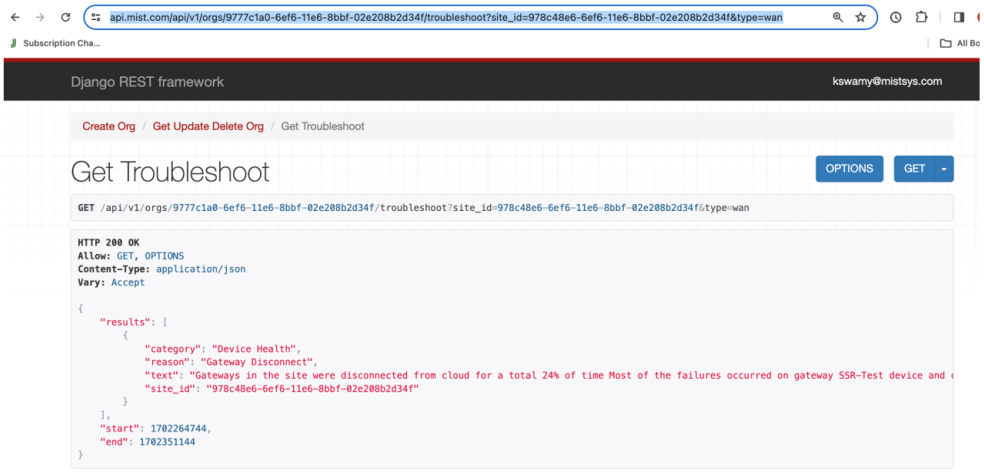
- Troubleshoot a site (wired)

  https://api.mist.com/api/v1/orgs/9777c1a0-6ef6-11e6-8bbf-02e208b2d34f/troubleshoot?site_id=978c48e6-6ef6-11e6-8bbf-02e208b2d34f&type=wired



- 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



To view the API documentation, see the Mist API Reference. For more information on troubleshooting using Marvis, see Troubleshoot Org.