Engineering Simplicity

Marvis

Published
2023-12-14

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

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

Marvis
Copyright © 2023 Juniper Networks, Inc. All rights reserved.

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

About This Guide | vi

1 Overview

Marvis Virtual Network Assistant | 2

Subscriptions for Marvis | 3

2 Marvis Actions

Marvis Actions Overview | 5

Marvis Actions for Wired, WAN, and Wireless Assurance | 9

Marvis Actions for Switches | 11

Marvis Actions for Layer 1 Connectivity | 19

Marvis Actions for WAN Edge Devices | 20

Marvis Actions for Client Connectivity Failures | 23

Marvis Actions for APs | 28

Other Marvis Actions | 35

Anomaly Detection Event Card | 36

3 Marvis Query Language

Marvis Query Language Overview | 39

Troubleshoot Using Marvis Query Language | 40

4 Marvis Client

Marvis Client Overview | 49

Marvis Android Client | 51

Before You Begin | 51

Deploy the Marvis Client Using the SOTI MDM | 52

Deploy the Marvis Client Using AirWatch or VMWare Workspace ONE | 54

Deploy Marvis Client Using Other MDMs | 54

Install Through Sideloading | 55

Verify the Installation | 58

Marvis-Zebra Integration | 59

Client Roaming Visualization | 62

5 **Marvis Conversational Assistant**

Marvis Conversational Assistant Overview | 69

Search Using the Conversational Assistant | 71

Troubleshoot Applications Using the Conversational Assistant | 74

Troubleshoot Devices Using the Conversational Assistant | 78

Troubleshoot a Wireless Client | 79

Troubleshoot Unhappy Wireless Clients | 79

Troubleshoot Wired Clients | 80

Troubleshoot APs | 81

Troubleshoot Unhappy APs | 81

Troubleshoot Switches | 82

Troubleshoot Unhappy Switches | 83

Troubleshoot WAN Edge Devices | 83

Troubleshoot Unhappy WAN Edge Devices | 84

Quick Reference to Troubleshoot Devices | 85

Troubleshoot Sites Using the Conversational Assistant | 86

6 **Marvis App for Teams**

Overview of the Marvis Conversational App for Microsoft Teams | 92

Enable or Integrate the Marvis App in Microsoft Teams | 92

Enable the Marvis App in Your Teams Environment | 93

Add the Permission Policy for the Marvis App | 94

Assign the Policy to Users | **94**

Install the Marvis App in Microsoft Teams | 95

Install the Marvis App in Teams | **95**

Connect to Your Mist Organization | **97**

Add the Marvis App to a Microsoft Teams Channel | **101**

Troubleshoot Using the Marvis App | 103

Troubleshoot a Wireless Client | **104**

Troubleshoot a Wired Client | **105**

Troubleshoot a Device | **105**

Troubleshoot Unhappy Devices or Clients | **107**

Troubleshoot a Site | **109**

Search and List Functions in the Marvis App | 111

View or Change the Organization in the Marvis App | 115

About This Guide

Use this guide to understand how you can proactively manage and troubleshoot your network using the Marvis® Virtual Network Assistant.

1

CHAPTER

Overview

Marvis Virtual Network Assistant | 2

Subscriptions for Marvis | 3

Marvis Virtual Network Assistant

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

Watch this video to learn how Marvis came to be, and what Marvis offers to you.

Video:

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

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

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

Here are the four main components of Marvis:

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

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

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

Watch this video to learn how you can use Marvis to troubleshoot your network:

Video:

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

Video:

Subscriptions for Marvis

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

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

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

See "Marvis Actions for Wired, WAN, and Wireless Assurance" on page 9 for more information.

2

CHAPTER

Marvis Actions

Marvis Actions Overview | 5

Marvis Actions for Wired, WAN, and Wireless Assurance | 9

Marvis Actions for Switches | 11

Marvis Actions for Layer 1 Connectivity | 19

Marvis Actions for WAN Edge Devices | 20

Marvis Actions for Client Connectivity Failures | 23

Marvis Actions for APs | 28

Other Marvis Actions | 35

Anomaly Detection Event Card | 36

Marvis Actions Overview

IN THIS SECTION

- Marvis Actions | 5

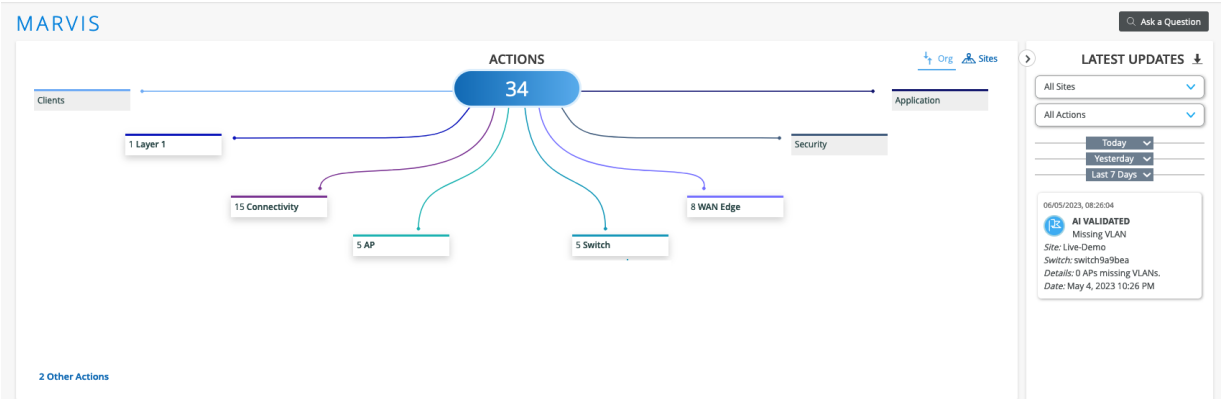
Marvis® leverages the Mist AI to identify the root cause of issues. Marvis can automatically fix issues (self-driving mode) or recommend actions that require user intervention (driver-assist mode). The Marvis Actions page lists the high-impact network issues that Marvis detects. Marvis Actions also displays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

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

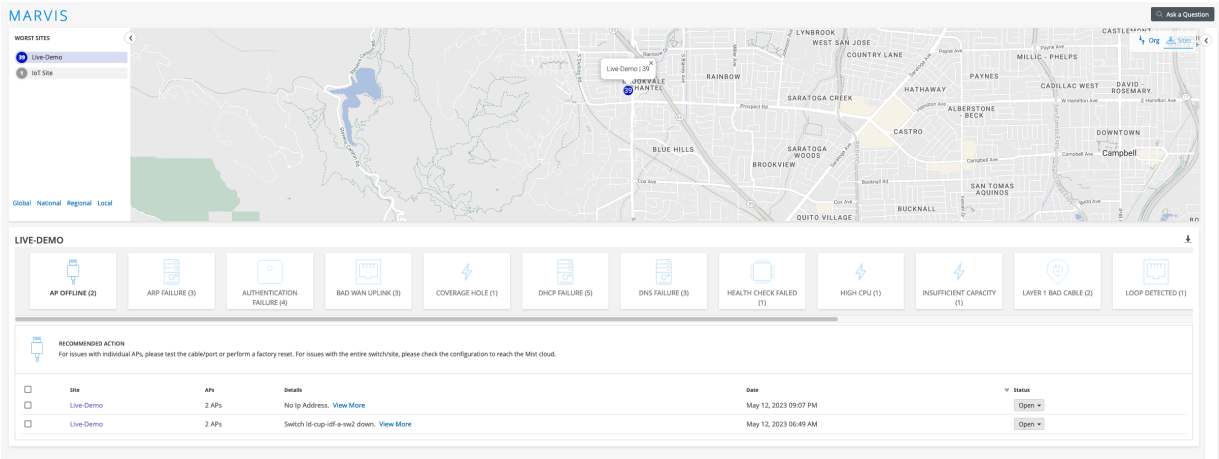
Marvis Actions

Marvis Actions is a one-stop information center that provides visibility into ongoing site-wide network issues that affect user experience in an organization. By default, the landing page of Marvis shows the Actions dashboard for 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.

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



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



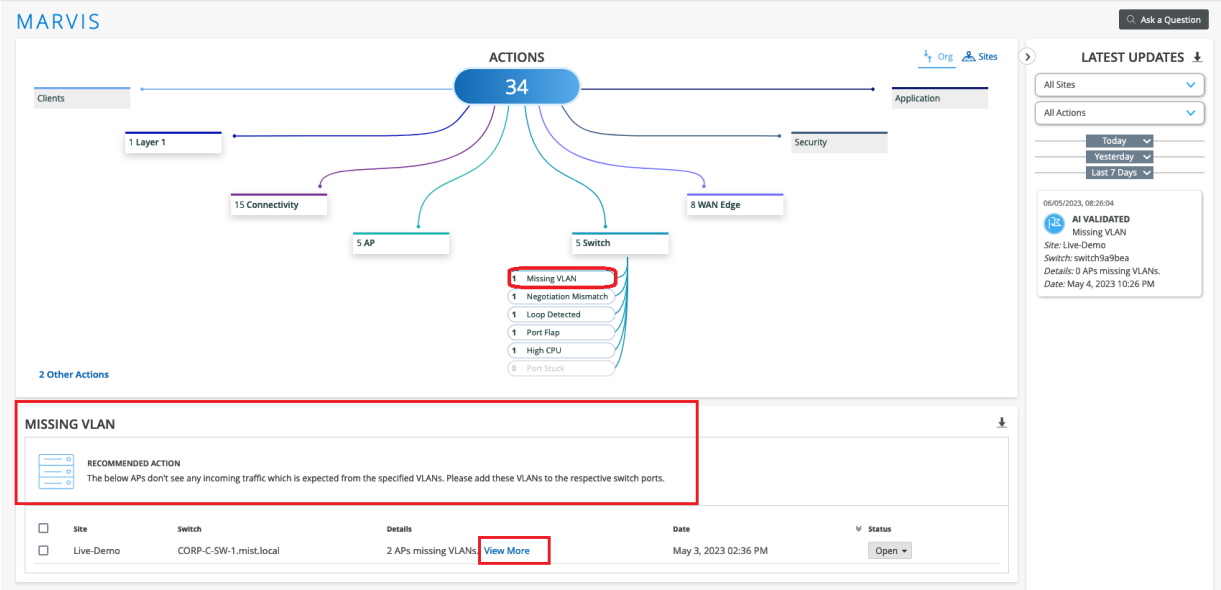
The following sections provide details about the Marvis Actions page.

Detailed View of Issues and Marvis Recommended Actions

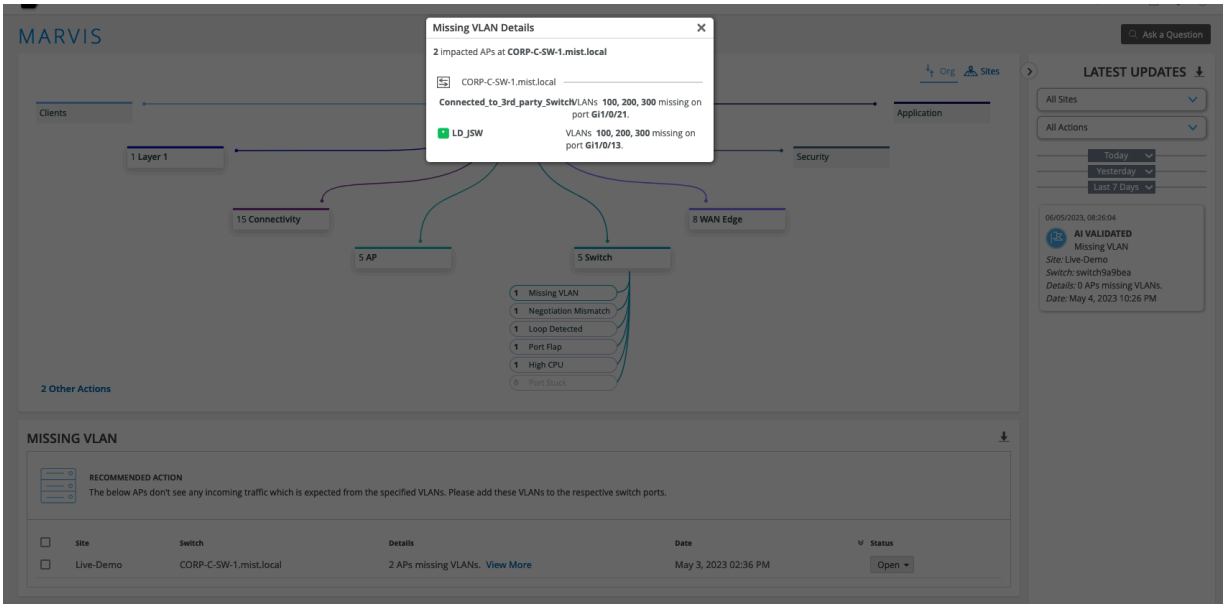
Each category has a group of actions under it. Each action can have one or multiple issues associated with it. If Marvis does not detect any anomalies associated with an action, the action appears dimmed.

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

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



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.

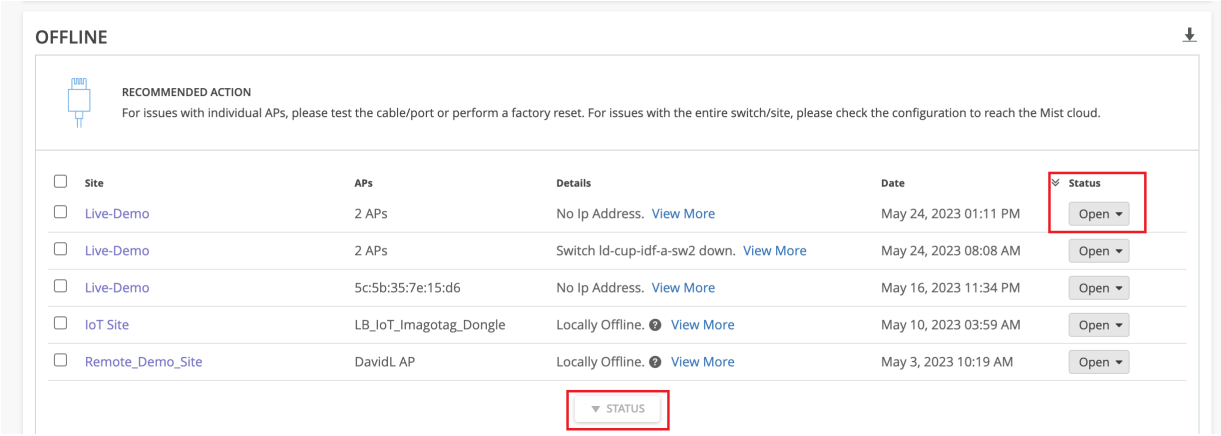


Downloadable List of Issues

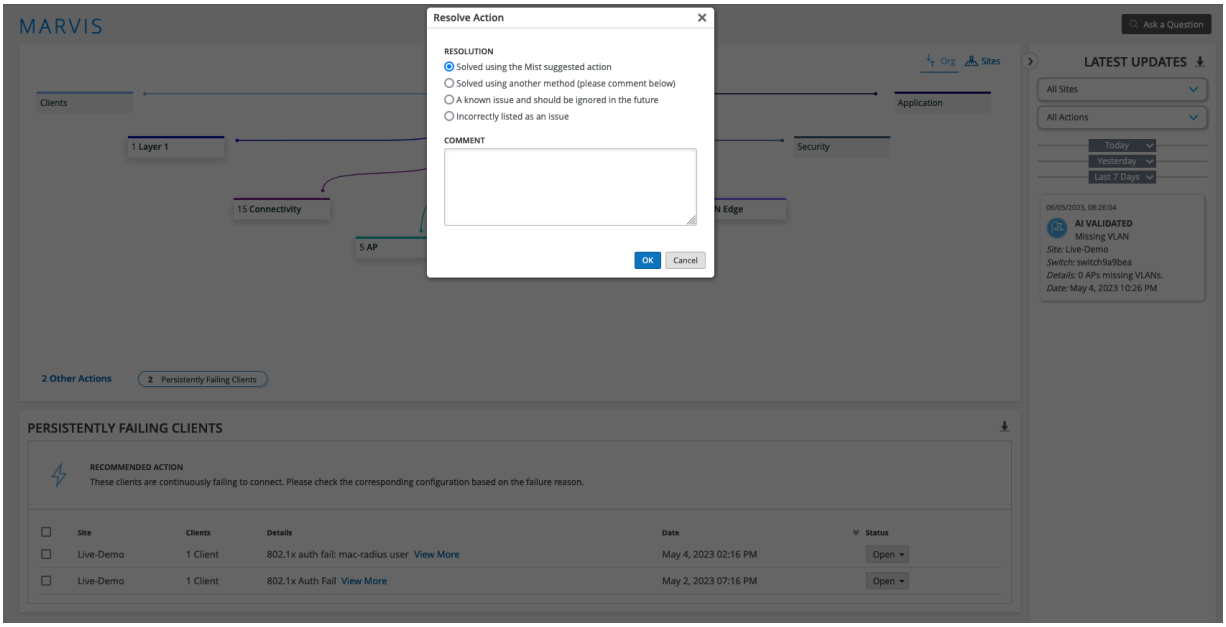
You can download the list of issues to a .CSV file format. The CSV file contains all the details visible on the Actions page, including the reason for failure and the device details. You can find the download (down arrow) icon on the upper-right corner of the Details section.

Issue Resolution

After you resolve an issue, you can change the status of an issue or multiple issues. Use the **STATUS** button at the bottom of the page if you want to change the status of a group of issues.



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

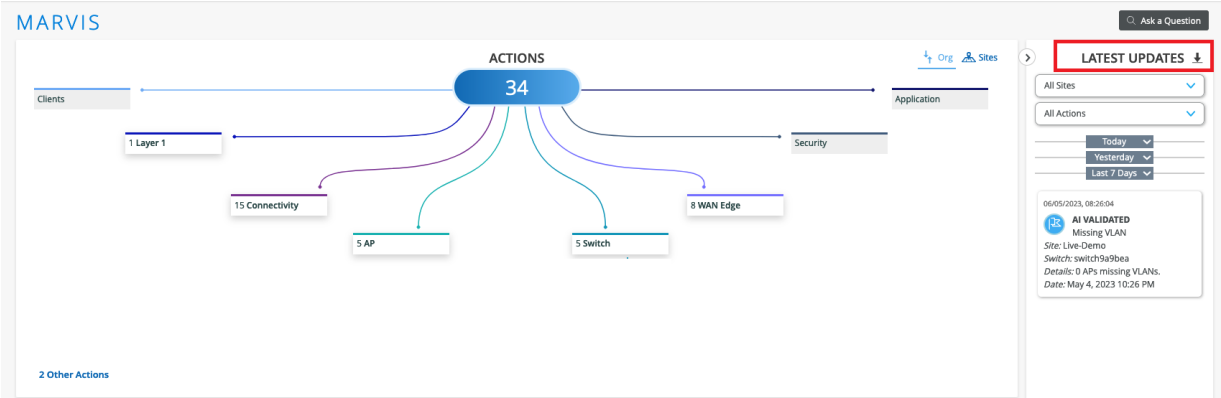


Latest Updates About Issues

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

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

- **Resolved**—Lists automated actions (such as auto upgrade, auto RMA) or manual actions (such as manual AP upgrade or manual RMA request) that completed successfully. Marvis classifies an issue as Resolved only if you trigger the action from the Actions page.
- **Reoccurring Issue**—Lists resolved issues that are either still not resolved or have reoccurred. At times, Marvis might find that an issue you marked as resolved is still not resolved completely. Marvis then classifies the issue as a reoccurring issue.



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

This video provides an introduction to Marvis Actions.

Video:

Marvis Actions for Wired, WAN, and Wireless Assurance

The type of subscription you have for your organization determines the Marvis Actions usage. The following three subscription types are required for Marvis Actions:

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

Table 1 on page 10 lists the actions available for each subscription type.

You can view Marvis Actions based on the active Marvis subscription types. The number of subscriptions for each Marvis subscription type (Wired, Wireless, or WAN) must be greater than 50 percent of the number of devices of the corresponding device type in the inventory. For example, if you have six APs in the inventory, you must have four or more active **Marvis for Wireless** subscriptions to be able to view all the categories applicable for the **Marvis for Wireless** subscription as listed in Table 1 on page 10.

Marvis Actions will be enabled on the Mist portal as long as the number of subscriptions is greater than 50 percent of the number of corresponding devices in the inventory.

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

Table 1: Marvis Actions for Wired, WAN, and Wireless Assurance

Category	Action	Marvis for Wired	Marvis for WAN	Marvis for Wireless
Layer 1	Bad Cable	x	x	✓
Connectivity	Authentication Failure	✓	x	✓
	DHCP Failure	✓	x	✓
	ARP Failure	x	x	✓
	DNS Failure	x	x	✓
AP	Offline	x	x	✓
	Health Check Failed	x	x	✓
	Non-compliant	x	x	✓
	Coverage Hole	x	x	✓
	Insufficient Capacity	x	x	✓
Switch	Missing VLAN	x	x	✓
	Negotiation Mismatch	✓	x	x
	Loop Detected	✓	x	x

Table 1: Marvis Actions for Wired, WAN, and Wireless Assurance *(Continued)*

Category	Action	Marvis for Wired	Marvis for WAN	Marvis for Wireless
	Port Flap	✓	x	x
	High CPU	✓	x	x
	Port Stuck	✓	x	x
	Traffic Anomaly	✓	x	x
Other Actions	Persistently Failing Clients	✓	x	✓
WAN Edge	MTU Mismatch	x	✓	x
	Bad WAN Uplink	x	✓	x
	VPN Path Down	x	✓	x

Marvis Actions for Switches

IN THIS SECTION

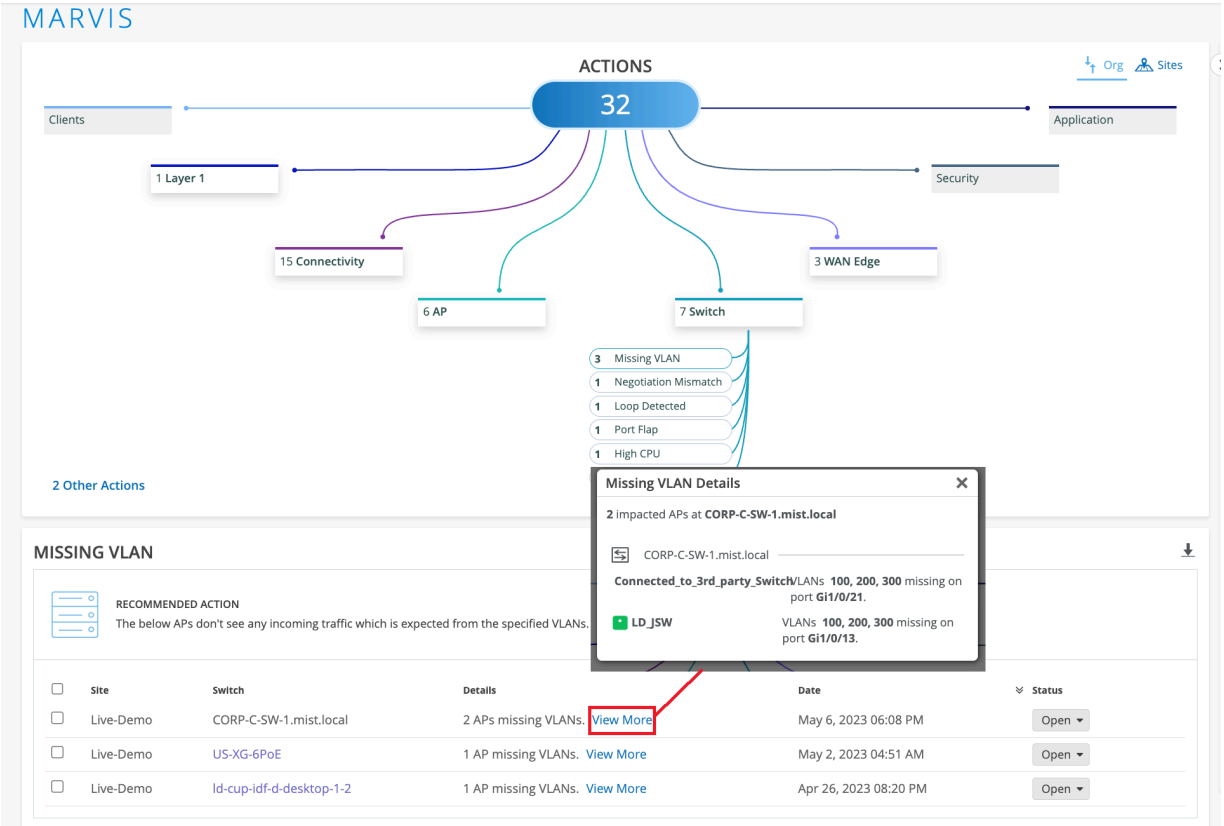
- Missing VLAN | 12
- Negotiation Mismatch | 13
- Loop Detected | 14
- Port Flap | 15
- High CPU | 17
- Port Stuck | 17
- Traffic Anomaly | 18

For switches, Marvis identifies issues such as mismatched port settings, Layer 2 (L2) loops, and continuous port flaps with an option to disable the port.

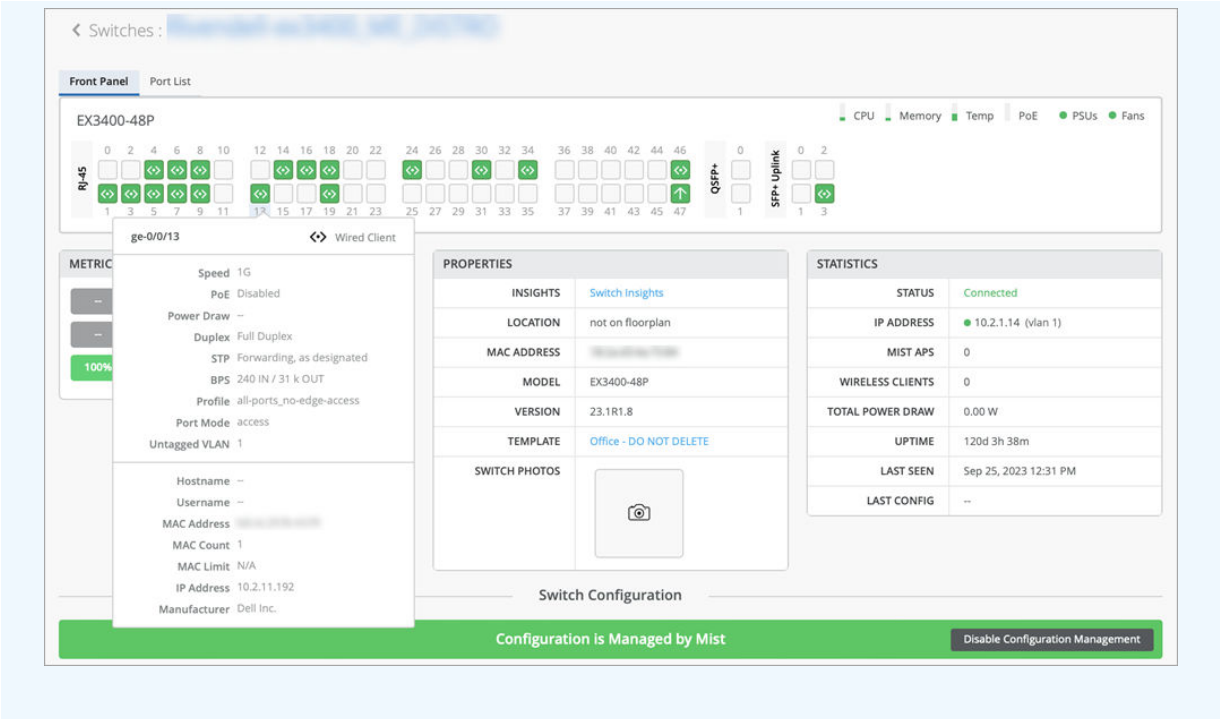
Missing VLAN

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

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



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 and appear in the Latest Updates section.

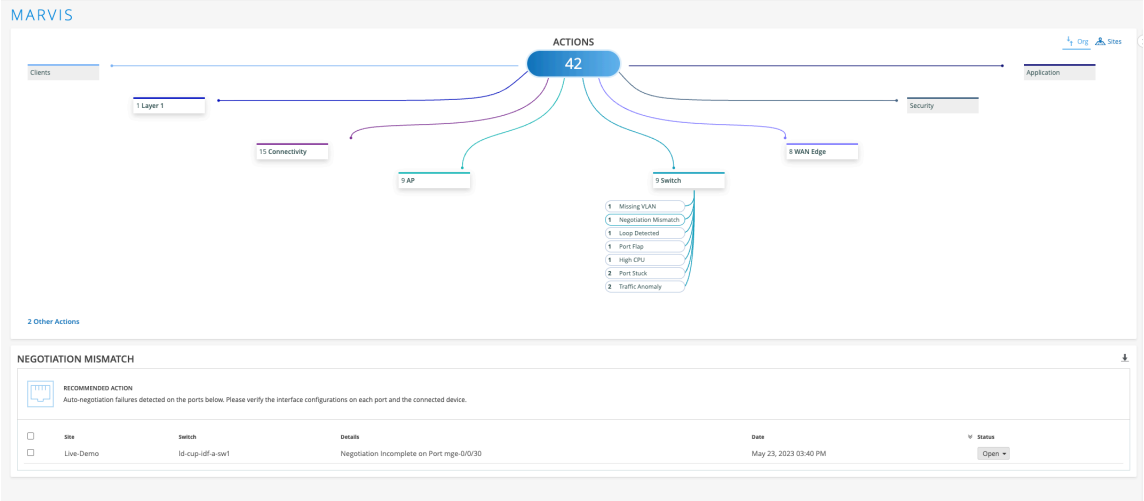
For more information about the Missing VLAN action, watch the following video:

Video:

Negotiation Mismatch

The Negotiation Mismatch action detects instances on switch ports where negotiation is incomplete. 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 Mismatch action. Notice that Marvis lists the switch and the port on which the negotiation mismatch occurred.

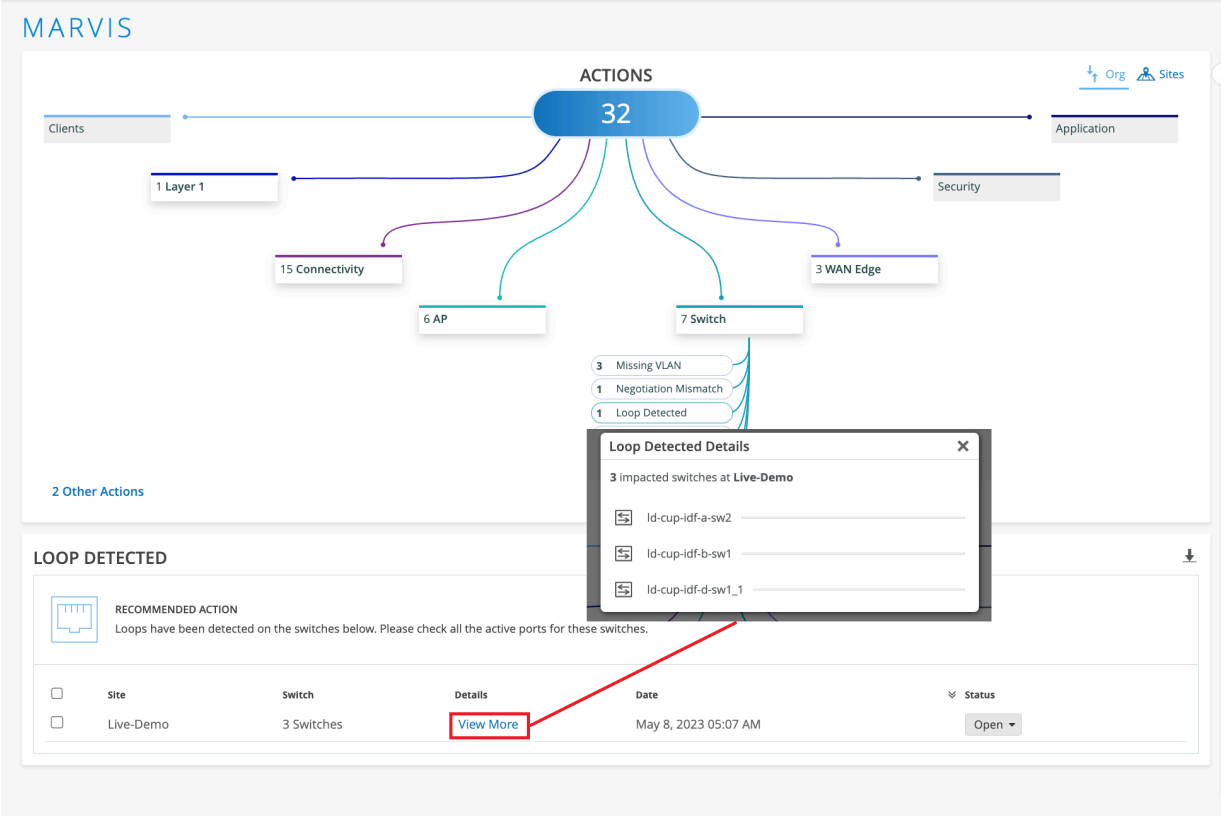


After you fix the issue in your network, the Negotiation Mismatch action automatically resolves and appears in the Latest Updates section within an hour.

Loop Detected

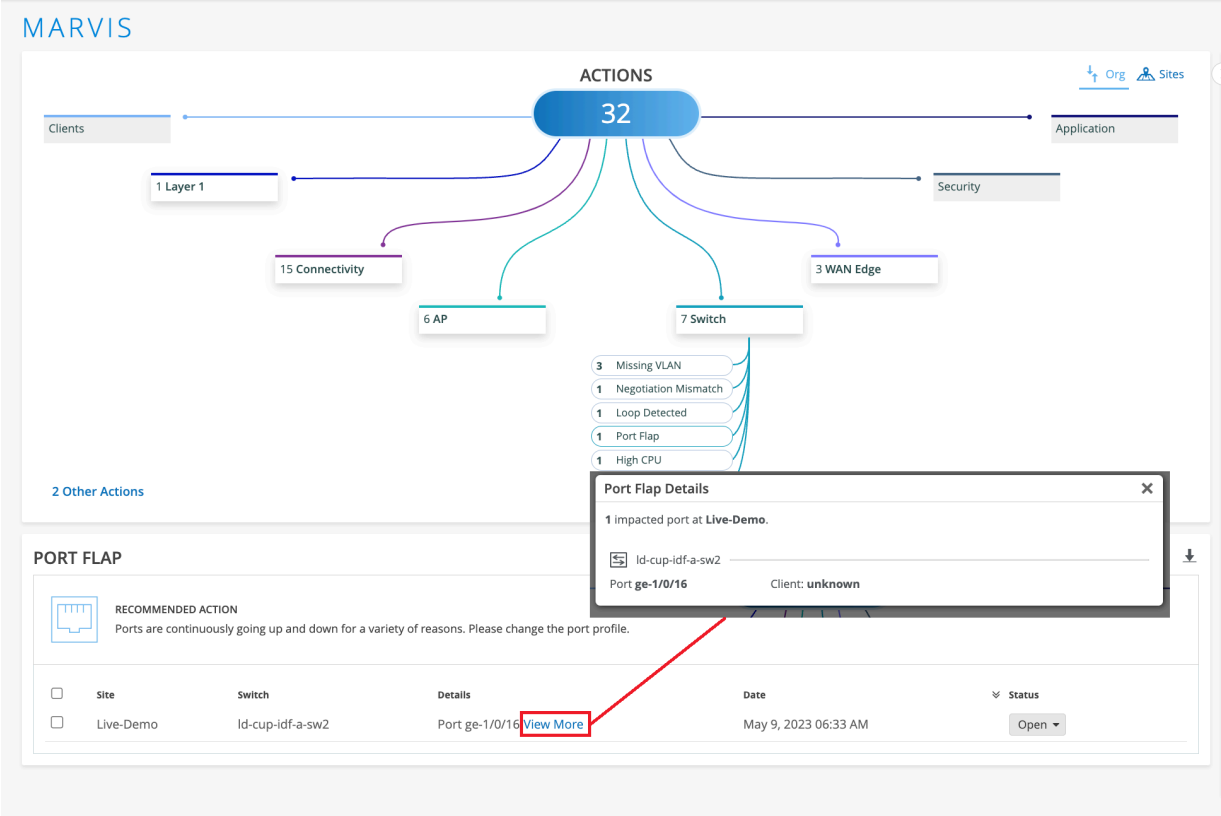
The Loop Detected action indicates a loop in your network resulting in the switch receiving the same packet that it sent out. A loop occurs when multiple links exist between devices. Redundant links are a common cause for L2 loops. A redundant link serves as a backup link for the primary link. If both 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:

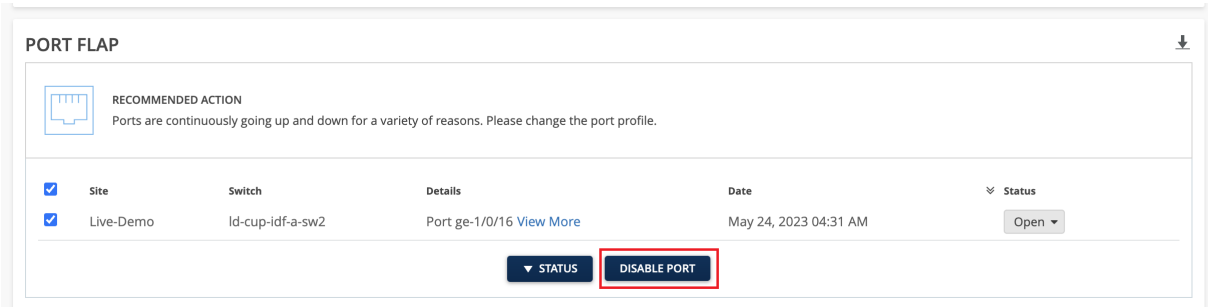


Port Flap

The Port Flap action identifies ports that bounce persistently over a short time interval, indicating that a port or client has an issue. Port flapping 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 a Port Flap action:



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



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

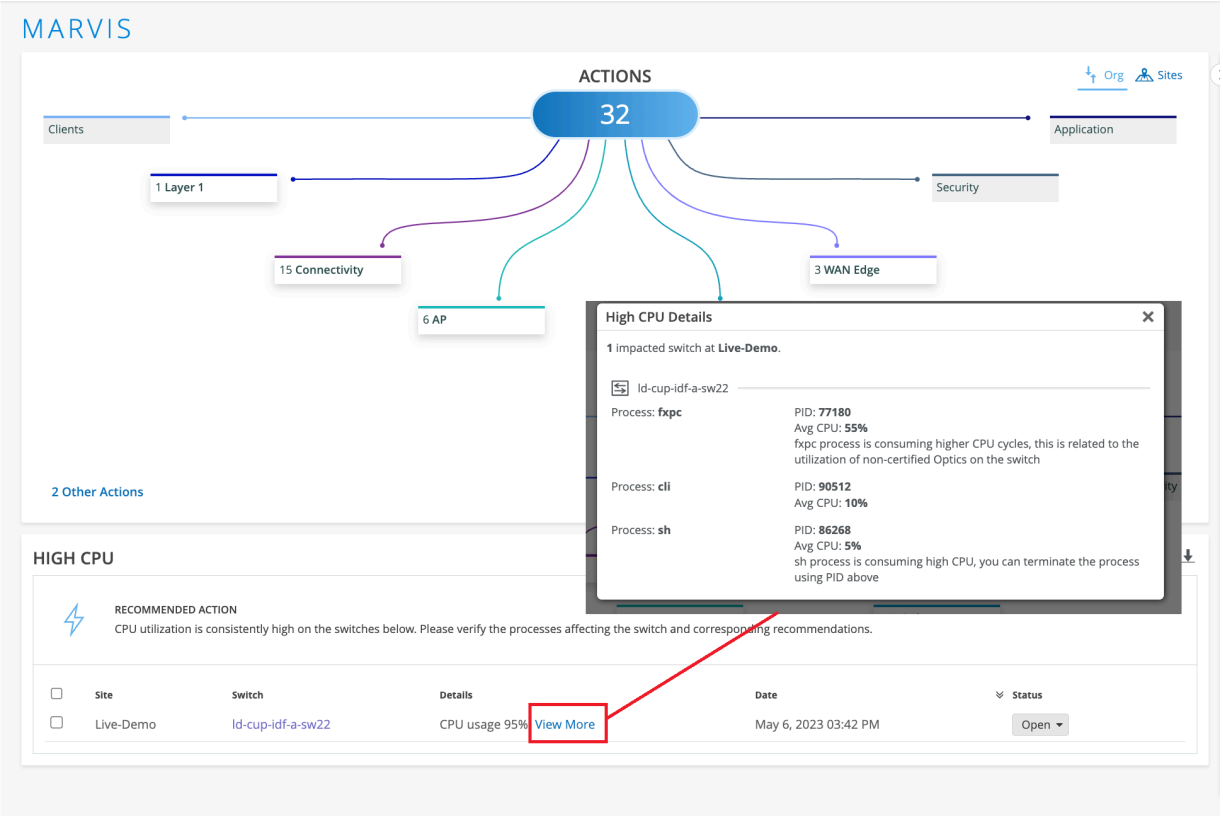
When you disable a port, the port configurations on the selected ports change to disabled and the ports go down. After you fix the issue, you can re-enable these ports by editing the port configuration on the Switch Details page. After you re-enable the ports, you can reconnect the devices to the ports.

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

Video:

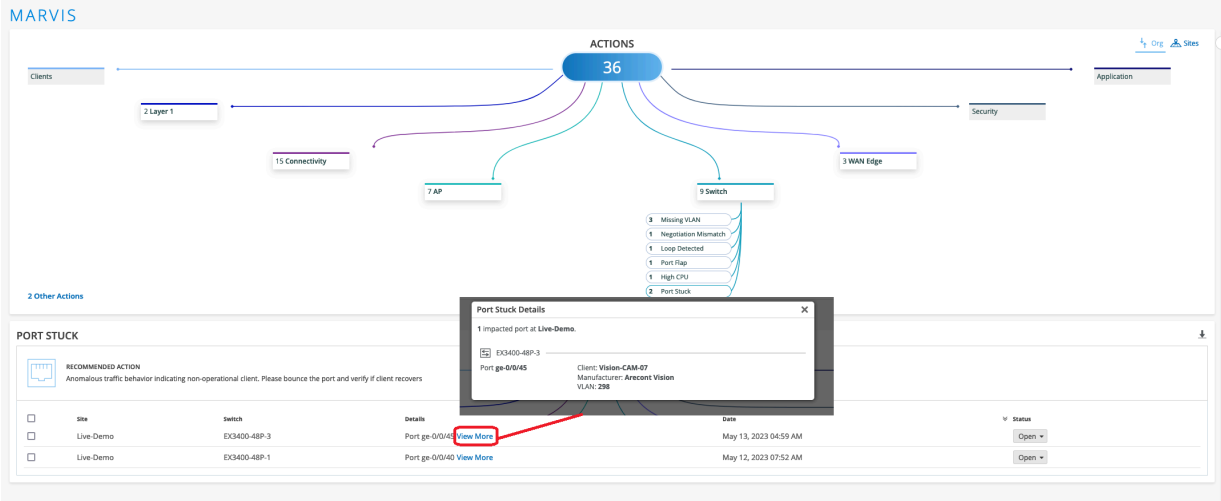
High CPU

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



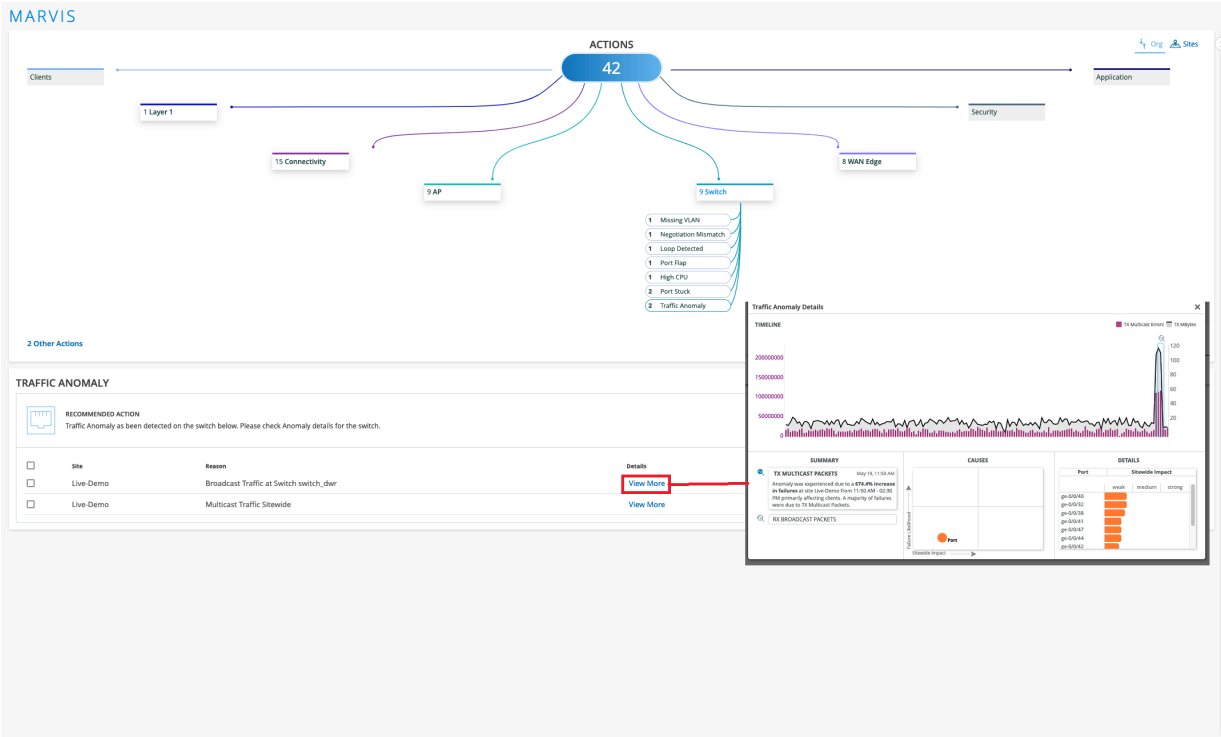
Port Stuck

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



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 Actions for Layer 1 Connectivity

IN THIS SECTION

- Bad Cable | 19

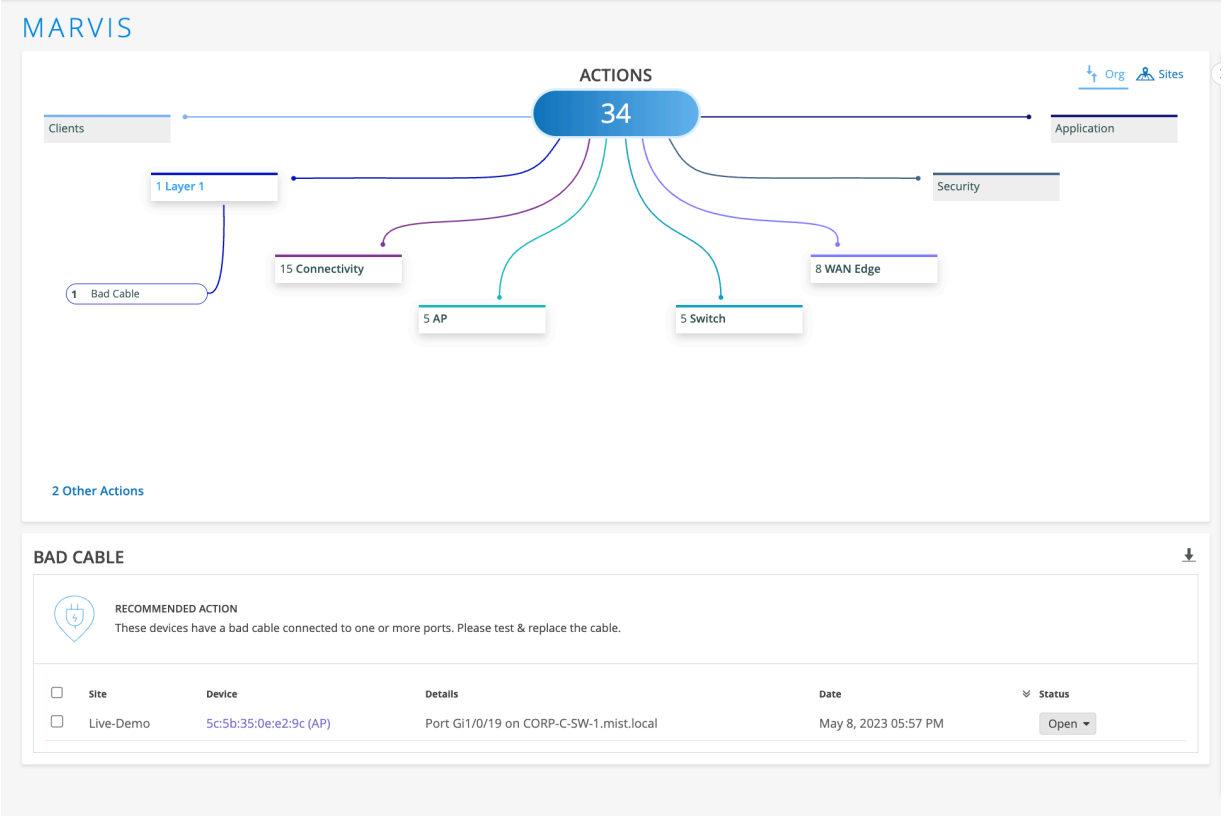
Marvis can detect a faulty cable that is connected to an access point (AP), a switch, or a WAN Edge device.

Bad Cable

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.

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 and appear in the Latest Updates section.

Video:

Marvis Actions for WAN Edge Devices

IN THIS SECTION

- MTU Mismatch | 21
- Bad WAN Uplink | 21
- VPN Path Down | 22

Marvis Actions provides proactive recommendations for WAN issues such as maximum transmission unit (MTU) mismatches, bad cables, and WAN link congestion and outages.

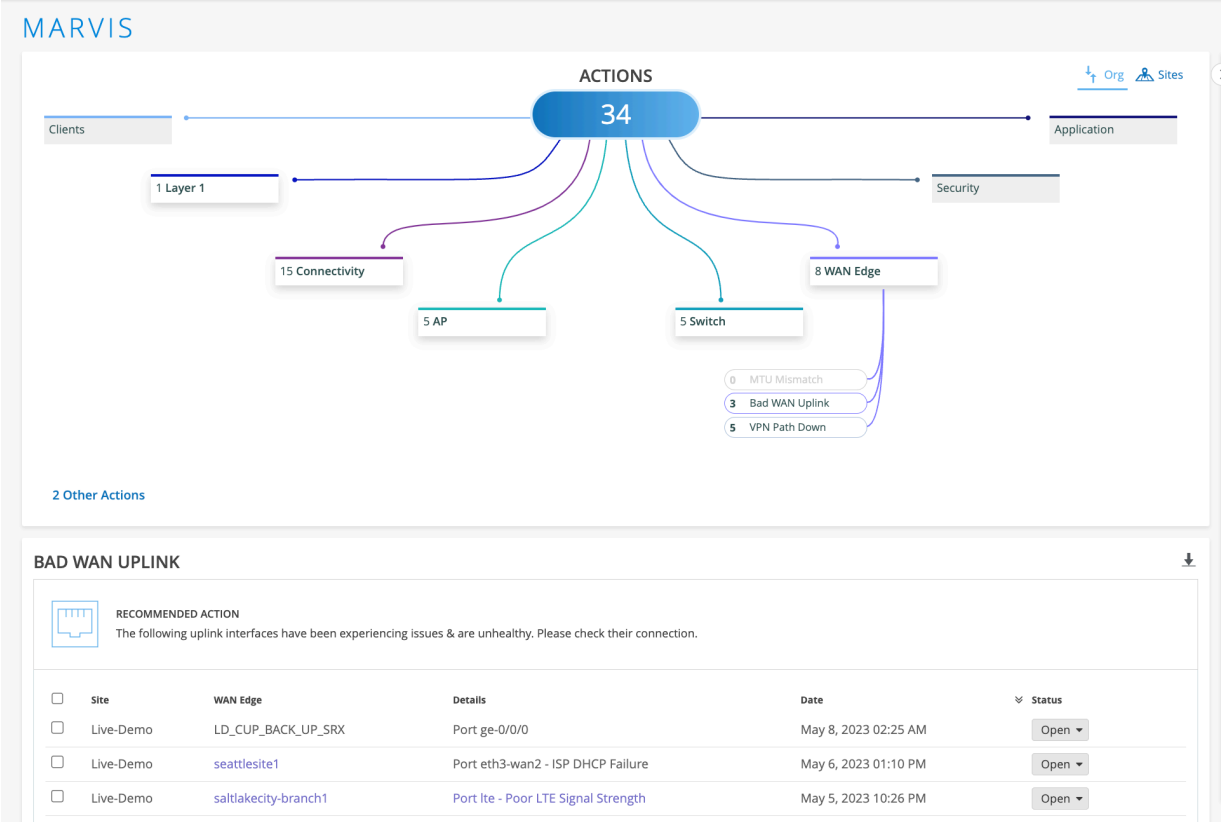
MTU Mismatch

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.

Bad WAN Uplink

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

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



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

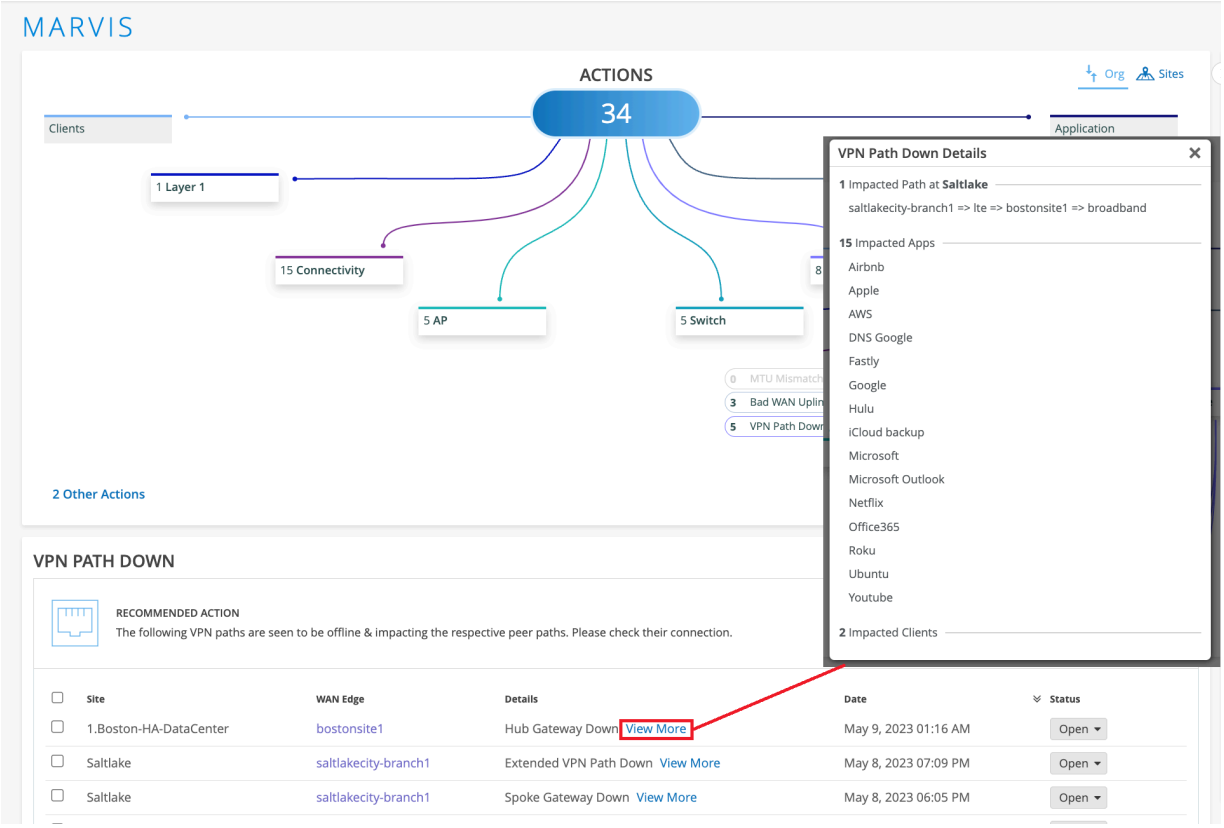
- Received signal strength indicator (RSSI)
- Reference Signal Received Power (RSRP)
- Signal-to-noise ratio (SNR)

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

VPN Path Down

Marvis monitors the VPN paths that are associated with WAN edge nodes (Juniper Networks® SRX Series Firewall or Session Smart™ Router) in the overlay network. If a VPN tunnel goes 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.



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

Marvis Actions for Client Connectivity Failures

IN THIS SECTION

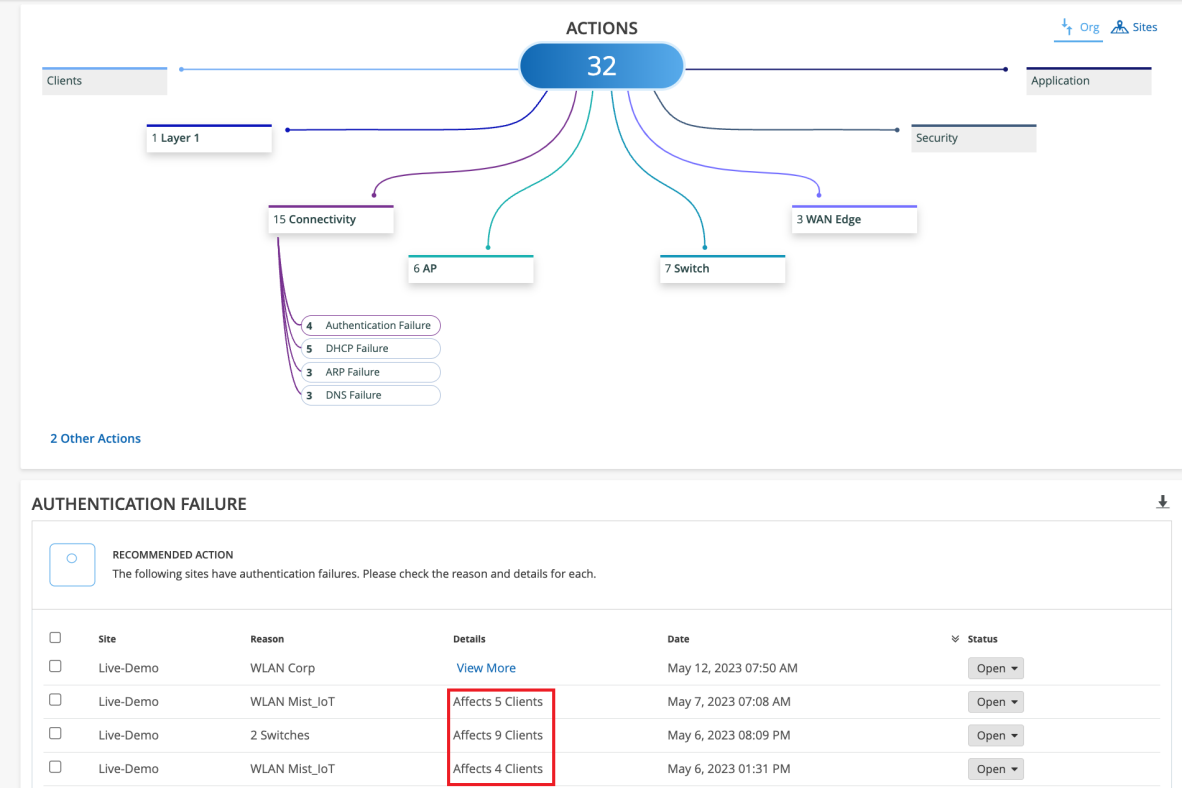
- Authentication Failure | 25
- DHCP Failure | 26
- ARP Failure | 27
- DNS Failure | 27

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 36.

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

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



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

Authentication Failure

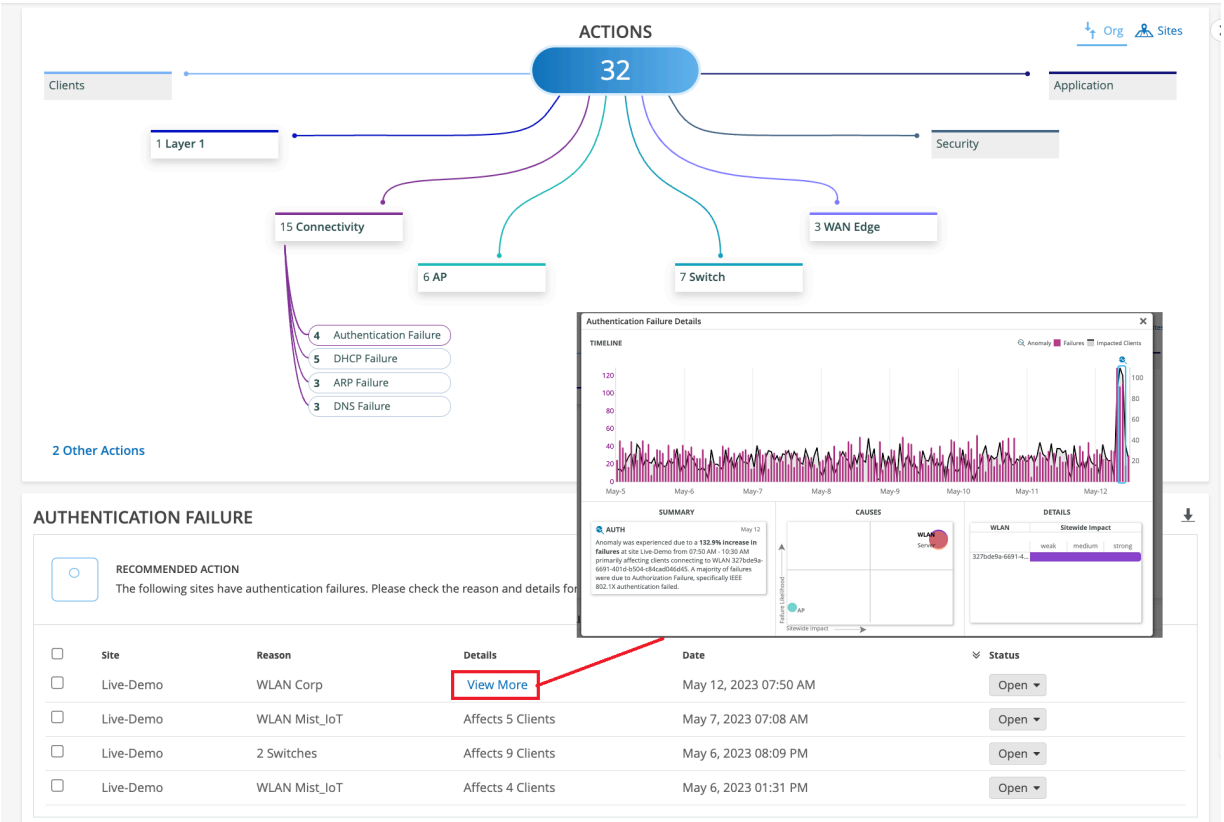
The Authentication Failure action shows both 802.1x and preshared key (PSK) failures.

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:



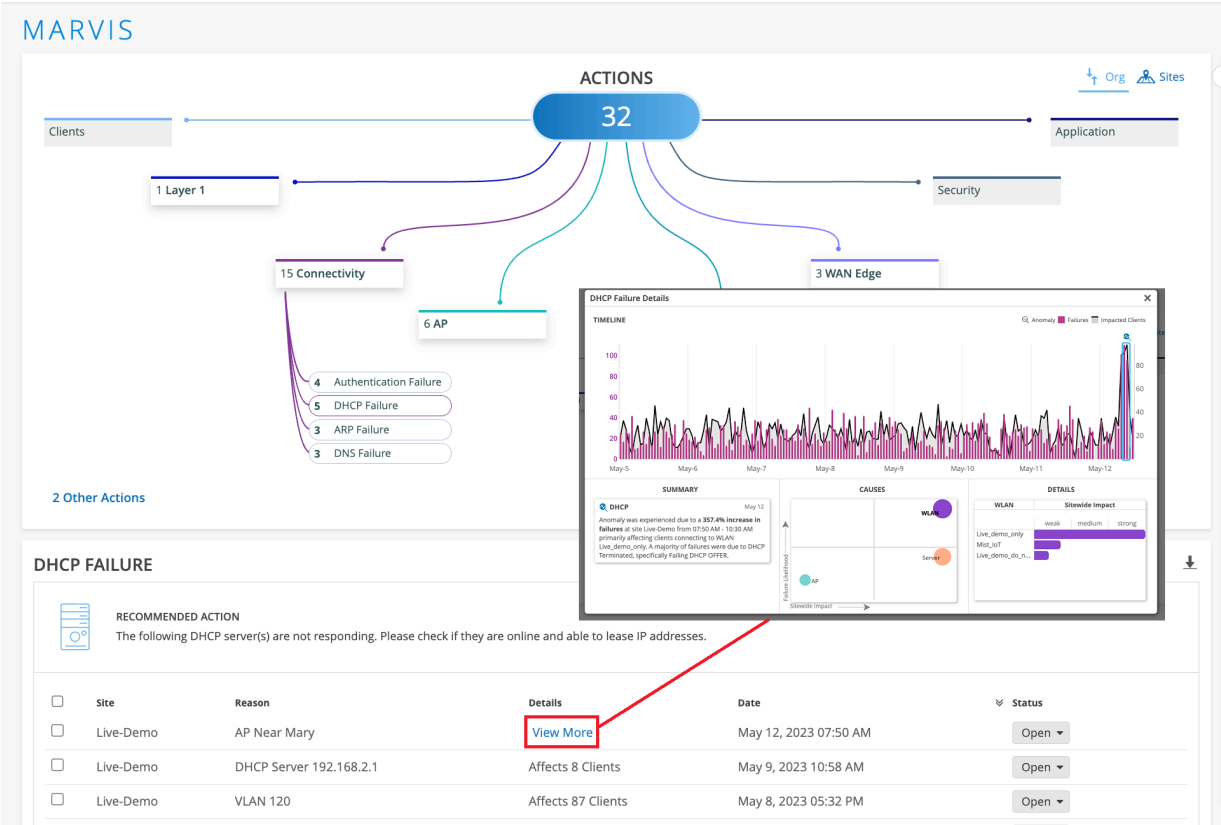
NOTE: Marvis detects authentication failures even in wired-only deployments.

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

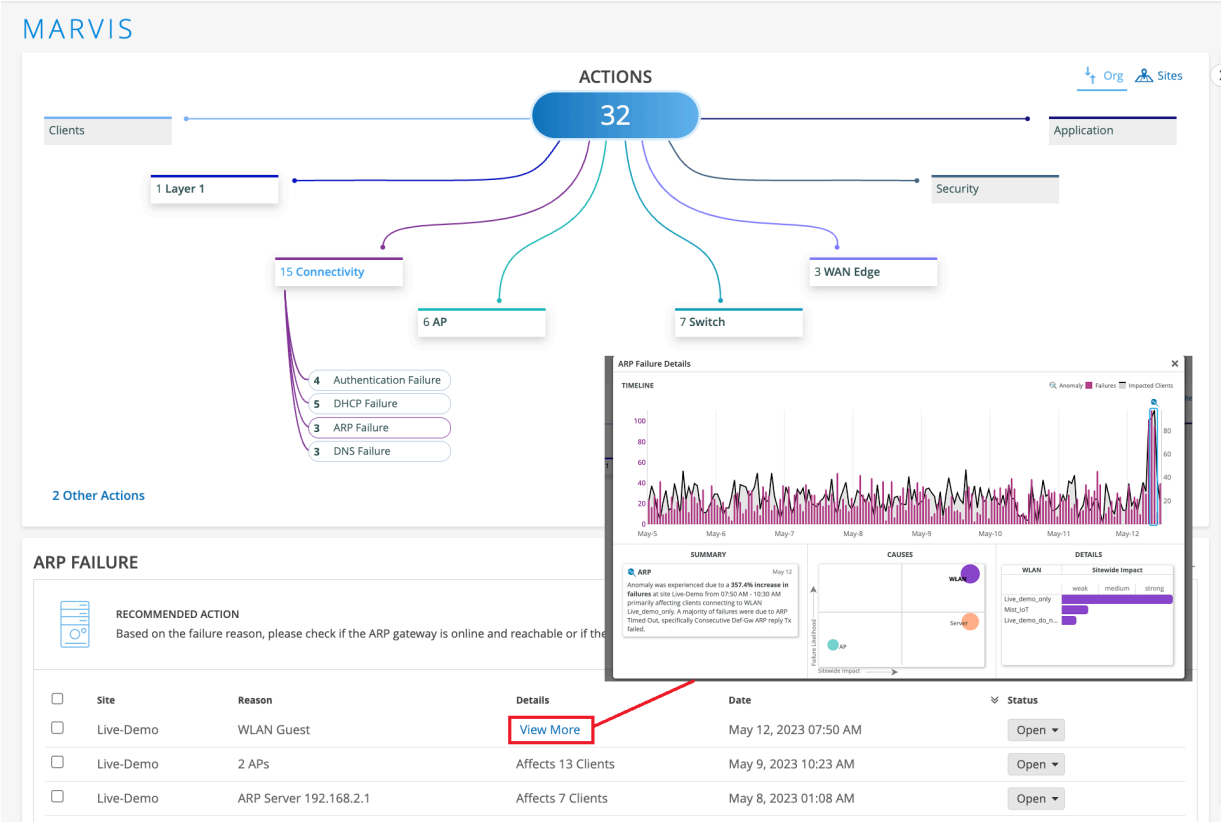
The DHCP Failure action appears when Marvis detects DHCP failures due to offline or unresponsive DHCP servers. Marvis provides details about these DHCP servers, thus enabling you to troubleshoot and resolve the problem quickly. When you see a DHCP Failure action, ensure that the DHCP servers are online and can lease IP addresses. Note that for wired-only deployments, you must enable DHCP snooping for Marvis to detect DHCP failures.



NOTE: Marvis detects DHCP failures even in wired-only deployments.

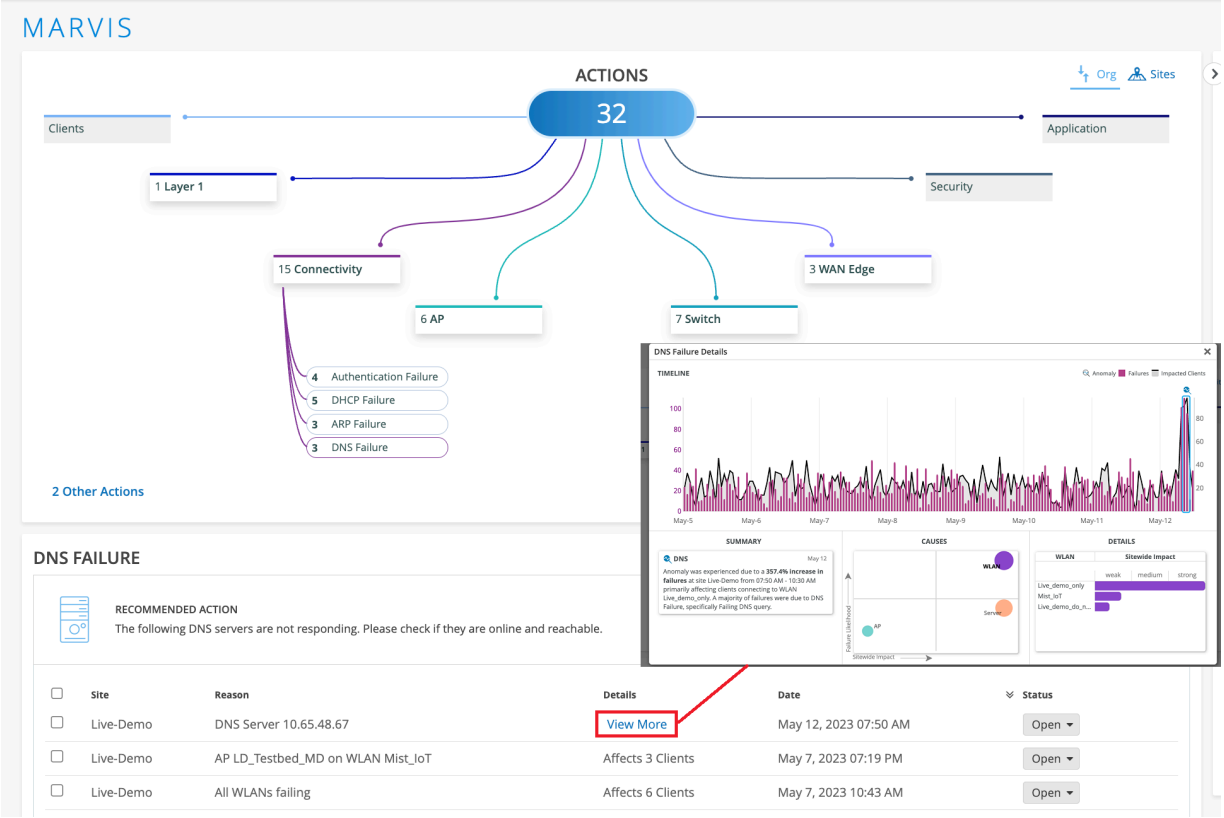
ARP Failure

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



Marvis Actions for APs

IN THIS SECTION

- Offline | 29
- Health Check Failed | 30
- Non-Compliant | 31
- Coverage Hole | 31
- Insufficient Capacity | 33

Marvis Actions can perform a number of tasks, as follows:

- Helps detect access points (APs) running an older firmware version.

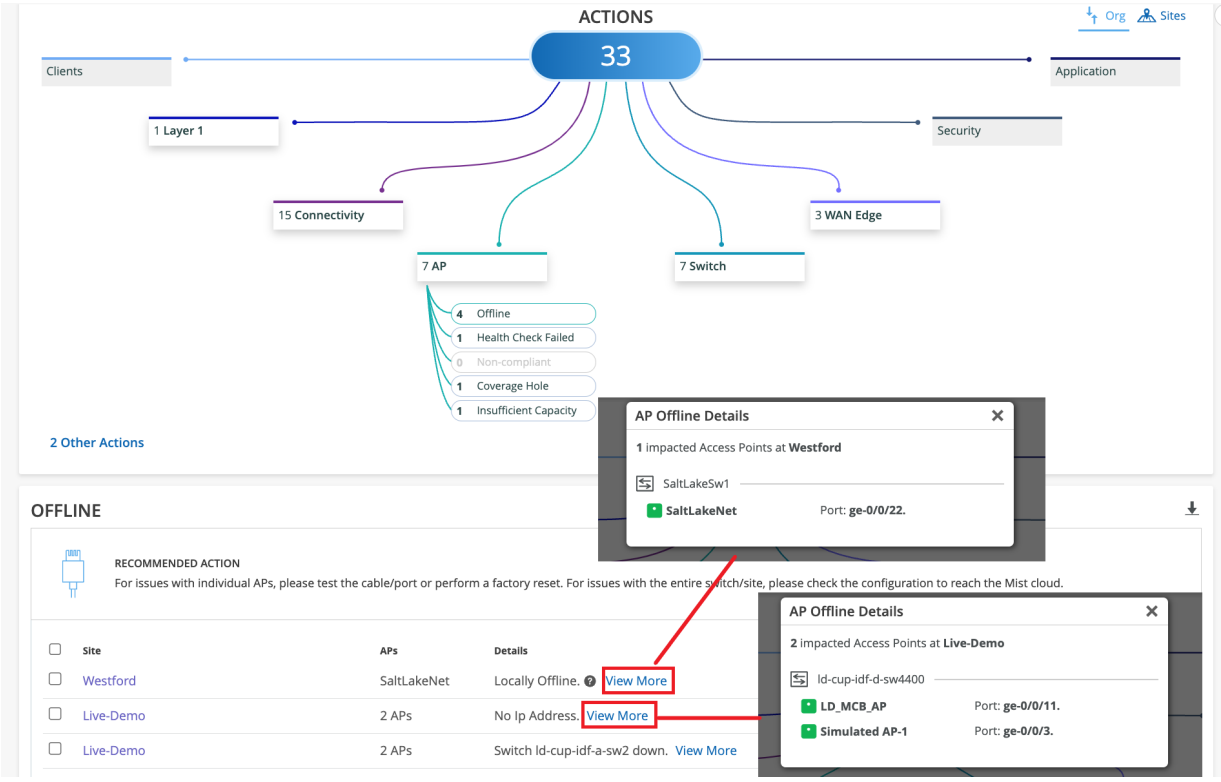
- Provides root causes and reasons for failure when an AP is offline.
- Detects coverage issues.
- Detects APs or locations with insufficient capacities.

Offline

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

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

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

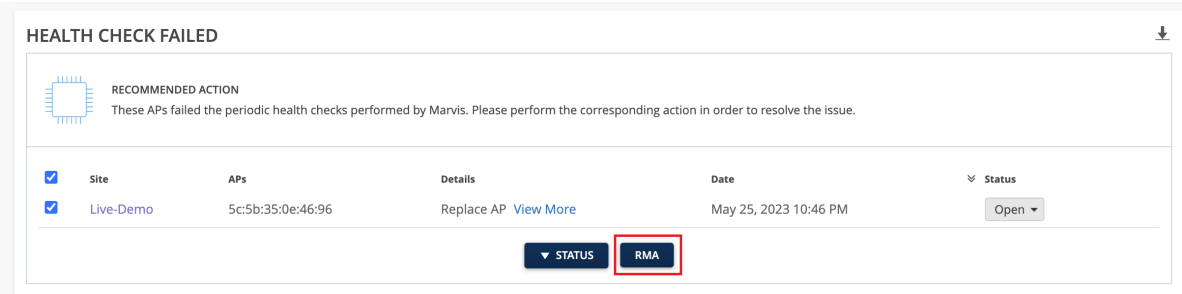


Health Check Failed

Marvis monitors the APs across all sites in your organization for potential hardware or software issues. Marvis shows the Health Check Failed action on your dashboard if it detects an AP experiencing:

- Issues that cannot be debugged, meaning that the AP needs to be replaced.

  You can request replacement of an AP directly from the Marvis Actions page by using the **RMA** button. You'll need to complete the form with your shipping address and contact information, and a representative from the support team will contact you.

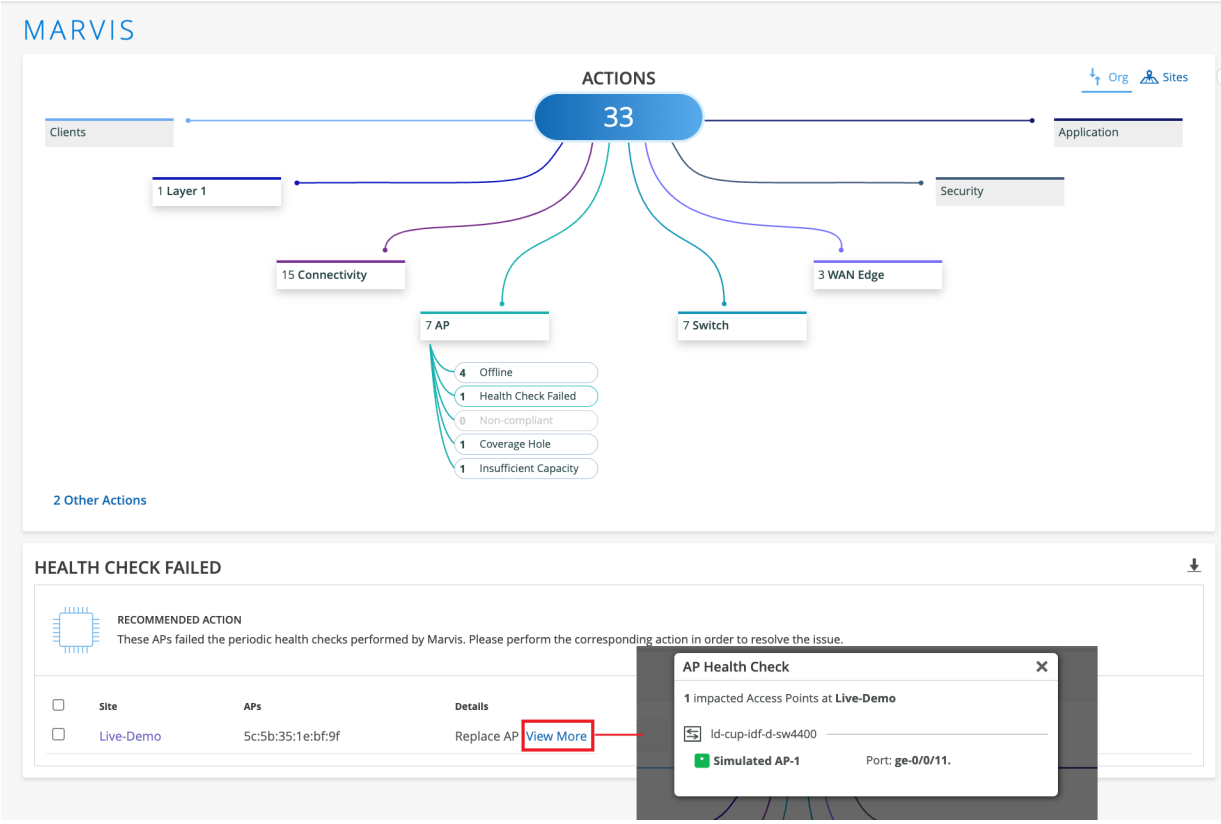


- A software issue that a newer firmware resolves.

  You can use the **Upgrade** button to upgrade the firmware directly from this page.

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

In the following example, Marvis identifies an AP that failed the periodic health checks and highlights the need to replace the AP:



Non-Compliant

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

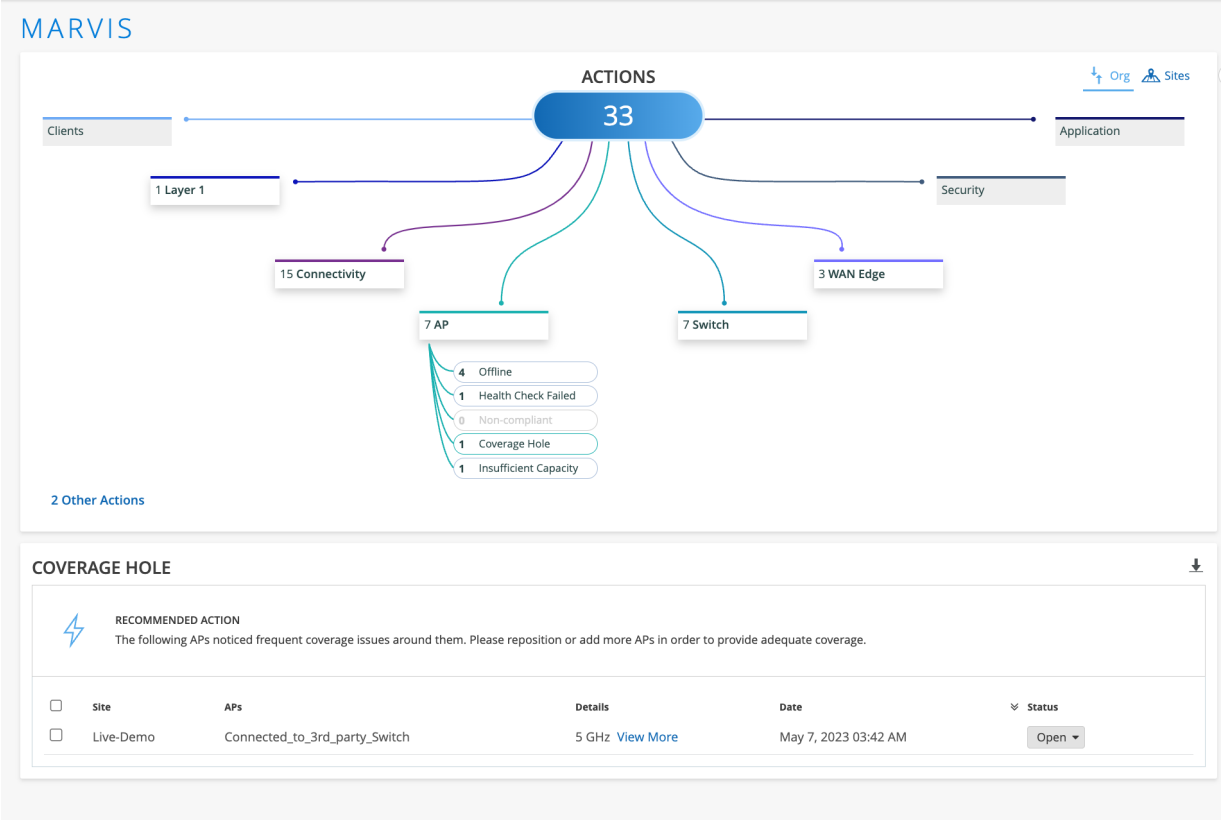
After you upgrade the APs to the proper version, the Non-Compliant action automatically resolves and appears in the Latest Updates section within 30 minutes.

Coverage Hole

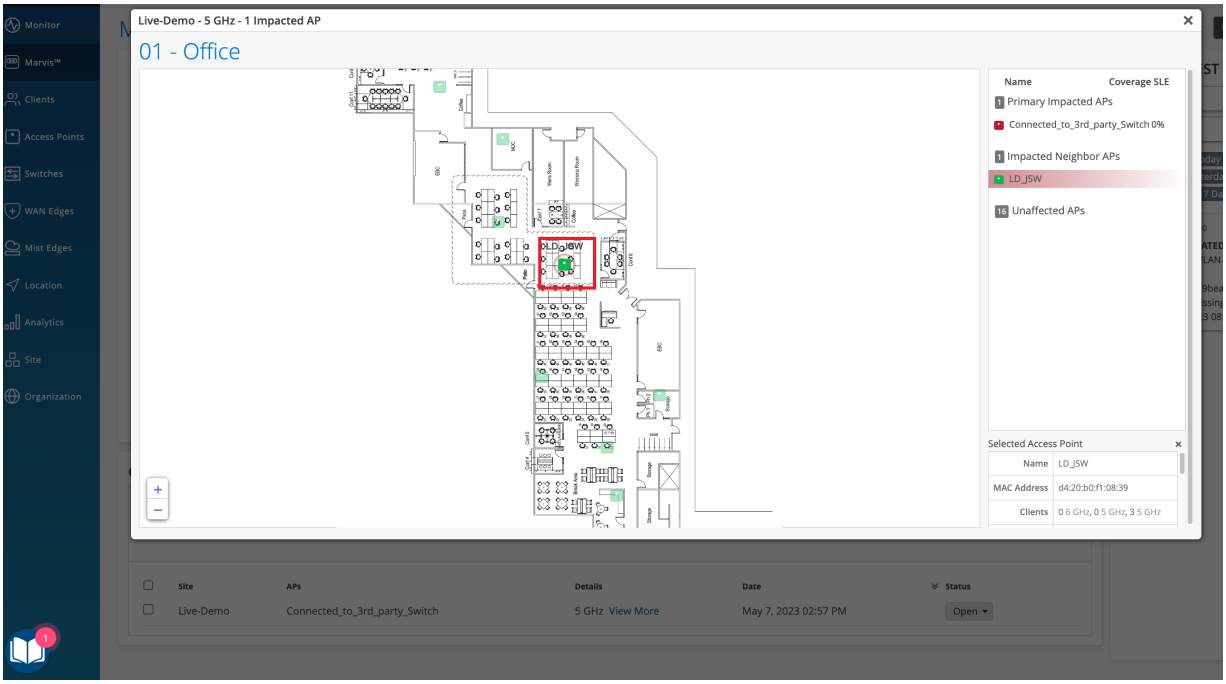
The Coverage Hole action detects coverage issues at your site and provides a floor plan visual indicating the APs experiencing these issues. You can use this visual representation to locate areas with low coverage and make necessary improvements such as adding APs, upgrading AP models, changing the placement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

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

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



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

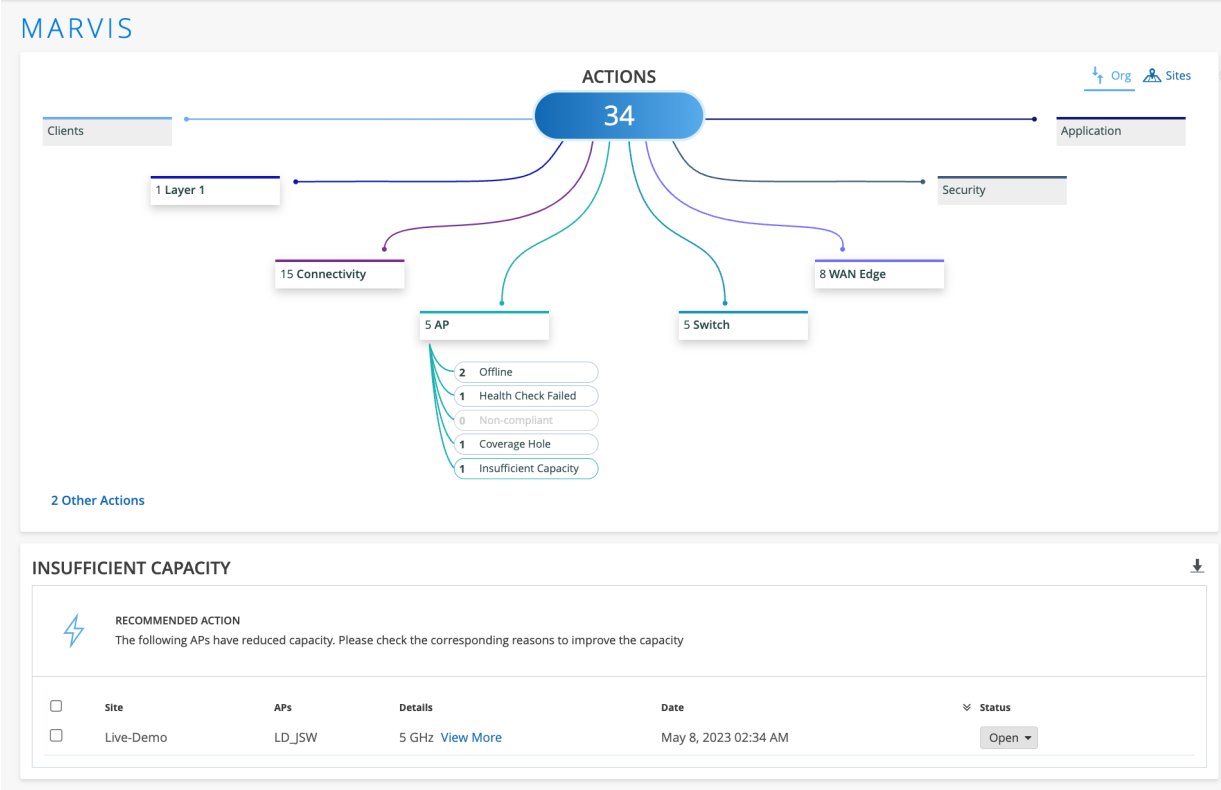


After you fix the issue in your network, Mist AI monitors the network for a certain period and ensures that the coverage is sufficient for the network. Hence, it might take up to 24 hours for the Coverage Hole action to automatically resolve and appear in the Latest Updates section.

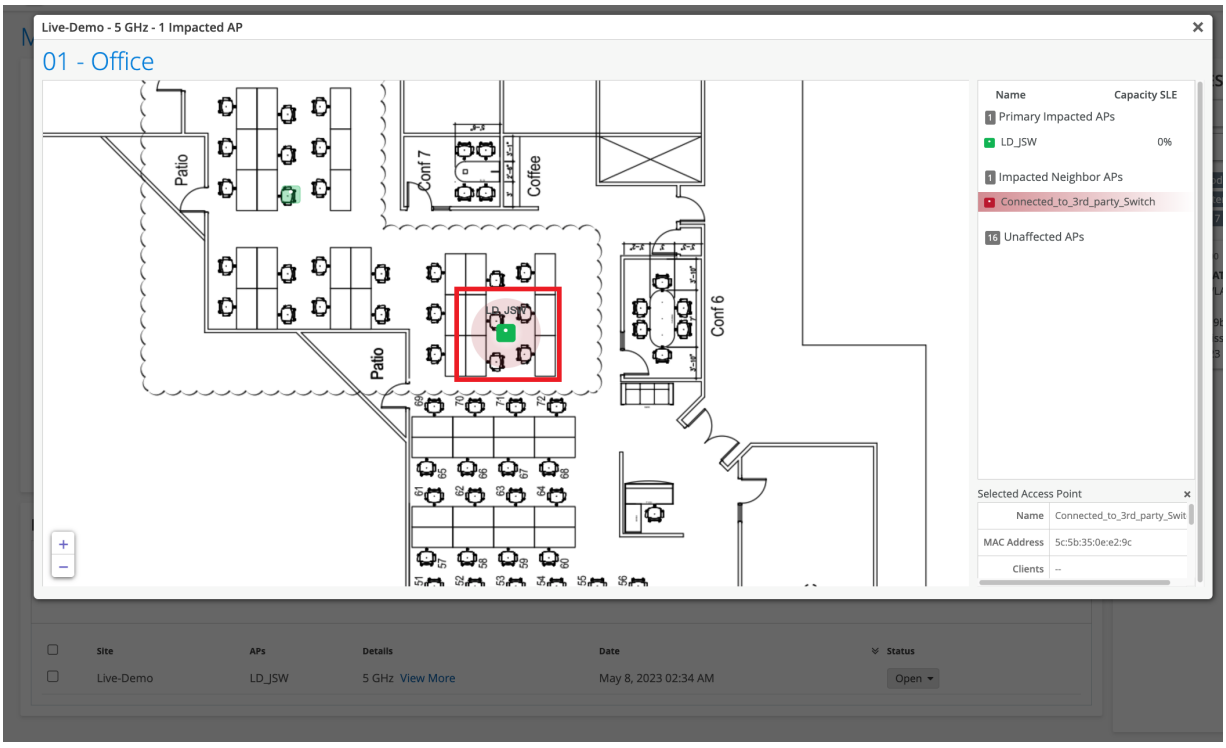
Insufficient Capacity

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

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



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



Other Marvis Actions

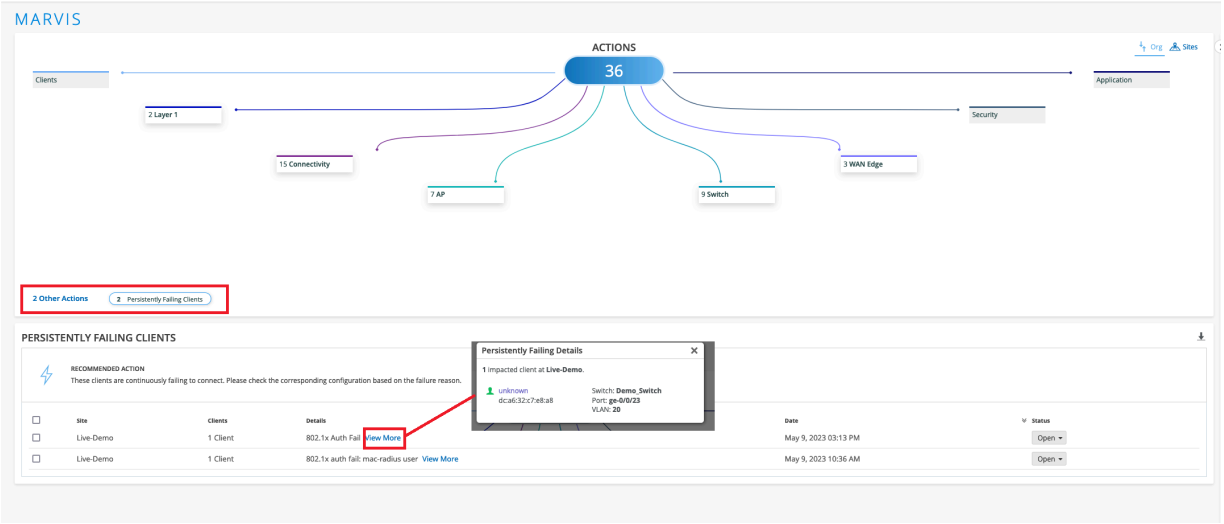
IN THIS SECTION

- Persistently Failing Clients | 35

You can view Other Actions below the Actions section. The Other Actions category lists low-priority issues that don't require immediate attention.

Persistently Failing Clients

The Persistently Failing Clients action highlights 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. As this action is considered low priority, Marvis does not list the Persistently Failing Clients action in the Latest Updates section or on the Sites tab.

Video:

Anomaly Detection Event Card

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 failures such as authentication, Domain Name System (DNS), and Dynamic Host Control Protocol (DHCP) failures. Authentication failures can include Extensible Authentication Protocol (EAP), 802.1x, and preshared key (PSK). To open an Event Card, navigate to one of the recommendations and click **View More**. The Event Card categorizes the information under the following four sections:

- **Timeline**—Shows a timeline view of the number of failure events corresponding to the number of affected clients during a time period. Marvis highlights the anomalies with a magnifying glass icon. Click the icon to select an anomaly and view the details.
- **Summary**—Provides 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**—Provides a graphical representation of the impact between 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**—Provides an in-depth view of the sitewide impact from each AP, WLAN, or radio band that you select in the **Causes** section.

Here's a sample Event Card that provides information about a DNS failure. You can see one anomaly. Selecting the WLAN circle in the **Causes** section displays the list of WLANs that contributed to the anomaly. In this example, you can see that the *Live_demo_only* WLAN has a stronger impact on this anomaly than other WLANs have. Similarly, if you select the AP circle, the **Details** section shows the list of APs associated with this anomaly.

Watch this video to learn more:

Video:

3

CHAPTER

Marvis Query Language

Marvis Query Language Overview | 39

Troubleshoot Using Marvis Query Language | 40

Marvis Query Language Overview

IN THIS SECTION

- Marvis Query Structure | 39

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.

You can start the query process by clicking the **Ask a Question** link in the upper-right corner of the Marvis page.

Marvis Query Structure

You can build a query in Marvis easily. You click inside the **Enter a query** text box to start and Marvis displays the available Query Types. A Query Type defines what you want Marvis to do. You can select each component of the query by following the hint text displayed below the text box. Marvis displays a drop-down list from which you can choose each query element. Each query element you choose determines the subsequent query elements. You can build the query step by step this way until it is complete. When your query is complete, you can run the query by pressing the **Enter** key.

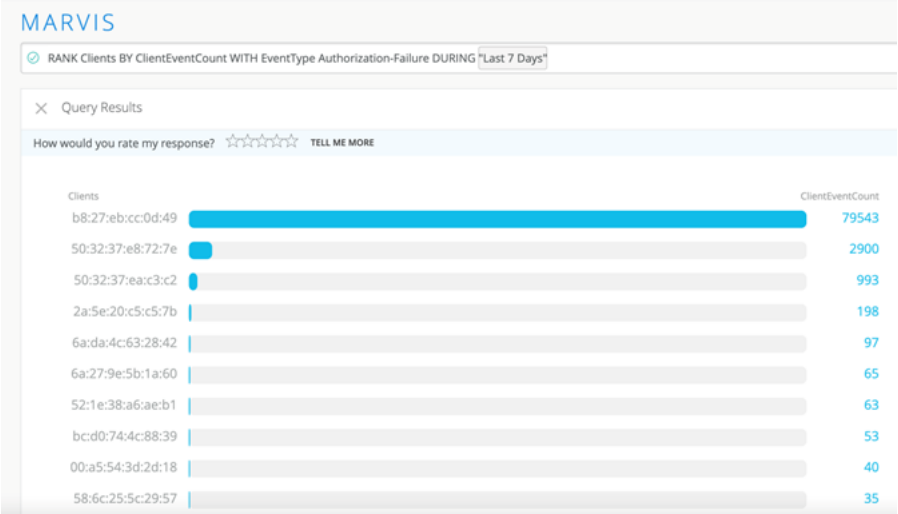
A query can contain the following elements:

- Query Type—Defines what you want Marvis to do (for example, COUNT, LIST, RANK, LOCATE, or TROUBLESHOOT).

- Value—Specifies a unique value that is specific to an organization, such as a client's name.
- Query Object—Indicates Mist-defined objects (for example, APEvents, ClientEvents)
- Clause—Acts as a qualifier for the overall query (for example, of, with, or by).
- Filter Type—Narrows the results based on pre-defined filter types.

You can also add a duration to the end of a Marvis query. Note that you need to press the **space bar** after entering each element to see the available options.

Here's an example of a RANK query that ranks clients based on the authentication failures:



Troubleshoot Using Marvis Query Language

IN THIS SECTION

- View Event and Device Details | **41**
- View Roaming Details of a Client | **44**
- View Status of a Client | **44**
- Troubleshoot APs, Sites, or Clients | **45**
- Locate APs, Sites, or Clients | **46**
- View Channel Utilization of an AP | **46**

This topic presents a few samples that show how you can use Marvis queries to monitor and troubleshoot your network.

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:

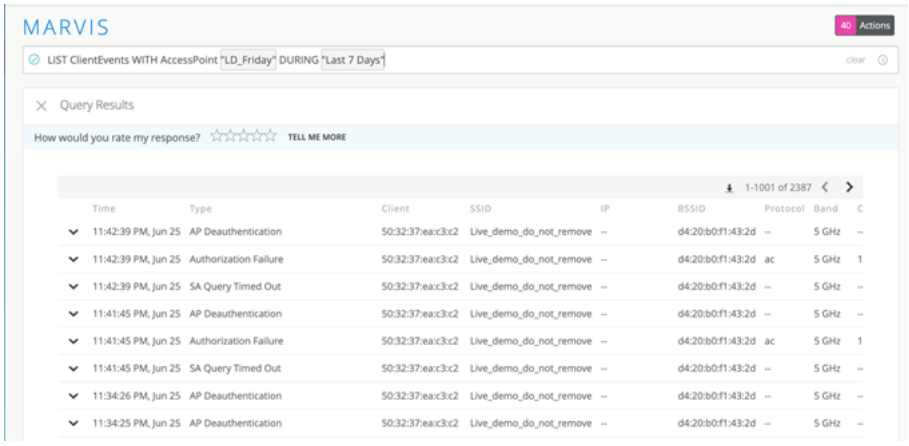
- Access points (APs)
- Clients (including wired clients)
- Switches
- AP events
- Client events
- Switch events

Table 2 on page 41 and Table 3 on page 42 provide a few LIST queries that you can use as a reference to build queries based on your requirements.

Table 2: 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>***

The following screenshot shows the events for all clients associated with a particular AP. You can click the expand arrow to view more details about the event.



Here's a screenshot showing the list for a specific event type:

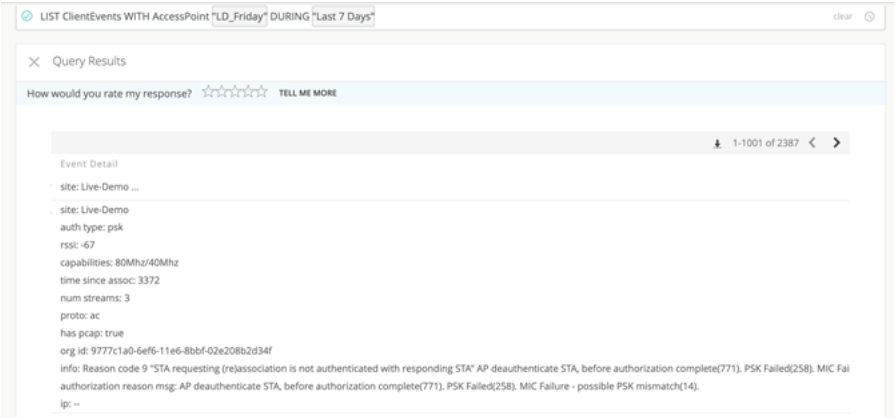
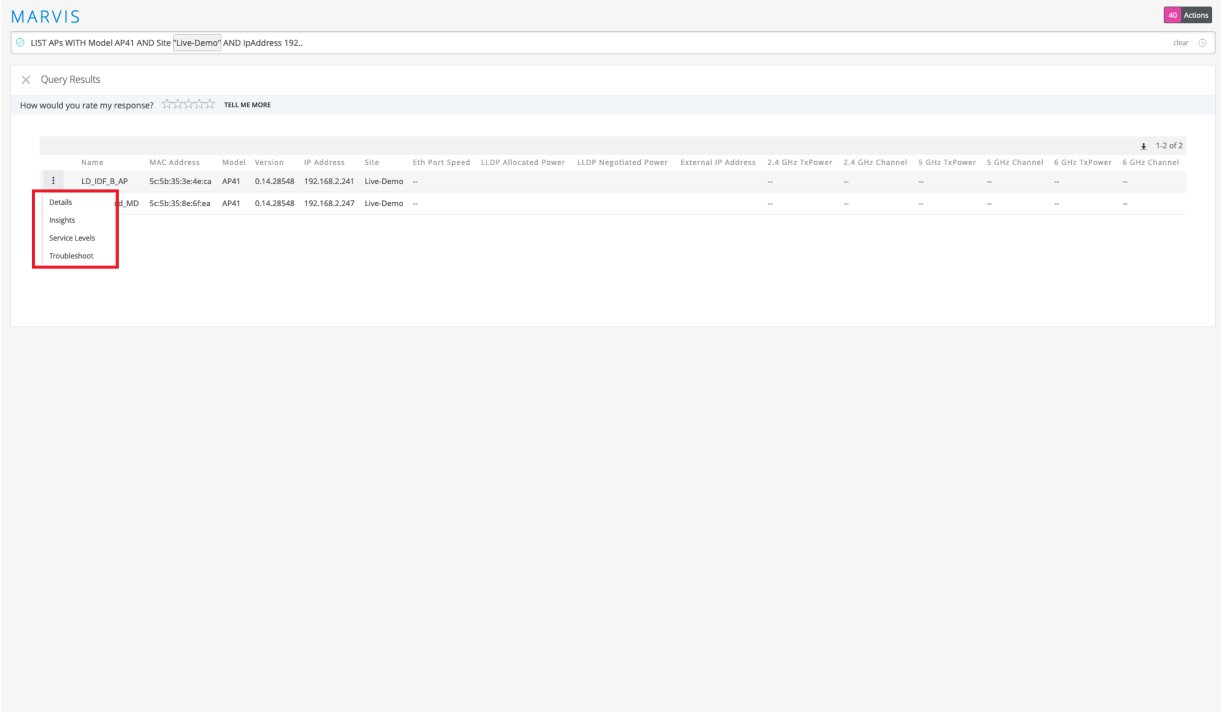


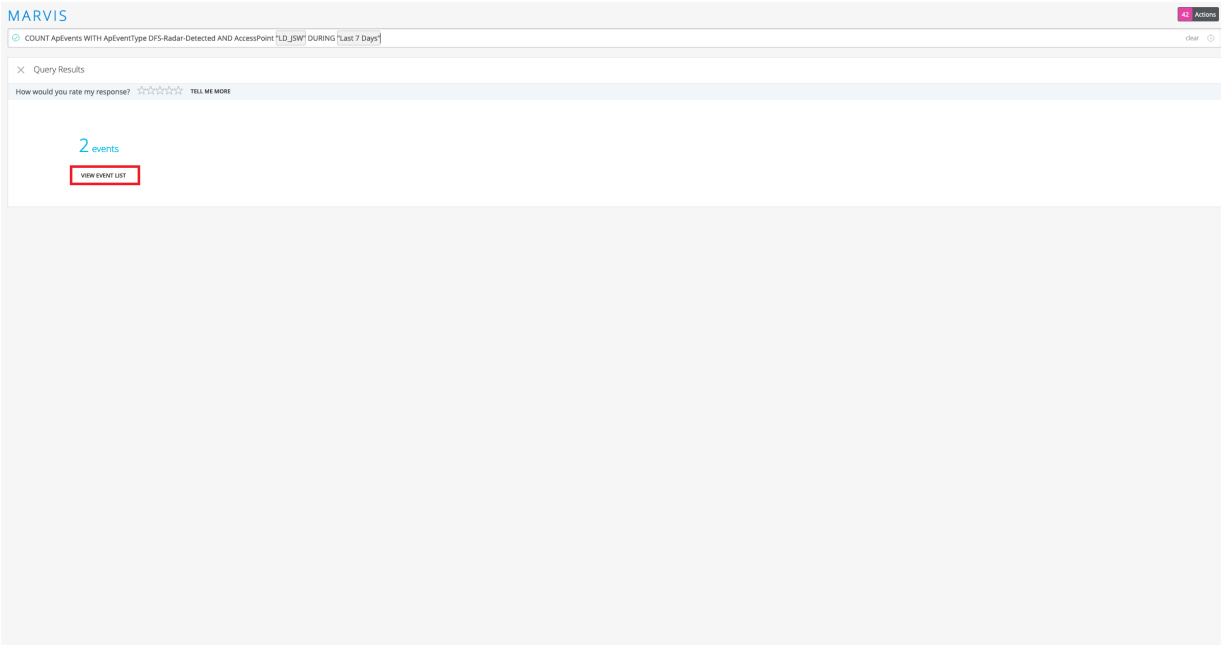
Table 3: Key LIST Queries to View Devices

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>***

Here's a sample screenshot that shows the output for a LIST query. Note that you can enter a partial IP address to search for devices in specific subnets. If you click the More Options icon (the vertical ellipsis) in the first column, you can access additional options to view more information.



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

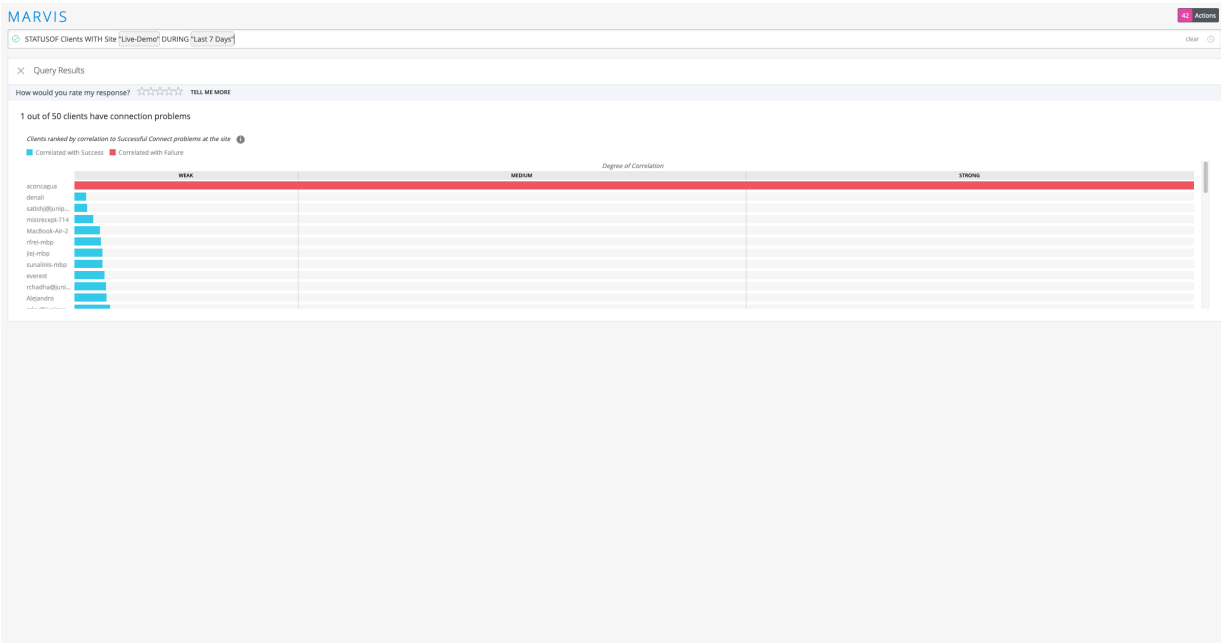
You can use the ROAMINGOF query to see a graphical view of a client roaming between different APs.

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.

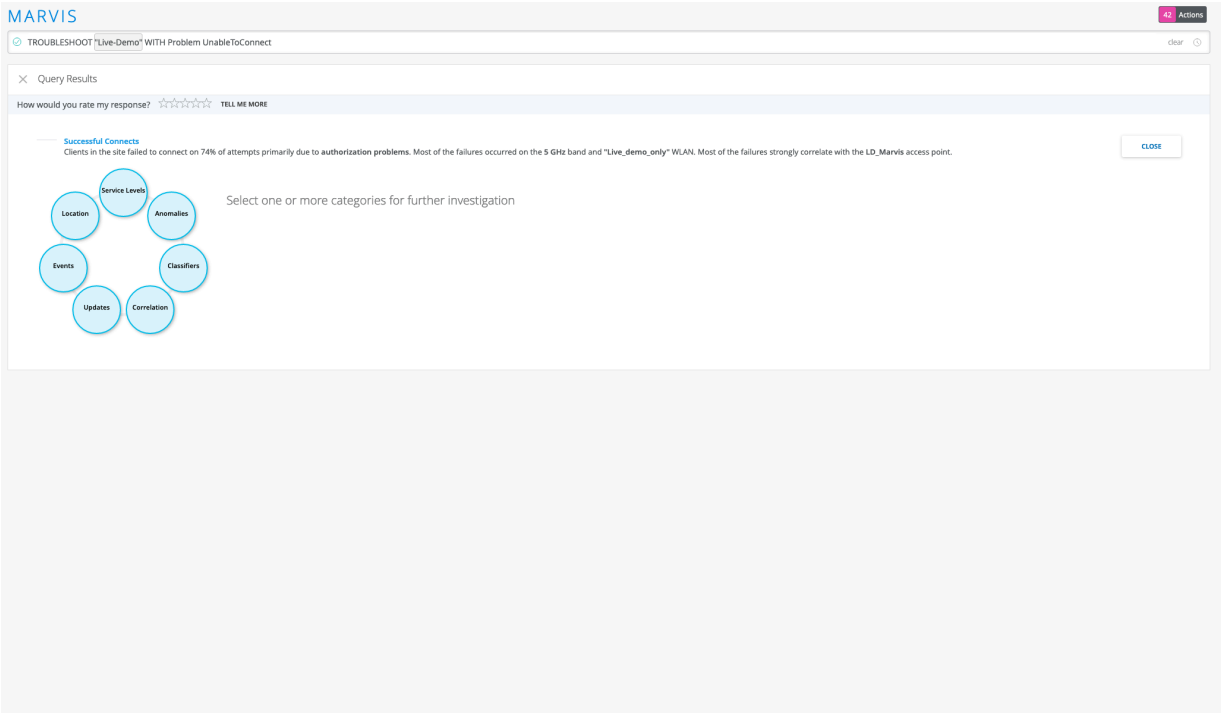
Troubleshoot APs, Sites, or Clients

Table 4 on page 45 lists a few TROUBLEHOOT queries that you can use to troubleshoot a site, a client, or an AP.

Table 4: 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>***

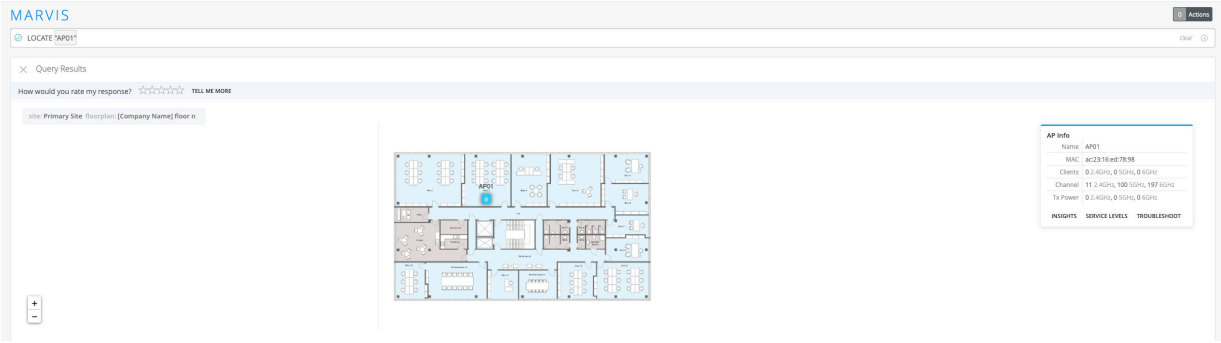
The following screenshot shows the output for the **TROUBLESHOOT <site name> WITH Problem UnableToConnect** query. You'll see that Marvis provides data such as the cause of the issue, the band, and the WLAN on which the issue occurred.



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

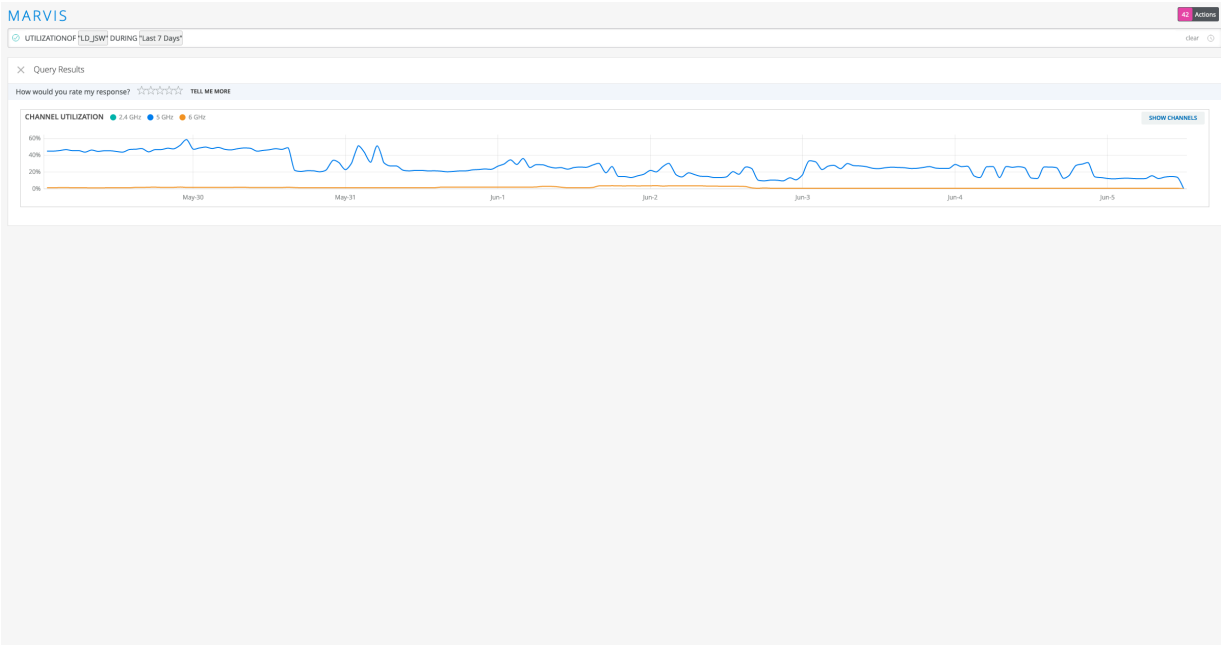
You can use the LOCATE query to find your site, AP, or client. The query output displays a map view of the site location that you configured in **Organization > Site Configuration**. For APs and clients, Marvis shows the location of these devices on your floorplan. Marvis also displays additional information 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.



4

CHAPTER

Marvis Client

Marvis Client Overview | 49

Marvis Android Client | 51

Marvis-Zebra Integration | 59

Client Roaming Visualization | 62

Marvis Client Overview

The Marvis client is a software agent that you install on end-user devices (clients) to view the network from the client's perspective. The Marvis client collects detailed data and telemetry about how the client experiences the wireless connection, including insight into client roaming behaviors. The Marvis client recognizes connection types (cellular or wireless) and the corresponding signal strength.

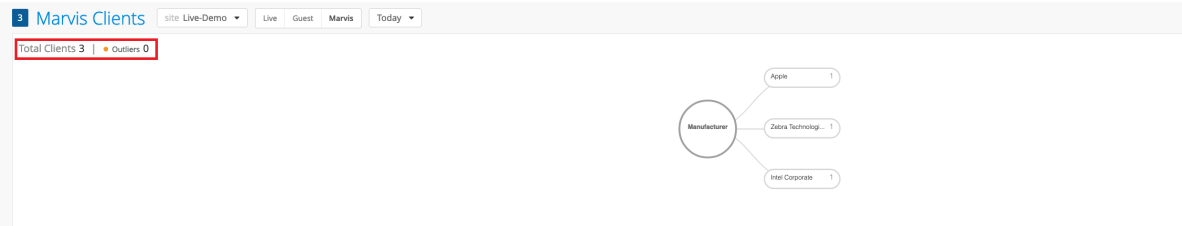
The Marvis client provides an additional layer of detail by displaying device type, manufacturer, and operating system, as follows:

- **Detailed wireless properties**: Mist's device fingerprinting provides the manufacturer, device type, and OS of the device. The Marvis client enhances this visibility by providing the OS version along with the radio hardware (adapter) and firmware (driver) versions. This level of visibility helps you identify:
  - Exceptions in terms of a device with different properties (such as the OS, radio hardware, and firmware) when compared to other devices of the same type.
  - Device-generic issues (for example, issues due to a firmware version).
- **Coverage issues due to asymmetry**: A Mist access point (AP) indicates the received signal strength indicator (RSSI) at which it detects a client. The Marvis client provides the RSSI at which the client detects the AP. This data helps you identify asymmetries in the power level between the client and AP. You can then resolve asymmetries that could result in a poor connection.
- **Connection type**: You can see when the device switches between a wireless and a cellular connection type, along with the corresponding signal strength.
- **Roaming behavior**: Roaming decisions and how a client decides to connect to an AP on a specific band is a client decision. The Marvis client provides visibility into how the client detects the neighboring APs.

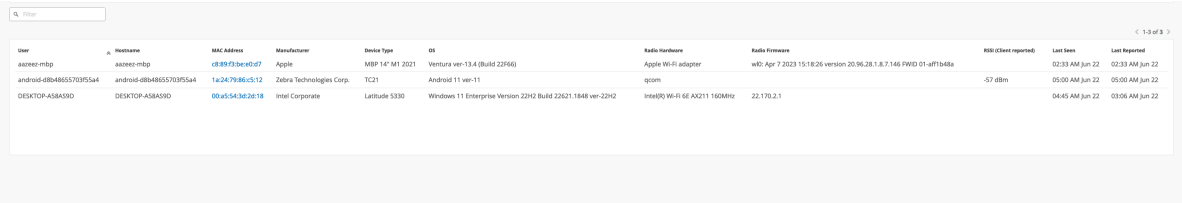
You can view all connected Marvis clients directly on the Mist portal on the WiFi Clients page (**Clients > WiFi Clients > Marvis** tab). You can view a graphical representation of your Marvis clients and their detailed information including manufacturer, device type, OS version, and radio hardware and firmware. You can see the current and historical snapshots of the connected clients in a specific site.

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

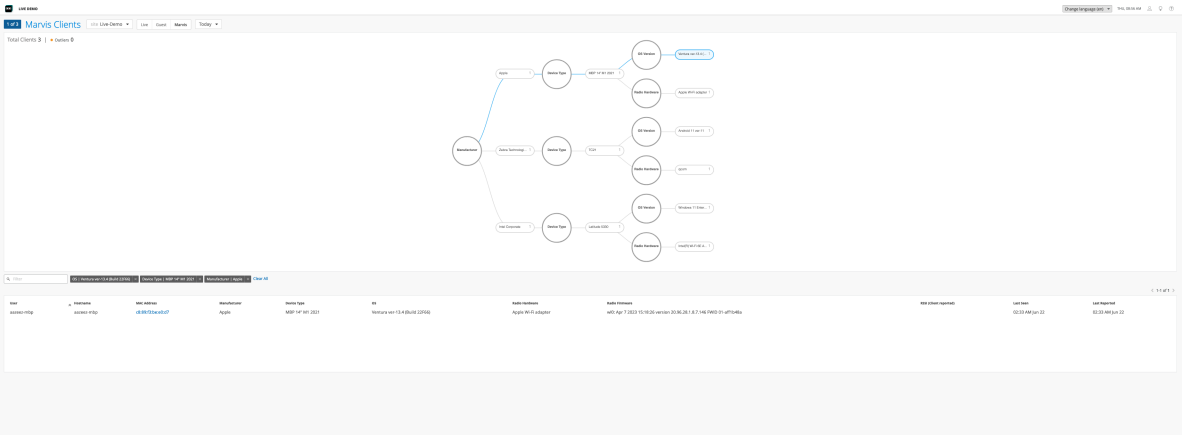
- **Tree view**: Groups clients based on their properties. Marvis classifies the clients by manufacturer, device type, OS version, radio hardware, and radio firmware. The tree view displays the total number of Marvis clients for the specified site and time range. It also highlights possible outliers that do not conform to the properties seen for other clients with the same manufacturer or device type.



- **List view**: Presents client information in a tabular format. The default columns include user, hostname, MAC address, manufacturer, device type, device OS, radio hardware, radio firmware, and client-reported RSSI value. The list view displays up to 50 clients on a single page. You can navigate between pages by using the arrow buttons located on the top-right corner of the list.



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.



We support the Marvis client on Android handheld devices and smartphones running OS 6.0 and higher versions.

NOTE: You must have a Marvis subscription to use the Marvis client. In addition, you must connect your client device to a Mist AP to use the Marvis client.

Marvis Android Client

IN THIS SECTION

- Before You Begin | 51
- Deploy the Marvis Client Using the SOTI MDM | 52
- Deploy the Marvis Client Using AirWatch or VMWare Workspace ONE | 54
- Deploy Marvis Client Using Other MDMs | 54
- Install Through Sideloading | 55
- Verify the Installation | 58

Juniper Networks® supports the Marvis client on Android handheld devices and smartphones running OS 6.0 and higher versions. The Marvis android client provides the following data:

- Device type
- OS, radio hardware, and firmware versions
- Client-reported received signal strength indicator (RSSI)
- Client-reported view of surrounding access points (APs)

This topic presents the background information and procedure to install the Marvis Android client.

Before You Begin

Before you start the installation:

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

  If your Mist organization resides in Amazon Web Services (AWS) cloud (default), use the following settings:

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

or HTTPS protocol port 443 for domain

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

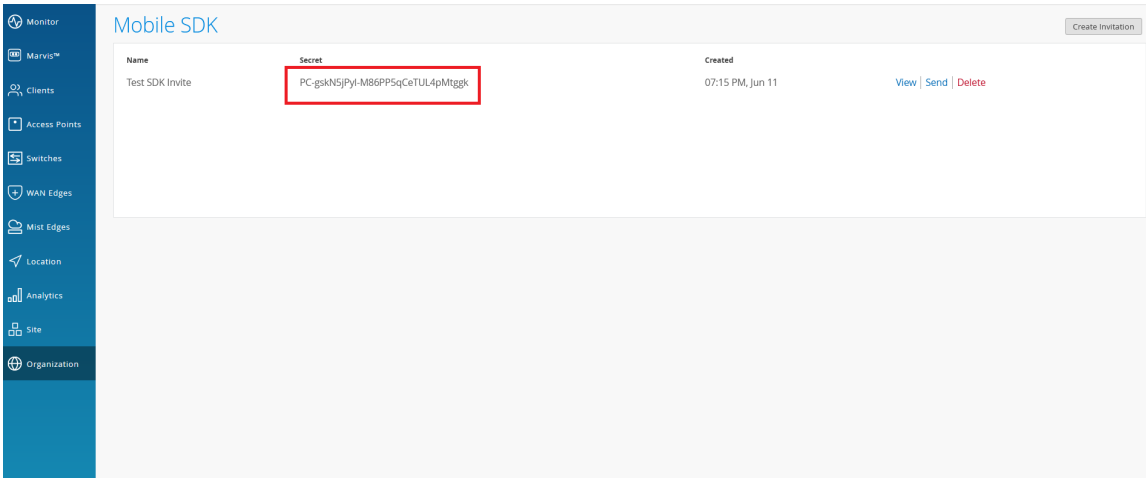
- wss://client-terminator.gc1.mist.com/ws or protocol WSS (websocket) port 443 for domain/path
- https://api.gc1.mist.com/

  or HTTPS protocol port 443 for domain

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

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

  1. Go to **Organization > Mobile SDK** in the Mist portal to locate your secret token or QR code.



  2. Click **View** to see the QR code.

     If an invitation doesn't exist, you can create one by using the **Create Invitation** button in the top-right corner. You'll need to enter a name for your organization invitation.

Deploy the Marvis Client Using the SOTI MDM

To deploy the Marvis client using a mobile device management (MDM) solution, you must customize the Android package kit (APK) package deployment. You customize the APK deployment with the Intent action to set the secret software development kit (SDK) token upon installation. When you launch the customized application package, the client will be fully preconfigured and onboarded for operation.

You can onboard the Marvis client using the SOTI MDM.

> **NOTE**: We do not present the overall generic Android application deployment process with SOTI. We present only the information necessary to customize the Android application to complete the client deployment.

Before you begin:

1. Ensure that you have a Windows device or a virtual machine (VM). You will run Package Studio, which runs only on Windows devices.
2. Download SOTI's MobiControl Package Studio (McStudio.exe).

To deploy the Marvis client using MDM:

1. On your Windows device or VM, launch Package Studio and create a package project with the following settings:
   - Processor—All (unless targeting specific CPU or device types)
   - Platform—Android
   - OS Version—5 to 13 (unless you want to use a specific version)
   - Version String—Set to the same versioning as the APK version
   - Vendor—Mist Systems, Inc.
   - Optional space requirement specifications
2. Add the Marvis client APK.
3. Add the following Script file:
   - Script Engine—Legacy
   - Script Type—Post-Install
4. Import the script file. The script file must have the following content:

```
sendintent -a "intent:#Intent;
action=android.intent.action.MAIN;component=com.mist.marvisclient/.MainActivity;S.MOBILE_SDK_S
ECRET=TheSecretValueHere;end;"
```

If you have configured a specific port on a Zebra device for voice calls, then the script file must have the following content:

```
sendintent -a "intent:#Intent;
action=android.intent.action.MAIN;component=com.mist.marvisclient/.MainActivity;S.MOBILE_SDK_S
ECRET=TheSecretValueHere;S.MOBILE_VOICE_CALL_PORT=5070;end;"
```

5. Build the package.

When you deploy the customized package with SOTI, the Marvis client is preconfigured and onboarded.

Deploy the Marvis Client Using AirWatch or VMWare Workspace ONE

We do not cover the overall generic Android app deployment process with AirWatch. We only cover the specific steps needed to complete the agent deployment.

Use the following intent command to deploy the agent:

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

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

```
mode=explicit,broadcast=false,action=android.intent.action.MAIN,package=com.mist.marvisclient,cla
ss=com.mist.marvisclient.MainActivity,extraString=MOBILE_SDK_SECRET=TheSecretValueHere,extraStrin
g=MOBILE_VOICE_CALL_PORT=5070
```

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

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

Deploy Marvis Client Using Other MDMs

If you are using any other MDM, verify that the MDM supports intent execution. If the MDM does not support intent deployment, then you can use the sideloading procedure described in "Install Through

Sideloading" on page 55. Here is another example for ADB based (developer/debug) deployment that you can use to adapt to an MDM of your choice:

```
adb shell am start -n "com.mist.marvisclient/com.mist.marvisclient.MainActivity" -a
android.intent.action.MAIN -c android.intent.category.LAUNCHER --es "MOBILE_SDK_SECRET"
"TheSecretValueHere" -t "text/plain"
```

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

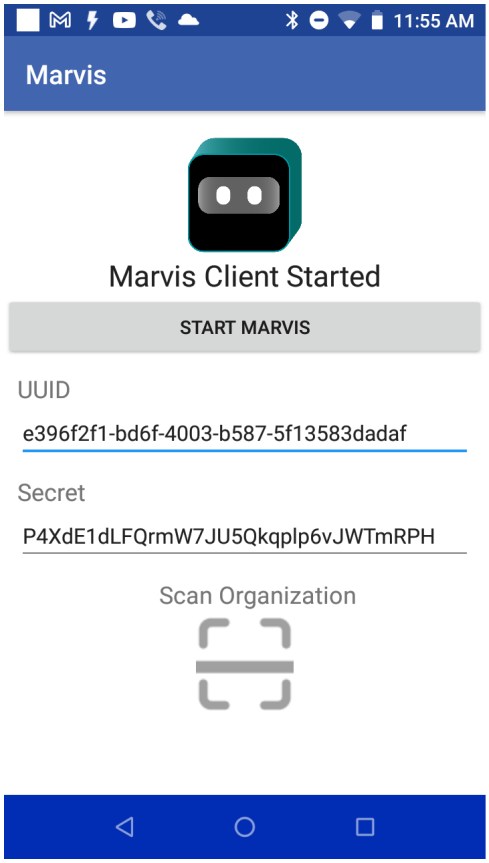
Install Through Sideloading

NOTE: Follow this procedure for internal use, development, testing, or debugging. This process is not for official customer deployments. However, you can use this procedure in cases where the MDM solution does not support executing Android Intents to automatically configure the secret token on installation.

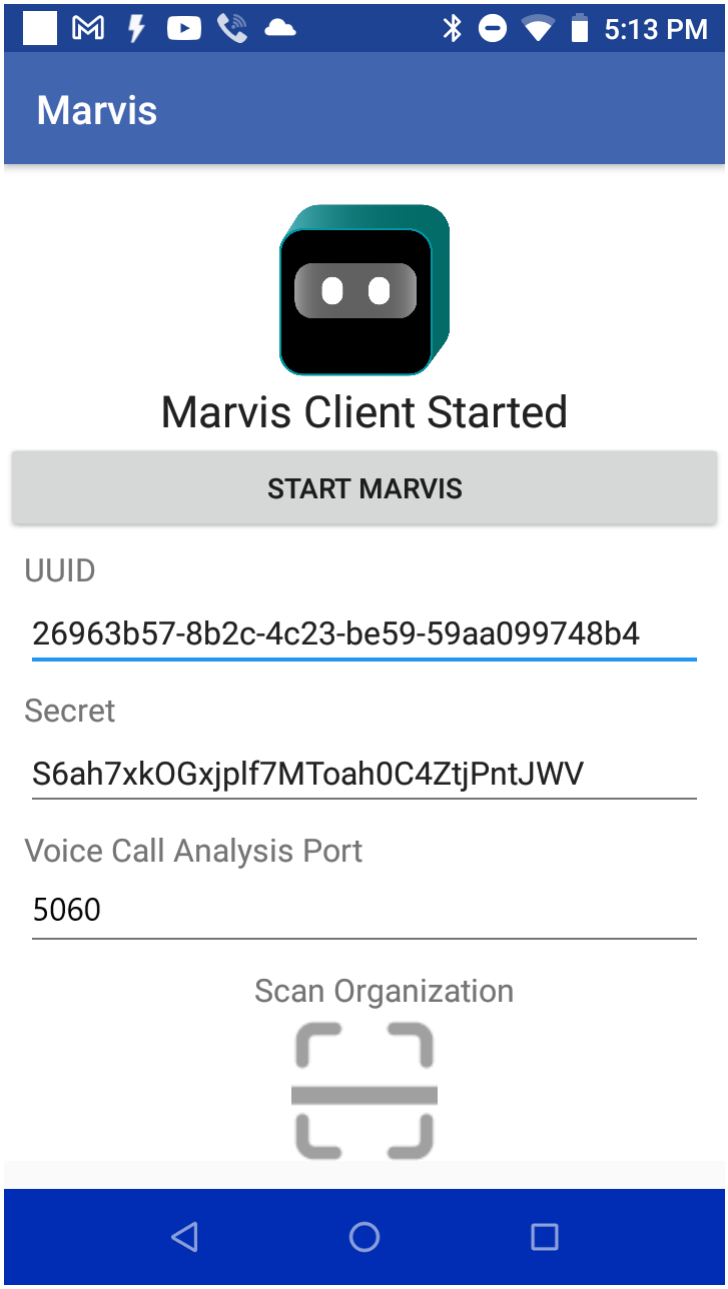
This procedure requires manual intervention for each device being onboarded.

1. Install the APK on the device. You can use Android Debug Bridge (ADB), MDM, or file manager (local device storage or an SD card containing the APK).
2. Open the Marvis client application on the device.

3. Tap the Marvis icon 7 times to open a special debug menu.



For Zebra devices, the debug menu shows the port that is configured for voice calls.



4. Onboard the client using the secret code or scan code:

   To use the QR code:

   a. Tap the **Scan Organization** button to open the camera and scan the invitation QR code. Provide the necessary permissions.

   b. When the QR code is scanned, the matching secret token value is inserted into the Secret field.

      The secret value is applied to the Marvis client automatically. A message appears indicating that the value is applied.

To use the secret code:

a. Type or paste the secret token value in the Secret field. The default value of Secret is empty.

b. Tap the gray **Start Marvis** button to apply the changes.

   A message appears indicating that the value is applied.

You have successfully onboarded the Marvis client.

Verify the Installation

After you install and onboard the Marvis client, verify that those processes have run correctly.

To verify the installation:

- Confirm that the secret token value is added correctly. Close the Marvis client process and then launch it again. Open the debug menu by tapping the Marvis icon 7 times, and verify that the secret token value is still stored in the field.

  If the secret token field is empty and the data does not persist, enter the secret token value manually, as described in "Install Through Sideloading" on page 55. You might also need to configure the application deployment to retain the application data.

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

  If the data is not available in the Mist dashboard, a problem occurred in the client workflow of collecting data and sending it to the Mist cloud. Contact the support team. If you are able to use tools such as logcat or Android Debug Bridge (ADB), then you can use them to collect the Marvis client logs and share the logs with the support team.

  For Zebra devices, use the RxLogger tool to collect logs.

  When you contact the support team, you must share the Marvis client UUID. You can find the UUID on the Marvis client debug mode screen. The UUID is used to track the data flow from the Marvis client to the Mist cloud.

Marvis-Zebra Integration

IN THIS SECTION

- Overview | 59
- Connection Events | 59
- Roaming Events | 60
- Voice Events | 61

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.

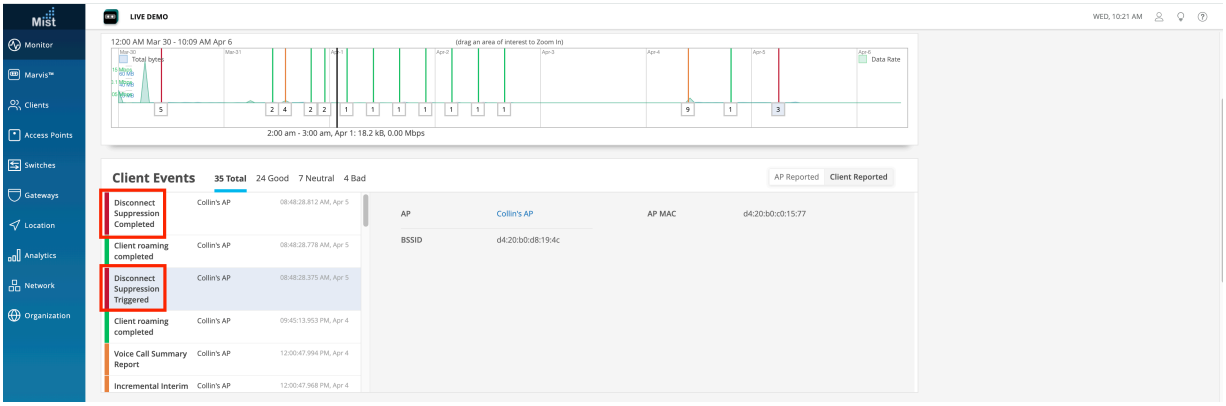
> **NOTE**: To view client events from your Zebra device, the device must have a valid Wireless Insights license and the Marvis Android Client (V33.x or later) installed.

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.

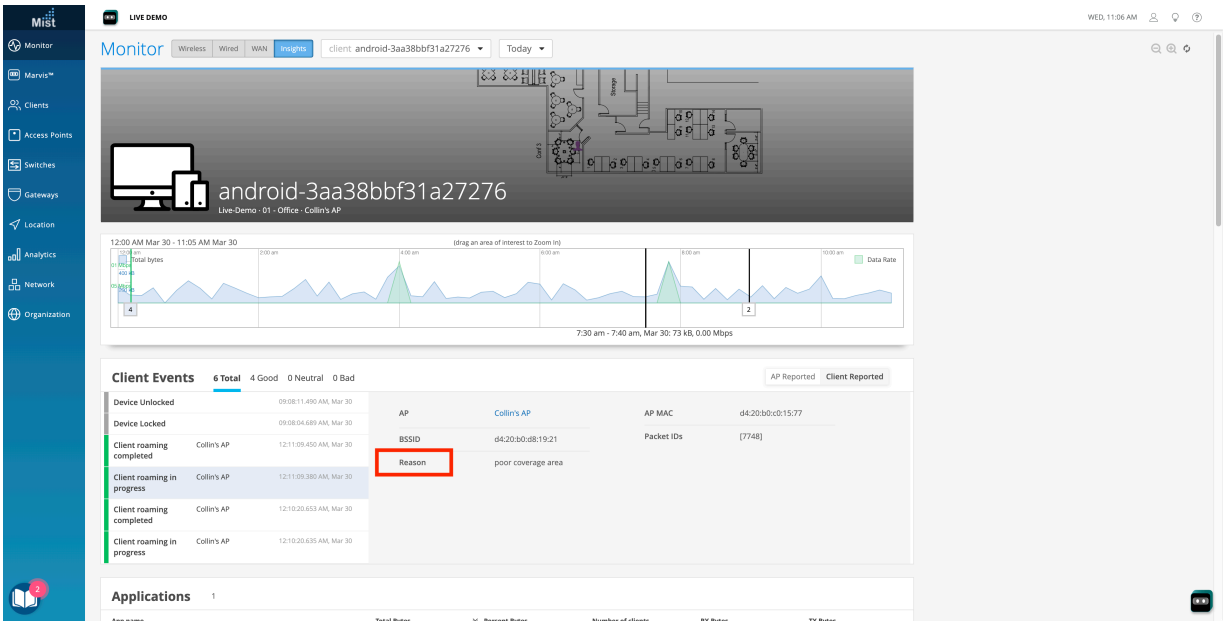
Here is a sample event and the condition that triggered the event:

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).



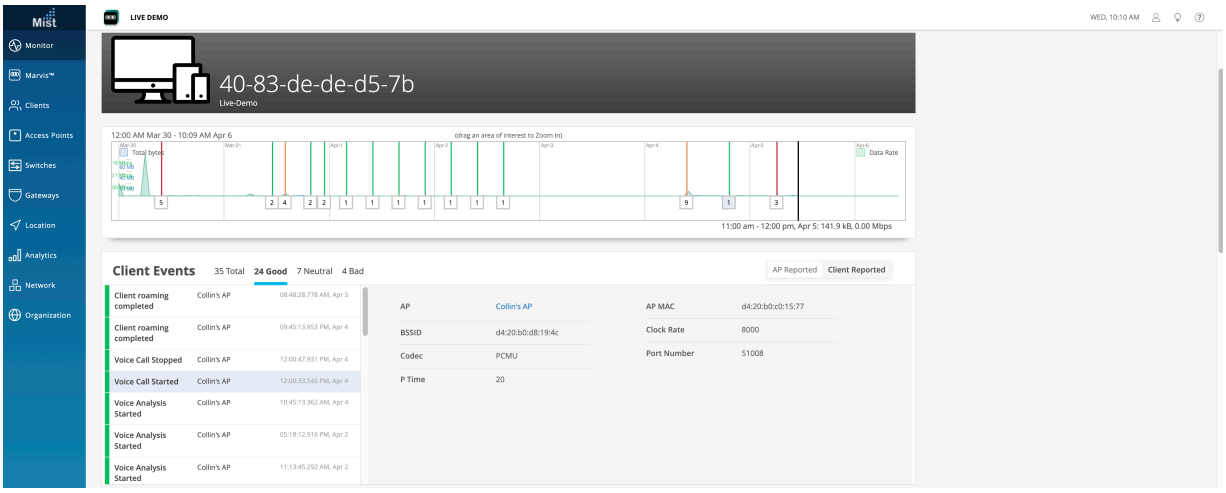
Roaming Events

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.

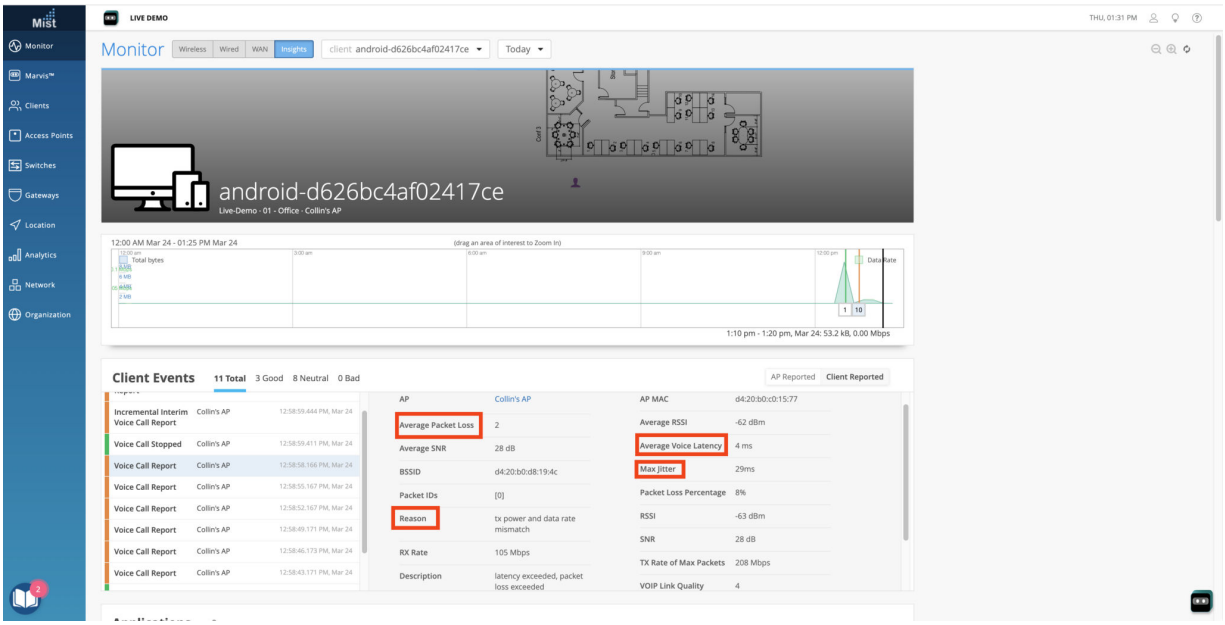


Voice Events

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.

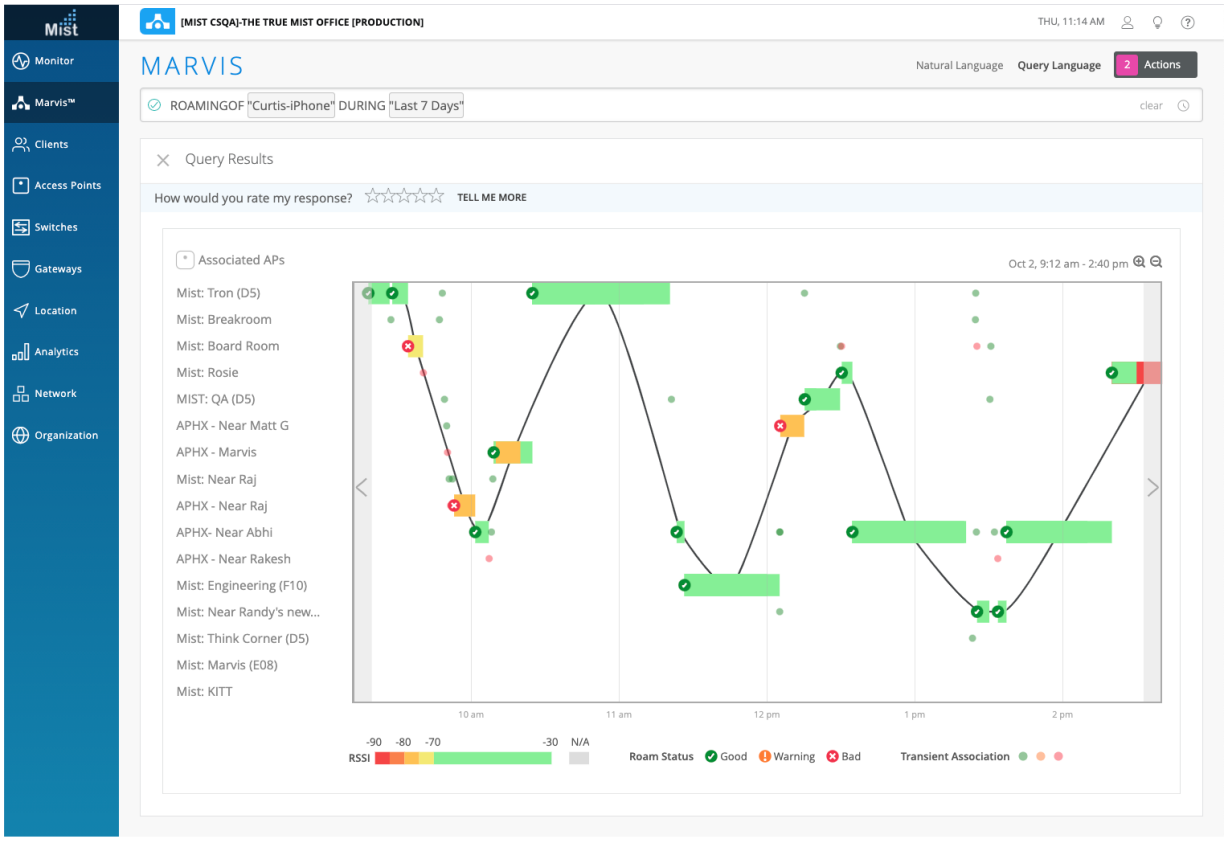


Client Roaming Visualization

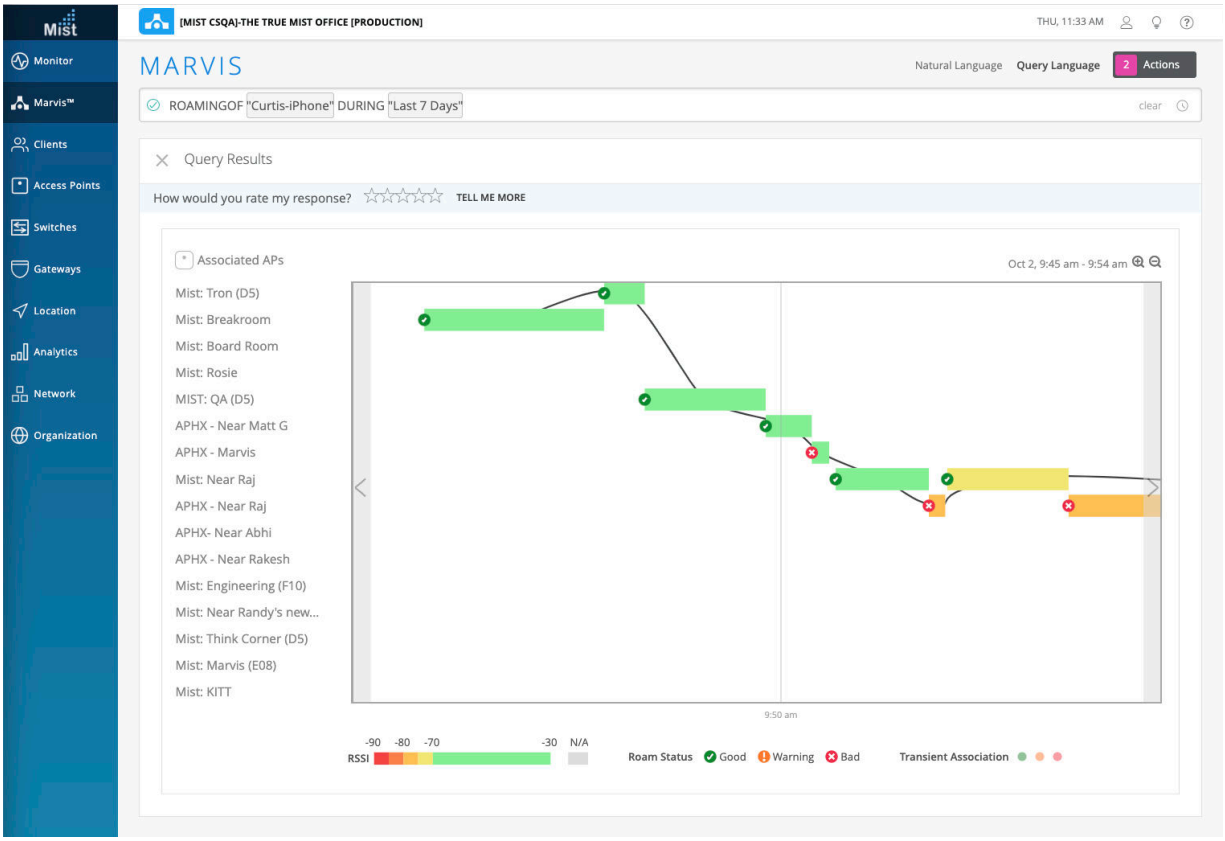
Marvis provides a visualization of your device's roaming history and behavior. It includes information about the access points (APs) and radio bands the device connects to, and the received signal strength indicator (RSSI) values of the connection. Marvis uses the data from **Client Events** to provide 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.

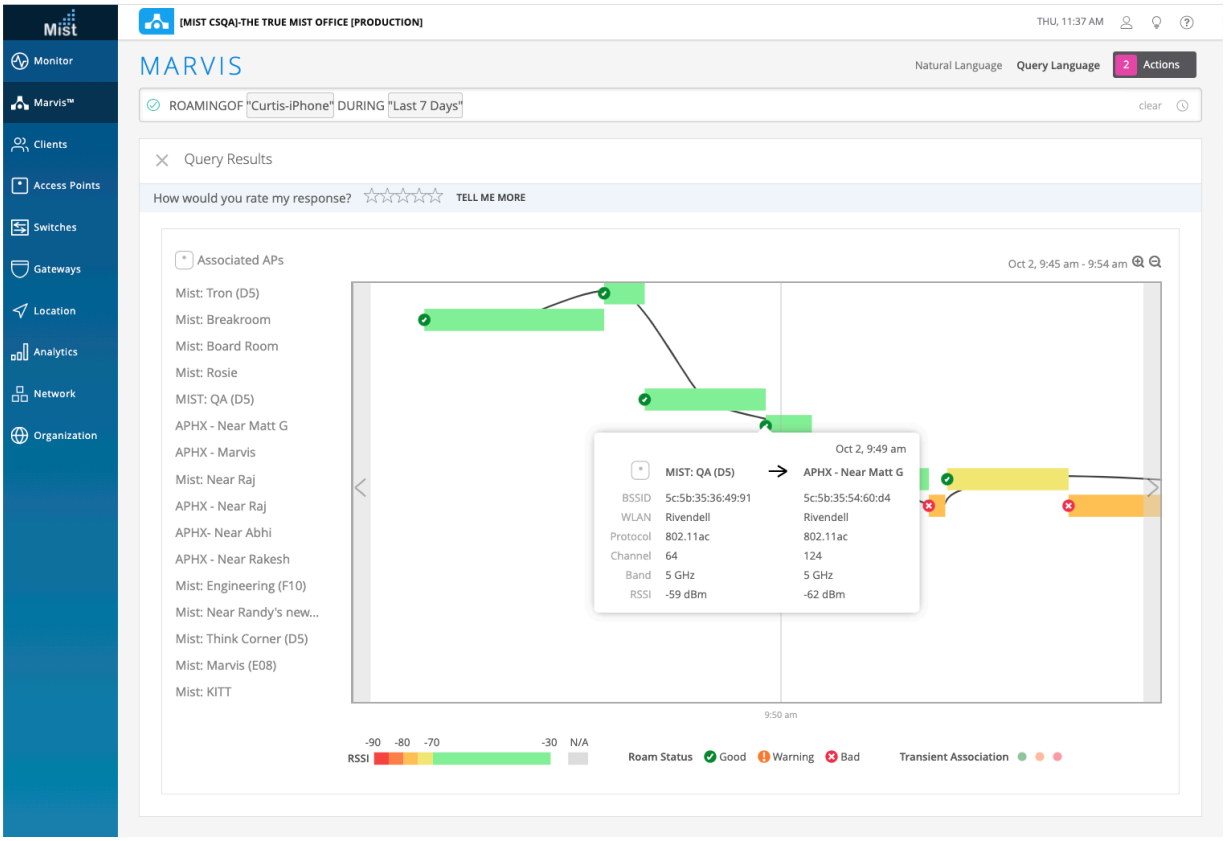
Marvis highlights information such as the roaming status, RSSI value, and transitions, to improve troubleshooting. The dots you see in this screenshot indicate Transient Associations, which means that the device was associated with the AP for a very short time.



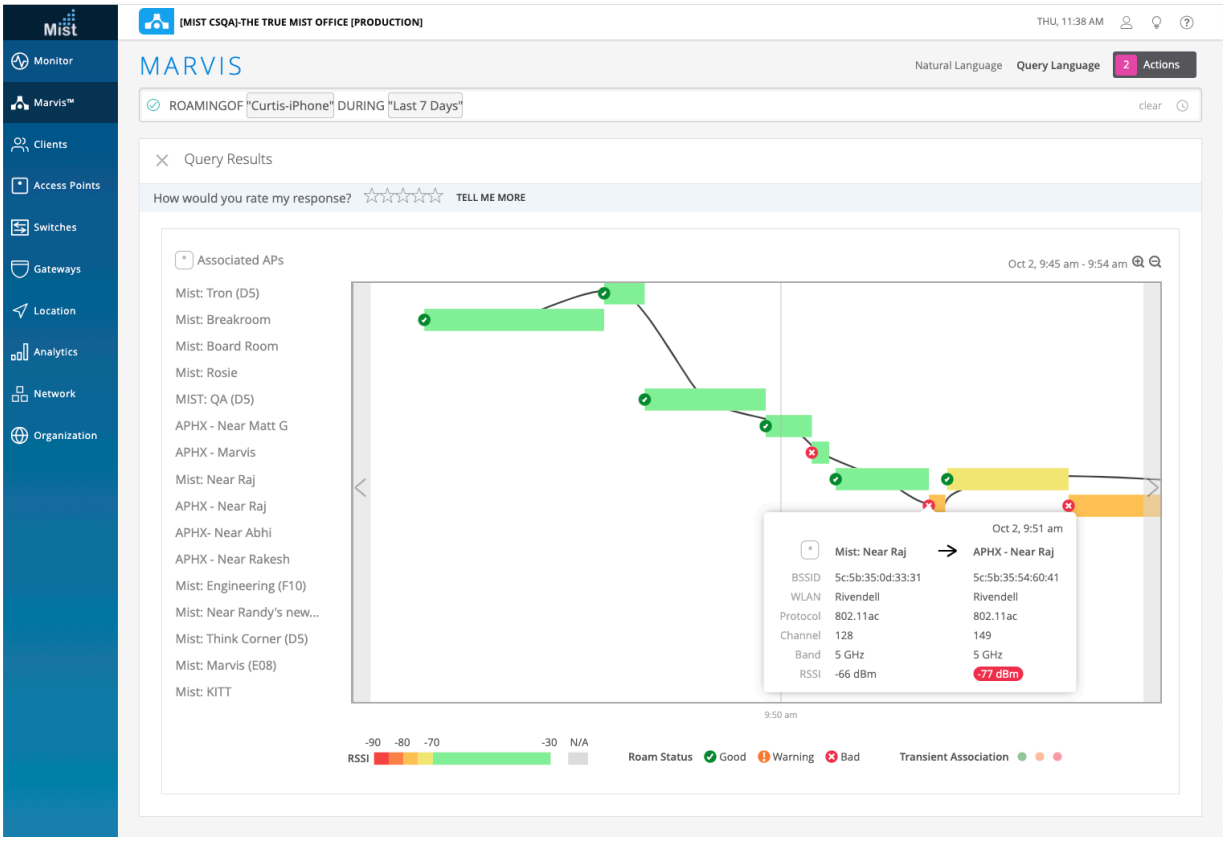
Here is a zoomed-in view of transient associations in the 9:45 a.m. – 9:54 a.m. time interval.



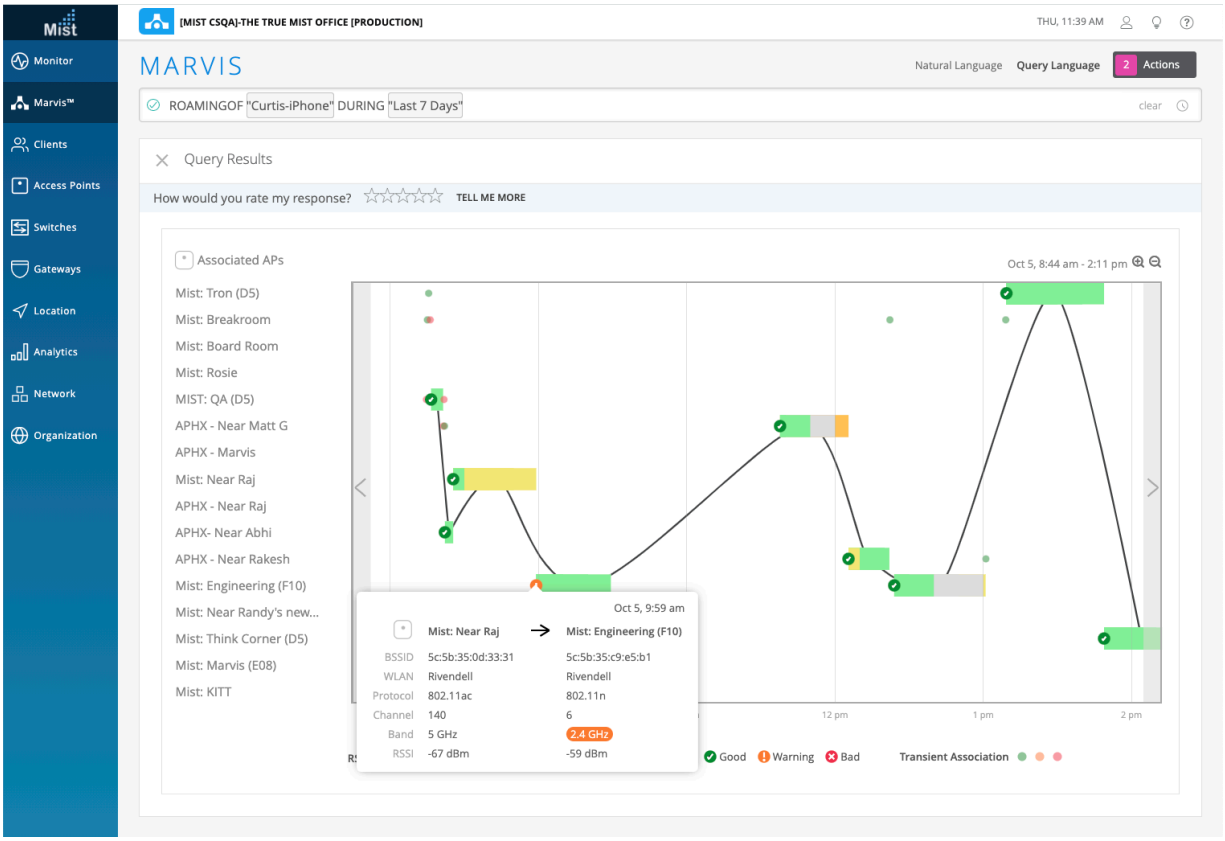
You can hover over the roaming status icons on the timeline to view detailed information about the roaming event, such as the WLAN, channel, band, and RSSI. Here you can see that the client experienced a good roaming event between the APs at 9:49 a.m.



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.


Mist
[MIST CSQA]-THE TRUE MIST OFFICE [PRODUCTION]
THU, 11:39 AM
Monitor
Marvis™
Clients
Access Points
Switches
Gateways
Location
Analytics
Network
Organization
MARVIS
Natural Language
Query Language
2 Actions
ROAMINGOF "Curtis-iPhone" DURING "Last 7 Days"
clear
Query Results
How would you rate my response?
TELL ME MORE
Associated APs
Oct 5, 8:44 am - 2:11 pm
Mist: Tron (D5)
Mist: Breakroom
Mist: Board Room
Mist: Rosie
MIST: QA (D5)
APHX - Near Matt G
APHX - Marvis
Mist: Near Raj
APHX - Near Raj
APHX- Near Abhi
APHX - Near Rakesh
Mist: Engineering (F10)
Mist: Near Randy's new...
Mist: Think Corner (D5)
Mist: Marvis (E08)
Mist: KITT
Oct 5, 9:59 am
Mist: Near Raj
Mist: Engineering (F10)
BSSID 5c:5b:35:0d:33:31 5c:5b:35:c9:e5:b1
WLAN Rivendell Rivendell
Protocol 802.11ac 802.11n
Channel 140 6
Band 5 GHz 2.4 GHz
RSSI -67 dBm -59 dBm
12 pm
1 pm
2 pm
Good
Warning
Bad
Transient Association

5

CHAPTER

Marvis Conversational Assistant

Marvis Conversational Assistant Overview | 69

Search Using the Conversational Assistant | 71

Troubleshoot Applications Using the Conversational Assistant | 74

Troubleshoot Devices Using the Conversational Assistant | 78

Troubleshoot Sites Using the Conversational Assistant | 86

Marvis Conversational Assistant Overview

The Marvis conversational assistant is a next-generation virtual network assistant that can answer your queries. With natural language processing (NLP) and natural language understanding (NLU) capabilities, the conversational assistant can answer product-specific or feature-specific questions. It can provide information about the network and help you find any type of network device.

The Marvis conversational assistant:

- Provides real-time answers about the network.
- Infers user intent from general statements and queries.
- Improves user experience by learning from user feedback.
- Answers generic questions beyond troubleshooting. You can ask questions like you would in a normal conversation. For example, “How many switches are connected?” or “How is the primary site working?”

NOTE: To use the conversational assistant, you must have:

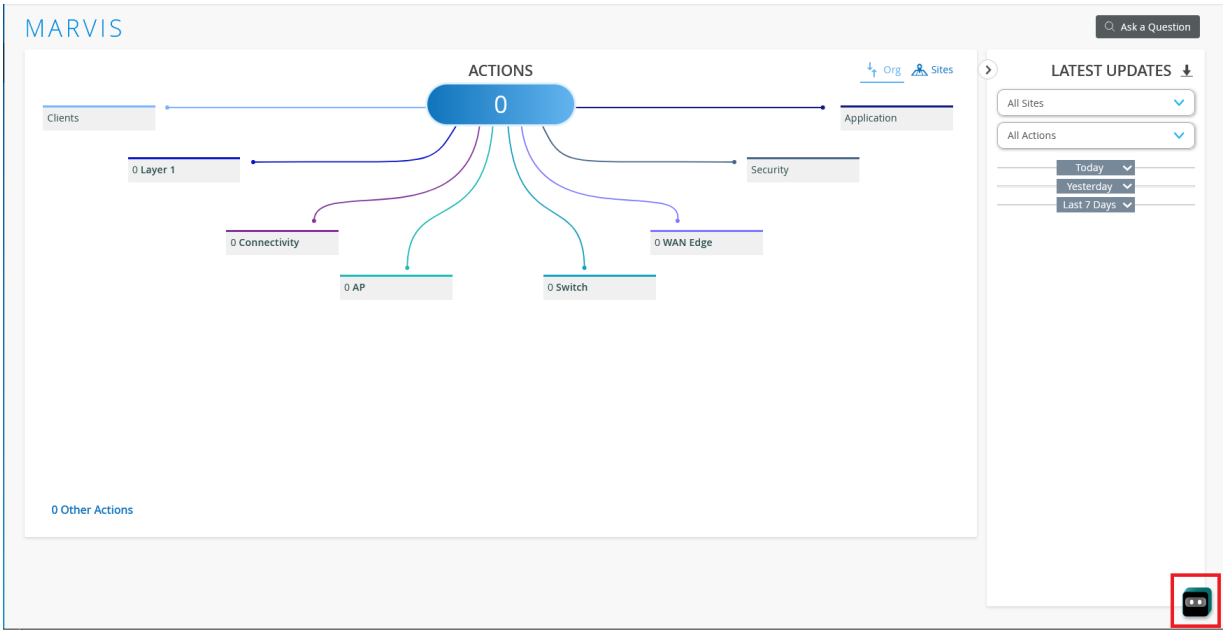
- A Marvis subscription (Wireless, Wired, or WAN)

  You can use the conversational assistant only if the number of subscriptions is greater than 50 percent of the corresponding number of devices in the inventory. If this condition is not met, then you’ll see a warning message.

- Access to all sites in the organization

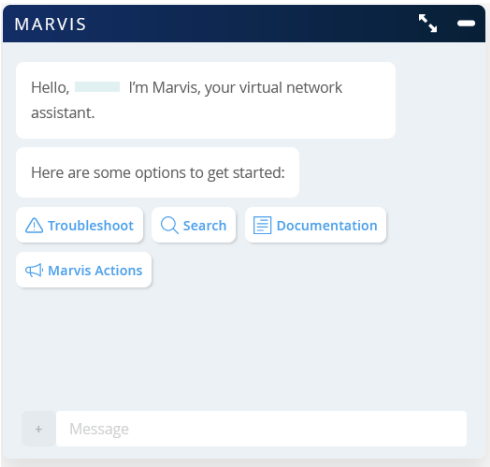
  You can access the conversational assistant even if you have only Read access to a site.

The conversational assistant is accessible from anywhere in the Mist portal. Simply click the Marvis icon in the lower-right corner of the portal and you can get started.



You can start asking questions or select any of the following menu options:

- Troubleshoot—Helps you troubleshoot site, application, device, and wired or wireless client issues.
- Search—Enables you to search for users, devices, and sites.
- Documentation—Enables you to search for documentation related to Mist.
- Marvis Actions—Displays pending actions from the Actions dashboard.



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.

Here's a video overview of the Marvis conversational assistant.

Video:

Search Using the Conversational Assistant

IN THIS SECTION

- Search for Devices and Sites | 71
- Search for Documentation | 72
- Product Feature Search | 73

You can use the conversational assistant to search for devices and sites. You can also search for documentation.

Search for Devices and Sites

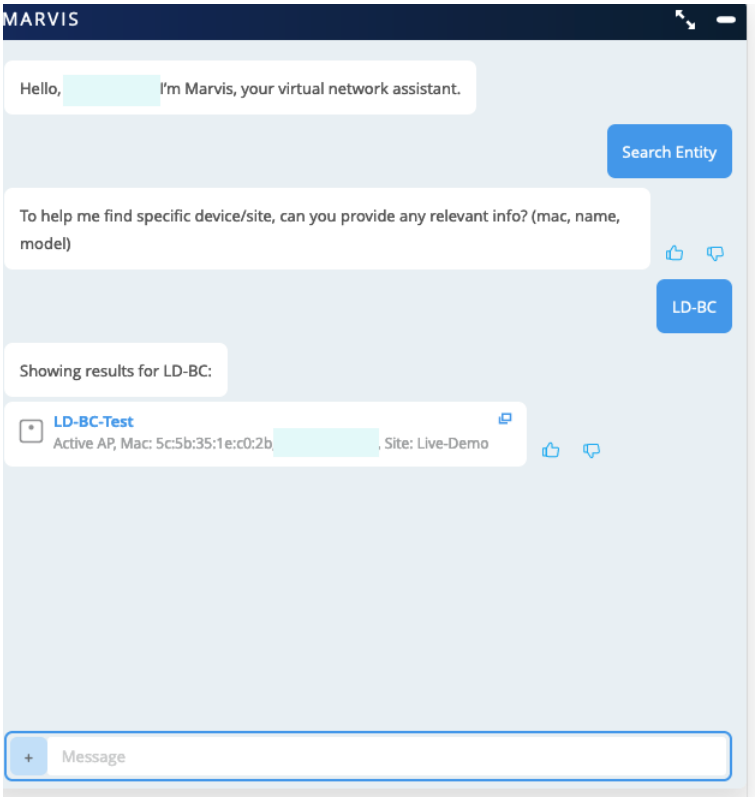
You can use the conversational assistant to search for devices such as wireless or wired clients, access points (APs), switches, and WAN edge devices based on the device's name or MAC address. You can also search for sites by site name.

The search results provide links to the Insights page for the device or site. Note that you can even search using partial names.

To search for a device or site, select the **Search** option in the conversational assistant window and enter any detail of the device or site. Here are some examples of phrases that you can use to search for a device or site:

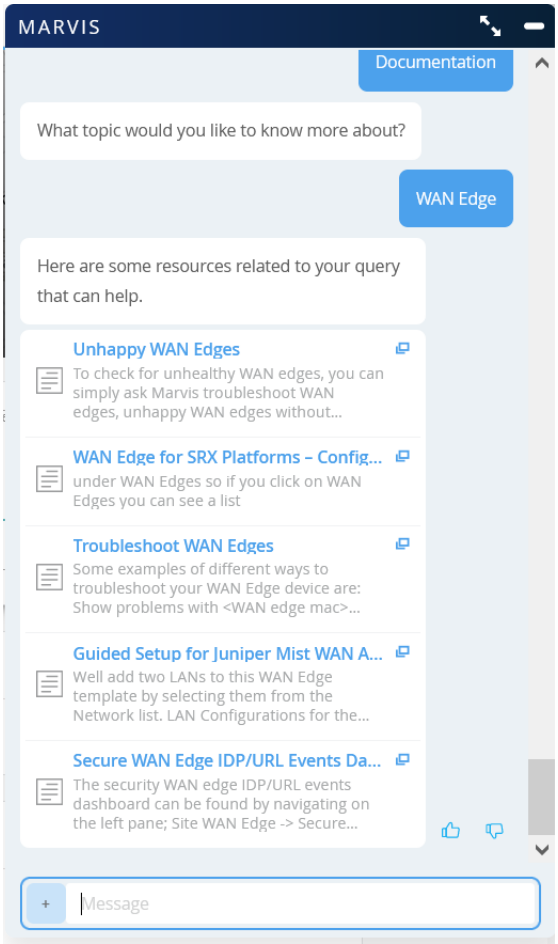
- <client name>
- Search <ap mac> <switch model>
- Find <WAN edge mac>
- <wired client mac>

- <site partial name>



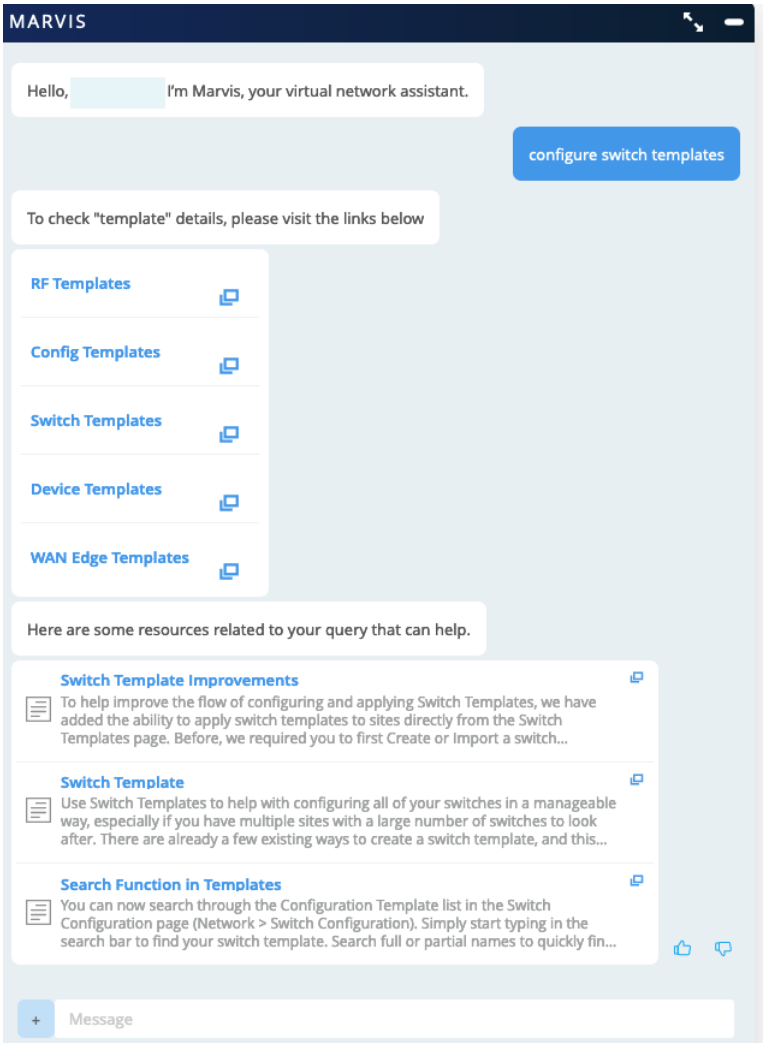
Search for Documentation

You can search for documentation without having to go to the Juniper documentation portal. To search for documentation, select the **Documentation** option in the conversational assistant window and enter the name of the topic that you want to view. 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.



Product Feature Search

You can also search for information about a feature. For example, if you search for templates, Marvis shows you a list of template pages that you can access in the Mist portal. It also lists documentation links that you can view for more information.



Troubleshoot Applications Using the Conversational Assistant

IN THIS SECTION

- Troubleshoot Applications Using the Menu | 75
- Troubleshoot Applications Using Natural Language | 78

To troubleshoot an application, Marvis maps the wired or wireless client (based on its MAC address) to its corresponding application session (based on IP address). Marvis uses this mapping information to present the entire client to cloud view or application view, as experienced by the client. Marvis categorizes Issues experienced by the client when using an application into Wireless, Wired, or WAN, with each category highlighting the relevant issues.

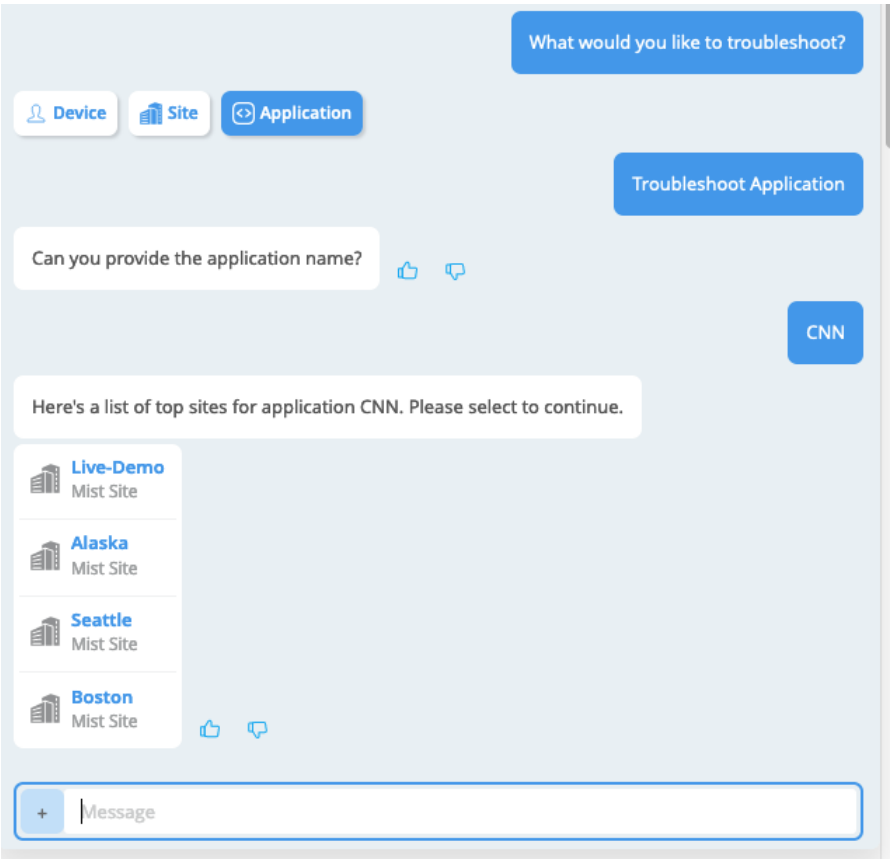
Marvis displays the troubleshooting results for a client based on the application data the WAN edge device collects. The WAN edge device can be either a Juniper Networks® SRX Series Firewall or a Juniper® Session Smart™ Router. You can troubleshoot application issues using the **Troubleshoot** option or natural language as described in the following sections.

Troubleshoot Applications Using the Menu

To troubleshoot an application using the menu option in the conversational assistant:

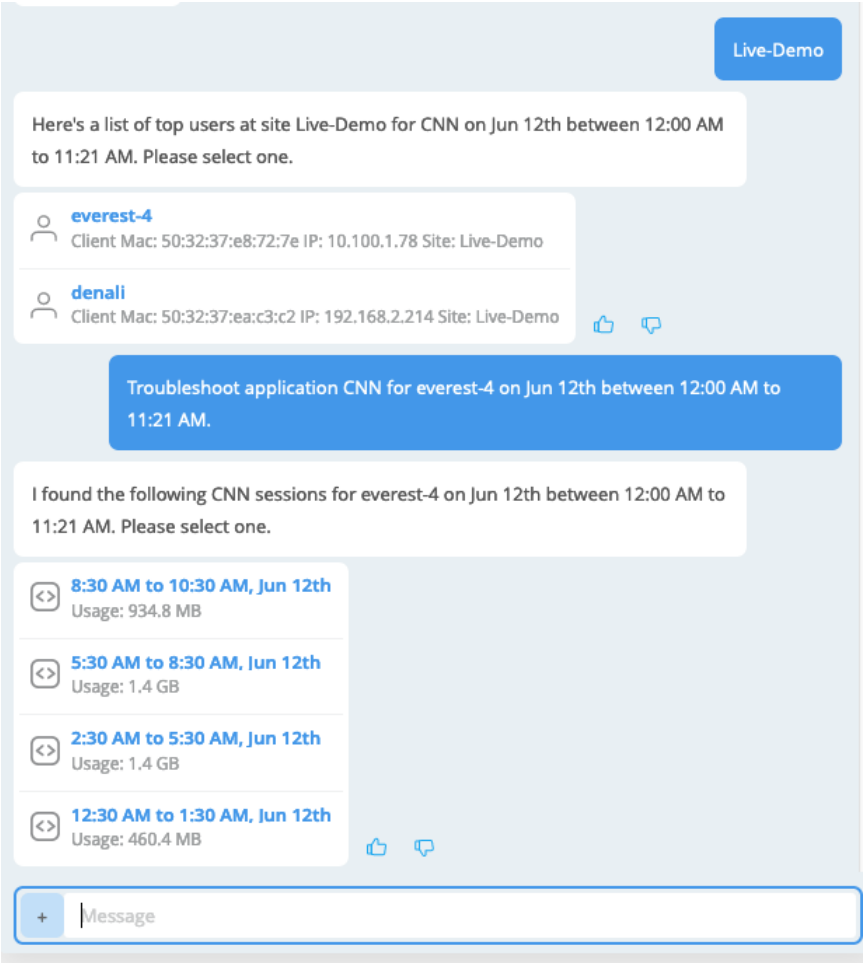
1. In the conversational assistant window, select **Troubleshoot > Application**.
2. Enter the application name.

   Marvis displays the list of sites that use this application.



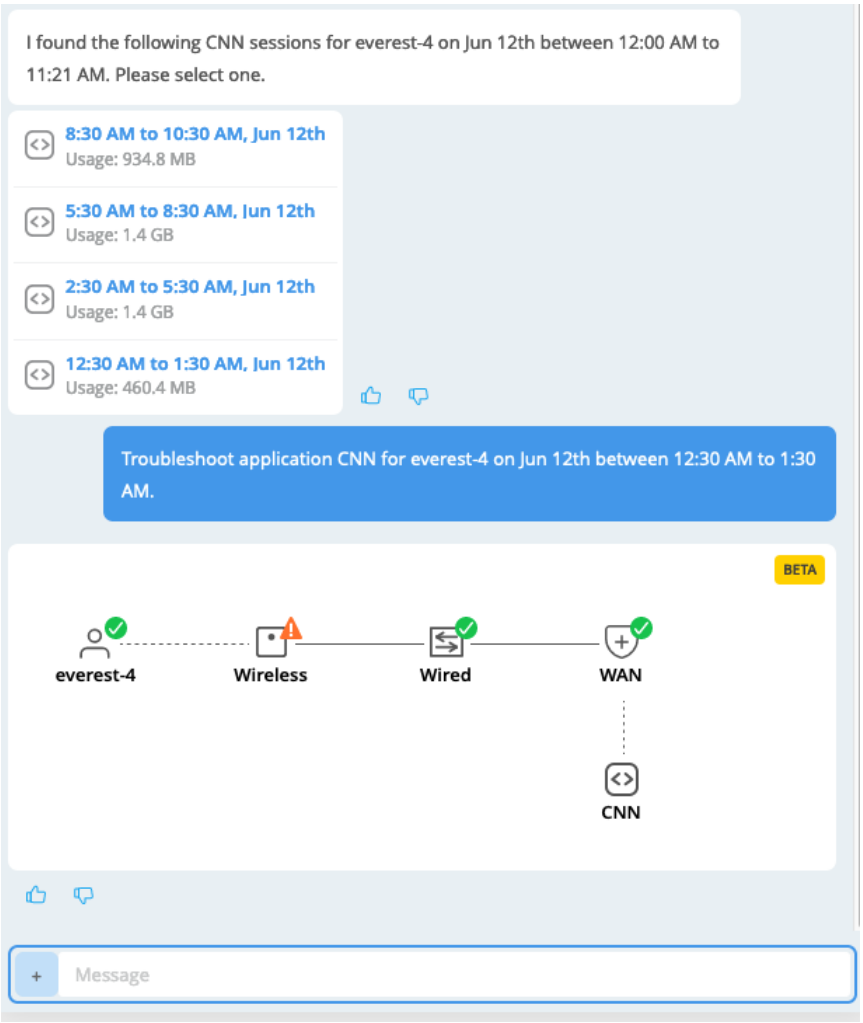
3. Select a site.

4. Select a device from the list.



5. Select a session.

   Marvis displays the Client - Application topology view. This view shows you the Wireless, Wired, and WAN categories and the status of each category. You can click any category to view issues that the device experienced when using the application.



- Click the device to view client details like the name and MAC address.
- Click **Wireless** to view the AP(s) that the device connected to for the longest time during the application session. This view also displays any issues that the AP or APs experienced.
- Click **Wired** to view the associated switches and the issues that they experienced.
- Click **WAN** to view the associated WAN edge devices and the issues that they experienced.
- Click the application to view the application details, such as server name or IP address.

> **NOTE**: Marvis includes ISP in the topology view if the ISP information is available.
>
> If your network contains only a Juniper WAN edge device and no other Juniper devices, the topology view displays only the corresponding categories such as WAN and application. The IP address of the device's application session identifies the device.

Troubleshoot Applications Using Natural Language

In the conversational assistant window, you can also type your query in natural language to troubleshoot applications. Here are a few examples:

- why zoom sessions dropped for <client>
- show outlook problems in <site> today
- troubleshoot instagram

Troubleshoot Devices Using the Conversational Assistant

SUMMARY

You can troubleshoot wireless or wired clients, access points (APs), switches, and WAN edge devices using the conversational assistant function of the Marvis® Virtual Network Assistant.

IN THIS SECTION

- Troubleshoot a Wireless Client | **79**
- Troubleshoot Unhappy Wireless Clients | **79**
- Troubleshoot Wired Clients | **80**
- Troubleshoot APs | **81**
- Troubleshoot Unhappy APs | **81**
- Troubleshoot Switches | **82**
- Troubleshoot Unhappy Switches | **83**
- Troubleshoot WAN Edge Devices | **83**
- Troubleshoot Unhappy WAN Edge Devices | **84**
- Quick Reference to Troubleshoot Devices | **85**

In the conversational assistant window of Marvis, you can select **Troubleshoot > Device** and you're ready to start troubleshooting. You can simply enter a phrase such as "troubleshoot *device name*" and Marvis can display the details. You can use these details to troubleshoot and fix the issue. The following

sections explain how you can use phrases in the conversational assistant to troubleshoot each device type.

Troubleshoot a Wireless Client

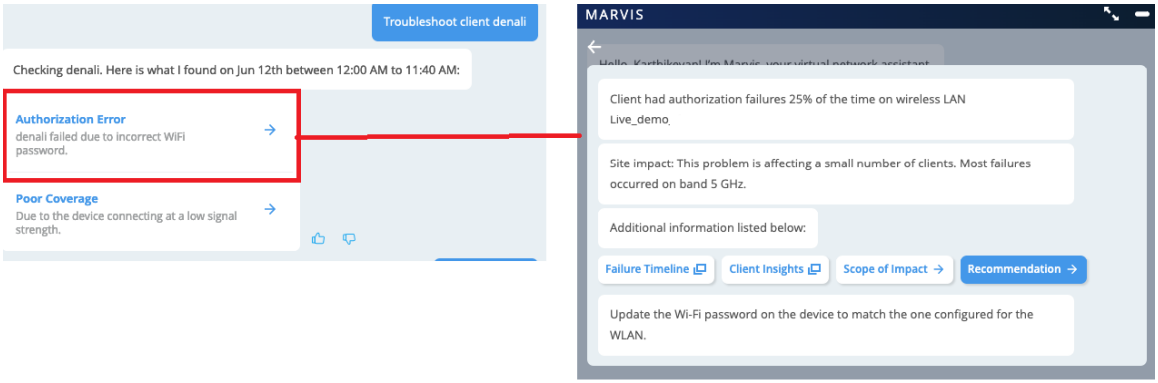
You can view failures of a wireless client and its associated access point (AP).

To check whether a wireless client is experiencing any issues, enter a phrase such as "How is *client*" or "Troubleshoot *client* for 5 july" in the conversational assistant 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 the following issues:

- An authentication error due to an incorrect Wi-Fi password
- Poor coverage due to low signal strength

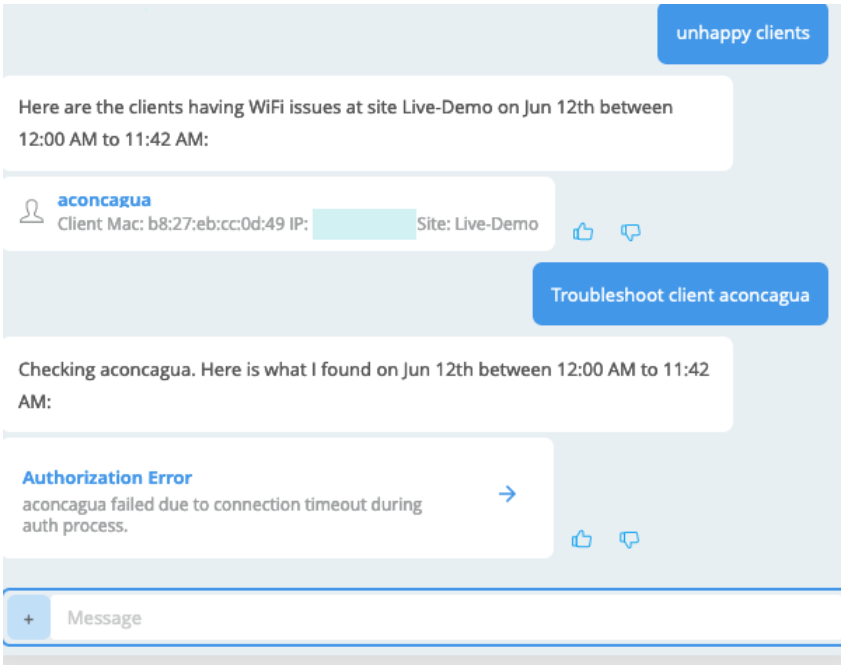
You can click each of the issues to view details about the issue. You can click the **Failure Timeline**, **Client Insights**, or **Scope of Impact** option for more details. In some cases, Marvis also provides recommendations to fix the issue, as the screenshot shows:



Troubleshoot Unhappy Wireless Clients

To determine which clients are experiencing connectivity issues (which we also refer to as *unhappy* clients), use phrases such as, "troubleshoot clients" or "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":



Troubleshoot Wired Clients

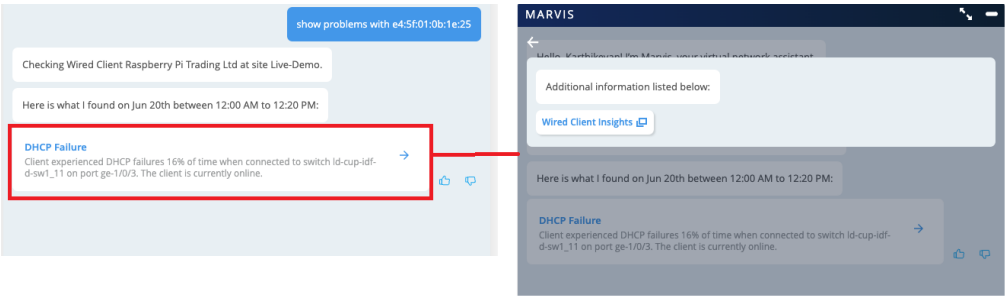
You can troubleshoot wired clients to see:

- The switch and the switch port to which the wired client is connected.
- Connection failures.
- Switch health.
- Interface status.

To view wired clients that are experiencing issues, use phrases such as the following:

- Show problems with <wired client mac>
- Was there any issue with <wired client> yesterday

  In the following example, Marvis shows that the wired client experienced a DHCP failure. If you click **DHCP Failure**, you can view more details as the screenshot shows:

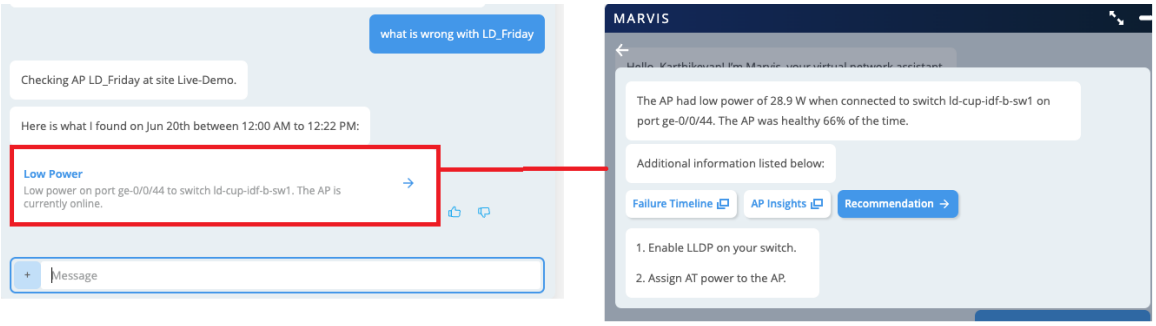


Troubleshoot APs

To troubleshoot an access point (AP), use one of the following phrases:

- What's wrong with <AP name>
- Show me problems for <AP mac>

Here's a sample screenshot that shows the output for "What's wrong with <AP name>." In this case, Marvis indicates low power on one of the AP ports that is connected to a switch. If you click the issue, Marvis displays detailed information as the screenshot shows:

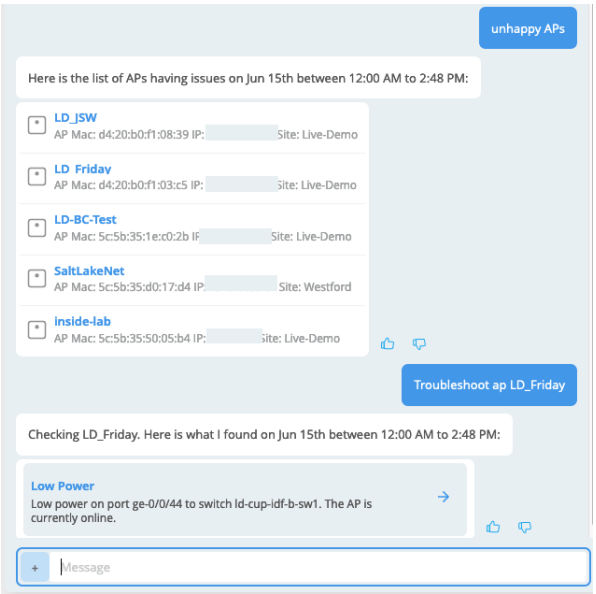


Troubleshoot Unhappy APs

Marvis can show you which APs are experiencing issues (which we refer to as unhappy APs).

To check for unhealthy APs or APs on which clients are unhappy, simply enter the phrase "troubleshoot APs" or "unhappy access points" in the conversational assistant window without providing details. You can select any AP from the list to view the troubleshooting results for that AP.

In the following screenshot, you can see that Marvis lists the APs that are experiencing issues. If you click an AP, Marvis shows the issues for that AP. In the screenshot, Marvis reports low power on a port. You can click the issue to view more details.

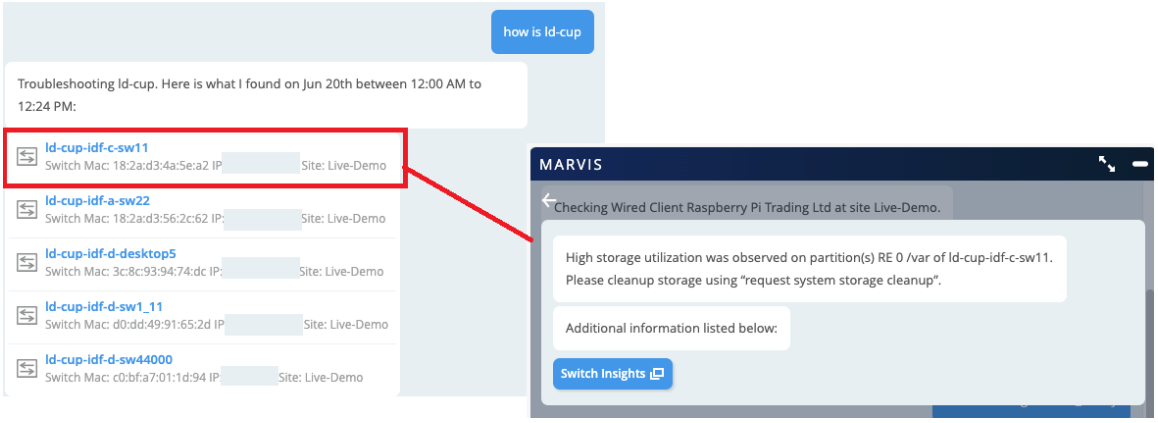


Troubleshoot Switches

To troubleshoot switches, use phrases such as:

- How is <partial name of a switch>
- show me issues for <switch>

Here is a sample screenshot that shows the results for "How is id-cup." You can click a switch to view more details about the issue.

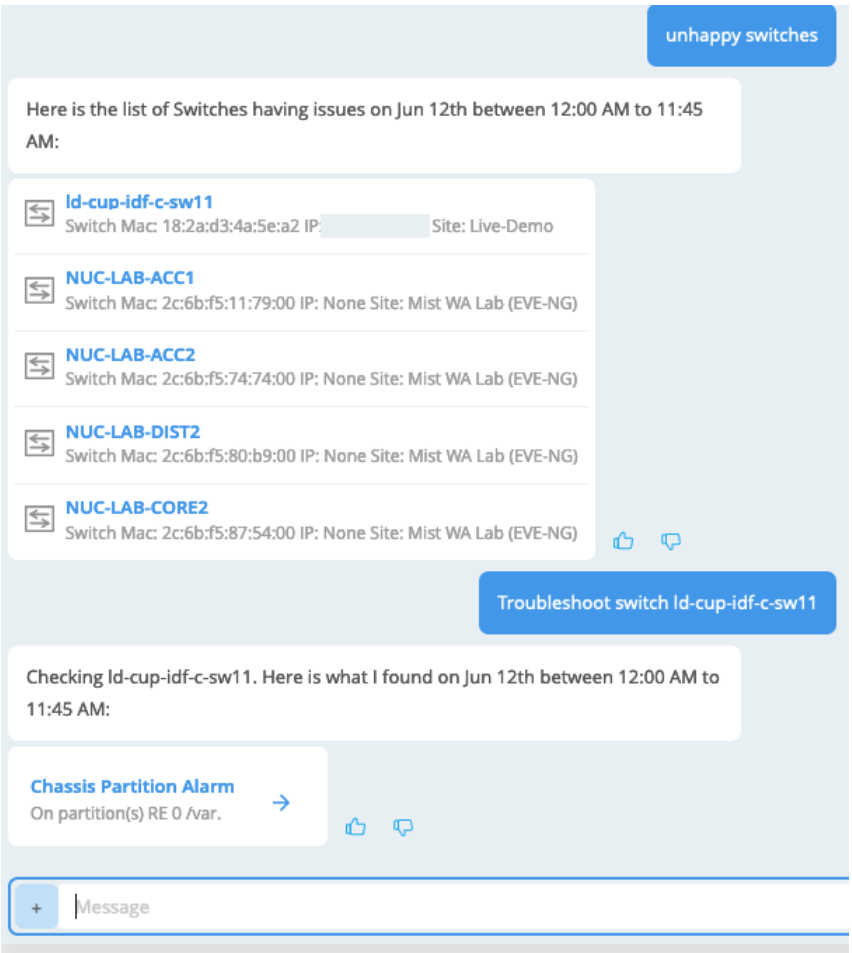


Troubleshoot Unhappy Switches

Marvis can show you the switches that are experiencing issues (which we refer to as *unhappy* switches).

To check for unhappy switches, simply enter the phrase "troubleshoot switches" or "unhappy switches" in the conversational assistant window, without providing details. You can select any switch from the list to view the troubleshooting results for the switch.

In the following example, you can see that Marvis displays all the switches that are experiencing issues. You can click any switch to view the issues. In this case, Marvis indicates that a chassis alarm has been triggered.



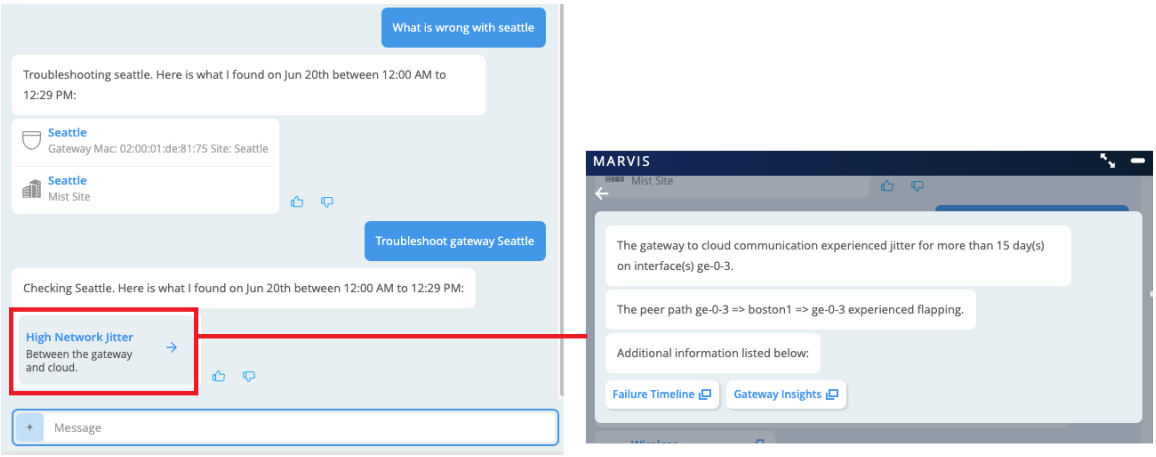
Troubleshoot WAN Edge Devices

To troubleshoot WAN edge devices, use phrases such as:

- Show problems with <WAN edge mac>

- What's wrong with <WAN edge>

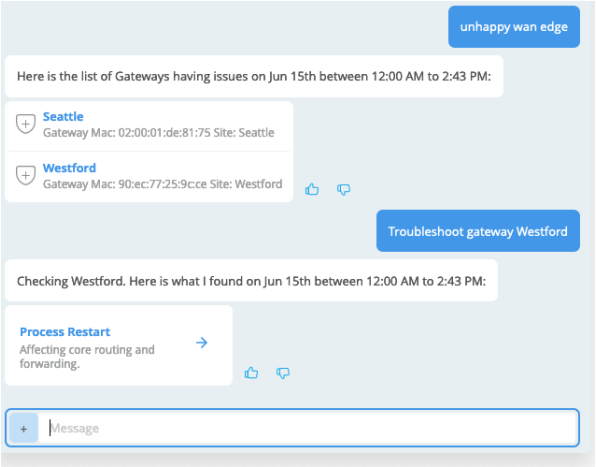
  The following screenshot shows the details that Marvis displays for the "What's wrong with <WAN edge>" phrase:



Troubleshoot Unhappy WAN Edge Devices

To check for unhappy WAN edge devices, simply enter the phrase "troubleshoot WAN edges" or "unhappy WAN edges" in the conversational assistant window, without providing details. You can select any WAN edge device from the list to view the troubleshooting results for the device.

In the following example, you can see that Marvis displays all the WAN edge devices that are experiencing issues. You can click any device to view the issues.



Quick Reference to Troubleshoot Devices

The following table summarizes the phrases presented in the related topics. You can use this table as a point of reference when you troubleshoot devices in a Mist network using the conversational assistant function of Marvis.

To Troubleshoot	Use
A wireless client	• How is *client* • Troubleshoot *client*
Unhappy wireless clients	• troubleshoot clients • unhappy clients
A wired client	• Show problems with *wired client mac* • Was there any issue with *wired client* yesterday
An AP	• What's wrong with *AP name* • Show me problems for *AP mac*
Unhappy APs	• troubleshoot APs • unhappy access points
A switch	• How is *partial name of a switch* • show me issues for *switch*
Unhappy switches	• troubleshoot switches • unhappy switches

(Continued)

To Troubleshoot	Use
A WAN edge device	• Show problems with *WAN edge mac* • What's wrong with *WAN edge*
Unhappy WAN edge devices	• troubleshoot WAN edges • unhappy WAN edges
List device, users (wired or wireless clients), firmware version	• List APs with Version *version-number* • List switches on site *site-name*

Troubleshoot Sites Using the Conversational Assistant

IN THIS SECTION

- Troubleshoot Sites Using the Menu Option | 86
- Troubleshoot Sites Using Natural Language | 89

You can use the **Troubleshoot > Site** menu option to troubleshoot sites to identify site-level failures and view details of the failures.

Troubleshoot Sites Using the Menu Option

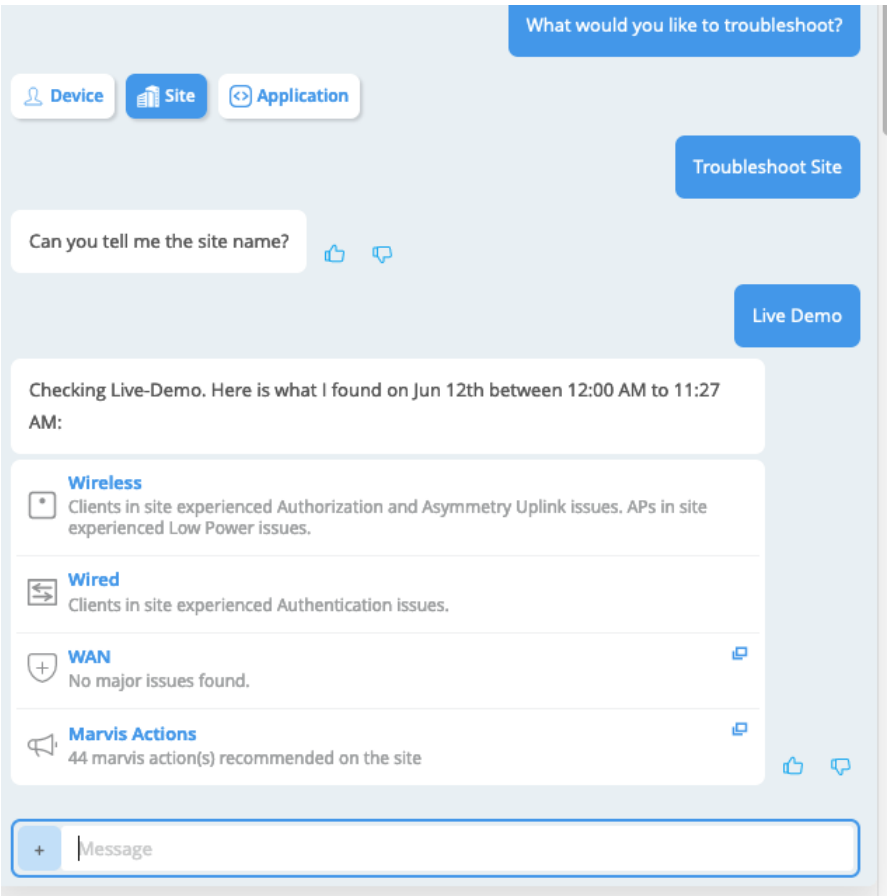
1. In the conversational assistant window, select **Troubleshoot > Site**.

Marvis prompts you for the site name.

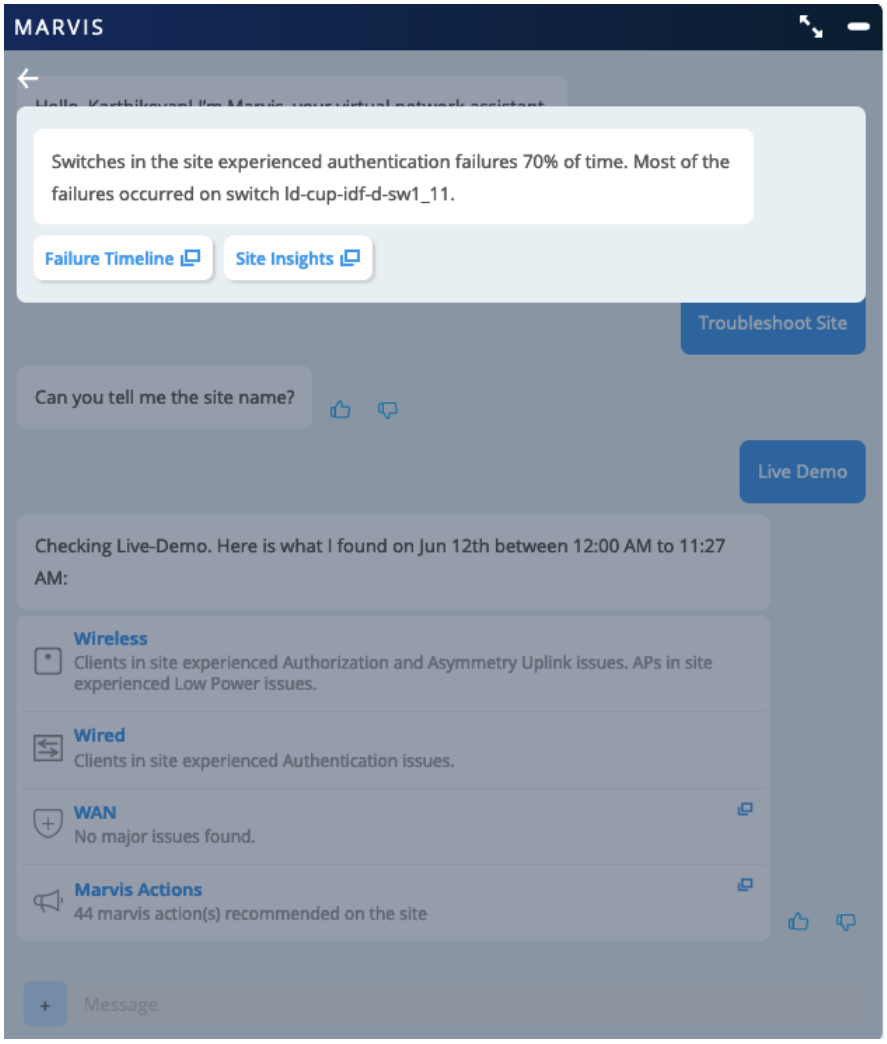
2. Enter the site name.

   Marvis shows the troubleshooting results for the site. Marvis indicates the top failures along with the reasons for the failure. Marvis classifies these failures under the following categories:

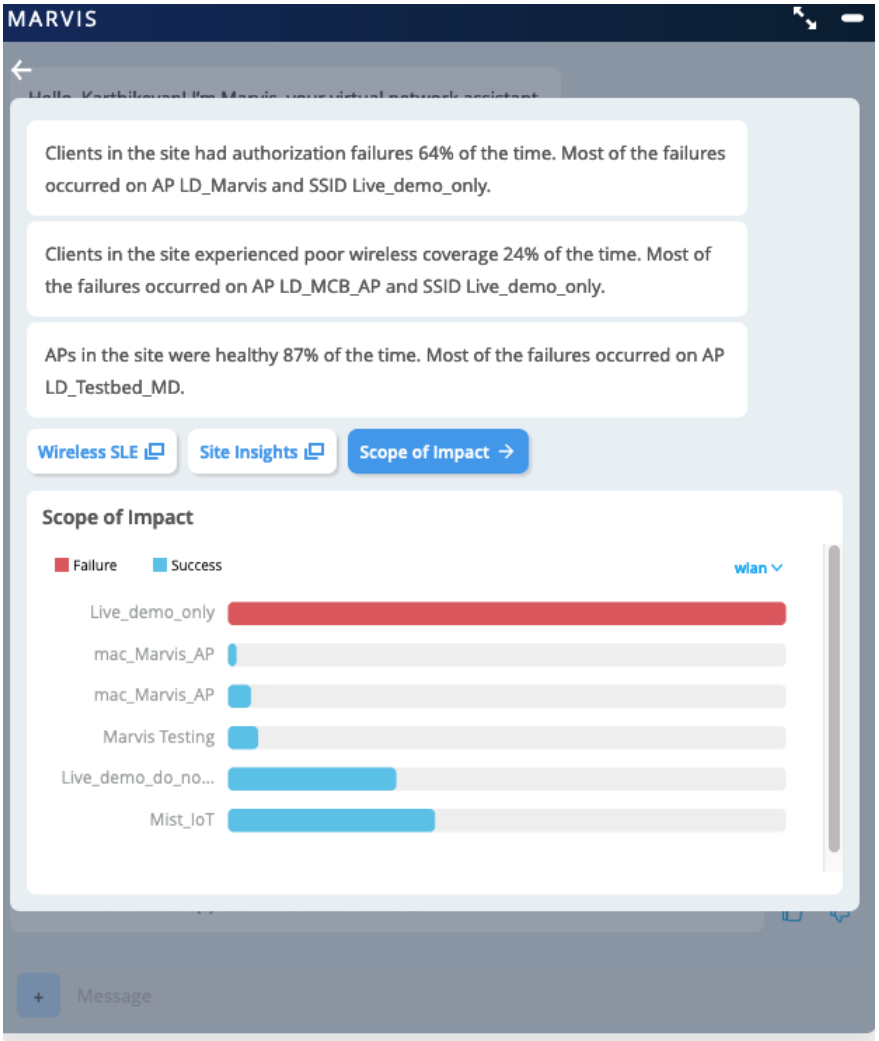
   - Wireless
   - WAN
   - Wired
   - Marvis Actions



3. Click a particular category to view details about the failure. The details vary based on the category you select. For example, here's an example of what you'll see when you click the Wired category. You can click **Failure Timeline** and **Site Insights** to view more details.



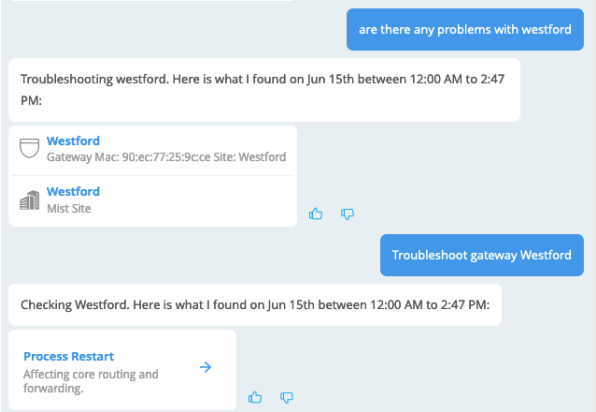
In the following screenshot, you can see the options displayed for the Wireless category. If you click **Scope of Impact**, Marvis displays the details at the bottom of the page. Marvis also shows recommendations, wherever applicable.



Troubleshoot Sites Using Natural Language

You can also choose to directly type your query in the conversational assistant window. Here are a few examples:

- How is <site-name>
- Are there any problems with <site-name>
- Troubleshoot site


are there any problems with westford
Troubleshooting westford. Here is what I found on Jun 15th between 12:00 AM to 2:47 PM:
Westford
Gateway Mac: 90:ec:77:25:9c:ce Site: Westford
Westford
Mist Site
Troubleshoot gateway Westford
Checking Westford. Here is what I found on Jun 15th between 12:00 AM to 2:47 PM:
Process Restart
Affecting core routing and forwarding.

6

CHAPTER

Marvis App for Teams

Overview of the Marvis Conversational App for Microsoft Teams | 92

Enable or Integrate the Marvis App in Microsoft Teams | 92

Install the Marvis App in Microsoft Teams | 95

Troubleshoot Using the Marvis App | 103

Search and List Functions in the Marvis App | 111

View or Change the Organization in the Marvis App | 115

Overview of the Marvis Conversational App for Microsoft Teams

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:

Enable or Integrate the Marvis App in Microsoft Teams

IN THIS SECTION

- Enable the Marvis App in Your Teams Environment | **93**
- Add the Permission Policy for the Marvis App | **94**
- Assign the Policy to Users | **94**

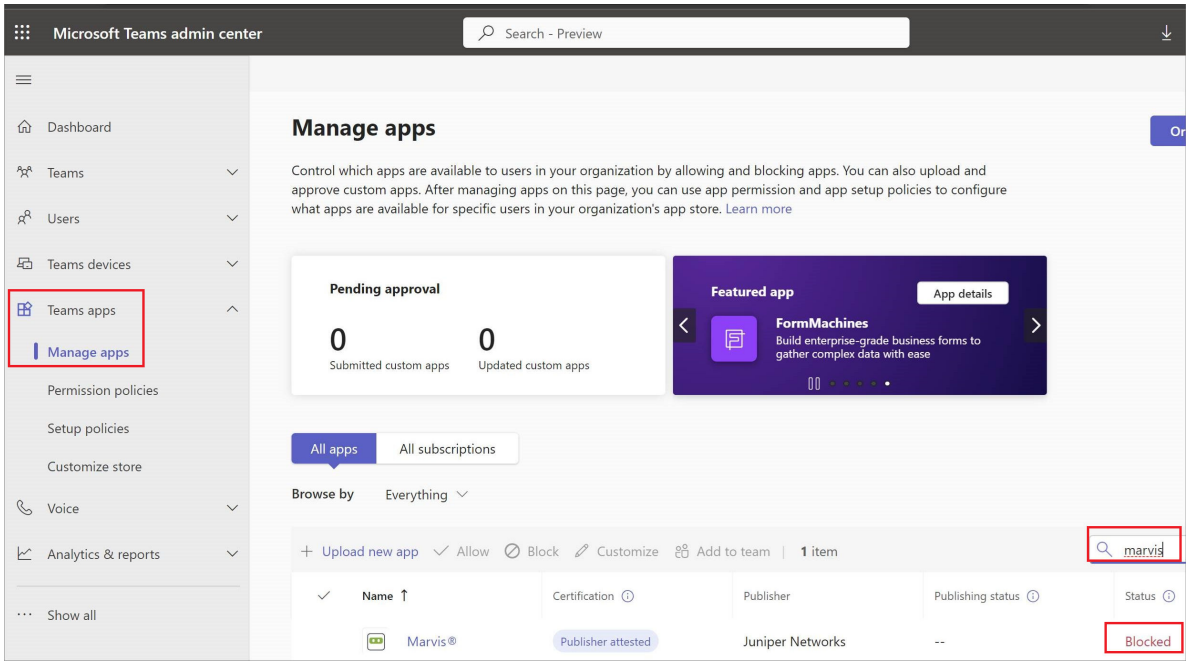
Your Microsoft Teams administrator can enable or integrate a third-party application such as Marvis in Teams. This topic provides the procedures to integrate the Marvis app in Teams.

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

IN THIS SECTION

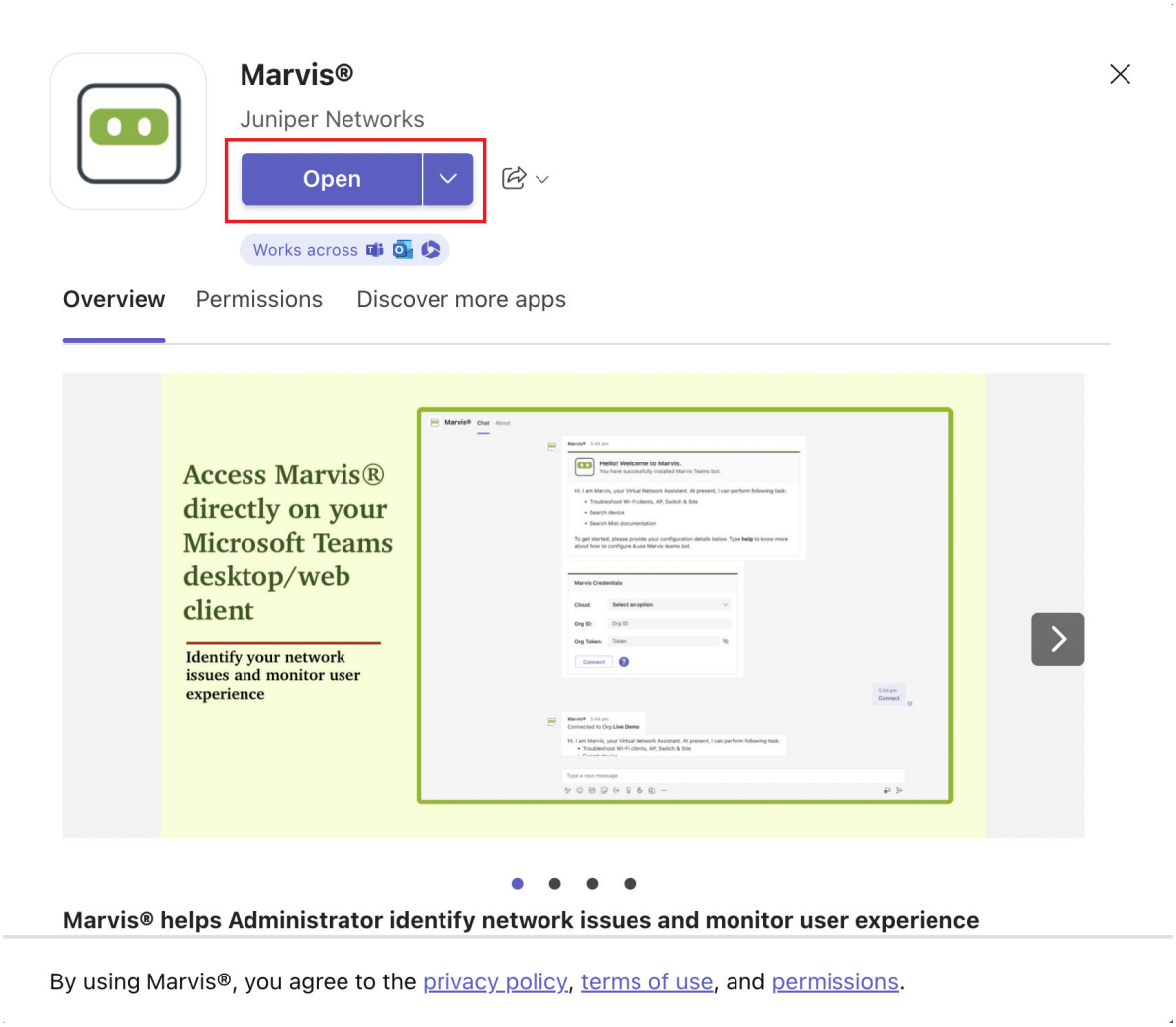
- Install the Marvis App in Teams | 95
- Connect to Your Mist Organization | 97
- Add the Marvis App to a Microsoft Teams Channel | 101

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 92.

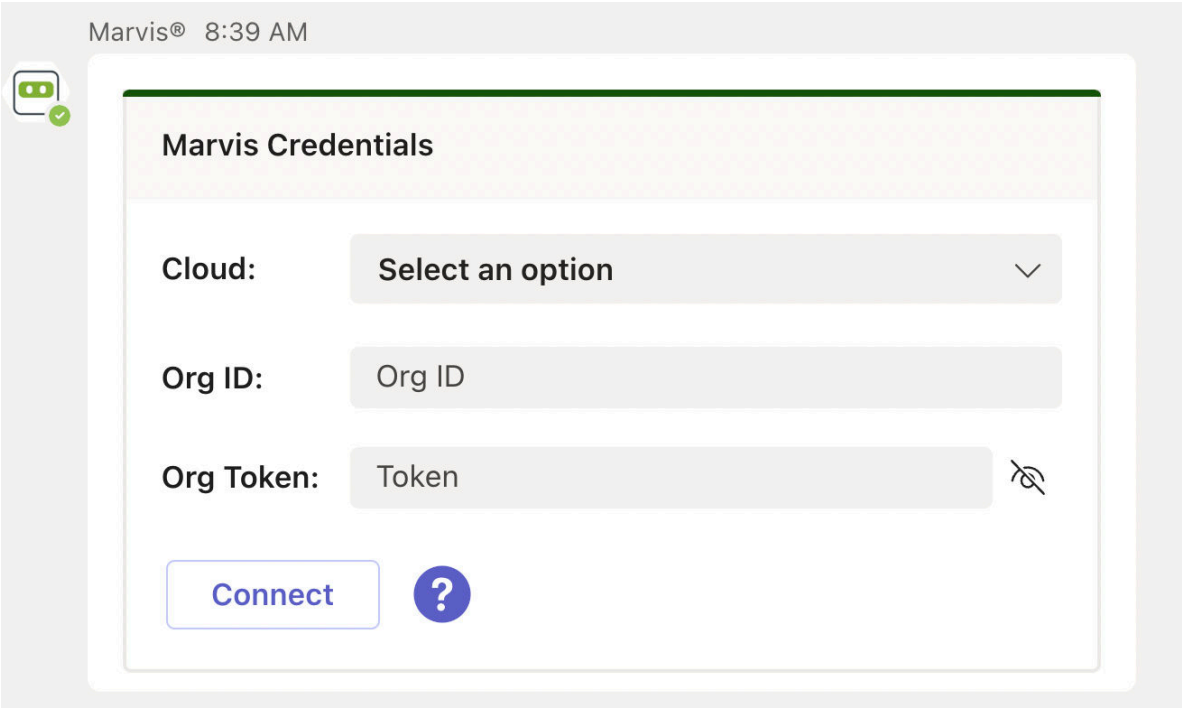
Install the Marvis App in Teams

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:

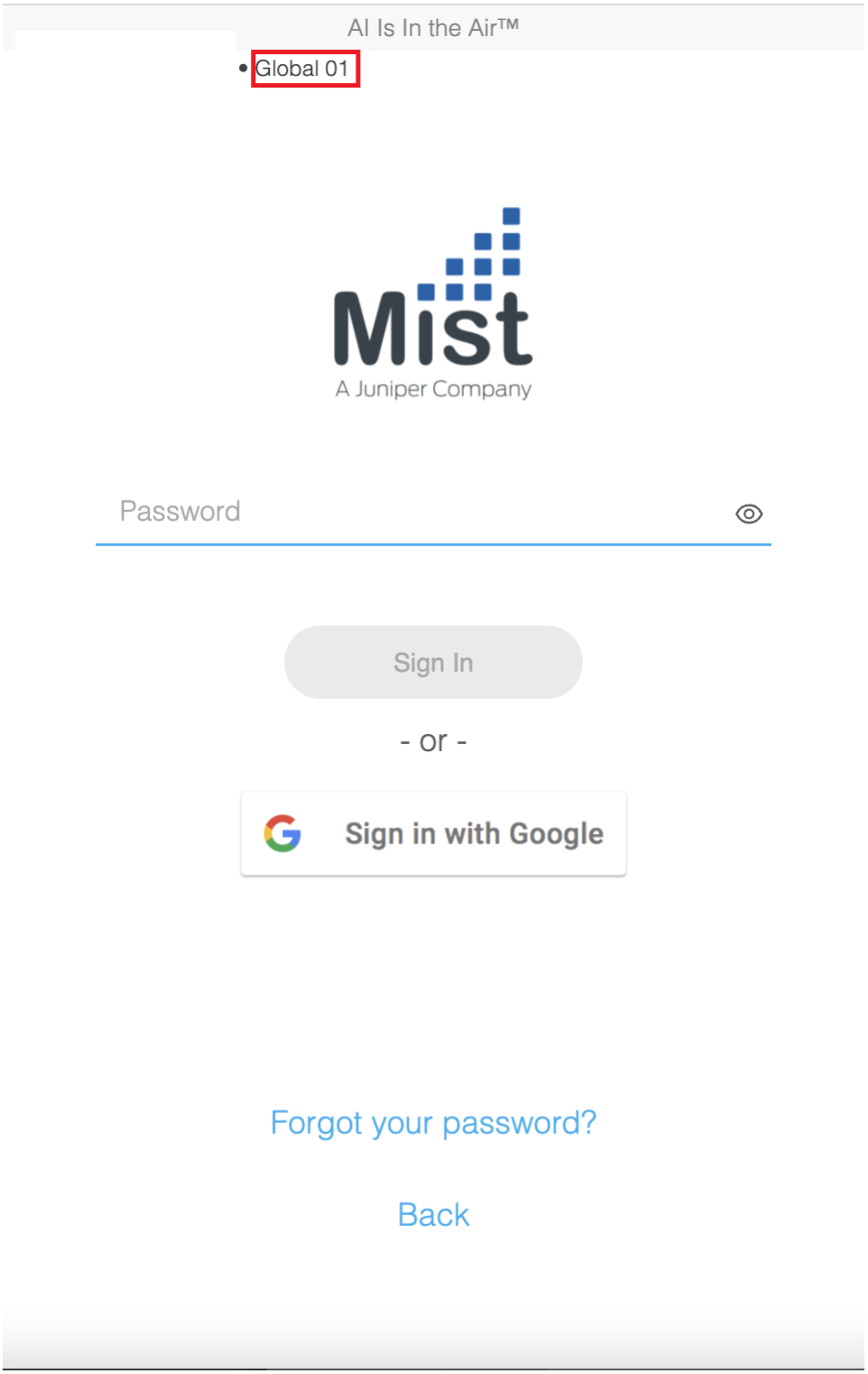


4. Next, you'll need to connect to your organization in the Mist portal.

Connect to Your Mist Organization

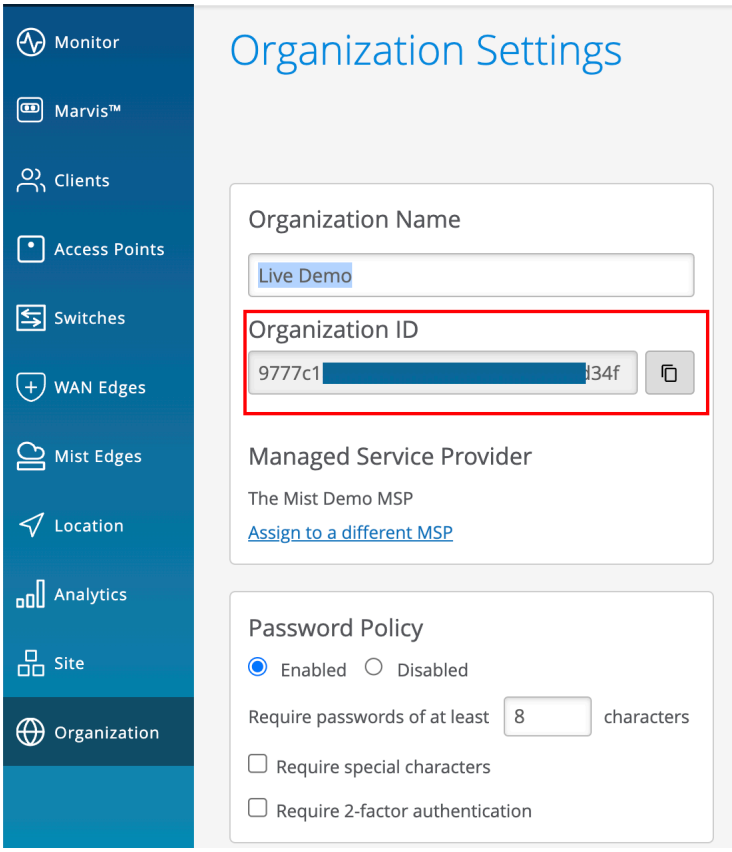
To connect to your Mist organization:

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.



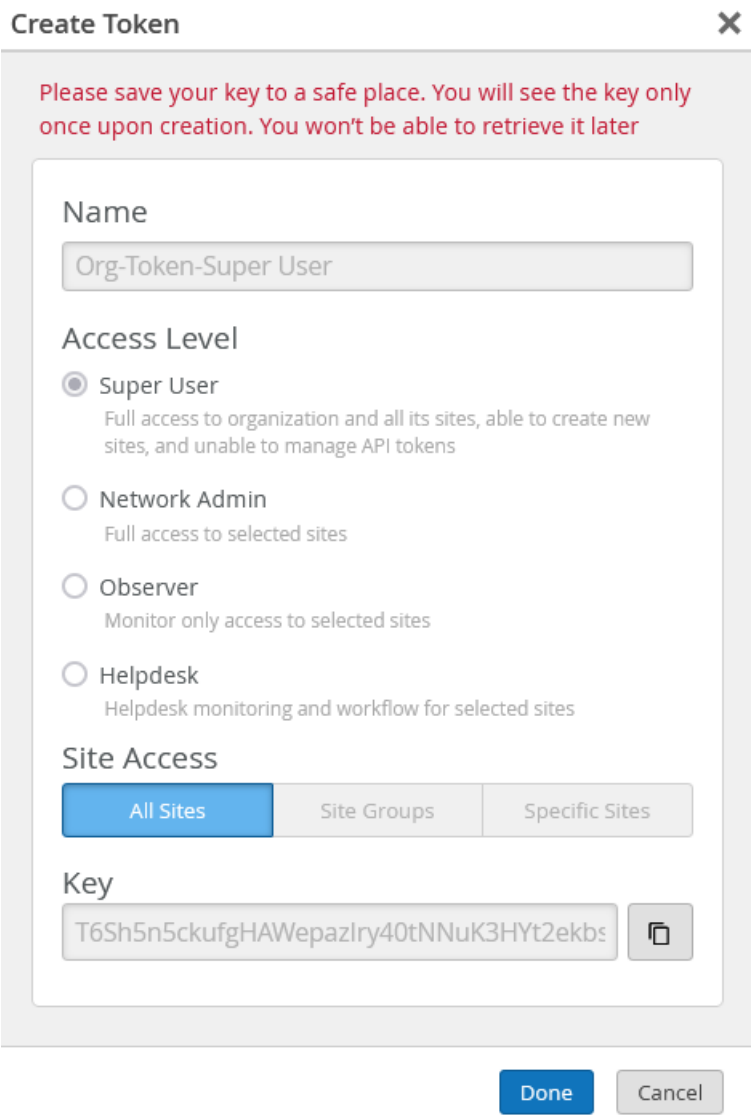
- Org Token

  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.

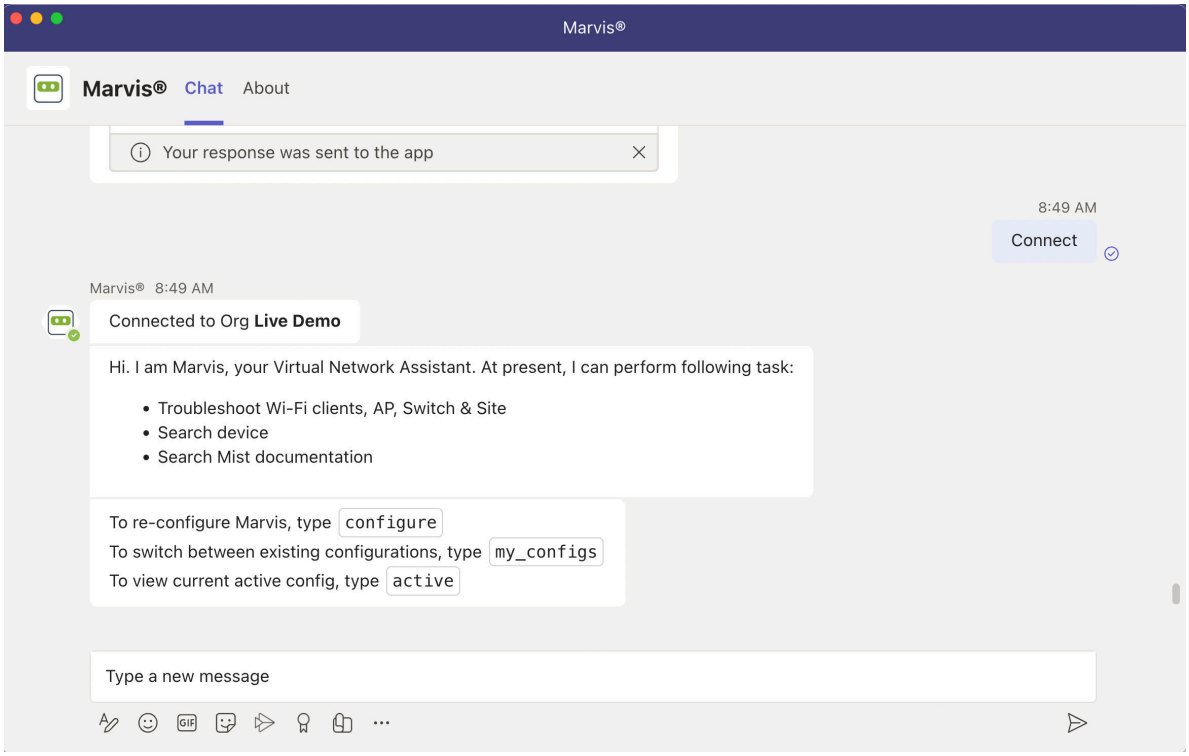
  To create a token:

  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.


Create Token
Please save your key to a safe place. You will see the key only once upon creation. You won't be able to retrieve it later
Name
Org-Token-Super User
Access Level
Super User
Full access to organization and all its sites, able to create new sites, and unable to manage API tokens
Network Admin
Full access to selected sites
Observer
Monitor only access to selected sites
Helpdesk
Helpdesk monitoring and workflow for selected sites
Site Access
All Sites
Site Groups
Specific Sites
Key
T6Sh5n5ckufgHAWepazIry40tNNuK3HYt2ekbs
Done
Cancel

2. Click **Connect**. A successful connection displays the following window:



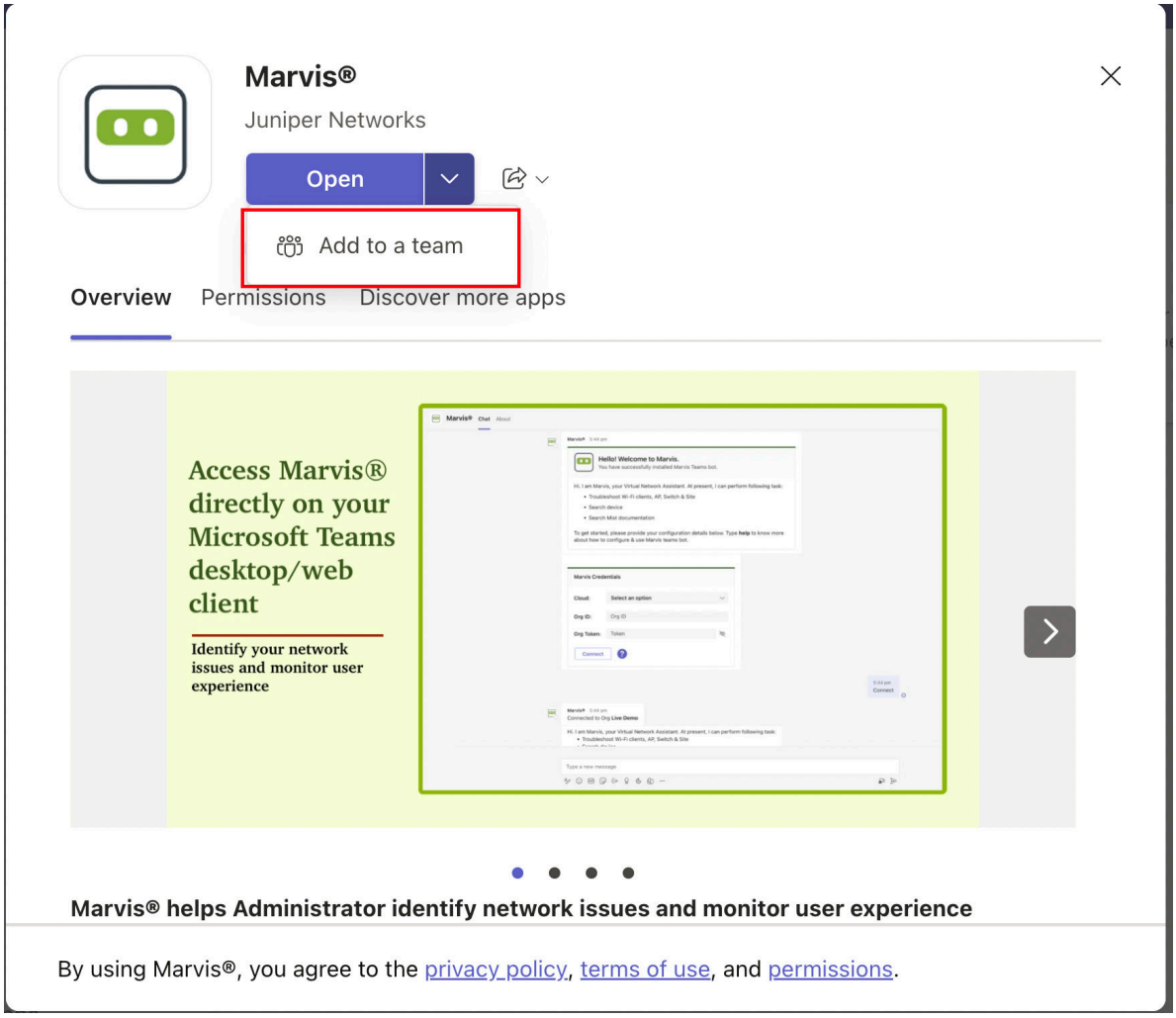
Add the Marvis App to a Microsoft Teams Channel

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.

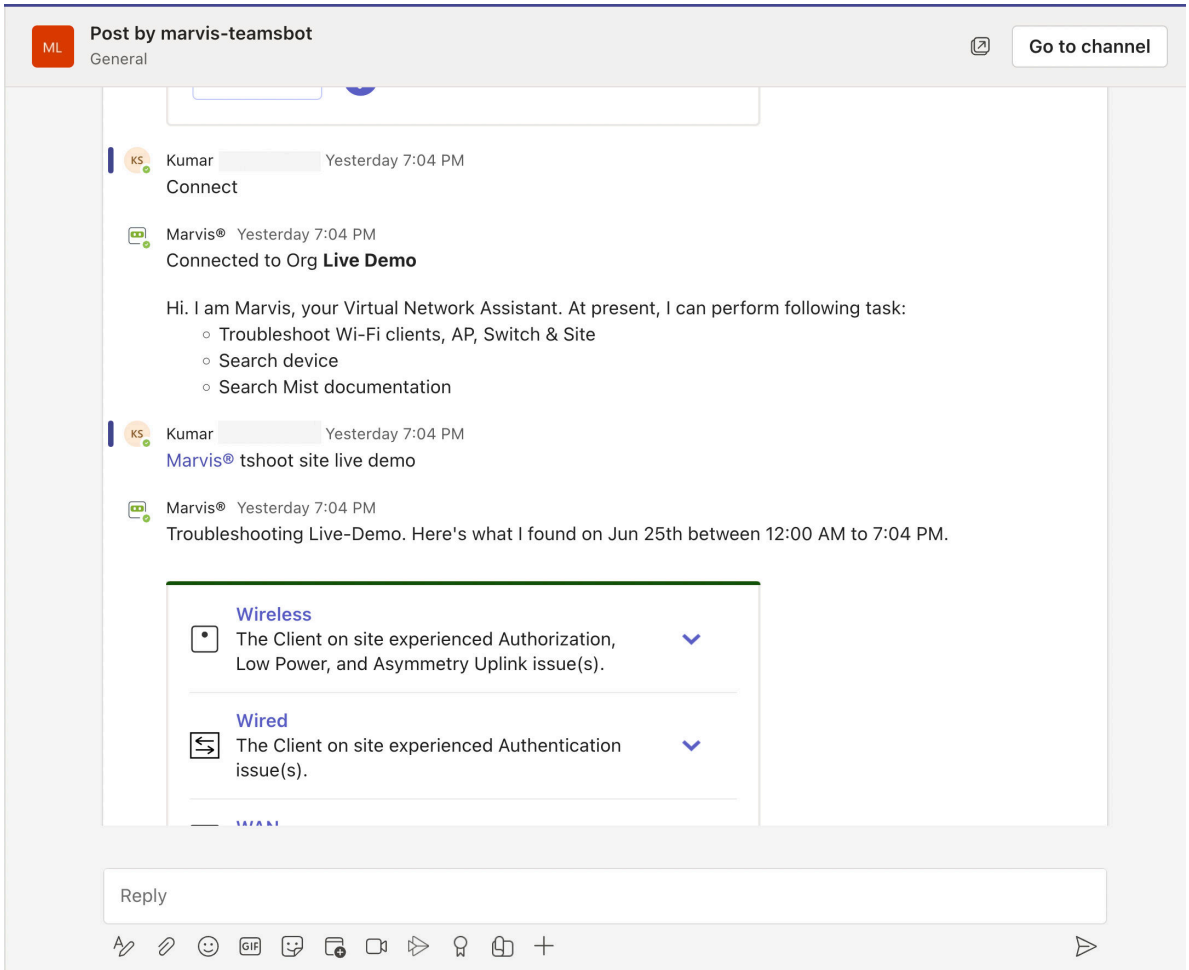
To add the Marvis app to a Microsoft Teams channel:

1. In the left pane of your Microsoft Teams window, select **Apps**.
2. Enter **Marvis** in the Search box and click the **Search** icon.
   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

IN THIS SECTION

- Troubleshoot a Wireless Client | **104**
- Troubleshoot a Wired Client | **105**
- Troubleshoot a Device | **105**
- Troubleshoot Unhappy Devices or Clients | **107**
- Troubleshoot a Site | **109**

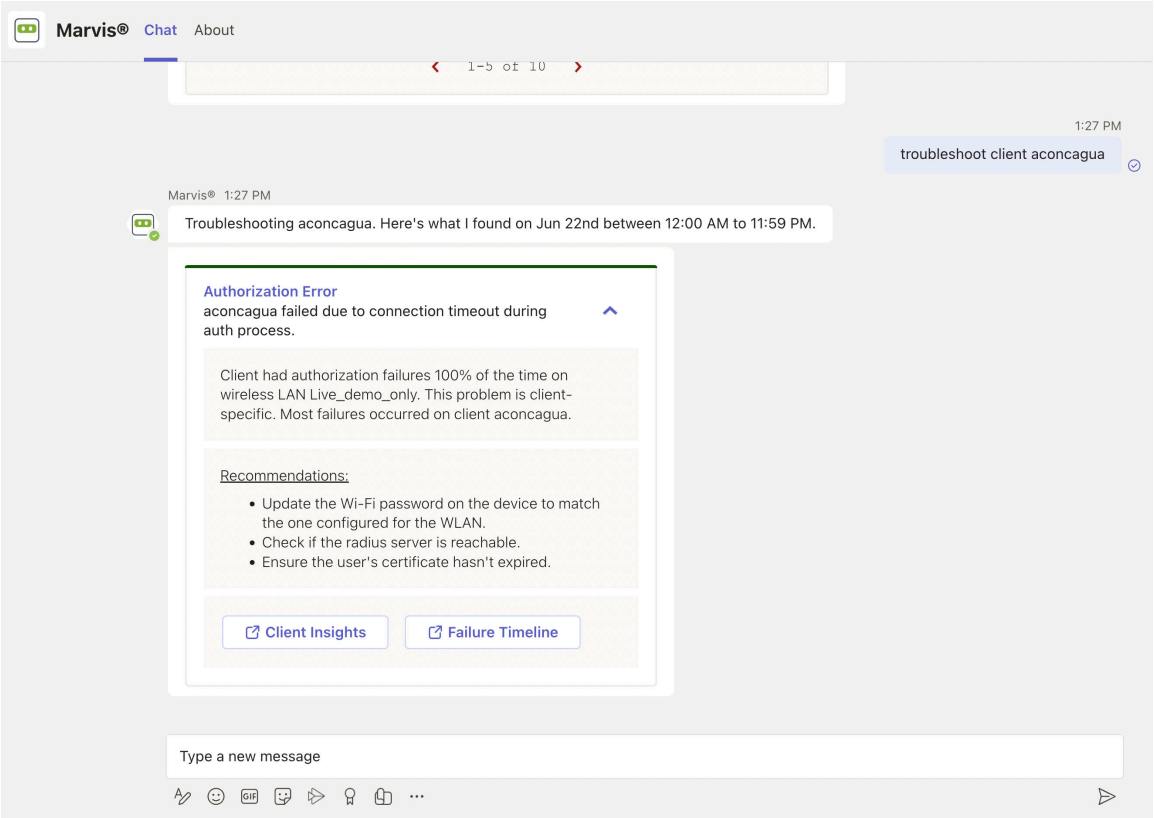
The following topics describe how to use the Marvis app to troubleshoot wireless and wired clients, devices, and sites.

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:

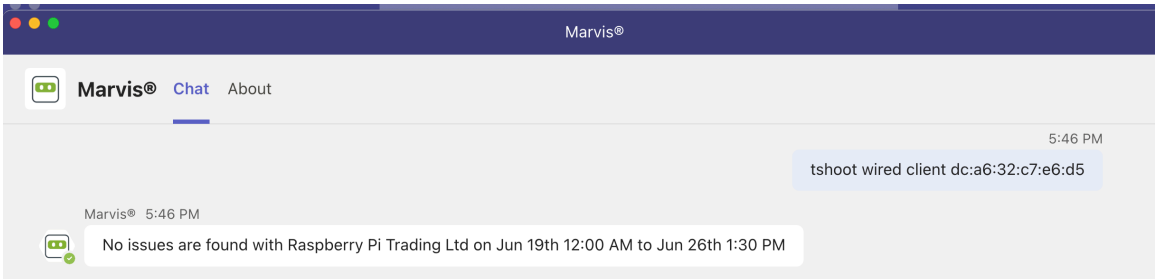
- how was <client name> on June 22nd
- tshoot client <mac or name> on June 21

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>".

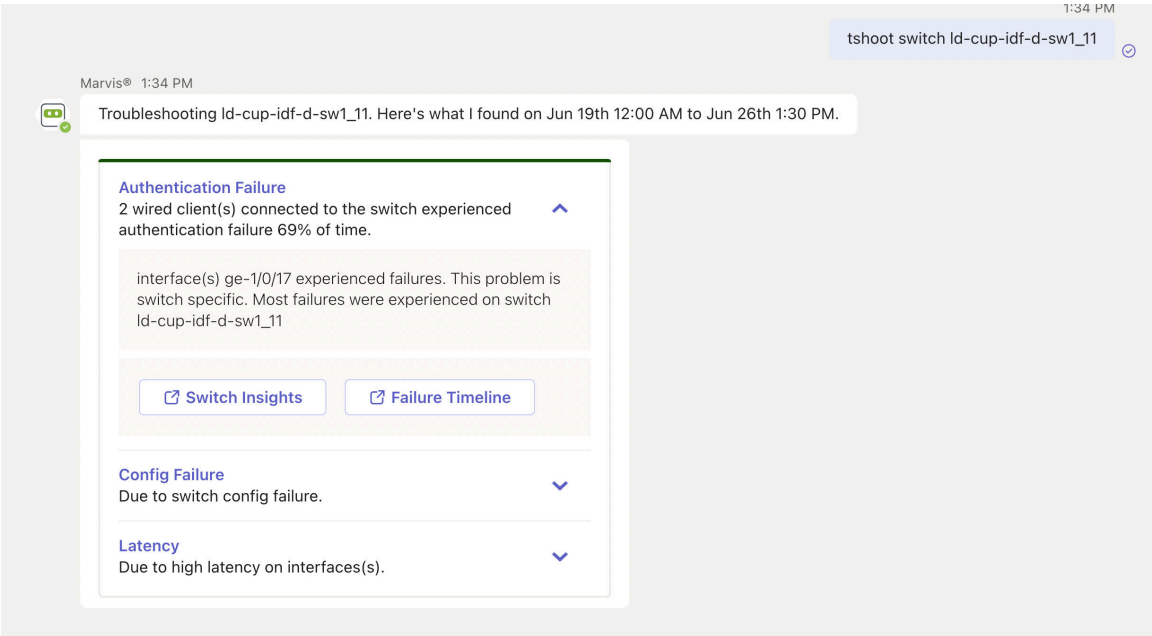


Troubleshoot a Device

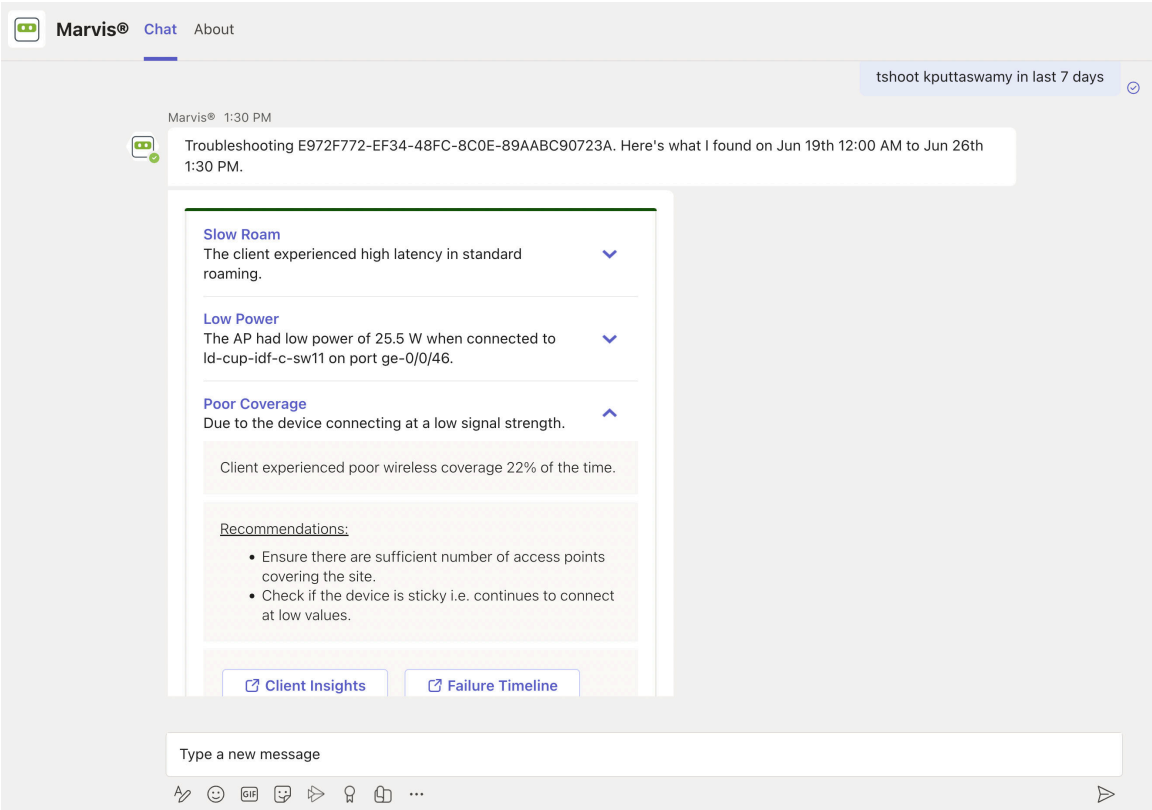
You can use the Marvis app to check for issues on APs, switches, or WAN edge devices.

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:

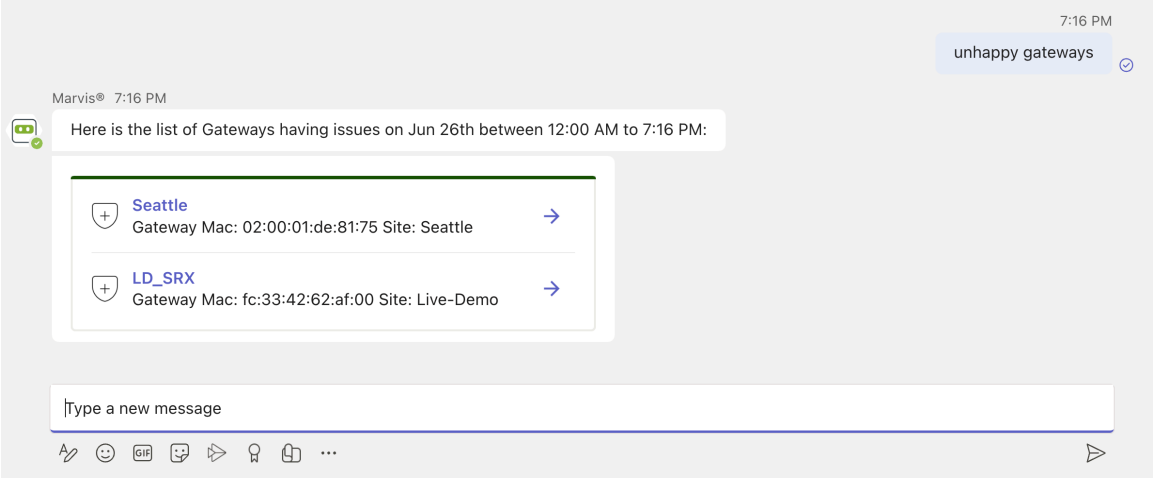


Troubleshoot Unhappy Devices or Clients

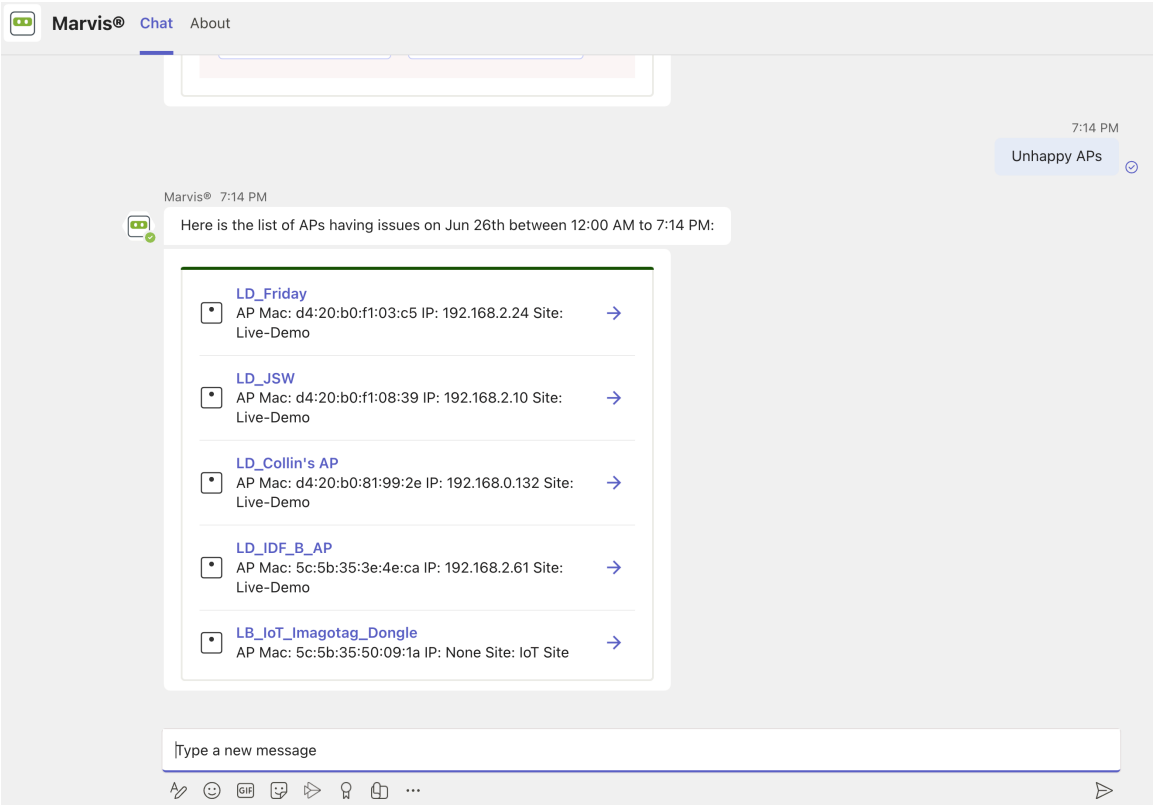
To check for devices experiencing issues (unhappy devices), simply enter the phrase "unhappy <device type>" in the Marvis chat window. For example, if you want to view unhappy WAN edge devices, enter "unhappy WAN edges" and Marvis will show all the WAN edges that are experiencing issues.

Here are a few examples. You can click any device to view the issues.

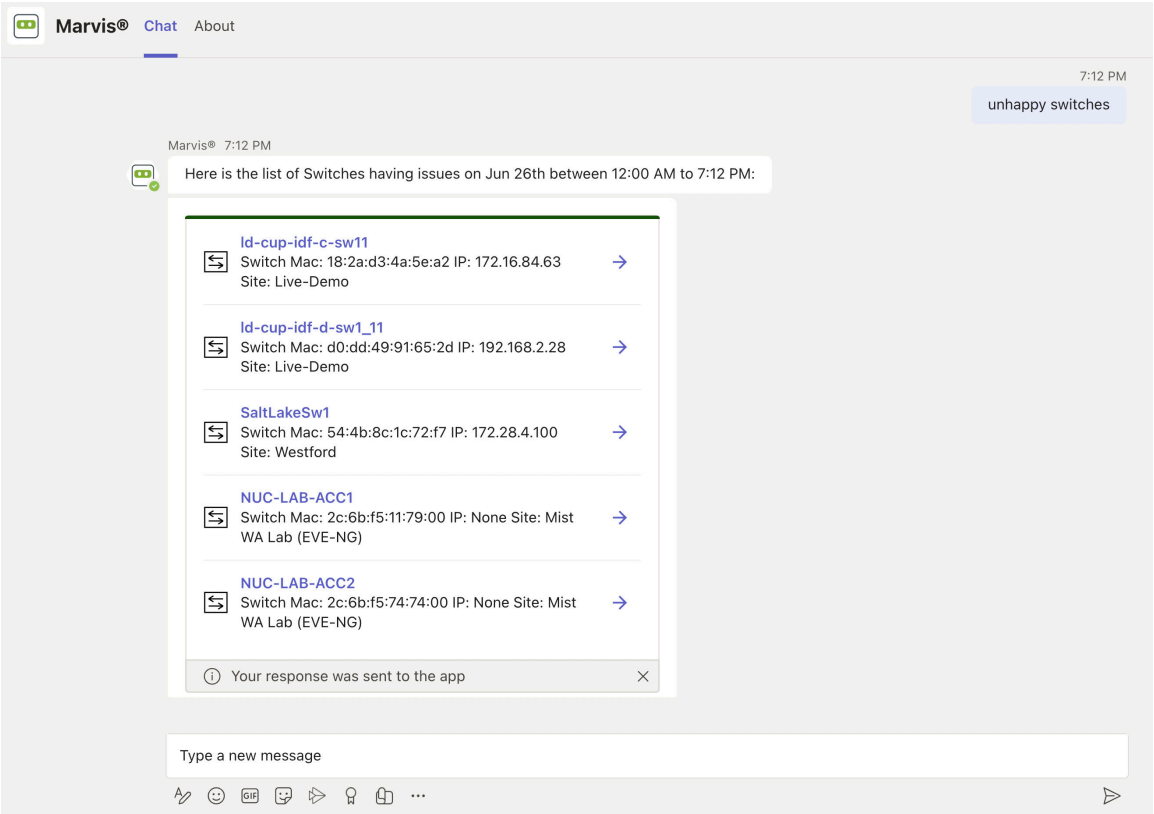
Unhappy WAN edges:



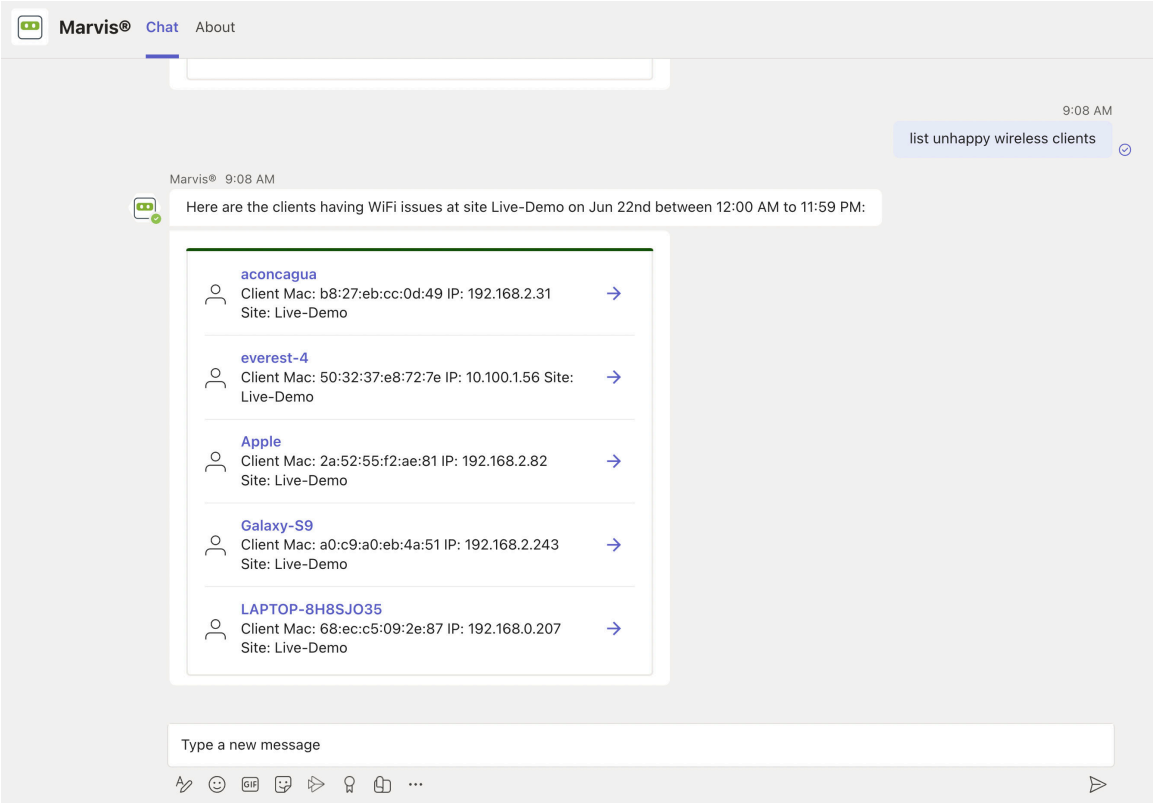
Unhappy APs:



Unhappy Switches:



Unhappy Wireless Clients:



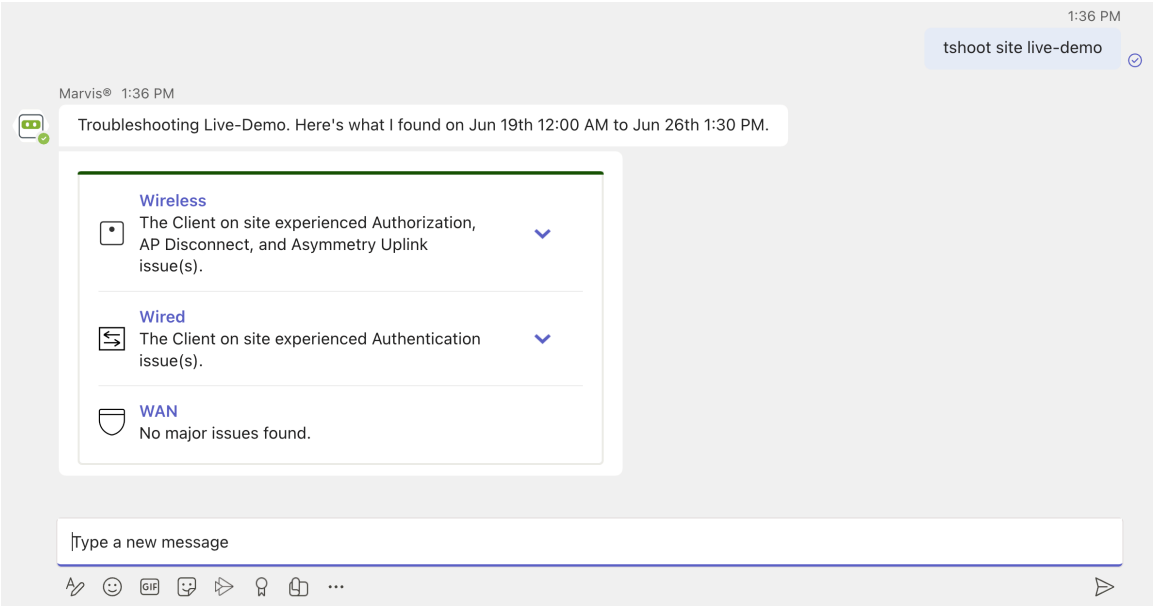
Troubleshoot a Site

You can use the Marvis app to troubleshoot sites to identify site-level failures.

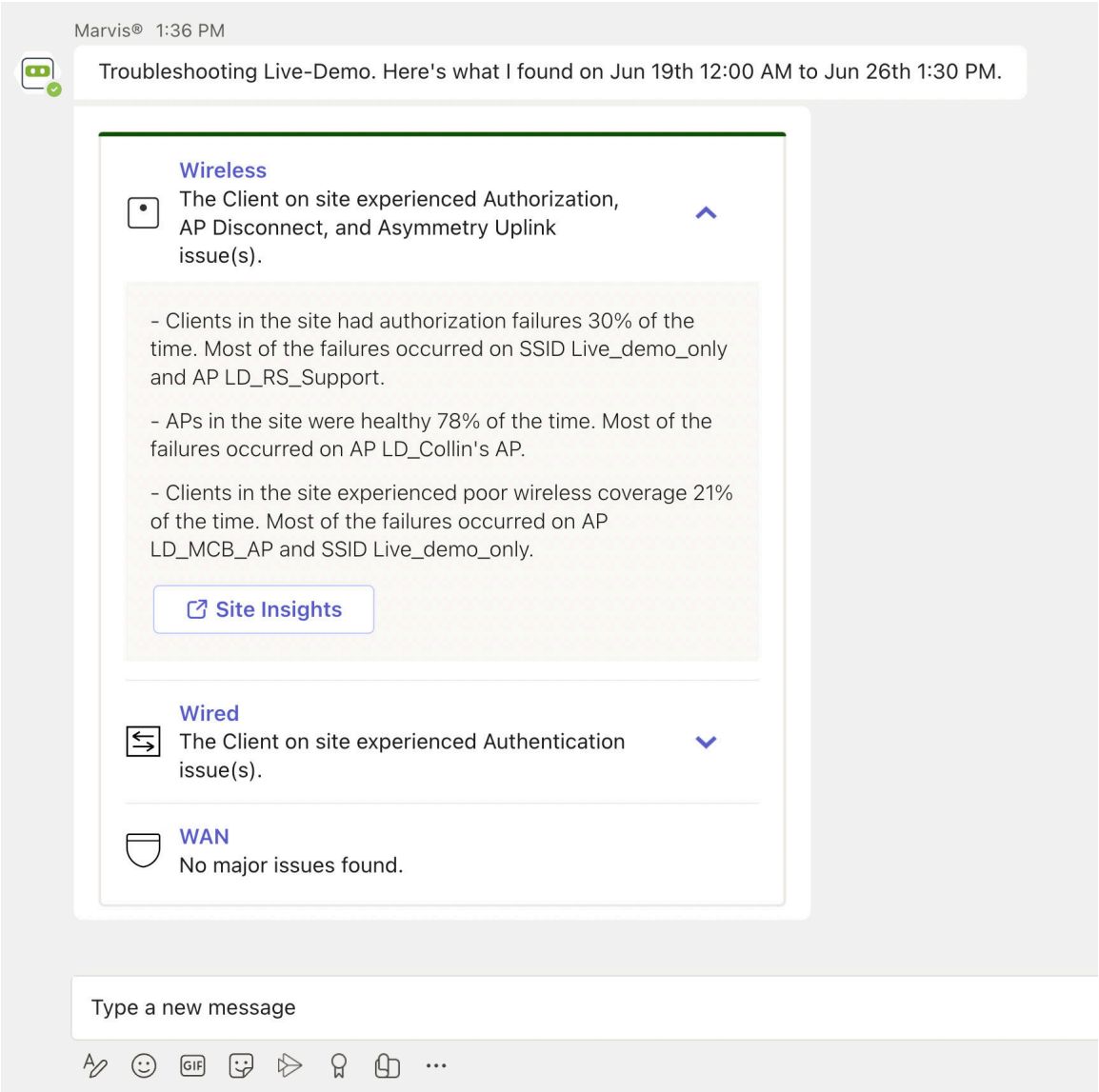
To check whether a device is experiencing any issues, enter a phrase such as "troubleshoot site *name*" in the Teams window.

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

IN THIS SECTION

- Search for Devices and Sites | **112**
- Search for Documentation | **113**
- List Function | **114**

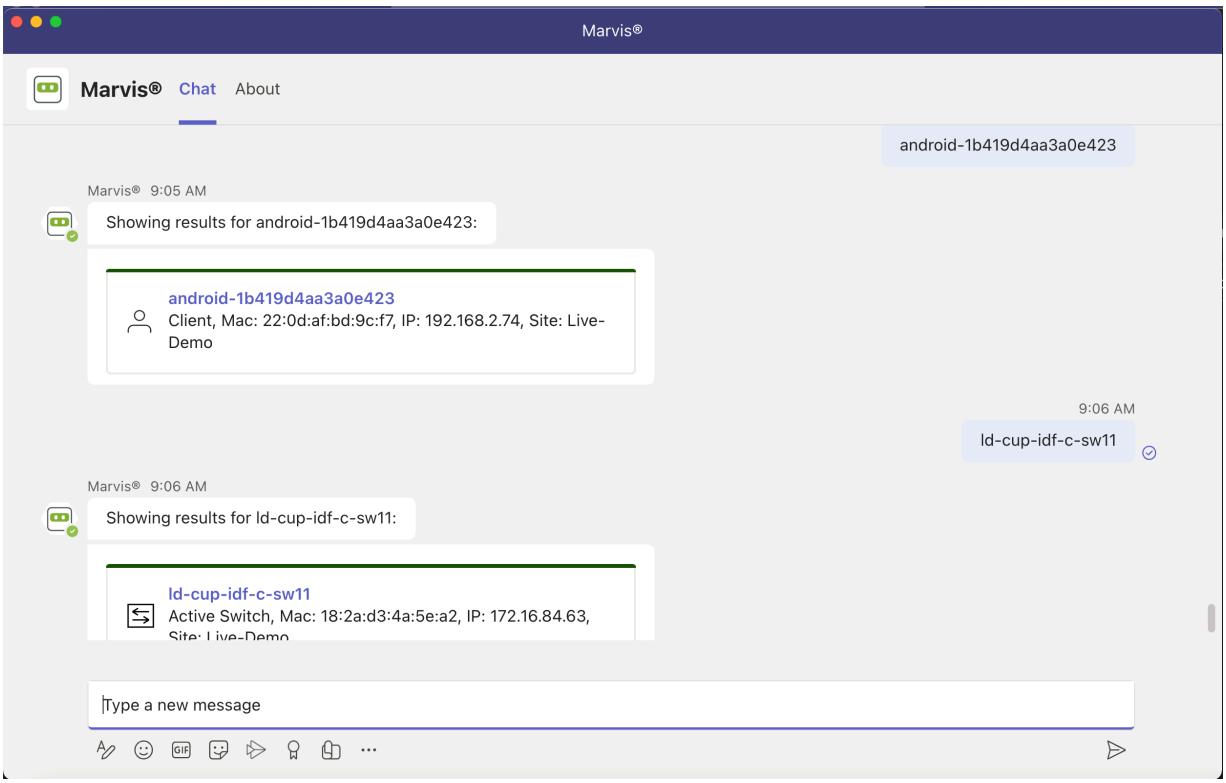
You can use the Marvis App to search for devices and sites. You can also search for documentation.

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:



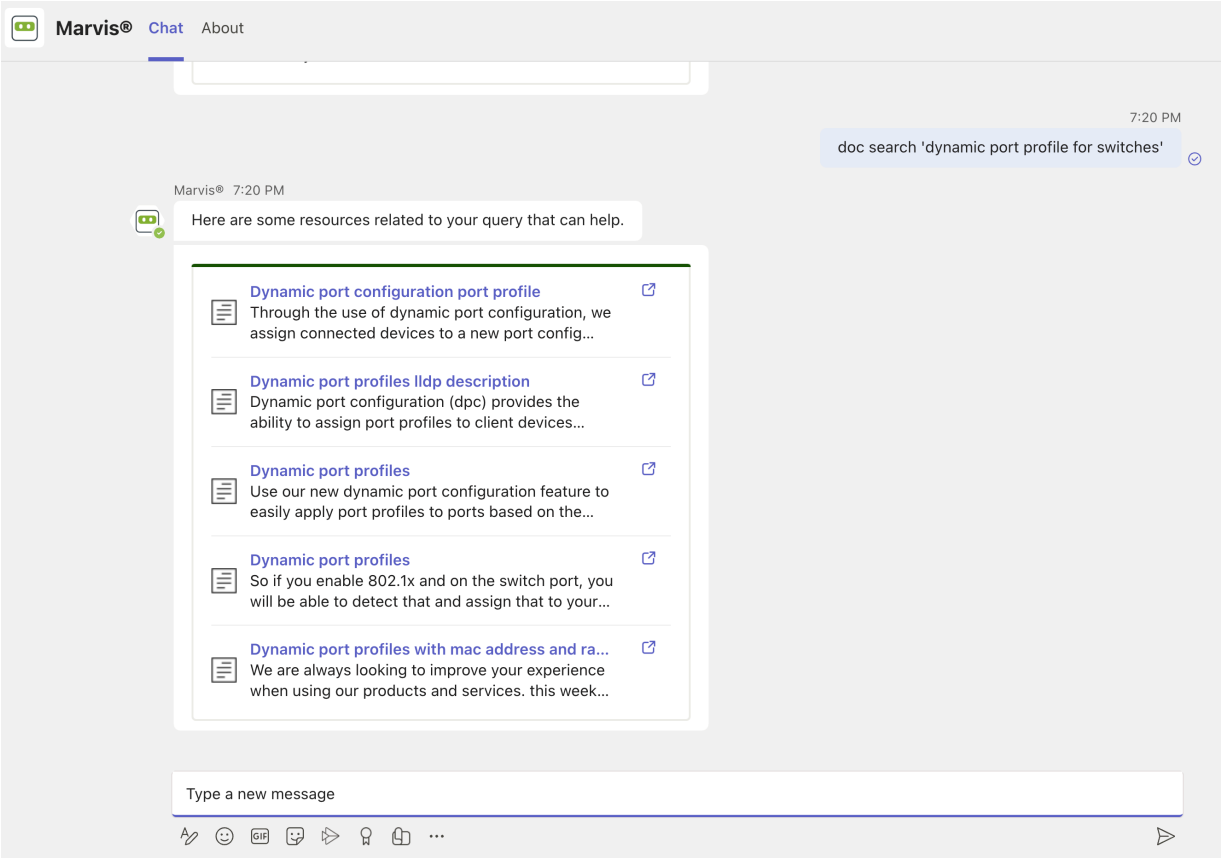
Here are some examples of phrases that you can use to search for a device or site:

- <client name>
- Search <ap mac> <switch model>
- Find <WAN edge mac>

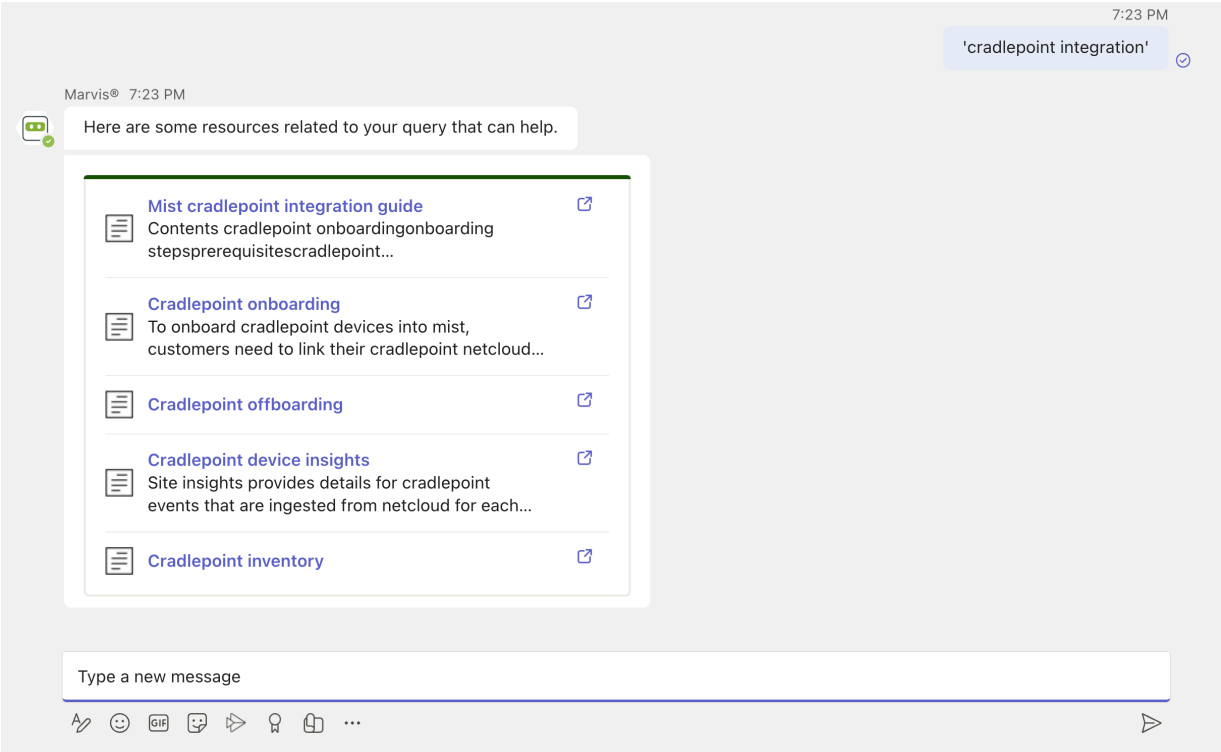
- <wired client mac>
- <site partial name>
- Locate <client username>

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.".



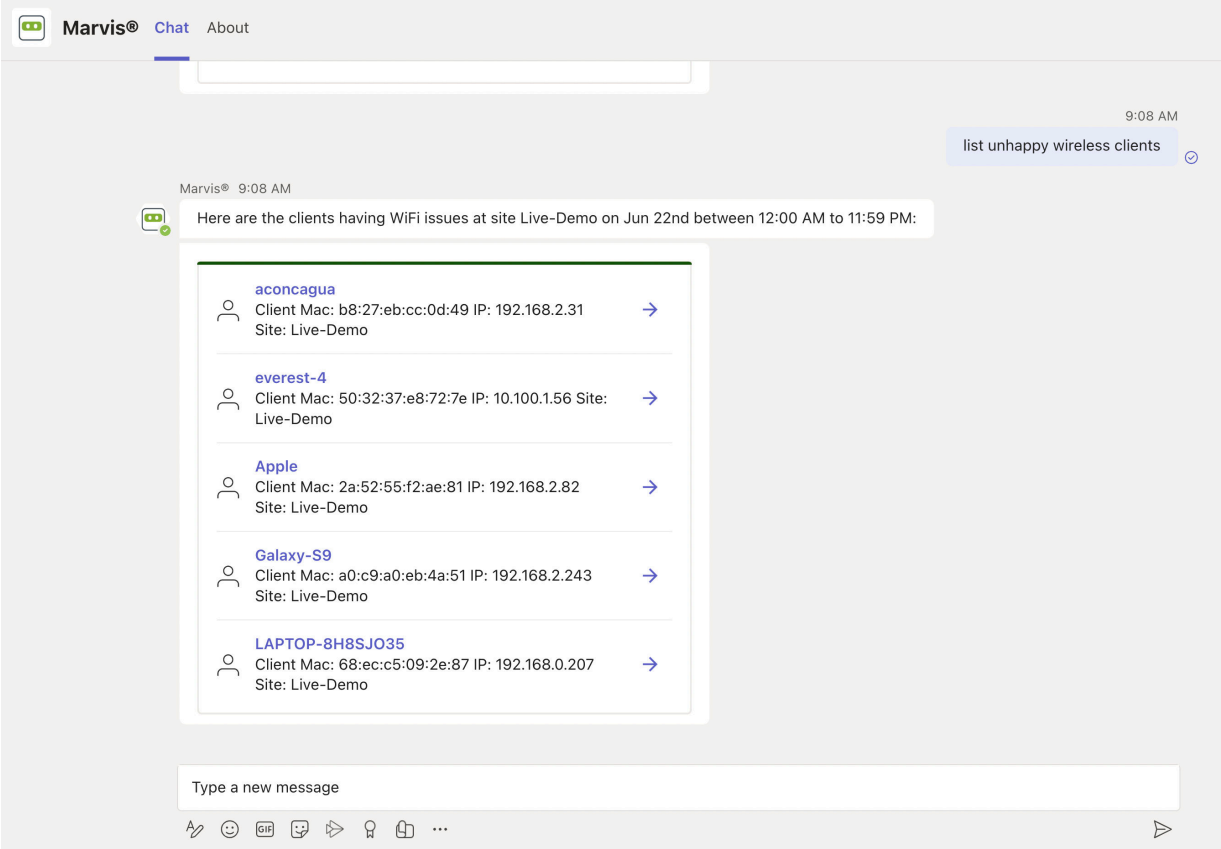
List Function

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."



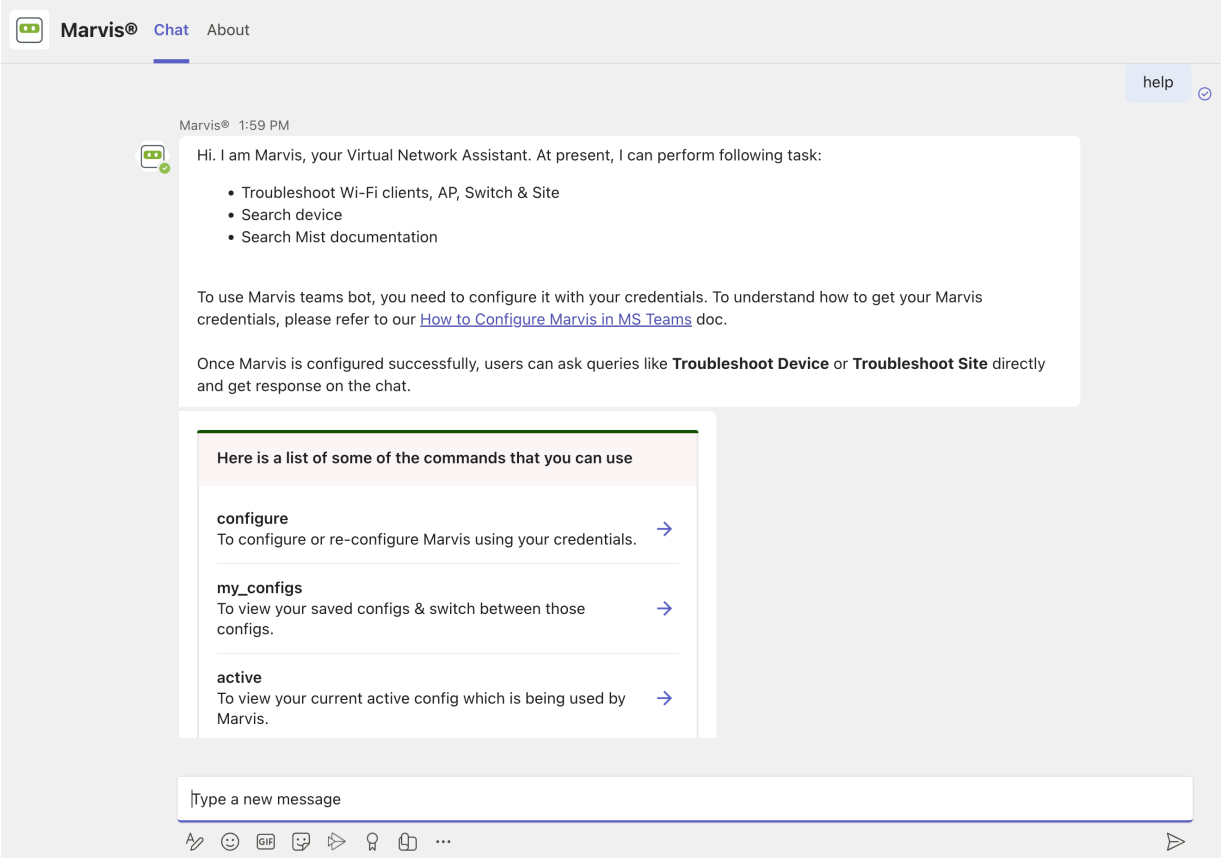
View or Change the Organization in the Marvis App

You can run queries against multiple organizations and also switch between organizations using the Marvis app,

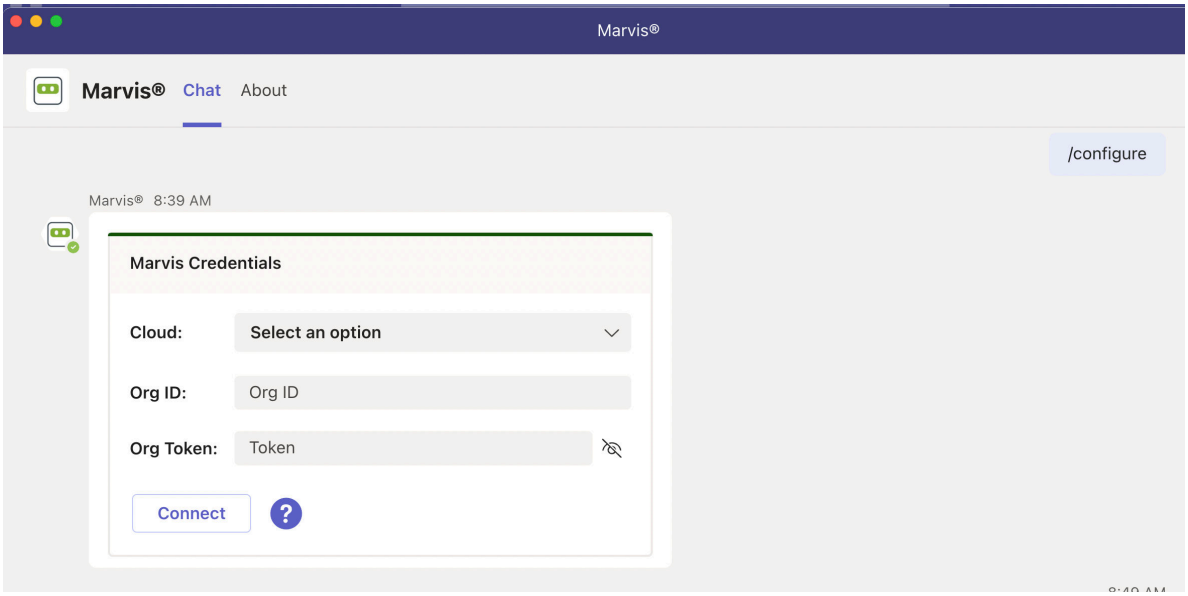
The Marvis app enables you to:

- Switch between organizations.
- View the current active organization (that is, the organization to which you're connected currently).
- 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:



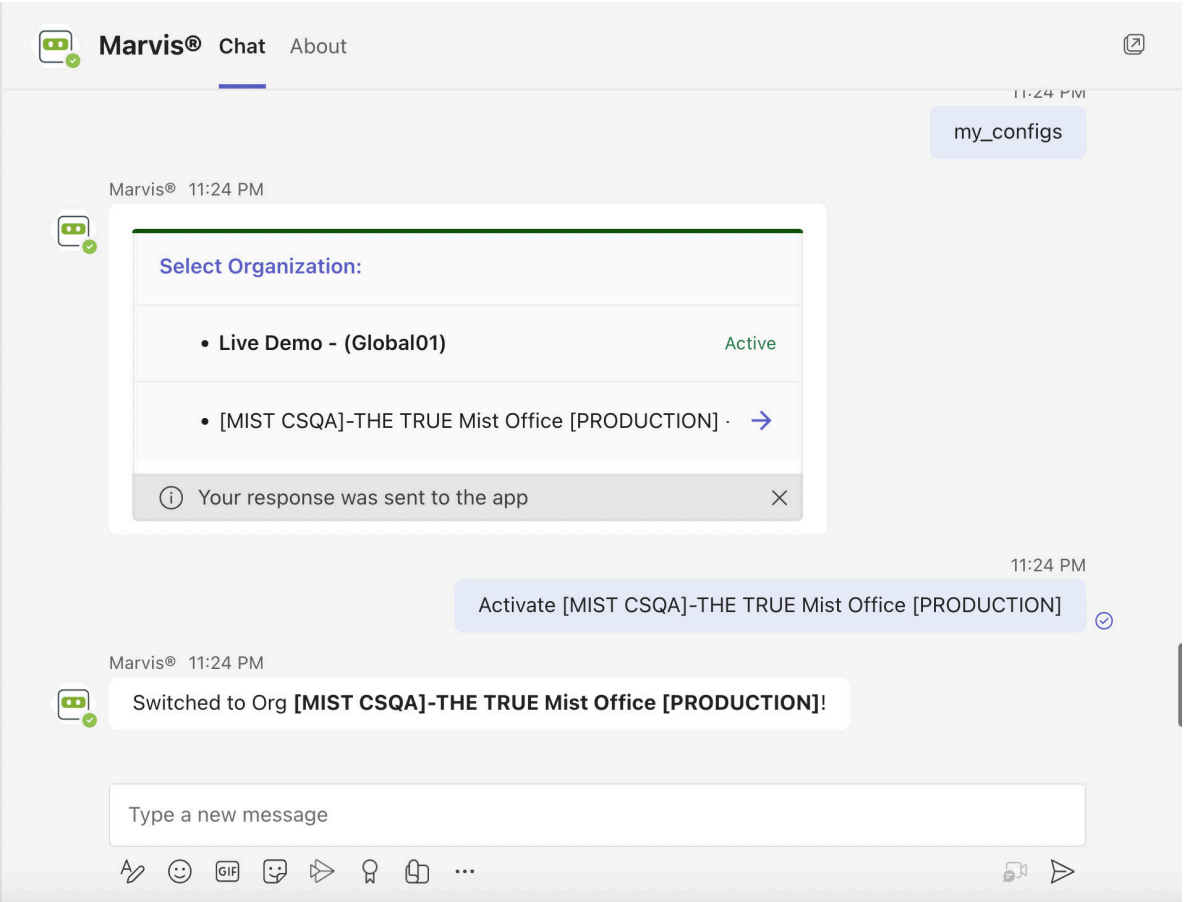
- If you enter **configure**, Marvis displays the login screen. You can either reconnect to the current active organization or connect to a different organization.



- If you enter **my_configs**, Marvis displays the following:
  - Organizations to which you are connected

- The current active organization

Clicking on the other organization makes it the active organization. You can query Marvis for information pertaining to the devices and sites that are part of that organization.



- If you enter **active**, Marvis displays the organization that is currently active.