

Juniper Mist Wireless Assurance Configuration Guide

Published
2024-05-16

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.

Juniper Mist Wireless Assurance Configuration Guide
Copyright © 2024 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

1

Get Started

Overview of Juniper Mist Wireless Assurance | 2

- Features and Benefits | 2

- Wireless Service Levels | 4

- Insights | 4

- Templates and Device Profiles | 5

Hardware for Your Wireless Network | 5

Deploy Your Wireless Network | 7

Explore Juniper Mist Features | 10

2

Access Points

Overview of Juniper APs | 13

Juniper Access Point Ports and Their Usage | 14

PoE Requirements for Juniper Mist APs | 21

AP Dashboard | 24

- Access Point Metrics | 24

Onboarding | 27

- Claim a Juniper Access Point | 27

- Obtain the Claim Code or Activation Code for an AP | 28

- Claim an AP Using a Web Browser | 28

- Claim an AP Using the Mist AI Mobile App | 29

- Assign Access Points to Sites | 31

- Enable Configuration Persistence | 32

- Adding and Scaling a Floorplan | 33

- Manually Upload Your Floorplan | 34

Import a Floorplan | 35

Scale a Floorplan | 36

Adding Access Points to a Floorplan | 38

Manually Place an Access Point on a Floorplan | 39

Autoplacement: Verify Access Point Positions for an Existing Site (BETA) | 42

Autoplacement: Position New Access Points (BETA) | 48

Auto-Orientation: Rotate Access Points (BETA) | 55

Rename a Juniper Access Point in the Mist Portal | 57

Release an Access Point from Inventory | 59

Upgrade the Firmware on a Juniper Access Point | 59

Firmware Version Tags for Juniper Mist Access Points | 60

Check for AP Firmware Updates | 62

Enable Auto Updates | 63

Upgrade the Firmware on an AP Manually | 66

Peer-to-Peer AP Firmware Upgrade | 67

Auto-Provisioning | 68

Configuration | 69

BLE Settings | 70

Ethernet Settings | 72

Enable PoE Passthrough | 75

Configure IP Settings | 76

Using APs in a Mesh | 79

Enable Mesh | 86

RTLS: AeroScout and Centrak | 86

Enable RTLS Support | 87

Using Electronic Shelf System (ESL) | 88

Enable Electronic Shelf Labels | 89

Enabling LEDs on the AP | 89

Enable Geofencing | 90

Data Rates | 91

DSCP Mapping | 93

Configure an AP for Survey Mode | 96

Configure Your Access Points as IEEE 802.1X Supplicants | 99

Deployment Considerations | 99

Enable Auto-Update to Version 0.14.x or Higher | 100

Enable 802.1X in the Switch Port Profile | 100

Assigning VLANs via RADIUS (If Applicable) | 104

Enable the 802.1X Supplicant Option in the Device Profile | 105

Apply the Device Profile to Your APs | 106

Import Your Certificate to Your RADIUS Server | 107

Enable Local Status Page | 108

Revert AP Configuration Automatically | 108

Device Profiles | 109

Device Profiles | 110

Device Profile Options | 111

Create a Device Profile | 113

Variables in Device Profiles | 114

Access Point FAQ | 114

3

WLANs and WLAN Templates

Configure a WLAN Template | 119

Add a WLAN to a Site or a WLAN Template | 121

WLAN Options | 122

Tips for Wi-Fi 6E (Video) | 131

Add a Bonjour Gateway to a WLAN | 132

Labels | 135

Using Labels in a WxLAN Policy | 139

4

Configure a Third-Party Tunnel | 141

Enable Wireless Bridging Mode | 142

WLAN Guest Portal

Compare WLAN Guest Portal Options | 149

Custom Guest Portal | 151

Add a Custom Guest Portal to a WLAN | 151

Form Fields for Custom Guest Portal | 153

Text and Language Options for Custom Guest Portal | 155

Layout Options for Custom Guest Portal | 158

Authorization Options for Custom Guest Portal | 162

Facebook App Creation | 168

Enable Guest Portal Social Login with Microsoft® Azure | 169

Use an External Portal for Guest Access | 178

Use PHP and Read-Me files to Create Your External Portal | 180

Use an Identity Provider for Guest Access | 187

Use Microsoft® Azure for Guest Portal Single Sign-On | 190

Enable Guest Portal Single Sign-On Access with OneLogin™ | 194

Authorize, Reauthorize, and Reconnect Guest Clients | 198

FAQs: Guest Portal | 200

5

Radio Management

Templates and Device Profiles | 203

Radio Management | 204

Radio Management (page) | 207

Radio Settings (RF Templates) | 213

Radio Management (dual-band) | 217

Dual Band Usage Examples | 219

WLAN Changes That Reset The Radio | 223

Transmit Power Notation for Juniper APs | 225

Security

RSSI, Roaming, and Fast Roaming | 230

Roaming | 230

Fast Roaming | 231

Enable Fast Roaming | 232

View Roaming History | 233

RADIUS | 235

Enable WPA2/WPA3 Enterprise (802.1X) Security on a WLAN | 235

Set the WLAN Security Type and Add Your RADIUS Server | 236

Use Site Variables to Add a Server | 237

NAS Identifier and NAS IP Address | 238

CoA/DM Server | 240

RadSec | 240

Configure an 802.1X WLAN to Redirect Clients to Specific Web Pages | 242

Change of Authorization (CoA) | 243

MAC RADIUS Authentication | 249

Guest Access Using RADIUS Server with MAC Authentication Bypass | 251

Flow of Guest Access Using RADIUS Server with MAC Authentication Bypass | 251

WLAN Configuration | 252

RADIUS Configuration | 252

Juniper Mist RADIUS Attributes | 254

Authentication Attributes | 254

RADIUS Accounting Attributes | 259

Dynamic Authorization Extensions | 262

Preshared Keys | 264

Preshared Keys | 265

Multi-Preshared Keys | 269

- Rotating PSKs | 272
- Leveraging Roles in a PSK (Use Case) | 275
- Enable Client Onboarding with a BYOD PSK Portal | 279
- Create a WxLAN Policy to Override Client VLANs | 287

Integrations | 290

- Configure Juniper Mist™ as a RADIUS Client in Aruba ClearPass | 291
- Integrate Juniper Mist™ with Aruba ClearPass Guest for Enhanced Access Control | 293
- Create a RADIUS Server using JumpCloud™ | 300
- Integrate Juniper Mist™ with Cisco® ISE for EAP | 303
- Enable Hotspot 2.0 for Seamless Wi-Fi Experience | 306

Rogues, Honeypots, and Neighbor APs | 310

- Find and Remove Rogues | 312
- Configure AP Threat Protection | 314
- Classify and Ban Designated Wireless Clients | 317
- Find Wireless Client MAC Addresses | 321

PCI DSS Compliance | 323

WxLAN Access Policies | 329

- Introduction | 330
- Site-Level and Organization-Level Policies | 331
- Labels | 331
- How Policy Rules Are Processed | 331
- Create a User Access Policy | 332

Wireless SLEs

Service Level Expectations (SLE) | 335

Wireless SLEs Overview | 344

Time to Connect SLE | 345

Wireless Successful Connects SLE | 347

Coverage SLE | 349

Roaming SLE | 351

Wireless Throughput SLE | 353

Capacity SLE | 355

AP Health SLE | 357

8

Troubleshooting

Using SLEs for Troubleshooting | 360

Wi-Fi Reason Codes | 361

Troubleshooting an Access Point | 366

AP Troubleshooting Overview | 366

What Does the AP Status LED Indicate? | 367

Troubleshoot AP Claiming Issues | 378

Troubleshoot AP Disconnection Issues | 379

Troubleshoot Insufficient Power for Access Points | 393

Troubleshoot AP Reboots | 394

Replace an Access Point | 396

Reset an Access Point to the Factory-Default Configuration | 401

Troubleshooting Wireless Issues | 402

Common Wi-Fi Issues | 403

Dynamic and Manual Packet Captures | 406

Dynamic Packet Captures | 407

Configure IEEE 802.11 on Wireshark | 408

View Wireless Packet Captures in Wireshark | 409

Manual Packet Capture Options | 410

Steer Clients to the 5-GHz Band | 411

Bonjour and Bluetooth Devices | 413

LLDP-MED Power Negotiation | 413

Troubleshoot Your Integration with Aruba ClearPass | 414

Use Labels to Identify "Unknown" Applications | 419

9

Technology Reference

Wireless Network Design Tutorial | 423

Wi-Fi 6 (802.11ax) Technology | 423

Considerations for 6 GHz Wireless | 425

1

CHAPTER

Get Started

[Overview of Juniper Mist Wireless Assurance](#) | 2

[Hardware for Your Wireless Network](#) | 5

[Deploy Your Wireless Network](#) | 7

[Explore Juniper Mist Features](#) | 10

Overview of Juniper Mist Wireless Assurance

SUMMARY

Juniper Mist Wireless Assurance is a cloud-based subscription service that serves as a single pane of glass for configuring, monitoring, and optimizing wireless access.

IN THIS SECTION

- [Features and Benefits | 2](#)
- [Wireless Service Levels | 4](#)
- [Insights | 4](#)
- [Templates and Device Profiles | 5](#)

Juniper Mist™ Wireless Assurance includes access points (APs), wireless LANs (WLANs), radio management, security, network segmentation, and a lot of automation. But perhaps the best benefits come from the telemetry streaming from Juniper APs, switches, and WAN (SSR, SRX) devices. Mist AI leverages this telemetry data to report on user's network experiences, and perform automated root-cause analysis using adaptive learning which reduces manual troubleshooting and increases overall network optimization.

NOTE: You'll configure and manage your wireless network by using the Juniper Mist portal. If you're just getting started with Juniper Mist, see the [Juniper Mist Quick Start Guide](#) and the [Juniper Mist Management Guide](#).

Features and Benefits



Video: [Mist Cloud-Based Architecture](#)

Features

- Customizable wireless service levels allow you to set and monitor service-level experiences (SLEs) for key performance metrics gathered on individual and multiple users.
- Data science applied to the aggregate SLE performance data to learn and optimize radio settings to assure performance and adapt signal interference.
- Dynamic Packet Capture automatically starts a packet capture when a user's connection fails.

- Using data science and machine learning, the Proactive Analytics and Correlation Engine (PACE) aides root-cause identification so you can identify and fix the issue.
- Guest access that provides flexible configuration options including:
 - Multiple language support.
 - Customizable branding.
 - Social login.
 - External captive portal integration.
 - AAA/RADIUS integration.
- WxLAN policies let you secure network resources (such as servers and printers) by allowing only selected users and devices to connect to them.

Benefits of Cloud-Based Architecture

Wireless assurance runs in the cloud. You don't have any on-premise intermediary controllers to install or manage, so your network is easy to scale.

To comply with data-residency regulations and optimize performance, Juniper deploys Mist clouds world-wide. Server locations include Europe, Asia, and Australia. In the United States, we have servers on the east and west coasts as well as a US federal cloud.

The Mist microservice architecture naturally supports multitenancy, and inherently scales with the elasticity of the cloud. Thus, for example, a Managed Service Provider (MSP) can manage wireless access for dozens of client organizations. Or a large retailer can accommodate various site-specific requirements yet still manage the organization centrally, with a single login per cloud, and a comprehensive view.

Benefits of Centralized Portal

From the Juniper Mist portal, you can configure radio management, set up access policies, and configure security (encryption, access, and malicious AP detection). You can also group and configure (or preconfigure), dozens, even thousands, of APs so they are automatically onboarded to the network once the AP is powered on and has Internet access. Likewise, you can define however many WLANs you want, for example, to provide a secure network for office spaces, one for guest portals, one for IoT devices, and another for the automated cranes in your warehouses.

When the network is configured, the Juniper APs send real-time telemetry representing users' network experiences to the Juniper Mist portal. Data is consolidated and measured against the performance metrics that you've set.

For strategic wireless network configuration updates, Mist AI aggregates AP data collected over multiple days, where it uses machine learning to identify trends and make performance optimizations.

Individually, a Juniper AP can automatically make real-time updates in response to acute changes in the network, for example in response to channel interference or congestion.

Wireless Service Levels

Service-level experiences (SLEs) help you understand a user's wireless network experience. Juniper APs collect key data of every user's wireless experience and normalizes the data to a user minute metric, which is then rolled up in the Juniper Mist cloud, which applies machine learning to create useful information. From the dashboard, you can visualize the data for the entire organization, individual sites, or even individual clients. For more information, see the ["Wireless SLEs chapter of this guide" on page 0](#).

Insights

Client and AP Insights provide an overview of the network experience across an entire site, including detailed views into your WLANs and APs. For example, you can select a site and a time period at the top of the page and then drill-down into AP level events that you are interested in. This is shown in Figure 1.

Figure 1: The AP Insights Page



When you select an event from the list, the Mist portal displays a summary of the event to the right of the list. You can do the same for the AP Events block by clicking the settings button in the upper-right corner of the block.

In the Access Points block, you can see the names of all APs associated with the selected site. Along with the AP name, you can see the connection status, MAC address, uptime, and other information. When you click the name of the AP, the configuration page for that AP appears, where you can view and edit the configuration details.

Templates and Device Profiles

In the Juniper Mist dashboard, you'll often find that the same configuration settings can be made in different places. For example, you can configure RRM and other radio settings directly on the Juniper APs, in a device profile, in an RF template, or in a WLAN template. The modular design makes it easy to scale configurations across different AP groupings, and it provides flexibility so you can quickly associate any combination of APs, WLANs, access policies, and RF configurations.

To learn about the different configuration options, see ["Templates and Device Profiles" on page 203](#).

Hardware for Your Wireless Network

SUMMARY

Get started selecting hardware for your wireless network. Compare Juniper access points, learn about Juniper Mist Edge, view specifications, and find deployment and installation instructions.

IN THIS SECTION

- [Juniper Access Points | 6](#)
- [Juniper Mist Edge | 6](#)

Juniper provides a wide range of hardware to support your wireless networking needs.



Juniper Access Points

All Juniper access points work in conjunction with Juniper Mist cloud and Mist AI to deliver premium wireless access capabilities.

- To quickly compare different models, see [Wireless Access Points and Edge](#).
- To see a list of all supported Access Points along with their descriptions, specifications, and installation instructions, see [Juniper Mist Supported Hardware - Wireless Access Points](#).

Juniper Mist Edge

The Juniper Mist Edge is available in various models for deployments of different sizes.

- To explore the full list of Mist Edge resources, see [Mist Edge Documentation](#).
- To view the Mist Edge datasheet, see [Mist Edge Datasheet](#).
- To learn about the features and configuration options available in the Juniper Mist™ portal, see [Mist Edge Guide](#).
- To learn how to design your network using the Mist Edge, see [Juniper Mist Edge Design Guide](#).
- To implement a virtual Mist Edge architecture, see [Virtual Mist Edge Solution Guide](#).

- To extend the corporate network to remote office workers, see [Juniper Mist Edge Teleworker Guide](#).

Deploy Your Wireless Network

SUMMARY

Complete these essential tasks to set up your organization and sites, ensure security, install your devices, and start configuring your network.

Table 1: Deployment Tasks and Links

Category	Task	More Information
Prerequisites	<p>Before you can configure your wireless network or onboard your devices, you need to complete these tasks in the Juniper Mist™ portal:</p> <ul style="list-style-type: none"> • Create your organization. • Set up at least one site, and activate your subscriptions. • Configure your firewall to allow outbound Juniper Mist traffic. <p>Recommended, but not required before you can configure your wireless network:</p> <ul style="list-style-type: none"> • Add user accounts for other personnel who are working with you to deploy Juniper Mist. You can even enable limited access for the personnel who are installing devices. • Set up other security options as needed. For example, manage certificates, disable Juniper Mist support access, or enable Single Sign-On. 	<ul style="list-style-type: none"> • Juniper Mist Quick Start • Firewall Configuration: Juniper Mist IP Addresses and Ports • Security Options
Device Installation	<p>Claim your devices into your organization.</p>	<ul style="list-style-type: none"> • Juniper Mist Access Points Quick Start (onboarding steps and troubleshooting tips) • Deployment Guides for Juniper APs (device requirements, specifications, and mounting instructions) • Juniper Mist Edge Guide

Table 1: Deployment Tasks and Links *(Continued)*

Category	Task	More Information
WLAN Setup	<p>Set up your WLAN templates and WLANs. Configure settings such as security, radio frequency, rate limits, QoS, and more.</p> <p>For all deployments, we recommend using WLAN templates. Templates streamline your tasks and ensure consistency. Future operations are made easier, because you can quickly update your template, while Juniper Mist applies the changes across all associated sites.</p>	<ul style="list-style-type: none"> • "Configure a WLAN Template" on page 119 • "Add a WLAN to a Site or a WLAN Template" on page 121 • "WLAN Options" on page 122
RF Templates and Device Profiles	<p>If you have multiple sites and device types, you can use RF templates and device profiles to streamline configuration and deployment.</p> <p>By doing so, you ensure consistent settings across sites. As with WLAN templates, Juniper Mist applies any changes across all associated sites and devices.</p>	<p>"Templates and Device Profiles" on page 5</p>
Auto-Provisioning	<p>For large deployments, consider enabling auto-provisioning. Juniper Mist can automatically assign device profiles, names, and sites to your APs as you onboard them.</p>	<p>"Auto-Provisioning" on page 68</p>

Explore Juniper Mist Features

IN THIS SECTION

- [Automatic Firmware Updates | 10](#)
- [Guest Portal | 10](#)
- [Location Services | 10](#)
- [AIOps | 11](#)

Now that your wireless network is up and running, explore other Juniper Mist features to meet your business needs.

Here are some features we think you'll find especially helpful.

Automatic Firmware Updates

Enable auto updates to streamline your operations. You can set up this feature to watch for new firmware and install updates on the schedule that you specify. For more information, see ["Enable Auto Updates" on page 63](#).

Guest Portal

Create your own guest portal page to welcome visitors and enable them to log in to your network. You can customize the portal with options such as terms of service, email/text login, or even allow social media login to help boost engagement. For more information, see ["WLAN Options" on page 122](#).

Location Services

You can deploy a number of location services onto your wireless network. For example, you can develop Juniper Mist SDK-enabled indoor wayfinding applications that guide visitors turn-by-turn through your site. You can also create applications that engage customers and visitors by displaying notifications and

promotions as visitors walk through your site. For more information, see the [Juniper Mist Location Services](#) guide.

AIOps

Juniper Mist includes AI-driven features to help you proactively monitor service levels and troubleshoot issues.

- **Service Levels**—Use the Monitor page to track current network performance against Service Level Expectations (SLEs). Get a bird's eye view of your entire organization, or focus on specific sites over specific timespans. Proactively discover problems before users report them. Select individual events to perform root cause analysis, assisted by AI-driven insights.

For more information:

- Start with ["Using SLEs for Troubleshooting" on page 360](#).
- For in-depth insight into monitoring, see the [Juniper Mist Network Monitoring Guide](#).
- **Marvis**—Dramatically reduce troubleshooting and time-to-resolution with the Marvis Virtual Network Assistant. (Subscription required. For more information, see [Marvis Virtual Network Assistant](#).) Explore AI-detected issues and click to view the root cause analysis and AI-driven recommendations. You can also interact with the conversational assistant to get the answers you need. For information about using Marvis features, see the [Juniper Mist Marvis Guide](#).

2

CHAPTER

Access Points

[Overview of Juniper APs | 13](#)

[Juniper Access Point Ports and Their Usage | 14](#)

[PoE Requirements for Juniper Mist APs | 21](#)

[AP Dashboard | 24](#)

[Onboarding | 27](#)

[Configuration | 69](#)

[Device Profiles | 109](#)

[Access Point FAQ | 114](#)

Overview of Juniper APs

Juniper® Series of High-Performance Access Points (APs) operate in conjunction with the Juniper Mist cloud to provide full-spectrum wireless networking. The APs support multiband and dual-band 5-GHz radios and 6-GHz frequency radios for high-density environments, Bluetooth Low Energy (BLE) for wayfinding, and for location tracking and IoT devices. You can manage APs by grouping them by site, use case, or model and manage them collectively with device profiles. You can also provision APs automatically with specific configurations as you onboard them to the site.

Figure 2: Juniper Access Points



Juniper APs stream telemetry data from the wireless and wired networks back to the Juniper Mist cloud. The data is aggregated and analyzed against service benchmarks to be used for AI-powered performance optimizations. This data is used to troubleshoot issues and manage the network from the central Juniper Mist dashboard.

The Juniper AP portfolio supports 802.11ax and 802.11ac Wi-Fi standards, and includes models for both indoor and outdoor locations. Most models include a third or fourth radio. The additional radios are used for performance monitoring, rogue AP detection, and real-time packet captures. Most APs include

a dynamic, virtual (vBLE) 16-element antenna array that provides location services with a resolution of 1 to 3 meters. All APs support automatic firmware upgrades.

See Supported Hardware: <https://www.juniper.net/documentation/us/en/software/mist/content/mist-supported-hardware.html>.

Juniper Access Point Ports and Their Usage

SUMMARY

Use the information in this topic to learn about the ports available on the Juniper Access points and determine how to use them in your network.

IN THIS SECTION

● [IoT Port Pins | 18](#)

Table 3 on page 14 lists the ports available on the Juniper access point (AP) models.

Table 3: Ports on the Juniper APs

Wireless Standard	AP Model	Ports	
		Ethernet	IoT
Wi-Fi 6E	AP24	Eth0: PoE 802.3at in + data in	–
	AP34	Eth0: PoE 802.3at in + data in	–

Table 3: Ports on the Juniper APs *(Continued)*

Wireless Standard	AP Model	Ports	
		Ethernet	IoT
	AP45	<p>Eth0: PoE 802.3bt in + data in</p> <p>Eth1: Data out</p> <p>If the Eth0 port is connected to 802.3bt power, the Eth1 port can operate as a PoE power sourcing equipment (PSE) providing up to 15.4 W power.</p>	–
	AP64	Eth0: PoE 802.3at/ 802.3bt in + data in	–
Wi-Fi 6	AP12	<p>Eth0: PoE 802.3at in + data in</p> <p>Eth1: Data out</p> <p>If the Eth0 port is connected to 802.3at power, the Eth1 port can operate as a PoE power sourcing equipment (PSE) providing up to 7 W power.</p> <p>Eth2 and Eth3: Data out</p>	–
	AP32	<p>Eth0: PoE 802.3at in + data in</p> <p>Eth1: Data out</p>	–

Table 3: Ports on the Juniper APs *(Continued)*

Wireless Standard	AP Model	Ports	
		Ethernet	IoT
	AP33	Eth0: PoE 802.3at in + data in Eth1: Data out	–
	AP43	Eth0: PoE 802.3at in + data in Eth1: Data Out If the Eth0 port is connected to 802.3bt power, the Eth1 port can operate as a PoE power sourcing equipment (PSE) providing up to 15.4 W power.	Supports digital inputs (0 to +5V), digital outputs (0 to +5V), and analog inputs (0 to +5V)
	AP63	Eth0: PoE 802.3at in + data in Eth1: Data out If the Eth0 port is connected to 802.3bt power, the Eth1 port can operate as a PoE power sourcing equipment (PSE) providing up to 15.4 W power.	–

Table 3: Ports on the Juniper APs (*Continued*)

Wireless Standard	AP Model	Ports	
		Ethernet	IoT
Wi-Fi 5	AP21	<p>Eth0: PoE 802.3at in + data in</p> <p>Eth1: Data Out</p> <p>If the PoE Passthrough feature is enabled, the Eth1 port can provide PoE out.</p> <p>NOTE: The Eth1 port is typically used to connect to the AP21 but it can also be used to obtain Ethernet access. You'll need to disable PoE Passthrough on the AP before connecting the device to the Eth1 port.</p>	–
	AP41	<p>Eth0: PoE 802.3at in + data in</p> <p>Eth1: Data out</p>	Supports digital inputs (0 to +5V), digital outputs (0 to +5V), and analog inputs (0 to +5V)
	AP61	<p>Eth0: PoE 802.3at in + data in</p> <p>Eth1: Data out</p> <p>The Eth1 port does not support PoE out.</p>	–

Table 3: Ports on the Juniper APs (*Continued*)

Wireless Standard	AP Model	Ports	
		Ethernet	IoT
	BT11	<p>Eth0: PoE 802.3at in + data in</p> <p>Eth1: Data out</p> <p>If the PoE Passthrough feature is enabled, the Eth1 port can provide PoE out.</p> <p>NOTE: The Eth1 port is typically used to connect to the BT11 but it can also be used to obtain Ethernet access. You'll need to disable PoE Passthrough on the AP before connecting the device to the Eth1 port.</p>	–

IoT Port Pins

The IoT port on the AP41 and AP43 contains 8 pins:

- 2 digital IN pins that you can use only as input
- 1 digital OUT pin
- 4 analog pins that you can use for both input and output
- 1 ground pin

The following figure shows the IoT port connector that you can connect to the IoT port on the AP.

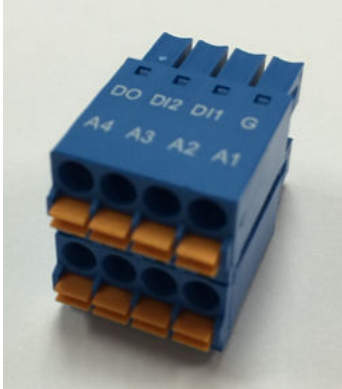


Table 4: IoT Port Connector Pins

Pin	Function
DO	Digital output
DI2	Digital input 2
DI1	Digital input 1
G	Ground
A4	Analog input 4
A3	Analog input 3
A2	Analog input 2
A1	Analog input 1

How to Enable the IoT Port

Use the following API call to enable the IoT port. The **iot_config** attribute provides information about the status of the pins on the IoT port.

PUT : https://api.mist.com/api/v1/sites/:site_id/devices/:device_id

```
{
  "iot_config": {
    "DO": {
      "enabled": true,
      "value": <0 == OFF; 1 == ON>
    }
  }
}
```

NOTE: Ensure that you configure the SSID for 2.4 GHz or dual band; otherwise, the IoT devices will not detect any SSID or WLAN,

You can view the current state of the IoT port pins by using the following API call:

GET /api/v1/sites/:site_id/devices/:device_id/iot

You can view the AP statistics for a site by using the following API call:

GET /api/v1/sites/:site_id/stats/devices

The API output also includes the information from the integrated sensors as shown in the example below:

```
GET /api/v1/sites/:site_id/stats/devices // Environment stats
{
  "env_stat": {
    "cpu_temp": 51,
    "ambient_temp": 39,
    "humidity": 11,
    "attitude": 0,
    "pressure": 1015
    "accel_x": -0.012,
    "accel_y": 0.004,
```



```
“accel_z”: -1.012,  
“magne_x”: 0.0,  
“magne_y”: 1.3,  
“magne_z”: 0.0,  
“vcore_volatge”: 0  
},
```

PoE Requirements for Juniper Mist APs

Table 5 on page 21 lists the PoE requirements for the Juniper Mist Access Points (APs).

Table 5: PoE Requirements for Juniper Mist APs

Generation	Model	Minimum PoE Required	Wattage Required for Full Wi-Fi Functionality	Notes
Wi-Fi 6E	AP64	802.3af	13 W	AP64 requires 802.3af power for full functionality.

Table 5: PoE Requirements for Juniper Mist APs *(Continued)*

Generation	Model	Minimum PoE Required	Wattage Required for Full Wi-Fi Functionality	Notes
	AP45	Dynamic	29.3 W	<p>AP45 requires 802.3bt power for full functionality. On 802.3at power, it has dynamic functionality based on the configuration.</p> <p>The AP can operate in 4×4 mode on any two data radios, or 2×2 mode on 2.4 GHz, 4×4 mode on 5 GHz, and 2×2 mode on 6 GHz with three data radios enabled. For example:</p> <ul style="list-style-type: none"> • If you configure only two bands in the WLAN configuration, the AP operates in the 4×4 mode on both the data radios. • If you configure three bands in the WLAN configuration, then all three data radios are active. The AP operates in the 2×2 mode on 2.4 GHz, 4×4 mode on 5 GHz, and 2×2 mode on 6 GHz. • If you enable dual 5 GHz, then all three data radios are active. The AP operates in the 2×2 mode on 2.4 GHz, 4×4 mode on 5 GHz, and 2×2 mode on 6 GHz. <p>The dedicated scanning radio and BLE are always active regardless of power.</p>
	AP34	Dynamic	20.9 W	<p>AP34 requires 802.3at power for full functionality. You can use 802.3af power to connect to the Mist cloud but you'll see a warning message stating that the power is insufficient.</p>
	AP24	802.3af	13 W	<p>AP24 requires 802.3af power for full functionality.</p>
Wi-Fi 6	AP63	802.3at	25.2 W	
	AP43	802.3at	25.5 W	

Table 5: PoE Requirements for Juniper Mist APs *(Continued)*

Generation	Model	Minimum PoE Required	Wattage Required for Full Wi-Fi Functionality	Notes
	AP33	802.3af	19.5 W	<p>AP33 requires 802.3at power for full functionality. However, the AP is capable of running on 802.3af power with reduced functionality as described below:</p> <ul style="list-style-type: none"> • The 5-GHz radio operates in 2×2 mode instead of 4×4 mode. • The Eth0 port operates at a maximum speed of 1 Gbps. • The Eth1 port is disabled.
	AP32	802.3af	19.5 W	<p>AP32 requires 802.3at power for full functionality. However, the AP is capable of running on 802.3af power with reduced functionality as described below:</p> <ul style="list-style-type: none"> • The 5-GHz radio operates in 2×2 mode instead of 4×4 mode. • The Eth0 port operates at a maximum speed of 1 Gbps. • The Eth1 port is disabled.
	AP12	802.3af	12.9 W	<p>AP12 requires 802.3at power only when you use the PoE out functionality. If you don't need to use PoE out, the AP can operate with full functionality using 802.3af power.</p>
Wi-Fi 5	AP61	802.3at	19.5 W	
	AP41	802.3at	19.5 W	
	AP21	802.3af	12.9 W	
Other	BT11	802.3af	5.5 W	

AP Dashboard

IN THIS SECTION

- [Access Point Metrics](#) | 24

Access Point Metrics

Juniper Mist™ uses the connectivity status, VLAN status, and firmware compliance to measure the overall operational health of the APs. With these metrics, you can proactively monitor the performance of APs at your site and quickly identify and troubleshoot connectivity and firmware compliance issues.

You can view these metrics when you go to the Access Points page on the Juniper Mist portal. On this page, each metric is represented as a percentage and is color coded. Here's the mapping between the color and the percentage range:

- Green—>98.5 %
- Orange—80 % to 98.5 %
- Red—<80 %

The following example shows the metrics that you see on the Access Points page.

Access Points site: Live-Demo

17 Access Points, 23 Wireless Clients, 1 AP21, 4 AP24, 1 AP33, 2 AP34, 3 AP41, 1 AP41E, 5 AP45

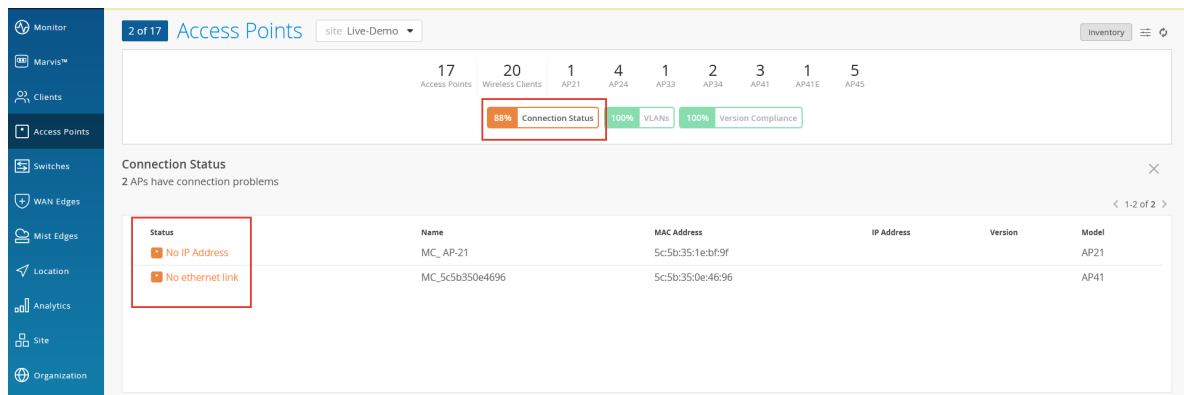
88% Connection Status, 100% VLANs, 100% Version Compliance

Warning: 1 AP has reduced functionality.

Status	Name	MAC Address	IP Address	No. Clients	Uptime	Total Bytes	Capabilities	VBLE	Model	2.4 GHz Channel	5 GHz Channel
Connected	LD_APEng	ac23:16:fc:03:7f	10.100.0.43	4	3d 12h 22m	7.3 GB	Wi-Fi 6E	N/A	AP34	1/20	132/20
Connected	LD_Conf2	a8:f7:d9:81:77:50	10.100.0.170	0	2d 8h 19m	3.2 GB	Wi-Fi 6E	⊙	AP45	6/20	136/20
Connected	LD_DataScience	a8:3a:79:30:19:0f	10.100.0.128	6	6d 15h 44m	15.4 GB	Wi-Fi 6E	⊙	AP45		136/20, 36/20
Connected	LD_IDF_B_AP-3rd-Party-Switch	5c5b:35:3e:4e:ca	10.100.0.131	0	6d 15h 42m	91.5 MB	Wi-Fi 6E	⊙	AP41	11/20	
Connected	LD_Kitchen	00:3e:73:07:e4:46	10.100.0.129	1	6d 15h 37m	4.9 GB	Wi-Fi 6E	N/A	AP24		132/20
Connected	LD_Marvis	a8:3a:79:30:1a:40	10.100.0.142	1	6d 15h	2.2 GB	Wi-Fi 6E	⊙	AP45		136/20, 36/20
Connected	LD_MCB_AP	ac23:16:fc:05:e6	10.100.0.42	5	3d 12h 21m	9.9 GB	Wi-Fi 6E	N/A	AP34	1/20	132/20
Connected	LD_MHMD	d4:20:b0:f1:05:4b	192.168.2.75	3	6d 9h 37m	8.7 GB	Wi-Fi 6E	⊙	AP45		136/20, 36/20
Connected	LD_NewBobFriday	00:3e:73:07:e3:c9	10.100.0.30	1	3d 12h 21m	5.9 GB	Wi-Fi 6E	⊙	AP24		136/20
Connected	LD_RS_Support	a8:3a:79:30:18:fb	10.100.0.41	1	3d 12h 22m	2.7 GB	Wi-Fi 6E	⊙	AP45	1/20	136/20
Connected	LD_Testbed_MD	5c5b:35:8e:6f:ea	10.100.0.113	0	6d 15h 1m	3.7 GB	Wi-Fi 6E	⊙	AP41	11/20	132/20
No IP Address	MC_AP-21	5c5b:35:1e:bf:9f		0	0 B	0 B	Wi-Fi 6E	⊙	AP21		
No ethernet link	MC_5c5b350e4696	5c5b:35:0e:46:96		0	0 B	0 B	Wi-Fi 6E	⊙	AP41		
Connected	MC_AP24_RLB1	00:3e:73:07:e5:bd	192.168.1.61	0	5d 19h 35m	3.7 MB	Wi-Fi 6E	N/A	AP24		136/20

You can view the following metrics on the Access Points page:

- **Connection Status**—This metric shows the percentage of APs that are online at your site. Click this metric to see the list of APs that are offline. In this example, you can see that Juniper Mist reports that two APs are experiencing connectivity issues. Notice that Juniper Mist also lists the reasons—No IP Address and No Ethernet Link—that cause these issues. You can then investigate further by observing the LED blink patterns and take corrective actions. See ["What Does the AP Status LED Indicate?" on page 367](#).



- **VLANs**—This metric shows the percentage of APs for which all the wired VLANs are active. Click this metric to view the APs that have inactive VLANs and the respective VLAN IDs. Inactive VLANs result in users being unable to obtain an IP address. This issue might arise if you did not correctly configure the VLAN on the switch port to which the AP is connected.
- **Version Compliance**—This metric shows the percentage of APs that use the same firmware version. Juniper Mist uses the following formula to calculate the version compliance percentage:

$(\text{APs running the expected version per model} / \text{Total number of APs per model}) * 100$

- If you selected the **Enable Auto Update** check box under the AP Firmware Upgrade section in the Site Configuration page, the Version Compliance metric displays the percentages as follows:
 - **100%** if all the APs run the version that you've selected for the automatic firmware upgrade.

NOTE: If you enabled the automatic update option, then the firmware on the APs is upgraded only if the current firmware version number of the APs is lower than that of the selected version for automatic upgrade.

If the APs run a firmware version that is later than the version configured for the automatic upgrade, Juniper Mist does not downgrade the firmware version.

- **0%** if none of the APs run the configured version for the automatic update.
- **Less than 1 %** if less than 1 % of the APs run the configured version for the automatic update.

- If you disabled the **Enable Auto Update** option under the AP Firmware Upgrade section in the Site Configuration page, Juniper Mist considers the most common firmware version across all the APs (per AP model) as the compliant version. For example: If three Juniper® AP41 High-Performance Access Points run version 0.7.20383 and two AP41 Access Points run version 0.5.17445, then Juniper Mist considers 0.7.20383 as the compliant version.

You can click the Version Compliance metric to view the APs that run noncompliant firmware versions.

Note that version noncompliance has no impact on AP performance. If all the APs per model run the same firmware version and if the version is different from the version that you have configured in the AP Firmware Upgrade settings, the Version Compliance metric shows 0%. If you clear the **Enable Auto Update** check box, the percentage changes to 100%.

NOTE: The Access Points page displays a warning message for APs that operate in a reduced functionality mode.

Here is an example of the Access Points page that displays the warning message about an AP operating in the reduced functionality mode. You'll also see a warning icon displayed beside the AP. You can view the AP operating mode details such as the configured radio bands and the supported antenna chains in each band by hovering your mouse over the warning icon.

17 Access Points site: Live-Demo Inventory

17 Access Points 17 Wireless Clients 1 AP21 4 AP24 1 AP33 2 AP34 3 AP41 1 AP41E 5 AP45

88% Connection Status 100% VLANs 100% Version Compliance

Warning: 1 AP has reduced functionality

	Status	Name	MAC Address	IP Address	No. Clients	Uptime	Total Bytes	Capabilities	VBLE	Model	2.4 GHz Channel	5 GHz Channel
<input type="checkbox"/>	Connected	LD_APEng	ac:7f	10.100.0.43	1	16h 29m	774.2 MB		N/A	AP34	11/20	132/20
<input type="checkbox"/>	Connected	LD_Conf2	a8:50	10.100.0.170	0	19d 2h 58m	3.6 GB			AP45	1/20	136/20
<input type="checkbox"/>	Connected	LD_DataScience	a8:0f	10.100.0.128	4	23d 10h 21m	12.7 GB			AP45		136/20, 36/20
<input type="checkbox"/>	Connected	LD_IDF_B_AP-3rd-Party-Switch	5c:ca	10.100.0.131	0	23d 10h 19m	148.4 MB			AP41	6/20	
<input type="checkbox"/>	Connected	LD_Kitchen	00:46	10.100.0.129	1	23d 10h 16m	8.2 GB		N/A	AP24		132/20
<input type="checkbox"/>	Connected	LD_Marvis	a8:40	10.100.0.142	0	23d 9h 40m	9.8 GB			AP45		132/20, 36/20
<input type="checkbox"/>	Connected	LD_MCB_AP	ac:e6	10.100.0.42	5	20d 7h	7.5 GB		N/A	AP34	6/20	132/20
<input type="checkbox"/>	Connected	LD_MHMD	d4:4b	192.168.2.75	2	16h 30m	2 GB			AP45		136/20, 36/20
<input type="checkbox"/>	Reduced functionality [21] 6GHz(2x2) 5GHz-High(2x2) 5GHz-Low(4x4)		77:e3:c9	10.100.0.30	0	20d 7h	4.6 GB		N/A	AP24		136/20
<input type="checkbox"/>	Connected	LD_RS_Support	a8:fb	10.100.0.41	3	20d 6h 59m	9.2 GB			AP45	1/20	136/20
<input type="checkbox"/>	Connected	LD_Testbed_MD	5c:ea	10.100.0.113	1	23d 9h 37m	5.2 GB			AP41	1/20	136/20

AP43 and AP45 support the reduced functionality mode, when specific configurations are applied. An AP45 requires the 802.3bt standard for a 4×4 antenna chain support in all the configured radio bands. However, if you enable an AP45 with the 802.3at standard, it operates with a fewer number of chains. The AP43 operates in the reduced functionality mode when USB peripherals are activated.

Onboarding

IN THIS SECTION

- [Claim a Juniper Access Point | 27](#)
- [Assign Access Points to Sites | 31](#)
- [Enable Configuration Persistence | 32](#)
- [Adding and Scaling a Floorplan | 33](#)
- [Adding Access Points to a Floorplan | 38](#)
- [Rename a Juniper Access Point in the Mist Portal | 57](#)
- [Release an Access Point from Inventory | 59](#)
- [Upgrade the Firmware on a Juniper Access Point | 59](#)
- [Auto-Provisioning | 68](#)

Claim a Juniper Access Point

IN THIS SECTION

- [Obtain the Claim Code or Activation Code for an AP | 28](#)
- [Claim an AP Using a Web Browser | 28](#)
- [Claim an AP Using the Mist AI Mobile App | 29](#)

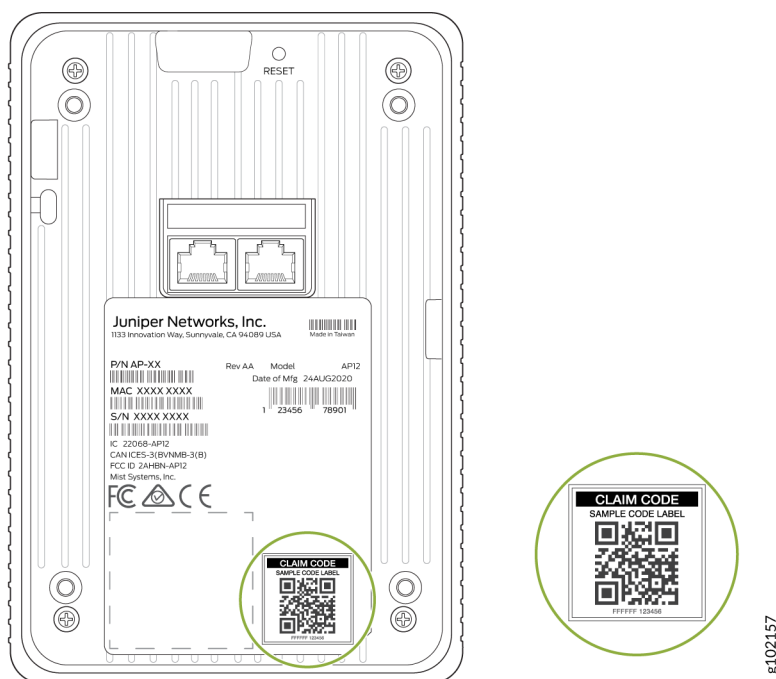
You need to claim an access point (AP) to be able to manage it from the Juniper Mist cloud. You'll need either a claim code or an activation code to claim an AP. With either, you can claim an AP by using one of the following methods:

- Mist AI Mobile App
- A Web browser

Obtain the Claim Code or Activation Code for an AP

You can claim either a single AP using a claim code or multiple APs using an activation code. You can use any of these methods to claim an AP:

- To claim a single AP, use the claim/QR code located on the rear of the AP.



- To claim multiple APs, you'll need to use an activation code. When you purchase multiple APs, we provide you with an activation code along with your PO information.

Claim an AP Using a Web Browser

You can onboard a single AP or multiple APs using a Web browser. If you're onboarding a single AP, use the claim code or QR code located on the rear of the AP. If you're onboarding multiple APs, use the activation code that is listed in your purchase order.

NOTE: You can simultaneously claim multiple APs and activate the subscriptions listed in the PO using the activation code. See [Activate a Subscription](#).

To claim an AP using a Web browser:

1. Log in to your account at <https://manage.mist.com/>.

If you don't have an account, see [Create a Mist Account and Organization](#) for details about creating one.

2. Go to **Organization > Inventory > Access Points** and click **Claim APs**.
3. Enter the activation code or claim code.

4. (Optional) Select the site to which you want to assign the AP.
You can choose to assign the AP to a primary site (default) or any other site. If you want to assign the AP to a site later, clear the **Assigned claimed APs to site** check box.
5. (Optional) Select the **Generate names for APs, with format:** check box and enter a name format for the AP.
You can use this option only if you are assigning the AP to a site.
You can also choose to rename and assign an AP to a site after you claim the AP.
6. Click **Claim**.
Review the information and close the window.

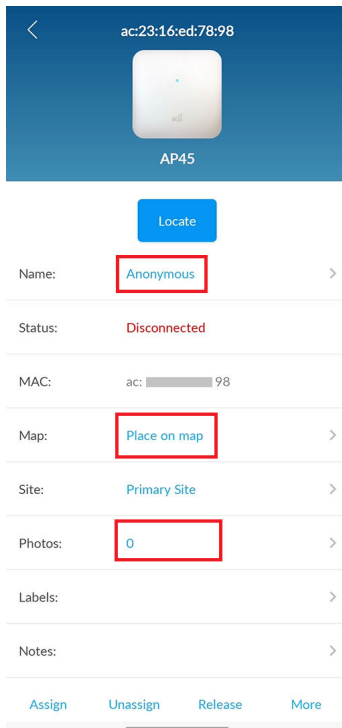
Claim an AP Using the Mist AI Mobile App

To onboard a single AP using the Mist AI mobile app from your mobile phone:

1. Download and install the Mist AI app from the Google [Play Store](#) or Apple [App Store](#).
2. Open the Mist AI app and log in using your account credentials.
If you do not have an account, see [Create a Mist Account and Organization](#) for details about creating one.
3. Select your organization.
4. Tap the site to which you want to assign the AP.
5. Ensure that the Access Points tab is selected and tap +.
6. Locate the QR code on the AP. The QR code is located on the rear panel of the AP.
7. Focus the camera on the QR code.

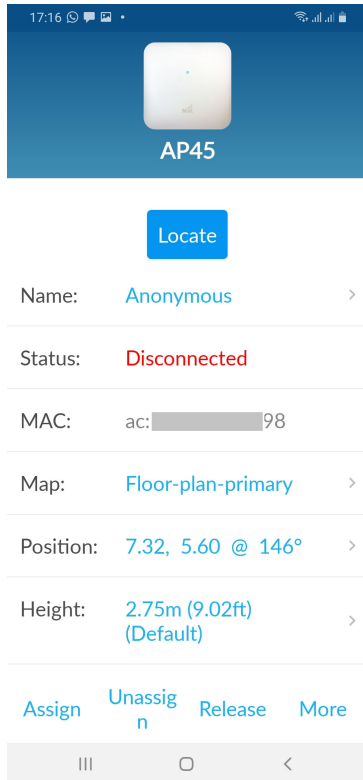
The app automatically claims the AP and adds it to your site. You'll see the new AP listed under the Access Points tab.

8. Tap the AP to view its details.



You can perform various tasks from the AP details screen such as renaming the AP, setting it on a floor plan, releasing an AP, or even adding a photo. Simply tap the option and you can update the details. To rename an AP, tap the AP name and enter a new name.

To place an AP on a floor plan, tap **Place on map**. You need to have a floor plan already uploaded in **Location > Live View** in the Juniper Mist™ portal to use this option. See [Adding and Scaling a Floorplan](#). After you place the AP on the floor plan, you'll see more details such as the position of the AP and the height at which the AP is mounted (default value that you can modify).



The following video also depicts the process of claiming a Mist AP using the Mist AI mobile app. Please start the video at 4:00 to see this process.

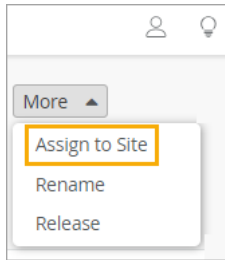


Video: [Mist Access Point Onboarding](#)

Assign Access Points to Sites

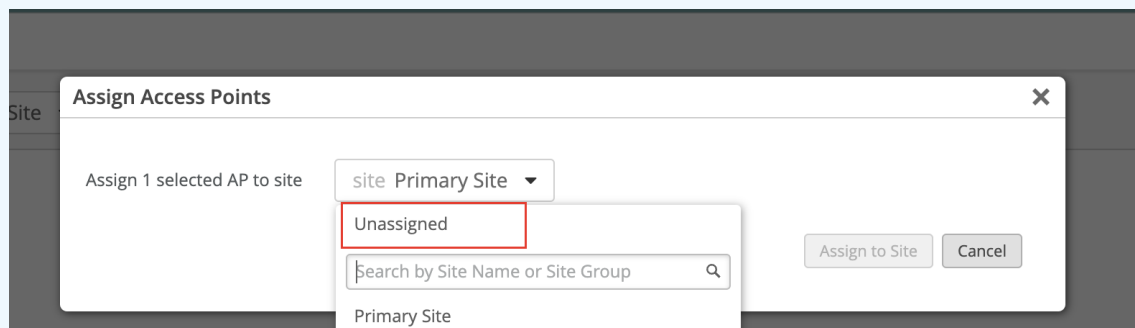
Access Points (APs) that you've not assigned to any site display the status as Unassigned on the Inventory page in the Juniper Mist portal. To assign an AP to a site:

1. From the left menu of the Juniper Mist™ portal, select **Organization > Inventory**.
2. Click the **Access Points** button at the top of the page.
3. Select the check box for one or more APs.
4. Click the **More** button near the top-right corner of the page, and then click **Assign to Site**.



5. In the pop-up window, select the site, and then click **Assign to Site**.

NOTE: If you need to change the site to which the AP is assigned, then select **Unassigned** in step 5.



Mist unassigns the AP from the current site and places the AP back in the inventory with the status as Unassigned. You can then follow steps 1 through 5 (above) to assign the AP to the desired site.

Enable Configuration Persistence

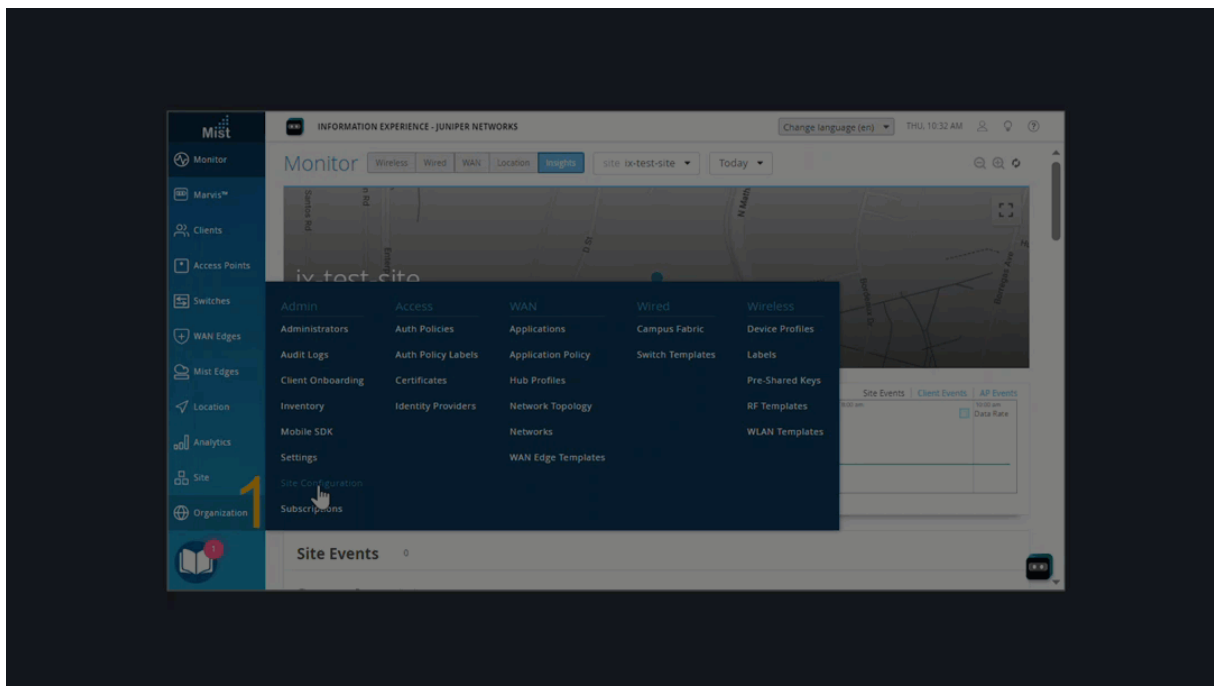
To ensure access point (AP) stability, you can enable configuration persistence. With configuration persistence, an AP stores its full configuration on board. If it can't connect to the Juniper Mist cloud, it can reboot from the stored configuration. Configuration persistence also enables an AP to continue providing wireless service even if it loses connectivity to the cloud.

Without configuration persistence, an AP stores only critical information, such as its static IP address. If the AP loses power, it must connect to the Juniper Mist™ cloud to access its full configuration and reboot. If it can't connect, it can't retrieve its configuration.

We recommend that you enable AP configuration persistence on your sites.

You'll need to enable configuration persistence if you want to use an AP in survey mode. See ["Configure an AP for Survey Mode" on page 96](#).

Watch the following video to learn how to enable configuration persistence:



To enable configuration persistence for all APs in a site:

1. From the left menu of the Juniper Mist portal, select **Organization** > **Site Configuration**.
2. Click the site that you want to configure.
3. Scroll down to the AP Config Persistence section of the page.
4. Select **Enable**.
5. Click **Save**.

Adding and Scaling a Floorplan

IN THIS SECTION

- [Manually Upload Your Floorplan | 34](#)
- [Import a Floorplan | 35](#)
- [Scale a Floorplan | 36](#)

Floorplans provide a helpful visualization for managing the placement of Juniper Mist™ Access Points (APs) and other devices in your deployment.

For location services deployments, every site needs at least one accurately scaled floorplan,

To add a floorplan to a site, upload an image or import a complete floorplan from a third-party application such as Ekahau or iBwave. Then set the scale.

For details, continue to the next topics in this guide.

Manually Upload Your Floorplan

IN THIS SECTION

- [Before You Begin | 34](#)
- [Video Overview | 34](#)
- [Procedure | 34](#)

Before You Begin

- Obtain an image file in a supported format: PNG (recommended), JPG, JPEG, GIF, or BMP.
- Crop the image so that there is little white space around the perimeter of the floorplan as possible.
- Determine the known physical distance of two points and correlate them to the same two points on the floor plan. For example, the width of a room or the length of a hallway.

You'll need this information to set the scale. If you don't have this information, you can look for a standard doorway on the floorplan and scale to a typical width of 0.91 meters (3 feet).

Video Overview



Video: [Manually Upload a Floorplan](#)

Procedure

1. From the left menu of the Juniper Mist portal, select **Location** > **Live View**.
2. Upload your image file:
 - a. Click **Add Floorplan**.
 - b. Follow the on-page prompts to enter a name and upload the image.
3. Click **Save** (in the top right corner of the page).

Next steps:

- ["Scale a Floorplan" on page 36](#)
- ["Manually Place an Access Point on a Floorplan" on page 39](#)
- *Validate Your Floorplan*

Import a Floorplan

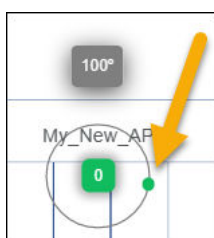
To import a floorplan:

1. From the left menu of the Juniper Mist portal, select **Location** > **Live View**.
2. Select the site.
3. Click **Import Floorplans** (near the top right corner of the page).
4. At the bottom of the dialog box, click **More Options**, and then select the import options that you want to enable.
 - **Include floorplans with unmatched APs**
 - When this option is selected, Juniper Mist imports all floorplans in the file, even if the APs have not been adopted or claimed in your organization.
 - When this option is unselected, the import only includes floorplans with APs that have been claimed or adopted by your organization. If a floorplan includes an AP that is not in your organization, the floorplan will not be imported.
 - **Import AP height**—The import includes any information that the floorplan contains about AP height. AP height is a required attribute for location accuracy. If you don't import this data, you'll need to enter it in the device details.
 - **Import AP orientation**—The import includes any information that the floorplan contains about AP orientation. AP orientation refers to the placement of the AP based on the direction in which the AP LED is facing. AP orientation is a required attribute for location accuracy. If you don't import this data, you'll need to enter it in the device details.
5. Under **Floorplan Definition**, click the button to import the file.
6. Click **Save** (in the top right corner of the page).
7. Review the floorplan to ensure that it depicts accurate information about the position, height, and orientation of each AP.
8. If you need to make changes, click **Setup Floorplan**, and then make changes as needed.
 - To edit the position—Manually drag the AP to the correct position. You can also click the AP, click **Edit**, and enter the **X position** and the **Y position**.

Selected Access Point	
Name	My_New_AP
MAC	d4:dc:09:24:ee:12
Minor	49232
x, y (m)	19.4902, -2.3477
Height (m)	2.75
Rotation	260°
Mount	Floor

AP Details • **Edit** • Remove

- To edit the height—Click the AP, click **Edit**, and then enter the height (in meters).
- To change the orientation—Click the AP and drag the green dot so that it represents the physical orientation of the LED on the AP. You can also click the **Edit** button in the **Selected Access Point** section, and then enter the **Rotation** in degrees.



NOTE: To visualize the concept of orientation, mentally draw a line from the Juniper Mist logo through the LED to an endpoint such as the nearest wall. The green dot needs to align with that imaginary path.

Next steps:

- ["Scale a Floorplan" on page 36](#)
- ["Manually Place an Access Point on a Floorplan" on page 39](#)
- *Validate Your Floorplan*

Scale a Floorplan

IN THIS SECTION

- [Video Overview | 37](#)

After you "upload" on page 34 or "import" on page 35 your floorplan, you need to set the scale.

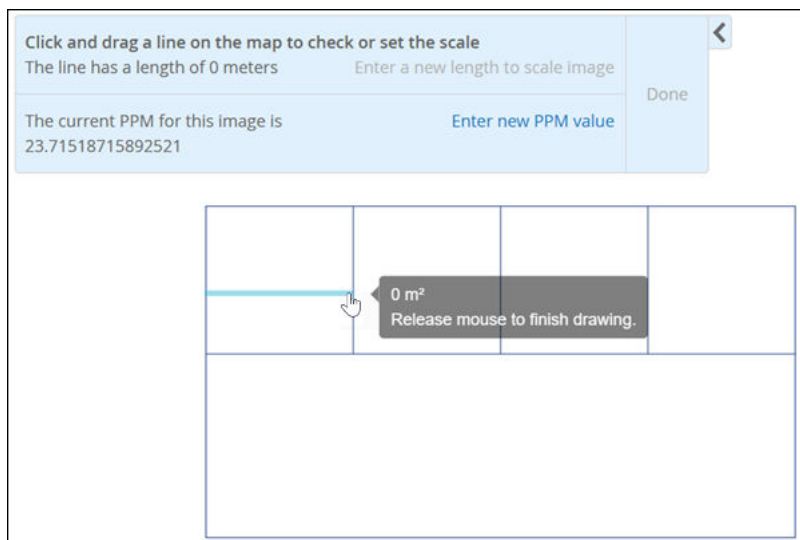
Video Overview



Video: [Scale a Floorplan](#)

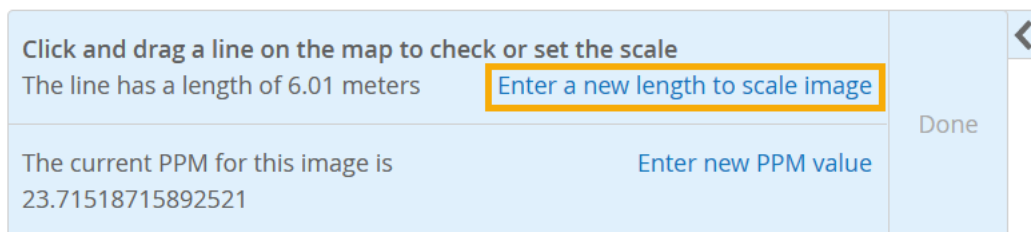
1. From the left menu of the Juniper Mist portal, select **Location** > **Live View**.
2. Select the site and the floorplan.
3. Click **Set Up Floorplan**.
4. Click **Set Scale** (near the top left corner of the floorplan).
5. Drag a line between two points on the floorplan.

For example, you might draw a line across the width of a room or the length of a hallway.



TIP: If you don't know the actual dimensions, look for a standard door on the floorplan and scale that door to 0.91 meters (3 feet). This will get you close to the actual scale.

6. Click **Enter a new length to scale image**.



7. Enter the measurement and the unit (**Meters** or **Feet**).

Ensure that the scale is accurate. If a hallway is 60 feet long, the floorplan needs to show it as 60 feet long. Otherwise, the location information will be inaccurate.

8. Click **Done**.



9. Click **Save** in the upper-right corner of the page.

Next steps:

- ["Manually Place an Access Point on a Floorplan" on page 39](#)
- *Validate Your Floorplan*

Adding Access Points to a Floorplan

IN THIS SECTION

- [Manually Place an Access Point on a Floorplan | 39](#)
- [Autoplacement: Verify Access Point Positions for an Existing Site \(BETA\) | 42](#)
- [Autoplacement: Position New Access Points \(BETA\) | 48](#)
- [Auto-Orientation: Rotate Access Points \(BETA\) | 55](#)

Adding Juniper Mist™ Access Points (APs) to the floorplan provides a helpful visualization for your deployment.

For Location Services deployments, correct positions of Juniper Mist™ APs are critical, as this ensures location accuracy.

You can add APs in these ways:

- ["Manually Place an Access Point on a Floorplan" on page 39](#)
- ["Autoplacement: Position New Access Points \(BETA\)" on page 48](#)

If you've already added APs to a floorplan, you can use the Auto Placement feature to check the positions of the APs on the floorplan and correct any issues. See ["Autoplace: Verify Access Point Positions for an Existing Site \(BETA\)" on page 42](#).

Manually Place an Access Point on a Floorplan

IN THIS SECTION

- [Before You Begin | 39](#)
- [Procedure | 40](#)

Before You Begin

Install your access points (APs) and claim or adopt them into your organization.

Obtain the following information about each AP:

- The MAC address of the AP
- The actual position of the AP at the site
- The height of the AP (the distance between the floor and the AP)
- The orientation of the AP

To visualize the concept of orientation, stand below the AP and mentally draw a line from the Juniper Mist logo through the LED to an endpoint such as the nearest wall. Make a note of that endpoint ("The LED points to the north wall.") This information will help you to correctly indicate the orientation on the floorplan in the Juniper Mist portal.

The following figure shows the location of the LED on an AP.



Procedure

1. From the left menu of the Juniper Mist portal, select **Location** > **Live View**.
2. Select the site and the floorplan.
3. To ensure that APs appear on the floorplan:
 - a. Click the **Settings** button (near the top right corner of the page).



- b. Select the check boxes to show BT11 and Wi-Fi APs.

Location Settings

☐ Show WiFi Clients

☐ Show BLE Clients

☐ Show Assets

☐ Show WiFi Clients Associated AP

☐ Show client trails for the most recent locations

☒ Show BT11 Access Points

☒ Show WiFi Access Points

☒ Connected

☒ Disconnected

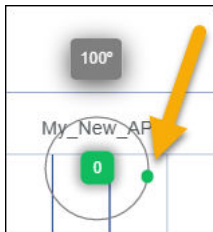
- c. Close the **Location Settings** window.

4. Click **Set Up Floorplan**.
5. Click the **APs** tab (on the right side of the page).
6. Under **Available APs**, drag an AP into position on the floorplan.
Ensure that the position on the floorplan corresponds to its actual position at your site.
7. In the **Selected Access Point** section, check the MAC address of the AP. Ensure that you have selected the correct AP for this area of the floorplan.

Selected Access Point	
Name	My_New_AP
MAC	d4:dc:09:24:ee:12
Minor	49232
x, y (m)	19.4902, -2.3477
Height (m)	2.75
Rotation	260°
Mount	Floor

AP Details • Edit • Remove


8. To set the orientation, drag the green dot so that it represents the actual orientation of the LED on the AP. You can also click **Edit** in the **Selected Access Point** section, and then enter the **Rotation** in degrees.



NOTE: In the "Before You Begin" on page 39 section, we imagined drawing a line from the Juniper Mist logo through the LED to an endpoint on the north wall. Here, we drag the green dot so that it aligns with that imaginary path.

9. Set the AP height:
 - a. Click the AP.
 - b. Click **Edit** in the **Selected Access Point** section.

Selected Access Point	
Name	My_New_AP
MAC	d4:dc:09:24:ee:12
Minor	49232
x, y (m)	19.4902, -2.3477
Height (m)	2.75
Rotation	260°
Mount	Floor

AP Details • **Edit** • Remove 

c. Enter the height of the AP in meters.

d. Click **Save**.

10. Continue to add APs until the **Available APs** list is empty.

11. Click **Save** (near the top right corner of the page).

Next Steps

As a final step in setting up your floorplan, *validate it*.

Autoplacement: Verify Access Point Positions for an Existing Site (BETA)

If you've already placed access points (APs) on your uploaded floorplan, you can use the autoplacement feature to check AP positions and correct any issues.

For Location Services deployments, correct positions on the floorplan are critical to ensure location accuracy.

NOTE: You should only attempt autoplacement during a maintenance window. During the autoplacement process, wireless clients cannot connect to APs as the APs will not broadcast the SSIDs. The amount of downtime you need to schedule depends on how many APs are on the floorplan.

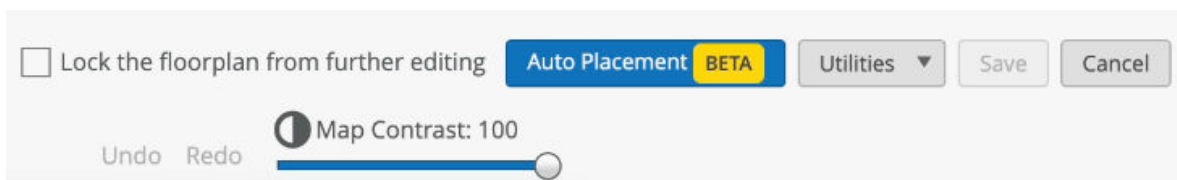
Before you use the autoplacement feature in an existing deployment, ensure that:

- You have physically installed all APs at the site.
- You have claimed or adopted the APs into your Juniper Mist organization.
- You have placed the APs on the floorplan in the Juniper Mist portal.

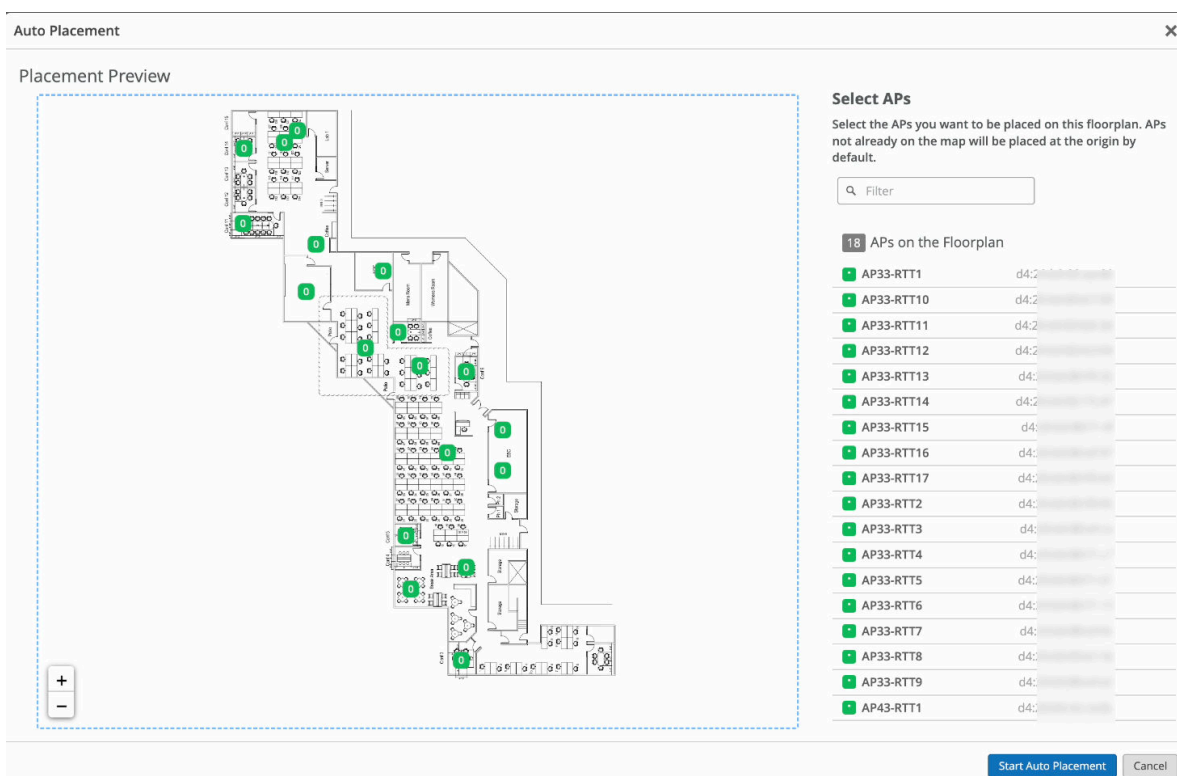
NOTE: If the preceding description doesn't fit your situation, see ["Autoplacement: Position New Access Points \(BETA\)"](#) on page 48.

To use autoplacement to verify AP positions on a floorplan:

1. From the left menu of the Juniper Mist portal, select **Location** > **Live View**.
2. Select the site and the floorplan.
3. Click **Setup Floorplan**.
4. Click the **Auto Placement** button near the top right corner of the page.

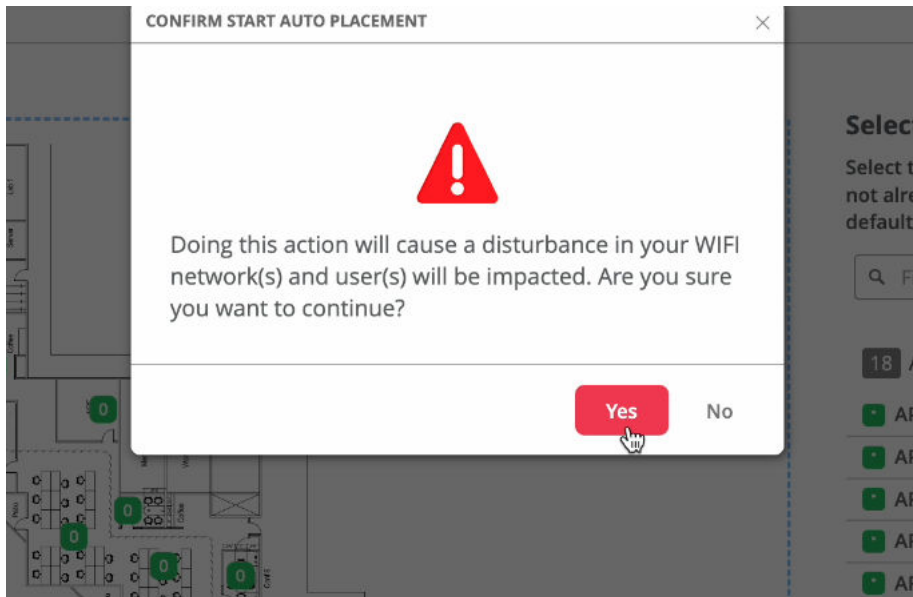


5. On the list of APs in the Floorplan section on the right side of the page, select the APs for which you want to verify the floorplan position.

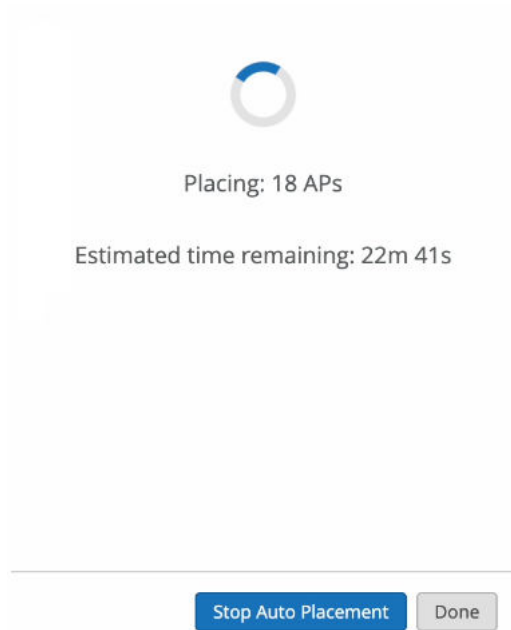


NOTE: Optionally, you also can select APs from the **Available APs** list. The APs on this list have not yet been placed on the floorplan. Juniper Mist will add them to the floorplan during this process.

6. Click **Start Auto Placement**.
7. When the warning appears, read the information, and then click **Yes** to continue or **No** to cancel.



It takes a few moments for Juniper Mist to complete the operation and display the X,Y coordinates of the APs. The amount of time it takes depends on how many APs are on the floorplan. The more APs you place on the floorplan, the longer it takes the autoplacement operation to complete.



8. On the right side of the page, view the progress and final status message:

- If you see the Placement Preview and a large check mark on the right side of the page, it indicates that the autoplacement process is complete. You can review the results and either accept or reject the results. See the Evaluate the Results section below.
- If you see “APs Misplaced” on the right side of the window instead of a large check mark, this means that an error occurred. You need to restart the autoplacement process.

Evaluate the Results in the List View

After you initiate autoplacement, Juniper Mist™ displays the Placement Preview. Use the List View to evaluate the results.

Example: Placement Preview with Completed Status

Auto Placement

Placement Preview

List

Map

Filter

#	<input checked="" type="checkbox"/>	Confidence	Name	MAC	Original x,y (m)	New x,y (m)	Delta	Verified
1	<input checked="" type="checkbox"/>	High	AP33-RTT1	d4:...	0, 0	9.5537, -6.3471	-9.5537, 6.3471	
10	<input checked="" type="checkbox"/>	High	AP33-RTT2	d4:...	0, 0	4.0992, -7.0744	-4.0992, 7.0744	
11	<input checked="" type="checkbox"/>	High	AP33-RTT3	d4:...	4.5494, -17.257	4.5494, -17.257	0, 0	<input checked="" type="checkbox"/>
12	<input checked="" type="checkbox"/>	High	AP33-RTT4	d4:...	0, 0	13.719, -19.9008	-13.719, 19.9008	
13	<input checked="" type="checkbox"/>	Medium	AP33-RTT5	d4:...	0, 0	22.6446, -23.5041	-22.6446, 23.5041	
14	<input checked="" type="checkbox"/>	High	AP33-RTT6	d4:...	0, 0	12.4628, -26.2479	-12.4628, 26.2479	
15	<input checked="" type="checkbox"/>	High	AP33-RTT7	d4:...	0, 0	24.7273, -31.6694	-24.7273, 31.6694	
16	<input checked="" type="checkbox"/>	High	AP33-RTT8	d4:...	0, 0	20.3306, -33.7851	-20.3306, 33.7851	
17	<input checked="" type="checkbox"/>	High	AP33-RTT9	d4:...	30.9058, -37.3378	30.9058, -37.3378	0, 0	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	High	AP33-RTT10	d4:...	0, 0	33.8182, -36.9917	-33.8182, 36.9917	
3	<input checked="" type="checkbox"/>	High	AP33-RTT11	d4:...	0, 0	38.6116, -44.6612	-38.6116, 44.6612	
4	<input checked="" type="checkbox"/>	High	AP33-RTT12	d4:...	0, 0	31.3058, -47.7686	-31.3058, 47.7686	
5	<input checked="" type="checkbox"/>	Medium	AP33-RTT13	d4:...	0, 0	38.6446, -50.0826	-38.6446, 50.0826	
6	<input checked="" type="checkbox"/>	High	AP33-RTT14	d4:...	0, 0	25.686, -58.876	-25.686, 58.876	
7	<input checked="" type="checkbox"/>	High	AP33-RTT15	d4:...	34.0434, -63.537	34.0434, -63.537	0, 0	<input checked="" type="checkbox"/>
8	<input checked="" type="checkbox"/>	High	AP33-RTT16	d4:...	0, 0	26.3471, -65.9835	-26.3471, 65.9835	

Placed

Verified

Isolated

Error

Start Auto Placement Again

Accept 18 Placement

Reject 18 Placement

Cancel

Completed

18 Access Points have been automatically placed on the floorplan.

Example: Partially Complete Autoplacement

Auto Placement

Placement Preview

List

Map

Filter

#	<input type="checkbox"/>	Confidence	Name	MAC	Original x,y (m)	New x,y (m)	Delta	Verified
1	<input checked="" type="checkbox"/>	High	AP33-RTT1	d4:...	9.5537, -6.3471	9.5537, -6.3471	0, 0	
10	<input checked="" type="checkbox"/>	High	AP33-RTT2	d4:...	4.0992, -7.0744	4.0992, -7.0744	0, 0	
11	<input checked="" type="checkbox"/>	High	AP33-RTT3	d4:...	4, -17.157	4, -17.157	0, 0	
12	<input checked="" type="checkbox"/>	High	AP33-RTT4	d4:...	13.719, -19.9008	13.719, -19.9008	0, 0	
13	<input type="checkbox"/>		AP33-RTT5	d4:...	22.6446, -23.5041	22.6446, -23.5041	0, 0	
14	<input checked="" type="checkbox"/>	High	AP33-RTT6	d4:...	12.4628, -26.2479	12.4628, -26.2479	0, 0	
15	<input checked="" type="checkbox"/>	High	AP33-RTT7	d4:...	24.7273, -31.6694	24.7273, -31.6694	0, 0	
16	<input checked="" type="checkbox"/>	High	AP33-RTT8	d4:...	20.3306, -33.7851	20.3306, -33.7851	0, 0	
17	<input checked="" type="checkbox"/>	High	AP33-RTT9	d4:...	27.5372, -36.1983	27.5372, -36.1983	0, 0	
2	<input checked="" type="checkbox"/>	High	AP33-RTT10	d4:...	33.8182, -36.9917	33.8182, -36.9917	0, 0	
3	<input checked="" type="checkbox"/>	High	AP33-RTT11	d4:...	38.6116, -44.6612	38.6116, -44.6612	0, 0	
4	<input checked="" type="checkbox"/>	High	AP33-RTT12	d4:...	31.3058, -47.7686	31.3058, -47.7686	0, 0	
5	<input checked="" type="checkbox"/>	High	AP33-RTT13	d4:...	38.6446, -50.0826	38.6446, -50.0826	0, 0	
6	<input checked="" type="checkbox"/>	High	AP33-RTT14	d4:...	25.686, -58.876	25.686, -58.876	0, 0	
7	<input checked="" type="checkbox"/>	High	AP33-RTT15	d4:...	33.7851, -63.0083	33.7851, -63.0083	0, 0	
8	<input checked="" type="checkbox"/>	High	AP33-RTT16	d4:...	26.3471, -65.9835	26.3471, -65.9835	0, 0	

Placed

Verified

Isolated

Error

Start Auto Placement Again

Accept 16 Placement

Reject 16 Placement

Cancel

Partially Complete

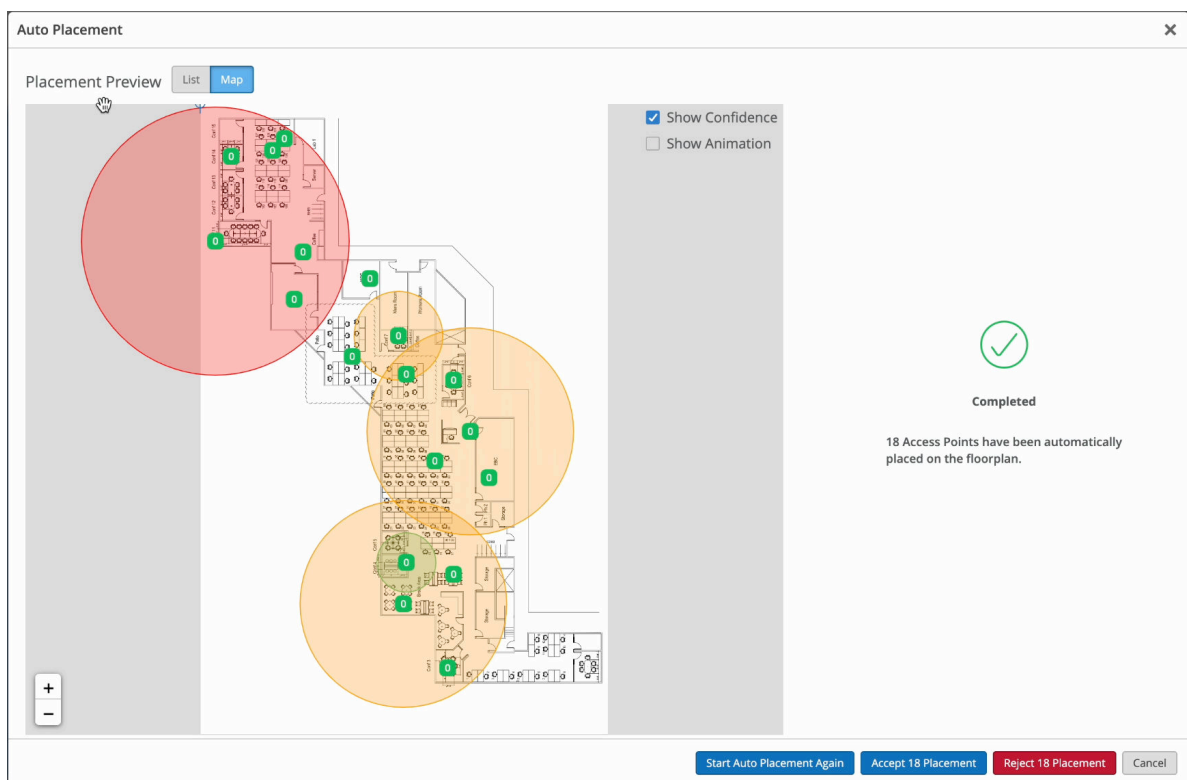
16 APs have been automatically placed on the floorplan. Verify AP placement values near isolated APs.

Icons

- Green check mark—For existing deployments, a green check mark in the Verified column indicates that Juniper Mist successfully verified the AP position.
- Blue square—A blue square next to the AP name indicates that the AP is isolated and cannot communicate with other nearby APs. Juniper Mist cannot place these APs on the floorplan automatically, which is why the autoplacement status is Partially Complete.

View More Information in the Map View

Click the **Map View** button, and then select the **Show Confidence** check box in the top right corner of the map. Juniper Mist displays the confidence levels for the APs.



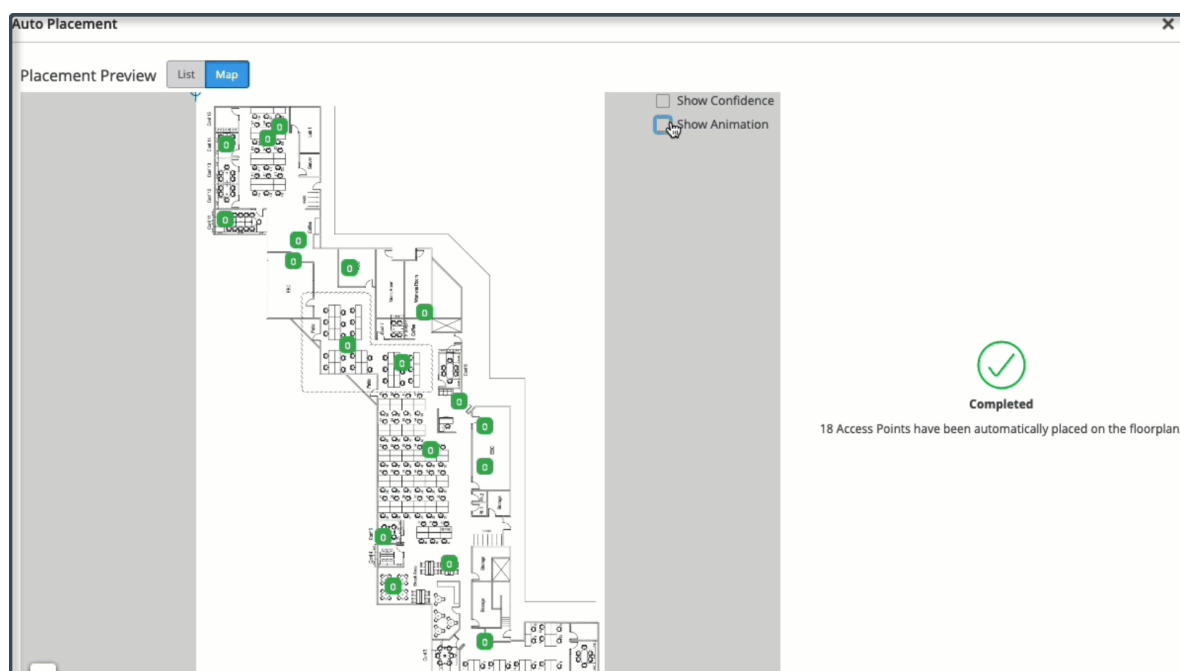
TIP: To view the confidence level for an individual AP, hover your mouse over the AP.

The confidence level indicates how confident Mist is with the autoplacement of the APs. Confidence levels are high, medium, and low. Mist displays a radius to indicate the probability of where the APs might be located. The algorithm places the APs in the most probable location.

- A low confidence level (red) is associated with a larger radius area and indicates low certainty about the actual location of the APs. If Mist indicates a low confidence level, then you'll need to manually place the APs on your floorplan within the radius predicted by Mist. Note that Mist cannot place isolated APs automatically on the floor plan—you'll need to manually place them on the floor plan.
- A high confidence level (green) indicates a smaller probability area and therefore high certainty about the AP location.
- A medium confidence level is indicated by orange color.

To get a visual of how the APs were autoplace, click the **Show Animation** check box in the top right corner of the map.

Example: Autoplacement for Existing Site (Animation)



Accept or Reject the Results

You can accept or reject the results for individual APs or for all APs.

Select or clear the check boxes as needed, and then click **Accept** or **Reject**.

Autoplacement: Position New Access Points (BETA)

With the autoplacement feature, Juniper Mist™ can place the access point (AP) X,Y coordinates on a floorplan for you automatically. This feature saves time and makes for an easier deployment.

NOTE: You should only attempt autoplacement during a maintenance window. During the autoplacement process, wireless clients cannot connect to APs as the APs will not broadcast the SSIDs. The amount of downtime you need to schedule depends on how many APs are on the floorplan.

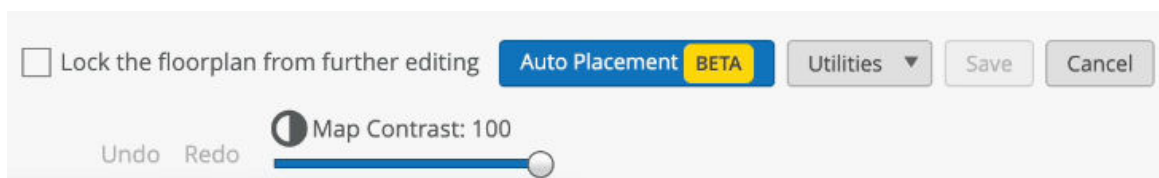
Before you use the autoplacement feature in a new deployment, ensure that:

- You have physically installed the APs at the site.
- You have claimed or adopted the APs into your Juniper Mist organization.
- You *have not* placed any APs placed on the floorplan in the Juniper Mist portal.

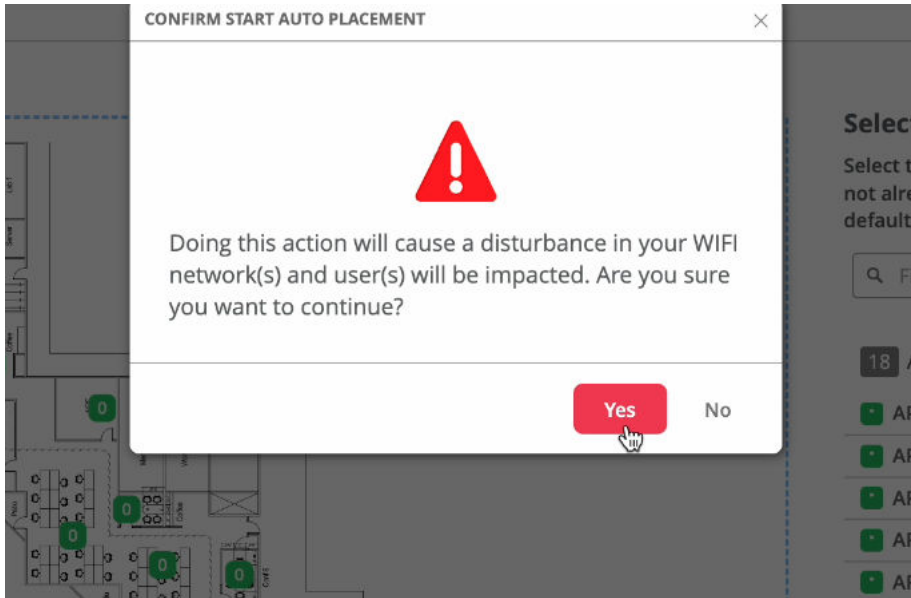
NOTE: If the preceding description doesn't fit your situation, see ["Autoplacement: Verify Access Point Positions for an Existing Site \(BETA\)"](#) on page 42.

To place access points on a floorplan automatically:

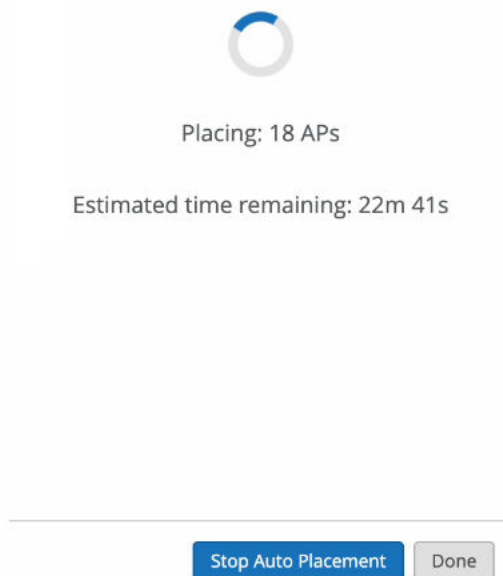
1. From the left menu of the Juniper Mist portal, select **Location > Live View**.
2. Select the site and the floorplan.
3. Click **Setup Floorplan**.
4. Click the **Auto Placement** button near the top right corner of the page.



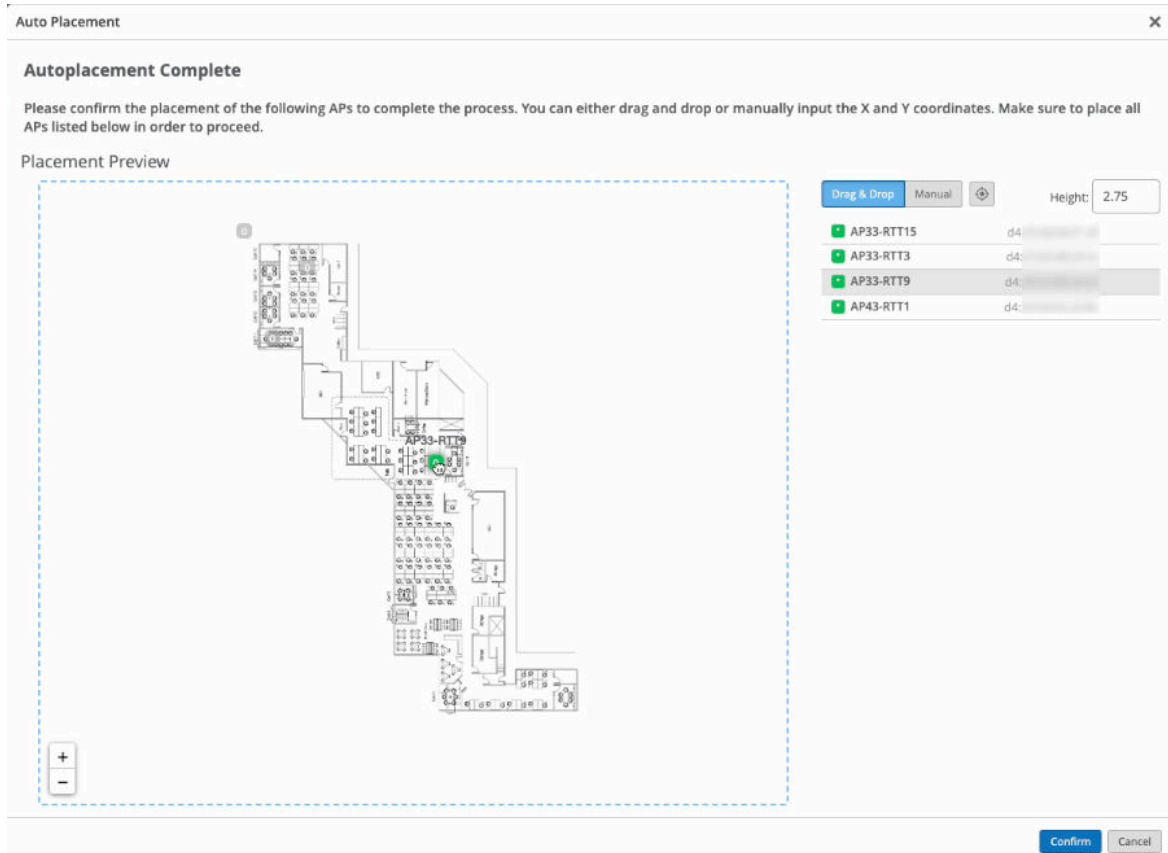
5. Select the APs that you want to place on the floorplan.
6. Click **Start Auto Placement**.
7. When the warning appears, read the information, and then click **Yes** to continue or **No** to cancel.



It takes a few moments for Juniper Mist to complete the operation and display the X,Y coordinates of the APs. The amount time it takes depends on how many APs are on the floorplan. The more APs you place on the floorplan, the longer it takes the autoplacement operation to complete.



Upon completion of the autoplacement scanning, Juniper Mist prompts you to select your reference APs. You need to identify the positions of these APs manually. The reference APs act as a source of truth that Juniper Mist uses to calculate the locations to place the remaining APs automatically.



8. Do one of the following:
 - Drag and drop the reference APs onto the floorplan.
 - Edit the APs' location with the X,Y position, height, and orientation angle. Make sure to set these values correctly as Mist uses the positions of the reference APs to calculate the positions of the remaining APs.
9. Click **Confirm**.
It takes a few moments to complete the operation and display the X,Y coordinates of the APs. The amount of time it takes depends on how many APs are on the floorplan.
10. On the right side of the page, view the progress message and the final status message:
 - If you see the Placement Preview and a large check mark on the right side of the page, it indicates that the autoplacement process is complete. You can review the results and either accept or reject the results. See the Evaluate the Results section below.
 - If you see "APs Misplaced" on the right side of the window instead of a large check mark, this means that an error occurred. You need to restart the autoplacement process.

Evaluate the Results in the List View

View the results in the List View of the Placement Preview.

Example: Placement Preview with Completed Status

Auto Placement

Placement Preview

List

Map

Filter

#	✓	Confidence	Name	A	MAC	Original x,y (m)	New x,y (m)	Delta	Verified
1	✓	High	AP33-RTT1	d4:		0, 0	9.5537, -6.3471	-9.5537, 6.3471	
10	✓	High	AP33-RTT2	d4:		0, 0	4.0992, -7.0744	-4.0992, 7.0744	
11	✓	High	AP33-RTT3	d4:		4.5494, -17.257	4.5494, -17.257	0, 0	✓
12	✓	High	AP33-RTT4	d4:		0, 0	13.719, -19.9008	-13.719, 19.9008	
13	✓	Medium	AP33-RTT5	d4:		0, 0	22.6446, -23.5041	-22.6446, 23.5041	
14	✓	High	AP33-RTT6	d4:		0, 0	12.4628, -26.2479	-12.4628, 26.2479	
15	✓	High	AP33-RTT7	d4:		0, 0	24.7273, -31.6694	-24.7273, 31.6694	
16	✓	High	AP33-RTT8	d4:		0, 0	20.3306, -33.7851	-20.3306, 33.7851	
17	✓	High	AP33-RTT9	d4:		30.9058, -37.3378	30.9058, -37.3378	0, 0	✓
2	✓	High	AP33-RTT10	d4:		0, 0	33.8182, -36.9917	-33.8182, 36.9917	
3	✓	High	AP33-RTT11	d4:		0, 0	38.6116, -44.6612	-38.6116, 44.6612	
4	✓	High	AP33-RTT12	d4:		0, 0	31.3058, -47.7686	-31.3058, 47.7686	
5	✓	Medium	AP33-RTT13	d4:		0, 0	38.6446, -50.0826	-38.6446, 50.0826	
6	✓	High	AP33-RTT14	d4:		0, 0	25.686, -58.876	-25.686, 58.876	
7	✓	High	AP33-RTT15	d4:		34.0434, -63.537	34.0434, -63.537	0, 0	✓
8	✓	High	AP33-RTT16	d4:		0, 0	26.3471, -65.9835	-26.3471, 65.9835	

Placed

Verified

Isolated

Error

Start Auto Placement Again

Accept 18 Placement

Reject 18 Placement

Cancel

✓

Completed

18 Access Points have been automatically placed on the floorplan.

Example: Partially Complete Autoplacement

Auto Placement

Placement Preview

List Map Filter

#	<input type="checkbox"/>	Confidence	Name	MAC	Original x,y (m)	New x,y (m)	Delta	Verified
1	<input checked="" type="checkbox"/>	High	AP33-RTT1	d4: [REDACTED]	9.5537, -6.3471	9.5537, -6.3471	0, 0	
10	<input checked="" type="checkbox"/>	High	AP33-RTT2	d4: [REDACTED]	4.0992, -7.0744	4.0992, -7.0744	0, 0	
11	<input checked="" type="checkbox"/>	High	AP33-RTT3	d4: [REDACTED]	4, -17.157	4, -17.157	0, 0	
12	<input checked="" type="checkbox"/>	High	AP33-RTT4	d4: [REDACTED]	13.719, -19.9008	13.719, -19.9008	0, 0	
13	<input type="checkbox"/>		AP33-RTT5	d4: [REDACTED]	22.6446, -23.5041	22.6446, -23.5041	0, 0	
14	<input checked="" type="checkbox"/>	High	AP33-RTT6	d4: [REDACTED]	12.4628, -26.2479	12.4628, -26.2479	0, 0	
15	<input checked="" type="checkbox"/>	High	AP33-RTT7	d4: [REDACTED]	24.7273, -31.6694	24.7273, -31.6694	0, 0	
16	<input checked="" type="checkbox"/>	High	AP33-RTT8	d4: [REDACTED]	20.3306, -33.7851	20.3306, -33.7851	0, 0	
17	<input checked="" type="checkbox"/>	High	AP33-RTT9	d4: [REDACTED]	27.5372, -36.1983	27.5372, -36.1983	0, 0	
2	<input checked="" type="checkbox"/>	High	AP33-RTT10	d4: [REDACTED]	33.8182, -36.9917	33.8182, -36.9917	0, 0	
3	<input checked="" type="checkbox"/>	High	AP33-RTT11	d4: [REDACTED]	38.6116, -44.6612	38.6116, -44.6612	0, 0	
4	<input checked="" type="checkbox"/>	High	AP33-RTT12	d4: [REDACTED]	31.3058, -47.7686	31.3058, -47.7686	0, 0	
5	<input checked="" type="checkbox"/>	High	AP33-RTT13	d4: [REDACTED]	38.6446, -50.0826	38.6446, -50.0826	0, 0	
6	<input checked="" type="checkbox"/>	High	AP33-RTT14	d4: [REDACTED]	25.686, -58.876	25.686, -58.876	0, 0	
7	<input checked="" type="checkbox"/>	High	AP33-RTT15	d4: [REDACTED]	33.7851, -63.0083	33.7851, -63.0083	0, 0	
8	<input checked="" type="checkbox"/>	High	AP33-RTT16	d4: [REDACTED]	26.3471, -65.9835	26.3471, -65.9835	0, 0	

Placed Verified Isolated Error

Partially Complete

16 APs have been automatically placed on the floorplan. Verify AP placement values near isolated APs.

Start Auto Placement Again Accept 16 Placement Reject 16 Placement Cancel

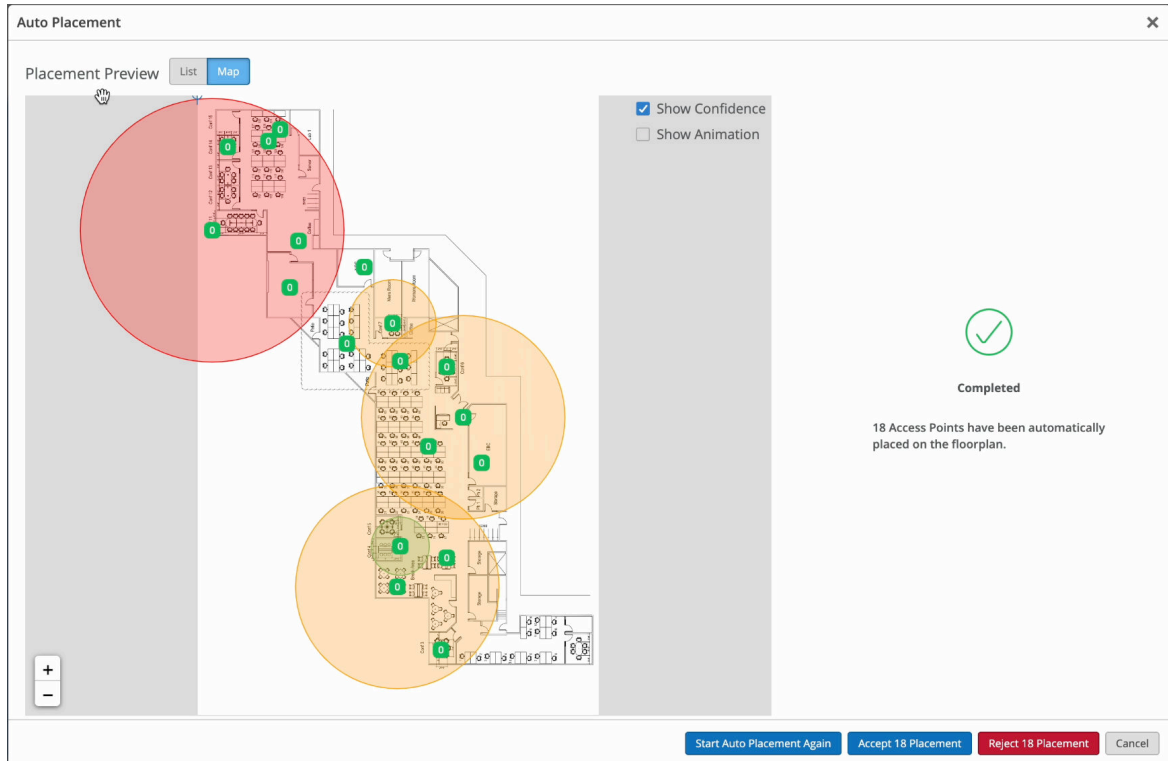
Icons

- Green check mark—For new site deployments, a green check mark appears only when a reference AP has been placed correctly.
- Blue square—A blue square next to the AP name indicates that the AP is isolated and cannot communicate with other nearby APs. Juniper Mist cannot place these APs on the floorplan automatically, which is why the autoplacement status is Partially Complete.

View More Information in the Map View

You can use the map view to evaluate the autoplacement.

Click the **Map View** button, and then select the **Show Confidence** check box in the top right corner of the map. Juniper Mist displays the confidence levels for the APs.



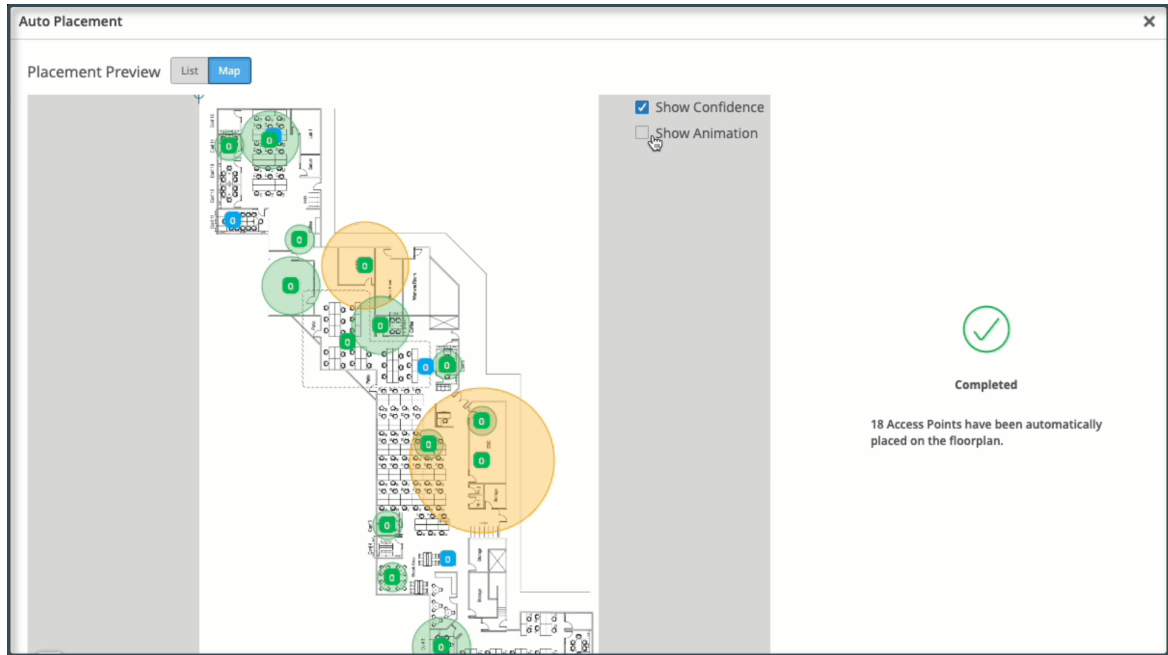
TIP: To view the confidence level for an individual AP, hover your mouse over the AP.

The confidence level indicates how confident Mist is with the autoplacement of the APs. Confidence levels are high, medium, and low. Mist displays a radius to indicate the probability of where the APs might be located. The algorithm places the APs in the most probable location.

- A low confidence level (red) is associated with a larger radius area and indicates low certainty about the actual location of the APs. If Mist indicates a low confidence level, then you'll need to manually place the APs on your floorplan within the radius predicted by Mist. Note that Mist cannot place isolated APs automatically on the floor plan—you'll need to manually place them on the floor plan.
- A high confidence level (green) indicates a smaller probability area and therefore high certainty about the AP location.
- A medium confidence level is indicated by orange color.

To get a visual of how the APs were autoplaced, click the **Show Animation** check box in the top right corner of the map.

Example: New Site Autoplacement (Animation)



Accept or Reject the Results

You can accept or reject the results for individual APs or for all APs.

Select or clear the check boxes as needed, and then click **Accept** or **Reject**.

Auto-Orientation: Rotate Access Points (BETA)

If you've already placed access points (APs) on a Juniper Mist™ floorplan and have performed autoplacement, you can use the Auto-Orientation feature to check AP orientations and correct any issues.

NOTE: Auto-Orientation does NOT need to be run during a maintenance window. However, use of this feature requires a firmware dependency of version 0.14.28806 or higher, and is only supported by the following AP models: AP32, AP33, AP34, AP43, AP45.

Before you use the Auto-Orientation feature, ensure that you have:

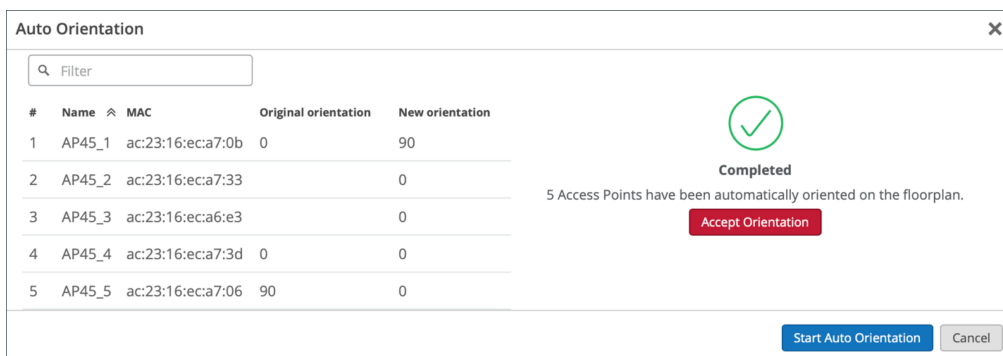
- Physically installed the AP at the site.
- Claimed or adopted the APs into your Juniper Mist organization.
- Placed the APs on the floorplan in the Juniper Mist portal.
- Performed ["Auto-Placement"](#) on page 48.

To use Auto-Orientation:

1. On the Juniper Mist portal, navigate to **Location > Live View**.
2. Select the applicable floorplan.
3. Select the **Setup Floorplan** button.
4. Select the **Auto Orientation** button.

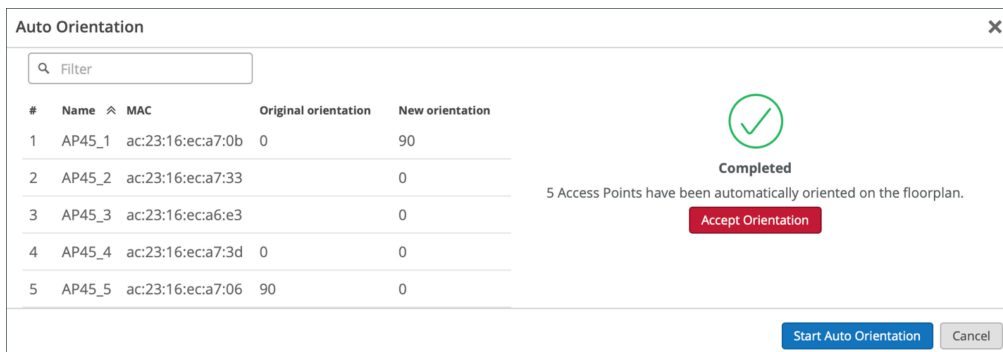


5. Select **Start Auto Orientation**.



Back on the Floorplan Setup section, you will see an “In Progress” status just below the Auto Orientation button. It will take 24 hours before you are returned with the rotation in degrees of the AP(s).

6. After 24 hours, return to the floorplan and select the Auto Orientation button to view the results. When the auto-orientation has completed, you will see a green checkmark in the window. It will also indicate the number of APs that were automatically oriented on the floorplan.



7. Accept the changes by selecting **Accept Orientation** or deny the changes by selecting **Cancel**. When you Accept the changes, you will see that your AP(s) have rotated into position on the floorplan.



8. You can optionally undo the changes by clicking on the Auto Orientation button, and then clicking the **Revert to Original** button from within the window.

Auto Orientation

Filter

#	Name	MAC	Original orientation	New orientation
1	AP45_1	ac:23:16:ec:a7:0b	0	
2	AP45_2	ac:23:16:ec:a7:33		
3	AP45_3	ac:23:16:ec:a6:e3		
4	AP45_4	ac:23:16:ec:a7:3d	0	
5	AP45_5	ac:23:16:ec:a7:06	90	

✓

Completed

5 Access Points have been automatically oriented on the floorplan.

Revert to Original

Start Auto Orientation

Cancel

RELATED DOCUMENTATION

- Autoplacement: Position New Access Points (BETA) | 48
- Autoplacement: Verify Access Point Positions for an Existing Site (BETA) | 42

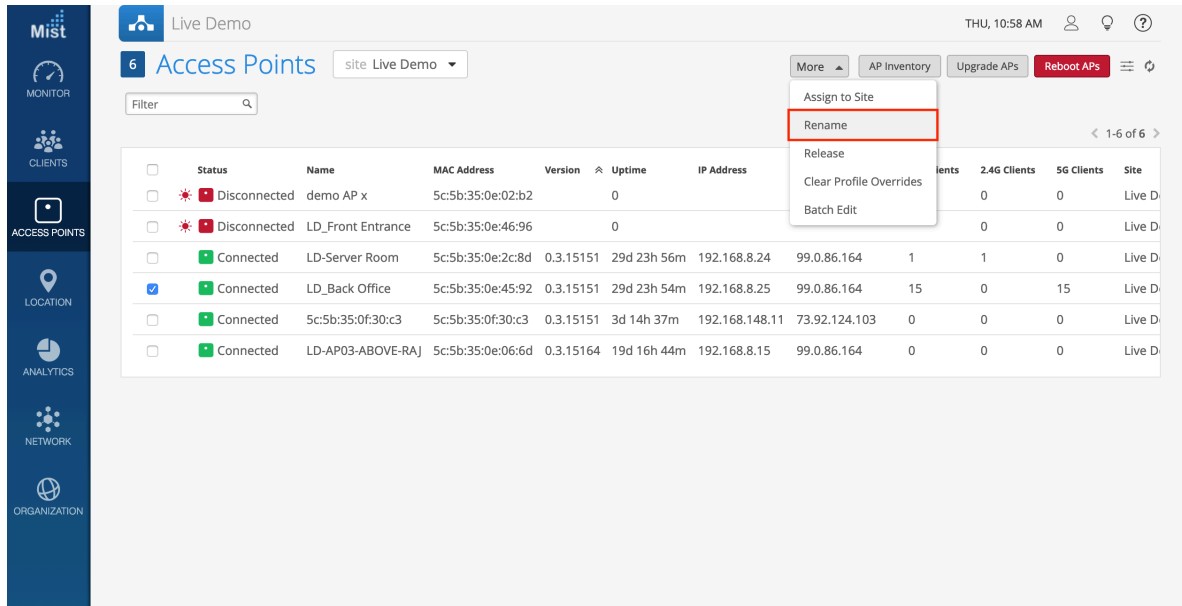
Rename a Juniper Access Point in the Mist Portal

You can rename the APs on your network for easy identification of APs. You can also use the Juniper Mist portal to automate the naming of APs by using variable fields in the name format. You can optionally include the site name, MAC address of the AP, and an incremental counter value in the name. Mist automatically updates these values when you add or rename an AP.

Note that when you initially claim an AP, Mist assigns the MAC address of the AP as its name by default.

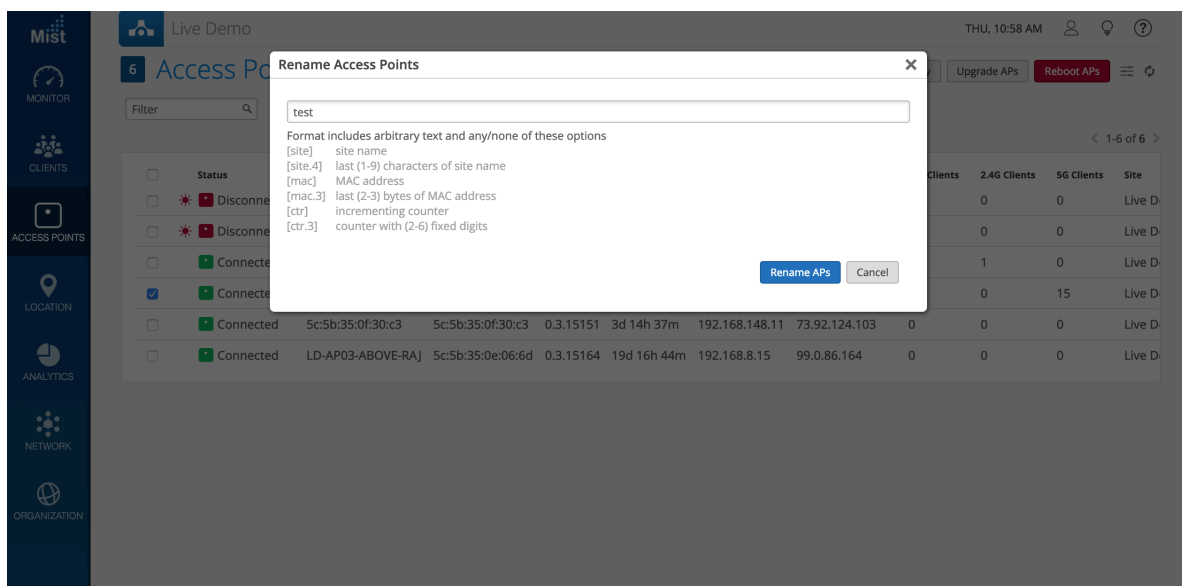
You can rename multiple APs at once. To rename APs in the Mist portal:

1. Navigate to the **Access Points** page on the Mist portal.
2. Select the APs that you want to rename.
3. Click **Rename** in the **More** menu in the top-right corner.



4. Enter a name on the **Rename Access Points** page.

You can use variable options to automatically name APs. If you include the counter (**{ctr}**) option, multiple APs are assigned names sequentially. You can also enter the starting value for the counter. The default counter value is 1. For example, consider that you need to rename three APs and you enter the name format as **primary-ap{ctr}** and a counter value as 2. Mist assigns the names as: primary-ap2, primary-ap3, and primary-ap4.



NOTE: You must include the **[mac]** or **[ctr]** field in the name format when renaming multiple APs at a time.

5. Click **Rename APs**.

Release an Access Point from Inventory

If you no longer want to include an access point (AP) in your Juniper Mist™ organization, you can release it from your inventory.

1. From the left menu of the Juniper Mist portal, select **Organization > Inventory**.
2. Click the **Access Points** button at the top of the page.
3. Select the check box for one or more APs.
4. Click the **More** button near the top-right corner of the page, and then click **Release**.
5. When the message appears, confirm that you want to release this AP.

The AP is no longer claimed by this organization and no longer managed by Juniper Mist.

Upgrade the Firmware on a Juniper Access Point

IN THIS SECTION

- [Firmware Version Tags for Juniper Mist Access Points | 60](#)
- [Check for AP Firmware Updates | 62](#)
- [Enable Auto Updates | 63](#)
- [Upgrade the Firmware on an AP Manually | 66](#)
- [Peer-to-Peer AP Firmware Upgrade | 67](#)

You can upgrade the firmware on an access point (AP) either manually or automatically. With the automatic upgrade method, you can only upgrade the firmware, whereas you can use the manual process to upgrade or downgrade the firmware.

Firmware Version Tags for Juniper Mist Access Points

IN THIS SECTION

Tag Definitions | 60

Notes | 61

Tag Definitions

The Juniper Mist™ portal displays tags to indicate the status of the firmware for Juniper Mist access points (APs).

These tags include:

- production
- rc2
- rc1

The firmware version also can appear without a tag.

Example

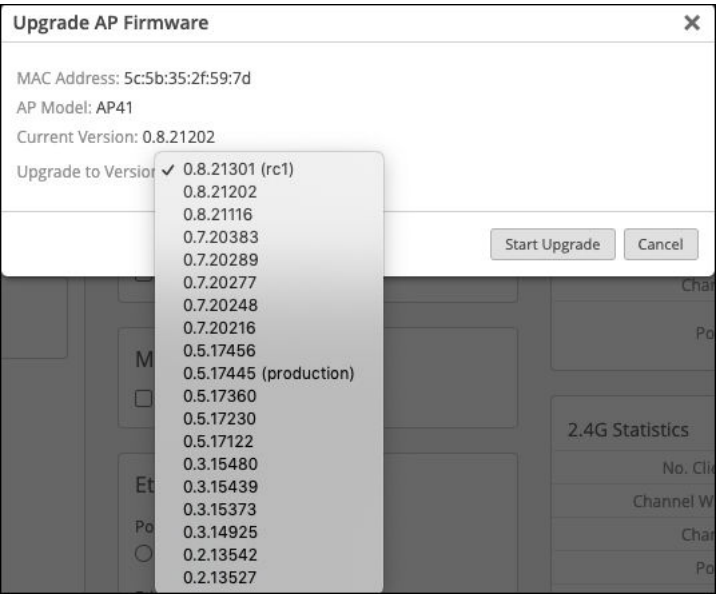


Table 6: Tag Definitions

production	This firmware is tested completely for the supported feature set. It is the most stable version of firmware. However, its features are limited compared to rc1 and rc2, which contain more recent features and bug fixes. Production firmware will not be modified, except to address security vulnerabilities.
rc2	This firmware has recent functionalities that are still under test. Features are complete, but we are adding critical bug fixes. This firmware is relatively stable to be deployed in the field.
rc1	This firmware is under active development. It has more recent bug fixes and functionalities than the rc2 firmware. This firmware is less stable than rc2.
untagged	This firmware is intended for demos and proof-of-concept purposes, allowing customers to evaluate certain features or functionalities. This firmware has more recent bug fixes and functionalities than the rc1 firmware.

Notes

Higher-numbered firmware contains all the fixes and features in the lower-numbered versions.

Regardless of tag status, we usually recommend a particular version for an AP model. Here's an example:

Upgrade APs Firmware

×

Total Access Points selected to upgrade: 1

Access Point Model: AP45

Selected Access Points: LD_Conf2

Upgrade To Version:

Select Version

Select Version

Suggested

0.12.27139 (rc1)

All

0.14.29313

0.14.29132

0.14.29091

0.14.28806

0.12.27299

0.12.27147

0.12.27139 (rc1)

0.12.27066

0.12.27043

0.12.27029

0.12.26980

Start Upgrade

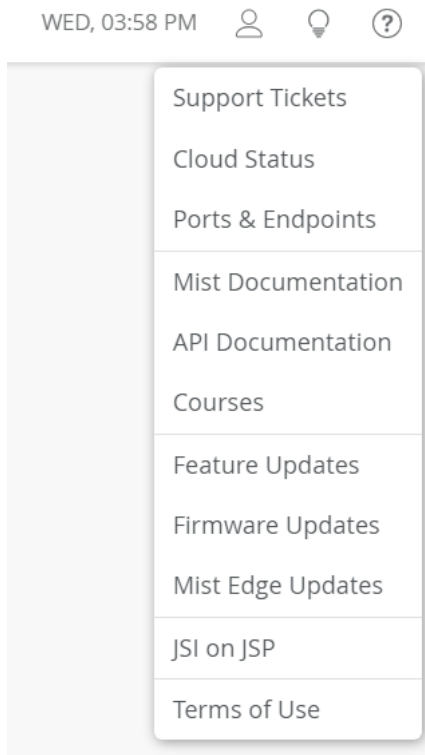
Cancel

Name	MAC Address	IP Address	Version	Model
LD_APEng	fc:03:7f	10.100.0.43	0.14.29331	AP34
LD_Bad_cable_AP	1e:c0:2b	10.100.0.221	0.14.29237	AP21
LD_Conf2	81:77:50	10.100.0.170	0.14.29331	AP45

Check for AP Firmware Updates

You can check for current firmware versions supported on AP models, features supported in a firmware version, and resolved issues. To view details about AP firmware:

1. Log in to the Mist portal using your credentials.
2. Click the ? (question-mark) icon in the top-right corner.
A drop-down menu appears.
3. Select **Firmware Updates** from the drop-down menu.



You'll see the Firmware page that provides information about the firmware versions. You can also view the recommended firmware version for each AP model under the **Current Firmware Versions** section.

NOTE: You can also click **Feature Updates** to see the release notes for the AP firmware.

Enable Auto Updates

SUMMARY

In your site configuration, you can enable automatic firmware upgrades for access points (APs).

IN THIS SECTION

- [Apply the Latest Production or Beta Firmware to All APs | 64](#)
- [Apply Specific Firmware to Specific Models | 65](#)

Auto updates will run on the schedule that you specify. On the specified date and time, Juniper Mist™ will check for updates. If found, Juniper Mist will apply the new firmware to your access points.

You can configure auto updates as follows:

- Apply the latest production or beta firmware to all APs
- Apply a specific firmware to specific AP models

Apply the Latest Production or Beta Firmware to All APs

With this option, Juniper Mist will check weekly for available updates and apply them to all APs. You determine whether to install the latest production firmware or the latest beta release.

To configure auto updates to apply the latest production or beta firmware:

1. From the left menu of the Juniper Mist portal, select **Organization > Site Configuration**.
2. Under AP Firmware Upgrade, select the check box for **Enable Auto Update**.
3. Under **Upgrade Version**, select one of these options:
 - **Auto upgrade to production firmware**—With this option, you'll get the latest official firmware release.
 - **Auto upgrade to rc2 firmware**—With this option, you'll get the latest beta release.

AP Firmware Upgrade

☒ Enable Auto Update

Upgrade Version

☐ Auto upgrade to production firmware

☐ Auto upgrade to rc2 firmware

☐ Auto upgrade to custom firmware [Select Version](#)

Upgrade Schedule
(Scheduling for the first time must be done 2 hours prior to scheduled time)

Time of Day required Day of Week

2:00 am Day: Sunday

4. Under **Upgrade Schedule**, select the time and day when you want the upgrade to run.

Upgrade Schedule
(Scheduling for the first time must be done 2 hours prior to scheduled time)

Time of Day required Day of Week

2:00 AM

12:00 AM

12:30 AM

1:00 AM

Day: Sunday

NOTE: If you want this upgrade to run today (the same day that you're enabling this feature), set the Time of Day to at least 2 hours from now. For example, let's say it's currently Tuesday at 5 PM. If you set Day of Week to Tuesday and Time of Day to 7 PM, the upgrades will run tonight at 7 PM. However, if you set an earlier time, the upgrades will not run until *next* Tuesday.

5. Click **Save** near the top-right corner of the page.

Apply Specific Firmware to Specific Models

With this option, Juniper Mist will check the specified models in your AP inventory to see if they need to be upgraded to the firmware version that you specify.

To configure auto updates to apply specific firmware to specific models:

1. From the left menu of the Juniper Mist portal, select **Organization > Site Configuration**.
2. Under AP Firmware Upgrade, select the check box for **Enable Auto Update**.
3. Click **Auto upgrade to custom firmware**, and then click **Select Version**.

AP Firmware Upgrade

☒ Enable Auto Update

Upgrade Version

☐ Auto upgrade to production firmware

☐ Auto upgrade to rc2 firmware

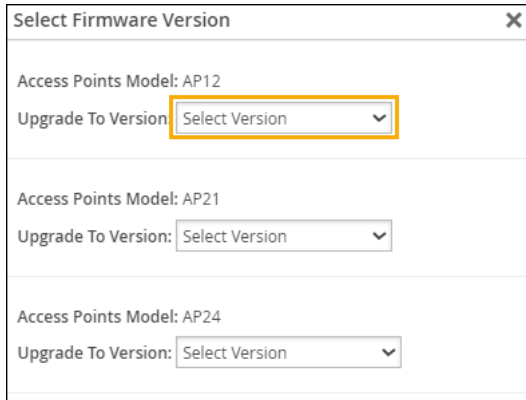
☒ Auto upgrade to custom firmware [Select Version](#)

Upgrade Schedule
(Scheduling for the first time must be done 2 hours prior to scheduled time)

Time of Day required

Day of Week

4. In the Select Firmware Version window, select the firmware version for each model that you want to auto-update.



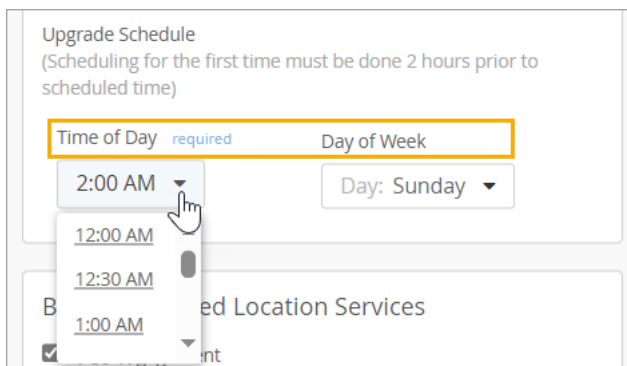
Select Firmware Version

Access Points Model: AP12
Upgrade To Version: Select Version

Access Points Model: AP21
Upgrade To Version: Select Version

Access Points Model: AP24
Upgrade To Version: Select Version

5. At the bottom of the Select Firmware Version window, click **Done**.
6. Under **Upgrade Schedule**, select the time and day when you want the upgrade to run.



Upgrade Schedule
(Scheduling for the first time must be done 2 hours prior to scheduled time)

Time of Day required Day of Week

2:00 AM
12:00 AM
12:30 AM
1:00 AM

Day: Sunday

NOTE: If you want this upgrade to run today (the same day that you're enabling this feature), set the Time of Day to at least 2 hours from now. For example, let's say it's currently Tuesday at 5 PM. If you set Day of Week to Tuesday and Time of Day to 7 PM, the upgrades will run tonight at 7 PM. However, if you set an earlier time, the upgrades will not run until *next* Tuesday.

7. Click **Save** near the top-right corner of the page.

Upgrade the Firmware on an AP Manually

You can select either a single AP or multiple APs for firmware upgrades.

NOTE: With the manual upgrade process, you can upgrade or downgrade the firmware on your AP. With the automatic upgrade process, you can only upgrade the firmware; you cannot downgrade the firmware.

To manually upgrade the AP firmware:

1. From the left menu of the Mist portal, select **Access Points**.
2. Select the APs that you want to update.
3. Click the **Upgrade APs** button in the top-right corner of the **Access Points** page.
The **Upgrade APs Firmware** page appears.
4. Select the firmware version to install.
5. Click **Start Upgrade**.

NOTE: If you try to manually upgrade a disconnected AP, the upgrade process starts only when the AP reconnects to the Juniper Mist cloud.

Peer-to-Peer AP Firmware Upgrade

You can use the peer-to-peer upgrade option if you need to upgrade many APs of the same model at a time. This option allows firmware image downloads directly from peer APs, instead of relying on a cloud download for every AP.

Mist randomly selects an AP as the seed AP, which downloads the firmware files from the cloud. The remaining APs then download the firmware files from the seed AP locally. You can upgrade a maximum of 10 APs using one seed AP. By limiting the cloud download to just one AP, you can decrease the time needed for upgrading multiple APs.

NOTE: You can use the peer-to-peer upgrade option only if you manually upgrade the firmware.

To upgrade the firmware using peer to peer upgrades:

1. Navigate to the Access Points page on the Mist portal.
2. Select the APs that you want to upgrade. Note that you'll need to select APs of the same model.
3. Click **Upgrade APs**.
4. In the Upgrade APs Firmware window, select the firmware version.
5. Select the **Upgrades using peer to peer communication** check box. Note that you'll see this check box only if you selected multiple APs of the same model.

Upgrade APs Firmware

Total Access Points selected to upgrade: 2

Access Point Model: AP45

Selected Access Points: LD_Conf2, LD_DataScience

Upgrade To Version: 0.12.27139 (rc1) ▼



Upgrades using peer to peer communication

6. Click **Upgrade**.

All the APs, except for the seed AP, reboot once the firmware upgrade is complete. The seed AP reboots only after all the other APs have rebooted.

Auto-Provisioning

To streamline onboarding and configuration, you can configure auto-provisioning for your access points (APs).

You can use auto-provisioning to:

- Automatically generate device names for your APs based on the LLDP ports that they're connected to.
- Assign device profiles to your APs based on the model, the device name, the DNS suffix, the LLDP system name, or the subnet that you connect the AP to.

- Assign APs to sites based on the model, the device name, the DNS suffix, the LLDP system name, or the subnet that you connect the AP to.

You can set up auto-provisioning on the Organization Settings page of the Juniper Mist™ portal. See [Auto-Provisioning](#).

Configuration

IN THIS SECTION

- [BLE Settings | 70](#)
- [Ethernet Settings | 72](#)
- [Enable PoE Passthrough | 75](#)
- [Configure IP Settings | 76](#)
- [Using APs in a Mesh | 79](#)
- [Enable Mesh | 86](#)
- [RTLS: AeroScout and Centrak | 86](#)
- [Enable RTLS Support | 87](#)
- [Using Electronic Shelf System \(ESL\) | 88](#)
- [Enable Electronic Shelf Labels | 89](#)
- [Enabling LEDs on the AP | 89](#)
- [Enable Geofencing | 90](#)
- [Data Rates | 91](#)
- [DSCP Mapping | 93](#)
- [Configure an AP for Survey Mode | 96](#)
- [Configure Your Access Points as IEEE 802.1X Supplicants | 99](#)
- [Enable Local Status Page | 108](#)
- [Revert AP Configuration Automatically | 108](#)

BLE Settings

Most Juniper APs have built-in virtual Bluetooth Low Energy (vBLE) capabilities that support location services. These APs are equipped with an internal 16-element vBLE antenna array that sends out eight directional beams. This setup allows for precise location accuracy within a range of 1 to 3 meters.

Figure 3: vBLE Antenna Array

Juniper's Dynamic vBLE Antenna

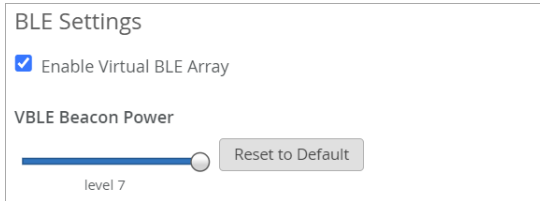


Even though BLE utilizes the 2.4 GHz frequency to communicate, the BLE signal does not conflict with the 2.4 GHz radio in the APs. When RRM is set to auto, Juniper Mist automatically chooses channels 1, 6, and 11 to avoid BLE interference. In addition, the BLE signal is only 2 MHz wide, and transmits on channels 37, 38, and 39 (advertising channels that are between the commonly used channels 1, 6, and 11).

You can use device profiles or the device-level configuration page of the AP to configure BLE settings:

- For multiple devices, you can use device profiles to enable or disable vBLE across all supported APs. You can also configure the beacon power, although this is rarely necessary. From the Mist portal,

select **Organization > Device Profiles**, click a device profile, and scroll down to the BLE Settings section.



BLE Settings

☒ Enable Virtual BLE Array

VBLE Beacon Power

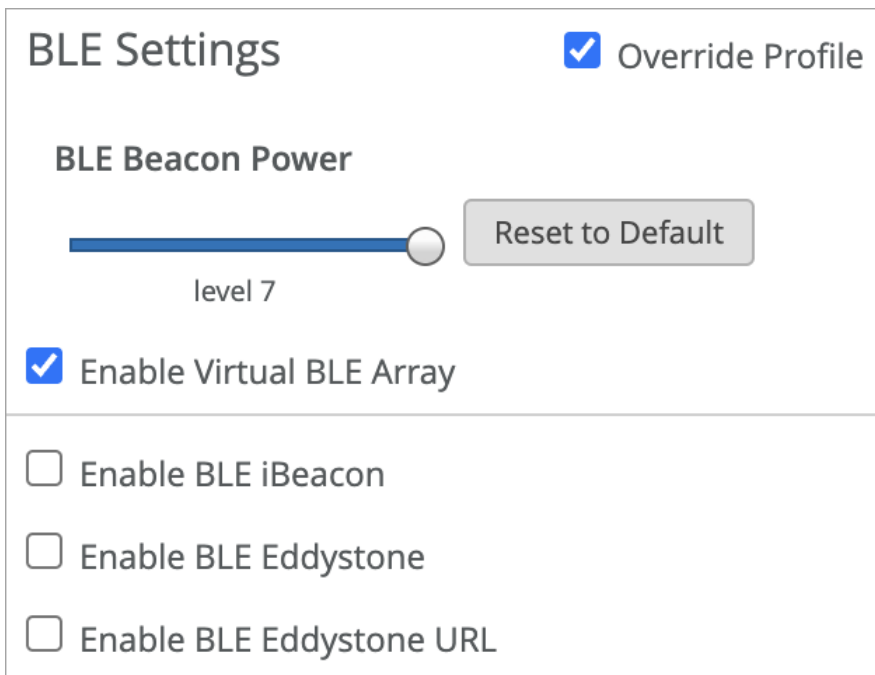
level 7

Reset to Default

- **Enable Virtual BLE Array**—Enable or disable vBLE for all APs associated with the device profile.
- **vBLE Beacon Power**—Use the configuration slider to adjust the vBLE signal range, which affects the accuracy of location services that rely on vBLE. Moving the slider allows you to fine-tune the range or level of detail provided by the vBLE-based location services.
 - Level 7 is higher power, and corresponds to +9 dBm or +12 dBm, depending on the AP model.
 - Level 1 is lower power, and corresponds to -8 dBm or -11dBm, depending on the AP model.

On the slider, dBm values for the different levels are more or less evenly distributed from high to low.

- Device settings for iBeacon, LE Eddystone, and Eddystone URL are available for additional customization and are configurable in the device-level configuration page of the AP. From the Access Points page, click an AP, and scroll down to the BLE Settings section.



BLE Settings

☒ Override Profile

BLE Beacon Power

level 7

Reset to Default

☒ Enable Virtual BLE Array

☐ Enable BLE iBeacon

☐ Enable BLE Eddystone

☐ Enable BLE Eddystone URL

RELATED DOCUMENTATION

<https://www.juniper.net/us/en/products/cloud-services/user-engagement.html>

<https://www.juniper.net/us/en/research-topics/what-is-virtual-bluetooth-le-vble-technology.html>

Ethernet Settings

The Ethernet ports on Juniper Mist Access Points (APs) generally require no extra configuration, especially for wireless-only use cases. The cloud automatically ensures the correct VLANs are plumbed to the AP Ethernet ports auto-learned from the configured WLANs.

The most common use case for modifying the AP's Ethernet port configurations is when you want to use the AP's secondary Ethernet interface(s) for connecting downstream wired devices to the AP.

You can configure AP-specific Ethernet settings. This includes wireless clients connecting through the AP. Alternatively, you can create a device profile with the desired configurations and apply them to a group of APs all at once. If there are conflicting configurations between the individual AP settings and the device profile, the individual settings will prevail unless you disable the Override Profile option on the AP configuration page.

Ethernet Properties

PoE Passthrough

☒ Enable ☐ Disable

Ethernet Port Configurations

☒ Enable ☐ Disable

Note: This will take over the automatically generated VLAN settings. Please ensure all necessary VLANs are specified on all ports.

Eth0

List of VLAN ID(s)

☐ Port VLAN ID (optional)

Eth1

☒ Enable interface ☐ Disable interface

List of VLAN ID(s)

☐ Port VLAN ID (optional)

Eth2

Note: This is only applicable for AP12

☒ Enable interface ☐ Disable interface

List of VLAN ID(s)

☐ Port VLAN ID (optional)

Eth3

Note: This is only applicable for AP12

☒ Enable interface ☐ Disable interface

List of VLAN ID(s)

☐ Port VLAN ID (optional)

Module

☒ Enable interface ☐ Disable interface

List of VLAN ID(s)

- **PoE Passthrough**—Many Juniper APs can act as power sourcing equipment (PSE), allowing them to provide Power over Ethernet (PoE) to devices connected to Eth1 on the AP. However, model-specific considerations may apply. You can enable this option to extend power from the AP to its *enabled* Ethernet ports.

NOTE: On both the AP41 and AP61, the module port provides PSE functionality. This allows for convenient power distribution to compatible devices.

- **Ethernet Port Configurations**—The VLAN settings configured here take precedence over those made in the **IP Address** section for VLAN ID, at both the device profile and individual AP level.
 - **Eth0 List of VLAN IDs**—Specify the VLANs that the AP can connect to through its Eth0 connection to the switch. Recall that Eth0 traffic is comprised of both AP management packets, and wireless client data packets. Use this configuration when you want to explicitly control the active VLANs on the AP switch port. For example, if you are adding extra VLANs for the wired ports on an AP12 that are not included in the WLAN VLANs.
 - **Port VLAN IDs**—This is the untagged VLAN on the port. Normally you should enter VLAN 1, unless you specify management VLAN in the IP Address section.
- **Eth1, Eth2, Eth3, and Module**—Enable or disable individual Ethernet ports on the AP, as available. Furthermore, you can specify any VLAN ID(s) required for the connection.
- **802.1X Supplicant**—Enable this option to support existing 802.1X authentication on the network that the AP is connecting to. The authentication method used is EAP-TLS. The APs must have firmware version 0.14 or later to utilize this feature.
- **Notes:**
 - For the RADIUS server to validate certificates presented by the Juniper APs, it needs to have a copy of the Mist organization certificate. You can get one from the **Organization > Settings** page.
 - To have the AP receive the supplicant configuration on its initial network connection, enable the **802.1x supplicant** option in the AP-level configuration rather than in a device profile.

The exact Power over Ethernet (PoE), Ethernet port specs, and other details can also vary according to the AP model. See below for links to AP datasheets and other model-specific considerations. Additionally, not all settings displayed on the screen will apply to every AP model. In such cases, the AP will simply ignore any unsupported settings.

RELATED DOCUMENTATION

Enable PoE Passthrough

Most Juniper APs can act as a Power Sourcing Equipment (PSE), allowing them to provide Power over Ethernet (PoE) to devices connected to Eth1 on the AP. However, model-specific considerations might apply. If you have supported devices that are connected to a PoE-enabled switch port, you can enable the PoE Passthrough option to extend power from the AP to the *enabled* Ethernet ports and/or the module port. For example, you can use the PoE Passthrough option to support daisy chaining of multiple BT11s. See [Daisy Chain BT11 Access Points](#).

To enable **PoE Passthrough** on APs attached to the device profile:

1. From the Mist portal, click **Organization > Device Profiles** and scroll down to the **Ethernet Properties** section.
2. Enable **PoE Passthrough**.

Ethernet Properties

PoE Passthrough
☒ Enable
☐ Disable

Ethernet Port Configurations
☐ Enable
☒ Disable

Eth1
☒ Enable interface
☐ Disable interface

Eth2

Note: This is only applicable for AP12

☒ Enable interface
☐ Disable interface

Eth3

Note: This is only applicable for AP12

☒ Enable interface
☐ Disable interface

Module
☒ Enable interface
☐ Disable interface

802.1X Supplicant
☐ Enable
☒ Disable

Download the Mist Certificate in [Organization Settings](#) for use by RADIUS servers to validate certificates presented by Mist APs.

3. Click **Save** in the upper right corner of the screen.

Configure IP Settings

Juniper Mist APs support both native and tagged VLANs, and for each Ethernet interface on the AP you can specify multiple VLAN IDs.

When powered on for the first time, Juniper Mist APs send a DHCP request through the Eth0 interface. The switch port connected to the AP must be a trunked port, or be configured with a native VLAN where VLAN ID is 1. This connection provides the path to the cloud, where you can configure the AP from the Juniper Mist portal.

When setting up Eth0 on the AP, you can use any VLAN you like. However, note that if it is misconfigured, the AP cannot connect to the network using the specified VLAN. If this process fails, you will have to do a factory reset on the AP to get back to VLAN=1.

If the AP cannot obtain an IP address, the LED will blink three times. See ["What Does the AP Status LED Indicate?" on page 367](#).

You can also assign a static IP address to the AP.

You can set up IP settings for each AP on the AP configuration page. Alternatively, you can use a device profile to configure these settings and apply them to multiple APs at once. If there are conflicting settings between the device profile and the individual AP settings, the AP will keep using its own settings until you choose to disable the Override Profile option on the individual AP configuration page.

To configure IP settings in a device profile:

1. From the Mist portal, click **Organization > Device Profiles**. Click a device profile and scroll down to the **IP address** section.
2. Configure the following:
 - **DHCP**—Select this option if you're using a DHCP service to assign IP addresses to the APs in the profile.
 - **Static**—Not configurable from the Organization > Device Profiles page. Use the AP configuration page instead.
 - **VLAN ID**— Specify the VLAN ID that the AP will connect to.
 - **MTU**—Enable this option to change the default MTU from 1500 to the value you specify. The AP uses this MTU with the switch.

← Device Profiles : **New Profile**

Name

Applies To

0 Access Points

WLAN Templates

APs associated with the Profile will inherit configuration from these Templates (if the AP is in a site to which the template applies)

Associate the profile with [WLAN Templates](#) in order to use their configuration

Mesh

☐ Enable mesh networking

IP Address

☒ DHCP ☐ Static

☐ VLAN ID (1 - 4094)

☐ MTU default

Ethernet Properties

PoE Passthrough

☐ Enable ☒ Disable

Ethernet Port Configurations

☐ Enable ☒ Disable

Eth1

☒ Enable interface ☐ Disable interface

3. Click **Save** in the upper right corner of the screen.
4. To verify whether the settings for an AP are being overridden at the individual level, click **Access Points** in the Mist menu and review the configurations for each AP in the device profile.

Using APs in a Mesh

IN THIS SECTION

- [Base and Relay APs | 79](#)
- [Requirements | 80](#)
- [Enabling Wireless Mesh in the Site Configuration | 80](#)
- [Use Case 1: Basic Configuration | 80](#)
- [Use Case 2: Connecting a Switch on a Relay AP | 82](#)

Using APs in a mesh simplifies wireless AP deployment and expands coverage. APs leverage neighboring APs to relay traffic to and from a base AP that is connected to the access switch. The interconnection between the APs is single, wireless hop, and occurs automatically after setup.

Base and Relay APs

In a mesh, APs are classified as a *base* or *relay*. A base has an Ethernet connection to a switch. Each relay can maintain mesh connections with up to four base APs. If a base AP goes offline, the relay APs can automatically failover to another base AP. In addition, you can create mesh groups so that a base AP will only accept failovers from relay APs that are members of a given group. You do this by assigning a Group ID, from 1 to 9, to the relay APs, and then configuring the base AP to only accept fail-over connections from relay APs with that group ID.

Before set up, you need to designate each AP in the mesh as either a base or relay. In addition, for the initial mesh set up, all the APs need to have a wired connection to the Mist cloud so they can receive the configuration. After that, you can disconnect wired links from the Relay APs.

To broadcast an SSID from a relay AP (but not from its base AP), specify the VLAN ID(s) in the SSID field of the Base AP on Eth0 or Eth1 port (not in a device profile or site configuration).

When both the relay AP and base AP are operating on the same 5 GHz frequency, the bandwidth on the base AP is shared between them. Although the bandwidth is shared, it has a minimal impact on the overall throughput.

If needed for a given use case, you can physically connect a switch to a Relay AP.

Requirements

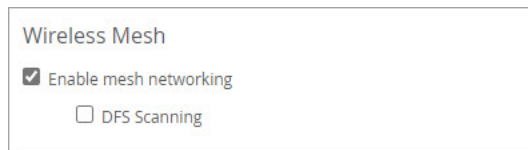
- AP41, AP61, and AP43 support mesh single hop with a base AP and up to 6 relay APs connected to the base AP via wireless mesh link.

You can use different models in the same mesh. Mesh is supported on the models listed below:

- AP41/AP41E
- AP61/AP61E
- AP32/AP32E/AP33
- AP43/AP43E
- AP63/AP63E
- AP Firmware—Mesh is supported on firmware version 0.8.18563 and later. All APs in a mesh should be running the same firmware version.

Enabling Wireless Mesh in the Site Configuration

First, enable wireless mesh networking on the **Organization > Site Configuration** page.

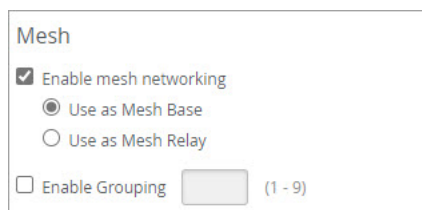


Wireless Mesh

☒ Enable mesh networking

☐ DFS Scanning

Next, enable wireless mesh networking in the AP configuration or the device profile.



Mesh

☒ Enable mesh networking

☒ Use as Mesh Base

☐ Use as Mesh Relay

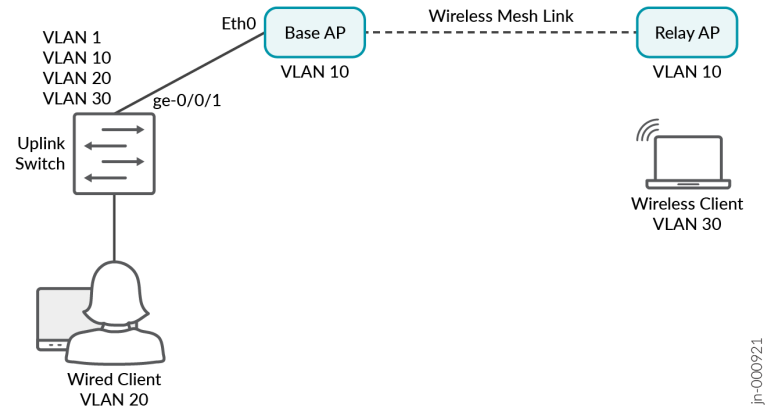
☐ Enable Grouping (1 - 9)

Use Case 1: Basic Configuration

In this use case, all the required VLANs in the network are being tagged in the SSIDs.

Topology

The uplink switch interface ge-0/0/1 has a wired connection to the base AP, which has a wireless mesh link to the Relay AP.



Requirements

- Uplink Switch VLANs (where Base AP gets connected) = 1,10,20,30
- Management Vlan (through which APs will get IP)= 10
- Wireless SSID B= tag with VLAN 30
- Wireless client should get IP address from VLAN 30.
- Both Base and Relay AP should get IP from management Vlan 10.

Port Configuration

Configure the uplink switch port as follows.

```
set interfaces ge-0/0/1 native-vlan-id 10
```

```
set interfaces ge-0/0/1 unit 0 family ethernet-switching interface-mode trunk vlan members [1,10,30]
```

Base AP Configuration

Mesh

☒ Enable mesh networking

☒ Use as Mesh Base

☐ Use as Mesh Relay

☒ Enable Grouping (1 - 9)

Ethernet Properties

Ethernet Port Configurations

☐ Enable ☒ Disable

Eth1

☒ Enable interface ☐ Disable interface

Relay AP Configuration

Mesh

☒ Enable mesh networking

☐ Use as Mesh Base

☒ Use as Mesh Relay

☒ Enable Grouping (1 - 9)

Ethernet Properties

PoE Passthrough

☐ Enable ☒ Disable

Ethernet Port Configurations

☐ Enable ☒ Disable

Eth1

☒ Enable interface ☐ Disable interface

WLAN Configuration

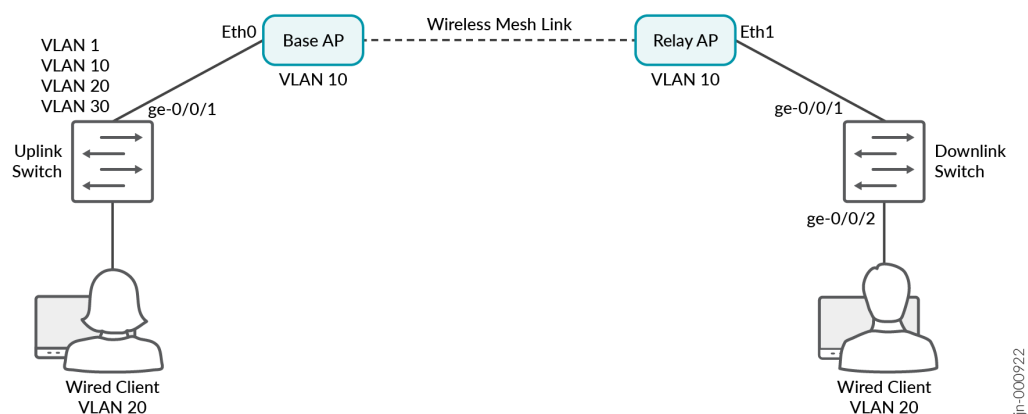
2 WLANS Site: Mist Wireless Add WLAN											
Filter	SSID	Enabled	Template	Band	Security	VLAN ID	WLAN Limit	Client Limit	Guest Portal	WLAN Labels	Applies to APs
	gateway	<input checked="" type="checkbox"/>	none	2.4GHz, 5GHz	Open Access		Unlimited / Unlimited	Unlimited / Unlimited	Disabled		All APs in Site
	v30_all	<input checked="" type="checkbox"/>	none	2.4GHz, 5GHz	Open Access	30	Unlimited / Unlimited	Unlimited / Unlimited	Disabled		All APs in Site

Use Case 2: Connecting a Switch on a Relay AP

In this scenario, we need to connect a switch on a Relay AP and configure a VLAN on a downlink switch that is not being tagged in the SSIDs.

Topology

The uplink switch interface ge-0/0/1 has a wired connection to the base AP, which has a wireless mesh link to the Relay AP. The Relay AP connects to a downlink switch on interface ge-0/0/1, and a PC on an access port configured with VLAN 20 connects over interface ge-0/0/2 on the downlink switch.



The configuration for this use case is similar to Use Case 1, but we also need to enable the Ethernet port configurations in order to pass vlan-id 20, which is not in the wireless network.

Requirements

- The Wired PC on the downlink switch should get its IP from VLAN 20.
- No wireless SSID is tagged on VLAN 20.
- Wireless clients get IPs on VLAN 30.
- Switches and APs get IPs on VLAN 10.

Uplink Switch Configuration

Configure the uplink switch port as follows.

```
set interfaces ge-0/0/1 native-vlan-id 10
```

```
set interfaces ge-0/0/1 unit 0 family ethernet-switching interface-mode trunk vlan members [1,10,20,30]
```

Downlink Switch Configuration

On the downlink switch, configure the two ports as follows.

- ge-0/0/1
 - *set interfaces ge-0/0/1 native-vlan-id 10*
 - *set interfaces ge-0/0/1 unit 0 family ethernet-switching interface-mode trunk vlan members [1,10,20,30]*
- ge-0/0/2

```
set interfaces ge-0/0/2 unit 0 family ethernet-switching interface-mode access vlan member 20
```

Base AP Configuration

Enable mesh, as in Use Case 1. Also enable Ethernet Port Configurations and enter the settings shown below.

Ethernet Properties

Ethernet Port Configurations

☒ Enable ☐ Disable

Note: This will take over the automatically generated VLAN settings. Please ensure all necessary VLANs are specified on all ports.

Eth0

full duplex, 1000 mbps, 0 (errors), 39 MB (bytes), 110.5 k (packets), 180.1 k (peak bps)

List of VLAN ID(s)

1,10,20,30

☒ Port VLAN ID (optional)

1

Eth1

☐ Enable interface ☒ Disable interface

no link

List of VLAN ID(s)

1,10,20,30

☒ Port VLAN ID (optional)

10

Mesh

List of VLAN ID(s)

1,10,20,30

☒ Port VLAN ID (optional)

10

Relay AP Configuration

Enable mesh, as in Use Case 1. Also enable Ethernet Port Configurations and enter the settings shown below.

Ethernet Properties

PoE Passthrough

☐ Enable ☒ Disable

Ethernet Port Configurations

☒ Enable ☐ Disable

Note: This will take over the automatically generated VLAN settings. Please ensure all necessary VLANs are specified on all ports.

Eth0

no link

List of VLAN ID(s)

1,10,20,30

☐ Port VLAN ID (optional)

Eth1

☒ Enable interface ☐ Disable interface

full duplex, 1000 mbps, 0 (errors), 5 MB (bytes), 29.1 k (packets), 19.9 k (peak bps)

List of VLAN ID(s)

1,10,20,30

☒ Port VLAN ID (optional)

10

Mesh

List of VLAN ID(s)

1,10,20,30

☒ Port VLAN ID (optional)

10

WLAN Configuration

WLANs

site: Mist Wireless

Add WLAN

Filter

<input type="checkbox"/>	SSID	Enabled	Template	Band	Security	VLAN ID	WLAN Limit	Client Limit	Guest Portal	WLAN Labels	Applies to APs	Forwarding
<input type="checkbox"/>	gateway	<input checked="" type="radio"/>	none	2.4GHz, 5GHz	Open Access		Unlimited / Unlimited	Unlimited / Unlimited	Disabled		All APs in Site	Disabled
<input type="checkbox"/>	v30_all	<input checked="" type="radio"/>	none	2.4GHz, 5GHz	Open Access	30	Unlimited / Unlimited	Unlimited / Unlimited	Disabled		All APs in Site	Disabled



Enable Mesh

Once you enable mesh at the site level in your organization, you can enable it in specific device profiles to target selected APs. When clients traverse a relay in the mesh, their authentication, access control, and VLAN assignments remain unaffected.

To broadcast an SSID only from a relay AP and not from its base AP, you can specify the VLAN ID(s) of the SSID on the Eth0 or Eth1 port of the base AP. This configuration is done directly on the AP itself, separate from the device profile or site configuration.

To simplify the setup of APs in a mesh, you can create separate device profiles for base APs and relay APs. This allows you to easily apply the appropriate profile to different groups of APs. Alternatively, you can designate APs individually on their respective configuration pages. This approach helps streamline the configuration process by focusing on the specific requirements of each AP type within the mesh.

To enable Mesh for APs attached to the device profile:

1. From the Mist portal, click **Organization > Device Profiles** and scroll down to the **Mesh** section.
2. Select **Enable mesh networking**.
3. Choose the role you want for the APs attached to the device profile, base or relay:
 - **Use as a Mesh Base** (AP must have a cable connection to the access switch).
 - **Use as a Mesh Relay** (AP will transit both client traffic, and management traffic, through a base AP).
4. Click **Enable Grouping** and enter a group number (1 through 9) to control which relay APs can fail-over to a given base AP.
5. Click **Save** in the upper right corner of the screen.

RTLS: AeroScout and Centrak

Juniper APs can support Real-Time Location System (RTLS), or asset tracking systems, including AeroScout and Centrak. These systems use Wi-Fi tags to send a proprietary beacon to the Juniper AP, which receives the signal and sends data to the RTLS.

More Information

In the AeroScout system, AeroScout tags are placed on assets in a monitored area. These tags periodically transmit a short Wi-Fi message, which is picked up by whatever Juniper APs are within range of the signal. The Juniper APs measure the Received Signal Strength Indication (RSSI) of the message and forward it, along with the RSSI data, to the AeroScout engine server. The RSSI information

is used to calculate the spatial location of the tagged asset relative to each of the Juniper APs that are forwarding the data.

Note that at least three Juniper APs need to receive the signal for good trilateration. In addition, the Juniper APs must be running supported firmware, and, of course, they must be configured to both listen for the signal and have a path back to the main RTLS system.

Enable RTLS Support

Juniper APs can support Real-Time Location System (RTLS) asset tracking, including AeroScout and Centrak. You can set this up individually on selected APs, or in a device profile, so that all supported APs attached to the device profile can inherit the settings.

To enable AeroScout on APs attached to the device profile:

1. From the Mist portal, click **Organization > Device Profiles** and scroll down to the **AeroScout & Centrak** section.
2. Select **Configure AeroScout**.
3. Complete the configuration with the following settings:
 - **Host**—The hostname or IP address of the AeroScout Location Engine, that is, the address to send SSID location reports
 - **Port**—For AeroScout, the default is TCP/IP 1144
 - **Wi-Fi Client Location**—Wi-Fi client location includes fields in addition to those sent for AeroScout tags. Two examples are client and radio type, and the client MAC address.
4. Click **Save** in the upper right corner of the screen.

To enable AeroScout on a given APs:

To configure AeroScout from the Mist UI, navigate to your **Access Points Details** page and provide a Host address in the **AeroScout** section. Make sure to select the **Configure AeroScout** checkbox as well.

1. From the Mist portal, click **Access Points** and then choose from the list that appears the APs you want to configure.
2. Scroll down the page to the **AeroScout & Centrak** section and then select **Configure AeroScout**.
3. Complete the configuration with the following settings:
 - **Host**—The hostname or IP address of the AeroScout Location Engine, that is, the address to send SSID location reports

- **Port**—For AeroScout, the default is 1144
- **Wi-Fi Client Location**—Wi-Fi client location includes fields in addition to those sent for AeroScout tags, for example client and radio type

4. Click **Save** in the upper right corner of the screen.

RELATED DOCUMENTATION

| [RTLS: AeroScout and Centrak](#) | 86

Using Electronic Shelf System (ESL)

The USB port on certain Juniper APs can be used to connect third-party USB dongles for an electronic shelf labels (ESL) system, which provides up-to-date product and pricing information about the shelf edge in real-time. The dongle uses Mist vBLE on the AP to establish a 2.4 GHz wireless connection with the ESL for periodic advertisement with response. Support is native on other models.

This connection is secure, follows standard protocols, and operates with very low power consumption. For V:Cloud, the APs communicate directly over a TLS tunnel – the data is transmitted between the V:Cloud and ESL tags by TLS tunnel and does not go through the Mist Cloud.

NOTE: The Juniper Mist APs and portal use TLS version 1.3 and AES_128_GCM for encryption and authentication.

As a general guideline, you can assume each AP can support from 7,000 to 15,000 ESL tags depending on the vendor and AP model.

To support ESL, you must be running AP firmware version 0.12x and later, with version 0.14x or 0.15x recommended. The APs must support IEEE 802.11ax:

- AP24, AP32, AP33, AP34, AP43, AP45

The following ESL systems are currently supported:

- SES-Imagotb v1 USB dongle
- SoluM USB dongle
- Hanshow USB dongle

Enable Electronic Shelf Labels

The USB port on some Mist AP models supports third-party USB dongles for use with an electronic shelf labels (ESL) system. After connecting the dongle to the USB, you can configure the port as described here.

- APs must be running firmware version 0.14x or 0.15x. And, depending on AP model, you need support for IEEE 802.3at or 802.3bt for PoE.
- We recommend that you disable the 2.4-GHz band and enable ["Dual Band Radio" on page 217](#).

To enable ESL for (already activated) APs attached to the device profile:

1. From the Mist portal, click **Organization > Device Profiles** and scroll down to the **Electronic Shelf Label Bridge** section.
2. Select **Configure ESL Bridge**.
3. Choose the ESL type you are using, **Native** or **2.4/HF**:
 - a. Choose **Native** if you are using a SES-Imagotag BLE.
 - b. Choose **2.4/HF** if your ESL connects via dongle.
4. Complete the configuration with the following settings:
 - **Host**
 - **Port**
 - **Override Channel**
 - **SSL Verification**
5. Click **Enable vBLE Array** under BLE settings (BLE must also be enabled in the site configuration).
6. Click **Save** in the upper right corner of the screen.

Enabling LEDs on the AP

LEDs on the Juniper AP provide operational status and help troubleshoot connectivity issues.

To ensure that the LED setting applied in the device profile takes effect when enabled, you need to enable the corresponding setting in the site configuration page for the parent site of the device profile as well:

Click **Organization > Site Configuration** (under Admin) and then scroll down to the **Access Point Settings** section.

- **Enable LEDs**—Enable or disable LEDs for all APs attached to the device profile.
- **LED Brightness**—Control LED brightness for all APs attached to the device profile.

Click **Save** in the upper-right corner when done.

For help decoding the LED blink pattern seen on the Juniper AP, see the following:

RELATED DOCUMENTATION

No Link Title

Enable Geofencing

Geofencing is when the AP prevents clients with an RSSI below a set level from connecting to the network, for example to keep users from outside your facility from using your wireless network. Existing clients are not dropped or blocked if their RSSI becomes poor.

Geofencing is available for the 2.4-GHz, 5-GHz, and 6-GHz radio bands. Note that for the 2.4-GHz and 5-GHz bands, the APs need to be running firmware version 0.8.x or later, and the 6-GHz radio band requires firmware version 0.12.x or later.

To enable geofencing on a WLAN:

1. From the Mist portal, select **Site > Wireless | WLAN** and click the **Add WLAN** button or select an existing WLAN from the list.
2. Scroll down the WLAN setting page to the **Geofence** section.

3. Select the radio band for which you want to enable a geofence, and then enter a value for minimum RSSI, for example -70 or -75.
4. Scroll to the top of the page and click **Save**.

After enabling geofencing for a given WLAN, you can apply it to any collection of APs you want using a device profile. Do this by including your SSID (WLAN) in a WLAN template and attaching that template to a device profile. Add APs to the device profile, and when you save the profile, the attached APs will inherit the geofence.

Data Rates

Disabling clients with lower data rates can improve WLAN performance in three ways:

- Increase throughput by ensuring clients are transmitting data only at higher rates.
- Encourage clients to roam, reducing the effects of a sticky client.
- Reduce management frame overhead by increasing the MBR.

You can also lower the AP transmit power for cell sizing purposes and to limit co-channel inference. In some cases, you might want to configure static channel and power settings instead of dynamic RF.

Rather than limiting data rates, a better option may be to use WiFi 6E, which disallows older generation Wi-Fi devices (slower, thus extensive airtime consumption) in the 6 GHz band. You can also enable dual band to automatically eliminate unnecessary 2.4 GHz radios. See ["Radio Management \(dual-band\)" on page 217](#).

For high-capacity WLANs, use 802.11n or 802.11ac frequency bands and select a high minimum data rate, such as 18 Mbps (disable legacy 802.11a/b/g APs).

Figure 4: Data Rates for Custom

No Legacy									
2.4Ghz Rate Setting					5GHz Rate Setting				
1	N/A	12	Optional		6	Basic			
2	N/A	18	Optional		9	Optional			
5.5	N/A	24	Optional		12	Basic			
6	Basic	36	Basic		18	Optional			
9	N/A	48	Optional						
11	N/A	54	Optional						
Compatible									
2.4GHz Rate Setting					5GHz Rate Setting				
1	Basic	12	Optional		6	Basic			
2	Basic	18	Optional		9	Optional			
5.5	Basic	24	Optional		12	Basic			
6	Optional	36	Optional		18	Optional			
9	Optional	48	Optional			HT +VHT			
11	Basic	54	Optional						
HT +VHT									
High Density									
2.4GHz Rate Setting					5GHz Rate Setting				
1	N/A	12	N/A		6	Optional			
2	N/A	18	N/A		9	Optional			
5.5	N/A	24	Basic		12	Optional			
6	N/A	36	Optional		18	Optional			
9	N/A	48	Optional						
11	N/A	54	Optional						
HT MCS3-7,11-15,19-23,27-31		VHT MCS3-9			HT MCS3-7,11-15,19-23,27-31				

DSCP Mapping

IN THIS SECTION

- [Wi-Fi Multimedia](#) | 93

Wi-Fi Multimedia

The Wi-Fi Multimedia (WMM) standard defines voice, video, best effort, and background access categories that can be given different performance priorities on the wireless network. To be effective, these priorities must then align with the QoS, or traffic prioritization, scheme configured for the wired network.

To bridge the two, Differentiated Service Code Point (DSCP) values provide a way to map WMM priorities to QoS treatments.

Juniper Mist APs will overwrite existing DSCP values of upstream traffic using its own Access Categories (AC) values. The original DSCP values are not retained.

The DSCP to AC mappings are given in the tables below.

Table 7: WMM Access Categories

0 (Background)	DSCP CS2 (0x40)
1 (Best Effort)	DCSP CS3 (0x60)
2 (Video)	DSCP CS4 (0x80)
3 (Voice)	DSCP CS7 (0xe0)

Table 8: DSCP to AC Mapping

DSCP 0	AC 1
DSCP 1	AC 1
DSCP 2	AC 1

DSCP 3	AC 1
DSCP 4	AC 1
DSCP 5	AC 1
DSCP 6	AC 1
DSCP 7	AC 1
DSCP 8	AC 1
DSCP 9	AC 1
DSCP 10	AC 1
DSCP 11	AC 1
DSCP 12	AC 1
DSCP 13	AC 1
DSCP 14	AC 1
DSCP 15	AC 1
DSCP 16	AC 1
DSCP 17	AC 1
DSCP 18	AC 1
DSCP 19	AC 1
DSCP 20	AC 1
DSCP 21	AC 1
DSCP 22	AC 1
DSCP 23	AC 1

DSCP 24	AC 1
DSCP 25	AC 1
DSCP 26	AC 1
DSCP 27	AC 1
DSCP 28	AC 1
DSCP 29	AC 1
DSCP 30	AC 1
DSCP 31	AC 1
DSCP 32	AC 2
DSCP 33	AC 2
DSCP 34	AC 2
DSCP 35	AC 2
DSCP 36	AC 2
DSCP 37	AC 2
DSCP 38	AC 2
DSCP 39	AC 2
DSCP 40	AC 2
DSCP 41	AC 2
DSCP 42	AC 2
DSCP 43	AC 2
DSCP 44	AC 2

DSCP 45	AC 2
DSCP 46	AC 2
DSCP 47	AC 2
DSCP 48	AC 3
DSCP 49	AC 3
DSCP 50	AC 3
DSCP 51	AC 3
DSCP 52	AC 3
DSCP 53	AC 3
DSCP 54	AC 3
DSCP 55	AC 3
DSCP 56	AC 3
DSCP 57	AC 3
DSCP 58	AC 3
DSCP 59	AC 3
DSCP 60	AC 3

Configure an AP for Survey Mode

You can configure your access point (AP) to support site surveys, which you perform to test wireless coverage before you deploy APs. During a site survey, you place an AP at different locations at the site to measure signal strength, throughput, signal interference, packet loss, and other key parameters. Site surveys help you to determine the number of APs required for your site and the placement of APs to provide optimal wireless coverage.

To configure your AP for use in survey mode:

1. Claim your AP and assign it to a site. See ["Claim a Juniper Access Point" on page 27](#) and ["Assign Access Points to Sites" on page 31](#).
2. Power on your AP. Ensure that the AP has connectivity to the Juniper Mist cloud so that the configurations can be pushed to the AP.
3. Ensure that AP configuration persistence is enabled and AP uplink monitoring is disabled:
 - a. From the left menu of the Juniper Mist portal, select **Organization > Site Configuration**. The Site Configuration page appears.
 - b. Click a site.
 - c. Scroll down to the AP Config Persistence section of the page and ensure that you've selected the **AP Config Persistence** check box. Additionally, ensure that you cleared the **AP Uplink Monitoring** check box in the AP Uplink Monitoring section.

The screenshot shows three configuration sections in the Juniper Mist portal:

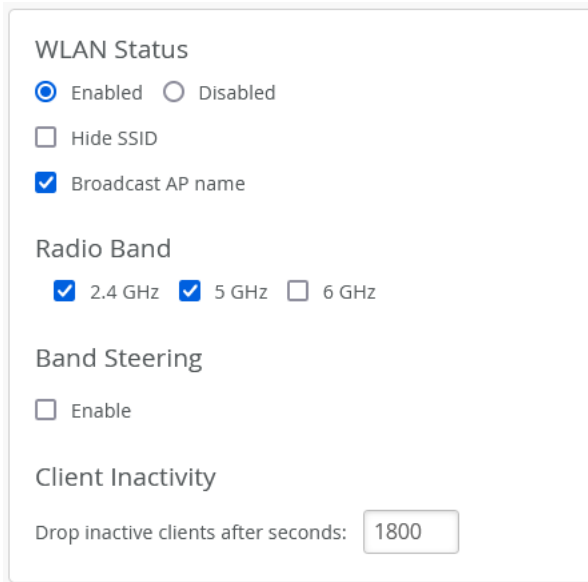
- AP Config Persistence:** The "Enable" checkbox is checked, with the description "Store on the AP its last known configuration".
- AP Uplink Monitoring:** The "Enable" checkbox is unchecked, with the description "Disable WLANs based on uplink monitoring".
- Juniper ATP:** The "Disabled" radio button is selected, with the "Enabled" radio button unselected.

The AP stores the complete configuration if AP configuration persistence is enabled for your site. When the AP is unable to connect to the Juniper Mist cloud, the AP can reboot from this stored configuration and continue to transmit beacons.

When AP uplink monitoring is enabled, the AP broadcasts the service set identifier (SSID) only if an Ethernet link is present. When you operate the AP in survey mode, you connect the AP only to a portable power source such as a Power over Ethernet (PoE) injector or a battery pack. Without a connection to a switch, the AP lacks an Ethernet link. You must disable AP uplink monitoring to ensure that in survey mode, the AP can broadcast the SSID.

4. Create a WLAN.
 - a. From the left menu of the Juniper Mist portal, select **Site > WLANs**. The WLANs page appears.

- b. Click **Add WLAN**.
- c. Configure the WLAN settings. See ["WLAN Options" on page 122](#).
- d. (Optional) Navigate to the WLAN Status section and enable **Broadcast AP name**. This setting enables you to view the name of the AP in third-party Wi-Fi tools.



The image shows a configuration panel titled "WLAN Status". It contains several settings:

- WLAN Status:** Two radio buttons, "Enabled" (selected) and "Disabled".
- Hide SSID:** An unchecked checkbox.
- Broadcast AP name:** A checked checkbox.
- Radio Band:** Three checkboxes, "2.4 GHz" (checked), "5 GHz" (checked), and "6 GHz" (unchecked).
- Band Steering:** An unchecked checkbox labeled "Enable".
- Client Inactivity:** A section with a label "Drop inactive clients after seconds:" followed by a text input field containing the value "1800".

- e. Click **Create**.
5. Configure the power and channel settings for your AP:
- a. From the left menu of the Juniper Mist portal, select **Access Points**.
The Access Points page appears.
 - b. Click an AP.
 - c. Configure the power and channel settings for your AP.
 - d. Click **Save**.

Now, your AP will start beaconing a WLAN at your desired channel and power. As AP Config Persistence is enabled, you can remove cloud connectivity on the AP. The AP continues to beacon even after it reboots. You can use this AP to perform site surveys. You can move the AP around the site and measure its received signal strength indicator (RSSI) by using third-party site survey tools such as Ekahau AI Pro, NetAlly AirMagnet, iBWave, and Hamina Onsite.

Configure Your Access Points as IEEE 802.1X Supplicants

SUMMARY

For added security, use this feature to block traffic to an access point until its credentials are verified.

IN THIS SECTION

- [Deployment Considerations | 99](#)
- [Enable Auto-Update to Version 0.14.x or Higher | 100](#)
- [Enable 802.1X in the Switch Port Profile | 100](#)
- [Assigning VLANs via RADIUS \(If Applicable\) | 104](#)
- [Enable the 802.1X Supplicant Option in the Device Profile | 105](#)
- [Apply the Device Profile to Your APs | 106](#)
- [Import Your Certificate to Your RADIUS Server | 107](#)

Juniper Mist APs can authenticate to their uplink wired switch by using IEEE 802.1X authentication. When 802.1X authentication is implemented, the switch blocks traffic to the AP at the port until its credentials are presented and matched on the authentication server (a RADIUS server). When the AP is authenticated, the switch stops blocking traffic.

To get the 802.1X supplicant feature working on your Juniper Mist™ APs, ensure that the APs have the required firmware, enable 802.1X the switch port profile and the device profile, and add the Juniper Mist CA certificate to your RADIUS server.

Deployment Considerations

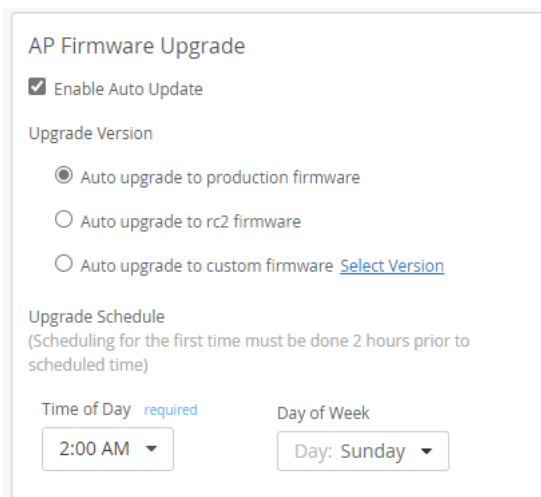
The preferred method to deploy your Juniper Mist APs with 802.1X at the edge is to leverage a guest VLAN on the switch side. With a guest VLAN that is completely locked down, except for access to the Mist cloud, the AP can connect to the cloud, receive its configuration, and download the correct AP firmware version (if required). Once it has the supplicant configuration, the AP will attempt to authenticate to the network.

Requirements: AP firmware version 0.14.x or higher is required. To ensure that all APs meet this requirement, the processes below include enabling auto-upgrade in the site settings. This way, all APs automatically get the required firmware to support this feature.

Enable Auto-Update to Version 0.14.x or Higher

802.1X is supported in Juniper Mist AP firmware version 0.14.x or higher. To ensure that all APs meet this requirement, enable auto-upgrade in the site settings. This way, all APs automatically get the required firmware to support this feature.

1. From the left menu of the Juniper Mist portal, select **Organization > Admin | Site Configuration**.
2. Select a site to open the Site Configuration page.
3. Under AP Firmware Upgrade, select **Enable Auto Update**.
4. Under Upgrade Version, select **Auto upgrade for production firmware** to get the latest firmware.



AP Firmware Upgrade

☒ Enable Auto Update

Upgrade Version

☒ Auto upgrade to production firmware

☐ Auto upgrade to rc2 firmware

☐ Auto upgrade to custom firmware [Select Version](#)

Upgrade Schedule
(Scheduling for the first time must be done 2 hours prior to scheduled time)

Time of Day required

Day of Week

5. Select the **Time of Day** and **Day of Week** when you want the auto-upgrade to run.
Allow at least 2 hours for the new settings to take effect. For example, if you are configuring these settings at 2 PM and you want to update your APs today, set the time to 4 PM or later.
6. Click **Save** near the top-right corner of the Site Configuration page.

Enable 802.1X in the Switch Port Profile

On your switch, enable 802.1X authentication for the ports that your APs connect to. We recommend using a Guest VLAN, server reject VLAN, or MAC auth fallback with a default VLAN that allows AP connectivity to the Mist Cloud, at least for initial deployment of the site. This way, APs can safely connect to the cloud to receive the initial configuration and AP firmware.

To configure 802.1X in the Port Profile:

1. Select **Organization > Switch Templates**, and then click the switch template that you want to configure.
2. In the **Authentication Servers** section, add your RADIUS servers.

< Switch Templates : **branch_template**

INFO
Name

APPLIES TO SITES
1 sites 2 switches **Assign to Sites**

All Switches Configuration

AUTHENTICATION SERVERS

Authentication Servers

Authentication Servers
No servers defined
[Add Server](#)

Timeout: (0 - 1000 seconds)

NTP
NTP Servers

xxx.xxx.xxx.xxx or {{siteVar}}.xxx.xxx (comma-separated Hostnames / IPs)

DNS SETTINGS
DNS Servers

CLI CONFIGURATION
Additional CLI Commands ⓘ

OSPF AREAS
No areas defined

3. In the **Shared Elements** section, enable 802.1X and either MAC Authentication or Guest Network.
 - 802.1X with MAC Authentication—With this option, your RADIUS server has full visibility and control. When an AP connects, the switch performs MAC authentication. RADIUS should return a default/unknown device VLAN with access to the Mist Cloud. Then the AP connects to the cloud, downloads firmware if necessary, and receives the supplicant configuration. Next, the AP requests RADIUS authentication. When the AP is authenticated, the switch places the AP in the specified VLAN(s).

PORT PROFILES

Port configuration for a set of related ports

★ System defined

New Port Profile ✓ ✕

Name

new-profile

Port Enabled

☒ Enabled ☐ Disabled

Description

Add Description

Mode

☐ Trunk ☒ Access

Port Network (Untagged/Native VLAN)

default 1 ✓

VoIP Network

None ✓

☒ Use dot1x authentication

☒ Mac authentication

☐ Mac authentication only

Authentication Protocol

None ✓

☐ Use Guest Network

- **802.1X with Guest Network**—With this method, you use a Guest VLAN to provide limited access to new APs until they connect to the Mist cloud and get their configuration. When an AP connects, it is placed on the Guest VLAN. Then it connects to cloud, downloads firmware if necessary, and receives the supplicant configuration. Next, the AP requests RADIUS authentication. When the AP is authenticated, the switch places the AP in the specified VLAN(s).

PORT PROFILES

Port configuration for a set of related ports

★ System defined

New Port Profile

Name

new-profile

Port Enabled

☒ Enabled
 ☐ Disabled

Description

Add Description

Mode

☐ Trunk
 ☒ Access

Port Network (Untagged/Native VLAN)

default 1

VoIP Network

None

☒ Use dot1x authentication
☐ Mac authentication
☒ Use Guest Network

NOTE: Also identify the VLAN in the port profile so that the APs are assigned to the desired VLAN(s). Alternatively, assign VLANs via RADIUS. See ["Assigning VLANs via RADIUS \(If Applicable\)"](#) on page 104.

4. Apply the Port Profile to the ports where you'll connect the APs.

You can apply the profiles by using **Dynamic Port Configuration** or by editing the port configuration in the **Select Switches Configuration** section.

DYNAMIC PORT CONFIGURATION

Apply port profiles to ports based on properties of connected clients. First matching rule will be applied. Port range must have dynamic configuration enabled.

New Rule

Check

RADIUS Filter-ID

☐ Select the 2nd segment (separated by)

☐ Start at character offset 0 (0 = first character)

If text starts with

mist-ap

comma-separated values

Apply Configuration Profile

AP

default(1), trunk, edge

☐ Do not reset to default profile when link is down

NOTE: For help configuring a Juniper Mist switch template, see the [Juniper Mist Wired Assurance Configuration Guide](#).

Assigning VLANs via RADIUS (If Applicable)

If you use Mist Edge and tunnel all of your WLANs, then likely an AP connecting to a switch port configured as access will suffice. However if you don't use Mist Edge, or have WLANs local traffic breakout, then you probably need the switch port to be a trunk. Most switch operating systems allow you to return multiple VLANs from RADIUS.

For Junos, you can either return multiple Egress-VLANID or Egress-VLAN-Name.

Example for Egress-VLAN-Name:

- 1 = tagged
- 2 = untagged
- vlan-2 and vlan-3 are the VLAN names on the switch

In the example below, VLAN 1vlan-2 is tagged, and VLAN 2vlan-3 is untagged:

```
001094001144 Cleartext-Password := "001094001144"  
    Tunnel-Type = VLAN,  
    Tunnel-Medium-Type = IEEE-802,  
    Egress-VLAN-Name += 1vlan-2,  
    Egress-VLAN-Name += 2vlan-3,
```

NOTE: For help with configuration, see your Junos OS documentation.

Enable the 802.1X Supplicant Option in the Device Profile

To quickly configure multiple APs at once, set up a device profile with this feature enabled. You'll then apply the device profile to the APs. When the AP connects to the cloud for the first time, it will receive the supplicant configuration straight away.

1. Select **Organization > Device Profiles** from the left menu of the Juniper Mist portal.
2. Click an existing profile or click **Create Profile**.
3. In the **Ethernet Properties** section of the Device Profile, find the **802.1X Supplicant** option, and click **Enable**.

< Device Profiles : **New Profile**

Name

Applies To

0 Access Points

WLAN Templates

APs associated with the Profile will inherit configuration from these Templates (if the AP is in a site to which the template applies)

Associate the profile with WLAN Templates in order to use their configuration

LEDs

☒ Use Site Setting

Electronic Shelf Label Bridge

☐ Configure ESL Bridge

AeroScout & CenTrak

☐ Configure AeroScout

☐ Configure CenTrak

Mesh

☐ Enable mesh networking

IP Address

☒ DHCP ☐ Static

☐ VLAN ID (1 - 4094)

☐ MTU default

Ethernet Properties

PoE Passthrough

☐ Enable ☒ Disable

Ethernet Port Configurations

☐ Enable ☒ Disable

Eth1

☒ Enable interface ☐ Disable interface

Eth2

Note: This is only applicable for AP12

☒ Enable interface ☐ Disable interface

Eth3

Note: This is only applicable for AP12

☒ Enable interface ☐ Disable interface

Module

☒ Enable interface ☐ Disable interface

802.1X Supplicant

☒ Enable ☐ Disable

Download the Mist Certificate in Organization Settings for use by RADIUS servers to validate certificates presented by Mist APs.

2.4 GHz Settings ☐ Override Site Setting

2.4 GHz band configured by site settings

5 GHz Settings ☐ Override Site Setting

5 GHz band configured by site settings

6 GHz Settings ☐ Override Site Setting

6 GHz band configured by site settings

Dual Band Radio Settings ☐ Override Site Setting

Device Profile Variables

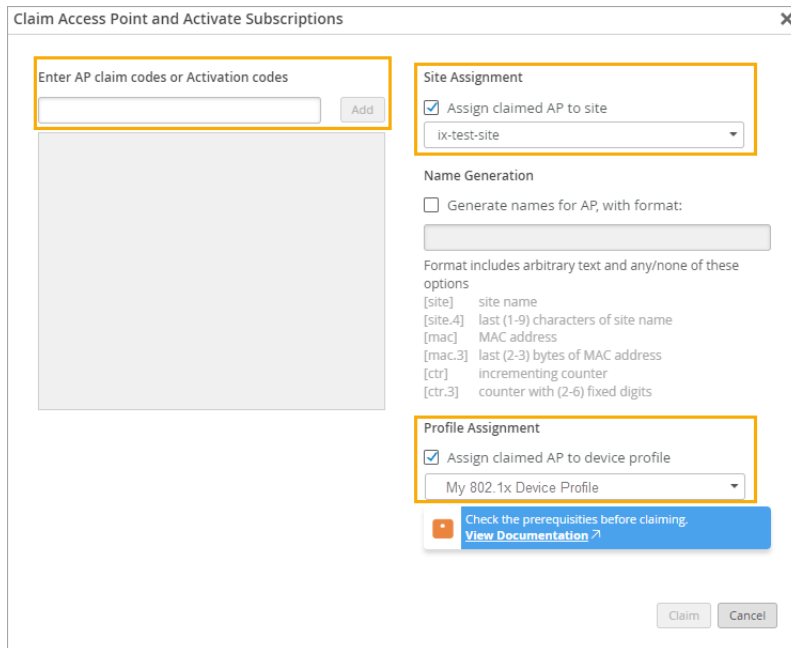
Variables	Values

4. Configure any other desired settings for this device profile.
5. Click **Save** near the top-right corner of the Device Profile page.

Apply the Device Profile to Your APs

When you claim your APs into your organization, apply the device profile and identify the site. This way, when you bring your APs online, they'll get the firmware through the auto-upgrade settings in the site configuration, and they'll get the AP configuration from the device profile.

1. Select **Access Points** from the left menu of the Juniper Mist portal.
2. Click **Claim APs** at the top-right corner of the Access Points page.
3. In the pop-up window, enter the activation codes or claim codes, select the site, and select the device profile.



Claim Access Point and Activate Subscriptions

Enter AP claim codes or Activation codes

Site Assignment

☒ Assign claimed AP to site

Name Generation

☐ Generate names for AP, with format:

Format includes arbitrary text and any/none of these options

[site] site name

[site.4] last (1-9) characters of site name

[mac] MAC address

[mac.3] last (2-3) bytes of MAC address

[ctr] incrementing counter

[ctr.3] counter with (2-6) fixed digits

Profile Assignment

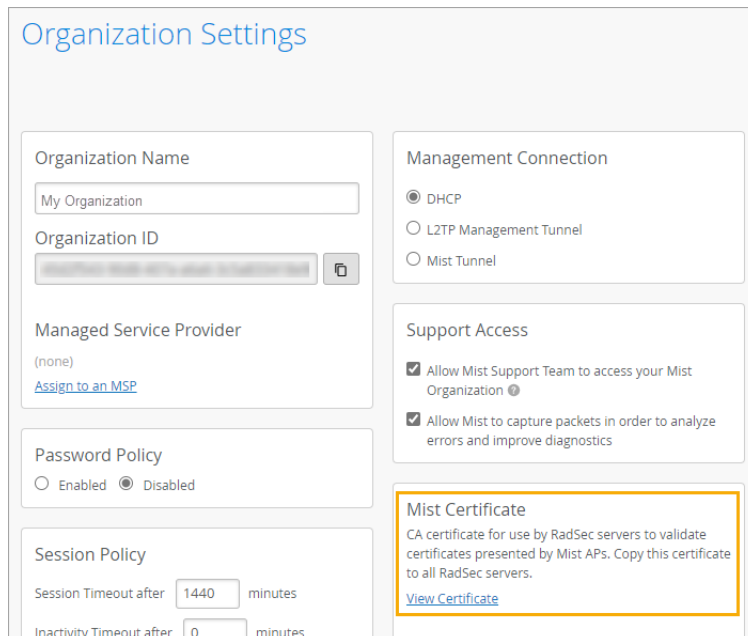
☒ Assign claimed AP to device profile

4. Click **Claim**.

Import Your Certificate to Your RADIUS Server

Juniper Mist generates a unique CA certificate for your organization. You need to import this certificate to your RADIUS server so that the server can authenticate your APs.

You can find your **Mist Certificate** on the **Organization > Settings** page.



Organization Settings

Organization Name

Organization ID

Managed Service Provider

(none)

[Assign to an MSP](#)

Password Policy

☐ Enabled ☒ Disabled

Session Policy

Session Timeout after minutes

Inactivity Timeout after minutes

Management Connection

☒ DHCP

☐ L2TP Management Tunnel

☐ Mist Tunnel

Support Access

☒ Allow Mist Support Team to access your Mist Organization

☒ Allow Mist to capture packets in order to analyze errors and improve diagnostics

Mist Certificate

CA certificate for use by RadSec servers to validate certificates presented by Mist APs. Copy this certificate to all RadSec servers.

[View Certificate](#)

Enable Local Status Page

You can configure a local status page for all APs at your site. Clients can use this local status page to view information about the AP to which the client is connected along with the details of the client. This information is useful during troubleshooting. Clients connecting to any of the WLANs on the site can access the local status page from a web browser.

Here is an example of a local status page:



NOTE: If you configured a local status page for your site, all the APs at the site will obtain their own IP address for the Management VLAN. The APs will also obtain an address for each of the VLANs configured on the AP. You'll need to consider this aspect during DHCP planning.

To set up a local status page:

1. From the left menu of the Juniper Mist™ portal, select **Organization > Site Configuration**.
2. Scroll down to the Access Point Settings section and select the **Enable Local Status Page** check box.
3. Enter the hostname. You can enter any name as long as it is not an existing hostname such as `www.google.com` or `www.juniper.net`.
Clients connected to a WLAN can enter the hostname in a browser to view the local status page.
4. Click **Save** in the top-right corner of the Site Configuration page.

Revert AP Configuration Automatically

You can configure the APs at a site to automatically revert to their last working configuration if the APs lose connectivity to the cloud. APs can get disconnected from the cloud due to various reasons such as Internet issues or configuration issues.

NOTE: You can configure this feature only on APs running firmware version 0.7.x or newer.

To enable the AP to revert to the last working configuration:

1. From the left menu of the Juniper Mist™ portal, select **Organization > Site Configuration**.
2. Scroll down to the Access Point Settings section and select the **Automatically Revert Configuration** check box.

Access Point Settings

☐ Enable Local Status Page

☒ Automatically Revert Configuration

!

 Auto-revert requires firmware v0.7.x or higher

(In case AP disconnects from cloud after configuration change, automatically revert to last working configuration)

☐ Enable LEDs

3. Click **Save** in the top-right corner of the Site Configuration page.

Device Profiles

IN THIS SECTION

- [Device Profiles | 110](#)
- [Device Profile Options | 111](#)
- [Create a Device Profile | 113](#)

Device Profiles

You use device profiles like a template, where you configure and save a set of AP settings so they can be reused on other APs within a site. For example, say you are planning a large deployment of APs in a campus or retail location and you need a variety of AP configurations to support the different AP roles. To cover all the scenarios you need, you can create multiple device profiles, such as one for IoT devices, another for high-density environments, and another to restrict access to one or more specified WLANs.

When you associate APs with a given device profile, the APs will automatically inherit the settings defined in that profile. You can use the same method for onboarding new APs – assign the APs to a device profile when you claim them to have them configured when they come online.

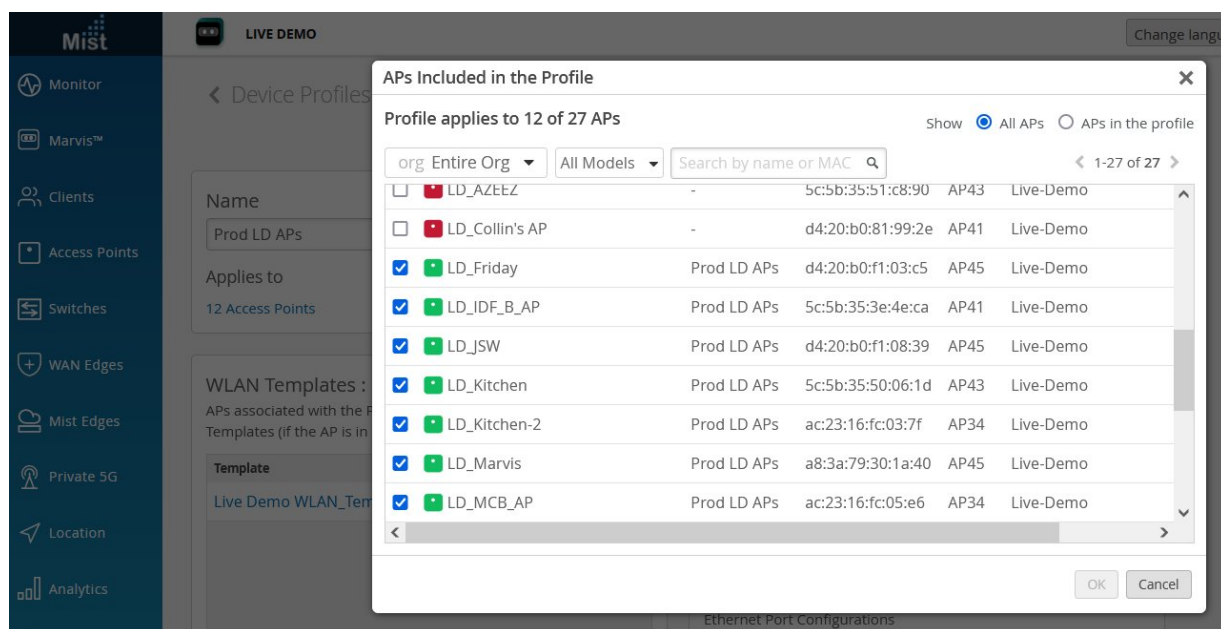
Name	APs	Templates	WLANs
AX APs			
BostonHQ			
Goddard-Remote-AP		UK-WFH-Edge-Demo	UK-WFH-PSK
Manual-Dual-5-GHz			
Outdoor APs			
Prod LD APs	12	Live Demo WLAN_Template_DO_NOT_DELETE	Live_demo_do_not_remove, Mist_IoT, Live_de
WD-TEST-APs			
Wired-Auth			

You can have settings from a device profile override settings made on the individual APs, or, conversely, you can have the AP-level settings take precedence over those of the profile. The same is true for settings made at the site level.

When you add or remove a Juniper AP from a device profile, the change takes effect immediately. However if you change a configuration setting in the device profile, you need to push the change to the

Juniper APs manually, by clicking the **Optimize Now** button in the Radio Management page. You can also wait a few minutes for the change to occur automatically.

Configurations available through device profiles include radio frequency, 802.1x security, VLAN connections, and Ethernet port settings. You can also attach one or more WLAN Templates to the profile, which has the effect of extending those settings (such as WLANs and/or user access policies) to all APs in the device profile.



Device Profile Options

To access the Device Profiles page, select **Organization > Device Profiles** from the left menu of the Juniper Mist™ portal.

Table 9: Device Profile Options

Option	Default	Summary
"WLAN Options" on page 122	none	Defines WLAN characteristics such as SSID, the authentication protocol, radio band availability, and Guest portal availability. Also defines user-access policies and support for tunneling wireless client traffic to third-party devices.

Table 9: Device Profile Options *(Continued)*

Option	Default	Summary
"LEDs" on page 89	not enabled	Enables or disables LEDs for all APs attached to the device profile. You can also set the brightness of the LED.
"Electronic Shelf Label Bridge" on page 88	none	Defines settings for the USB port on the AP for interoperability with third-party electronic shelf labels (ESL) system dongles.
"AeroScout & Centrak" on page 86	none	Defines settings for interoperability with third-party Real-Time Location System (RTLS), or asset tracking systems, including AeroScout and Centrak.
"Mesh" on page 79	not enabled	Defines whether the AP is a relay or base for use in mesh networks.
"IP Settings" on page 76	DHCP	Defines how the AP and clients get an IP address: manually (static) or automatically from a DHCP server.
"Ethernet Properties" on page 72	not enabled	Defines PoE and VLAN settings for the Ethernet ports on the AP.
"BLE Settings" on page 70	not enabled	Enables or disables vBLE for location services on Juniper APs. Also adjusts beacon power.
"2.4 GHz, 5 GHz, 6 GHz Radio Band Settings" on page 207	Inherit from Site	Defines whether the Juniper AP should use the 2.4 GHz, 5 GHz, and/or 6 GHz radio band settings configured for the site (default) or the device-level radio band settings configured on the AP. At the device-level, you can enable/disable a given radio band, set radio power levels, and control which channels are used.
"Dual Band Radio Settings" on page 217	Auto	Enables/disables 5 GHz on dual-band AP radios. By default, the AP radios operate on 2.4 GHz and 5 GHz. When only 5 GHz is enabled on a dual-band AP, both radios can operate on the 5 GHz.

Table 9: Device Profile Options (*Continued*)

Option	Default	Summary
"Device Profile Variables" on page 114	none	Defines variables in the device profile so you can customize the WLAN setup for different groups of APs while keeping a common configuration base. You can create variables for SSIDs, passphrases, VLAN, bands and the AAA server.

Create a Device Profile

Use device profiles as you would a template to define and apply a common set of AP configurations to APs in the same site.

To assign a device profile to a domain:

1. Click **Organization > Device Profiles** in the Mist portal. The **Device Profiles** screen appears.
2. Click **Create Profile** to start a new profile. Or, to edit an existing profile, select it from the list.
To save time, you can clone an existing profile and make modifications to the copy.
3. Give the profile a name.
4. Under **Applies To**, click the link to select the APs you want to attach the profile to.
 - Use the search box to find APs by model type or MAC address in the site or organization.
 - To see a list of APs currently included in the profile, select **APs in the profile**.
 - If no APs appear in the list, you most likely need to adopt or claim them from your Access Point Inventory. In the Mist menu, click **Access Points** and then click the **Inventory** button in the upper-right corner of the screen to show and claim an AP.
5. Click **OK** to attach the device profile to the APs you've selected.
6. Fill out the remaining configuration choices on the page as needed.
 - See [Device Profile Options on page 111](#) for an explanation of the settings and associated tasks.
7. Click **Save** at the top of the screen when you are done.

Variables in Device Profiles

Use variables in a device profile to customize the WLAN settings for a particular group of APs while maintaining a common configuration for the rest. Just like in other parts of the Mist portal, you use the `{{name}}`, *value* format to create variables. These variables can then be used in a WLAN configuration.

In a device profile, the most commonly used variables are for SSIDs, passphrases, VLAN IDs, and naming schemes.

Syntax and Rules for Variables

- Variables must be enclosed in double curly braces, for example `{{variable}}`, and `{{guest2_VLAN_id1}}`.
- Except for underscores, don't use spaces or special characters.
- Upper case is OK.
- Numbers are OK.
- Use double brackets `{{variable}}` to define the variable name.

After defining variables in the device profile, you include them in the WLAN configuration and then add that to the WLAN template. You then attach the WLAN template to a given device profile, and in this way it is possible to both scale your configuration, while at the same time having AP-specific settings that vary according to the WLAN.

In cases where you have multiple variables, WLANs, and device profiles configured for a site, it can be hard to figure out exactly which variable values are being applied in a given WLAN. For this, using the Juniper Mist API to show the actual, applied configuration is preferable to checking **Site > WLANs** to see the variables for a given WLAN. Documentation for the Mist API is available once you log on to the Juniper Mist portal: <https://api.mist.com/api/v1/docs/Home>.

Access Point FAQ

IN THIS SECTION

- [How much power do Juniper Mist APs need? | 115](#)
- [What are the mounting options for Juniper APs? | 115](#)
- [How long does it take for an AP to boot and be operational? | 115](#)

- How do I apply specific RF settings to the APs across all my sites? | 116
- What are the antenna gains for each model AP? | 116
- Can I configure an AP so that it reboots successfully even if it can't connect to the Mist cloud? | 116
- Which types of configuration changes reset the AP radios? | 116
- How do I reset an AP? | 116
- What is the recommended length of the Ethernet cable for powering up and connecting the Mist APs to cloud? | 117
- Can I run an Ethernet cable longer than 100 meters long while putting an Ethernet (PoE+) extender in the path? | 117
- What do the different AP firmware tags mean? | 117

How much power do Juniper Mist APs need?

For information about the PoE and wattage requirements for each AP model, see ["PoE Requirements for Juniper Mist APs" on page 21](#).

What are the mounting options for Juniper APs?

For mounting instructions, see the deployment guide for the AP model. Deployment guides are listed in [Juniper Mist Supported Hardware](#).

How long does it take for an AP to boot and be operational?

After you connect your AP to power, wait a few minutes for it to boot completely. For detailed instructions about connecting an AP, see the deployment guide for the AP model. Deployment guides are listed in [Juniper Mist Supported Hardware](#).

How do I apply specific RF settings to the APs across all my sites?

Use RF templates to update radio configurations for specific AP models across all sites. Set up different templates to apply model-specific settings to cover your use cases. For example, enable or disable radio bands, manage channel width, set transmission power, and configure AP antenna gain. For more information, see ["Radio Settings \(RF Templates\)" on page 213](#).

What are the antenna gains for each model AP?

For information about the antenna gain, see the datasheet for each AP model. Datasheets are listed in [Juniper Mist Supported Hardware](#).

Can I configure an AP so that it reboots successfully even if it can't connect to the Mist cloud?

By default, an AP only keeps critical information such as the Static IP (if used). In the event of a power failure, the AP needs to talk to the Mist cloud to come back up. However, if you enable configuration persistence, then the AP will remember its full configuration and can come back up without an internet connection. For help enabling configuration persistence, see ["Enable Configuration Persistence" on page 32](#).

Which types of configuration changes reset the AP radios?

Some configuration changes require the affected access points (APs) to restart in order to apply the new settings. During this time, clients will be deauthenticated on the AP and thus disconnected from the WLAN for the minute or two it takes to restart. For a full list of these configuration changes, see ["WLAN Changes That Reset The Radio" on page 223](#).

How do I reset an AP?

For help resetting an AP to its factory default settings, see ["Reset an Access Point to the Factory-Default Configuration" on page 401](#).

What is the recommended length of the Ethernet cable for powering up and connecting the Mist APs to cloud?

We usually recommend a max length of 100 meters for the Ethernet cable between the AP and the switch port to guarantee proper function.

Can I run an Ethernet cable longer than 100 meters long while putting an Ethernet (PoE+) extender in the path?

A PoE extender is not the same as an Ethernet transceiver. With the power extender, the AP may power on but the Ethernet link will not be transmitting over such long cable. In this case, you might be getting 2 yellow blinks on the AP which indicates the AP is unable to receive Ethernet link from the switch.

What do the different AP firmware tags mean?

When looking at lists of available firmware, you'll see various tags such as production, rc2, and rc1. For help interpreting these tags, see ["Firmware Version Tags for Juniper Mist Access Points" on page 60](#).

3

CHAPTER

WLANs and WLAN Templates

[Configure a WLAN Template | 119](#)

[Add a WLAN to a Site or a WLAN Template | 121](#)

[WLAN Options | 122](#)

[Tips for Wi-Fi 6E \(Video\) | 131](#)

[Add a Bonjour Gateway to a WLAN | 132](#)

[Labels | 135](#)

[Using Labels in a WxLAN Policy | 139](#)

[Configure a Third-Party Tunnel | 141](#)

[Enable Wireless Bridging Mode | 142](#)

Configure a WLAN Template

In the Juniper Mist portal, wireless LANs (WLANs) are modular elements that contain the security and other configuration settings for a service set identifier (SSID). A WLAN template is a collection of WLANs, access policies, and tunneling policies that you can use to streamline WLAN configuration and management at the organizational level.

WLAN templates are modular and can be attached different sites or device profiles. In this way, you can mix and match whichever permutation of WLAN, site, and APs you need to cover all the use cases in your organization. Your wireless clients will only see the SSIDs you want them to see.

NOTE: For a discussion of Juniper Mist templates and profiles, see ["Templates and Device Profiles"](#) on page 203.

When working with WLAN templates, it's generally best to create them after you've set up your sites, either before or after claiming the APs. To keep things clear in the Mist portal, it helps to give the WLAN template the same name as the WLAN/SSID (which is what the clients will see). The idea behind all this is that once all your sites, WLANs, WLAN templates, and device profiles have been created, it will then be easy to make the associations.

The screenshot displays the Juniper Mist portal interface for configuring a WLAN template. The sidebar on the left contains navigation icons for Monitor, Marvis, Clients, Access Points, Switches, WAN Edges, Mist Edges, Private 5G, Location, Analytics, Site, and Organization. The main content area is titled 'WLAN Templates :: Live Demo WLAN_Template' and includes a 'Delete' button and 'Clone', 'Save', and 'Cancel' buttons. The configuration section is divided into several fields:

- Name:** A text field containing 'Live Demo WLAN_Template'.
- Applies to:** A section with tabs for 'Entire Org.' and 'Sites and Site Groups'. Under 'Sites and Site Groups', there is a list containing 'Live-Demo' with a plus icon to add more.
- Except for these sites (exceptions):** A section with a list containing 'Remote Users' with a plus icon to add more.
- Limited to APs in profiles:** A checkbox that is checked, with a list containing 'Prod LD APs' and a plus icon to add more.

On the right side, there is a table titled 'WLANs' with an 'Add WLAN' button. The table has columns for SSID, Band, VLAN ID, and Security. The data rows are as follows:

SSID	Band	VLAN ID	Security
Live_demo_do_not_remove	5GHz, 6GHz		WPA3/SAE (+WPA2)
Mist_IoT	5GHz	24	WPA2/PSK (multicast)
Live_demo_only	5GHz, 6GHz		WPA3/SAE (+WPA2)
Guest Wi-Fi	5GHz	2	WPA2/PSK
Live_demo_6G	6GHz		WPA3/SAE

For each template, you can select which APs to include, that is, which APs will broadcast the SSID. If the settings in a given WLAN or WLAN template conflict with those specified for a given AP, or with those applied elsewhere to the site as a whole, you will be prompted to select which setting should take precedence.

Watch the video below for a quick overview.



Video: [Create a WLAN](#)

To create a WLAN template:

1. From the left menu of the Juniper Mist portal, select **Organization > Wireless | WLAN Templates**.
2. Click **Create Template** at the top-right corner of the WLAN Templates page.
3. In the New Template window, enter a **Template Name**, and then click **Create**.

The name will appear in the WLAN Template list. It's generally most convenient to use the same name as the SSID, although it can be unique.

4. Add at least one WLAN:
 - a. Click **Add WLAN**.
 - b. At minimum, enter an **SSID** name, select a **Security Type**, and set up VLAN(s).
 - c. Enter other settings, as needed.

NOTE:

["WLAN Options" on page 122](#)

- d. Click **Create** at the bottom of the Create WLAN window.
Juniper Mist generates a WLAN ID. Anytime that you need to look up this ID or edit your WLAN settings, simply click the WLAN in the WLAN list.
- e. If needed, repeat these steps to add more WLANs to this template.
5. Specify the scope for this template by completing one or more of these sections:
 - **Applies to**—If you complete this section, the template is available only to the sites and site groups that you specify here. Click the add icon (+), and then select an option from the list. Repeat as needed to add more sites and site groups.
 - **Except for**—If you complete this section, the template is available to all sites except those that you specify here. Click the add icon (+), and then select an option from the list. Repeat as needed to add more sites.
 - **Limited to**—If you complete this section, the template is available only to APs with the device profiles that you specify here.

6. As needed, define user access policies and/or support third-party tunnels.

For help, see:

- ["WxLAN Access Policies" on page 329](#)
- ["Configure a Third-Party Tunnel" on page 141](#)

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

Add a WLAN to a Site or a WLAN Template

You can create a site-level WLAN or add a WLAN to an organization-level WLAN template.

To add a WLAN to a site or WLAN template:

1. Start from the organization level or site level as described below.
 - For an organization-level WLAN (in a WLAN template), select **Organization > Wireless | WLAN Templates**, then ["create a WLAN template" on page 119](#) or select an existing template. To add a WLAN to your template, click **Add WLAN**.
 - For a site-level WLAN, select **Site > Wireless | WLANs**, and then click **Add WLAN**.
2. At minimum, enter an **SSID** name, select a **Security Type**, and set up VLAN(s).
3. Enter other settings, as needed.

NOTE:

["WLAN Options" on page 122](#)

4. Click **Create** at the bottom of the Create WLAN window.

Juniper Mist generates a WLAN ID. Anytime that you need to look up this ID or edit your WLAN settings, simply click the WLAN in the WLAN list.

NOTE: If you're working at the organization level (WLAN template), save the template. For help, see ["Configure a WLAN Template" on page 119](#).

WLAN Options

IN THIS SECTION

- [Navigating to the WLAN Settings Window | 122](#)
- [WLAN Configuration Settings | 122](#)

Navigating to the WLAN Settings Window

- For a WLAN in a WLAN template, select **Organization > Wireless | WLAN Templates** from the left menu, then ["create a WLAN template" on page 119](#) or select an existing template. To add a WLAN to your template, click **Add WLAN**. To edit an existing WLAN in the WLANs list, click it.
- For a site-level WLAN, select **Site > Wireless | WLANs** from the left menu, and then click **Add WLAN**. To edit an existing WLAN on the WLANs page, click it.

WLAN Configuration Settings

Table 11: WLAN Settings

Setting	Summary
SSID	<p>This is the name the WLAN will broadcast for clients to see.</p> <p>While you can configure as many as 15 service set identifiers (SSIDs) per radio, a good rule of thumb for device profiles and WLAN templates is to use only two or three WLANs per AP. The idea is to minimize the airtime overhead incurred by beacon management frames, which are sent every 102.4 ms per radio, at the Minimum Basic Rate (MBR). In other words, unless you are carefully considering data rates and co-channel contention in order to achieve four, six, or even eight active WLANs on an AP, we recommend two or three WLANs per AP max.</p>
WLAN Status	<p>Use this to set whether an AP broadcasts the WLAN. You can also hide the SSID, and broadcast the AP by name.</p>

Table 11: WLAN Settings (*Continued*)

Setting	Summary
Radio Band	<p>Choose which radio frequencies to broadcast on the WLAN: 2.4 GHz, 5 GHz, or 6 GHz. Wireless clients typically experience better performance when connected to the 5-GHz band rather than the 2.4-GHz band because the 5-GHz band has more channels, and so less co-channel contention. The 6-GHz band has still more channels, wider channel, more advanced security options, and greater data rates.</p> <p>See "Radio Management " on page 204, "Radio Management (page)" on page 207, and "Radio Settings (RF Templates)" on page 213.</p>
Band Steering	<p>Available when multiple radio bands are selected. Band steering detects whether a connected client has dual-band (2.4 GHz and 5 GHz) capabilities. This option steers clients with dual-band capability to join the 5-GHz band if the signal is good. Both the 2.4-GHz and 5-GHz radios need to be enabled on the WLAN. Band steering is disabled by default.</p> <p>Note that even with band steering, clients can still hear beacon frames from the 2.4-GHz radios and can sometimes connect to these radios.</p> <p>See "Radio Management (dual-band)" on page 217 and "Dual Band Usage Examples" on page 219.</p>
Client Inactivity	<p>You configure an inactivity timer on your WLAN to prevent congestion. The AP deauthenticates inactive clients, as defined by the time you set here. The default time is 1800 seconds.</p>
Geofence	<p>Geofencing can prevent clients with a received signal strength indicator (RSSI) below a specified level from joining the network. You can set a minimum client RSSI, per radio band, to prevent clients who are beyond a given distance or range from joining the WLAN. Geofencing applies only to the initial association. Therefore, if a client is already associate with the network, the client will not be dissociated if its RSSI value falls below the configured threshold. The default is disabled for all radio-bands.</p> <p>See "Enable Geofencing" on page 90.</p>

Table 11: WLAN Settings (*Continued*)

Setting	Summary
Data Rates	<p>Set data rates to prevent clients with slow connections from degrading the overall WLAN performance.</p> <p>The default is Compatible, which allows all connections. The other options are:</p> <ul style="list-style-type: none"> • No Legacy (2.4G, no 11b)—Prevents 802.11b and 802.11g devices from joining the WLAN. This option has the effect of adding capacity to the network. • High Density (disable all lower rates)—Prevents 802.11b and 802.11g clients from joining the network if they don't meet a minimum signal level. • Custom Rates—See "Data Rates" on page 91.
Wi-Fi Protocols	You use this option to enable or disable Wi-Fi 6 on the supported APs.
WLAN Rate Limit	You use this option to configure a WLAN rate limit to enforce an uplink and downlink rate for the WLAN. You can configure rate limits per AP, per client, and per application. You can also limit the total bandwidth allocation for a given application. Note, however that rate limiting bandwidth per client is often self-defeating, as it can have the effect of increasing the clients airtime consumption (by prolonging downloads).
Per-Client Rate Limit	Set the uplink and downlink rate per client.
Application Rate Limit	This option limits the uplink or downlink rate per client for the specified application. You must identify applications by their name or hostname.
Apply to Access Points	Select the APs you want this WLAN to apply to: All, Specific, or according to the AP label.

Table 11: WLAN Settings (Continued)

Setting	Summary
Security Types	<ul style="list-style-type: none"> • WPA3 using Enterprise (802.1X)—RADIUS-based authentication. With this security type, you also can enable additional options: <ul style="list-style-type: none"> • WPA3+WPA2 Transition—Transition modes can help ease adoption to WPA3 and OWE by offering existing security types. For more information, see "Considerations for 6 GHz Wireless" on page 425. • 192-bit Encryption—This option offers the highest level of 802.1X security in Wi-Fi by offering GCMP-256 encryption over the air and requiring more secure certificates. • WPA3 with Personal (SAE)—Passphrase-based authentication. You can configure a single passphrase or multiple passphrases. • WPA2 using Enterprise (802.1X)—RADIUS-based authentication. • WPA2 with Personal (PSK)—Wi-Fi Protected Access (WPA) 2 using a standard preshared key (PSK). You can configure a single passphrase or multiple passphrases. • Opportunistic Wireless Encryption (OWE)—You can configure WPA3/OWE transition modes on 6 GHz multiband SSIDs, in order to allow for easier adoption of transition mode SSIDs. For more information, see "Considerations for 6 GHz Wireless" on page 425. • Open Access—Unencrypted, typically used for guest networks.
Other Security Options	<ul style="list-style-type: none"> • MAC address authentication by using RADIUS lookup—A MAC address is presented to a RADIUS server to authorize the device. Unavailable with certain security types. • Prevent banned clients from associating—This option prevents clients that have been ban on the Network Security page from associating with this WLAN. • Fast Roaming— A security method based on 802.11r for authenticating new clients.

Table 11: WLAN Settings (*Continued*)

Setting	Summary
VLAN	<ul style="list-style-type: none"> • Untagged—Doesn't use VLANs; this is the default setting. • Tagged—Select this option if you have static VLANs on the network. In the field that appears, enter the VLAN ID. Make sure that the switch port connected to the access point (AP) also uses a tagged VLAN. • Pool—Select this option to assign wireless clients a randomly selected IP address from one of the VLANs listed in the pool. When using this for PSK-based network segmentation, specify all the VLAN IDs you will need for the VLAN ID field of the PSK (Organization > WLAN Templates > Pre-Shared Key > Add Key button, and then VLAN ID). Alternatively, to put clients in different VLANs according to their site, use a site variable for the Pools VLANs and leave the VLAN ID field blank in the PSK configuration page. • Dynamic—Select this option to connect wireless users to a given VLAN, as configured in the RADIUS server.
Isolation	<p>Peer-to-peer isolation prevents Layer 2 peer traffic on the same WLAN, AP, or wired or wireless subnet. This option is disabled by default. (For Layer 3 filtering, you can create WxLAN policies.)</p> <p>Subnet isolation requires firmware version 0.12 or later, and clients must have a DHCP address.</p>

Table 11: WLAN Settings (*Continued*)

Setting	Summary
Filtering (Wireless) <ul style="list-style-type: none"> • ARP • Broadcast/Multicast <ul style="list-style-type: none"> • Allow mDNS • Allow SSDP • Allow IPv6 Neighbor Discovery • Ignore Broadcast SSID Probe Requests 	<p>These filters reduce the amount of management frames sent by APs in the WLAN. Filtering can significantly improve performance by freeing up radio air time which is otherwise consumed as a routine part of the operational overhead.</p> <ul style="list-style-type: none"> • The ARP filter prevents Address Resolution Protocol (ARP) broadcast requests to a given WLAN interface. If not enabled, the proxy ARP will try to resolve all unknown Ethernet address requests by flooding the request to any unfiltered interfaces. We recommend leaving the ARP filter enabled. (By default, Mist APs support proxy ARPs, which means the AP sends an ARP response on behalf of the client instead of forwarding the packet over the air.) • The Broadcast / Multicast filter prevents the AP from propagating broadcast and multicast frames on the wireless network. It filters IPv6 broadcasts, multicast, and IPv4/IPv6 mDNS frames, although these can be individually exempted. DHCP broadcasts are not included in this filter. <ul style="list-style-type: none"> • Allow mDNS frames by exempting this traffic from being filtered when broadcast/multicast filtering is selected. mDNS is needed for Apple Bonjour for network discovery. • Allow Simple Service Discovery Protocol (SSDP) advertisement beacons by exempting this traffic being filtered when broadcast/multicast filtering is selected. SSDP is needed Universal Plug and Play (UPnP) device discovery. • Allow IPv6 Neighbor Discovery frames by exempting this traffic when broadcast/multicast filtering is selected. • The AP can Ignore Broadcast SSID Probe Requests from wireless clients, that is, not send a probe response (which advertises its SSID, supported data rates, and other 802.11 capabilities).

Table 11: WLAN Settings (*Continued*)

Setting	Summary
Custom Forwarding	<p>By default, the WLAN forwards tagged or untagged client traffic through the primary Ethernet port, Eth0. You use custom forwarding in conjunction with Mist Edge, or for example, to ensure that guest and corporate traffic use different networks.</p> <ul style="list-style-type: none"> • Eth0 + PoE—Default. Forward traffic out the Eth0 port. • Eth1—Forwards traffic through the second Ethernet port of the AP. This mode requires the WLAN VLAN to be untagged. You must connect Port Eth1 to a physically separate LAN.
SSID Scheduling	<p>You use this option to have the WLAN broadcast the SSID only on certain days and times. When scheduled to be disabled, the AP will not broadcast the SSID (that is, the SSID will not be visible to clients searching for available networks). The change in broadcast status does not reset the radio or disable the AP.</p> <p>SSID scheduling supports multiple time ranges for each day. By default this mode is disabled.</p>
802.1X Web Redirect	<p>Applies to VLANs with security type Enterprise (802.1X).</p> <p>Select the Enabled check box to redirect a client to a particular web page (for example, a quarantined portal for compliance checks) after it completes the 802.1X authentication. For this feature to work, your firmware version must be 0.7 or newer. For more information, see "Configure an 802.1X WLAN to Redirect Clients to Specific Web Pages" on page 242.</p>

Table 11: WLAN Settings *(Continued)*

Setting	Summary
QoS Priority	<p>Use quality of service (QoS) to prioritize traffic so that the more important traffic does not get held up in a queue during congestion. Juniper APs can prioritize wireless traffic to optimize the shared radio for maximum application performance.</p> <ul style="list-style-type: none"> • 0=Background (not used by Juniper APs) • 1=Best Effort • 2=Video • 3=Voice <p>Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance specification based on the IEEE 802.11e wireless QoS standard to support traffic prioritization. This specification uses the following access categories to prioritize transmission:</p>
Multimedia Extensions	<p>When multiple concurrent applications compete for network resources, Juniper APs can use MMEs to define and improve the wireless signal quality and performance.</p> <p>Multimedia extensions (MMEs) are architectural extensions to general-purpose processors to boost the performance of multimedia workloads. Throughput is not guaranteed by WMM.</p>
AirWatch	<p>AirWatch™ is 3rd-party mobile device management system. When this setting is enabled, the APs allow traffic to pass only for those clients already identified in the AirWatch console. If enabled, you need to specify the AirWatch console URL, the API key, and your login credentials for the managed devices.</p>

Table 11: WLAN Settings (*Continued*)

Setting	Summary
Bonjour Gateway	<p>Default is not configured. Configure this setting on a per WLAN basis, from either the WLAN configuration page or WLAN Templates. This feature automatically enables broadcast/multicast filtering. As such, be sure to select the option to allow mDNS frames.</p> <p>The following services are available, but must explicitly enabled to be discoverable:</p> <ul style="list-style-type: none"> • AirDrop, AirPlay, AirPrint, Apple HomeKit • Amazon Devices, GoogleCast, Roku, Spotify Connect • NFS, Scanner, SleepProxy (Wake-On-Network) <p>See "Add a Bonjour Gateway to a WLAN" on page 132.</p>
Security	<p>Supports WPA3, WPA2, Legacy, OWE, and Open Access, with either Enterprise (802.1X) and Personal (SAE), as well as single or multiple passphrases, TKIP, etc.</p> <p>See:</p> <ul style="list-style-type: none"> • "Enable WPA2/WPA3 Enterprise (802.1X) Security on a WLAN" on page 235 • "Rogues, Honeypots, and Neighbor APs" on page 310 • "Classify and Ban Designated Wireless Clients" on page 317 • "Preshared Keys" on page 265 • "Multi-Preshared Keys" on page 269

Table 11: WLAN Settings (*Continued*)

Setting	Summary
Fast Roaming	<p>Enable fast roaming to allow clients that are connected to the network using WPA2 or WPA3 security to remain connected as they roam between APs. With fast roaming, WPA2 and WPA3 clients do not need to re-authenticate with the authentication server every time they change APs in the same network.</p> <ul style="list-style-type: none"> • Default—Local PMKID caching only; there is no sharing of the PMKID between Mist APs on the network. This may be appropriate for some use cases, but does not scale. • .11r—Standards-based method of fast roaming, described in 802.11r. <p>See also: "Enable Fast Roaming" on page 232.</p>
VLAN	<p>Required for each WLAN. Specify the type of VLAN the AP will use in the switch connection.</p> <ul style="list-style-type: none"> • Untagged—Doesn't use VLANs; this is the default setting. • Tagged—Use with static VLANs on the network (the switch port connected to the AP must also use tagged VLAN). • Pool—Use to assign wireless clients a randomly selected IP address from one of the VLANs listed in the pool. • Dynamic—Use to connect wireless users to a given VLAN, as configured in the RADIUS server. <p>For information about using VLAN Pools with Pre-Shared Keys for segmentation, see "Leveraging Roles in a PSK (Use Case)" on page 275.</p>
Guest Portal	<p>You can enable guest access by creating a sign-in portal in Juniper Mist, using your own external portal, or enabling Single Sign-On. For more information, see "WLAN Guest Portal" on page 0 .</p>

Tips for Wi-Fi 6E (Video)

Wes Purvis, Juniper Mist product management director, describes what we've learned after a full year with large-scale Wi-Fi 6E deployments (May 2023 presentation).



Video:

Topics include:

- SSID Strategy
- Migrating to WPA3 Enterprise, WPA3 Personal, or OWE
- 6 GHz Roaming
- 6 GHz Resources

Add a Bonjour Gateway to a WLAN

Bonjour is a standards-based protocol from Apple that provides a way for devices and services on the same network to discover one another. It works by forwarding multicast Domain Name System (mDNS) frames to clients on the LAN so they can automatically discover and connect to the advertised service (such as a printer or AirPlay device).

On wireless networks, however, it is common for clients and the various services to connect to the same WLAN from different VLANs. As such, to use the Bonjour services, it becomes necessary to bridge mDNS frames originating on one VLAN to wireless clients connected on another VLAN. You do this by setting up a Bonjour gateway on the WLAN. The gateway can bridge local VLANs on the WLAN, as discussed in this topic, as well as by tunneling through a Mist Edge, which will require the assistance of Juniper technical support.

Figure 5: Adding a Bonjour Gateway

Bonjour Gateway

! Bonjour requires firmware v0.8.x or higher

☒ Enabled ☐ Disabled

Services [Add Custom Service](#)

Amazon Devices ? ✓ ×

Discoverable on the same Site ?

☐ Restricted to RADIUS group Floorplan ?

Discovery VLANs AP ?

20,30,{{prime}},210

= 20,30,{{prime}},210

VLAN IDs must be numeric values from 1-4094 or variable enclosed in {{*}}. Please enter comma separated values.

In Mist, the Bonjour gateway receives discovery queries from eligible clients (as explained below) on the Wi-Fi network, and forwards them to VLANs listed in the Discovery VLANs field of the gateway configuration. These VLANs can be part of the WLAN, or a part of the wired infrastructure. Responses from any Bonjour device on the network (that is, the WLAN, a wireless VLAN, or a wired VLAN) are forwarded (unicast) to the requesting client and added to the local cache. In this way, the gateway learns and builds a list of all users and devices that need to discover each other.

Access Control

When setting up a Bonjour gateway, you can also employ access control so a given Bonjour service is only discoverable for the specified user roles or locations. For example, for a classroom setting, you could leverage existing RADIUS roles for students and teachers to have screen casting in the Apple AirPlay service available only to teachers. You also use location-based access control to achieve similar results. For example, you can use your site floor plan when setting set up wireless printer service on the gateway in a way that ensures the printers are only discoverable by users who are on the same floor.

Custom Bonjour Services

Bonjour service labels use syntax such as the following: **airplay._tcp._local**. If you need to add a service that is not already on the list, you add your own custom service by providing the service-name portion of the label, for example, **homeconnect** in the **Add Custom Service** option. The rest of the label (the **._tcp._local** part) will be appended automatically to that name.

Role-based Bonjour Discovery

Role-based access lets you limit Bonjour service discovery within a WLAN to specified user role(s). It requires a RADIUS server for providing users' authentication, authorization, and accounting (AAA) profile, and Mist user labels in order to map those attributes so they can be used in the Mist policy framework. The result is that you can use labels to filter out non-matching users so they cannot discover the selected Bonjour service, while at the same time it is available to authorized users. See ["Use Case: Labels for a Bonjour Gateway" on page 136](#).

Best Practices

Juniper recommends that you filter (that is, drop) most broadcast and multicast frames on the wireless network so APs don't waste airtime in sending them. By default, this filtering includes mDNS frames when Bonjour is enabled.

Design your WLAN to minimize the volume of protocol chatter. Both SSDP (for plug-n-play devices) and mDNS can be very chatty protocols. As such, they can quickly degrade wireless performance by flooding the channel and consuming airtime. The design principles below can help reduce the chatter:

- Define a flood boundary for the Bonjour gateway.
- Pool Bonjour devices to use the minimal number of discovery VLANs.
- Use location or role-based service discovery.

- Test on the small scale before deploying in the network, especially before using custom Bonjour applications.
- Enable broadcast and multicast filtering on the wireless network.

To add a Bonjour gateway to a WLAN:

1. Navigate to the WLAN.

NOTE:

- If the WLAN is in a WLAN template, select **Organization > Wireless | WLAN Templates**, click the template, and then click the WLAN.
- For a site-level WLAN, select **Site > Wireless | WLANs**, and then click the WLAN.

2. In the Bonjour gateway section, select **Enabled**.
3. From the list of services that appears, select the one(s) you are making discoverable, or click **Add Custom Service** to define your own.
4. Click a Bonjour service, and if you want to limit its discoverability by proximity to the Mist AP, select one of the following options:
 - Floorplan—Use this option to use Live View to choose APs on the floor plan will forward mDNS frames, and in so doing, make the Bonjour service discoverable by clients. Both the client and Bonjour service must be connected to the AP. Note you should only use this method if you are sure AP placement is accurate and that the RF design is good.
 - AP—Select this option to have the Bonjour service discoverable only by clients that are connected to the same AP (not WLAN).
 - Site—(Default) Select this option to have the Bonjour service discoverable by clients throughout the site.
5. If you want to limit the discoverability of the service based on the user label, click **Restricted to RADIUS groups**, and then enter the user label(s) that you created to map RADIUS attributes. Delimit multiple groups with a comma.
6. Under **Discovery VLANs**, specify the VLAN ID(s) or site variables for every VLAN in the wireless network with a wireless client or Bonjour services that you want to support.
7. Specify any wired VLANs (that are not already part of the WLAN) that you want to support.
Note that these VLANs must be enabled with Bonjour services and must be identified in the AP configuration page for the interface that connects to the switch.
8. In the **Filtering (Wireless)** section, select **Broadcast/Multicast** filtering and **Allow mDNS** to pass the frames to the wireless clients.

Isolation

Prohibit peer to peer communication

☒ Disabled ☐ Same AP ☐ Same Subnet

Filtering (Wireless)

☒ ARP

☒ Broadcast/Multicast

☒ Allow mDNS

☐ Allow SSDP

☐ Allow IPv6 Neighbor Discovery

☐ Ignore Broadcast SSID Probe Requests

DTIM Period

DTIM Period

9. Click **Save** at the top of the page.

Labels

Juniper Mist uses the concept of labels to represent a collection of users or resources, similar to how tags, or groups, are used in some other applications. The idea is to represent a group of related items under a central, clear name so that you can reference the label rather than having to specify all the constituents every time you want to include the items in a configuration. Labels are similar to variables in this way, but the values in a label are absolute – there is no dynamic swapping as is the case with variables.

You can create labels at the organization level or at the site level. Organization-level labels can be used only in the WLAN templates. Site-level labels can only be referenced at that specific site.

To create labels:

- Organization-level—From the left menu of the Juniper Mist portal, select **Organization > Wireless | Labels**.
- Site-level—From the left menu of the Juniper Mist portal, select **Site > Wireless | Labels**.

Types of Labels

You can create user labels and resource labels.

- User Labels
 - AAA attributes—Currently there are two options under AAA attributes user group or RADIUS Username.
 - Client Name
 - Client MAC

- Users connected to a specific WLAN/WLANs
- Resource Labels
 - Application
 - Hostname
 - IP Address—List of IPs or CIDR
 - Port
 - Emails / File Sharing / Online Backup / Social / Videos and Music applications (pre-defined by Mist)

NOTE: Resources cannot be dynamically discovered or based on AAA attributes like users. Resources need to be statically defined.

Use Case: Labels for a Bonjour Gateway

You can use user labels in conjunction with a Bonjour gateway to prevent or allow access to Bonjour services that are available on a different VLAN than the WLAN or user.

The following RADIUS attributes, present in **access-accept** AAA message type, are supported for user labels: **Filter-Id**, **aruba-user-role**, and **Airespace-ACL-Name**.

Figure 6: User Labels

The screenshot shows the Juniper Mist portal interface for creating a new user label. The sidebar on the left contains navigation links: Monitor, Marvis™, Clients, Access Points, Switches, WAN Edges, Mist Edges, Location, Analytics, Site, and Organization. The main content area is titled 'Organization Labels : New Label' and features a 'Create' button and a 'Cancel' button. The form includes the following fields:

- Label Name:** A text input field containing 'AirPlay_OK'.
- Label Type:** A dropdown menu set to 'AAA Attribute'. Below the dropdown, it says 'This is a User label if used in Template WxLan'.
- Label Values:** A section with a 'User Group' dropdown menu and a 'User Group Values' icon. Below this is a large text input field containing 'Filter-Id'. A note at the bottom of this section states 'Note: Requires newer firmware'.

To creating a user label for Bonjour filtering:

1. In the Juniper Mist portal, click **Organization > Admin | Labels**.
2. Click **Add Label**.
3. Enter a name and define your label:
 - **Label Type**—Select **AAA Attribute**.
 - **Label Values**—Select **User Group**.
 - **User Group Values**—Enter the RADIUS attribute value you want to connect this user role to.
4. Click **Create** at the top of the page.

Site vs Organization Labels

For both organization and site-level policies, rules are evaluated from top to bottom, with any matching conditions executed prior to the next evaluation.

Adding APs and Clients to an Existing Label

You can also add individual APs and clients to an existing label, as shown in the following animation and step-by-step procedure.

Figure 7: Adding a Label to Selected Clients

The screenshot shows the Mist WiFi Clients interface. The left sidebar contains navigation icons for Monitor, Marvis, Clients, Access Points, Switches, WAN Edges, Mist Edges, Location, Analytics, Site, and Organization. The top bar includes a 'LIVE DEMO' indicator, a language dropdown set to 'en', and the time 'THU 4:04 PM'. The main header shows '21 WiFi Clients' and a site dropdown set to 'Live-Demo'. Below this is a summary bar with client counts: 21 Wireless Clients, 1 2.4 GHz, 19 5 GHz, 1 6 GHz, 8 802.11ac, 11 802.11ax, and 2 802.11n. A search filter is available. The main table lists clients with columns: User, IPv4 Address, MAC Address, Device Type, AP Name, SSID, and Pre-shared Key. The table contains 11 rows of client data.

User	IPv4 Address	MAC Address	Device Type	AP Name	SSID	Pre-shared Key
Alejandro	192.168.24.10	34:af:b3:e9:83:57	Unknown	LD_NewBobFriday	Mist_IoT	echos
android-5bd931eb44a4d28b	10.100.0.49	32:87:69:e6:ffe5	Zebra TC58	LD_RS_Support	Live_demo_do_not_remove	
android-9e4bf1bc9423bf09	192.168.1.109	d2:d0:4a:ac:3a:5f	Zebra MC3300AX	MC_DavidL AP	Marvis Testing	
Apple	10.100.0.81	2a:5e:20:c5:c5:7b	Apple	LD_RS_Support	Live_demo_only	
denali	10.100.1.26	50:32:37:ea:c3:c2	Mac	LD_Kitchen	Live_demo_do_not_remove	
E972F772-EF34-48FC-8C0E-89AABC90723A	10.100.1.12	f8:4d:89:7b:60:e9	Mac	LD_NewBobFriday	Live-Demo-NAC	
Galaxy-S9	10.100.0.20	a0:c9:a0:eb:4a:51	Samsung Galaxy S9	LD_MHMD	Live_demo_only	
Galaxy-S10e	10.100.0.244	4e:7b:fb:a9:ef:38	Samsung Galaxy S10e	LD_NewBobFriday	Live_demo_only	
Google	192.168.24.16	ac:67:84:0e:d4:74	Google	LD_MHMD	Mist_IoT	nests
hal	192.168.24.211	dca6:32:c7:e7:e6	Raspberry Pi Trading Ltd	LD_24_JSW	Mist_IoT	mist-rpi

NOTE: To replay the animation, right-click, and open it in a new tab. Use the refresh button to replay it as needed.

1. In the left menu, select **Clients > WiFi Clients**.
2. Select the client(s) that you want to assign to a label.
3. Click **Edit Clients** in the top-right corner of the page.

NOTE: The button appears only when clients are selected.

4. Select **Add Labels**.
5. Click the plus sign (+), and select a label. Repeat this step as needed to add more labels.
6. Click **OK**.

Using Labels in a WxLAN Policy

When creating a WxLAN policy in a WLAN template, the idea is to create a line of logic that associates Users with Resources, connected by an action such as **Allow** or **Deny**, to control the users' access to the resource. In this context, user labels represent things like Wi-Fi clients or APs, and resources labels represent things like applications (specific or by category) and IP addresses. By connecting them, you can create some rules to allow guest users access social media, or others to prevents corporate users from using streaming video services other than, say, YouTube.

If you don't already have a label defined to represent a given group of users, you can create one from within the policy while making the rule. However, we do recommend that you plan your labels before starting the policy so they will be available in a drop-down list.

To create a label, you give it a name and then choose from a variety of predefined types, such as AAA attributes, APs, WLANs, or IP addresses, and then add your specific parameters in the corresponding values field. To use a label, for example when creating a user access policy for the organization, select it from the drop-down of available labels and add it to the rule.

Figure 8: Creating Labels

Label Name

New Label

Label Type

Application

This is a Resource label if used in Template WxLan

Label Values

Add Application +

Search

AWS	Cloud Traffic
Microsoft Azure	Cloud Traffic
Google Cloud Platform	Cloud Traffic
Apple iCloud	Cloud Traffic
GSuite	Collaboration/Productivity
Office365	Collaboration/Productivity
Okta	Collaboration/Productivity
Oracle	Collaboration/Productivity
SAP	Collaboration/Productivity
Atlassian	Collaboration/Productivity
Apps	Collaboration/Productivity

Close

Policies created in a WLAN template take precedence over policies created for an individual site. In other words, the rules in a site-level policy will only take effect if no other rules, from an organization policy that includes the site, already match one or more of the conditions.

In addition, only organization-level labels are available for WxLAN policies; site level labels do not show up in the drop-down.

To create labels for a WLAN access policy:

1. From the Mist portal, select **Organization > Wireless | Labels**.
2. Click **Add Label** and then give your label a descriptive name (the label names will appear in the policy drop-down when adding rules to a policy in the WLAN Templates page).

3. Select an option from the **Label Type** drop-down list, and then enter a value in the corresponding **Label Values** field. Depending on the label type that you select, you can either enter your parameters directly in the field or click the button that appears and enter values for the specified parameters.
4. Click **Create** in the upper-right corner of the page.

Configure a Third-Party Tunnel

With Juniper Mist, you can create a tunnel to third-party VPN concentrators by using Layer 2 Tunneling Protocol version 3 (L2TPv3), which is the default protocol, or dynamic multipoint VPN (DMVPN). Additional tunnel options include aggregating the Ethernet interfaces on the access point (AP), supporting dynamic or static tunnels, and IPsec.

To configure a third-party tunnel:

1. Select **Organization > Wireless | WLAN Templates**, and click the WLAN template that you want to add the tunnel to.
2. In the 3rd Party Tunnels section, click **Add Tunnel**.
3. When the Create Tunnel page appears, enter a name for the tunnel.
4. Specify the IP address or hostname of the remote peer at the opposite end of the tunnel.
5. Specify the outer maximum transmission unit (MTU) value of the TCP packet.
Packets larger than this are split. Note that GRE tunnels add a 24-byte header to the packet.
6. Select an authentication method.
We recommend Hashed Message Authentication Code (HMAC)-SHA1.
7. If you need to support multipoint VPN tunneling, select **DMVPN**, or leave it unselected to use L2TPv3.

For example, you would enable DMVPN for multisite communication over a service provider network where IP address assignment is subject to change.

If you enable DMVPN, also configure the settings:

- **Hosts Routed via DMVPN**—Enter the IP addresses (separated with a comma) that you want to route through this tunnel.

IPSec—Enable this option (recommended) to encrypt traffic on the tunnel. In the **PSK** field, type your preshared key.
8. Under **Protocol**, specify whether to use an IP or UDP port for the remote peer.
If you select UDP, also enter the port number used by the peer.
 9. Select the type of tunnel:

- **Dynamic**—These tunnels are set up only for the time of use. If you select this option, also specify the Router ID and host names in the **SCCRQ Control Message Overrides** field to identify the endpoints for which you want to override the SCCRQ messages.

Static—These tunnels remain established even when not in use.

10. Under **SessionS (pseudowireS)**, set up Ethernet-based or VLAN-based sessions to tunnel client AP traffic to the remote end.

- Enter the **Remote End ID**.

Specify connection type. Select **Ethernet** to tunnel native Ethernet frames, or select **VLAN**. With VLAN, you can select **802.1ad** to support double-tagging.

- If needed, click **Create a Session** to add more sessions.

11. Click **Create** at the bottom of the Create Tunnel page to add the tunnel to the WLAN template.

12. To save the template changes, click **Save** at the top of the page.

Enable Wireless Bridging Mode

By default Juniper Mist drops unknown DHCP responses to wireless clients. Essentially the client must be directly associated to the AP for DHCP to be forwarded. This will cause bridged virtual machines to fail DHCP. However, you can enable wireless bridging if you want to allow bridged VMs to be able to connect to a Juniper Mist access point.



NOTE: We recommend caution when enabling this feature outside of home, lab, and small scale/ niche production use. If you enable bridging, broadcast and unicast DHCP packets will be forwarded over the air, without filtering, on every AP that this WLAN is enabled on. This will lead to increased channel utilization. There's also the security aspect to consider of allowing the VM to bridge onto the network.

You can configure wireless bridging via API.

For Site WLANS, the URI is `/api/v1/sites/:site_id/wlans/:wlan_id`.

```
put /api/v1/sites/:site_id/wlans/:wlan_id

{

    "enable_wireless_bridging": true
}
```



```
}
```

For template WLANs, the URI is `/api/v1/orgs/:org_id/wlans/:wlan_id`.

```
put /api/v1/orgs/:org_id/wlans/:wlan_id

{

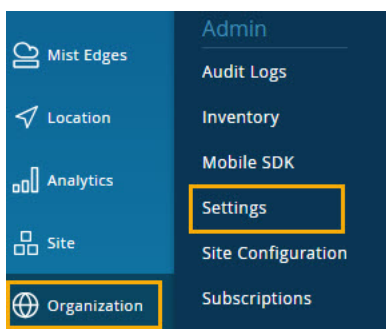
  "enable_wireless_bridging": true

}
```

There are many ways to modify the API, such as writing a script, using a tool like Postman, or simply using a web browser, as described below.

To enable wireless bridging mode:

1. (For template WLANs) Look up the org ID for the URI.
 - a. (For template WLANs) Select the **Organization > Settings** from the left menu of the Juniper Mist portal.

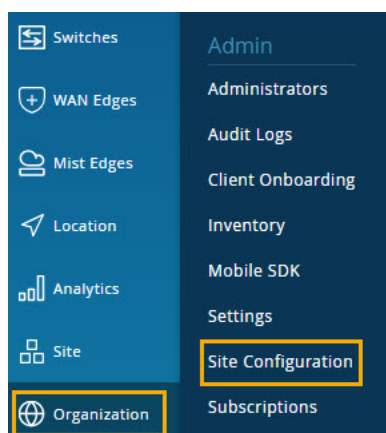


- b. Click the **Copy** button next to the **Organization ID** field.

c. Paste the ID into a text file so that you can retrieve it later.

2. (For site WLANs) Look up the site ID for the URI.


a. Select the **Organization > Site Configuration** from the left menu of the Juniper Mist portal.



b. Click the **Copy** button next to the **Organization ID** field.

Edit WLAN

SSID
Live-Demo-NAC

WLAN ID
a4b5c7e8-9012-4567-8901-234567890123 

WLAN Status
☒ Enabled
 ☐ Disabled

- d. Paste the ID into a text file so that you can retrieve it later.
4. In your web browser, enter the full URI as shown below, filling in the actual IDs.
 - For Template WLANs—https://api.mist.com/api/v1/orgs/org_id/wlans/wlan_id
 - For Site WLANs—https://api.mist.com/api/v1/sites/site_id/wlans/wlan_id
5. When the Django REST framework page appears, scroll to the bottom and enter the command shown below.

```
{
    "enable_wireless_bridging": true
}
```


Django REST framework

Get Update Delete Site / Getall Create / Get Update Delete

Get Update Delete

DELETE OPTIONS GET

GET /api/v1/sites/d4b6c1c5-823f-4b37-ad14-285805fc49d3/wlans/1b56900a-15b5-462a-aab6-3be839335d1d

HTTP 200 OK
 Allow: PUT, OPTIONS, GET, DELETE
 Content-Type: application/json
 Vary: Accept

```
{
  "ssid": "1b56900a-15b5-462a-aab6-3be839335d1d",
  "sle_excluded": true,
  "enabled": true,
  "hide_ssid": false,
  "hostname_ie": false,
  "no_static_ip": false,
  "no_static_dns": false
}
```

```
{
  "po": "1b56900a-15b5-462a-aab6-3be839335d1d",
  "mxtunnel_id": null,
  "wxtunnel_id": null,
  "interface": "all"
}
```

Media type: application/json

Content:

```
{
  "enable_wireless_bridging": true
}
```

PUT

6. Click **Put**.

NOTE: You can find more information about `enable_wireless_bridging` in the [Juniper Mist API Documentation Site](#).

4

CHAPTER

WLAN Guest Portal

[Compare WLAN Guest Portal Options | 149](#)

[Custom Guest Portal | 151](#)

[Use an External Portal for Guest Access | 178](#)

[Use an Identity Provider for Guest Access | 187](#)

[Authorize, Reauthorize, and Reconnect Guest Clients | 198](#)

[FAQs: Guest Portal | 200](#)

Compare WLAN Guest Portal Options

SUMMARY

To allow your guests to access the internet, you can set up the WLAN Guest Portal to allow direct access, enable a simple sign-in form, forward guests to an external sign-in form, or enable Single Sign-On with your identity provider.

You can configure Guest Portal options in your WLAN settings. Keep the default settings to give your guests direct access to the internet, or choose from other options described in the following video and comparison table.

NOTE: This topic covers the Guest Portal options in the Edit/Create WLAN window. Alternatively, you can configure guest access via RADIUS server. See ["Guest Access Using RADIUS Server with MAC Authentication Bypass"](#) on page 251.

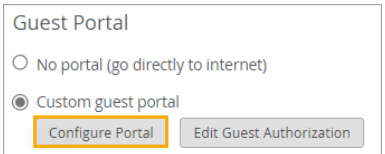
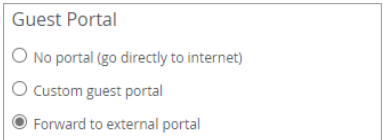
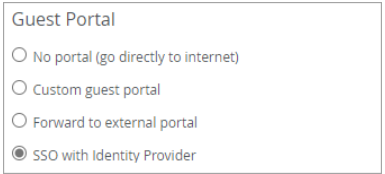


Video: [Mist Guest Portal](#)

Table 13: Compare WLAN Guest Portal Options

Option	Description	Setup
Direct Access (No Portal)	<p>Guests get immediate internet access without authentication.</p> <p>This is the easiest option unless you have a business need for additional security or you want to collect information about your guests.</p>	<p>No action is needed. This is the default Guest Portal option in WLAN settings.</p> <div><p>Guest Portal</p><p><input checked="" type="radio"/> No portal (go directly to internet)</p><p><input type="radio"/> Custom guest portal</p><p><input type="radio"/> Forward to external portal</p><p><input type="radio"/> SSO with Identity Provider</p><p><input checked="" type="checkbox"/> Bypass guest/external portal in case of exception</p></div>

Table 13: Compare WLAN Guest Portal Options *(Continued)*

Option	Description	Setup
Custom Guest Portal	<p>Guests get internet access by completing a simple sign-in form that you set up in Juniper Mist™.</p> <p>This is an easy-to-configure approach that allows you to collect some information from your guests.</p> <p>Optionally, you can enable options such as authorization codes, sponsored guest access, social sign-in, and more.</p>	<p>Select Custom guest portal in the WLAN settings. Keep the default settings or click Configure Portal to change features such as the background image, form fields, text, and authorization methods.</p>  <p>For help, see "Add a Custom Guest Portal to a WLAN" on page 151.</p>
External Portal	<p>Guests get internet access by going to a sign-in portal that you've developed outside Juniper Mist.</p> <p>With this option, you use a sign-in portal that your web developers have specifically designed for your business and your use cases.</p>	<p>Select Forward to external portal in the WLAN settings. Then enter your portal URL and configure other optional settings.</p>  <p>For help, see "Use an External Portal for Guest Access" on page 178.</p>
Single Sign-On (SSO) with an Identity Provider	<p>Guests get internet access by using your identity provider's sign-in page. (A few examples include Okta, Microsoft Azure, and OneLogin, but most IdPs are supported.)</p>	<p>Select SSO with Identity Provider in the WLAN settings. Then enter the settings for your IdP.</p>  <p>For help, see "Use an Identity Provider for Guest Access" on page 187.</p>

Custom Guest Portal

IN THIS SECTION

- [Add a Custom Guest Portal to a WLAN | 151](#)
- [Form Fields for Custom Guest Portal | 153](#)
- [Text and Language Options for Custom Guest Portal | 155](#)
- [Layout Options for Custom Guest Portal | 158](#)
- [Authorization Options for Custom Guest Portal | 162](#)

Add a Custom Guest Portal to a WLAN

SUMMARY

With the Custom Guest Portal option, guests must complete a sign-in form to get internet access. This option is easy to set up and allows you to collect information from your guests.

You can keep the default settings for quick setup or customize the form fields, the text, the layout, the images, and the authentication methods.

Before you begin: Create the WLAN that you want to add the guest portal to. For more information, see ["Configure a WLAN Template" on page 119](#).

To add a custom guest portal to your WLAN:

1. Navigate to the WLAN.

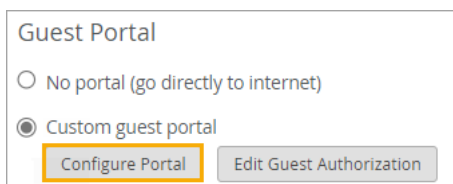
NOTE:

- If the WLAN is in a WLAN template, select **Organization > Wireless | WLAN Templates**, click the template, and then click the WLAN.

- For a site-level WLAN, select **Site > Wireless | WLANs**, and then click the WLAN.

2. In the **Edit WLAN** window, under **Guest Portal**:

- Click **Custom guest portal**.
- Click **Configure Portal**.



Guest Portal

☐ No portal (go directly to internet)

☒ Custom guest portal

[Configure Portal](#) [Edit Guest Authorization](#)

3. In the **Guest Portal Options** window, go through each tabbed page to review the defaults and make changes if needed.

- Click **Form Fields** to set up the user input fields. For more information, see ["Form Fields for Custom Guest Portal" on page 153](#).
- Click **Customize Labels** to review and modify the on-screen text. You can even set up your portal for different languages. For more information, see ["Text and Language Options for Custom Guest Portal" on page 155](#).
- Click **Customize Layout** to add a logo, change the background, and make other changes in the appearance of the portal. For more information, see ["Layout Options for Custom Guest Portal" on page 158](#).
- Click **Authorization** to enable features such as social login, sponsored access, emailed or text-based confirmation codes, and so on. For more information, see ["Authorization Options for Custom Guest Portal" on page 162](#).

4. As you make changes, click **Preview Guest Portal** to see how your portal looks.

The preview appears in a new browser tab.

5. When finished with all changes on all tabs, click **OK** at the bottom of the Guest Portal Options window.

NOTE: The **OK** button is unavailable if any configurations are incomplete. For example, the default layout includes terms of service. If you keep this option, you must either enter text in the Terms of Service text box or enter a Terms Link on the Customize Labels tab. For help with this option, see ["Layout Options for Custom Guest Portal" on page 158](#).

6. Select or clear the **Bypass guest/external portal in case of exception** check box at the bottom of the Guest portal section.

When this feature is selected, each access point will try to reach the portal or IdP. If it is not reachable then the AP will automatically authorize the guests to connect to the WLAN.

7. Click **Save** at the bottom of the Edit WLAN window.

To verify the appearance and functionality of your guest portal, use your wireless device to connect to your WLAN. You can then adjust the portal configuration as needed.

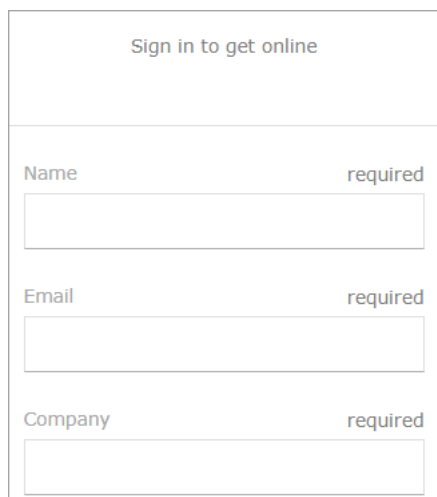
Form Fields for Custom Guest Portal

SUMMARY

If you've enabled a custom guest portal, you can keep the preset form fields or customize them to collect exactly the information that you want your guests to provide.

In your custom guest portal, you can keep the default form fields or use the **Form Fields** tab to collect the exact information that you want your visitors to provide.

If you keep the default settings, your guests will need to enter their Name, Email, and Company, as shown in the custom guest portal below.



Sign in to get online

Name required

Email required

Company required

You can make changes on the **Form Fields** tab of the **Guest Portal** options window.

Guest Portal Options [X]

Form Fields | Customize Label | Customize Layout | Authorization

Required Portal Fields
(if selected, users must provide some data for the field)

☒ Full Name ☒ Email Address ☒ Company

Custom Portal Fields
(Select to show data field during login, deselect to hide)

<input type="checkbox"/> Custom Field 1	<input type="checkbox"/> Required (Data required if enabled)
<input type="checkbox"/> Custom Field 2	<input type="checkbox"/>
<input type="checkbox"/> Custom Field 3	<input type="checkbox"/>
<input type="checkbox"/> Custom Field 4	<input type="checkbox"/>

NOTE: This topic describes one aspect of Custom Guest Portal setup. To get started with your custom guest portal, see ["Add a Custom Guest Portal to a WLAN" on page 151](#).

The options include:

- **Required Portal Fields**—Select or clear these check boxes to add or remove the required fields (**Full Name**, **Email Address**, and **Company**). If you select these fields, your guests must complete them to get access.

TIP: What if you want one of these fields, such as **Company**, to be optional? First, clear the check box from the field (because you don't want this *required* portal field). Then add a Custom Portal field, such as **Custom Field 1**. On the **Customize Labels** tab, edit the text for **Custom Field 1** so that it says **Company**. When you preview your portal, you'll see that you now have a **Company** field that is not required.

- **Custom Portal Fields**—Select the checkbox for each additional field that you want to display on the form. Optionally, if you want to require users to complete a field, drag the **Required** slider to the right.

NOTE: At this point, the new fields have default labels such as **Custom Field 1**, **Custom Field 2**, and so on. You'll be able to replace this text with your own labels on the **Customize Label** tab.

Text and Language Options for Custom Guest Portal

SUMMARY

If you've enabled a custom guest portal, you can keep the preset words and phrases or enter your own text to better represent your brand.

IN THIS SECTION

- [Changing the Text | 155](#)
- [Setting Up Different Sets of Labels for Different Languages | 156](#)

You can change the top-of-page greeting, the form field labels, the button names, and other on-screen text. You can even set up a multi-language portal.

You can make these changes on the **Customize Label** tab of the **Guest Portal Options** window.

NOTE: This topic describes one aspect of Custom Guest Portal setup. To get started with your custom guest portal, see ["Add a Custom Guest Portal to a WLAN" on page 151](#).

Changing the Text

You can see the default text in the **Message Text** box and on the right side of the **Label Customization** section. Read the default text to understand the purpose, and then make your changes by typing in the box.

Guest Portal Options

Form Fields
Customize Label
Customize Layout
Authorization

Select Locale
Default Locale

Message Text
You may enter a plain text message or an HTML fragment. If you provide HTML content you will be able to include images, links, and custom fonts/colors.

Sign in to get online

Label Customization

Page Title	Welcome
Accept Terms	I accept the Terms of Service
Terms Link	Terms of Service
Opt Out Label	Do Not Store My Personal Informa
Back to Sign In	Back to Sign In
Terms of Service Error	Please review and accept the Term
Required Field Label	required
Name Label	Name
Name Error	Please provide your name

[Preview Guest Portal](#)
OK
Cancel

NOTE: Certain fields only appear if you enable the relevant options on the other tabbed pages. For example, you only need to enter Custom Field labels if you added custom fields on the Form Fields tab. You only need to enter text for Facebook social sign-in if you enabled that option on the Authorization tab.

Setting Up Different Sets of Labels for Different Languages

By default, the portal supports one language, with one set of labels. For a single-language portal, keep **Default Language** as the locale.

Guest Portal Options

Form Fields Customize Label Customize Layout Authorization

Select Locale Default Locale ▼

TIP: What if you want a single-language portal in a language other than English? For example, let's say that you want your portal to be in French. Keep Default Language as the locale, and then change all of the English text to French words and phrases.

If you want to set up a multi-language portal, you'll use the **Select Locale** option to set up a different set of labels for each language. For example, say that your guest portal is for a city event, and your city's policy is to present all information in English, Spanish, and Korean. You want English to be the default language. You also want to allow your guests to switch to Spanish or Korean, as shown in the guest portal below.

Sign in to get online

Default Language

Default Language

Spanish (Spain) (Español (España))

Korean (Korea) (한국어 (韩国))

Name required

Email required

To achieve this result, first, you'd customize the labels for the default language. This is the language that people first see when the portal appears. It can be whichever language you prefer. For this example, it's English. Then you'd select the next language (for our example, Spanish) and replace the default text with the appropriate words and phrases in that language. Then you'd continue until you've entered phrases for all the languages.

To go back and forth between the different languages, simply change the locale.

NOTE: Juniper Mist provides text in English only. For all languages that you want to support, you'll enter your own words and phrases to replace the sample text.

Layout Options for Custom Guest Portal

SUMMARY

If you've enabled a guest portal, you can keep the preset layout or add your logo and background photo to better represent your brand. You also can adjust other settings.

In your custom guest portal, you can keep the default layout or redesign certain features. For example, you can add your own logo and background image. You can add or remove features such as a Terms of Service agreement and an Opt Out option.

This example shows a guest portal that is configured with the default options.



You can make changes on the **Customize Layout** tab of the **Guest Portal Options** window.

Guest Portal Options

Form Fields

Customize Label

Customize Layout


Authorization

Layout Customization

☒ Responsive Layout


Alignment
☒ left
☐ center
☐ right

Logo



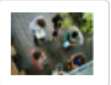
Use Default

Primary Color



Use Default

Background



Use Default

☐ Hide 'Powered by Mist'

☒ Require acceptance of [Terms of Service](#)

☐ Do not save user data

☒ Show 'Opt Out'

☒ 'Opt Out' as default

Preview Guest Portal

OK

Cancel

NOTE: This topic describes one aspect of Custom Guest Portal setup. To get started with your custom guest portal, see ["Add a Custom Guest Portal to a WLAN" on page 151](#).

The options include:

- **Responsive Layout**—When you select this check box, the guest portal layout adapts to the screen width of the user's device.
- **Alignment**—This selection determines whether the sign-in form appears on the left, center, or right of the browser window.
- **Logo**—Upload a new logo.

Requirements:

- File size—100 kB maximum
- Image width: 500 pixels maximum
- Height: 200 pixels maximum
- **Primary color**—This selection determines the color of the sign-in button, link text, active fields, and other elements of the guest portal.
- **Background**—Upload a new background photo.
 - File size—100 kB maximum
 - Image width: 500 pixels maximum
 - Height: 200 pixels maximum

NOTE: To change the Logo, Primary Color, or Background, click the respective tile (see image above).

- **Hide 'Powered by Mist'**—Select this check box if you do not want your form to display *Powered by Mist*. When the check box is selected, this message appears at the bottom of the form.
- **Require acceptance of Terms of Service**—If you want to require guests to agree to your terms of service, select the check box. Then click **Terms of Service**, enter the information that you want users to see, and click **OK** to save the text.

Guest Portal Options

Form Fields

Customize Label

Customize Layout

Authorization

Layout Customization



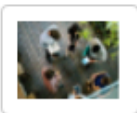
☒ Responsive Layout

Alignment
 ☒ left
 ☐ center
 ☐ right

Logo

Primary Color

Background

[Use Default](#)
[Use Default](#)
[Use Default](#)

☒ Hide 'Powered by Juniper Mist'
 ☒ Require acceptance of [Terms of Service](#)

☐ Do not save user data
 ☐ Show 'Opt Out'

[Preview Guest Portal](#)

OK

Cancel

NOTE: **Require acceptance of Terms of Service** must be present for all guest portals in the European Union and United Kingdom. This is due to the European GDPR requirement that an individual must consciously consent.

Alternatively, you can enter a **Terms Link** on the Customize Labels tab. In this case, when users click Terms of Service, they'll go to the link that you specify instead of seeing the words that you enter in the Terms of Service pop-up window.

- **Do not save user data**—Select this check box if you do not want to save the users' entries.

- **Show 'Opt Out'**—If you select this check box, the guest portal displays a **Do Not Store My Personal Information** option. If you also select the **'Opt Out' as default** option, then the **Do Not Store My Personal Information** is automatically selected. Users would uncheck the box if they want to opt in.

Authorization Options for Custom Guest Portal

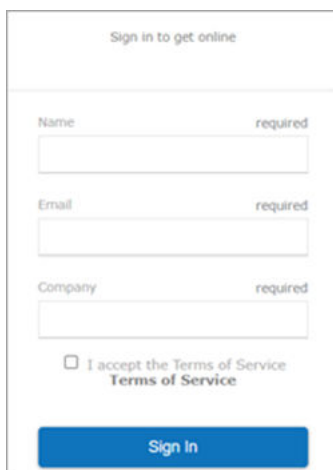
SUMMARY

If you've enabled a custom guest portal, you can keep the preset authorization method or set up another method such as a configured passphrase, an emailed authorization code, sponsored access, or social sign-in.

IN THIS SECTION

- [Facebook App Creation | 168](#)
- [Enable Guest Portal Social Login with Microsoft® Azure | 169](#)

With the default guest portal sign-in method, guests complete the form fields and click the **Sign In** button.



The screenshot shows a web form titled "Sign in to get online". It contains three text input fields: "Name" (marked as "required"), "Email" (marked as "required"), and "Company" (marked as "required"). Below these fields is a checkbox labeled "I accept the Terms of Service" with a link to "Terms of Service". At the bottom of the form is a blue button labeled "Sign In".

You can set up other sign-in options on the **Authorization** tab of the **Guest Portal Options** window.

Guest Portal Options

Form Fields

Customize Label

Customize Layout

Authorization

Authorization Options

Users will be able to sign in with any of the selected authorization methods. If none are selected users may sign in without authorization.

☐ Passphrase


.....


Reveal


☐ Authentication code via Email


☐ Authentication code via Text Message


☐ Sponsored Guest Access

☐
 Google Sign In

☐
 Facebook Sign In

☐
 Amazon Sign In

☐
 Microsoft Sign In

☐
 Azure Sign In

Authorization Settings

Devices remain authorized for

1

Days

☐ After authorization redirect to URL

Preview Guest Portal

OK

Cancel

NOTE: This topic describes one aspect of Custom Guest Portal setup. To get started with your custom guest portal, see ["Add a Custom Guest Portal to a WLAN"](#) on page 151.

Passphrase

Passphrase—Select this check box to require users to enter a passphrase. Then enter the passphrase in the text box.

Authentication Code via Email

Authentication code via Email—Select this check box to require users to enter an email address to receive an authentication code. They must then use that code to complete the sign-in process.

After you select the check box, additional fields appear at the bottom of the **Guest Portal Options** window:

Email Access Code valid for Minutes

Customize Message

Code {{code}} expires in {{duration}} minutes.

The message will be sent in this format. The {{code}} and {{duration}} variables are required in the custom message.

- **Email Access Code valid for**—Enter the amount of time (in minutes) that the code remains valid after the email is sent.
- **Customize Message**—Add any additional text that you want to include in the email message.
 - When the message is sent, the {{code}} variable displays the code that the user needs to enter.
 - The {{duration}} variable displays the amount of time until the code expires.

Authentication Code via Text Message

—Select this check box to require users to enter a phone number to receive an authentication code. They must then use that code to complete the sign-in process.

The authentication code can either be sent via a free method via the cell provider, or a paid aggregator. Sending through the cell provider relies upon Email to SMS. The available providers are listed in the **Paid service** drop-down menu. Select a provider, and then enter your account information.

☒ Authentication code via Text Message

☐ Free through cell provider

☒ Paid service

BroadNet Ser

BroadNet Us

BroadNet Pa

Validate Con

(Add phone number of the recipient to receive validation SMS)

SEND

NOTE: We have begun to receive reports of guests not receiving the authentication code intermittently or not receiving at all for some of the cell providers.

We have received feedback from cell providers they are deprecating or enforcing limits on the Email to SMS service, and they recommend using aggregator services instead.

Based on this feedback, you may wish to investigate using a paid aggregator service such as Twilio or Broadnet.

For both methods (free or paid), also complete the fields at the bottom of the **Guest Portal Options** window:

The screenshot shows a form with two main sections. The first section is labeled 'SMS Access Code valid for' followed by a text input field containing the number '5' and the word 'Minutes'. The second section is labeled 'Customize Message' and contains a large text area with the placeholder text 'Code {{code}} expires in {{duration}} minutes.' Below the text area, a note states: 'The message will be sent in this format. The {{code}} and {{duration}} variables are required in the custom message.'

- **SMS Access Code valid for**—Enter the amount of time (in minutes) that the code remains valid after the text message is sent.
- **Customize Message**—Add any additional text that you want to include in the text message. When the message is sent, the `{{code}}` variable displays the code that the user needs to enter. The `{{duration}}` variable displays the amount of time until the code expires.

Sponsored Guest Access

Sponsored Guest Access—Select this check box if you want to require a sponsor to approve guests before they can use your network.

- **Pre-defined sponsors**—Select this option if you want to list specific personnel who can act as sponsors for guest access. Guests must select a sponsor from the list to request access.

Also complete these tasks:

- Enter the **Name** and **Email** address.
- For additional sponsors, click **Add Sponsor**, and enter their contact information.
- At the bottom of the Guest Portal Options window, enter the number of minutes that the sponsor request remains valid.

Guest Portal Options

are selected, users may sign in without authorization.

☐ Passphrase [Hide](#)

☐ Authentication code via Email

☐ Authentication code via Text Message

☒ **Sponsored Guest Access**

☒ Pre-defined sponsors


Name	Email
<input type="text"/>	<input type="text"/>


[Add Sponsor](#)


☒ Notify all sponsors (Max 10)


☐ Sponsor authorized domains


☐ Email guest when approved/denied

☐  Google Sign In

☐  Facebook Sign In

☐  Amazon Sign In

☐  Microsoft Sign In

☐  Azure Sign In

Authorization Settings

Devices remain authorized for

☐ After authorization redirect to URL

Sponsor email request will remain valid for

[Preview Guest Portal](#)

- **Sponsor authorized domains**—Select this option to notify everyone on a specified domain.
- Enter the domain, such as *MyCompany.com*. If you want to enter multiple domains, enter a comma between each one.
- At the bottom of the **Guest Portal Options** window, enter the number of minutes that the sponsor request remains valid.

☐ Authentication code via Text Message
☒ Sponsored Guest Access
☐ Pre-defined sponsors
☒ Sponsor authorized domains required
☐ Email guest when approved/denied
☐ Google Sign In
☐ Facebook Sign In
☐ Amazon Sign In
☐ Microsoft Sign In
☐ Azure Sign In
Authorization Settings
 Devices remain authorized for
☐ After authorization redirect to URL
 Sponsor email request will remain valid for
[Preview Guest Portal](#)

- **NOTE:** If you want guests to receive an email when the sponsor takes action, select **Email guest when approved/denied**.

Social Sign-In Options

Social Sign-In Options—Select the check box to allow guests to connect by using Google, Facebook, Amazon, or Microsoft Azure. Then enter the information to enable the authorization.

NOTE: Google has changed the behavior for Google Sign In for the gmail.com domain. Users are no longer able to sign in through pop-up windows.

The following error message appears: *"Error 403: disallowed_user agent"*. So far, this change appears to only affect users who sign in with a gmail.com email address. This issue does not seem to affect corporate domains leveraging Google for Single Sign-On.

We recommend using another sign-in provider if you intend for gmail.com users to sign in.

For more information, [see this article at the Google for Developers site](#).

For help creating custom applications, see:

- ["Facebook App Creation" on page 168](#)

- ["Enable Guest Portal Social Login with Microsoft® Azure" on page 169](#)

Authorization Settings

- **Devices remain authorized**—Keep the default settings, or enter the number and the unit. For example, you could allow guests to remain connected for 60 minutes, 2 hours, 2 days, or other time frames.
- **After authorization redirect to URL**—Select this option if you want to display a specific webpage after users connect. For example, display your company's home page. Or, at a convention, link to the daily events page.

Facebook App Creation

SUMMARY

Use this information if you've enabled a guest portal and want to set up a Facebook app for user authentication.

If you want to allow users to log in to the wireless network by using their Facebook login credentials, you must first create a Facebook App Integration.

NOTE: The results of this procedure will enable you to complete the procedure to enable the Facebook social login option on the Authorization tab.

To create a Facebook app, follow the [Facebook Login Use Case](#) instructions, which are outlined below:

1. Navigate to the [Apps Dashboard](#), then select **Create App**.
2. Select the **Authenticate and request data from users with Facebook Login** use case.
3. When asked if you are building a game, select **no**, then select **Next**.
4. Next, navigate to [Basic Settings](#). Copy and save the **App ID** and **App Secret** which you will need to enter in the Juniper Mist™ portal to enable Guest Portal Social Login.
5. Enter the following app details:
 - [Display Name](#)
 - [Contact Email](#)
 - [Privacy Policy URL](#)

- [App Category](#)
 - [App Domains](#)—Enter `https://www.juniper.net`
6. [Customize your app](#). Set the OAuth settings including the **Redirect URI**, which ensures that the user will be sent to the location you specify here once they are authorized.
- **Redirect URI**— `https://www.juniper.net`
7. If applicable, [add more use cases](#).

Enable Guest Portal Social Login with Microsoft® Azure

SUMMARY

Use this information if you've enabled a guest portal and want to integrate with Microsoft Azure® for user authorization.

IN THIS SECTION

- [Enter Information About the Mist Portal | 172](#)
- [Navigate to the Mist Portal to set up the social login for your WLAN | 174](#)
- [Add a new guest user in Azure | 176](#)
- [Assign an application to the guest user | 177](#)

The Guest Portal Social Login feature allows guests to log into the wireless network using their social network logins such as Google, Facebook, and Amazon accounts.


To enable Guest Portal Social Login with Microsoft® Azure:

Create Registration in Microsoft® Azure

1. Register or login to the [Azure Portal](#).
2. On your Azure portal, select **Microsoft Entra ID**.


Welcome to Azure!

Don't have a subscription? Check out the following options.




Start with an Azure free trial
Get \$200 free credit toward Azure products and services, plus 12 months of popular [free services](#).

[Start](#)



Manage Microsoft Entra ID
Manage access, set smart policies, and enhance security with Microsoft Entra ID.

[View](#) [Learn more](#)




Access student benefits
Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

[Explore](#) [Learn more](#)

Azure services

[+ Create a resource](#)



Microsoft Entra ID

[Application Insights](#)
[App Services](#)
[Quickstart Center](#)
[Virtual machines](#)
[Storage accounts](#)
[SQL databases](#)
[Azure Cosmos DB](#)
[More services](#)

3. Click on **App registrations**. If you cannot find this, click on **More Services** and search for **App registrations**.

4. Select **New Registration**.

App registrations [↗](#)

[+ New registration](#)
[🌐 Endpoints](#)
[🔧 Troubleshooting](#)
[🔄 Refresh](#)
[⬇ Download](#)
[📄 Preview features](#)
[💡 Got feedback?](#)

i Try out the new App registrations search preview! Click to enable the preview. →

i Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

All applications **Owned applications** Deleted applications (Preview)

🔍 Start typing a name or Application ID to filter these results

This account isn't listed as an owner of any applications in this directory.

[View all applications in the directory](#)

5. Add the name you wish to add for the App.

6. Select any account type.

7. Under **Redirect URI** select **Web** and the URL should be **https://www.juniper.net/documentation/us/en/software/mist/mist-wireless/topics/task/azuresociallogin.html** .

[Home](#) > [App registrations](#) >

Register an application

*** Name**

The user-facing display name for this application (this can be changed later).

Azure Social Login ✓

Supported account types

Who can use this application or access this API?

☐ Accounts in this organizational directory only (Default Directory only - Single tenant)
☒ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

8. Click **Register**.

Once the registration is complete, the following page is displayed:

[Delete](#) [Endpoints](#) [Preview features](#)

Essentials

Display name	: Azure Social Login	Client credentials	: 0 certificate, 1 secret
Application (client) ID	: b4ee41b0-8f58-440f-9427-7e92733a7016	Redirect URIs	: 1 web, 0 spa, 0 public client
Object ID	: 1e284e1f-6c4b-416e-b961-d06be7a245f0	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: d141071b-6aa9-4e71-add1-a69348cc0fce	Managed application in I...	: Azure Social Login
Supported account types	: Multiple organizations		

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. [Add MPN ID to verify publisher](#)

Examples:

- **Application (client) ID** — b4ee41b0-8f58-440f-9427-7e92733a7016

- **Directory (tenant) ID** — d141071b-6aa9-4e71-add1-a69348cc0fce

Copy and save the **Application (client) ID** and the **Directory (tenant) ID**. These will be entered into the **Guest Portal Options** window of the Juniper Mist portal in a few moments.

Enter Information About the Mist Portal

1. Next, to generate the Secret ID, click on **Certificates & secrets**.

Azure Social Login | Certificates & secrets

Search (Cmd+/) << Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates
Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	Certificate ID
No certificates have been added for this application.			

Client secrets
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
No client secrets have been created for this application.			

2. Click **New client secret** and enter the **Description** and **Expire** time.

Add a client secret

Description

Expires

Recommended: 6 months

Add

Cancel

- Click **Add** and a secret key will be generated.

NOTE: You must copy the contents of the **Value** field and use that as the secret ID for the Mist Portal configuration. Do not use the secret ID.

Client secrets			
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.			
+ New client secret			
Description	Expires	Value	Secret ID
test	1/22/2022	Umdbo.d_n0GvVx7fdl-_H1-BsRxxX5Yhn	5cd86536-8da2-4ff1-9f67-7c2b3bdb01d4

- Select **Branding**.
- For the **Home page URL**, enter **https://portal.mist.com** and for the **Terms of service URL**, enter **https://portal.mist.com/tos**.

Azure Social Login | Branding

Search (Cmd+/) << Save Discard Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Name * ⓘ Azure Social Login

Logo None provided

Upload new logo ⓘ Select a file

Home page URL ⓘ https://portal.mist.com ✓

Terms of service URL ⓘ https://portal.mist.com/tos ✓

Privacy statement URL ⓘ e.g. https://example.com/privacystatement

NOTE: portal.mist.com is the URL for organizations in the Global 01 region. To find the correct Guest Wi-Fi Portal URL for the cloud instance used by your portal, see *Juniper Mist Firewall Ports and IP Addresses for Firewall Configuration*.

Navigate to the Mist Portal to set up the social login for your WLAN

Next, navigate to the Mist portal where you will paste the **Application (client) ID**, **Secret ID (Value)**, and **Directory (tenant) ID** that you obtained previously. You need these values to set up the social login for your WLAN.

1. In the Juniper Mist portal, select the WLAN that you want to add the guest portal to.

NOTE:

- To select a site-specific WLAN, navigate to **Site > WLANs**, and then click the WLAN.
- To select a template-based WLAN, navigate to **Organization > WLAN Templates**, click the template, and then click the WLAN.

2. Scroll down to the **Guest Portal** section and select **Custom guest portal**.
3. Select **Configure Portal**.
4. Select the **Authorization** tab at the top of the window.
5. Select **Azure Sign In**, and then enter the **Client ID**, **Secret ID** (copied from the Value field in Azure), and **Tenant ID** that you obtained from the Azure portal.

Guest Portal Options

×

Form Fields

Customize Label

Customize Layout

Authorization

Authorization Options


Users will be able to sign in with any of the selected authorization methods. If none are selected users may sign in without authorization.


☐ Passphrase [Reveal](#)


☐ Authentication code via Email


☐ Authentication code via Text Message


☐ Sponsored Guest Access

☐  Google Sign In

☐  Facebook Sign In

☐  Amazon Sign In

☐  Microsoft Sign In

☒  Azure Sign In

Client ID

Secret ID

Tenant ID

Authorization Settings

Devices remain authorized for

Days ▾

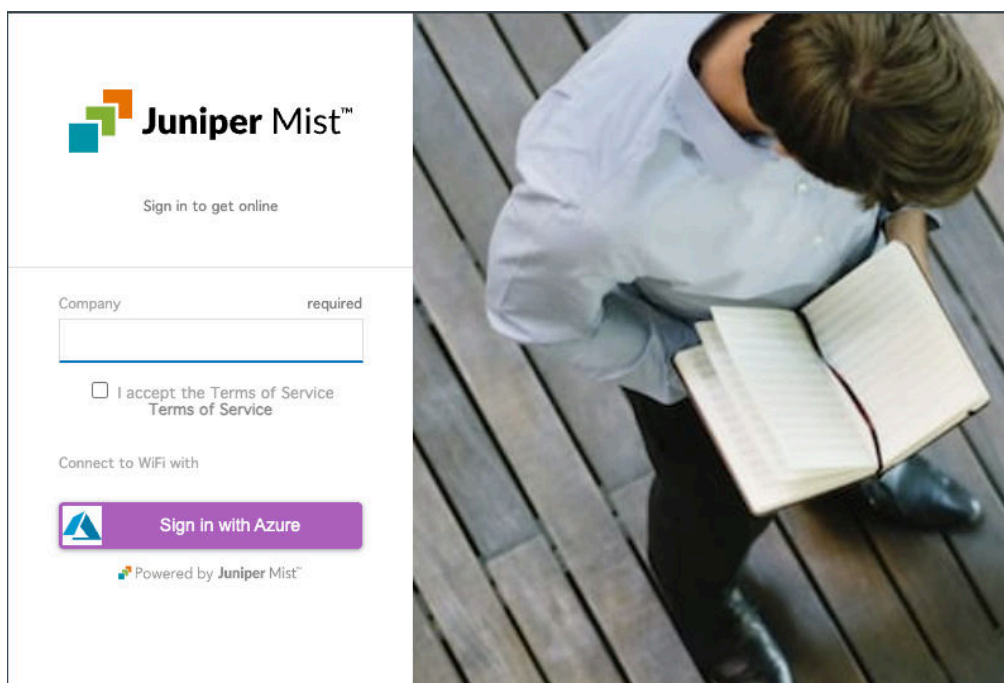
☐ After authorization redirect to URL

[Preview Guest Portal](#)

OK

Cancel

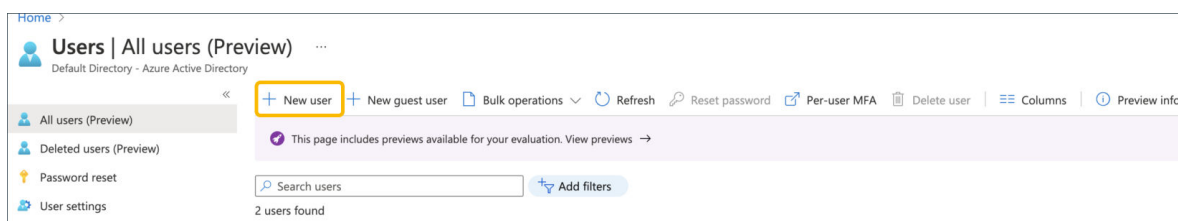
6. Click **OK** on the Guest Portal Options window, then click **Save** on the Edit WLAN window. .
7. You will see this pop up when connecting to the wireless network. **Enter your Company name** to assist with authentication, **accept the terms and conditions**, and then select **Sign in with Azure**. Once credentials are validated, click **Done**.



Add a new guest user in Azure

If you receive an error similar to "User account 'abc@mist.com' from identity provider doesn't exist in the tenant 'Microsoft services'", this means you need to add the user in your Azure portal. The following steps explain how to achieve this. The next section explains how to then assign an application to the guest user.

1. Log in to the [Azure Portal](#) as an administrator.
2. Select **Azure Active Directory** or **Microsoft Entra ID**.
3. Under **Manage**, select **Users**.
4. Click **New user**.



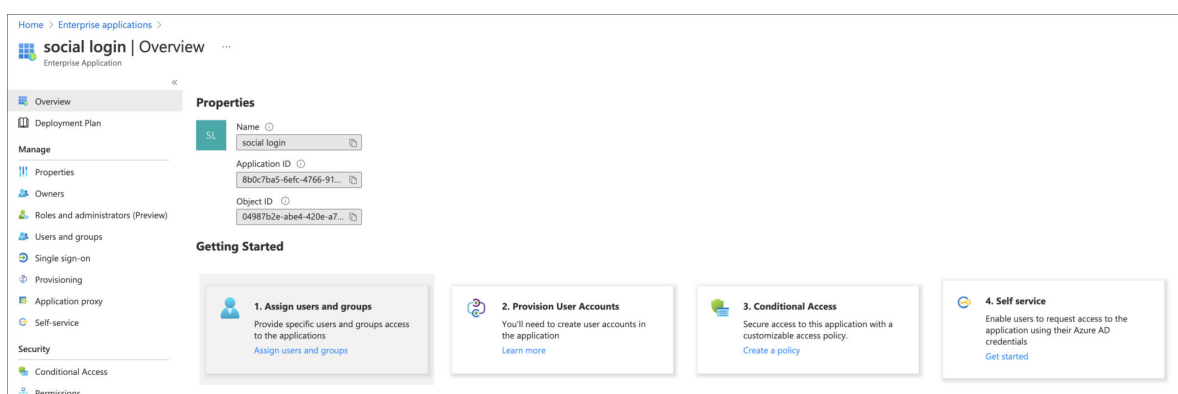
5. On the **New user** page, select **Invite user** and then add the guest user's information.
 - **Name** – This is the first and last name of the guest user.
 - **Email address (required)** – Enter the email address of the guest user.
 - **Personal message (optional)** – Include a personal welcome message that will display for the guest user.

6. Select **Invite** to automatically send the invitation to the guest user. A notification appears in the upper right with the message **Successfully invited user**. After you send the invitation, the user account will automatically be added to the directory as a guest.

Assign an application to the guest user

Next, assign an application to the guest user. For example, you can add the Salesforce app to your test tenant and assign the test guest user to the app.

1. Sign in to the Azure portal as an administrator.
2. From the left pane, select **Enterprise applications**.
3. Select **application**, then in the **Add from the gallery** section, search for **Social Login**, and then select it.



4. Select **Add**. Then, under the **Manage** section, select **Single sign-on**, and under **Single Sign-on Mode**, select **Password-based Sign-on**, and click **Save**.
5. Under **Manage**, select **Users and groups** > **Add user** > **Users and groups**.
6. Use the search box to search for the test user you created (if necessary) and select the test user from the list. Then click **Select**.
7. Finally, click **Assign** to assign the app to the guest user.
8. Now sign in as the guest user to accept the invitation by signing in to your test guest user's email account.
 - a. In the test user's inbox, find the "You're invited" email and in that email, select **Get Started**.
 - b. A Review permissions page opens in the browser. Select **Accept**. The Access Panel opens which lists the applications the guest user can access.

RELATED DOCUMENTATION

[Register a client application in Microsoft Entra ID](#)

[Add a guest user to the Azure Active Directory](#)

[Invite the guest user to an app in Azure](#)

Use an External Portal for Guest Access

SUMMARY

Enable an external portal if you want guests to go to a sign-in portal that your web developers have designed on your own website.

IN THIS SECTION

- [Use PHP and Read-Me files to Create Your External Portal | 180](#)

An external portal is a webpage that your WLAN users see after they select your SSID. For example, you can send guests to your company's home page or a sign-in portal that your web developers have set up specifically for your organization.

For added security, you can specify authorized users, allowed subnets, and allowed hostnames. You also can enter a list of hostnames to block.

1. Navigate to the WLAN.

NOTE:

- If the WLAN is in a WLAN template, select **Organization > Wireless | WLAN Templates**, click the template, and then click the WLAN.
- For a site-level WLAN, select **Site > Wireless | WLANs**, and then click the WLAN.

2. In the Edit WLAN window, under **Guest Portal**, click **Forward to external portal**.

Edit WLAN

Portal URL must start with http:// or https://

Guest Portal

☐ No portal (go directly to internet)
☐ Custom guest portal
☒ Forward to external portal

[Edit Guest Authorization](#)

Portal URL

Allowed Subnets

Allowed Hostnames

Hostname Exceptions
 Block access to these hostnames, even if the parent domain is allowed

API Secret

☐ SSO with Identity Provider
☒ Bypass guest/external portal in case of exception

3. (Optional) Click the **Edit Guest Authorization** button if you want to limit access to specific users. Then complete these steps:

a. In the Authorized Guests window, click **Add**.

Authorized Guests ✕

<input checked="" type="checkbox"/>	Authorization Time	Expiration Time	MAC Address	Name	Mobile	Carrier	Auth Method	Role	Email Address	Sponsor Email Address
There are no authorized guests										

[Add](#) [Edit](#) [Unauthorize](#) [Cancel](#)

b. On the Authorize Guest window, enter the guest's **MAC Address** (required), optional user information, and the period that the user remains authorized.

NOTE: You can use the **Search Client** option to search for a client that is already connected to the WLAN.

- c. Click **Authorize** at the bottom of the Authorize Guest window.
- d. Repeat these steps to add more guests to the list.
4. Enter the Portal URL, beginning with http:// or https://.

NOTE: Use the other fields to finetune access. For example, allow only certain subnets or hostnames.

5. Select or clear the **Bypass guest/external portal in case of exception** check box.
When this feature is selected, each access point will try to reach the portal or IdP, but if it is not reachable then the AP will automatically authorize the guests to connect to the WLAN.
6. Click **Save** at the bottom of the Edit WLAN window.

Use PHP and Read-Me files to Create Your External Portal

1. Create your external portal by referring to the following sample PHP files and Read-Me Information.

index.php

```

<?php
    /*
        These parameters are sent by Mist on the 302 redirect to this portal page:
        wlan_id - WLAN object's UUID
        ap_mac - MAC address of the AP
        client_mac - MAC address of the client device
        url - Originally requested url by the client, ie: http://www.mist.com
        ap_name - Name of the AP
        site_name - Name of the Site

        If you want to send the guest to a content page after authorization, configure the $url
        instead of using the valued that is passed as a parameter.
    */

    $wlan_id = $_GET['wlan_id'];
    $ap_mac = $_GET['ap_mac'];
    $client_mac = $_GET['client_mac'];
    $url = $_GET['url'];
    $ap_name = $_GET['ap_name'];
    $site_name = $_GET['site_name'];
?>

<html>
    <body>
        <form action="authme.php" method="post">
            <input type="hidden" name="wlan_id" value="<?php echo($wlan_id) ?>" />
            <input type="hidden" name="ap_mac" value="<?php echo($ap_mac) ?>" />
            <input type="hidden" name="client_mac" value="<?php echo($client_mac) ?>" />
            <input type="hidden" name="url" value="<?php echo($url) ?>" />
            <input type="hidden" name="ap_name" value="<?php echo($ap_name) ?>" />
            <input type="hidden" name="site_name" value="<?php echo($site_name) ?>" />

            <table>
                <tr>
                    <td><b>Your Full Name</b></td>
                    <td><input type="text" name="name" /></td>
                </tr>
                <tr>
                    <td><b>Your Email Address</b></td>
                    <td><input type="text" name="email" /></td>
                </tr>
            </table>
        </form>
    </body>
</html>

```



```

        </tr>
        <tr>
            <td><input type="submit" value="Login" /></td>
        </tr>
    </table>
</form>
</body>
</html>

```

authme.php

```

<?php
    $secret = ''; // WLAN API Key, obtained from the Mist Web GUI after creating the WLAN
    $wlan_id = $_POST['wlan_id'];
    $ap_mac = $_POST['ap_mac'];
    $client_mac = $_POST['client_mac'];
    $url = $_POST['url'];
    $ap_name = $_POST['ap_name'];
    $site_name = $_POST['site_name'];

    $authorize_min = 525600; // Duration (in minutes) the guest MAC address is authorized
    before they are redirected back to the portal page
    $download_kbps = 0; // Download limit (in kbps) per client. Recommended to leave as 0
    (unlimited), as this can be set globally in the WLAN
    $upload_kbps = 0; // Upload limit (in kbps) per client. Recommended to leave as 0
    (unlimited), as this can be set globally in the WLAN
    $quota_mbytes = 0; // Quota (in mbytes) per client. Recommended to leave as 0 (unlimited)
    $context = sprintf('%s/%s/%s/%d/%d/%d/%d',
        $wlan_id, $ap_mac, $client_mac,
        $authorize_min,
        $download_kbps, $upload_kbps, $quota_mbytes
    );
    $token = urlencode(base64_encode($context));

    // The below portal fields are passed back to Mist and shown in the Guest Portal
    Information
    $name = $_POST['name'];
    $email = $_POST['email'];
    $field1 = 'Whatever you want Custom field 1 to be';
    $field2 = 'Whatever you want Custom field 2 to be';
    $field3 = 'Whatever you want Custom field 3 to be';
    $field4 = 'Whatever you want Custom field 4 to be';

```



```

$forward = urlencode($url); // URL the user is forwarded to after authorization
$extra = '&forward=' . $forward;
$extra .= '&name=' . urlencode("$name");
$extra .= '&field1=' . urlencode("$field1");
$extra .= '&field2=' . urlencode("$field2");
$extra .= '&field3=' . urlencode("$field3");
$extra .= '&field4=' . urlencode("$field4");
$extra .= '&email=' . urlencode("$email");
$expires = time() + 120; // The time until which the authorization URL is valid
$payload = sprintf('expires=%d&token=%s%s', $expires, $token, $extra);

$signature = urlencode(base64_encode(hash_hmac('sha1', $payload, $secret, true)));
$final_url = sprintf('http://portal.mist.com/authorize?signature=%s&%s', $signature,
$payload);

/*
    Debug code used for testing purposes only
    If set to true, display the variable details without authorizing the guest in the Mist
cloud
*/
$debugging = false;
if ($debugging) {
    header('Content-Type: text/plain');
    echo sprintf('token          : urlencode(base64(%s))', $context) . PHP_EOL;
    echo sprintf('          %s', $token) . PHP_EOL;
    echo sprintf('foward          : %s', $url) . PHP_EOL;
    echo sprintf('          %s', $foward) . PHP_EOL;
    echo sprintf('payload-to-sign: %s', $payload) . PHP_EOL;
    echo sprintf('signature       : %s', $signature) . PHP_EOL;
    echo sprintf('URL             : %s', $final_url) . PHP_EOL;
    echo sprintf('client_mac      : %s', $client_mac) . PHP_EOL;
    echo sprintf('ap_mac          : %s', $ap_mac) . PHP_EOL;
    echo sprintf('ap_name         : %s', $ap_name) . PHP_EOL;
    echo sprintf('wlan_id         : %s', $wlan_id) . PHP_EOL;
    echo sprintf('site_name       : %s', $site_name) . PHP_EOL;
    echo sprintf('name            : %s', $name) . PHP_EOL;
    echo sprintf('email           : %s', $email) . PHP_EOL;
    echo sprintf('field1          : %s', $field1) . PHP_EOL;
    echo sprintf('field2          : %s', $field2) . PHP_EOL;
    echo sprintf('field3          : %s', $field3) . PHP_EOL;
    echo sprintf('field4          : %s', $field4) . PHP_EOL;
}

```



```

    else {
        // Guest is redirected to the Mist portal for authorization. If successful, the Mist
        portal will then redirect the guest to the $url
        header('Location: ' . $final_url);
    }
?>

```

Read-Me Information

This sample code shows how to use the PHP POST method to pass the below parameter values from the landing page (index.php) to the authorization page (authme.php). The authorization page will also request the user to provide some information.

Authorization HOW-TOs

=====

Syntax: signature=<signature>&expires=<epoch-seconds>&token=<token>&forward=<forward>

Note: Wired captive portal does not support this mechanism, please use the JWT based one.

<forward>: url to forward the user to after authorization

<token>: base64("wlan-id/ap-mac/client-mac/authorize_min/0/0/0")

<signature>: base64(hmac_sha1(<secret>, "expires=..."))

Example

token : urlencode(base64("be22bba7-8e22-e1cf-5185-b880816fe2cf/5c5b35001234/d58f6bb4c9d8/480/0/0/0")) =

YmUyMmJiYTctOGUyMi1lMWNmLTUxODUtYjg4MDgxNmZlMmNmLzVjNWlZNTAwMTIzNC9kNTNmJiNGM5ZDgvNDgwLzAvMC8w

expires : 1768587994

forward : urlencode("http://www.mist.com")
http%3A%2F%2Fwww.mist.com%2F

payload-to-sign:

expires=1768587994&token=YmUyMmJiYTctOGUyMi1lMWNmLTUxODUtYjg4MDgxNmZlMmNmLzVjNWlZNTAwMTIzNC9kNTNmJiNGM5ZDgvNDgwLzAvMC8w&forward=http%3A%2F%2Fwww.mist.com%2F

secret : test-secret (only used by /authorize-test for testing purpose)

signature : J7VJlf2Zlcs%2B0xhVxCf8hL0XYC0%3D

final URL : http://portal.mist.com/authorize-test?signature=J7VJlf2Zlcs


```
%2B0xhVxCf8hL0XYC0%3D&expires=1768587994&token=YmUyMmJiYTct0GUyMi1lMWNmLTUxODUtYjg4MDgxNmZlMmNmLzVjNWIZNTAwMTIzNC9kNThmNmJiNGM5ZDgvNDgwLzAvMC8w&forward=http%3A%2F%2Fwww.mist.com%2F
```

Alternatively, you can use JWT tokens:

Syntax: jwt=<jwt token>

Payload:

```
{
  "ap_mac": "5c5b35001234",
  "wlan_id": "be22bba7-8e22-e1cf-5185-b880816fe2cf",
  "client_mac": "d58f6bb4c9d8",
  "minutes": 480,
  "expires": 1768587994,
  "forward": "http://www.mist.com",
  "authorize_only": false
}
```

Notes:

authorize_only: if true and authorization is successful, 200 OK will be returned instead of 302 Redirect the user to the `forward` URL

Example

```
...

import jwt

secret = "test-secret"
payload = {
    "ap_mac": "5c5b35001234",
    "wlan_id": "be22bba7-8e22-e1cf-5185-b880816fe2cf", # only for _wireless_ captive portal
    "site_id": "ce22bba7-8e22-e1cf-5185-b880816fe2ce", # only for _wired_ captive portal"
    "port_name": "eth0", # only for _wired_ captive portal"
    "client_mac": "d58f6bb4c9d8",
    "minutes": 480,
    "expires": 1768587994,
    "forward": "http://www.mist.com",
    "authorize_only": False
}

encoded_jwt = jwt.encode(payload, secret, algorithm='HS256')
...
```



```

encoded_jwt:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdXRob3JpemVfb25seSI6ZmFsc2UsImV4cGlyZXMjE3Njg1ODc5ODQsImFwX21hYyI6IjVjNWl3NTAwMTIzNCIsImZvcndhcmQiOiJodHRwOi8vd3d3Lm1pc3QuY29tIiwiaWY2xpZW50X21hYyI6ImQ1OGY2YmI0YzlkOCIsIm1pbnV0ZXMiOjQ4MCwid2xhbl9pZCI6ImJlMjJiYmE3LTlmjItZTFjZi0MTg1LWI4ODAwMTZmZTJjZiJ9.msBloHe05XzbzaMEqjsi8XSNWa_3uc--4wucKz3dQGk
final URL : http://portal.mist.com/authorize-test?
jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdXRob3JpemVfb25seSI6ZmFsc2UsImV4cGlyZXMjE3Njg1ODc5ODQsImFwX21hYyI6IjVjNWl3NTAwMTIzNCIsImZvcndhcmQiOiJodHRwOi8vd3d3Lm1pc3QuY29tIiwiaWY2xpZW50X21hYyI6ImQ1OGY2YmI0YzlkOCIsIm1pbnV0ZXMiOjQ4MCwid2xhbl9pZCI6ImJlMjJiYmE3LTlmjItZTFjZi0MTg1LWI4ODAwMTZmZTJjZiJ9.msBloHe05XzbzaMEqjsi8XSNWa_3uc--4wucKz3dQGk

```

NOTE: Replace `portal.mist.com` with the appropriate Guest Wi-Fi Portal URL based on the cloud instance in which your Mist organization was created. To look up the Guest Wi-Fi Portal URL for your region, see the [Mist Cloud IP Addresses and Ports information](#) in the Juniper Mist Management Guide.

2. To get the value that you need for `$secret` in `auth.php`, reopen the Edit WLAN window, and copy the **API Secret**.
3. Configure your authorization page (`authme.php`) to call the Juniper Mist backend with the required query string parameters: `?signature=signature&expires=expires&token=token&optional`
 - *expires* – The epoch timestamp until which the authorization URL is valid.
 - For example: 1768587994 (This means the authorization URL would expire on January 16, 2026 at 6:26:34 PM UTC.)
 - *token* – A base64 string having format: `wlan_id/ap_mac/client_mac/authorize_min/0/0/0`
 - For example: `be22bba7-8e22-e1cf-5185-b880816fe2cf/5c5b35001234/d58f6bb4c9d8/480/0/0/0`
 - *signature* – A base64 string of hashed values, using sha1 as the hashing algorithm and the Guest WLAN's API Secret as the key. This would have the following format:
 - `expires=expires&token=token&optional`
 - For example: `J7VJlf2Zlcs%2BOxhVxCf8hLOXYC0%3D`
 - *optional* – The optional guest details and the URL to which the user is forwarded after authorization, having the following format:
 - `forward=url&name=name&email=email&company=company&field1=field1&field2=field2&field3=field3&field4=field4`

Note: Ensure all parameter values are passed as base64.

- For example: forward=http%3A%2F%2Fwww.mist.com%2F
4. Configure your authorization page to call Juniper Mist for guest authorization. The final authorization URL would look something like this: `http://portal.mist.com/authorize?signature=J7VJ1f2Zlcs%2B0xhVxCf8hL0XYC0%3D&expires=1768587994&token=YmUyMmJiYTctOGUyMi1lMWNmLTUxODUtYjg4MDgxNmZlMmNmLzVjNWIZNTAwMTIzNC9kNThmNmJiNGM5ZDgvNDgwLzAvMC8w&forward=http%3A%2F%2Fwww.mist.com%2F`
 5. Test the external captive portal by connecting a device and attempting to authenticate. The device should be redirected to the Juniper Mist portal for authorization. If authentication is successful, the user will be redirected to the URL as defined in your external captive portal code.

NOTE: Use /authorize for the live portal. For testing purposes, you can use /authorize-test, which requires the dummy example values as provided in the Read-Me Information.

Use an Identity Provider for Guest Access

SUMMARY

If you want to give your guests Single Sign-On access, set up an integration with your Identity Provider.

IN THIS SECTION

- [Use Microsoft® Azure for Guest Portal Single Sign-On | 190](#)
- [Enable Guest Portal Single Sign-On Access with OneLogin™ | 194](#)

To use an Identity Provider for guest access:

1. In your IdP admin portal (such as Microsoft Entra ID or OneLogin), create a SAML 2.0 application, set the signature algorithm to SHA-256, add your roles and users, and then copy your new application's identifier and login URL.

As you go through this procedure, you'll go back and forth between your IdP admin portal and the Juniper Mist portal to complete the necessary fields on both sides. For example:

- From your IdP admin portal, you'll need your application's identifier (such as application ID or issuer URL) and your application's URL/endpoint to complete the guest portal configuration in the Juniper Mist portal.
- From the Juniper Mist portal, you'll need your Portal SSO URL to complete the application configuration in your IdP admin portal.

2. Navigate to the WLAN.

NOTE:

- If the WLAN is in a WLAN template, select **Organization > Wireless | WLAN Templates**, click the template, and then click the WLAN.
- For a site-level WLAN, select **Site > Wireless | WLANs**, and then click the WLAN.

3. In the Edit WLAN window, select **Open Access** as the security type.

4. Under **Guest Portal**, click **SSO with Identity Provider**.

5. Enter the first set of information that you need to provide for your SSO application, as shown below.

- **Issuer**—Enter your application's identifier (such as application ID or issuer URL).

- **SSO URL**—Enter your application's URL/endpoint.
 - **Certificate**—Enter some placeholder text, such as the word *certificate*. Later in this procedure, you'll enter your application's actual certificate.
6. Click **Save** at the bottom of the Edit WLAN window.
You need to save the configuration so that Juniper Mist can generate the Portal SSO URL for the next step.
 7. Click the WLAN to reopen the Edit WLAN window, and then copy the **Portal SSO URL**.
The **Portal SSO URL** and Copy button appear near the end of the SSO section.

8. Keep the Edit WLAN window open because you'll need to add the actual certificate later in this procedure.
9. In your IdP admin portal, finish configuring your application by entering the **Portal SSO URL** and downloading your application's certificate.
Refer to your IdP documentation for help configuring your application.

10. Copy the contents of your application's certificate and paste it into the **Certificate** field in the Edit WLAN window.
11. Enter other settings as needed.
For example, you can enter authorized roles, subnets, and hostnames.
12. Select or clear the **Bypass guest/external portal in case of exception** check box.
When this feature is selected, each access point will try to reach the portal or IdP, but if it is not reachable then the AP will automatically authorize the guests to connect to the WLAN.
13. Click **Save** at the bottom of the Edit WLAN window.

Test your configuration by connecting to the WLAN. You should be redirected to your IdP's sign-in form to get access.

Use Microsoft® Azure for Guest Portal Single Sign-On

SUMMARY

Use this information if you want to integrate with Microsoft® Azure to authenticate guest users.

When you configure a WLAN in the Juniper Mist™ portal, you can set up a guest portal that allows users to sign on by using an Identity Provider (IdP). This topic provides tips for using Microsoft® Azure. You'd follow similar steps for other IdPs.

Set up your application in Microsoft Entra ID (previously Azure Active Directory):

- Set up an application in Microsoft Entra ID (Azure AD) with single sign-on enabled.
- Choose SAML (Security Assertion Markup Language) as the single sign-on method.
- Copy and save the Microsoft Entra Identifier (Azure ID Identifier) and the Login URL.
- Add Users or Groups and assign them to the application so that they will be able to authenticate via the SSO application.

NOTE: If you need help adding a SAML application in Entra, consult your Microsoft support information. For example, consider this topic on the Microsoft site: [How to Enable single sign-on for an enterprise application](#).

To set up your guest portal SSO with Azure:

1. In your WLAN configuration, select **SSO with Identity Provider**, as described in ["Use an Identity Provider for Guest Access"](#) on page 187.
2. Enter the information you obtained from Microsoft Entra in the **Issuer** and **SSO URL** fields.

Edit WLAN

SSO URL must start with http:// or https://

☐ Hide SSID
☐ Broadcast AP name

Radio Band
☒ 2.4 GHz ☒ 5 GHz ☐ 6 GHz

Band Steering
☐ Enable

Client Inactivity
 Drop inactive clients after seconds: 1800

Geofence
☐ Minimum client RSSI (2.4G) 0
☐ Minimum client RSSI (5G) 0
☐ Minimum client RSSI (6G) 0
 Block clients having RSSI below the minimum

Data Rates
☒ Compatible (allow all connections)
☐ No Legacy (2.4G, no 11b)
☐ High Density (disable all lower rates)
☐ Custom Rates

WiFi Protocols

Guest Portal
☐ No portal (go directly to internet)
☐ Custom guest portal
☐ Forward to external portal
☒ SSO with Identity Provider
 Edit Guest Authorization

Issuer
 https://sts.windows.net/255d31b5-3f25-457a-b6ed → **Azure ID Identifier**

Name ID Format
☒ Email ☐ Unspecified

Signing Algorithm
 SHA1

Certificate
 1

SSO URL
 https://login.windows.net/255d31b5-3f25-457a-b6ed → **Login URL**

☐ Override IDP role, replacing it with:
 Default role (if not provided by IDP):
 Devices remain authorized for 1 Days
☐ After authorization redirect to URL
 Allowed Subnets
 Allowed Hostnames

Delete Save Cancel

3. Fill in the **Certificate** field (you can fill this in with random information for now).
4. Click **Save**.
 The Portal SSO URL is generated.
5. Copy and save the Portal SSO URL.

Edit WLAN

Client Inactivity
Drop inactive clients after seconds: 1800

Geofence
☐ Minimum client RSSI (2.4G) 0
☐ Minimum client RSSI (5G) 0
☐ Minimum client RSSI (6G) 0
 Block clients having RSSI below the minimum

Data Rates
☒ Compatible (allow all connections)
☐ No Legacy (2.4G, no 11b)
☐ High Density (disable all lower rates)
☐ Custom Rates

WiFi Protocols
WiFi-6 ☒ Enabled ☐ Disabled

WLAN Rate Limit
☐ Limit uplink to 10 Mbps
☐ Limit downlink to 20 Mbps

Issuer
 https://login.microsoftonline.com/235a2715b1-8025-4d79-a8b1-...

Name ID Format
☒ Email ☐ Unspecified

Signing Algorithm
SHA1

Certificate
1

SSO URL
 https://login.microsoftonline.com/235a2715b1-8025-4d79-a8b1-...

☐ Override IDP role, replacing it with:

Default role (if not provided by IDP):

Devices remain authorized for 1 Days

☐ After authorization redirect to URL

Allowed Subnets

Allowed Hostnames

Hostname Exceptions
 Block access to these hostnames, even if the parent domain is allowed

Portal SSO URL
 Portal SSO URL will be generated after saving the WLAN.

☒ Bypass guest/external portal in case of exception

Delete Save Cancel

6. Go to the Microsoft Entra portal and complete these tasks:
 - Edit the Basic SAML Configuration you created for Juniper Mist and paste the Portal SSO URL into the **Identifier**, **Reply URL**, and **Sign on URL** fields. Click **Save**.
 - Edit the **User Attributes & Claims** section.
 - Delete the claims ending in **"/emailaddress"** and **"/name"**.
 - Edit the **"givenname"** claim. Clear the contents of the **Namespace** field, then change the **Name** field to **"FirstName"**.
 - Edit the **"surname"** claim. Clear the contents of the **Namespace** field, then change the **Name** field to **"LastName"**.
 - Navigate back to the SAML configuration page and edit the SAML Signing Certificate.
 - In the Signing Option field, select **Sign SAML** response and assertion.

- Click **Save**.
- Download the **Base 64 Certificate**.
- Open the certificate as a text file and copy its contents.

7. In the Juniper Mist portal, navigate to the WLAN.

NOTE:

- If the WLAN is in a WLAN template, select **Organization > Wireless | WLAN Templates**, click the template, and then click the WLAN.
- For a site-level WLAN, select **Site > Wireless | WLANs**, and then click the WLAN.

8. Select **SHA256** for the **Signing Algorithm** and paste the contents of the certificate into the **Certificate** field.
9. You can optionally configure the **Default role** field with **Guest** for guest authorization.
10. Add the Microsoft FQDNs into the **Allowed Hostnames** field to allow the guest clients to authenticate.

Edit WLAN ✕

Microsoft account is an invalid hostname

Client Inactivity

Drop inactive clients after seconds:

Geofence

☐ Minimum client RSSI (2.4G)

☐ Minimum client RSSI (5G)

☐ Minimum client RSSI (6G)

Block clients having RSSI below the minimum

Data Rates

☒ Compatible (allow all connections)

☐ No Legacy (2.4G, no 11b)

☐ High Density (disable all lower rates)

☐ Custom Rates

WiFi Protocols

WiFi-6 ☒ Enabled ☐ Disabled

WLAN Rate Limit

☐ Limit uplink to Mbps

☐ Limit downlink to Mbps

Per-Client Rate Limit

☒ SSO with Identity Provider

[Edit Guest Authorization](#)

Issuer

Name ID Format
☒ Email ☐ Unspecified

Signing Algorithm
SHA256

Certificate
-----BEGIN CERTIFICATE-----
MIIC8DCCAdigAwIBAgIQEYFQ8lwZZ6INSEGTryzH9

SSO URL

☐ Override IDP role, replacing it with:

Default role (if not provided by IDP):

Devices remain authorized for Days

☐ After authorization redirect to URL

Allowed Subnets

Allowed Hostnames

Hostname Exceptions
Block access to these hostnames, even if the parent domain is allowed

Portal SSO URL

Delete Save Cancel

For a complete list of the necessary Microsoft FQDNs, refer to your Microsoft documentation. Our suggestions include: login.microsoftonline.com, mobileappcommunicator.auth.microsoft.com, aadcdn.msauth.net, aadcdn.msftauth.net, Microsoft account , aadcdn.msauthimages.net, autologon.microsoftazuread-sso.com, msftconnecttest.com.

Enable Guest Portal Single Sign-On Access with OneLogin™

SUMMARY

Use this information if you want to integrate with OneLogin™ to authenticate guest users.

When you configure a WLAN in the Juniper Mist™ portal, you can set up a guest portal that allows users to sign on by using an Identity Provider (IdP). This topic explains how to set up a guest portal SSO with OneLogin. You'd follow similar steps for other IdPs.

Before completing these steps, go to your OneLogin portal and set up a SAML application to be used for SSO with this guest portal.

- Set the SAML Signature Algorithm to **SHA-256**.
- Copy and save the **Issuer URL**, the **SAML 2.0 Endpoint**, and the **X.509 Certificate**. You'll need this information to complete your guest portal configuration in the Juniper Mist portal.

NOTE: If you need help adding a SAML application in OneLogin, consult your OneLogin support information. For example, consider this topic on the OneLogin site: [Configuring SSO for SAML-Enabled Applications](#).

To enable guest portal SSO access with OneLogin™:

1. In your WLAN configuration, select **SSO with Identity Provider**, as described in "[Use an Identity Provider for Guest Access](#)" on page 187.
2. Use your OneLogin application's information to complete the following fields:
 - **Issuer**—Paste the Issuer URL for your OneLogin application.
 - **SSO URL**—Paste the SAML 2.0 Endpoint for your OneLogin application.
 - **Certificate**—Paste the X.509 Certificate for your OneLogin application.
 - **Signing Algorithm**—Select **SHA-256**.
 - Select the **After authorization redirect to URL** check box and then enter: **http://juniper.net**

Guest Portal

- ☐ No portal (go directly to internet)
- ☐ Custom guest portal
- ☐ Forward to external portal
- ☒ SSO with Identity Provider

Issuer

`https://app.onelogin.com/saml/metadata/b17170`

Name ID Format

- ☒ Email ☐ Unspecified

Signing Algorithm

SHA256 ▼

Certificate

`Es3a7/loI/nabaoil/gl
-----END CERTIFICATE-----`

SSO URL

`boost/sso/b1717045be-7a88-4848-9c81-97cd4c57`

☐ Override IDP role, replacing it with:

Default role (if not provided by IDP):

Devices remain authorized for

1

Days ▼

☒ After authorization redirect to URL

`http://juniper.net`

3. If this is a new WLAN, enter any other necessary information for your WLAN.

NOTE: For help configuring a WLAN in Juniper Mist, see ["Configure a WLAN Template" on page 119](#).

4. At the bottom of the Create/Edit WLAN window, select **Save** (if you're editing an existing WLAN) or **Create** (if you're creating a new WLAN).
5. Reopen the Edit WLAN window by clicking the WLAN that you just edited/created.
6. Copy and save the **Portal SSO URL** that was generated near the bottom of the Guest Portal section.
7. Keep the Edit WLAN window open because you'll return to it later in this procedure.
8. In your OneLogin portal, open your SAML application, and complete these steps:
 - a. Paste your **Portal SSO URL** into the following fields:
 - **RelayState**
 - **Audience (EntityID)**
 - **Recipient**
 - **ACS (Consumer) URL Validator***
 - **ACS (Consumer) URL**
 - **Login URL**
 - b. For the **SAML signature element**, select **both**.
This will ensure that the SAML signature element is in both the assertion and the response.
 - c. Save the changes to your application.

NOTE:
[Advanced SAML Custom Connector](#)

- d. Apply the application to your users who need to access your new guest portal.
You can optionally enter the user's email address in the username field. If you choose to do that, make sure you select **Email** as the **Name ID Format** in the guest portal configuration.

NOTE:
[Manually Assign Apps to Users](#)

9. In the Juniper Mist portal, return to the Edit WLAN window.

10. Enter the **Allowed Hostnames** for your OneLogin users.

This step is necessary so that the page properly populates when a user is redirected to OneLogin to log in. You can do a packet capture to see the hostnames.

11. Click **Save** at the bottom of the Edit WLAN window.

12. Click **Save** at the top right corner of the WLAN Templates page.

You can verify that everything is working correctly by logging out of the OneLogin portal, then, join the OneLogin SSO Wi-Fi Network you just created. You should be redirected to the OneLogin splash page where you can enter your login credentials.

If you can login successfully and are redirected to the Juniper homepage, you have successfully set up SSO with OneLogin.

Authorize, Reauthorize, and Reconnect Guest Clients

Users with helpdesk-level login credentials or higher can track and manage Wi-Fi clients on the **Clients > WiFi Clients | Guest** tab of the Juniper Mist™ portal. Here you can find, authorize, deauthorize, and reconnect client devices on the network.

- **Reconnect**—Have the AP send a deauthentication frame to the selected clients, thereby removing them from the guest client list and triggering a reconnect. This is typically used to nudge the device to roam to another AP.
- **Reauthorize**—Log selected clients off the guest portal, thereby forcing them to re-authenticate with the AP and cloud. This is typically used after updating the guest-portal passphrase, to force client on to the new credentials. These clients are removed from the guest client list and must log in to the guest portal again.

• Figure 9: Reconnect and Reauthorize

Monitor

Marvis™

Clients

Access Points

Switches

WAN Edges

Mist Edges

Location

Analytics

Site

Organization

< Guest Clients : iPad Pro 11" (3rd Gen)

Name

iPad Pro 11" (3rd Gen)

Labels

+

Statistics

	Insights	Client Insights
RX PHY Rate		573.5 Mbps
TX PHY Rate		24 Mbps
RX Bit Rate		77.3 kbps
TX Bit Rate		18.5 kbps
Total Bytes		55.9 MB
RX Bytes		24.3 MB
TX Bytes		31.6 MB
Total Packets		696.5 k
RX Packets		17.0 k
TX Packets		679.5 k
Total Retries		7.5 k
RX Retries		68
TX Retries		7.5 k

Guest Portal Information

Name	
Mobile	
Carrier	
Auth Method	Passphrase
Role	
Email	matt@mm.com
Company	
Sponsor Email	

Properties

MAC

H

U

De

Man

Operatin

Status

Conne

IPv

IPv

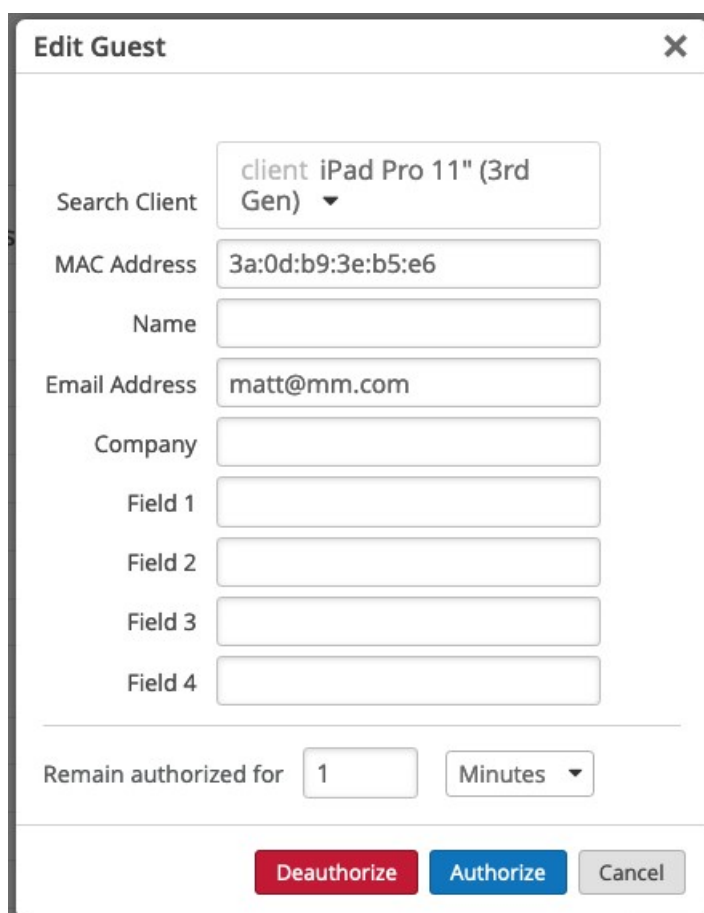
Association

Acc

Pre-sh

To get here, click **Clients > WiFi Clients**. Select the **Guest** tab, then select a single client from the list that appears.

- **Edit Guest Authorization**—Appears after selecting a single Guest client. You can find a given client by its MAC address, and then manually **Authorize** or **Deauthorize** the device on the Guest network. This selection also provides a way to change the client's authorization window and other details that appear in the **Guest Clients** page of the Mist portal.



Edit Guest [X]

Search Client: client iPad Pro 11" (3rd Gen) ▼

MAC Address: 3a:0d:b9:3e:b5:e6

Name: []

Email Address: matt@mm.com

Company: []

Field 1: []

Field 2: []

Field 3: []

Field 4: []

Remain authorized for: 1 [Minutes ▼]

[Deauthorize] [Authorize] [Cancel]

FAQs: Guest Portal

IN THIS SECTION

- Why is the captive portal (or splash page) not coming up when I try to access the wireless network? | 201

Why is the captive portal (or splash page) not coming up when I try to access the wireless network?

This could be caused by a few issues. If the splash page is not coming up when you try to access the wireless network, try the following suggestions:

- Ensure that the Mist Portal FQDN (<http://portal.mist.com>) is permitted through the customer firewall. For more information, see [Juniper Mist Firewall Ports and IP Addresses for Firewall Configuration](#).
- Verify that the client has a valid and working DNS entry, which is needed to resolve the client captive portal URL.
- Check the WLAN setting to see if the guest portal is configured correctly. You can use the custom guest portal option on the Mist WLAN page to design a splash page in the Mist Cloud. For more information, see [Add a Custom Guest Portal to a WLAN](#).
- Ensure that the client is receiving a valid IP address. To verify this, look for the client in the active Wi-Fi client list, and select it to see the details and client events.
- Use Marvis Conversational Assistant (if enabled) and troubleshoot <client mac address>.
- Ensure that you are connected to the correct SSID.
- Sometimes, Windows systems or Apple CNA browsers do not load the splash page automatically. In such cases, open a browser and try entering an HTTP URL such as <http://neverssl.com> manually. This applies if the client has an IP address.

If the above suggestions do not help, contact Mist support.

Note that the splash page might not come up if the guest is already authenticated.

See also: [Guest Network Does Not Work](#).

5

CHAPTER

Radio Management

[Templates and Device Profiles](#) | 203

[Radio Management](#) | 204

[Radio Management \(page\)](#) | 207

[Radio Settings \(RF Templates\)](#) | 213

[Radio Management \(dual-band\)](#) | 217

[Dual Band Usage Examples](#) | 219

[WLAN Changes That Reset The Radio](#) | 223

[Transmit Power Notation for Juniper APs](#) | 225

Templates and Device Profiles

You can configure RRM and other radio settings in several different places in the Mist portal, as well as on the Juniper APs. These include RF templates, device profiles, WLAN templates, and on the AP itself.

Having multiple edit points for the same setting can be confusing at first, but the long-term benefit is convenience and consistency. For example, you can configure a core set of site settings in an RF template, and then use a device profile to create exceptions for a subset of APs.

When the same settings exist in different places, the AP-specific settings have precedence, followed by those made in device profiles, and then RF templates. You can always override these defaults, and the Mist portal will prompt you whenever it detects a conflict.

- **RF Template**—(Organization > RF Templates) Model-specific settings for APs can be set from within the RF Template. AP-specific default settings are available for all AP models, for each radio band. Settings made here can apply to all APs in the organization.
 - You can also use multiple RF templates to cover different use cases within the same site.
 - You can also include various model-specific tweaks within the same RF template by selecting the model. You select the model from the Default Settings drop-down and make the change for that model only.
- **Device Profile**—(Organization > Device Profiles) Settings made in a device profile apply to all Juniper APs attached to the profile. This profile is applied to all Juniper APs of the same model. You use device profiles to configure and save a set of AP settings so they will be available for re-use on other APs within a site.
 - This comes in handy in large deployments where you want to apply the same profile settings to many APs.
 - When you associate an AP with a given device profile, the AP will automatically inherit the settings defined in that profile.
- **WLAN Template**—(Organization > WLAN Templates) Settings made to a WLAN template apply to all WLANs attached to that template.
- **WLAN**—(Site > WLANs) Settings made for a WLAN apply to that WLAN only.
- **Radio Management**—(Site > Radio Management | Radio Settings) Settings made here can over-ride those configured in a site-level RF template for the selected radio band and specified APs.
- **AP**—(Access Point | AP) Settings made at the device level apply to that AP only. As noted, you can also attach the AP to a device profile to inherit those settings, or get the settings from an RF Template attached to the site.

In the case of configuration conflicts, AP-specific settings have precedence, followed by those made in device profiles, and then RF templates. You can override these defaults. The Mist portal prompts you whenever it detects a conflict.

Dual Band Settings and RRM optimizations for 2.4-GHz and 5-GHz radios can be configured using:

- RF Template
- Device Profile
- AP Level

Radio Management

Juniper Mist AI-driven radio resource management (RRM) describes machine learning technology available in both Juniper APs and on the Juniper Mist cloud. RRM is enabled by default and most of the optimizations occur automatically, in the background.

On the cloud, RRM collects data from multiple APs in the WLAN or site, gathered as a part of ["Service Level Expectations \(SLE\)" on page 335](#) such as the ["Capacity SLE" on page 355](#) as shown in the following video.



Video:

RRM applies continual reinforcement learning to analyze as many as 30 days' worth of performance data. Thus it can identify event-driven trends that occur over the course of a day, week, or month, for example, to deprioritize a channel that has been observed to encounter frequent interference from some sort of neighboring device. In addition to creating a long baseline, this continual observation and learning acts to prevent the kind of system drift and manual intervention that is inherent to static Wi-Fi implementations.

At the level of individual APs, RRM ensures optimal channel optimization by reacting to events like channel interference. It can also automatically, and immediately react to radar hits, and adjust transmit power or channel usage.

Table 15: Comparing Global and Local RRM

Global RRM	Local RRM
Scheduled automatically runs nightly, per site.	Reacts to local events (relative to the AP)

Table 15: Comparing Global and Local RRM (Continued)

Global RRM	Local RRM
Manual is triggered per radio band	Cloud independent
Uses reinforcement learning	Ad hoc – runs as needed
Leverages a multi-day dataset to make informed decisions	Includes the following events: <ul style="list-style-type: none"> • Auto-channel selection • Auto-triggered ACS • Interference AP co-channel • Interference non-Wi-Fi • Neighbor AP down • Neighbor AP recovered • Radar detected • Post radar

Another feature of RRM is called dual-band radio management. Here, RRM leverages the third (or fourth) radio on the AP to identify unnecessary 2.4-GHz radios and automatically convert them to the 5-GHz band (or 6 GHz). This is particularly useful in high-density environments, and occurs without causing the neighboring APs to increase their transmit power.

To manage dual-band, local RRM works with neighboring APs to assess 2.4-GHz radio signal strength and density (how many 2.4-GHz radios are transmitting in a given area). If a particular AP model does not support dual-band, RRM can disable the 2.4-GHz radio rather than convert it to drive traffic to the 5-GHz band. See ["Radio Management \(dual-band\)" on page 217](#).

At both the organization level, and the site level of the configuration, you can override automatic settings by manually configuring which radios to disable, setting the channel width and availability, etc.

As shown in Figure 1, some defaults are tied to the country selection.

Figure 10: The Radio Management Page

Juniper Mist™ MADHU-SG-OFFICE

After saving, reoptimize AP radios using RRM by clicking "Optimize"

Information

Template Name
AP43e-20wide-no-DFS-EU

Country
Germany

2.4 GHz Settings

Default Settings

Band Enabled
☒ Enabled ☐ Disabled ☐ Auto

Channel Width
20 MHz

Preamble
Short

Radio Resource Management

Power
☐ Automatic ☒ Set power
8 dBm

Channels
☒ Automatic ☐ Set allowable channels

External Antenna Gain

Radio Management (page)

IN THIS SECTION

- [Navigation | 207](#)
- [Current Radio Values | 208](#)
- [Distribution | 211](#)
- [Radio Events | 211](#)

Navigation

The Radio Management page (**Site > Radio Management**) provides a consolidated view of Juniper APs in the site. For example, you can see site-wide radio settings for a given radio band, view your overall channel and power distribution, and monitor RRM events.

Figure 11: Using the Radio Management Page



- (1) The **Site** selection controls which site in the organization you are viewing.
- (2) The **2.4 GHz**, **5 GHz**, and **6 GHz** radio frequency buttons control which radio band in the site you are viewing.
- (3) The **Radio Settings** button opens a summary of the site radio settings. From the page that opens, you can also see the radio configuration setting page and jump to Radio Frequency (RF) templates. RF templates provide a way to make uniform radio configurations that are shared by all sites in your organization.
- (4) The **Optimize Now** button manually pushes configuration changes to the APs for the selected radio band. This action shows up as a **Triggered site RRM** in the Check Radio Events table. Note that optimizations based on reinforcement learning from the past 24 to 48 hours are automatically pushed to the Juniper APs each night. Note too that local RRM events, such as reacting to channel interference and DFS events, occur on the AP immediately, as needed.

Below the button bar, the summary band provides a snapshot of AP health and performance.

- **Avg Noise**—This value indicates the overall noise floor for all APs in the site on the selected radio band. Individual Juniper APs can automatically adjust to instances of high noise, but a high Avg Noise score site-wide can explain poor Wi-Fi experience and prompt a search for the source of the interference.
- **Avg Neighbors**—This value indicates the average number of Juniper APs (not SSIDs) in the site that are hearing each other on the selected radio band.
- **Avg Co-Channel Neighbors**—This value indicates how many APs are broadcasting the same channel. It is the average for all Juniper AP in the site. A high number here can explain frequent co-channel interference on the site. Individually, RRM on the APs will try to manage co-channel interference, but site-wide, it can indicate something like high AP density. Following the initial deployment, this metric can also server as a quick check on whether physical installation of the APs complies with your deployment policy.
- **Avg APs Per Channel**—This value is a count of Juniper APs in the site that are using a given channel and is often considered in conjunction with Channel Distribution. Since the number of available channels varies by band, you need to consider the radio band as context for this value.

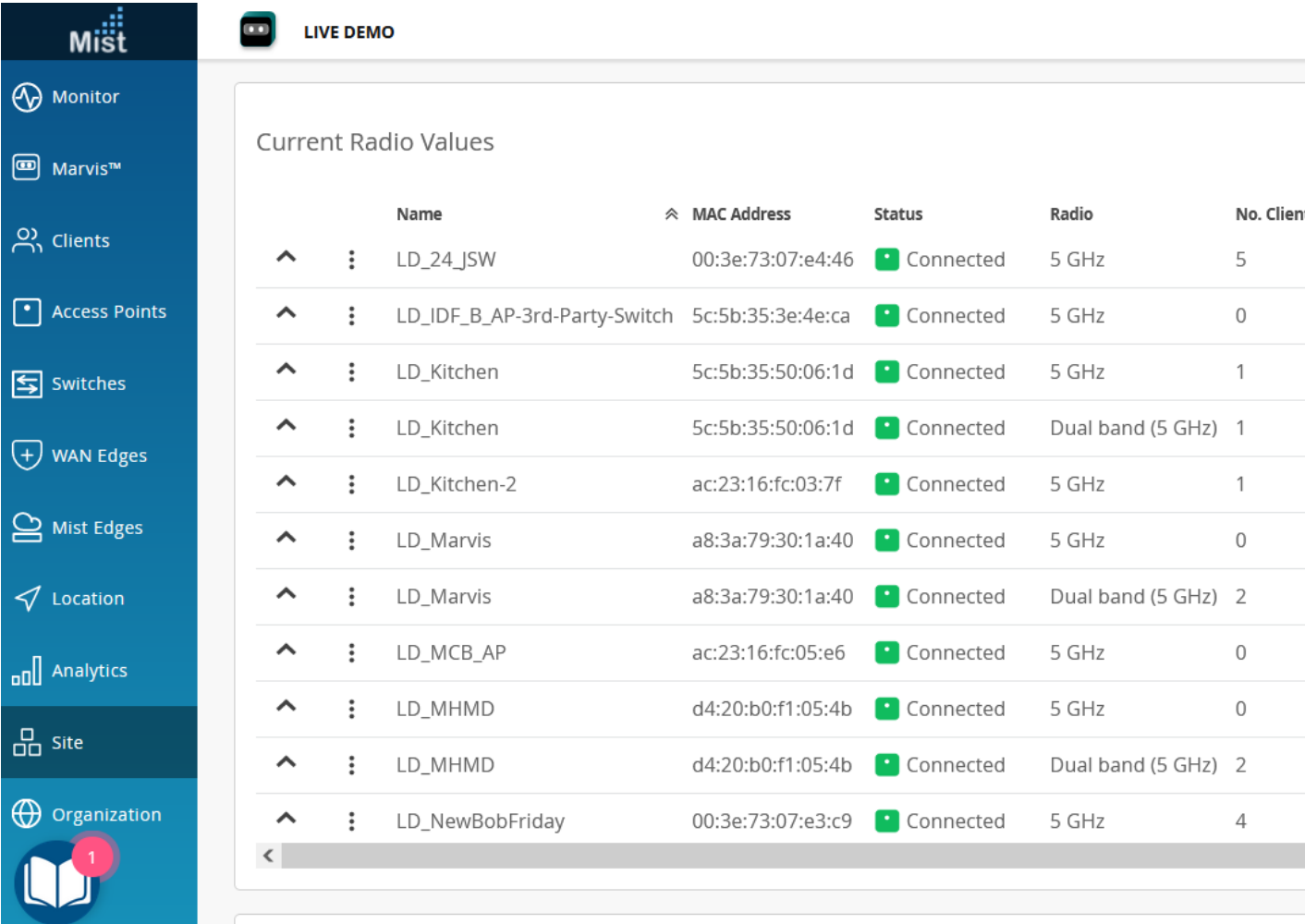
NOTE: You can set an RSSI threshold for neighbor detection on the **Organization > Site Configuration** page (in the Security Configuration section, the option appears when you select **Detect Rogue and Neighbor APs**).

- **Channel Distribution**—Values here range from 1 to 0, with 1 being uniform distribution, for example, the APs are not all broadcasting the same few channels. Anything below a value of 1 is something you may want to look into.
- **AP Density**—Values here also range from 1 to 0, with 1 indicating that all APs can hear one another. Values below 1 indicate that at least some of the APs are out of range of one another, or there's a problem with a scanning radio. A value of 0.7 to 0.8 or so is considered optimal.

Current Radio Values

Current Radio Values are given per site, and per radio band (2.4-GHz, 5-GHz, or 6-GHz). You select those parameters at the top of the page. They provide a summary of key details for each AP on the site, similar to the Access Points page on the dashboard. For any of the parameters shown in the table, you can drill down for further details. You can also change the view so you can see AP placement relative to the floor plan.

Figure 12: Exploring Radio Values

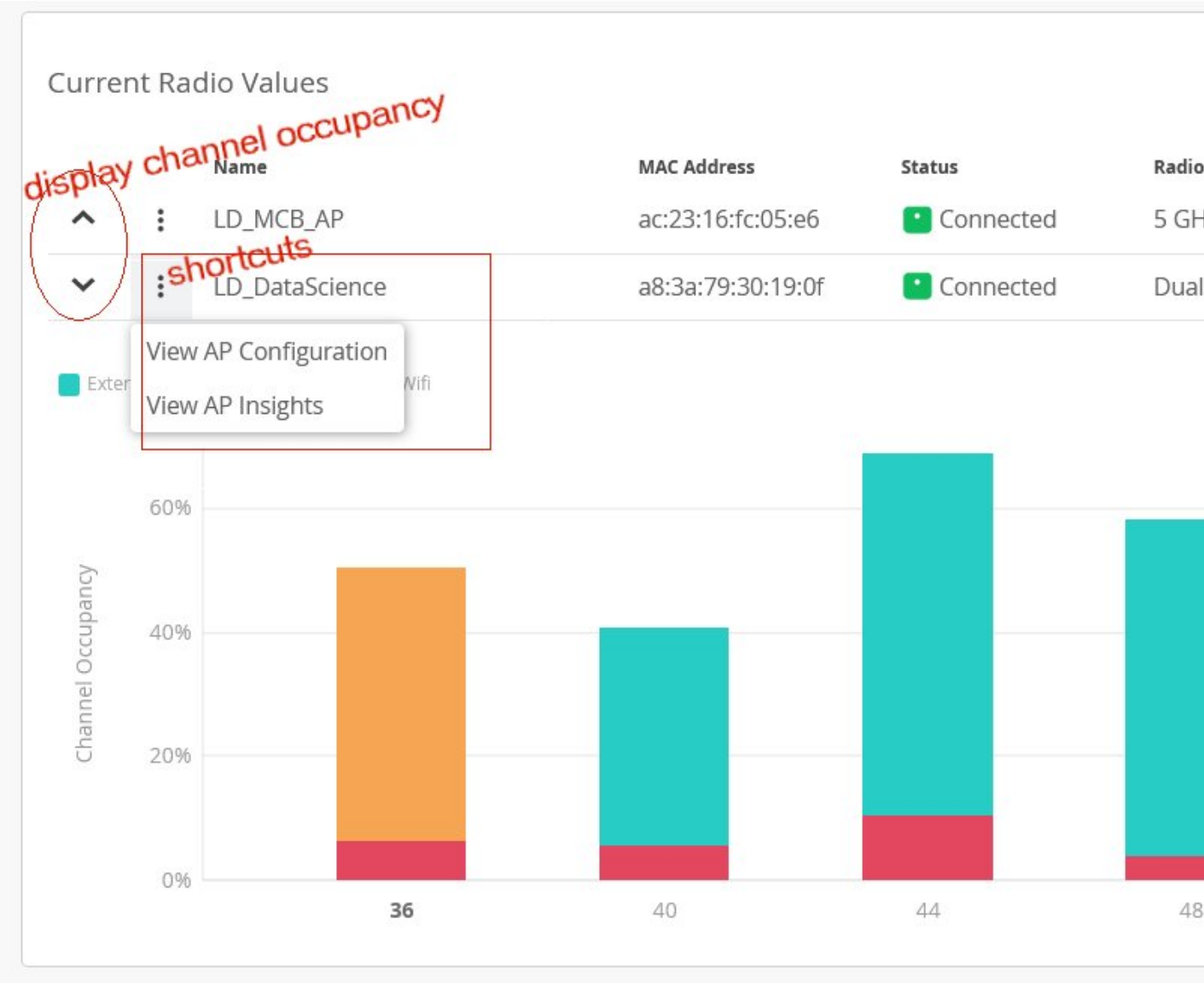


Use your browser's **Refresh** button to replay the illustration.

The drop-down and stacked dot controls at the beginning of each row (as shown above) have the following functions:

- Channel occupancy is shown per radio band, for the past 20 minutes (requires AP firmware version 0.09 or later). The channels occupied by the AP are shown in bold.
- Shortcut to the AP configuration page for the given AP.
- Shortcut to ["Wireless SLEs" on page 0](#).

Figure 13: Channel Occupancy



The channel occupancy chart uses data collected for the Capacity SLE for the selected site and radio band. It tells you at a glance how well the site or WLAN is adhering to your channel plan for the selected radio band. For example, columns that are mostly aqua or red indicate right away that you clients aren't using the channel because the AP is not offering it, because SLE telemetry indicates that there is a lot of interference from non-Wi-Fi devices or near-by APs that are not in your WLAN.

You can quickly find the root cause by clicking the shortcut to the Wireless SLEs, where you can drill down on the **Capacity** metric and look for the sub-metric that is contributing most to the issue.

Distribution

The **Distribution** chart gives an aggregate picture of how channels usage and power levels are distributed across a site.

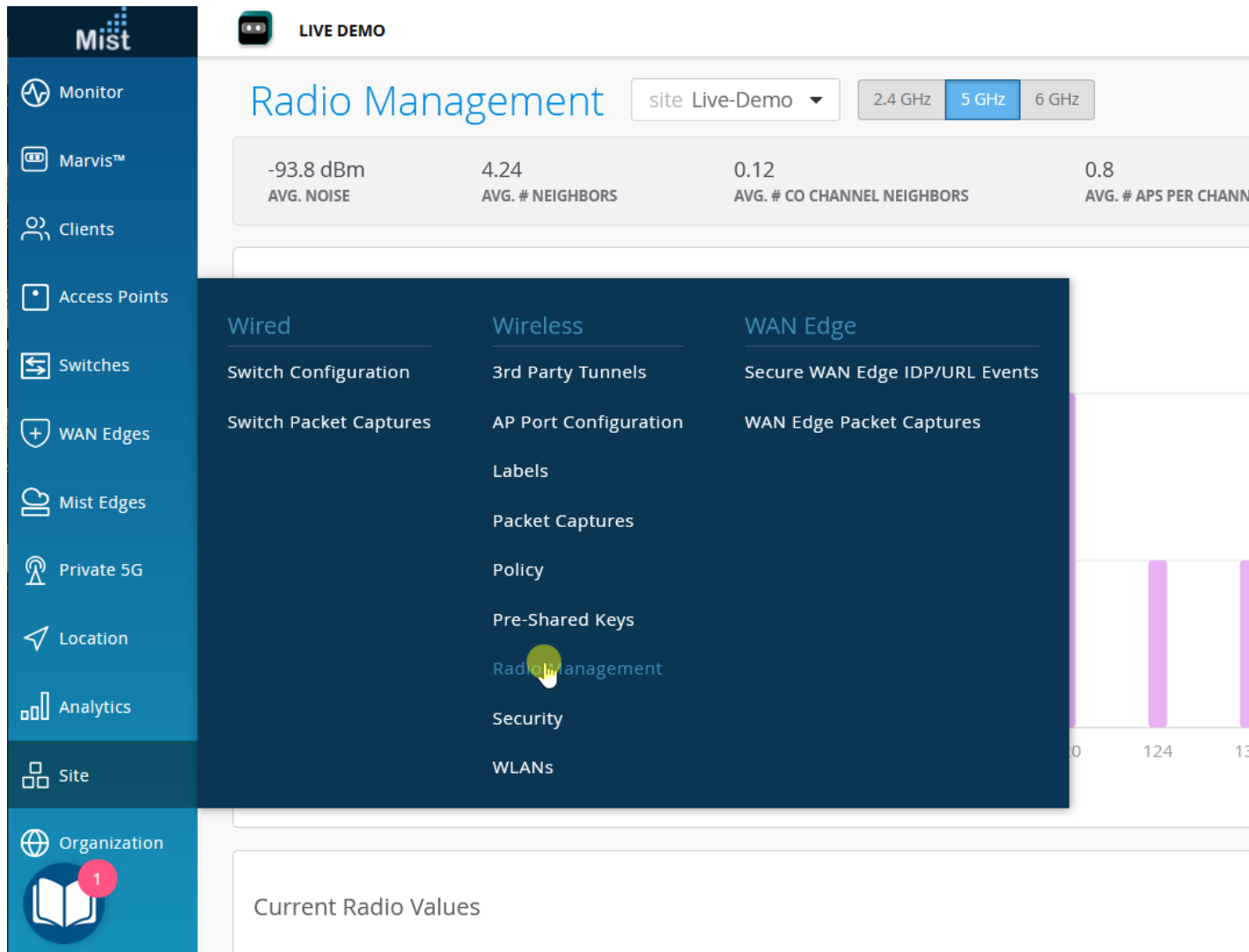
You can use the channel view to identify potential interference from co-channel neighbors, or to see whether certain channels are overrepresented or underrepresented at the location.

- Use the **Power** view to see how many radios (not APs) in the site are transmitting at a given power level.
- Sort by **Best to Worst** to emphasize APs where channel occupancy is highest.

Radio Events

In this chart, you can see a list of radio events from the past 24 hours or 7 days, including channel, bandwidth, and AP power. You can also see what triggered the update, for example, a scheduled RRM from the Mist cloud, a reaction to co-channel interference on the AP, or manual changes that were pushed to the AP.

Figure 14: RRM Events



Use your browser's **Refresh** button to replay the illustration.

Dynamic Frequency Selection (DFS) is a Wi-Fi function you can use with 5-GHz radios to leverage channels that are generally reserved for radar. These channels vary by country, so for different countries, the DFS channels listing will be different. In the United States, FCC regulations require that whenever the AP detects radar, it must immediately switch from the current operating channel to a random channel. Connected clients will need to reassociate with the AP.

In Mist, after 30 minutes, for non-static channel assignments, RRM then assigns a new, best-available channel according to current RRM scan data (this may be the original channel). For static channel assignments, the AP will resume using the configured channel.

- **Scheduled site RRM** indicates routine optimizations pushed from the Mist portal. See "[Radio Management](#)" on page 204.

- **Triggered site RRM** indicates a manual update, that is, updates pushed by the **Optimize Now** button. See ["WLAN Changes That Reset The Radio" on page 223](#).
- **Auto channel selection** indicates the occurrence of an RRM refresh. For example, APs added to a site will automatically receive RF settings configured for the site.
- **Auto Triggered ACS** occurs an hour or so following an automatic channel selection. RRM compares the channel plan on a given AP against its analytics to determine whether further optimization is possible.
- **Interference AP co-channel** indicates that RRM changed channels on the AP, most likely to improve performance due to neighboring APs using the same or overlapping channel. Because wireless is half-duplex (shared medium), sharing the same channel degrades performance as the APs spend air time waiting for the channel to clear before they can send. Connected clients will be re-associated with the AP upon the channel change.
- **Interference AP non wifi** occurs when 802.11 devices such as a microwave oven or wireless video camera, create interference due to broad RF spectrum emissions. The AP will change to another channel to improve the signal. Connected clients will be re-associated with the AP upon the channel change.
- **Radar detected** occurs on APs that are using DFS channels whenever radar is detected. The AP will immediately change to the next-best channel. Connected clients will have re-associated with the AP upon the channel change.
- **Post Radar** occurs as a follow-up to radar detection. The AP will have changed to a different channel upon detecting radar. Sometime subsequent to that change, the AP will automatically review the channel selection it made to see if a better channel is available (and if so, change the channel again).

Radio Settings (RF Templates)

IN THIS SECTION

- [RF Templates Settings | 214](#)

RF templates provide a way to make uniform radio configurations that are shared by all sites in your organization. RF templates do this while simultaneously allowing for model-specific exceptions to cover the different use cases that may occur in the organization or individual sites. Settings include enabling or

disabling radio bands, managing channel width, setting transmission power, and configuring AP antenna gain.

RF Templates Settings

AP-specific default settings are available for all models in the **Default Settings** drop-down, for each radio band. You can use these defaults to create model-specific exceptions within the RF Template.

- In the Mist menu, select **Organization > RF Template** and then either choose an existing template from the list that appears or click the **Create Template** button to create a new one.

Figure 15: Model-specific Default Settings

The screenshot displays the Mist UI for configuring an RF Template. The sidebar on the left contains navigation links: Monitor, Marvis™, Clients, Access Points, Switches, WAN Edges, Mist Edges, Location, Analytics, Site, and Organization. The main panel is titled 'RF Templates: RF Template' and includes a 'LIVE DEMO' button and a 'Change language (en)' dropdown. The top right shows the time 'MON 9:36 PM' and user icons. The 'Information' section has fields for 'Template Name' (RF Template) and 'Country' (United States). The '2.4 GHz Settings' section includes 'Band Enabled' (Enabled, Disabled, Auto), 'Channel Width' (20 MHz), 'Preamble' (Short), and 'Radio Resource Management' (Power: Automatic, Set power; Channels: Automatic, Set allowable channels; External Antenna Gain: 0 dBi). The '5 GHz Settings' section is expanded, showing 'Band Enabled' (Enabled, Disabled), 'Channel Width' (20 MHz), 'Radio Resource Management' (Power: Automatic, Set power; Channels: Automatic, Set allowable channels; External Antenna Gain: 0 dBi), and a 'Default Settings' dropdown menu with options: AP45, AP45E, AP61, AP61E, AP63, AP63E, and AP64. The 'Radio Resource Management' section also includes a 'Select All | Clear' button and a grid of channel selection checkboxes (36, 40, 44, 48, 52 (dfs), 56 (dfs), 60 (dfs), 64 (dfs), 100 (dfs), 104 (dfs), 108 (dfs), 112 (dfs), 116 (dfs), 120 (dfs), 124 (dfs), 128 (dfs), 132 (dfs), 136 (dfs), 140 (dfs), 144 (dfs), 149, 153, 157, 161, 165).

Use your browser's **Refresh** button to replay the illustration.

- **Template Name**—This is the name that appears in the templates list on the RF Templates page.
- **Country**—Your selection here determines which radio channels, and which power level defaults, are available for configuration.

- **Enabled/Disabled**—Turn on or off the given radio band for all APs in the template.
- **Auto**—When enabled for the 2.4-GHz radio band, auto will manage the 2.4-GHz radio band on the AP to maximize performance. For APs that support dual-band, this setting will convert the 2.4-GHz radio to 5-GHz according to RRM analysis. For APs such as AP12 and AP33 that don't support auto-conversion, *auto* will turn off the 2.4-GHz radio so the AP offers only the 5-GHz band, if RRM finds that doing so will improve network performance.

NOTE: You can configure **Auto** radio band management in the AP's local configuration settings, in device profiles, and in RF Templates. However, for **Auto** to work in a device profile, it must first be enabled in the RF template for the site. You can enable **Auto** for either for 2.4-GHz band setting, or for Dual Band Radio Settings in the AP configuration page, as shown below.

The screenshot displays the Mist RF Template configuration interface. The left sidebar contains navigation links: Monitor, Marvis™, Clients, Access Points, Switches, WAN Edges, Mist Edges, Private 5G, Location, Analytics, Site, and Organization. The main content area is divided into several sections:

- Information:** Template Name (RF Template), Country (United States).
- 2.4 GHz Settings:** Band Enabled (radio buttons: Enabled, Disabled, Auto), Channel Width (20 MHz), Preamble (Short), Radio Resource Management (Power: Automatic, Set power; Channels: Automatic, Set allowable channels), External Antenna Gain (0 dBi).
- 5 GHz Settings:** Band Enabled (radio buttons: Enabled, Disabled), Channel Width (20 MHz), Radio Resource Management (Power: Automatic, Set power; Channels: Automatic, Set allowable channels), External Antenna Gain (0 dBi).
- Dual Band Radio Settings:** AP43, AP45, AP63 Only (radio buttons: Auto, 5GHz, 2.4GHz), AP24 (radio buttons: Auto, 6GHz, 2.4GHz). A note states: "RRM will automatically decide the operating band of dual band radios."
- 6 GHz Settings:** (Section header visible at the bottom).

Red boxes highlight the "Band Enabled" settings for 2.4 GHz, 5 GHz, and the "Dual Band Radio Settings" section.

- **Channel Width**—For the 5-GHz and 6-GHz radio bands, you can set the channel width for all APs in the profile (2.4-GHz uses a fixed-width 20 MHz band). Likewise, you can also specify which channels the radios can use.
- **Preamble**—A set of bits within a packet header that synchronize transmission signals between a sender and receiver (the preamble is sent from the AP to the client). The options for Preamble are as follows:

- **Unconfigured** — If set to Unconfigured, this means that the additional header will not be added to synchronize transmission signals between sender and receiver (the preamble will not be sent from the AP to the client).
- **Short** — This is the default. This applies to the 2.4-GHz radio band only. If you are seeing association failures such as "client does not support short preamble," you can change the preamble the AP sends to clients. This is faster, but it requires that clients have the "Short Preamble" bit set in their association request, which not all client implementations do.
- **Long** — This is slower, but supports a wider range of clients.
- **Auto** — This is slower, but supports a wider range of clients.
- **Power**—This is the maximum transmit power allowed for a given data rate per transmit chain. Note that because total power out typically includes any MIMO gain, you should deduct MIMO gain (generalized, below) from the total power output (TPO) when configuring transmit power. See ["Transmit Power Notation for Juniper APs" on page 225](#).
- **Channels**—For the 5-GHz and 6-GHz radio bands, you can set the available channel selection (for your selected country) for all APs. When set to automatic, all allowed channels in the host country are available. For 6 GHz, the preferred scan channels (PSC) are as defined by the IEEE. The EU, for example, has half the channels allowed in the USA.
- **External Antenna Gain**—Mist supports 1 dBm increments (although we recommend using a range plus or minus 3 dBm from the median value indicated in a site survey predictive design). For example, some external antennas are certified up to certain level of gain, which depends on the combination of AP and antenna. To prevent the gain from exceeding the maximum allowed for a particular AP model and regulatory domain, you can adjust this setting.

NOTE: The amount of gain achieved depends on the specific AP and antenna used. For example, an AP43E model can support a directional antenna with up to 8 dBi gain on the 2.4-GHz band and up to 10 dBi gain on the 5-GHz band.

In addition to the RF Templates page described here, you can configure RRM and other settings in several other places in the Mist portal, as well as individually, on each Juniper AP. To understand the relationship and interaction between settings on these different levels, see ["Templates and Device Profiles" on page 203](#).

Push Template Changes to The APs

After making changes to the power or channel settings, you need to push the updates to the relevant APs:

1. Save your RF Template updates.

2. Go to the **Site > Radio Management** page.
3. Click the **Optimize now** button in the top right corner for each modified band (2.4-GHz and 5-GHz).
4. Verify your changes, on the Mist menu: click **Site > Radio Management** and scroll down the page that appears to the Radio Events section. Look for events labeled **Triggered site RRM**.

Date	AP	Radio	Band	Channel	Channel Width	Power	Event
Apr 22, 2024 4:00 PM	LD_NewBobFriday	5 GHz	5 GHz → 5 GHz	136 → 136	20 → 20 MHz	10 → 11 dBm	Triggered site RRM
Apr 22, 2024 4:00 PM	LD_Kitchen	5 GHz	5 GHz → 5 GHz	132 → 132	20 → 20 MHz	11 → 12 dBm	Triggered site RRM
Apr 22, 2024 4:00 PM	MC_AP24_RLB2	5 GHz	5 GHz → 5 GHz	136 → 136	20 → 20 MHz	7 → 9 dBm	Triggered site RRM
Apr 22, 2024 4:00 PM	LD_IDF_B_AP-3rd-Party-Switch	5 GHz	Disabled → 5 GHz	136 → 136	20 → 20 MHz	5 → 16 dBm	Triggered site RRM
Apr 22, 2024 4:22 PM	LD_DataScience	5 GHz	5 GHz → 5 GHz	132 → 136	20 → 20 MHz	9 → 9 dBm	Radar detected
Apr 22, 2024 5:00 PM	LD_NewBobFriday	5 GHz	5 GHz → 5 GHz	136 → 136	20 → 20 MHz	11 → 10 dBm	Triggered site RRM
Apr 22, 2024 5:00 PM	LD_Kitchen	5 GHz	5 GHz → 5 GHz	132 → 132	20 → 20 MHz	12 → 11 dBm	Triggered site RRM
Apr 22, 2024 5:00 PM	5c5b350e60:6e	5 GHz	5 GHz → 5 GHz	136 → 132	20 → 20 MHz	16 → 16 dBm	Triggered site RRM

Radio Management (dual-band)

By default, APs with two radios operate both the 2.4-GHz and 5-GHz radio bands. For AP models that support "dual-band," you can have the AP automatically convert the 2.4-GHz radio to 5-GHz (or 6-GHz for AP24, AP34, AP45, AP45E, and AP64). This is especially useful in high-density environments because the 5-GHz band can provide up to 25 non-overlapping channels, whereas only three or four are possible in the 2.4-GHz band. See ["Radio Management " on page 204](#) and ["Enable Fast Roaming" on page 232](#).

For APs that don't support auto-conversion, 2.4-GHz radios that are found to be surplus to necessary coverage can be automatically disabled.

This discretionary behavior is especially useful in the context of templates because you don't need to worry about model-specific exceptions. For mission critical or 2.4-GHz IoT devices, we recommend managing the radio bands manually. You would use auto RRM, on the other hand, to simplify radio management when there are many APs or sites involved.

The figure below shows a dual-band radio configuration with automatic radio management as configured in an RF Template (**Organization > Wireless | RF Template**). See ["Templates and Device Profiles" on page 203](#).

Figure 16: dual-band 5 GHz Configuration

The screenshot shows the Mist portal configuration interface. The left sidebar contains navigation links: Monitor, Marvis™, Clients, Access Points, Switches, WAN Edges, Mist Edges, Private 5G, Location, Analytics, Site, and Organization. The main content area is divided into sections for 2.4 GHz Settings, 5 GHz Settings, and Dual Band Radio Settings. Each section has a 'Default Settings' dropdown. The 2.4 GHz Settings section shows 'Band Enabled' set to 'Enabled', 'Channel Width' set to '20 MHz', 'Preamble' set to 'Short', 'Power' set to 'Automatic' (min 3 dBm, max 9 dBm), and 'Channels' set to 'Automatic'. The 5 GHz Settings section shows 'Band Enabled' set to 'Enabled', 'Channel Width' set to '20 MHz', 'Radio Resource Management' set to 'Automatic' (min 5 dBm, max 16 dBm), and 'Channels' set to 'Set allowable channels'. The Dual Band Radio Settings section shows 'AP43, AP45, AP63 Only' and 'AP24' both set to 'Auto'. A red box highlights the 'Dual Band Radio Settings' section, and another red box highlights the 'Band Enabled' sections for both 2.4 GHz and 5 GHz.

As the figure shows, you enable both the 2.4-GHz and the higher band radio (5-GHz here), and then also enable **Auto** under dual-band Radio Settings.

NOTE:

- When **auto** is enabled, the typical cancellation/conversion is 20-40 percent of APs in a site.
- When **auto** is enabled, it will not disable more than 50 percent of the 2.4-GHz radios in a site.
- When using auto-conversion or dual 5-GHz, we recommend 20 MHz-channel widths to maximize the number of 5-GHz radios.

Dual-band Radio Settings

There is no On/Off toggle to enable or disable dual-band radio in the Mist portal. Instead, you need to enable both radios on the AP and then setting dual-band to **Auto**. The AP will then use the scanning radio to determine whether the 2.4-GHz radio can be converted to 5-GHz (or disabled if conversion is not supported on the AP).

- Auto (Auto Conversion)—The following default behaviors apply to dual-band and non-dual-band APs.
 - Dual-Band APs (AP43 and 63)—If there are APs located close enough together that they can cumulatively provide enough 2.4-GHz band signal to cover the whole area, there are some important things to note. For those APs where the 2.4-GHz band radio is not needed, the 2.4-GHz band radio will be converted to operate on the 5-GHz radio band, and the 5-GHz channels will be divided like so:
 - Dedicated 5-GHz: 36 -64
 - Dual-band 5-GHz: 100 -165 (as per the bandwidth)
 - Non dual-band APs—If there are APs located close enough together that some of the APs can cumulatively provide enough 2.4-GHz band signal to cover the whole area, then for those APs where the 2.4-GHz band radio is not needed, the 2.4-GHz band radio will be turned off.

When both radios on an AP are broadcasting 5-GHz, the radios will divide the 5-GHz channels as shown in the following table to ensure sufficient separation:

Dual 5-GHz Radios

- • Dual-band Radio (5-GHz) – Channels 100-165
 - 5-GHz Radio – Channels 36-64
- AP45 (only)
 - Dual-band Radio (5-GHz) – Channels 36-64
 - 5-GHz Radio – Channels 100-165

Dual-band 2.4-GHz and 5-GHz (or 6-GHz)

- • Dual-band Radio (2.4-GHz) – All 2.4-GHz channels
 - 5-GHz Radio – All 5-GHz Channels

Dual Band Usage Examples

IN THIS SECTION

● [Carpeted Enterprise | 220](#)

- [College Dormitories | 221](#)
- [Conference Rooms and Auditoriums | 222](#)

Dual band technology allows a single radio to transmit on either 2.4 or 5-GHz. Mist RRM can turn off surplus 2.4-GHz radios and configure the radio to transmit on 5-GHz instead, which is especially useful for high-density environments. See ["Radio Management " on page 204](#) and ["Dual Band Usage Examples" on page 219](#).

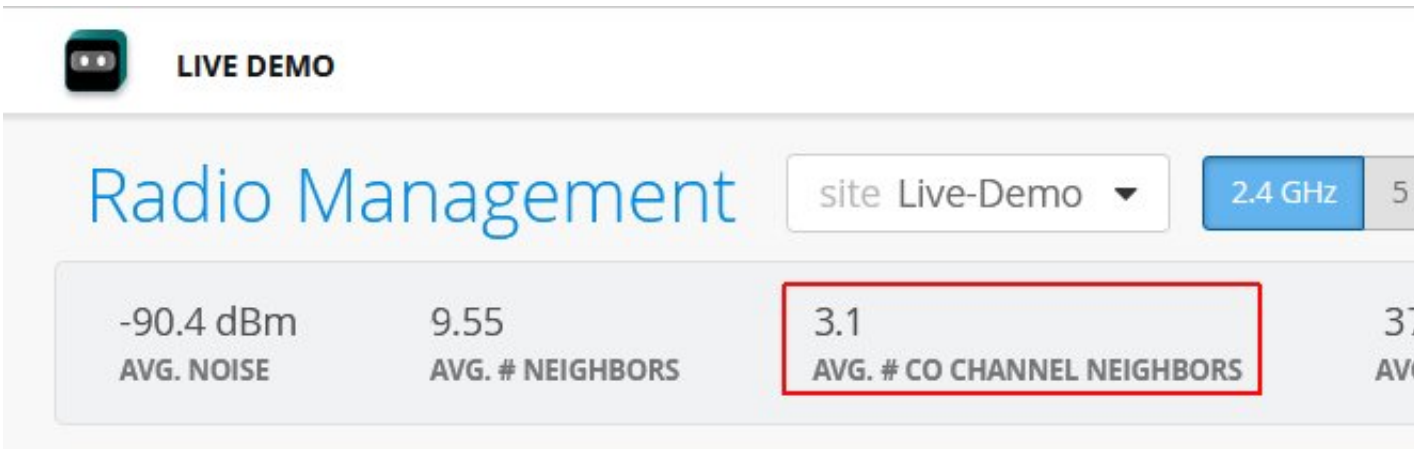
The following use cases can help illustrate how RRM works and you should use it.

Carpeted Enterprise

Let's consider a typical, carpeted enterprise, where the goal is to provide 5-GHz Wi-Fi for the high capacity it provides. Assume the Juniper APs are already up and running, and visible in the Mist portal.

The first thing you can do is go to the Mist portal and select the **Site > Radio Management** page, where you can see co-channel and density metrics.

Figure 17: Snapshot of APs in the Site



The APs have an average of 3.1 co-channel neighbors, which means that some neighboring APs are all using the same channel, which can cause co-channel congestion. The AP Density metric is 1.0, which means the APs are uniformly distributed across the site. We can conclude that this site is a great candidate for Mist RRM to auto-manage.

To enable auto-management for the 2.4-GHz radio:

1. In the Mist menu, select **Organization > Wireless | RF Templates**.
2. In the list of templates that appears, choose the site template (or click the **Create Template** button to start a new one).
3. In the 2.4 GHz Settings section, under Band Enabled, select **Auto**.
4. In the Dual Band Radio Settings section, also select **Auto**.
5. Click **Save** to apply your changes.

College Dormitories

College dormitories are also a good use case for RRM auto-management. Individual rooms typically have their own AP, while the AP model and standard WLAN configuration for hallways is different. Juniper AP12s are common in dorms, while AP33s or AP43s are common in the halls.

You can use the same RF template to cover both AP models. For the hallway APs, say you want to automatically convert the 2.4-GHz radio to 5-GHz wherever possible. And for the dorm rooms, you want to leave the 2.4-GHz radios as they are. You can create such an exception in the RF template for the AP12s.

NOTE: You can include any number of model-specific tweaks in the within the same RF template by selecting different AP models from the default settings drop-down list.

To configure dual settings in the same template:

1. In the Mist menu, select **Organization > Wireless | RF Templates**.
2. In the list of templates that appears, choose the template for the dorm site you are working on.
3. In the 2.4 GHz Settings section, under Band Enabled, select **Auto**.
4. In the same section, click the **Default Settings** drop-down list and select AP 12

. This opens (in the same pop-up window) a model-specific settings page that you will configure next.

5. Click **Save** to apply your changes.

Conference Rooms and Auditoriums

For areas where high client density is expected, you may want to control certain APs explicitly, for example, to enable dual band 5 GHz. For other areas, you may want to broadcast both 2.4-GHz and 5-GHz. You can use device profiles to accomplish both goals.

To configure dual-band settings for selected APs:

1. In the Mist menu, select **Organization > Wireless | Device Profiles**.
2. In the profiles page that appears, click **Create Profile**.
3. Give the profile a name, and then click Access Points links under **Applies To** to select the APs you want to include in the profile. These will be the APs that you to convert to dual 5-GHz. You can find APs by organization, by site, by model, by name, or MAC address.
4. After selecting the APs, click **OK** to close the window and attach the APs.
5. Scroll down to the Dual Band Radio Settings section and select **5GHz**. If the setting conflicts with any already in place on one or more of the selected APs, you can override the local or RF template settings in favor of the device profile configuration.

- When finished, scroll to the top of the page and click **Create** to apply the settings to the selected APs.

WLAN Changes That Reset The Radio

IN THIS SECTION

- [WLAN Configuration Changes | 223](#)

WLAN Configuration Changes

Some configuration changes require the affected access points (APs) to restart in order to apply the new settings. During this time, clients will be deauthenticated on the AP and thus disconnected from the WLAN for the minute or two it takes to restart.

The table below lists WLAN settings and says whether or not changing a given setting will cause the radio for that band to restart.

Table 16: WLAN Settings Changes and Radio Resets

Change	Effect
SSID (WLAN name)	Reset
Selecting specific radio	Reset
Data rate	Reset
Wi-Fi protocols	Reset
Selecting different authentication methods	Reset
Adding, deleting, modifying RADIUS Authentication, Accounting, CoA Servers	Reset

Table 16: WLAN Settings Changes and Radio Resets *(Continued)*

Change	Effect
Multimedia extensions	Reset
Fast roaming	Reset
Guest portal changes	Reset
WLAN Rate Limit	No Reset
Band steering	No Reset
Client Inactivity	No Reset
Geofence	No Reset
Filtering	No Reset
DTIM period	No Reset
SSID scheduling	No Reset
QoS priority	No Reset
Prohibiting peer to peer communication	No Reset
Application QoS	No Reset
Bonjour gateway	No Reset

Transmit Power Notation for Juniper APs

IN THIS SECTION

- [Radio Power Levels and Conversions](#) | 225

Radio Power Levels and Conversions

Radio resource management (RRM) provides sophisticated radio and antenna power management when enabled and set to auto, and we recommend that you use it. See ["Radio Management " on page 204](#). However, if you need to configure the settings manually or just want to understand the power calculations and values, the following explanation will help.

- In the Mist portal, the power values used are for the *total AP transmit power of the entire transmit (Tx) chain*.
- Transmit power for 6-GHz is limited by the power spectral density (PSD) in the United States (and some other regulatory domains) rather than by Effective Isotropic Radiated Power (EIRP). EIRP is a calculated value used to represent transmitter output power, cable loss, and antenna gain.
- For predictive power plan designs created in Ekahau, you need to subtract multiple-input multiple-output (MIMO) gains before using the values for transmit power in the Mist portal.

Figure 18: Power Levels in Current Radio Values

LIVE DEMO Change language (en) FRI 4:09 PM

Current Radio Values Confirm clear all 5 GHz overrides

	Name	MAC Address	Status	Radio	No. Clients	Channel	Channel Width	Power	Radio Enabled	Config Ov
▼	LD_24_JSW	00:3e:73:07:e4:46	Connected	5 GHz	5	120	20 MHz	10 dBm	Yes	No
▼	LD_IDF_B_AP-3rd-Party-Switch	5c:5b:35:3e:4e:ca	Connected	5 GHz	0	0	-	-	Yes	No
▼	LD_Kitchen	5c:5b:35:50:06:1d	Connected	5 GHz	4	64	20 MHz	12 dBm	Yes	No
▼	LD_Kitchen	5c:5b:35:50:06:1d	Connected	Dual band (5 GHz)	2	153	20 MHz	12 dBm	Yes	No
▼	LD_Kitchen-2	ac:23:16:fc:03:7f	Connected	5 GHz	1	112	20 MHz	10 dBm	Yes	No
▼	LD_Marvis	a8:3a:79:30:1a:40	Connected	5 GHz	0	149	20 MHz	10 dBm	Yes	No
▼	LD_Marvis	a8:3a:79:30:1a:40	Connected	Dual band (5 GHz)	0	64	20 MHz	10 dBm	Yes	No
▼	LD_MCB_AP	ac:23:16:fc:05:e6	Connected	5 GHz	0	140	20 MHz	11 dBm	Yes	No
▼	LD_MHMD	d4:20:b0:f1:05:4b	Connected	5 GHz	0	136	20 MHz	11 dBm	Yes	No
▼	LD_MHMD	d4:20:b0:f1:05:4b	Connected	Dual band (5 GHz)	3	48	20 MHz	11 dBm	Yes	No
▼	LD_NewBobFriday	00:3e:73:07:e3:c9	Connected	5 GHz	3	120	20 MHz	10 dBm	Yes	No

Rule of Thumb for MIMO Gain Values

A simple rule of thumb for manual settings for AP41, AP43, and AP45 devices is to add 6 dB for MIMO gain. For AP34 devices, add 3 dB. In terms of radios, the rule of thumb looks like this:

- 4 spatial streams (4x4): 6 dB of MIMO gain
- 3 spatial streams (3x3): 4.7 dB of MIMO gain
- 2 spatial streams (2x2): 3 dB of MIMO gain

AP	Type	2.4-GHz	5-GHz
AP32E	Directional	8 dBi	10 dBi
	Omni	4 dBi	6 dBi
AP41E	Directional	8 dBi	8 dBi
	Omni	No cert, use AP41	No cert, use AP41
AP43E	Directional	8 dBi	10 dBi
	Omni	4 dBi	6 dBi

AP61E	Directional	8 dBi	8 dBi
	Omni	4 dBi	6 dBi
AP63E	Directional	8 dBi	10 dBi
	Omni	4 dBi	6 dBi

Calculating TPO and EIRP

The total power output (TPO) for Juniper APs is equal to the transmit power per radio chain, plus the log value of the total number of radio chains. Radio chains are comprised of the transceiver, antenna, and hardware needed for signal processing.

- $TPO = \text{Tx power per chain} + 10\log(\text{Tx chains})$

So, for example, if you have a Juniper AP with 17 decibel-milliwatts (dBm) per chain, you add 6 dB MIMO gain for a total transmit power of 23 dBm.

Calculating the EIRP, which is a value for the estimated output power radiated by the antenna, is similar:

- $EIRP = TPO + \text{antenna gain} - \text{antenna losses}$

EIRP (for 6-GHz band radios)

Some regulatory domains, including the United States, use PSD rather than EIRP for radio transmit power limits. With PSD, the power density decreases as channel bandwidth increases.

For a fuller understanding of PSD and an illustration comparing EIRP and PSD across channel bandwidths, see: <https://blogs.juniper.net/en-us/industry-solutions-and-trends/power-spectral-density>.

In addition:

- Wide channels such as 80 MHz can yield higher EIRP than typical channel width (20 and 40-MHz).
- In the United States, the FCC allows up to 5 dBm/MHz PSD, or up to 30 dBm EIRP for low power indoor (LPI) operations.
- In the EU, regulators allow up to 10 dBm/MHz PSD, or up to 23 dBm EIRP for LPI.

Converting Between PSD and EIRP

EIRP is equal to PSD plus the log of the total channel width. You can use the formula shown here to convert between PSD and EIRP:

- $EIRP = PSD + 10\log(\text{channel width})$

So, if, for example, you have a PSD of 5 dBm/MHz and 40-MHz channels, the EIRP would be 5 + the base 10 log of 40, which is 1.6, for a total dBm of 21.

Table 17: PSD and EIRP Reference for LPO

Channel Width	PSD	EIRP	Noise Floor	Net EIRP	Available Channels
20-MHz	5 dBm/MHz	18 dBm	na	18 dBm	59
40-MHz	5 dBm/MHz	21 dBm	+3 dBm	18 dBm	29
80-MHz	5 dBm/MHz	24 dBm	+6 dBm	18 dBm	14
160-MHz	5 dBm/MHz	27 dBm	+9 dBm	18 dBm	7
320-MHz	5 dBm/MHz	30 dBm	+12 dBm	18 dBm	3

Working with Ekahau

As noted earlier, Ekahau considers total transmit power to be the combination of all transmitters on the AP (the total power out), whereas in the Mist portal, the value does not include the cumulative MIMO gains. Thus, to convert Ekahau transmit power to Mist transmit power, you must subtract the MIMO gain.

For example, say that in Ekahau, you see a value of **14 dBm** for the simulated transmit power of a Mist AP43. That same value would be **8 dBm** as used in the Mist portal.

In another example, consider two simulated APs in Ekahau, where one is a 1×1:1 and the other is a 4×4:4 (one radio vs four). Transmit power for both APs is set at 14 dBm. In the Ekahau design simulation, because the software does not take into consideration the number of transmitters in the AP, the predicted transmit radius of both APs would be the same.

6

CHAPTER

Security

RSSI, Roaming, and Fast Roaming | 230

RADIUS | 235

Preshared Keys | 264

Integrations | 290

Rogues, Honeypots, and Neighbor APs | 310

PCI DSS Compliance | 323

WxLAN Access Policies | 329

RSSI, Roaming, and Fast Roaming

IN THIS SECTION

- [Roaming | 230](#)
- [Fast Roaming | 231](#)
- [Enable Fast Roaming | 232](#)
- [View Roaming History | 233](#)

The received signal strength indicator (RSSI) is a measurement of the AP radio signal and is typically measured by the client. The scale runs from -100 dBm (weakest) to 0 dBm (strongest), but the values are usually in the range of -90 dBm to -25 dBm. Values from -70 dBm to 0 dBm are generally considered acceptable for the transmission of data, although in some cases clients might consider that to be poor. See [IOS clients may consider an RSSI of -70 dBm to be poor](#).

RSSI matters to preserve good network connectivity. Clients will drop a weak RSSI connection in favor of a stronger one from another AP. This is called roaming, and because it is the client (rather than the AP) that measures RSSI, it is the client that controls the decision when to roam and the SSID to which it will connect. Thus, poor RSSI can cause a lot of roaming.

Poor RSSI can also be a cause of low throughput between the AP and the client, but it doesn't automatically equate to low throughput. In fact, data transfer rates for a given RSSI level, even a poor RSSI, can vary from as much as 5 Mbps to 45 Mbps or more. An RSSI of -75 dBm is significant because of the effect on roaming more so than on throughput.

Roaming

When roaming, for security protocols such as WPA-3 and WPA-2, and where the APs are acting independently of each other, the client must repeat the authentication and authorization process each time it wants to roam (that is, reconnect to the network using a better RSSI). The user might need to re-login to the network. Even if they don't, reconnecting can disrupt service such as voice drops on VoIP calls or video stuttering in real-time video streams.

A client might consider a roam if the RSSI is less than -70 dBm and they have data to send. Typically, this means running a 20 millisecond scan of each channel, or it can be a poll of the current AP to get its neighbors (802.11k), or a suggestion (802.11v).

Most roaming issues involve sticky clients. Sticky clients do not initiate a roam to a better target AP when they should.

Fast Roaming

Fast roaming is a connection method that was developed to optimize how clients perform their initial WPA2/WPA3 security authentication. It also provides a way for clients to retain their login credentials so they can be carried over from one AP to another when roaming.

The methods for fast roaming are, *Default*, *Opportunistic Key Caching (OKC)* and *.11r*. For both these methods, there is no need to send access request packets to the RADIUS server.

The fast roaming option becomes available when you select WPA3 or WPA2 as your security type.

Default

- Mist APs locally cache the client Pairwise Master Key (PMK) ID obtained during the initial authorization and use it for subsequent re-associations on the same AP. This is also known as “fast secure roam back,” and is suitable for use cases where scale is not a factor because clients must fully re-authenticate at each new AP in the network until all the APs have their own local copy of the client's PMKID.

Opportunistic Key Caching

- OKC allows clients to roam quickly to new APs without having to perform a full authentication exchange. It works because Mist APs send their PMKID cache to neighboring APs through cloud updates. Thus, APs in the same network can share PMKs and clients can reuse the PMK learned by one AP when roaming to another AP.
- Juniper Mist APs use key information from a client's first association to generate keys for other APs in the network.
- OKC requires the SSID to use WPA2/EAP (802.1x) security. RADIUS attributes are also shared along with the PMK so the client need not re-authenticate on the RADIUS.
- OKC is a non-standard, fast roaming technology. It is supported by Microsoft Windows clients and some Android devices. Some wireless clients (including Apple iOS phones) do not support OKC.
- A common source of roaming issues is a target AP that does not have the client PMKID which it needs to acknowledge the Fast BSS Transition (FBT) request.

Fast BSS Transition (802.11r)

- Standard roaming takes eight messages, back and forth, between the client and AP (two authentications, two associations, and four key exchanges). All these messages use air time which add up when considering high-density, high-mobility environments.
- 802.11r, also called .11r, reduces the message exchange to four messages. It does this by overlaying the four key exchange messages on the two authentication and two associations messages.

The table below summarized the roaming options and RADIUS interactions for different security types.

Table 19: Security for different roaming options

Security	Roaming	RADIUS access request?	MAC lookup on RADIUS?
WPA-2/EAP (802.1X)	Default	Yes	Disabled
WPA-2/EAP (802.1X)	.11r	No	Disabled
WPA-2/EAP (802.1X)	OKC	No	Disabled
WPA-2/PSK with passphrase	Default	Yes	Either
WPA-2/PSK with passphrase	.11r	No	Either
Open Access	Disabled	Yes	Either

Enable Fast Roaming

Juniper APs support fast roaming (IEEE 802.11r, Fast BSS Transition), which provides a way for clients using WPA2/WPA3 security to retain authentication while roaming. This prevents them from having to reauthorize and reconnect to the network each time they change APs.

In addition, you can use Marvis to track clients' roaming history and help troubleshoot.

When you change fast roaming settings, the AP radio(s) reinitialize to obtain the new configuration. This will temporarily drop clients from the AP as it restarts.

To enable fast roaming on a WLAN:

1. In the Mist portal, select **Site > Wireless | WLAN** and then click the **Add WLAN** button. Or select an existing WLAN from the list that appears.
2. Go to the **Security** section.
3. Select **WPA3** or **WPA2**, Enterprise or Personal.

4. In the ["Fast Roaming" on page 231](#) section, select the type of roaming you want to use:
 - Default—Local PMKID caching only; there is no sharing of the PMKID between Mist APs on the network. This may be appropriate for some use cases, but does not scale.
 - Opportunistic Key Caching—Non standard, but a widely supported fast roaming method.
 - .11r—Standards-based method of fast roaming, described in 802.11r.
5. Scroll to the top of the page and click **Save**.

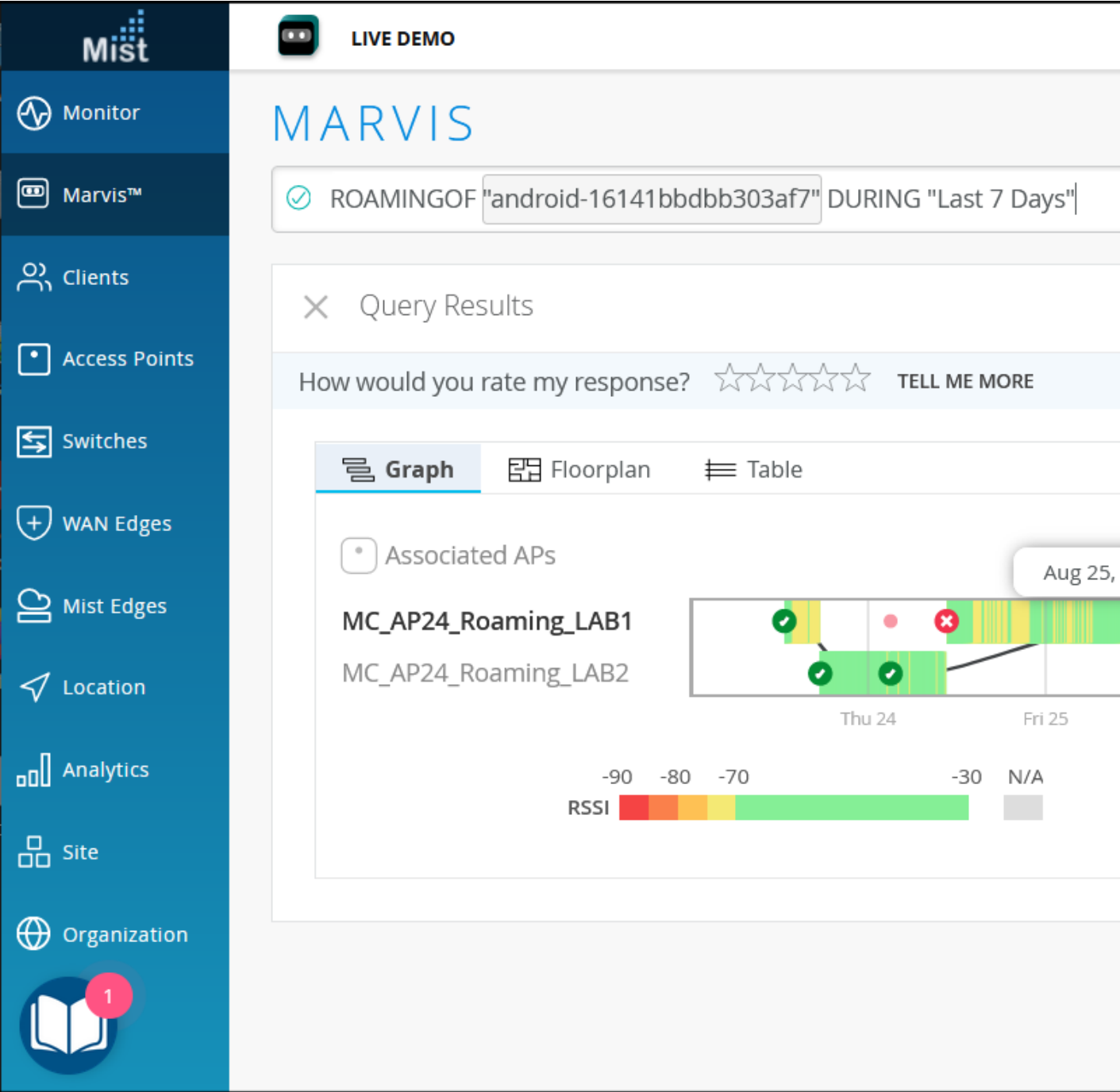
View Roaming History

In the Mist dashboard, you can see how clients roamed between APs, connected to the AP (RSSI strength), and also find things like bad roams. Data for the visualization comes from client events that Juniper APs send to the Mist portal.

You can view the data as a table (mapped against the floor plan) or as a table of events. The following parameters are available:

- roaming of <clientname>
- roaming of <clientmac>
- roaming of client <client name/mac>
- roaming history of <client name/mac>
- show me roaming <client name/mac>
- <client name> roaming history

Figure 19: Track and Troubleshoot Client Roaming



To view the roaming history of a given client:

1. Click **Marvis** on the Mist portal.
2. Click the **Ask a Question** button.
3. In the page that appears, click the query field, and then select **ROAMINGOF** from the drop-down list.

4. Choose a client from the list.
5. You can further qualify the query by adding a time period. Re-click the query field and type **During**, then select a time period from the drop-down list the appears (such as 24 hours or Past 7 days).
6. To view a different client, click the current client-name to re-open the drop-down list and select another from the list.

RADIUS

IN THIS SECTION

- [Enable WPA2/WPA3 Enterprise \(802.1X\) Security on a WLAN | 235](#)
- [Change of Authorization \(CoA\) | 243](#)
- [MAC RADIUS Authentication | 249](#)
- [Guest Access Using RADIUS Server with MAC Authentication Bypass | 251](#)
- [Juniper Mist RADIUS Attributes | 254](#)

Enable WPA2/WPA3 Enterprise (802.1X) Security on a WLAN

SUMMARY

Enable WPA2/WPA3 Enterprise on your WLAN for advanced authentication using a RADIUS server.

IN THIS SECTION

- [Set the WLAN Security Type and Add Your RADIUS Server | 236](#)
- [Use Site Variables to Add a Server | 237](#)
- [NAS Identifier and NAS IP Address | 238](#)
- [CoA/DM Server | 240](#)
- [RadSec | 240](#)
- [Configure an 802.1X WLAN to Redirect Clients to Specific Web Pages | 242](#)

Set the WLAN Security Type and Add Your RADIUS Server

Juniper Mist supports IEEE 802.1X security for WPA2 and WPA3.

NOTE: WPA3 or OWE are mandatory in 6 GHz. So for many customers to adopt 6 GHz, also means adopting WPA3.

To set the WLAN security type and add your RADIUS server:

1. Navigate to the WLAN.

- If the WLAN is in a WLAN template, select **Organization > Wireless | WLAN Templates**, click the template, and then click the WLAN.
- For a site-level WLAN, select **Site > Wireless | WLANs**, and then click the WLAN.

2. In the **Security** section of the Edit WLAN window:

- Click **WPA3** or **WPA2**.
- Click **Enterprise (802.1X)**.

RADIUS authentication is available only when you've selected WPA2/WPA3 and Enterprise (802.1X) in the Security section.

Edit WLAN

The screenshot shows the 'Edit WLAN' configuration page. On the left, there are fields for 'SSID' (containing 'New WLAN'), 'WLAN ID' (with a copy icon), and 'WiFi SLE' (with a checkbox 'Exclude this WLAN from WiFi SLEs (except AP Uptime SLE)'). On the right, the 'Security' section is highlighted with an orange box. It contains a 'Security Type' section with buttons for WPA3, WPA2, Legacy, OWE, Open Access, Enterprise (802.1X), and Personal (SAE). A warning icon and text 'WPA3/EAP* requires firmware v0.9.x or higher' are above the buttons. Below the buttons is a checkbox labeled 'Enable WPA3+WPA2 Transition'.

3. In the **Authentication Servers** section, add your server:

- Click **Add Server**.
- Enter the **Hostname** and the **Shared Secret**.

NOTE: You can use site variables instead of entering the hostname. See ["Use Site Variables to Add a Server" on page 237](#).

- c. Click the check mark button.
4. (Optional) Configure additional options for your WLAN if needed.
5. Save the WLAN configuration, and save the template changes (if the WLAN is part of a WLAN template).

Use Site Variables to Add a Server

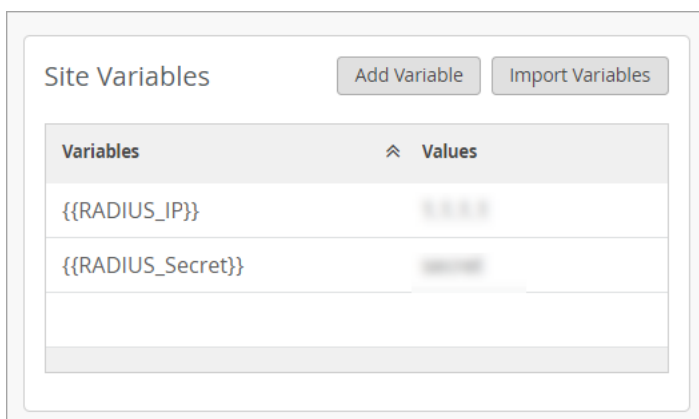
With site variables, you can easily apply the same WLAN configuration to APs at different sites even though certain attributes are different. In this scenario, imagine that Site A and Site B use different RADIUS servers. You'll use variables to add the RADIUS server in the WLAN configuration. Then you'll define the variables differently in the two site configurations.

To use site variables to add a server:

1. Define the site variables in the site configuration for the first site:
 - a. Select **Organization > Site Configuration** from the left menu of the Juniper Mist portal.
 - b. Click the site that you want to configure, such as Site A.
 - c. In the **Site Variables** section, click **Add Variable**.
 - d. Enter a variable name and value for the IP address of the RADIUS server, and then click **Save**.
As shown below, enter `{{RADIUS_IP}}` for **Variable**. Enter the actual IP address for **Value**.

The screenshot shows a modal dialog titled "Add Variables". It has a close button (X) in the top right corner. Inside the dialog, there are two labeled input fields. The first is labeled "Variable" and contains the text "{{RADIUS_IP1}}". The second is labeled "Value" and contains a placeholder IP address "192.168.1.1". At the bottom right of the dialog, there are two buttons: "Save" (in blue) and "Cancel" (in grey).

- e. Add a variable for the Shared Secret, such as `{{RADIUS_Secret}}`, and enter the actual Shared Secret for this server as the **Value**.
After you add the two variables, they appear in the **Site Variables** section of the Site Configuration page.



The 'Site Variables' window shows a table with two columns: 'Variables' and 'Values'. There are two buttons at the top: 'Add Variable' and 'Import Variables'.

Variables	Values
{{RADIUS_IP}}	192.168.1.1
{{RADIUS_Secret}}	secret

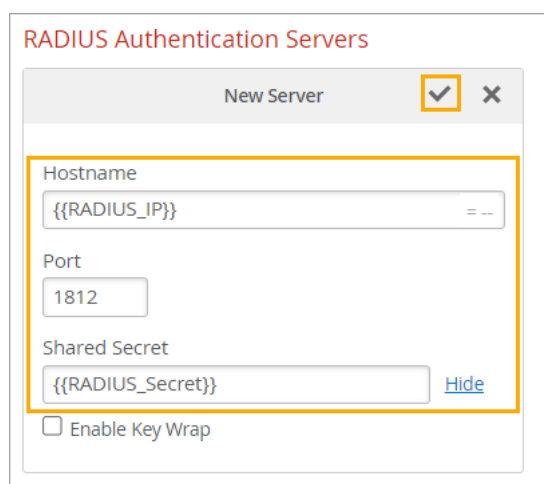
2. Add the same variables to the next site (Site B), and enter the correct values for that site's RADIUS server.

For example, in the site configuration for Site B, add the same `{{RADIUS_Server}}` variable. In the **Value** field, enter the actual IP address for Site B's RADIUS server. Also add the same `{{RADIUS_Secret}}` variable, and enter the correct Shared Secret for the **Value**.

3. Click **Save** at the top-right corner of the Site Configuration page.
4. "Set the WLAN Security Type and Add Your RADIUS Server" on page 236, and enter variables for the server details.

For example, use variables when adding a RADIUS server or a CoA/DM server.

In this example, the Hostname is `{{RADIUS_IP}}` and Shared Secret is `{{RADIUS_Secret}}`.



The 'RADIUS Authentication Servers' window shows a 'New Server' configuration form. The form has a title bar with a checkmark icon and a close button. The form fields are:

- Hostname: `{{RADIUS_IP}}`
- Port: 1812
- Shared Secret: `{{RADIUS_Secret}}` (with a 'Hide' link)
- ☐ Enable Key Wrap

5. Save the WLAN settings.

NAS Identifier and NAS IP Address

When you're enabling 802.1X security on a WLAN, you can add a **NAS Identifier** or **NAS IP Address** to customize the information that is passed to your RADIUS server.

For example, you could enter the site ID (in a site-level WLAN) or a site name variable (in a WLAN template) as the **NAS Identifier**. With this approach, you can associate all activity with a site to facilitate your auditing/accounting processes or to create different RADIUS rules for different sites. Another example is to enter the word *Mist* as the **NAS Identifier**. This way, you can create a different RADIUS rule or guest portal experience for traffic coming from Mist.

If you leave the NAS Identifier field blank, the WLAN ID is used as the NAS ID.

You can enter plain text and variables. The following variables are valid in this field:

- Device Name—{{DEVICE_NAME}}
- Model—{{DEVICE_MODEL}}
- MAC Address—{{DEVICE_MAC}}
- Site Name—{{SITE_NAME}}

This example shows how you can use both text and variables in the ID.

NAS Identifier

mist-guest-{{DEVICE_NAME}}-{{SITE_NAME}}

NAS IP Address

As shown below, when an AP on this WLAN sends an Access-Request, the variables are transformed to identify the AP.

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-01-03 14:53:20.217181	10.7.51.177	10.0.75.28	RADIUS	250	Access-Request id=33

```

> Frame 1: 250 bytes on wire (2000 bits), 250 bytes captured (2000 bits)
> Ethernet II, Src: CiscoMer_83:10:30 (f8:9e:28:83:10:30), Dst: VMware_4f:7:c:d3 (00:0c:29:4f:7:c:d3)
> Internet Protocol Version 4, Src: 10.7.51.177, Dst: 10.0.75.28
> User Datagram Protocol, Src Port: 49431, Dst Port: 1812
< RADIUS Protocol
  Code: Access-Request (1)
  Packet identifier: 0x21 (33)
  Length: 208
  Authenticator: 18bfdd21d7a0c20b7922eb803341cb08
  [The response to this request is in frame 2]
  Attribute Value Pairs
    > AVP: t=User-Name(1) l=14 val=led54bf81f02
    > AVP: t=User-Password(2) l=18 val=Encrypted
    > AVP: t=Service-Type(6) l=6 val=Call-Check(10)
    > AVP: t=NAS-Identifier(32) l=25 val=mist-guest-HQAP1-BRQLAB
      Type: 32
      Length: 25
      NAS-Identifier: mist-guest-HQAP1-BRQLAB
    > AVP: t=Called-Station-Id(30) l=28 val=5C-9B-35-5F-AF-C9:iseguest
    > AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
    > AVP: t=Calling-Station-Id(31) l=19 val=1E-05-4B-F8-1F-02
    > AVP: t=Connect-Info(77) l=24 val=CONNECT 11Mbps 802.11b
    > AVP: t=Connect-Info(77) l=24 val=CONNECT 11Mbps 802.11b
    > AVP: t=NAS-IP-Address(4) l=6 val=10.7.51.177
    > AVP: t=Message-Authenticator(80) l=16 val=0b9c2559c3c4b97f17dfab32c6071ee6
  
```

Alternatively, specify a **NAS IP Address**. Normally, Mist passes through the actual IP address of the AP. But you might want to specify an IP address to be used for all activity, so that you can reference it in your RADIUS policies.

You can add the NAS Identifier or NAS IP Address in the Edit/Create WLAN window.

CoA/DM Server

When you're enabling 802.1X security on a WLAN, you also can add a CoA/DM server on the Edit/Create WLAN window.

Change of Authorization (CoA) allows you to modify authorized RADIUS sessions after initial authentication to meet changing access requirements. For example, enable use cases such as administrator-initiated session resets or guest registration.

For more information about CoA/DM use cases and benefits, see ["Change of Authorization \(CoA\)" on page 243](#).

To add your server, select **Enabled** and enter the **IP Address** and **Shared Secret**. You can keep the default **Port** value or specify a port.

The screenshot shows the 'CoA/DM Server' configuration window. At the top, there are two radio buttons: 'Enabled' (selected) and 'Disabled'. Below this is a 'New Server' dialog box with a checkmark icon and a close 'X' icon. Inside the dialog, there are three input fields: 'IP Address', 'Port' (with the value 3799), and 'Shared Secret' (masked with dots). A 'Reveal' link is next to the 'Shared Secret' field. Below the dialog, there is an 'Event-Timestamp' section with two radio buttons: 'Mandatory' (selected) and 'Optional'.

RadSec

RadSec is a protocol that allows RADIUS servers to transfer data over TCP and TLS for increased security. With RadSec capabilities, you can transfer RADIUS packets through public networks while still ensuring end-to-end security through the transport layer.

To enable RadSec and install the certificates:

1. After you ["Set the WLAN Security Type and Add Your RADIUS Server" on page 236](#), add your RadSec server:
 - a. In the **Authentication Servers** section, select **RadSec** from the drop-down list.
 - b. Enter the **Server Name**.
 - c. Click **Add Server**, and enter the **Hostname**.

Authentication Servers

RadSec ▼

Server Name

Please ensure Mist CA cert is supplied to Radius servers, and Radius CA cert is supplied to Mist in Organization Settings.
[Organization Settings](#)

Server Addresses

New Server ✓ ✕

Hostname

Port

- d. Click the check mark button to add the server.
- e. Save the WLAN configuration, and save the template changes (if the WLAN is part of a WLAN template).
2. Get your Mist certificate from your organization settings:
 - a. Select **Organization** > **Settings** from the left menu of the Juniper Mist portal.
 - b. Under Mist Certificate, click **View Certificate**. Copy the certificate. You'll need it for the next step.
3. Go to your RadSec server and complete these tasks:
 - a. Load the copied Mist certificate.
 - b. Copy your RadSec certificate from your RadSec server. You'll need it for the next step.
4. Return to the Organization Settings page in Juniper Mist portal and add your RadSec certificate:
 - a. Under RadSec Certificates, click **Add a RadSec certificate**.
 - b. Paste the contents of the certificate from your RadSec server.
 - c. Click **Add**.
5. (Optional) If you want to use your own AP RadSec certificates (rather than the unique certificate that Mist generates for each AP), click **Add AP RadSec certificate**, and then enter the private key and the signed certificate for the CA certificate.
6. Click **Save** at the top-right corner of the Organization Settings page.

Configure an 802.1X WLAN to Redirect Clients to Specific Web Pages

SUMMARY

Use the web redirect feature if you want to perform additional compliance checks after clients complete RADIUS authentication.

When you've set up your WLAN with WPA2/WPA3 Enterprise (802.1X) security, you can opt to redirect clients to a webpage (for example, a quarantined portal) after they successfully complete the 802.1X authentication. You can use the web redirect feature to give clients full or partial access to the network.

NOTE: For this feature to work, your firmware version must be 0.7 or newer.

This feature enables you to perform compliance checks on clients with agents installed. During a client authentication, the RADIUS server sends an Access-Accept message containing a URL-redirect RADIUS Attribute Value Pair (AVP) to point the client to a quarantined portal for remediation.

When you enable this feature, the client is initially restricted to DHCP and DNS, specific subnets, and the specified redirect URL. When the client completes the requested action from the portal, then it is fully authorized and allowed to start passing traffic.

To configure a WLAN with the web redirect feature:

1. Navigate to the WLAN.
 - If the WLAN is in a WLAN template, select **Organization > Wireless | WLAN Templates**, click the template, and then click the WLAN.
 - For a site-level WLAN, select **Site > Wireless | WLANs**, and then click the WLAN.
2. In the **802.1X Web Redirect** section, select **Enabled**.

The **802.1X Web Redirect** box is available only for the WLANs with security type **Enterprise (802.1X)**.
3. Specify the allowed subnets and hostnames accessible to the clients being redirected.

802.1X Web Redirect

Allow 802.1X Web Redirect for quarantine or posture assessment based on RADIUS server response containing url-redirect AVP

☒ Enabled
 ☐ Disabled

Web Auth Whitelist

Allowed Subnets

Allowed Hostnames

4. Save the changes.

Change of Authorization (CoA)

SUMMARY

Explore the benefits of adding a Change of Authorization (CoA) server to your WLAN.

IN THIS SECTION

- [Benefits of Change of Authorization \(CoA\) in RADIUS | 243](#)
- [Overview | 244](#)
- [Message Flow | 245](#)
- [Disconnect Message: Posturing | 247](#)
- [Use Case: Guest Access | 247](#)

With Change of Authorization (CoA), you can modify authorized RADIUS sessions after initial authentication to meet changing access requirements. For example, CoA can enable use cases such as administrator-initiated session resets to terminate sessions. CoA also can be used to grant updated access to users after they successfully complete guest registration.

Benefits of Change of Authorization (CoA) in RADIUS

Benefits of Change of Authorization (CoA) in RADIUS:

- Enhances control over active user sessions: By allowing the RADIUS server to send unsolicited messages to the NAS, CoA gives you the ability to modify session characteristics after initial

authentication. This enhanced control can be used to terminate or re-authorize user sessions as required.

- **Overcomes limitations of standard RADIUS protocol:** The standard RADIUS protocol only allows messages to be initiated by the NAS. CoA extends this functionality, providing a more flexible and dynamic approach to session management.
- **Streamlines Network Administration:** The Disconnect Message feature of CoA allows for efficient session resets. This not only saves time and resources, but also simplifies administrative duties.
- **Facilitates Guest Access Management:** The CoA Re-Auth Message feature can be utilized to grant full network access after a guest user registers through a captive portal, making the process of managing guest access smoother and more effective.
- **Supports Vendor-Specific Attributes:** CoA's compatibility with vendor-specific attributes enables effective interoperation between the RADIUS server and NAS devices when sending CoA messages. This contributes to a seamless and efficient network operation.

Overview

When you implement the Change of Authorization (CoA) feature in your RADIUS environment, you empower the RADIUS server to actively send unsolicited messages to the Network Access Server (NAS) to modify session characteristics after the initial authentication process. This proactive approach addresses the limitations of the standard RADIUS protocol, which traditionally permits only the NAS to initiate messages.

In the CoA functionality, there are two primary message types that you can leverage:

- **Disconnect Message:** This message type is designed to terminate user sessions by incorporating the `Acct-Terminate-Cause` attribute in the message. A key application of this feature is when you need to reset sessions for various reasons.
- **CoA Re-Auth Message:** This message type prompts the NAS to re-authorize a session. In scenarios like Guest Access, this is particularly useful when a guest user completes registration through a captive portal, and consequently, the network grants them full access. To convey the re-authorize command effectively, the message employs vendor-specific attributes.

To ensure seamless interoperability between the RADIUS server and NAS devices, you might need to enable support for specific vendor attributes. By doing so, you facilitate the smooth functioning of CoA messages within your network infrastructure.

In summary, by incorporating the CoA feature in your RADIUS environment, you can achieve the following:

- Enable RADIUS servers to actively modify sessions after authentication, overcoming the constraints of the standard protocol.

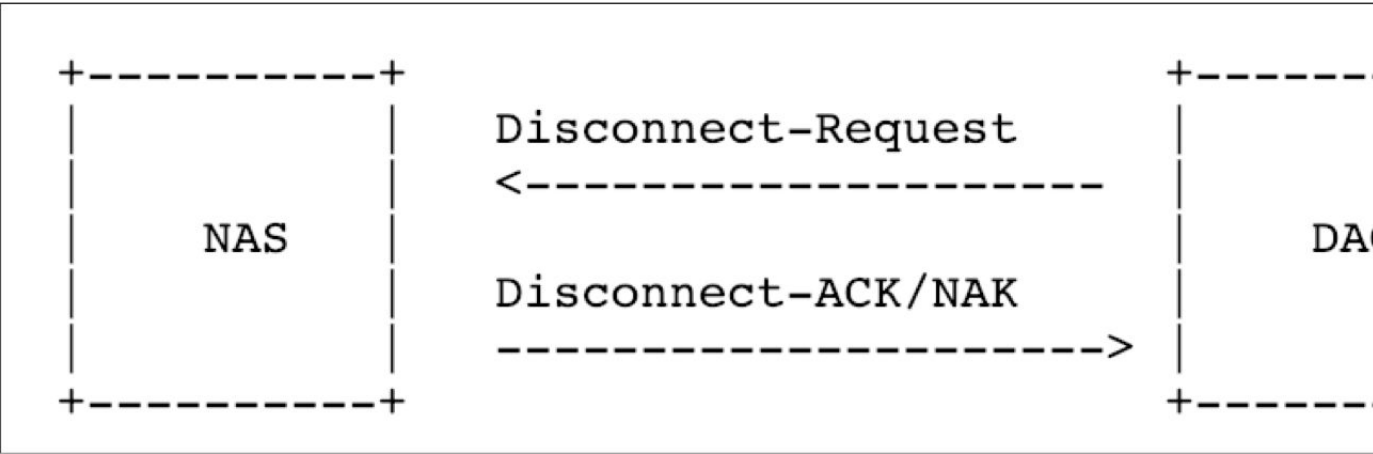
- Utilize two key message types (Disconnect and CoA Re-Auth) to manage different session scenarios effectively.
- Address various use cases, such as administrator-initiated session resets and granting full network access to guest users post-registration.
- Leverage vendor-specific attributes to ensure optimal compatibility and functionality of CoA across different network devices.

By adopting this approach, you can create a more dynamic and responsive network environment, capable of handling diverse session management requirements and providing a robust, secure experience for your users.

Message Flow

1. Disconnect Message: Session Termination

- AVP: Acct-Terminate-Cuase
- Value: Admin-Reset



+	1844	2018-11-20	18:46:49.328865	192.168.8.11	192.168.8.57	RADIUS	146	Disconnect-Request id=9
-	1845	2018-11-20	18:46:49.341454	192.168.8.57	192.168.8.11	RADIUS	86	Disconnect-ACK id=9

▶ Frame 1844: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits)

▶ Ethernet II, Src: Microsof_b2:e8:0c (00:15:5d:b2:e8:0c), Dst: Mist_2e:21:c5 (5c:5b:35:2e:21:c5)

▶ Internet Protocol Version 4, Src: 192.168.8.11, Dst: 192.168.8.57

▶ User Datagram Protocol, Src Port: 11474, Dst Port: 3799

▼ RADIUS Protocol

Code: Disconnect-Request (40)

Packet identifier: 0x9 (9)

Length: 104

Authenticator: a6e95d87167098b954e5e472db344cb0

[The response to this request is in frame 1845]

▼ Attribute Value Pairs

▶ AVP: t=NAS-IP-Address(4) l=6 val=192.168.8.57

▶ AVP: t=Calling-Station-Id(31) l=19 val=68-EC-C5-09-2E-69

▼ AVP: t=Acct-Terminate-Cause(49) l=6 val=Admin-Reset(6)

Type: 49

Length: 6

Acct-Terminate-Cause: Admin-Reset (6)

▼ AVP: t=Event-Timestamp(55) l=6 val=Nov 20, 2018 18:46:49.000000000 PST

Type: 55

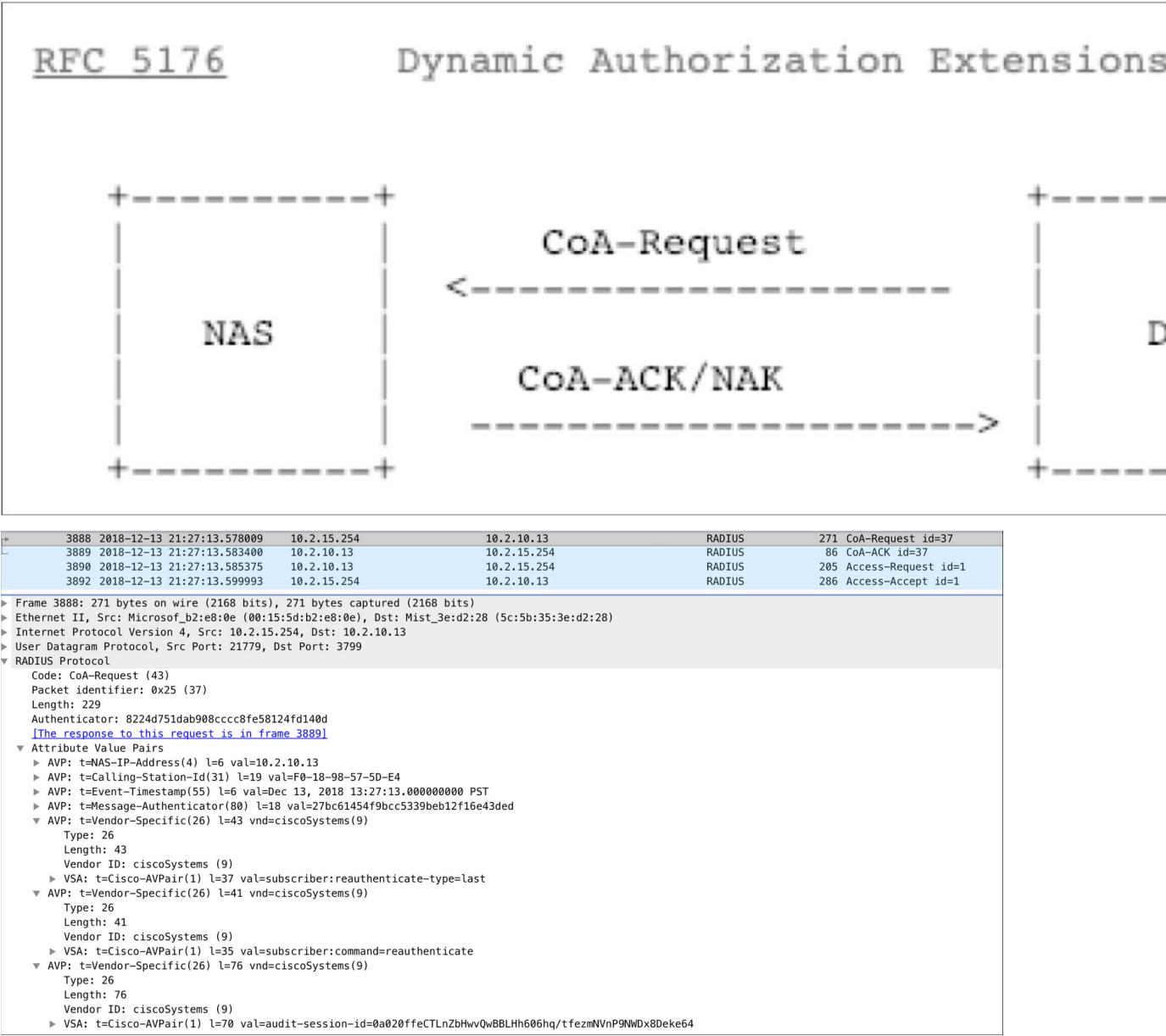
Length: 6

Event-Timestamp: Nov 20, 2018 18:46:49.000000000 PST

▶ AVP: t=Message-Authenticator(80) l=18 val=2701a9e759fa25f15d56e1a50f4ab250

▶ AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)

2. CoA: Session Re-authentication

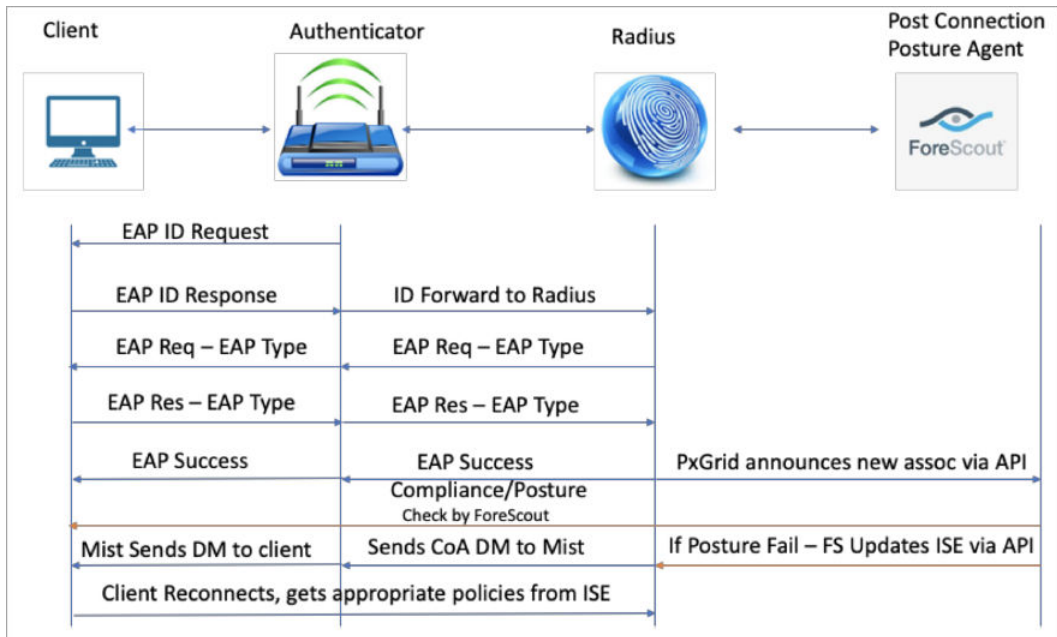


- AVP: Vendor Specific (Cisco-AVP)
- Value: Reauthenticate

CoA Messages that are not applicable to Juniper Mist:

- Session termination with Port-Shut
- Session termination with Port-Bounce

Disconnect Message: Posturing



Use Case: Guest Access

Enable MAC address authentication by RADIUS lookup. In your WLAN configuration, add your server as a RADIUS Authentication Server and CoA/DM Server.

Create WLAN

SSID

New WLAN

WIFI SLE

☐ Exclude this WLAN from WIFI SLES (except AP Uptime SLE)

WLAN Status

☒ Enabled ☐ Disabled

☐ Hide SSID

☐ Broadcast AP name

Radio Band

☒ 2.4 GHz ☒ 5 GHz ☐ 6 GHz

Band Steering

☐ Enable

Client Inactivity

Drop inactive clients after seconds: 1800

Geofence

☐ Minimum client RSSI (2.4G) 0

☐ Minimum client RSSI (5G) 0

☐ Minimum client RSSI (6G) 0

Block clients having RSSI below the minimum

Data Rates

☒ Compatible (allow all connections)

☐ No Legacy (2.4G, no 11b)

☐ High Density (disable all lower rates)

☐ Custom Rates

Security

Security Type

WPA3 WPA2 Legacy OWE **Open Access**

☒ MAC address authentication by RADIUS lookup

☐ Guest Access with Mac Authentication Bypass

☐ Prevent banned clients from associating

Edit banned clients in [Network Security Page](#)

Authentication Servers

RADIUS

RADIUS Authentication Servers

10.2.2.30 : 1812 primary ✓

[Add Server](#)

RADIUS Accounting Servers

☐ Enable Interim Accounting

No accounting servers defined

[Add Server](#)

☐ Randomize authentication and accounting server per AP

NAS Identifier

NAS IP Address

CoA/DM Server

☒ Enabled ☐ Disabled

10.2.2.30 : 3799 primary

[Add Server](#)

When a client associates to this WLAN:

1. The MAC address of the client is sent across to the RADIUS server via an Access-Request.
2. The RADIUS server looks up its database and if the client is not found in the database, sends back a Access_Accept with a redirection URL to the Mist AP.
3. The client now is provided with limited access to the network which includes access to the BOOTP, DNS and RADIUS server.
4. After the client receives an IP, the AP opens a web socket to and listens to any HTTP traffic initiated from the client.

5. Any HTTP traffic initiated from the client is intercepted and is responded with a URL that was sent by RADIUS server.
6. The client is presented with URL. Based on the policy: it might be a sponsored portal, a self registration portal or a hotspot portal.
7. Once the client provides necessary info on the URL, the ISE now install this client's MAC address in its database and also issues a CoA (Change of Authorization) request with a command to re-authorize this client.
8. The Mist AP, upon receiving the CoA request, acknowledges the request and sends back the same Access_Request as in step 1.
9. At this point, the client is available in the RADIUS server database and hence would be provided with a Access-Accept without any restrictions of URL-Redirect and the client would have network connectivity based on the policies defined.

MAC RADIUS Authentication

SUMMARY

Authenticate clients by using a RADIUS server to look up their MAC address and allow connections only from listed devices.

When configuring a WLAN, you can enable MAC Authentication with any security type except WPA3/WPA2 Enterprise.

Edit WLAN

At least one RADIUS authentication server must be added

SSID

New WLAN

WLAN ID

16fadeb2-8c5e-4275-ab0a-1821d4d0ddc4

WiFi SLE

☐ Exclude this WLAN from WiFi SLEs (except AP Uptime SLE)

WLAN Status

☒ Enabled ☐ Disabled

☐ Hide SSID

☐ Broadcast AP name

Radio Band

☒ 2.4 GHz ☒ 5 GHz ☐ 6 GHz

Security

Security Type

WPA3 WPA2 Legacy OWE **Open Access**

☒ MAC address authentication by RADIUS lookup

☐ Guest Access with Mac Authentication Bypass

☐ Prevent banned clients from associating

Edit banned clients in [Network Security Page](#)

Authentication Servers

RADIUS

RADIUS Authentication Servers

No authentication servers defined

[Add Server](#)

Keep these points in mind:

- **RADIUS Server**—A RADIUS Server is used to authenticate using MAC address as username and password.
- **Change of Authorization(COA)**—An external server can instruct the reauthentication of a client.
- The VLAN can be untagged, tagged, or dynamic.
- Guest Access with MAC Authentication Bypass can be enabled to leverage RADIUS-based guest portals.

NOTE: You also can configure Guest Access with MAC Authentication Bypass. For help, see "[Guest Access Using RADIUS Server with MAC Authentication Bypass](#)" on page 251.

Guest Access Using RADIUS Server with MAC Authentication Bypass

SUMMARY

Enable this option if you want to leverage RADIUS-based portals for guest access.

IN THIS SECTION

- [Flow of Guest Access Using RADIUS Server with MAC Authentication Bypass | 251](#)
- [WLAN Configuration | 252](#)
- [RADIUS Configuration | 252](#)

First get familiar with the flow of guest access using RADIUS server with MAC Authentication Bypass (MAB). Then configure your WLAN. Finally, do additional RADIUS configuration for authentication policies and authorization profiles.

Flow of Guest Access Using RADIUS Server with MAC Authentication Bypass

1. A WLAN is created in Juniper Mist with MAB being performed using RADIUS Lookup.
2. When a client associates to this WLAN, its MAC address is sent to the RADIUS server using an ACCESS_REQUEST.
3. The server looks for the MAC address in its database.
 - If the client is not found in the database, sends back an ACCESS_ACCEPT with a redirection URL to the Juniper Mist AP, and the flow continues with Step 4.
 - If the client is found in the database, the flow goes to Step 10.
4. The client is provided with limited access to the network which includes access to the BOOTP, DNS, and RADIUS server.
5. After the client receives an IP, the AP opens a web socket and listens to any HTTP traffic initiated from the client.
6. Traffic is intercepted and is responded with the redirect URL that was sent by RADIUS server.
7. The client is redirected to the specified URL. Based on your configured policy, it might be a sponsored portal, a self-registration portal, or a hotspot portal.
8. After the client provides the necessary info, the client's MAC address is installed in the database and a CoA (Change of Authorization) request is issued to reauthorize the client.
9. Upon receiving the CoA request, the AP acknowledges the request and sends back the same ACCESS_REQUEST as in step 2.

10. The client is available in the RADIUS server database and is provided with an ACCESS-ACCEPT without any restrictions of URL-Redirect and the client has network connectivity based on your configured policies.

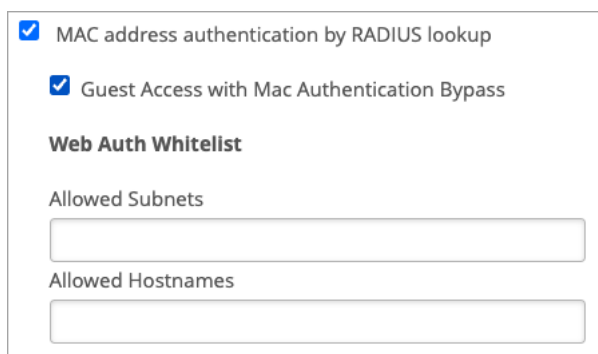
WLAN Configuration

Create or edit a WLAN, enable MAB, and add your RADIUS server.

1. Create or navigate to the WLAN that you want to set up with Guest Access using RADIUS Server with MAC Authentication Bypass.
 - For a template-based WLAN, navigate to **Organization > WLAN Templates**, click the template (or create a template), and then click the WLAN (or add a WLAN).
 - To select a site-specific WLAN, navigate to **Site > WLANs**, and then click the WLAN (or add a WLAN).
 -

For more information, see ["Configure a WLAN Template" on page 119](#).

2. In the **Security** section of the Create/Edit WLAN window, select **MAC address authentication by RADIUS lookup** and **Guest Access with Mac Authentication Bypass**.



☒ MAC address authentication by RADIUS lookup

☒ Guest Access with Mac Authentication Bypass

Web Auth Whitelist

Allowed Subnets

Allowed Hostnames

3. (Optional) Use the **Allowed Subnets** and **Allowed Hostnames** fields to specify resources that guests can access in the redirect state.

If these fields are left blank, the RADIUS server is the only IP address that guests can access.

4. Add your RADIUS server, as described in ["Enable WPA2/WPA3 Enterprise \(802.1X\) Security on a WLAN" on page 235](#).

Complete the additional RADIUS configuration tasks below.

RADIUS Configuration

Configure RADIUS policies and profiles to support the authentication flow.

1. **Authentication Policy**—Configure an authentication policy to “continue” if the user is not found in the database. This allows the client to get an IP and be placed in the redirect state.

Authentication Policy (3)

+	Status	Rule Name	Conditions	Use	Hits	Actions
	✓	MAB	OR <ul style="list-style-type: none"> Wired_MAB Wireless_MAB 	Internal Endpoints Options: If Auth fail: REJECT If User not found: CONTINUE If Process fail: DROP	48	⚙️

2. Authorization Policies: Configure two policies that will be hit during the process of the guest access flow.

✎	Status	Rule Name	Conditions	Use	Hits	Actions
✎	✓	Wi-Fi_Guest_Access	AND <ul style="list-style-type: none"> IdentityGroup-Name EQUALS Endpoint Identity Groups:HotSpot_Endpoints Wireless_MAB 	PermitAccess	0	⚙️
✎	✓	Wi-Fi_Redirect_to_Guest_Login	Wireless_MAB	Guest_Access	47	⚙️
	✓	Basic_Authenticated_Access	Network_Access_Authentication_Passed	PermitAccess	0	⚙️
	✓	Default		DenyAccess	0	⚙️

- The first policy is *Wifi_Redirect_to_Guest_Login*, which applies when the RADIUS server receives the request. This policy provides partial access to the client. (See Steps 2-3 of the flow.)
- The second policy is *Wifi_Guest_Access*, which applies upon successful completion of the CoA request. This policy provides the client with full access. (See Steps 9-10 of the flow.)

3. Authorization Profile: Configure a RADIUS authorization policy as shown in the example below. This policy provides the redirect URL for Steps 6-7 of the flow.

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Common Tasks

Centralized Web Auth: ACL: ACL_WEBAUTH_REDIRECT Value: Sponsored Guest Portal (default)

Display Certificates Renewal Message: ☒

Static IP/Host name/FQDN: 10.2.15.254

Suppress Profiler CoA for endpoints in Logical Profile: ☐

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
 Airespace-ACL-Name = ACL_WEBAUTH_REDIRECT
 cisco-av-pair = url-redirect=ACL_WEBAUTH_REDIRECT
 cisco-av-pair = url-redirect=https://10.2.15.254:port/gateway?sessionId=SessionId&value=port=7079c670-7159-11e7-a355-005056ba474&daysToExpiry=value&action=cwa

Juniper Mist RADIUS Attributes

SUMMARY

Use this information to understand the RADIUS attributes that have been implemented in Juniper Mist™ access points (APs).

IN THIS SECTION

- [Authentication Attributes | 254](#)
- [RADIUS Accounting Attributes | 259](#)
- [Dynamic Authorization Extensions | 262](#)

Authentication Attributes

IN THIS SECTION

- [IETF Standard Authentication Attributes | 254](#)
- [Supported Vendor-Specific Attributes | 257](#)

RADIUS services can be enabled on the Mist APs for WLAN user authentication. RADIUS services are *required* for WLANs implementing IEEE 802.1X authentication.

During authentication, the AP sends user information to the RADIUS server in an Access-Request message. The RADIUS server returns one of these responses:

- **Access-Reject**—Unconditionally denies access to the requested network resource. Failure reasons can include an invalid credential or an inactive account.
- **Access-Challenge**—Requests additional information from the user such as a secondary password, PIN, token, or card. Access-Challenge is also used in more complex authentication when a secure tunnel is established between the user and the Radius Server such as authentication using Extensible Authentication Protocol (EAP).
- **Access-Accept**—Permits access to the requested network resource. The Access-Request often includes additional configuration information for the user using return attributes.

IETF Standard Authentication Attributes

The following table describes the standard authentication attributes that have been implemented in Juniper Mist APs in accordance with RFC 2865. Additional extensions have also been implemented following the recommendations in RFC 2868 and RFC 2869.

Table 20: IETF Standard Authentication Attributes

Attribute Name	Type	RFC	Description
User-Name	1	RFC 2865	The <i>User-Name</i> attribute is forwarded in the <i>Access-Request</i> and indicates the name of the user to be authenticated.
User-Password	2	RFC 2865	The <i>User-Password</i> attribute is forwarded in the <i>Access-Request</i> . It indicates the password of the user to be authenticated, or the user's input following an <i>Access-Challenge</i> .
NAS-IP-Address	4	RFC 2865	<p>The <i>NAS-IP-Address</i> attribute is forwarded in the <i>Access-Request</i> and indicates the IP Address of the AP requesting user authentication.</p> <p>You can configure this attribute in the RADIUS settings for a WLAN. All APs on a WLAN send the configured value.</p>
Service-Type	6	RFC 2865	The <i>Service-Type</i> attribute is forwarded in the <i>Access-Request</i> and indicates the type of service the user has requested, or the type of service to be provided. The attribute value is always set to <i>Framed-User</i> by the AP for 802.1X/EAP WLANs or to <i>Call-Check</i> for the MAC-Auth enabled WLANs.
Framed-MTU	12	RFC 2865	The <i>Framed-MTU</i> attribute is forwarded in the <i>Access-Request</i> and indicates the Maximum Transmission Unit (MTU) to be configured for the user. The attribute value is always set to <i>1200</i> by the AP.
State	24	RFC 2865	The <i>State</i> attribute is available to be forwarded in the <i>Access-Challenge</i> . It must be sent unmodified from the client to the server in the <i>Access-Request</i> reply to that challenge, if any.
Called-Station-Id	30	RFC 2865	The <i>Called-Station-Id</i> attribute is forwarded in the <i>Access-Request</i> and indicates the BSSID and ESSID that the authenticating user is associated with. The Access Point will forward the attribute value using the following formatting: <i>XX-XX-XX-XX-XX-XX:ESSID</i> .
Calling-Station-Id	31	RFC 2865	The <i>Calling-Station-Id</i> attribute is forwarded in the <i>Access-Request</i> and indicates the MAC address of the authenticating user. It is only used in <i>Access-Request</i> packets. The Access Point will forward the attribute value using the following formatting: <i>XX-XX-XX-XX-XX-XX</i> .

Table 20: IETF Standard Authentication Attributes *(Continued)*

Attribute Name	Type	RFC	Description
NAS-Identifier	32	RFC 2865	<p>The <i>NAS-Identifier</i> attribute is forwarded in the <i>Access-Request</i>. You can configure this attribute in the RADIUS settings for a WLAN. All access points on a WLAN send the configured value.</p> <p>You can use variables to send the device name, model, MAC address, and site name. The variables are:</p> <p>{{DEVICE_NAME}}</p> <p>{{DEVICE_MODEL}}</p> <p>{{DEVICE_MAC}}</p> <p>{{SITE_NAME}}</p>
Proxy-State	33	RFC 2865	The proxy-state attribute is sent by proxy-server to another server when forwarding Access-Requests; this must be returned unmodified in the Access-Accept, Access-Reject or Access-Challenge and removed by the proxy server before sending the response to the network access server
NAS-Port-Type	61	RFC 2865	The <i>NAS-Port-Type</i> attribute is forwarded in the <i>Access-Request</i> and indicates the type of physical connection for the authenticating user. The attribute value is always set to <i>Wireless-802.11</i> by the Access Point.
Connection-Info	77	RFC 2869	The <i>Connection-Info</i> attribute is forwarded in the <i>Access-Request</i> and indicates the data-rate and radio type of the authenticating user. The Access Point will forward the attribute value using the following formatting: <i>CONNECT XXMbps 802.11X</i> .
EAP-Message	79	RFC 2869	The <i>EAP-Message</i> attribute is forwarded in <i>the Access-Request</i> , Access-Challenge, Access-Accept and Access-Reject and encapsulates Extended Access Protocol (EAP) packets.
Message-Authenticator	80	RFC 2869	The <i>Message-Authenticator</i> attribute is forwarded in the <i>Access-Request</i> and may be used to prevent spoofing of CHAP, ARAP or EAP Access-Request packets.
Tunnel-Private-Group-ID	81	RFC 2868	The <i>Tunnel-Private-Group-ID</i> attribute is forwarded in the <i>Access-Accept</i> and indicates the numerical VLAN ID to be assigned to the authenticating user. The attribute value must be set to a numerical value between 1 and 4094 or a string representing a named VLAN.

Table 20: IETF Standard Authentication Attributes (*Continued*)

Attribute Name	Type	RFC	Description
Filter-Id	11	RFC 2865	<p>The <i>Filter-Id</i> attribute may be forwarded in the <i>Access-Accept</i> and indicates user role client will be associated with. User Groups are used by the Mist WxLAN policy framework to assign network firewall rules.</p> <p>Format: Group-Name</p> <p>Example: employee</p>

Supported Vendor-Specific Attributes

The following table outlines vendor-specific attributes (VSAs) that are supported by Juniper Mist Access Points in accordance with RFC 2865.

Table 21: Supported Vender-Specific Attributes

Attribute Name	Type	Vendor ID	Attribute Number	Formatting	Description
Airespace-Interface-Name	26	14179	5	String	<p>The <i>Airespace-Interface-Name</i> attribute may be forwarded in the <i>Access-Accept</i> to indicate the dynamic VLAN membership of an 802.1X or RADIUS MA authenticated user. Returned attribute value is always a string formatted the VLAN. VLAN Name to VLAN ID translation must be configured under using VLAN IDs or Variables.</p> <p>Format: VLAN-Name</p> <p>Example: employee-vlan</p>
Airespace-ACL-name	26	14179	6	String	<p>The <i>Airespace-ACL-Name</i> attribute may be forwarded in the <i>Access-Accept</i> indicates user role client will be associated with. User Groups are used by WxLAN policy framework to assign granular network resource restriction</p> <p>Format: Group-Name</p> <p>Example: employee</p>

Table 21: Supported Vender-Specific Attributes (*Continued*)

Attribute Name	Type	Vendor ID	Attribute Number	Formatting	Description
Aruba-User-Role	26	14823	1	String	<p>The <i>Aruba-User-Role</i> attribute may be forwarded in the <i>Access-Accept</i> to indicate user role client will be associated with. User Groups are used by WxLAN policy framework to assign granular network resource restriction.</p> <p>Format: Group-Name</p> <p>Example: employee</p>
Cisco-AVPair	26	9	1	String	<p>The <i>Cisco-AVPair</i> attribute may be forwarded in the <i>Access-Accept</i> to inform the Mist Access Point that a client needs to be redirected for portal authentication and specify the redirect-URL location. This attribute is typically used for Guest Access integrations with Cisco ISE or Aruba Clearpass RADIUS servers or to enable Posture Redirect functionality for 802.1X/EAP users.</p> <p>AVPair URL Redirect</p> <p>Format: url-redirect=<URL value></p> <p>Example: url-redirect=https://ise28.89mistilbs.org:8443/portal/gateway?sessionId=0a004b1c/Jtf4peiJ5A8nPreloHRRITWvmhDCbnH3qXQ8MngtoA&portal=71984f3f55e-4439-ba6e-903d9f77c216&action=cwa&token=1f7dca2cc907b1ad56ee4880</p> <p>AVPair PSK</p> <p>The <i>Cisco-AVPair</i> attribute may also contain PSK attribute, indicating to the Access Point which passphrase is assigned to a certain client. Note that to provide a PSK value to the AP, two Cisco AVPair attributes must be sent simultaneously, one indicating that PSK will be sent in ASCII format and the other AVPair providing the actual Pre-Shared Key value.</p> <p>Format:</p> <p>psk-mode=ascii</p> <p>&</p> <p>psk=<passphrase></p>

Table 21: Supported Vender-Specific Attributes (*Continued*)

Attribute Name	Type	Vendor ID	Attribute Number	Formatting	Description
Eleven-Authentication-Find-Key	26	52970	3	TLV	The <i>Eleven-Authentication-Find-Key</i> attribute is used to supply additional information to the supported RADIUS servers to simplify wireless client lookup via RADIUS, removing the need to pre-associate a wireless client with a particular PSK ahead of time. This attribute is a TLV according to RFC6929 that contains multiple sub-attributes inside.
Eleven-EAPOL-Frame-2 (sub-attribute)			1	Octets	Eleven-EAPOL-Frame-2 sub attribute contains the second EAPOL frame sent from the wireless client to the Access Point during a 4way handshake
Eleven-EAPOL-Anonce (sub-attribute)			2	Octets	Eleven-EAPOL-Anonce sub attribute contains the first EAPOL frame sent from the Access Point to the wireless client during a 4way handshake
Eleven-EAPOL-SSID (sub-attribute)			3	String	Eleven-EAPOL-SSID sub-attribute contains current SSID name that the wireless client is trying to associate to
Eleven-EAPOL-APMAC (sub-attribute)			4	Octets	Eleven-EAPOL-APMAC sub-attribute contains BSSID in <code>xxxxxxxxxxxx</code> format
Eleven-EAPOL-STMAC (sub-attribute)			5	Octets	Eleven-EAPOL-STMAC sub-attribute contains wireless client MAC address in <code>xxxxxxxxxxxx</code> format

RADIUS Accounting Attributes

You can enable or disable RADIUS Accounting Servers in the WLAN configuration. You can use RADIUS accounting information to track users' network usage for billing purposes and to gather data for general network monitoring.

The following accounting configurations are supported:

- **Start-Stop**—Juniper Mist APs forward Accounting-Requests at the start and end of the user sessions. This behavior is enabled by default, as soon as at least one accounting server is configured under WLAN.

- **Start-Interim-Stop**—Juniper Mist APs forward Accounting-Requests at the start and end of the user sessions and periodically during the lifetime of the sessions. The Framed-IP-Address attribute will be included in the accounting messages.

NOTE: The Interim-Update interval can also be dynamically overridden by sending Acct-Interim-Interval (85) AVP from the RADIUS server.

The following table describes the standard RADIUS accounting attributes that have been implemented in the Juniper Mist Access Points in accordance with RFC 2866.

Table 22: Supported Accounting Attributes

Attribute Name	Type	RFC	Description
User-Name	1	RFC 2865	The <i>User-Name</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the name of the user.
NAS-IP-Address	4	RFC 2865	The <i>NAS-IP-Address</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the IP Address of the Access Point.
Framed-IP-Address	8	RFC 2865	<p>The <i>Framed-IP-Address</i> attribute is forwarded in the Accounting-Request packets and indicates current or last-known IP address of the wireless client. It is only sent when Interim Accounting is enabled on the WLAN.</p> <p>Note: during the first client connection, when client has not yet obtained an IP address, Framed-IP-Address AVP will be missing in the first Accounting-Start packet. However, as soon as the AP learns client IP address, it will send asynchronous (outside of normal Interim-Accounting update interval) Accounting Interim-Update message with Framed-IP-Address information.</p>
Class	25	RFC 2865	The <i>Class</i> attribute is optionally forwarded in the <i>Access-Accept</i> and should be sent unmodified by the client to the accounting server as part of the <i>Accounting-Request</i> packet if accounting is enabled. Mist Access Points support sending multiple Class attributes for each client.
Called-Station-Id	30	RFC 2865	The <i>Called-Station-Id</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the BSSID and ESSID that the user is associated with. The Access Point will forward the attribute value using the following formatting: <i>XX-XX-XX-XX-XX-XX:ESSID</i> .
Calling-Station-Id	31	RFC 2865	The <i>Calling-Station-Id</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the MAC address of the user. The Access Point will forward the attribute value using the following formatting: <i>XX-XX-XX-XX-XX-XX</i> .

Table 22: Supported Accounting Attributes (*Continued*)

Attribute Name	Type	RFC	Description
NAS-Identifier	32	RFC 2865	The <i>NAS-Identifier</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the user defined identifier configured under WLAN settings.
Acct-Status-Type	40	RFC 2866	The <i>Acct-Status-Type</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates whether the <i>Accounting-Request</i> marks the status of the accounting update. Supported values include <i>Start</i> , <i>Stop</i> and <i>Interim-Update</i> .
Acct-Delay-Time	41	RFC 2866	The <i>Acct-Delay-Time</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how many seconds the Access Point has been trying to send the accounting record for. This value is subtracted from the time of arrival on the server to find the approximate time of the event generating this <i>Accounting-Request</i> .
Acct-Input-Octets	42	RFC 2866	The <i>Acct-Input-Octets</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how many octets have been received from the user over the course of the connection. This attribute may only be present in <i>Accounting-Request</i> records where the <i>Acct-Status-Type</i> is set to <i>Stop</i> .
Acct-Output-Octets	43	RFC 2866	The <i>Acct-Output-Octets</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how many octets have been forwarded to the user over the course of the connection. This attribute may only be present in <i>Accounting-Request</i> records where the <i>Acct-Status-Type</i> is set to <i>Stop</i> .
Acct-Session-Id	44	RFC 2866	The <i>Acct-Session-Id</i> attribute is forwarded in the <i>Accounting-Request</i> and provides a unique identifier to make it easy to match <i>start</i> , <i>stop</i> and <i>interim</i> records in an accounting log file.
Account-Authentic	45	RFC 2866	The <i>Account-Authentic</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how the user was authenticated. When RADIUS accounting is enabled the Access Point will set this value to <i>RADIUS</i> .
Acct-Session-Time	46	RFC 2866	The <i>Acct-Session-Time</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how many seconds the user has received service for. This attribute may only be present in <i>Accounting-Request</i> records where the <i>Acct-Status-Type</i> is set to <i>Stop</i> .

Table 22: Supported Accounting Attributes (*Continued*)

Attribute Name	Type	RFC	Description
Acct-Input-Packets	47	RFC 2866	The <i>Acct-Input-Packets</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how many packets have been received from the user over the course of the connection. This attribute may only be present in <i>Accounting-Request</i> records where the <i>Acct-Status-Type</i> is set to <i>Stop</i> .
Acct-Output-Packets	48	RFC 2866	The <i>Acct-Output-Packets</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how many packets have been forwarded to the user over the course of the connection. This attribute may only be present in <i>Accounting-Request</i> records where the <i>Acct-Status-Type</i> is set to <i>Stop</i> .
Acct-Terminate-Cause	49	RFC 2866	The <i>Acct-Terminate-Cause</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how the session was terminated. This attribute may only be present in <i>Accounting-Request</i> records where the <i>Acct-Status-Type</i> is set to <i>Stop</i> .
Event-Timestamp	55	RFC 2869	The <i>Event-Timestamp</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the time that the accounting event occurred on the Access Point.
NAS-Port-Type	61	RFC 2865	The <i>NAS-Port-Type</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the type of physical connection for the user. This attribute value is always set to <i>Wireless-802.11</i> by the Mist Access Point.

Dynamic Authorization Extensions

IN THIS SECTION

- [Disconnect-Request Attributes | 263](#)
- [CoA-Request Attributes | 263](#)

The RADIUS authentication protocol originally did not support unsolicited messages sent from the RADIUS server to the Access Point. However, there are many instances in which it is desirable for changes to be made to session characteristics without requiring the Access Point to initiate the exchange.

To overcome these limitations several vendors have implemented additional RADIUS extensions that support unsolicited messages sent from the RADIUS server to an Access Point. These extensions

support Disconnect and Change-of-Authorization (CoA) messages that can be used to terminate an active user session or change the characteristics of an active session.

- **Disconnect-Request**—Causes a user session to be terminated. The Disconnect-Request packet identifies the NAS as well as the user session to be terminated by inclusion of the identification attributes shown in table 3.0.
- **CoA-Request**—Causes session information to be dynamically updated on the Access Point.

Disconnect-Request Attributes

The following table describes the required dynamic authorization attributes for Disconnect Requests.

The minimum set of attributes outlined in the table is sufficient for the Disconnect to work. If additional attributes are sent by the RADIUS server, some will also be evaluated (for example NAS-IP-Address value must match current IP address of the Mist AP, or Acct-Session-Id must match wireless client session ID), while other attributes that are not supported will be ignored (for example Acct-Terminate-Cause).

Table 23: Disconnect-Request Attributes

Attribute Name	Vendor	Attribute Number	Description
Event-Timestamp	IETF	55	Time at which Disconnect-Request has been issued. Time will be checked by the Mist AP. If clock drift is too big, Disconnect Request will be discarded. <i>Event-Timestamp attribute validation can be optionally disabled under WLAN configuration.</i>
Calling-Station-Id	IETF	31	MAC address of the user in XX-XX-XX-XX-XX-XX format.

CoA-Request Attributes

The following table describes the required dynamic authorization attributes for CoA Requests.

The minimum set of attributes outlined in the table is sufficient for the CoA to work. Other attributes also will be evaluated if sent by the RADIUS server and supported by Juniper Mist. For example, NAS-IP-Address value must match current IP address of the Juniper Mist AP, or Acct-Session-Id must match the wireless client's session ID. Attributes that are not supported will be ignored (for example, any additional Cisco-AVPair attributes).

Table 24: CoA-Request Attributes

Attribute Name	Vendor	Attribute Number	Description
Event-Timestamp	IETF	55	Time at which Disconnect-Request has been issued. Time will be checked by the Mist AP. If clock drift is too big, Disconnect Request will be discarded. <i>Event-Timestamp attribute validation can be optionally disabled under WLAN configuration</i>
Calling-Station-Id	IETF	31	MAC address of the user in XX-XX-XX-XX-XX-XX format.
Cisco-AVPair	Cisco (9)	1	subscriber-command:reauthenticate

Preshared Keys

IN THIS SECTION

- [Preshared Keys | 265](#)
- [Multi-Preshared Keys | 269](#)
- [Rotating PSKs | 272](#)
- [Leveraging Roles in a PSK \(Use Case\) | 275](#)
- [Enable Client Onboarding with a BYOD PSK Portal | 279](#)
- [Create a WxLAN Policy to Override Client VLANs | 287](#)

Preshared Keys

SUMMARY

Use this information to understand the benefits of using preshared keys (PSKs) and the options for enabling and managing PSK in the Juniper Mist™ portal.

IN THIS SECTION

- [Viewing and Managing PSKs | 268](#)
- [WPA Support | 268](#)

Juniper APs support preshared key (PSK), which is a standard for secure-channel encryption that does not require an additional authentication server. When enabled for a WLAN, clients must present a secure passphrase to connect to the wireless network.

Using PSKs makes onboarding new users to the SSID simple—they receive an email with a QR code to the SSID and authenticate using the PSK. In addition, you can use PSKs in WxLAN policies to control access on a per-user and per resource basis. For example, you could make it so wireless cameras can only connect to the video feed server, so if a camera is ever hacked, there is no path from it to the rest of the network. See ["Leveraging Roles in a PSK \(Use Case\)" on page 275](#).

You can view or edit PSKs in the Juniper Mist dashboard according to WLAN, to site, and for the org as a whole (the latter requires an Access Assurance subscription See— ["Features That Require Access Assurance" on page 272](#)).

Figure 20: Preshared Key Management for the Organization

Monitor

Marvis™

Clients

Access Points

Switches

WAN Edges

Mist Edges

Location

Analytics

Site

Organization

1

LIVE DEMO

26

Pre-Shared Keys

SSID		Role
Mist_IoT	11	Creditcarddevices
Demo-MPSK	7	Guest
Live_demo_only	3	IoT
Live_demo_do_not_remove	2	mistdemocorp
StorePSK	2	mistdemodefault

Filter

<input type="checkbox"/>	Key Name	MAC	Passphrase	Max U
<input type="checkbox"/>	Associate-PSK-v105		*****	Unlin
<input type="checkbox"/>	credit		*****	Unlin
<input type="checkbox"/>	creditcredit-new		*****	Unlin
<input type="checkbox"/>	echos		*****	5 Ma
<input type="checkbox"/>	Envoy visitor #107333836		*****	Unlin
<input type="checkbox"/>	Envoy visitor #108109416		*****	Unlin

You can use and assign PSKs individually, per user, or by groups, to multiple users (this is known as ["Multi-Preshared Keys" on page 269](#)). Likewise, you can assign a given PSK to a set number of devices, or it can be open-ended. The former requires firmware version 0.10 or later.

Key rotation, which is the timely expiration and replacement of PSKs, can also be automated via email. See ["Rotating PSKs" on page 272](#).

Figure 21: Site-Level Preshared Keys.

Juniper Mist™ **LIVE DEMO**

Pre-Shared Keys

site Live-Demo ▼

Create pre-shared keys for groups or individual clients for additional security

<input type="checkbox"/>	Key Name	⌵ Email	Passphrase	Usage
<input type="checkbox"/>	1st_Graders		*****	Multiple users
<input type="checkbox"/>	camera		*****	Multiple users
<input type="checkbox"/>	Envoy visitor #76255483		*****	Multiple users
<input type="checkbox"/>	Envoy visitor #76256860		*****	Multiple users
<input type="checkbox"/>	iot-users		*****	Multiple users
<input type="checkbox"/>	NewSudheerKey		*****	Multiple users
<input type="checkbox"/>	SudheerKey		*****	Multiple users
<input type="checkbox"/>	Test3		*****	Single user (aa:bb:cc:dd)

Viewing and Managing PSKs

On the Mist dashboard the PSK is listed alongside the client on the WiFi Clients page for the organization (select **Clients** > **WiFi Clients**). Here you can also find any given wireless client by their preshared key, or for multi-preshared keys (MPSK), group all the clients using the same key, just like you'd expect with traditional 802.1X accounting.

Best practices for PSK management include refreshing the PSK weekly, which you can also do from this page.

Figure 22: View and Manage Preshared Keys

The screenshot shows the Mist dashboard interface. On the left, the 'Clients' menu is expanded, showing options for App Clients, BLE Clients, WiFi Clients, and Wired Clients. The main content area displays the 'WiFi Clients' page for the 'Live-Demo' site. At the top, there are statistics for 21 Wireless Clients, 18 5 GHz, 3 6 GHz, 10 802.11ac, 10 802.11ax, and 1 802.11n. Below this is a table of clients with the following columns: AP Name, SSID, Pre-shared Key, Device Type, and IPv4 Address. The table lists 21 clients, including various devices like Zebra TC57, Mac, Apple, and Intel Corporate.

	AP Name	SSID	Pre-shared Key	Device Type	IPv4 Address
<input type="checkbox"/> Unknown	LD_RS_Support	Live_demo_only		Unknown	10.100.0.115
<input type="checkbox"/> android-1e2ffb2d7900b121	MC_AP24_Roaming_LAB1	LD_roaming		Zebra TC57	192.168.1.225
<input type="checkbox"/> android-5bd931eb44a4d28b	LD_RS_Support	Live_demo_do_not_remove		Zebra TC58	10.100.0.14
<input type="checkbox"/> everest	LD_Kitchen-2	Live_demo_do_not_remove		Mac	10.100.1.66
<input type="checkbox"/> Rodos-Mac-mini	LD_NewBobFriday	Live_demo_do_not_remove		Apple	10.100.0.82
<input type="checkbox"/> rthone	LD_Kitchen-2	Live-Demo-NAC		Mac MBP 16" M2 Max 2023	10.100.0.56
<input type="checkbox"/> iOS	LD_NewBobFriday	Live_demo_do_not_remove		iOS	10.100.0.102
<input type="checkbox"/> Apple	LD_Kitchen-2	Live_demo_only		Apple	10.100.0.107
<input type="checkbox"/> iOS	LD_Kitchen-2	Live_demo_only		iOS	10.100.0.55
<input type="checkbox"/> jrosentha-T480A	LD_MHMD	Live_demo_only		Intel Corporate	10.100.0.16
<input type="checkbox"/> MistsMarvisMRP	LD_RS_Support	Live_demo_only		Annie	10.100.0.19

From the WiFi clients page, you can drill-down to the Pre-Shared Keys page for a given client, or you can open the page by selecting **Organization** > **Wireless** | **Pre-Shared Keys** in the menu. Either way, you can find clients by PSK name, by SSID, or by role. You can also view and manage PSKs used in the organization, view all currently active clients and see which, if any, PSKs are due to expire soon.

WPA Support

Mist APs support WPA2-PSK, which you can use for multiple passphrases. WPA2-PSK uses Advanced Encryption Standard (AES).

Juniper APs running firmware v0.9.x or later support WPA3/802.1X WPA3 (Wi-Fi Protected Access 3) PSK. APs running firmware v0.8.x or later support WPA3/SAE. WPA3-Enterprise supports 192-bit encryption (128-bit for personal mode) individualized data encryption using Advanced Encryption

Standard (AES). WPA3-Enterprise supports 192-bit encryption, and WPA3-Personal mode supports 128-bit encryption.

For the sake of backward compatibility with legacy devices, Juniper Mist also supports (but does not recommend) WPA-PSK and Temporal Key Integrity Protocol (TKIP), the Wi-Fi Protected Access (WPA) security protocol, and Wired Equivalent Privacy (WEP), all of which have known vulnerabilities. These Legacy options are not available by default. If you must enable WPA with PSK/TKIP, Multimode, or WEP keys, contact the Juniper Mist support team by creating a support ticket. For help with support tickets, see the [Juniper Mist Management Guide](#).

Multi-Preshared Keys

SUMMARY

Use this information to understand the benefits of multi-preshared keys (MPSKs) and the options for enabling MPSK in the Juniper Mist™ portal.

IN THIS SECTION

- [Lookup Methods | 270](#)
- [MPSK Features and Benefits | 271](#)
- [Features That Require Access Assurance | 272](#)

The Juniper Mist portal supports multi-preshared keys (MPSK) (also known as private preshared keys or PPSK). Each PSK in the Mist platform gets its own key name, which is essentially an identity that can be leveraged for user-level accountability for WxLAN policies, key rotation, and visibility in the Mist dashboard. See the Mist API documentation for information on cloud-based PSK. MPSK uses WPA2/PSK.

For example, you can assign PSKs individually to corresponding VLANs for dynamic network segmentation within the same SSID. This is especially useful for IoT devices in, say, healthcare or warehouse environments because you can group devices of the same type, assign a PSK, or segment the different groups to different VLANs.

You can also use MPSKs in multi-user environments to automatically, and securely, onboard new devices, as well as authorize users' BYOD. MPSK/email pairs are especially useful in WxLAN policies, for example, when creating a policy for personal WLANs. Note that "[certain aspects and features of PSK require an Access Assurance subscription](#)" on page 272.

Lookup Methods

With WPA2, there are two methods of MPSK lookup for WLANs in the Mist portal: Local and RADIUS. With WPA3, you can enable RADIUS PSK.

- (WPA2 Only) With **Local** lookup, keys are stored on the AP and can be created at both the site and organization level. It does not require connectivity to the Mist Cloud. Local is typically used for IoT, where PSKs are configured per device. Key rotation occurs at the hour of expiration. Local lookup supports up to 5000 PSKs per AP. It's a good option when you want to support devices rather than clients and when the keys don't need to be changed often.

Security

Security Type

WPA3 **WPA2** Legacy OWE Open Access

Enterprise (802.1X) **Personal (PSK)**

☐ Passphrase

☐ TKIP with passphrase

☒ Multiple passphrases

☒ Local ☐ RADIUS PSK

Site or Org level keys used by this WLAN will be stored locally on the Access Points.

☐ Configure as a personal WLAN
(Multiple devices per PSK, no connectivity between devices with different PSKs)

- (WPA2 and WPA3) With **RADIUS** lookup, PSKs are stored on the RADIUS server and the AP sends a MAC authentication request to it. The RADIUS server returns the passphrase using Cisco AVPair. RADIUS is typically used when integrating with a third-party PSK hosting service. RADIUS lookup support includes Identity Services Engine (Cisco ISE), Aruba ClearPass, RG Nets, and Eleven Wireless. RADIUS lookup requires firmware version 0.8x or later.

Security ! RADIUS PSK Lookup requires firmware v0.8.x or higher

Security Type

WPA3 **WPA2** Legacy OWE Open Access

Enterprise (802.1X) **Personal (PSK)**

☐ Passphrase
☐ TKIP with passphrase
☒ Multiple passphrases

☐ Local ☒ RADIUS PSK

Default PSK [Reveal](#)

Default VLAN ID

RADIUS lookup will be performed for this WLAN to find the key. Keys are stored on the external RADIUS server.

☐ MAC address authentication by RADIUS lookup
☐ Use EAPOL v1 (for legacy clients)
☐ Prevent banned clients from associating
 Edit banned clients in [Network Security Page](#)

Fast Roaming

☒ Default
☐ .11r

MPSK Features and Benefits

MAC-less client device onboarding

- You don't have to plan out PSK or client MAC address pairings.
- Avoids the pitfalls of MAC randomization.

PSK life-cycle management

- Create, rotate, and auto-expire PSKs.
- If ever a single PSK is compromised, you can quickly identify the blast radius and rotate the affected PSK without disturbing other clients.

Dynamic traffic engineering

- Assign VLANs per PSK.
- Create user-specific WxLAN policies by assigning roles to PSKs.

Personal WLAN

- You can create virtual broadcast domains on a per-PSK basis.

User-level accountability

- With PSK naming you can view client sessions in the Mist portal.
- Supports third-party audit integration.

Automatic PSK provisioning and rotation

- Onboard users with their SSO login.
- Automatically create an identity pair from the SSO user name and a personal PSK.

Features That Require Access Assurance

You need an Access Assurance subscription for some MPSK features, including:

- Cloud-based PSK lookup.
- Support for more than 5000 PSKs at the organization level.
- Automatic client onboarding, and PSK portals.
- Features of the PSK life-cycle management, including PSK expiration, rotation, and per-PSK accounting and visibility (on the Wi-Fi Clients page of the Mist portal).

The Access Assurance subscription is calculated according to the number of concurrent, active, client devices that are using MPSK as aggregated over a seven-day period (which accommodates usage peaks).

Rotating PSKs

SUMMARY

Rotating PSKs is a best practice to reduce network exposure in the event that a key is compromised. Use

IN THIS SECTION

- [Manually Rotate A PSK | 274](#)

this information to understand the benefits of PSK rotation and the steps involved to rotate keys.

PSK rotation is the practice of replacing old encryption keys with new ones, typically on a scheduled basis. Regular PSK rotation reduces the amount of time the network is exposed in the event a key is compromised. We recommend PSK rotation, especially for IoT devices, and if you assign keys on a per-device basis.

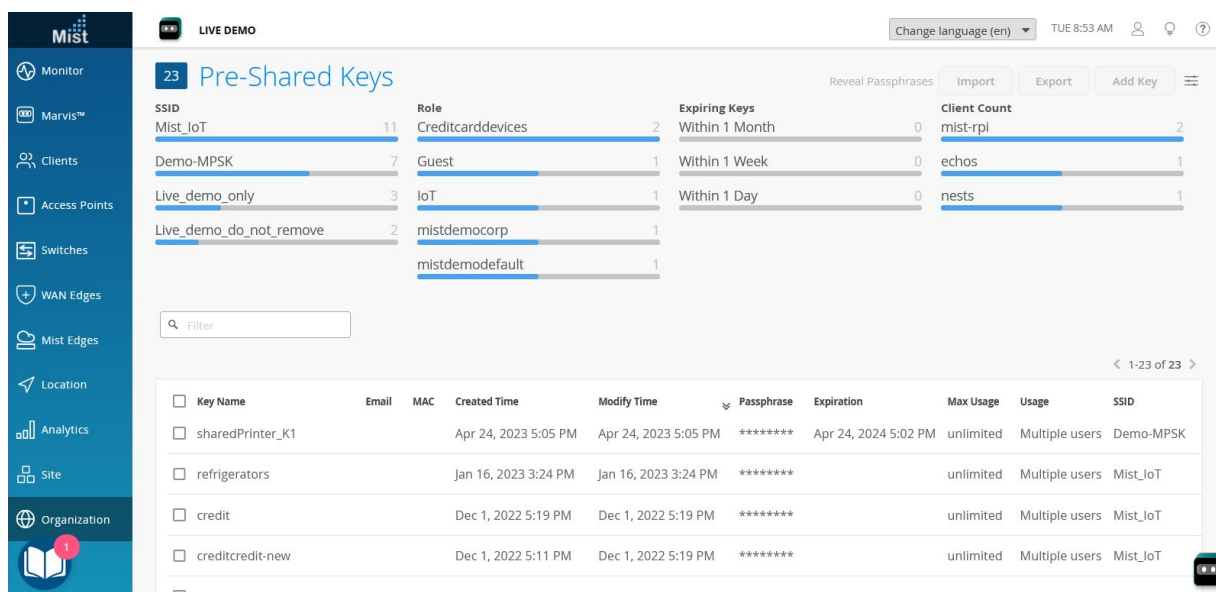
Certain aspects and features of PSK require an Access Assurance subscription. See ["Features That Require Access Assurance" on page 272](#) for details.

When creating or updating a PSK, you can set an expiration date for the key, or a duration during which time the key is valid. Likewise, you can schedule automatic PSK rotation for both users and devices. When a key rotation occurs, only the key itself will change. There is no disruption to the existing connection for IoT devices, and any VLANs, roles, and so on that are associated with the PSK will remain the same.

You can enable e-mail notifications for users when a PSK is created or updated. You can enable this option at the organization level (**Organization > Pre-Shared Keys**) or site level (**Site > Pre-Shared Keys**). You can also configure e-mail reminders to notify users about upcoming organization-level PSK expiry. Note that you can set the reminders only from the **Organization > Pre-Shared Keys** page or **Organization > Client Onboarding** page.

For wireless users, where you may want nominal participation, you can schedule PSK rotation and handle it through email. Users are automatically sent the new passphrase and expiration date for the SSID, as well as a QR code so they can conveniently make the update and reconnect using the new PSK.

Figure 23: PSK Status and Rotation



Manually Rotate A PSK

In the following procedure we will manually rotate a PSK by duplicating the old key (which includes all the existing properties and associations), switching the users over to the duplicate, and then getting rid of the original so it can no longer be used. The rotation is transparent to users.

To manually rotate a PSK:

1. From the Mist portal, select **Organization > Wireless > Pre-Shared Keys** and select the Key Name for the PSK that you want to rotate.
2. Click the **More** button that appears at the top of the page (it appears when you select the key name and choose **Duplicate**).
3. In the Duplicate Pre-Shared Keys page that opens, select **Modify Original Keys** and then **Add Suffix**.
4. In the **Add Suffix** field, type **-old**.
5. Under the New Key Options, select **Create New Passphrases** and set how many characters you want the passphrase to be.
6. Click **Duplicate** to create a copy of the key.

Back in the Pre-Shared Keys page, you'll see the new and old keys. Both are active, and you can click either one to see the number of clients (current to the previous hour).

Now you can reconfigure your clients with a new passphrase. Once there are no more active clients on the old PSK (that is, all of the clients have been moved to the new PSK), you can remove the old key manually or let it expire.

Leveraging Roles in a PSK (Use Case)

SUMMARY

Create PSK roles and leverage them in policies to get granular control over network resources and to limit the so-called blast radius if a PSK is compromised.

IN THIS SECTION

- [Assign a Role to a PSK | 275](#)
- [Create Labels for the PSK Role and Resources | 276](#)
- [Create the WxLAN Access Policy | 278](#)

You can use PSK roles in a WxLAN policy for network segmentation. For example, you can limit IoT devices so that they can only access specified resources. For example, only allow a Wi-Fi camera to access the Wi-Fi camera feed server.

In this use case, you'll use a role to allow BYOD devices to access the internet while blocking them from accessing your private networks.

By following this use case, you'll see how to create a role on an end-user PSK and how to create organization-level labels to define the role and the network resources. Finally, you'll create a WxLAN policy to specify the resources that the BYOD devices can or cannot access. When a client uses PSK to log on to the network, they'll inherit the specified role and will be able to access only the resources allowed by the policy.

Assign a Role to a PSK

To assign a role to a PSK:

1. From the left menu of the Juniper Mist portal, select **Organization < Wireless | Preshared Keys**
2. Click an existing end-user PSK, or click **Add Key** to create one.
3. On the Create/Edit Pre-Shared Key window, enter the following information to create the key for this example.
 - **Key Name**—Enter an email address.
 - **VLAN ID**—Enter a VLAN ID on the public network.

- **Role**—Enter **BYOD**.

Edit Pre-Shared Key

SSID + Passphrase must be unique for keys for multiple users.

Key Name
user@company.net

SSID
Demo-MPSK

VLAN ID
600
(1 - 4094)

Passphrase
***** [Reveal](#)
Characters: 16 [Generate random](#)

Expiration Date
Duration

Expire in: 1 Months

Usage
Multiple users

Max Usage ☒ Unlimited Devices ☐ Set number of devices

Role ☒ Role requires firmware v0.10.x or higher
BYOD

☐ Notify user by email

Active Clients Registered Clients

0 Active Clients

[Delete](#) [Save](#) [Cancel](#)

NOTE: For more information, see ["Preshared Keys" on page 265](#).

4. Click **Save**.

Create Labels for the PSK Role and Resources

In this use case, you'll create three labels to define the role and resources:

- A user group label to define BYOD devices.
- An IP address label to define the resources that the role can access (the internet).
- An IP address label to define the resources that the role cannot access (the private networks).

NOTE: To find out more about what labels are and how they work, see ["Using Labels in a WxLAN Policy" on page 139](#).

To create labels for use with the PSK role:

1. From the left menu of the Juniper Mist portal, select **Organization > Wireless | Labels**.
2. Click **Add Label** in the top-right corner of the page.
3. On the New Label page, enter the information for the BYOD label as follows:

Organization Labels : [New Label](#)

Label Name

BYOD

Label Type

AAA Attribute ▼

This is a User label if used in Template WxLan

Label Values IS

User Group ▼

User Group Values ⓘ

BYOD

Note: Requires newer firmware

- **Label Name**—Enter **BYOD**.
 - **Label Type**—Select **AAA Attribute**.
 - **Label Values**—Select **User Group**.
 - **User Group Value**—Enter **BYOD**.
4. Click **Create** at the top-right corner of the page.
 5. Create a label that will be used to define the internet. For this label, use these values:

- **Label Name**—Enter **internet**.
- **Label Type**—Select **IP Address**.
- **Label Values**—Enter **0.0.0.0/0**.

6. Create a label that will be used to define the private networks. For this label, use these values:

- **Label Name**—Enter **private-networks**.
- **Label Type**—Select **IP Address**.
- **Label Values**—Enter **10.10.10.0/8,172.168.0.0/12,192.168.0.0/16**

NOTE: By using the RFC1918 definition for private networks, you can cover all the internal networks.

You've created the necessary labels and are ready to use them in the WxLAN access policy.

Create the WxLAN Access Policy

To complete this use case, you need to use the role and the labels to create a policy that specifies the resources that the BYOD role can access.

DHCP and DNS traffic are automatically allowed. You don't need to create a special rule for them. In addition, it's good to know that WxLAN rules are enforced at the AP, and for the egress traffic only. Ingress rules are automatically adjusted based on outgoing traffic.

To create a WxLAN policy:

1. From the left menu of the Juniper Mist portal, navigate to the WLAN template where you want to add the rule.

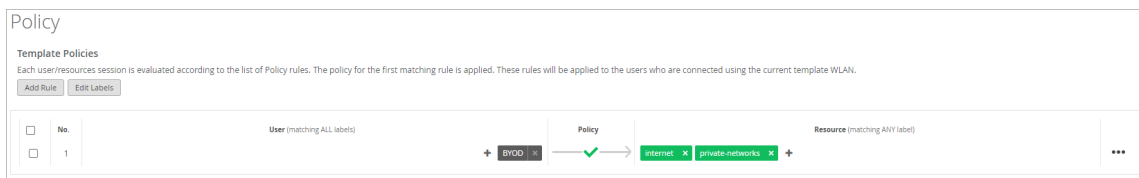
NOTE:

["WxLAN Access Policies" on page 329](#)

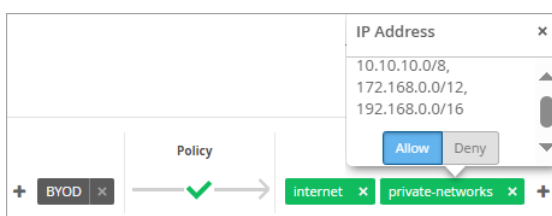
2. In the Policy section, click **Add Rule**.
3. In the **User** column, click the Add (+) button, and select the **BYOD** label.
4. Under **Policy**, keep the default, **Allow**.
5. Under **Resources**:

- Click the Add (+) button, and then click the **internet** label.
- Click the Add (+) button, and then select **private network**.

At this point, all resources are allowed, as shown below.



- Click the icon that you added for **private networks**, and then click **Deny**.



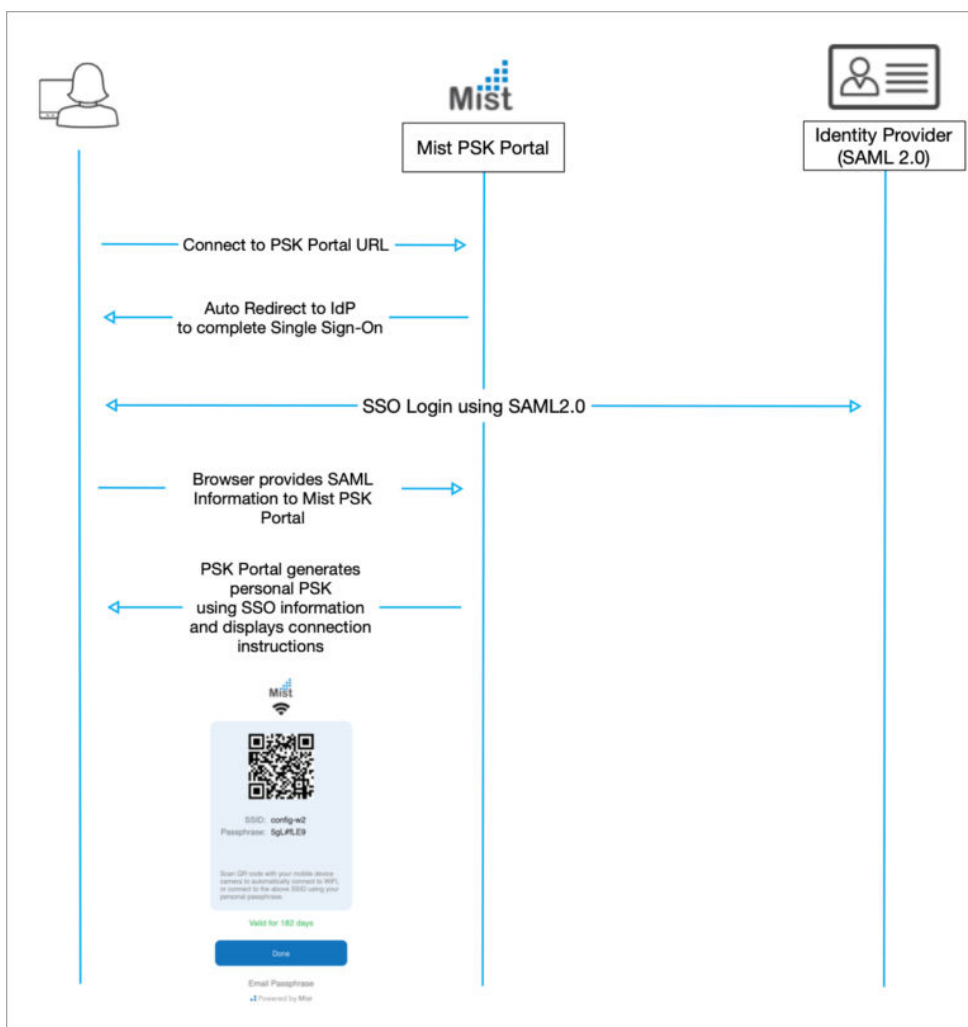
6. Click the ellipsis button (...) on the right side of the page, and then click **Enable**.
7. Click **Save** at the top-right corner of the page.

Enable Client Onboarding with a BYOD PSK Portal

SUMMARY

Set up a client onboarding workflow for a Bring Your Own Device (BYOD) Preshared Key (PSK) Portal. These portals allow users to self-provision PSKs.

When everything is set up, the “workflow” for the BYOD PSK Portal will look like this:



Before You Begin

- Obtain and activate a Juniper Mist™ Access Assurance subscription. For information about subscription management, see the [Juniper Mist Management Guide](#).
- In your Juniper Mist organization, configure at least one organization-level WLAN with Multi-PSK enabled (either local or cloud PSK options are fine). For more information, see ["Multi-Preshared Keys" on page 269](#).
- In your IdP admin console, configure a SAML 2.0 app integration. Your PSK portal will integrate with this application to enable Single Sign-On (SSO) access to your portal users. You can use a wide variety of IdPs (such as Okta and Microsoft Azure), as long as they support SAML 2.0. For help setting up a SAML 2.0 app integration, see your IdP documentation.

Copy the following information from your SAML 2.0 app integration, and save it so that you can use it to set up your PSK portal in Juniper Mist.

- Signing Algorithm

- Issuer ID

NOTE: Your IdP admin console might show a different name for the Issuer ID. For example:

- In Okta, this value is called Identity Provider Issuer.
- In Azure, it's called Azure AD Identifier.

- SSO URL

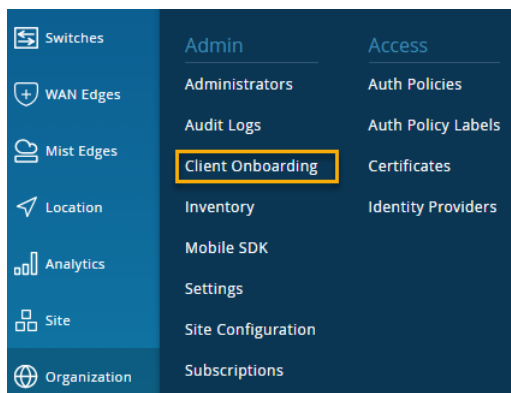
NOTE: Your IdP admin console might show a different name for the SSO URL. For example:

- In Okta, this value is called Identity Provider Single Sign-On URL.
- In Azure, it's called Login URL.

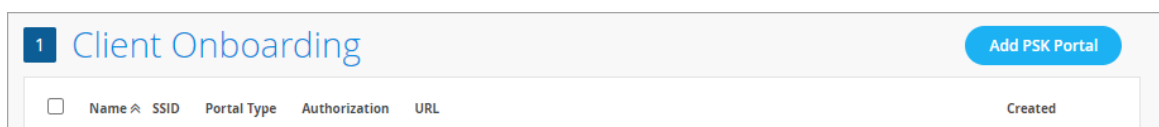
- Certificate—Copy the full text of the certificate, from the *BEGIN CERTIFICATE* line through the *END CERTIFICATE* line.

To set up client onboarding with a BYOD PSK Portal:

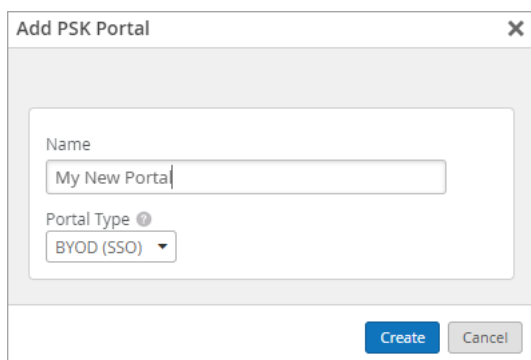
1. From the left menu of the Juniper Mist portal, select **Organization > Admin | Client Onboarding**.



2. Click **Add PSK Portal** at the top-right corner of the Client Onboarding page.

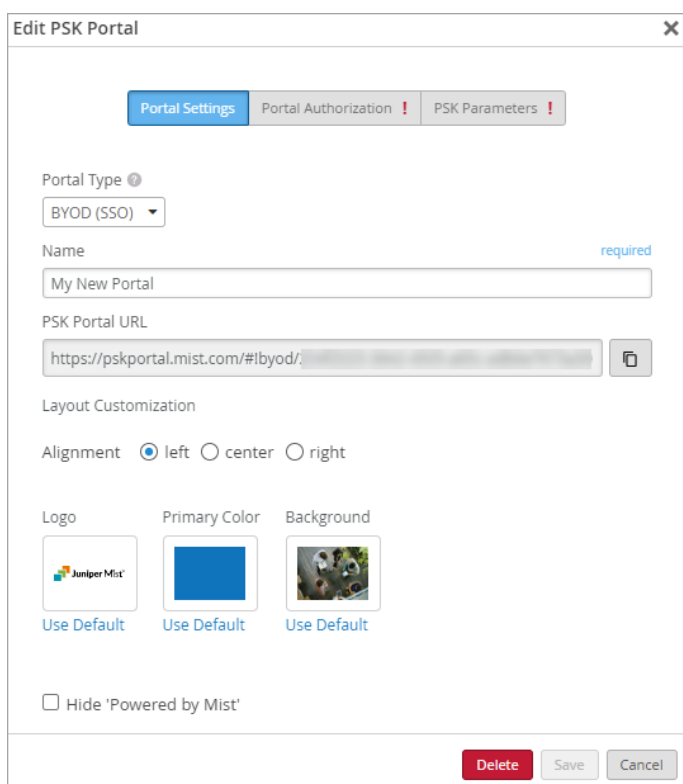


3. In the Add PSK Portal pop-up window, enter a **Name**, select **BYOD (SSO)** as the portal type, and then click **Create**.



The 'Add PSK Portal' dialog box contains a 'Name' text field with the value 'My New Portal' and a 'Portal Type' dropdown menu set to 'BYOD (SSO)'. At the bottom are 'Create' and 'Cancel' buttons.

4. On the **Portal Settings** tab of the Edit PSK Portal window:
 - Keep the default layout options, or make changes to customize the sign-in screen.
 - Copy the **PSK Portal URL** so that you can provide it to your users.



The 'Edit PSK Portal' window has three tabs: 'Portal Settings' (active), 'Portal Authorization', and 'PSK Parameters'. Under 'Portal Settings', the 'Portal Type' is 'BYOD (SSO)'. The 'Name' field is 'My New Portal' with a 'required' label. The 'PSK Portal URL' field contains 'https://pskportal.mist.com/#byod/'. Below is a 'Layout Customization' section with 'Alignment' set to 'left' (radio buttons for left, center, right). There are three 'Use Default' links for 'Logo' (Juniper Mist), 'Primary Color' (blue square), and 'Background' (nature image). A checkbox for 'Hide 'Powered by Mist'' is at the bottom. At the very bottom are 'Delete', 'Save', and 'Cancel' buttons.

5. On the **Portal Authorization** tab of the Edit PSK Portal window:
 - Enter the **Issuer**, **Signing Algorithm**, **SSO URL**, and **Certificate** that you copied from your app integration in your IdP admin console.
 - Select a **Name ID Format**. Most people use the e-mail address for the name ID. If you use a different identifier for your IdP user accounts, select **Unspecified**.

Edit PSK Portal

Portal Settings | **Portal Authorization** | PSK Parameters

SSO Issuer is required
Provide your Identity Provider information to authenticate end-users.

Issuer

Name ID Format
☒ Email ☐ Unspecified

Signing Algorithm
 SHA256

Certificate

SSO URL

Portal SSO URL
 https://api.mist.com/api/v1/pskportal/254f2025-3642-4505-a65c-adb6e7673e

Delete Save Cancel

6. Copy the **Portal SSO URL**.
7. Open a separate browser window, and complete these steps to finalize your SAML 2.0 app integration:
 - a. Navigate to your IdP admin console.
 - b. Go to the settings for your SAML 2.0 app integration.
 - c. Enter the copied value into the appropriate field to identify your Juniper Mist PSK portal to your IdP. For help, see your IdP documentation.
 - d. Save the changes.

Your IdP might have different names for the field where you need to paste the Portal SSO URL. Consider the following examples, and see your IdP documentation for help.

Okta Example

In this example, the **Portal SSO URL** from Juniper Mist is copied into the appropriate fields in the Okta Admin Console.

Portal SSO URL

<https://api.mist.com/api/v1/pskportal/>

A SAML Settings

General

Single sign on URL [?](#)

<https://api.mist.com/api/v1/pskportal/>

☒ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) [?](#)

<https://api.mist.com/api/v1/pskportal/>

Microsoft Azure Example

In this example, the **Portal SSO URL** from Juniper Mist is copied into the appropriate fields in the Azure Admin Console.

Portal SSO URL

<https://api.mist.com/api/v1/pskportal/>

Basic SAML Configuration

Save | Got feedback?

[Want to leave this preview of the SAML Configuration experience? Click here to leave the preview. →](#)

Identifier (Entity ID) * [?](#)

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

<https://api.mist.com/api/v1/pskportal/> ☒ [Add identifier](#)

Patterns: <https://api.MISTCLOUDREGION.mist.com/api/v1/saml/SSOUID/login>

Reply URL (Assertion Consumer Service URL) * [?](#)

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

<https://api.mist.com/api/v1/pskportal/> ☒ [Add reply URL](#)

Patterns: <https://api.<MISTCLOUDREGION>.mist.com/api/v1/saml/<SSOUID>/login>

8. Return to the Juniper Mist portal.
9. On the **PSK Parameters** tab of the Edit PSK Portal window:
 - Select the **SSID** (required).

NOTE: The list includes only SSIDs for organization-level WLANs that have Multi-PSK enabled.

- Adjust the optional settings as needed. For example:
 - Set the **Passphrase Settings** to enforce your policies for password complexity.
 - Specify a **VLAN ID** if you want the users of this portal to be assigned to a particular VLAN. To use this option, you must enter a VLAN that is included in the VLAN list for the WLAN.
 - Adjust the **PSK Validity** options to set the expiration period and to send reminders before key expiration.
 - Under **Max Usage**, you can limit the number of devices that can connect to your portal.
 - Under **Role**, you can specify a role to limit access to certain types of user accounts (using the roles that you set up for your IdP user accounts).

Edit PSK Portal

Portal Settings Portal Authorization ! **PSK Parameters !**

SSID is required
The following settings will determine passphrase complexity and validity parameters, as well as network policy and segmentation rules applied to Pre-Shared Keys created via this PSK Portal.

SSID
Select

VLAN ID ⓘ
(1 - 4094)

Passphrase Settings
Characters: 8

Includes
☒ Letters
☒ Numbers
☒ Special Characters
 000_%@#&\$

PSK Validity
PSK would remain valid for 6 Months

☐ Send reminder 2 Days before key expiration

Max Usage
☒ Unlimited Devices ☐ Set number of devices

Role

Delete Save Cancel

10. Click **Save** at the bottom of the Edit PSK Portal window.

NOTE: The button is unavailable until you enter the required settings on the various tabs. The required settings are labeled in red type.

11. Verify that your portal works as expected by going to the **PSK Portal URL** that you copied from the Portal Settings tab of the Edit PSK window.
12. Provide your users with the **PSK Portal URL** so that they can connect to your portal.

TIP: Create a CNAME in your DNS to create a more user friendly URL that is associated with your domain.

Create a WxLAN Policy to Override Client VLANs

SUMMARY

Support per site VLAN flexibility with Multi-Pre-Shared Key (mPSK) by creating WxLAN policies that override client VLANs.

Let's illustrate the value of this feature by looking at a common use case when implementing Multiple-PSK. In this scenario, Site A needs the flexibility to use VLAN A for PSK A and VLAN B for PSK B. Site X needs to use VLAN X for PSK A and VLAN Y for PSK B. You can create WxLAN policies to assign VLANs to clients based on the PSK user role. The WxLAN-driven VLANs override any other VLAN assignments on a client. For example, this policy would override a dynamic VLAN that was received from RADIUS.

You can use this feature in addition to the normal methods of assigning a user to a VLAN by policy such as through RADIUS AVPs (Tunnel-Private-Groupid or Airespace-Interface-Name) or VLAN attached to MPSK.

Requirements

- APs must have firmware version 0.14.29091 or newer.
- The VLANs must be configured either in the VLAN list in the WLAN settings, ETH0 port configuration, or Mist Tunnel.

To create a WxLAN policy to override client VLANs:

1. From the left menu of the Juniper Mist portal, select **Organization > Admin | Labels**.
2. Click **Add Label**, and set up the label for the VLAN that you want to use in your WxLAN policy:
 - **Label Type**—Select **VLAN**.
 - **VLAN ID**—Enter the VLAN ID that you want to associate with this label.


In this example, *vlan5* is the name of the label, and *5* is the VLAN ID.


← Organization Labels : **New Label**


Label Name

Label Type

VLAN

 VLAN Label requires firmware v0.14.x or higher

Label Value  IS

VLAN ID (1-4094) 

3. Click **Save** to save the new label.
4. Click **Add Label**, and set up the label for the PSK user role that you want to use in your WxLAN policy:
 - **Label Type**—Select **AAA Attribute**.

NOTE: Alternatively, you could create a client label, but it is suggested to use AAA Attribute at scale.

- **Label Values**—Select **User Group**.
- **Username Values**—Enter a user role to associate with this label.

In this example, *student-psk* is the name of the label, and *student* is the user role.

Label Name

student-psk

Label Type

AAA Attribute

This is a User label if used in WxLan

Label Values

User Group

User Group Values ⓘ

student

Note: Requires newer firmware

5. Click **Save** to save the new label.
6. Create a WxLAN Policy that assigns users to a VLAN:
 - a. From the left menu of the Juniper Mist portal, select **Organization > Wireless | WLAN Templates**.
 - b. Click the template that you want to add the policy to.
 - c. In the Policy section, click **Add Rule**.
 - d. In the **User** area, click the plus sign (+), and then enter the label that you created for the user role (for our example, you'd enter *student-psk*).
 - e. In the **Resources** area, click the plus sign (+), and then enter the label that you created for the VLAN (for our example, you'd enter *vlan5*).

As shown below, the policy assigns these users to the specified VLAN.

Policy site Hanover Save Cancel

Site Policies
Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied.

Add Rule Edit Labels

<input type="checkbox"/>	No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)
<input checked="" type="checkbox"/>	1	+ student-park	✓	✓ + vlan5	0 ***
	Last	All Users	✓	All Resources	

- f. Click **Save**.
- g. Click the ellipsis button (...) to enable the new rule.

Integrations

SUMMARY

Use the information in this section to integrate Juniper Mist with third-party products.

IN THIS SECTION

- [Configure Juniper Mist™ as a RADIUS Client in Aruba ClearPass | 291](#)
- [Integrate Juniper Mist™ with Aruba ClearPass Guest for Enhanced Access Control | 293](#)
- [Create a RADIUS Server using JumpCloud™ | 300](#)
- [Integrate Juniper Mist™ with Cisco® ISE for EAP | 303](#)
- [Enable Hotspot 2.0 for Seamless Wi-Fi Experience | 306](#)

What Do You Want to Do?

Table 25: Top Tasks

If you want to...	Use these resources:
Integrate with Aruba ClearPass	<ul style="list-style-type: none">• "Configure Juniper Mist™ as a RADIUS Client in Aruba ClearPass" on page 291• "Integrate Juniper Mist™ with Aruba ClearPass Guest for Enhanced Access Control" on page 293
Integrate with JumpCloud	"Create a RADIUS Server using JumpCloud™" on page 300
Integrate with Cisco ISE	"Integrate Juniper Mist™ with Cisco® ISE for EAP" on page 303
Integrate with Hotspot 2.0	"Enable Hotspot 2.0 for Seamless Wi-Fi Experience" on page 306

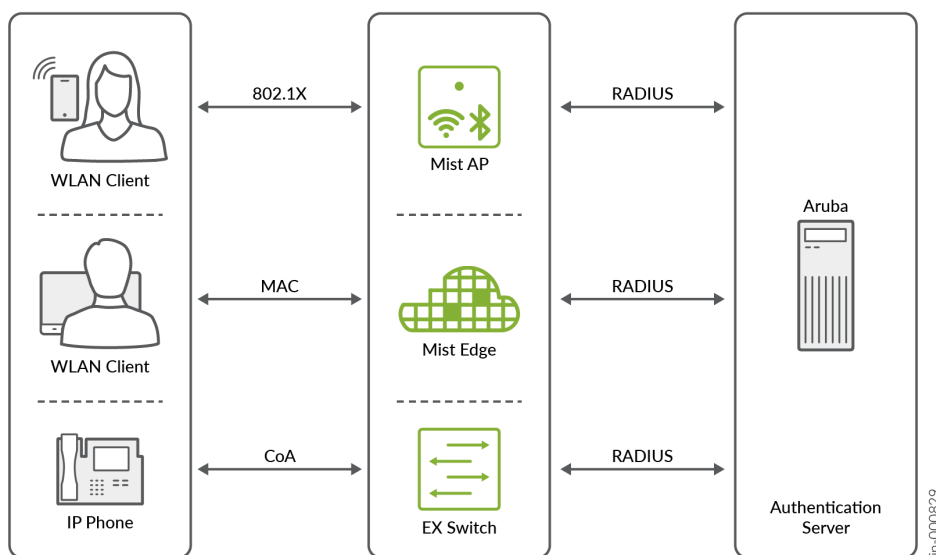
NOTE: For additional information about third-party integrations, see [Juniper Mist Access Assurance Guide](#).

Configure Juniper Mist™ as a RADIUS Client in Aruba ClearPass

SUMMARY

Follow this procedure to integrate Juniper Mist™ with Aruba ClearPass Policy Manager™ for secure user authentication.

You can configure Juniper Mist™ as a Radius Client in the Aruba ClearPass Policy Manager™, a platform from which you can configure and manage your security requirements.



To configure Mist as a RADIUS Client in Aruba ClearPass:

1. Go to the admin console for Aruba ClearPass Policy Manager.
2. Add Mist as a Radius Client.

NOTE: For help, see [Adding a Network Device](#) on the Aruba support site.

3. Create a role.

NOTE:
[Adding and Modifying Roles](#)

4. Add a Role Mapping Policy and associate it with the role that you created.

NOTE: For help, see [Adding and Modifying Role-Mapping Policies](#) on the Aruba support site.

5. Add the relevant attributes to an existing Enforcement Profile or add a new Enforcement Profile.

NOTE: For help, see:

- [Modifying an Existing Enforcement Profile](#)

- [Configuring Enforcement Profiles](#)

6. Finally, configure a Service to reflect the profile and policy you just created.

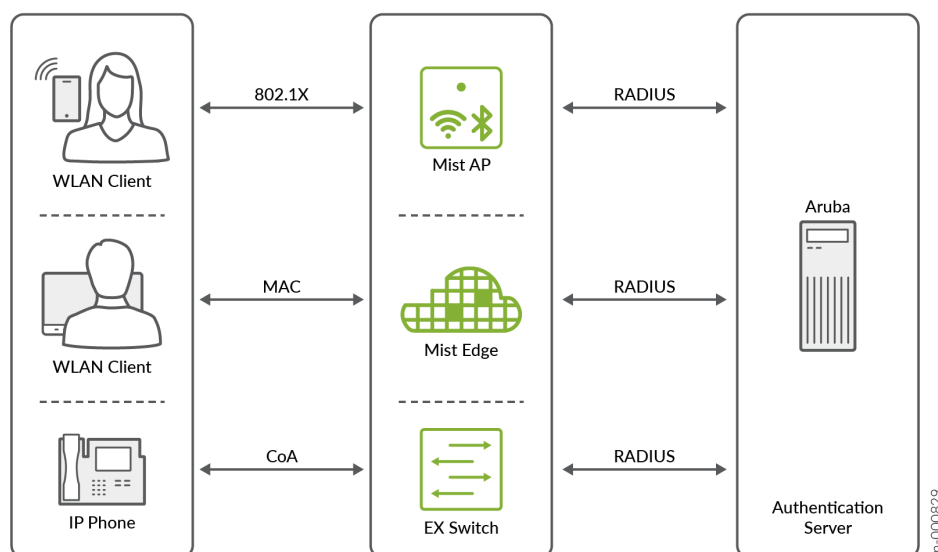
NOTE: For help, see [Adding a New Service](#) on the Aruba support site.

Integrate Juniper Mist™ with Aruba ClearPass Guest for Enhanced Access Control

SUMMARY

Follow this procedure to integrate Juniper Mist™ with Aruba ClearPass Guest™ for secure user authentication.

Juniper Mist™ can seamlessly integrate with network access management platforms, such as Aruba ClearPass Guest, to leverage extensive access control customization options for guest users on the network.



NOTE: For information about Aruba products, go to resources on the Aruba support site, such as [About ClearPass Guest](#).

To integrate Juniper Mist™ with Aruba ClearPass Guest:

1. Go to the admin console for Aruba ClearPass Policy Manager, and create a Change of Authorization (CoA) Profile for the Mist Access Points (APs).

NOTE: For help, see [Configuring Enforcement Profiles](#) on the Aruba support site.

- a. Find the [Cisco – Reauthenticate-Session] profile, select it, and then **Copy** it.
- b. Edit the new copy of that profile. Rename it as [Mist - Reauthenticate-Session].
- c. Configure the following attributes for the Mist CoA profile:

Table 26: Table 1:

Type	Name	Value
Radius:IETF	CallingStation-Id	%{Radius:IETF:Calling-Station:Id}
Radius:Cisco	Cisco-AVPair	subscriber:command=reauthenticate
Radius:IETF	NAS-IPAddress	%{Radius:IETF:NAS-IP-Address}
Radius:IETF	Event-Timestamp	%{Authorization:[Time Source]:Now}

2. Create a Guest Registration page on the ClearPass Guest Manager by duplicating the default self-registration web page template. For help, go to resources on the Aruba support site, such as [Accessing the Self-Registration Customization Forms](#).
 - a. For the self registration instance, select **Enable self-registration**, and then save the changes.
 - b. Enable Sponsor Confirmation since you're enabling a sponsored guest workflow.
 - c. Configure a login delay, which will give ClearPass time to send the CoA back to the Mist AP and reauthorize a newly registered guest client. Set a login delay of 10 seconds (anything lower may

cause inconsistent behavior with ClearPass). Then save the changes. For help, go to resources on the Aruba support site, such as [Editing Self-Registration Pages](#).

d. Configure NAS Vendor Settings as follows:

- **Enabled**—Enable guest login to a Network Access Server
- **Default URL**—Enter <http://www.mist.com>.
- **Override Destination**—Select **Force Default Destination for all clients**.

For help, go to resources on the Aruba support site, such as [Editing and Enabling NAS Login Properties](#).

3. Create Guest Access configuration with MAC Caching and move through the tabs to configure the settings as follows:

- **Name Prefix**—Mist
- **Wireless SSID**—Guest-Access
- **Controller IP Address**—Add the management IP subnet of the Mist APs to allow them to talk to ClearPass through RADIUS.
- Set the default expiration times for each type of guest as required.
- Select Filter ID based enforcement and provide guest role names.

For help, go to resources on the Aruba support site, such as [Guest Authentication with MAC Caching Service Template](#).

4. Select **Add Service**, and then you will see that new services were added.

5. Edit existing Enforcement Profiles and Policies in order to integrate the Mist APs. For help, go to resources on the Aruba support site, such as [Modifying an Existing Enforcement Profile](#).

a. Edit the default mist Captive Portal Profile and from the attributes tab:

- Delete the existing Filter-id attribute.
- Add a new url-redirect attribute to let the AP know where a client needs to be redirected to. Follow this syntax when configuring the value:

```
url-redirect=https:///guest/.php?&mac=%{Connection:Client-Mac-Address-Colon}
```

- Save the changes.

Also, edit Mist Guest Device Profile and remove the last attribute that was pre-created during the wizard:

b. Edit the Mist Guest Device Profile and remove the last attribute that was automatically created.

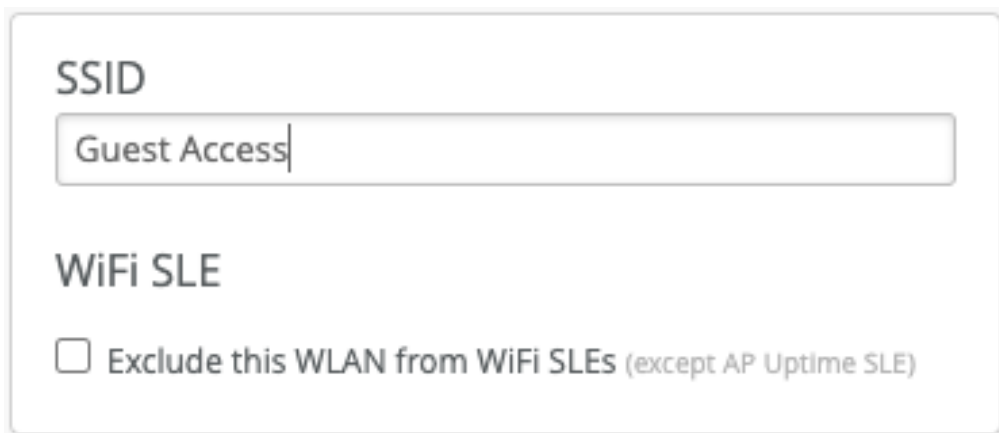
- c. Navigate to Enforcement Policies and Edit the Mist MAC Authentication Enforcement Policy to send a redirect URL for any unknown/unregistered clients:
 - In the Enforcement tab, select Mist Captive Portal Profile as the Default Profile.
 - Save the changes.
6. Create a new Enforcement Policy to handle guest user authentication through the Captive Portal hosted by ClearPass. For help, go to resources on the Aruba support site, such as [Configuring Enforcement Policies](#).
 - a. Set the Enforcement Type as WEBAUTH.
 - b. Set the Default Profile as [RADIUS_CoA] [Mist – Reauthenticate Session].
 - c. Click **Next**, then create a rule to cache a client MAC once a user is authenticated as Guest. Choose the duration specified on the guest manager settings.
 - d. Save the changes.
7. Create a new WebAuth Service. For help, go to resources on the Aruba support site, such as [Adding Services](#).
 - a. In the Service tab, configure the following:
 - **Type**—Select **Web-Authentication**.
 - **More Options**—Select **Authorization**.
 - Add another condition to match on the guest page that contains “Mist” in the name.
 - Click **Next**.
 - b. In the Authentication tab:
 - Select [Guest User Repository] as your authentication source.
 - Click **Next**.
 - c. In the Authorization tab:
 - Add [Endpoints Repository] and [Time Source] as additional authorization sources.
 - Click **Next**.
 - d. In the Roles tab:
 - Select the Role Mapping policy “Mist User Authentication with MAC Caching Role Mapping”.
 - Click **Next**.
 - e. In the Enforcement tab:
 - Select the enforcement policy that you created in the previous step.

- Click **Save**.

8. In the Juniper Mist portal, navigate to the WLAN or create a new one.

NOTE: For help, see ["Configure a WLAN Template" on page 119](#) or ["Add a WLAN to a Site or a WLAN Template" on page 121](#).

9. Enter the same SSID that you configured in ClearPass.



SSID

Guest Access

WiFi SLE

☐ Exclude this WLAN from WiFi SLEs (except AP Uptime SLE)

10. In the Security section:

- • Select **Open Access**.
- Select **MAC address authentication by RADIUS lookup**.
- Select **Guest Access with Mac Authentication Bypass**.
- In the **Allowed Hostnames** field, enter the FQDN of the ClearPass server where a guest user will be redirected to. Also add any additional FQDNs that need to be allowed before the user is authenticated.

Security

Security Type

WPA3	WPA2	Legacy	OWE	Open Access
------	------	--------	-----	-------------

☒ MAC address authentication by RADIUS lookup

☒ Guest Access with Mac Authentication Bypass

Web Auth Allow List

Allowed Subnets

Allowed Hostnames

☐ Prevent banned clients from associating

Edit banned clients in [Network Security Page](#)

11. In the Authentication Servers section, click **Add Server**, enter the IP address, port, and shared secret for the ClearPass server, and then click the checkmark icon to save the changes.
12. In the CoA/DM Server section, select **Enabled**, click **Add Server**, enter the **IP Address**, **Port**, and **Shared Secret** for the ClearPass server, and then click the checkmark to save the changes.

CoA/DM Server

☒ Enabled ☐ Disabled

No CoA/DM servers defined

[Add Server](#)

Event-Timestamp ?

☒ Mandatory ☐ Optional

CoA/DM Server

☒ Enabled ☐ Disabled

New Server



IP Address

192.168.5.75

Port

3799

Shared Secret

.....

[Reveal](#)

Event-Timestamp ?

☒ Mandatory ☐ Optional

13. Save the WLAN settings.

NOTE: If the WLAN is in a WLAN template, ensure that you've applied the template to the desired site(s).

14. Verify that integration was successful by looking at the Access Tracker in the Aruba ClearPass Policy Manager. For help, go to resources on the Aruba support site, such as [Live Monitoring: Access Tracker](#).

Create a RADIUS Server using JumpCloud™

SUMMARY

Follow this procedure to integrate Juniper Mist™ with JumpCloud™ for secure user authentication.

You can use JumpCloud™ to provide a RADIUS server for secure user authentication on your Juniper Mist™ network. See [RADIUS Configuration and Authentication](#).

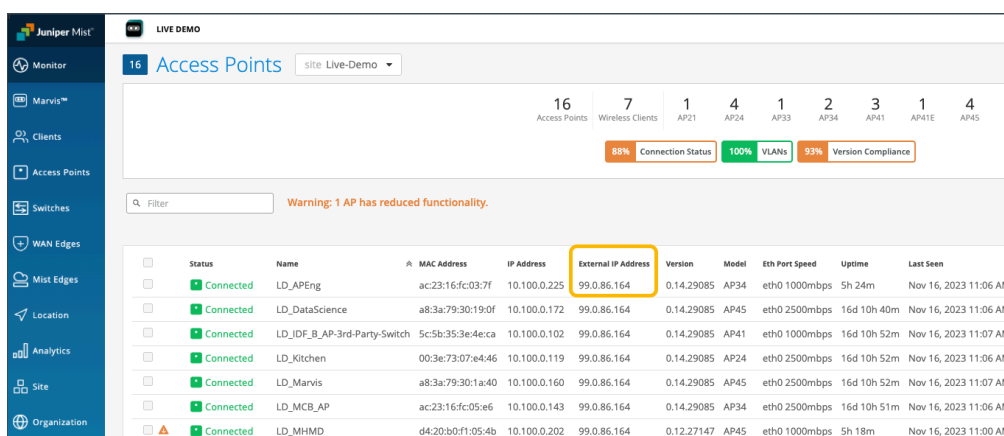
To configure a JumpCloud RADIUS server for Juniper Mist™:

1. From the left menu of the Juniper Mist portal, select **Access Points**.
2. Find the AP in the list, and note its External IP Address, which you'll need to use in the JumpCloud Admin portal.

If you do not see the External IP Address column on the Access Points page, click the Settings button



near the top-right corner of the page and add the column.



Status	Name	MAC Address	IP Address	External IP Address	Version	Model	Eth Port Speed	Uptime	Last Seen
Connected	LD_APENG	ac23:16:fc:03:7f	10.100.0.225	99.0.86.164	0.14.29085	AP34	eth0 1000mbps	5h 24m	Nov 16, 2023 11:06 AM
Connected	LD_DataScience	a8:3a:79:30:19:0f	10.100.0.172	99.0.86.164	0.14.29085	AP45	eth0 2500mbps	16d 10h 40m	Nov 16, 2023 11:06 AM
Connected	LD_IDF_B-AP-3rd-Party-Switch	5c:5b:35:3e:4e:ca	10.100.0.102	99.0.86.164	0.14.29085	AP41	eth0 1000mbps	16d 10h 52m	Nov 16, 2023 11:07 AM
Connected	LD_Kitchen	00:3e:73:07:e4:46	10.100.0.119	99.0.86.164	0.14.29085	AP24	eth0 2500mbps	16d 10h 52m	Nov 16, 2023 11:06 AM
Connected	LD_Marvis	a8:3a:79:30:1a:40	10.100.0.160	99.0.86.164	0.14.29085	AP45	eth0 2500mbps	16d 10h 52m	Nov 16, 2023 11:07 AM
Connected	LD_MCB_AP	ac23:16:fc:05:e6	10.100.0.143	99.0.86.164	0.14.29085	AP34	eth0 2500mbps	16d 10h 51m	Nov 16, 2023 11:06 AM
Connected	LD_MHMD	d4:20:b0:f1:05:4b	10.100.0.202	99.0.86.164	0.12.27147	AP45	eth0 1000mbps	5h 18m	Nov 16, 2023 11:00 AM

3. On the JumpCloud Admin console, add a RADIUS Server.

- Add a RADIUS server. For help, see [Adding a RADIUS Server \(Details Tab\)](#) on the JumpCloud support site.

Enter the appropriate information including the Juniper Mist AP's External IP Address that you obtained in the previous step. Copy and save the Shared Secret to be used in a later step.

- Create a User Group and add your users. For help, see [Creating User Groups](#) and [Adding Users to a Group](#) on the JumpCloud support site.
- On the RADIUS tab of the User Groups configuration, map your AP.
- Configure any additional RADIUS attributes as per your requirements.

4. In the Juniper Mist portal, navigate to the WLAN or create a new one.

NOTE: For help, see ["Configure a WLAN Template"](#) on page 119 or ["Add a WLAN to a Site or a WLAN Template"](#) on page 121.

5. For the **Security Type**, select **WPA2** and **Enterprise (802.1X)**.

6. In the **Authentication Servers** section, click **Add Server**, enter the information for the JumpCloud server, and then click the checkmark in the New Server section to save the server.

Enter the IP address and shared secret for JumpCloud's RADIUS server. Enter 1812 for the port. Select **Enable Key Wrap** if it is applicable to your deployment. This feature enables additional fields for Key Wrap Type such as ASCII and Hexadecimal, and corresponding Key value fields.

Authentication Servers

RADIUS

RADIUS Authentication Servers

New Server ✓ ✕

Hostname

54.203.27.225

Port

1812

Shared Secret

.....

[Reveal](#)

☐ Enable Key Wrap

7. Save the WLAN settings.

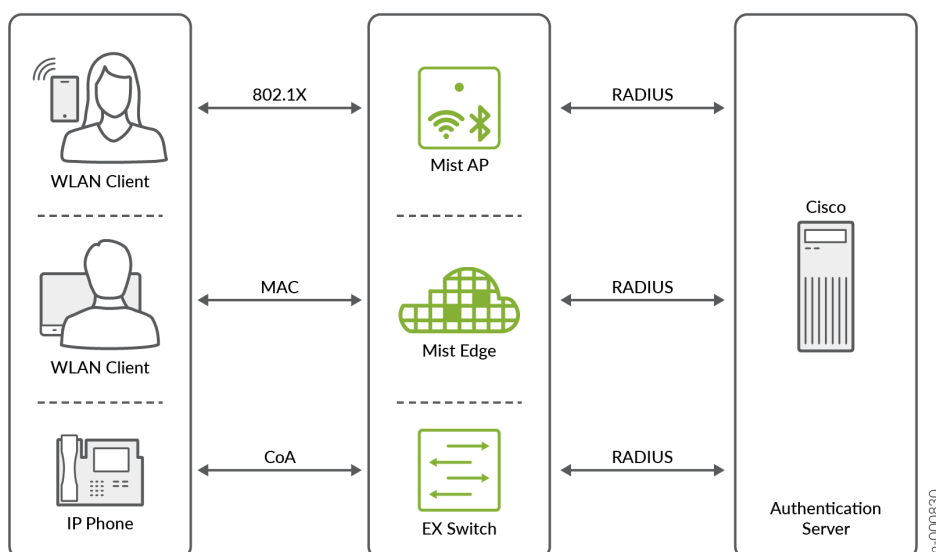
NOTE: If the WLAN is in a WLAN template, ensure that you've applied the template to the desired site(s).

Integrate Juniper Mist™ with Cisco® ISE for EAP

SUMMARY

Follow this procedure to integrate Juniper Mist™ with Cisco® ISE for EAP for secure user authentication.

Juniper Mist™ can seamlessly integrate with Cisco® Identity Services Engine (ISE) to leverage Extensible Authentication Protocol (EAP), which provides a secure way for wireless networks to send identification information for network authentication purposes.



To integrate Juniper Mist with Cisco ISE:

1. In the Juniper Mist portal, navigate to the WLAN or create a new one.

NOTE: For help, see ["Configure a WLAN Template" on page 119](#) or ["Add a WLAN to a Site or a WLAN Template" on page 121](#).

2. For Security Type, select **WPA2** and **Enterprise (802.1X)**.

< WLANs : **New WLAN**

At least one RADIUS authentication server must be added

SSID

Labels

+

WiFi SLE

☐ Exclude this WLAN from WiFi SLEs (except AP Uptime SLE)

WLAN Status

☒ Enabled ☐ Disabled

☐ Hide SSID

☐ Broadcast AP name

Radio Band

Security

Security Type

WPA3

WPA2

Legacy

OWE

Open Access

Enterprise (802.1X)

Personal (PSK)

☐ MAC address authentication by RADIUS lookup

☐ Use EAPOL v1 (for legacy clients)

☐ Enable EAP-Reauth

☐ Prevent banned clients from associating

Edit banned clients in [Network Security Page](#)

Fast Roaming

☒ Default

☐ Opportunistic Key Caching (OKC)

☐ .11r

3. In the Authentication Servers section, click **Add the RADIUS Server**, and then enter in the IP Address (Hostname), Port, and Shared Secret of the ISE server. Click the checkmark near the top right corner of the section to save the changes.

Authentication Servers

RADIUS

RADIUS Authentication Servers

New Server ✓ ✕

Hostname
10.2.2.30

Port
1812

Shared Secret
..... [Reveal](#)

☐ Enable Key Wrap

4. Save the WLAN settings.

NOTE: If the WLAN is in a WLAN template, ensure that you've applied the template to the desired site(s).

5. On the left menu of the Juniper Mist™ portal, select **Access Points (APs)**.
6. Select the AP, then scroll down to the Status section to obtain the AP's IP Address to be used in the Identity Services Engine (ISE).
7. From the Identity Services Engine (ISE), click **Add a Network Device** and enter in the following information:
 - **Name**—Enter the name of the Mist AP.
 - **IP Address**—Enter the AP's IP Address that you obtained in step 9.

- **Shared Secret**—Enter the RADIUS Shared Secret.

NOTE: For help, see [Adding and Editing Devices](#) on the Cisco support site.

Enable Hotspot 2.0 for Seamless Wi-Fi Experience

SUMMARY

Follow this procedure to integrate Juniper Mist™ with Hotspot 2.0 for secure user authentication.

IN THIS SECTION

- [Enable Hotspot 2.0 | 306](#)

Hotspot 2.0 (also known as Passpoint) enables seamless and secure connection between public Wi-Fi and cellular networks by requiring WPA2 enterprise encryption. Juniper Mist™ allows you to easily deploy Hotspot 2.0 networks by providing pre-canned templates for each operator and service provider. To enable Hotspot 2.0, you must enable Hotspot 2.0 support on the wireless LAN (WLAN), then configure the authentication server toward your operator or service provider.

Enable Hotspot 2.0

1. In the Juniper Mist portal, navigate to the WLAN or create a new one.

NOTE: For help, see ["Configure a WLAN Template" on page 119](#) or ["Add a WLAN to a Site or a WLAN Template" on page 121](#).

2. In the Security section, select **WPA2** and **Enterprise (802.1X)**.

Edit WLAN ✕

At least one RADIUS authentication server must be added

SSID

WLAN ID

WiFi SLE

☐ Exclude this WLAN from WiFi SLEs (except AP Uptime SLE)

Security

Security Type

WPA3 WPA2 Legacy OWE Open Access

Enterprise (802.1X) Personal (PSK)

☐ MAC address authentication by RADIUS lookup

☐ Use EAPOL v1 (for legacy clients)

☐ Enable EAP-Reauth

Delete Save Cancel

3. In the Hotspot 2.0 section, select **Enabled**, then select your **Operators** (service providers).

Edit WLAN ✕

At least one RADIUS authentication server must be added

Band Steering

☐ Enable

Client Inactivity

Drop inactive clients after seconds:

Geofence

☐ Minimum client RSSI (2.4G)

☐ Minimum client RSSI (5G)

☐ Minimum client RSSI (6G)

Block clients having RSSI below the minimum

802.1X Web Redirect

Allow 802.1X Web Redirect for quarantine or posture assessment based on RADIUS server response containing url-redirect AVP

☐ Enabled ☒ Disabled

Hotspot 2.0 ! Hotspot 2.0 requires firmware v0.8.x or higher

☒ Enabled ☐ Disabled

Operators

+

Venue Name

➤ Advanced Settings

Data Rates

Delete Save Cancel

NOTE: If multiple operators are selected, an authentication broker is required to proxy different operator realms to the correct destination. Boingo is one authentication broker, for example, who can proxy authentication traffic for each mobile carrier (T-Mobile, AT&T, Sprint etc) to the correct destination.

4. (Optional) Enter the venue name in the Venue Name field. The contents of this field will be advertised by the Mist Access Point. If this field is not configured, the Mist Access Point will automatically advertise the Site Name as the Venue Name.
5. (Optional) Click **Advanced Settings** and configure additional settings.

Edit WLAN

At least one RADIUS authentication server must be added

Band Steering

☐ Enable

Client Inactivity

Drop inactive clients after seconds:

802.1X Web Redirect

Allow 802.1X Web Redirect for quarantine or posture assessment based on RADIUS server response containing url-redirect AVP

☐ Enabled ☒ Disabled

Geofence

☐ Minimum client RSSI (2.4G)

☐ Minimum client RSSI (5G)

☐ Minimum client RSSI (6G)

Block clients having RSSI below the minimum

Hotspot 2.0 Hotspot 2.0 requires firmware v0.8.x or higher

☒ Enabled ☐ Disabled

Operators

Venue Name

Data Rates

☒ Compatible (allow all connections)

☐ No Legacy (2.4G, no 11b)

☐ High Density (disable all lower rates)

☐ Custom Rates

WiFi Protocols

WiFi-6 ☒ Enabled ☐ Disabled

WLAN Rate Limit

☐ Limit uplink to Mbps

Advanced Settings

Advanced settings will override parameters inherited from the high level operator template

Domain Name

(Comma-separated domains)

Roaming Consortium ID

(Comma-separated IDs, 6 or 10 hex characters)

NAI Realm

Name **EAP Type**

- Domain Name—Identifies the realm of administrative authority
- Roaming Consortium ID—Used for Wi-Fi Hotspot 2.0 negotiation
- NAI Realm (Network Access Identifier)—Used for Wi-Fi Hotspot 2.0 negotiation.

NOTE: Configuring the Advanced Settings will override parameters inherited from the high-level operator template.

6. In Authentication Servers section, click **Add Server**, select the server type (RADIUS or RadSec), and then enter the information, and click the checkmark to save the settings.

Consult with your Hotspot 2.0/Passpoint service provider to ensure that you configure the correct RADIUS or RadSec settings.

Edit WLAN

At least one RADIUS authentication server must be added

☐ Limit downlink to Mbps

Per-Client Rate Limit
☐ Limit uplink to Kbps

☐ Limit downlink to Mbps

Application Rate Limit
☐ Enabled ☒ Disabled

Authentication Servers

RADIUS

RADIUS Authentication Servers

No authentication servers defined

Add Server

RADIUS Accounting Servers
☐ Enable Interim Accounting

No accounting servers defined

Add Server

☐ Randomize authentication and accounting server per AP

NAS Identifier

NAS IP Address

CoA/DM Server
☐ Enabled ☒ Disabled

VLAN

7. Save the WLAN settings.

NOTE: If the WLAN is in a WLAN template, ensure that you've applied the template to the desired site(s).

8. If you configured a RadSec authentication server, copy the Juniper Mist™ certificate to your RadSec servers, and add the RadSec certificates to your Juniper Mist organization.

NOTE: For help, see [Manage Certificates](#) in the Juniper Mist Management Guide.

Rogues, Honeypots, and Neighbor APs

SUMMARY

Get familiar with essential terms: rogue, neighbor, and honeypot so that you can manage them appropriately when they're detected by Juniper Mist™.

IN THIS SECTION

- [Find and Remove Rogues | 312](#)
- [Configure AP Threat Protection | 314](#)
- [Classify and Ban Designated Wireless Clients | 317](#)
- [Find Wireless Client MAC Addresses | 321](#)

Rogue, neighbor, and honeypot APs are unauthorized devices operating on or near your network, often with the goal of fooling users into connecting to the "false" access point in order to steal data or monitor communications. These kinds of anomalous devices can be hard to detect, and they can pose a significant security threat to both the unwitting user, and the organization whose network is being compromised.

To protect against this kind of threat, Juniper APs include a dedicated scanning radio to detect and remove risky APs and their clients from your network and your facilities. The dedicated scanning radios operate on both the 2.4-GHz and 5-GHz bands. They provide data for real-time performance adjustments on the AP, as well as streaming telemetry to the Mist portal, for site-wide optimizations on the basis of artificial intelligence and machine learning.

To see any threats, select **Site > Wireless | Security** in the Mist portal to open the Security page. A list of all the anomalous APs detected appears. You can drill down on any item to find the physical location, Ethernet connection, and even rogue clients connected to the AP. You can also terminate rogue AP and prevent unwanted clients from rejoining the network. See "[Classify and Ban Designated Wireless Clients](#)" on page 317.

Figure 24: AP Threat Detection and Classification

SSID	Type	No. of Clients	BSSID	Band	Channel	Avg. RSSI	Seen By	Nearest AP	Location	Action
Guest Wi-Fi	Honey pot	5	5c:5b:35:54:6f:64	5GHz	153	-49.4 dBm	6 APs	LD_NewBobFriday	01 - Office	
Guest Wi-Fi	Honey pot	6	5c:5b:35:54:6f:44	5GHz	64	-55.6 dBm	3 APs	LD_NewBobFriday	01 - Office	
Guest Wi-Fi	Rogue	6	d4:20:b0:f1:56:a5	5GHz	48	-59.3 dBm	1 APs	LD_MHMD	01 - Office	
Live-Demo-NAC	Honey pot	15	5c:5b:35:54:6f:65	5GHz	153	-49.3 dBm	5 APs	LD_NewBobFriday	01 - Office	
Live-Demo-NAC	Honey pot	3	5c:5b:35:54:6f:45	5GHz	64	-55.7 dBm	3 APs	LD_NewBobFriday	01 - Office	
Live-Demo-NAC	Rogue	--	00:3e:73:63:d1:48	6GHz	5	-42.5 dBm	1 APs	LD_24_JSW	01 - Office	
Live-Demo-NAC	Rogue	5	a8:3a:79:34:ba:65	5GHz	60	-60.0 dBm	1 APs	LD_RS_Support	01 - Office	
Live_demo_6G	Rogue	--	00:3e:73:63:d1:47	6GHz	5	-44.3 dBm	1 APs	LD_24_JSW	01 - Office	
Live_demo_do_not_remove	Honey pot	3	5c:5b:35:54:6f:61	5GHz	153	-49.0 dBm	5 APs	LD_NewBobFriday	01 - Office	
Live_demo_do_not_remove	Honey pot	6	5c:5b:35:54:6f:41	5GHz	64	-55.0 dBm	3 APs	LD_NewBobFriday	01 - Office	
Live_demo_only	Honey pot	--	5c:5b:35:54:6f:62	5GHz	153	-49.7 dBm	5 APs	LD_NewBobFriday	01 - Office	
Live_demo_only	Honey pot	--	5c:5b:35:54:6f:42	5GHz	64	-55.4 dBm	3 APs	LD_NewBobFriday	01 - Office	
Live_demo_only	Rogue	15	00:3e:73:63:d1:46	6GHz	5	-43.0 dBm	1 APs	LD_24_JSW	01 - Office	
Live_demo_only	Rogue	6	a8:3a:79:34:ba:62	5GHz	60	-35.0 dBm	1 APs	LD_RS_Support	01 - Office	

Unique security threats arise in the wireless environment:

- *Rogue APs* are any wireless APs installed on your wired network without authorization. Typically, this AP is connected to the LAN through an Ethernet cable. The intent of rogues can be malicious, such as to gain illicit access to the network, or benign, such as an employee setting up their own Wi-Fi hotspot to cover a perceived deadspot. *Rogue clients* are users who've connected to the rogue AP.
- Malicious *Neighbor APs* are not connected to your network, but they lurk in the vicinity and may have both the strongest signal and no authorization requirements. As a result, clients may connect to the neighbor AP, assuming it's yours and thus that it's secure. Neighbor APs can also be a way for users in your facility to get around security restrictions on your network, such as streaming music or accessing blocked sites, or to avoid paying for services. *Nonmalicious neighbor APs* are SSIDs from another organization. In other words, legitimate SSIDs belonging to one organization will also be listed as neighbors for another organization.
- *Honeypots*, also known as *Evil Twins*, are unauthorized APs that advertise your SSID, typically with the goal of capturing client login credentials. Here, a bad actor may copy or approximate your Wi-Fi hotspot, spoof your organization's login screen, and then collect the username and password of unsuspecting users as they try to login to "your" network. The bad actor can then use the credentials to log in to your actual network and wreak whatever havoc they have in mind. *Non-malicious Honeypots* are SSIDs from another organization that are broadcasting the same WLAN.

NOTE: You can exempt "friendly" SSIDs and BSSIDs from repeated misclassification. Do so in the Mist portal by adding the MAC address of the AP in the **Approved SSIDs** field on the

Organization > Admin | Site Configuration page (under **Security Configuration**). Be sure to delimit multiple MACs with a comma, no space.

Find and Remove Rogues

SUMMARY

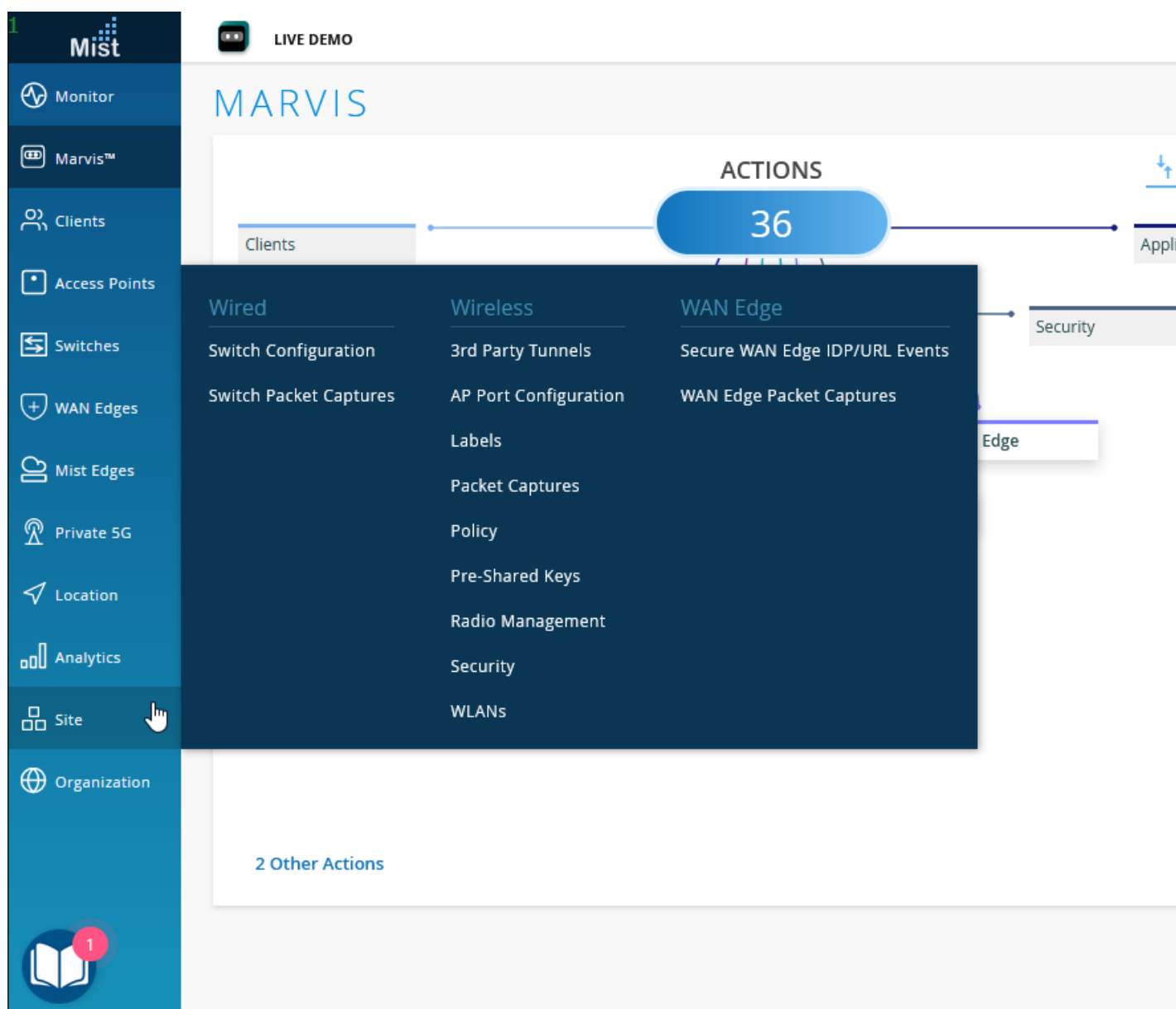
To protect your network, use the Security page to find and remove access points that have been installed on your network without authorization.

You can discover and remove rogue clients from your network on the **Site > Wireless | Security** page of the Juniper Mist™ portal.

NOTE: What is a rogue client? See "[Rogues, Honeypots, and Neighbor APs](#)" on page 310.

The following animation shows how to find rogue APs and remove them. Basically, when you click the **Terminate** button, nearby Juniper APs will send deauthentication frames to the rogue clients, which are identified by their MAC addresses through their association with the rogue AP. The deauthentication frame is a notification, not a request, and the rogue client will be dropped.

Figure 25: Discover and Remove Rogue APs



NOTE: If you want to prevent these rogue clients from rejoining the network, you can classify them as banned, and they will not be re-authenticated by any AP in the site. See "[Classify and Ban Designated Wireless Clients](#)" on page 317. Conversely, to allow certain terminated clients back on the network, you can classify them as *approved*, and the APs will not reject the authentication attempt.

To find and remove rogue APs:

1. From the left menu of the Juniper Mist portal, select **Site > Wireless | Security**.
2. At the top of the page, use the drop-down list to select a **Site**.

NOTE: You also can adjust the time period (the past hour or the past 24 hours).

3. Keep the default options to show Threats and List view.
4. In the Threats table, find the rogue AP that you want to remove from the network.
5. In the **Action** column, click the action button, and then click **Terminate Rogue**.

SSID	Type	No. of Clients	BSSID	Band	Channel	Avg. RSSI	Seen By	Nearest AP	Location	Action
**KF-Open-1	Rogue	0	00:0C:4C:00:00:00	5GHz	100	-50.0 dBm	1 AP	MC_AF24_RLB1	Unknown	⋮ Terminate Rogue
**KF-OPEN-ISE	Rogue	0	00:0C:4C:00:00:00	5GHz	157	-79.0 dBm	1 AP	LD_Testbed_MD	01 - Office	⋮
**KF-OPEN-ISE	Rogue	0	00:0C:4C:00:00:00	5GHz	36	-62.0 dBm	1 AP	LD_APEng	01 - Office	⋮
**KF-OPEN-ISE	Rogue	0	00:0C:4C:00:00:00	5GHz	140	-54.0 dBm	1 AP	LD_MHMD	01 - Office	⋮
#santosh-owe-mab-coa	Rogue	0	00:0C:4C:00:00:00	5GHz	52	-60.0 dBm	1 AP	LD_APEng	01 - Office	⋮
BBCave	Rogue	4	00:0C:4C:00:00:00	5GHz	153	-55.0 dBm	1 AP	MC_DavidL AP	Unknown	⋮

Configure AP Threat Protection

SUMMARY

To protect your network, enable Juniper Mist™ to detect unauthorized access points (APs) across your site.

Juniper APs include a dedicated scanning radio that can detect errant APs. Honeypot and neighbor detection are enabled by default, and you can also enable rogue detection. This is a site-wide feature that enables detection by all Juniper APs in the site.

NOTE: What are rogues, honeypots, and neighbor APs? See ["Rogues, Honeypots, and Neighbor APs" on page 310](#).

When threat protection is enabled, you'll see the detected APs on the Monitor > Alerts page, as shown below.

Figure 26: Viewing Alerts for Rogues, Honeypots, and Neighbor APs

The screenshot shows the Juniper Mist portal interface. The left sidebar contains navigation options: Monitor, Marvis™, Clients, Access Points, Switches, WAN Edges, Mist Edges, Private 5G, Location, Analytics, Site, and Organization. The main content area displays a summary of alerts: 107 Total, 19 Infrastructure, 0 Marvis, and 88 Security. Below this, a table lists individual alerts with columns for Alert, Site, Recurrence, First Seen, Last Seen, and Details. The alerts include 'Honeypot SSID detected' and 'Client Connection to rogue AP detected'.

Alert	Site	Recurrence	First Seen	Last Seen	Details
Honeypot SSID detected	Live-Demo	3	Aug 25, 2023 11:54 AM	Aug 25, 2023 11:54 AM	Network Security
Client Connection to rogue AP detected	Live-Demo	2	Aug 25, 2023 11:53 AM	Aug 25, 2023 11:59 AM	Network Security
Client Connection to rogue AP detected	Live-Demo	6	Aug 25, 2023 11:37 AM	Aug 25, 2023 11:47 AM	Network Security
Honeypot SSID detected	Live-Demo	2	Aug 25, 2023 11:32 AM	Aug 25, 2023 11:41 AM	Network Security
Client Connection to rogue AP detected	Live-Demo	4	Aug 25, 2023 11:20 AM	Aug 25, 2023 11:26 AM	Network Security
Honeypot SSID detected	Live-Demo	1	Aug 25, 2023 11:08 AM	Aug 25, 2023 11:08 AM	Network Security
Client Connection to rogue AP detected	Live-Demo	3	Aug 25, 2023 11:03 AM	Aug 25, 2023 11:04 AM	Network Security
Honeypot SSID detected	Live-Demo	4	Aug 25, 2023 10:41 AM	Aug 25, 2023 10:44 AM	Network Security

As you view these alerts, you might need to adjust certain settings to meet your business needs. For example, you can exempt known SSIDs and BSSIDs so that they won't be classified as threats. You can adjust the detection thresholds for neighbor APs based on signal strength and duration.

To configure AP threat protection:

1. From the left menu of the Juniper Mist portal, select **Organization > Admin | Site Configuration**.
2. Click the site that you want to configure.
3. In the **Security Configuration** group, select the options that you want to enable.

Security Configuration

☒ Detect Rogue and Neighbor APs

Neighbor RSSI Threshold

Neighbor Time Threshold mins

☒ Detect Honeypot APs

Approved SSIDs

Approved BSSIDs

☒ Auto-Prevent Clients

Prevent client from associating for seconds when having at least auth failures within seconds

- **Detect Rogue and Neighbor APs**—If you enable this option, the Alerts page will include alerts such as *Rogue AP detected* and *Client Connection to rogue AP detected*.

You can adjust the detection thresholds:

- **Neighbor RSSI Threshold**—This threshold is based on the strength of the AP signal. For example, with the default threshold of -80 dBm, Juniper Mist ignores APs with RSSI of -80 or above. The supported range is -40 dBm to -100 dBm.
- **Neighbor Time Threshold**—This threshold is based on the duration of the AP signal. For example, if you notice neighbor APs constantly appearing and disappearing from the Monitor > Alerts page as the signal waxes and wanes, you can set a longer time threshold. Then only APs with enduring signals are detected as potential threats.
- **Detect Honeypot APs**—When you select this option, the Alerts page will include alerts such as *Honeypot SSID detected*.
- **Approved SSIDs and Approved BSSIDs**—Use these fields to identify any known SSIDs or BSSIDs that you want to ignore. Enter their MAC addresses, separated with a comma (no space).

You can use wildcards in these fields. This feature is useful if you want to allow multiple SSIDs that have similar names, as you might see when your users connect through Wi-Fi Direct to printers or TVs. For example, if you enter *direct** in the Approved SSIDs list, Juniper Mist ignores SSIDs such as *DIRECT-roku-123-44AABB* and *DIRECT-printer9999*. Likewise, the Approved BSSIDs field supports partial matching, for example *"cc-73-*"*.

- **Auto-Prevent Clients**—Select this option to prevent connections from clients with multiple authorization failures. The Alerts page will include alerts such as *802.11 Auth Denied* and as *Blocked: Repeated Authorization Failure*.

Adjust the settings as needed:

- Set the number of **seconds** that the client is prevented from associating with the WLAN. For example, with the default setting of 60 seconds, a client is banned for 60 seconds.
- Set the number of **auth failures** that trigger the auto-prevent action. For example, with the default setting of 4, a client is banned after failing four times.

4. Click **Save** at the top-right corner of the Site Configuration page.

Classify and Ban Designated Wireless Clients

SUMMARY

To protect your network, use this feature to allow or ban access points based on their MAC addresses.

IN THIS SECTION

- [Classify Clients | 317](#)
- [Block Banned Clients | 320](#)

To simplify wireless security and control, you can identify wireless clients that you want to ban or approve. Then in your WLAN security settings, enable the option to prevent banned clients from associating.

- **Banned clients**—Rogue clients are banned as a result of connecting to the rogue AP, after which they are prevented from rejoining the network, even if they try through a valid AP.

Approved clients—The approved clients classification is a special category for clients that were previously connected to the network through a rogue AP, but then were terminated to shut down the rogue. When you *approve* a legitimate client, they can rejoin the network by reconnecting through a valid AP. Unclassified clients are considered neutral.

Depending on the AP firmware, clients can be banned or approved from a specific site or from the entire organization. Up to 512 client classifications for a given SSID can be stored locally, on the relevant APs, for APs running firmware version 0.14.x and later (any more than 512 are stored only on the cloud).

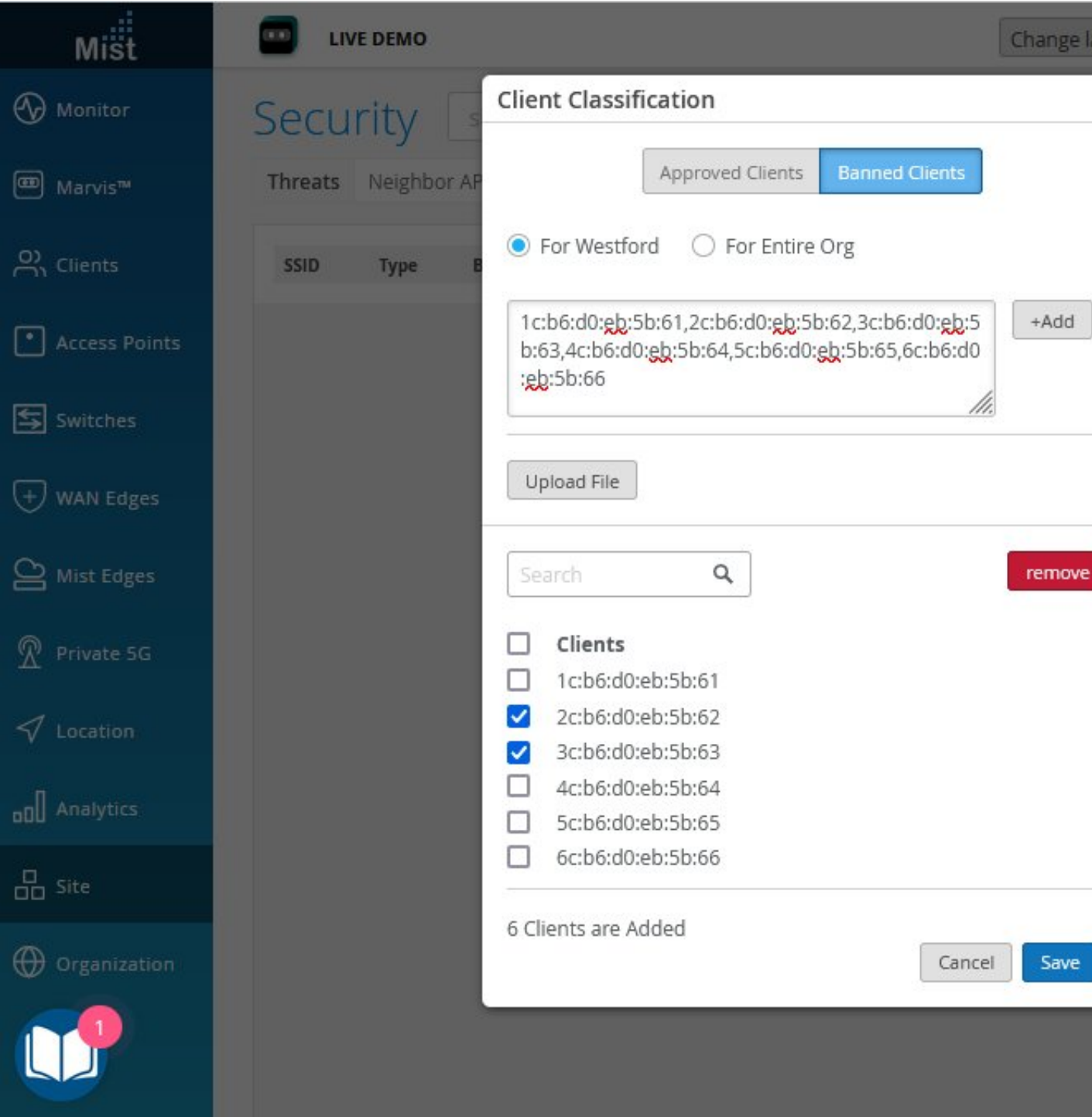
For firmware before version 0.14.x, client classifications are stored on the Mist cloud, which obviously means the AP must be connected to the cloud to reference and enforce the classification. The minimum AP firmware required for site-level classification, or for organization-wide classification (which includes site-level), is version 0.9.x or later.

Classification uses the client's MAC addresses for identification. You can find the MAC addresses of rogue clients by mousing over the *client count* in the Security page (see ["Find Wireless Client MAC Addresses" on page 321](#)), or by looking them up in the WiFi Clients page.

Classify Clients

Typing MAC addresses is tedious, so the best way to use the classification app is to copy and paste from a list or to upload a .csv file, one for approved clients and the other for banned clients. Separate MAC addresses on a single line with a comma (no space).

Figure 27: Classify Clients



For .csv files, you can also use a line break such as you would get from copying a column of data from a spreadsheet. Mist supports the following MAC address formats:

To classify wireless clients:

1. From the Mist portal, select **Site > Wireless | Security**.
2. Click the **View Client Classification** button in the upper right corner of the page that appears.
 - For both the Approved tab and Banned tab, paste your MAC addresses in the field and click the **+Add** button.
 - Alternatively, click the **Upload File** button to load a **.csv** file with the MAC addresses.
3. Click **Save** to incorporate the list and close the page.

Block Banned Clients

Figure 28: Prevent Banned Clients from Associating with the SSID

The screenshot displays the Mist management console interface for configuring a WLAN. The left sidebar contains navigation links: Monitor, Marvis™, Clients, Access Points, Switches, WAN Edges, Mist Edges, Private 5G, Location, Analytics, Site, and Organization. The main content area is titled 'WLANs : SaltLakeNet'. The configuration fields include:

- SSID:** SaltLakeNet
- WLAN ID:** d79e641d-6bd2-109bc004cb8-82ae-898ce
- Labels:** A redacted label is shown.
- WiFi SLE:** ☐ Exclude this WLAN from WiFi SLEs (except AP Health SLE)
- WLAN Status:** ☒ Enabled, ☐ Disabled; ☐ Hide SSID; ☒ Broadcast AP name
- Radio Band:** (Field is empty)
- Security:** Security Type is set to WPA3. The 'Enterprise (802.1X)' option is also visible. The 'Prevent banned clients' checkbox is checked and highlighted with a red box. Below it, a warning icon and the text 'Banned clients' are visible, along with a link to 'Edit banned clients'.
- Fast Roaming:** ☒ .11r, ☐ Default, ☐ Opportunistic K, ☐ Zebra Comp

Note that banning rogue clients from an SSID should be considered in the larger context of *client blocking*, which has, in at least one case, led to [FCC actions against the blocker](#). Banned clients will not be able to connect to the Juniper AP, nor will they see a message or notification explaining the cause.

To prevent banned clients from associating with an SSID:

1. From the Mist portal, select **Site > Wireless | WLANs**.
2. Click the **Add WLAN** button in the upper right corner of the page or choose an existing SSID from the list that appears.
3. In the Security section, select **Prevent banned clients from associating**.
4. Click **Save**.

Find Wireless Client MAC Addresses

SUMMARY

When investigating and managing security issues, use this procedure to look up a client's MAC address.

You can use MAC addresses to classify clients and deny wireless access, as well as to pull up client insights with the Marvis chatbot. Two methods are presented below, the only difference being which entry point you prefer to use.

Figure 29: Find the MAC Address for a Wireless Client



Method 1: To find client MAC addresses:

1. From the Mist portal, select **Clients > WiFi Clients**
2. Scroll down the list that appears, and, for any given user, click the MAC address. A client-details page appears.
3. Copy the client's MAC address and then click **Cancel** to close the page.

Method 2: To find client MAC addresses:

1. From the Mist portal, select **Site > Wireless | Security**
2. Scroll down the list that appears, and for any given rogue client, click the client count number. The Rogue Clients List page appears with the MAC address of each detected rogue.
3. Copy the client's MAC address and then click **X** to close the page.

PCI DSS Compliance

SUMMARY

If your organization is subject to Payment Card Industry Data Security Standard (PCI DSS) requirements, use this information to understand how the Juniper Mist™ cloud supports PCI DSS across the wired, wireless, and SD-WAN domains.

Introduction

PCI DSS was created as a common standard to protect against credit card and payment data fraud in the retail space (and other industries, like banking, where online payments are made). By providing consistent and holistic security policies and best practices, PCI DSS enables security personnel and network administrators to effectively thwart various threats to payment data. PCI DSS 3.2.1 went into effect for assessments in May 2018.

The network is a critical cornerstone of PCI DSS compliance as it is the primary channel for transmitting payment data. PCI DSS requirements are designed to ensure that network security operations and practices eliminate or minimize known risks. Plus, they ensure that the organization defines traceable well-structured policies, procedures, and practices that can be audited.

The wireless network in particular is especially important to retail environments as business operations and digital engagement technologies rely upon mobile connectivity. Point of Sale devices, scanners, barcode readers, printers, and mobile computers, for example, all operate on Wireless LANs (WLAN) that serve as the lifeblood of retail operations. Given the importance of WLANs, there are two types of requirements specifically outlined for the PCI DSS compliance of wireless networks. These include:

- **Generally applicable wireless** These are requirements that apply even when the wireless network is not in scope of the Cardholder Data Environment (CDE). They include strong network segmentation to protect the CDE network and security against attacks from rogue or unknown wireless Access Points (APs) and clients.

- **Securing wireless in a CDE** These are requirements mandated for systems that transmit payment card information over wireless and wired technology. In addition to generally applicable wireless requirements, they impose additional security requirements for changing default passwords and configurations, using strong encryption and authentication, regular updating of the system with compliant software, and monitoring access.

PCI DSS 3.2.1 Attestation of Compliance (AOC)

Juniper Mist solution has been assessed by an independent PCI DSS security assessor to meet PCI DSS 3.2.1 Attestation of Compliance (AOC).

Cloud Security

The Mist cloud is outside the CDE environment as it does not carry any wireless packet data. Regardless, Mist takes additional measures to ensure the highest level of security in the Mist cloud to ensure confidentiality, processing integrity, and availability. For example:

- Mist uses a SOC2 Type 2 / ISO 27001 / PCI cloud data
- Maintains an information security policy.
- User access is highly
- Use of network application firewalls / access control lists.
- Use of Intrusion Detection System (IDS) / Intrusion Protection System (IPS).
- Industry standard encryption is utilized at various levels.
- Any information stored in the cloud is obfuscated with an organization-specific
- Security is integrated with development cycles, and pen tests are performed to detect vulnerabilities at the network and application
- Perform regularly scheduled internal and external vulnerability scans.
- Implement annual security awareness training for all in-scope employees.
- Perform an annual risk assessment of the in-scope business environment.
- Have in place incident response plan.
- Annual PCI DSS Attestation of Compliance (AOC) by independent PCI DSS security assessor

Network Segmentation The following schemas can be implemented in a Mist environment to ensure network segmentation:

Physical Segmentation: One way to achieve network segmentation is to connect the wireless APs on a wired network that is physically separate from the CDE network. This would imply having an overlay

wired and wireless infrastructure that does not have any intersection with the wired network for the CDE environment. In this scheme, there is no firewall or internet connection that is shared between the CDE and non-CDE networks.

VLAN based logical segmentation: It is common to use Virtual LANs (VLANs) to segment the networks into logical subnets. While it is possible to achieve logical segmentation by having the wireless network and the CDE in different VLANs, this methodology is not considered a safe and secure way to protect the network, without adequate access control policies between VLANs.

Firewall separation: If the wireless LAN is connected to the CDE, instituting a Firewall between the Wireless network and the CDE network is an acceptable form of segmentation that conforms to PCI DSS 3.2.1 requirements.

Software defined policy engine. Mist's integrated WxLAN policy engine can be used to isolate any wireless traffic into the CDE environment. Mist delivers a powerful platform when it comes to creating policies for role, user, application, and resource-based access on the network via its inline policy engine – WxLAN. The Mist wireless infrastructure allows policies to be enforced on any wired network with access to the LAN blocked for all WLANs configured in the system.

Protect Network from External Attacks

To ensure the wireless network is compliant with the generally applicable requirements for PCI DSS, retailers need to pay special attention to the following:

- **Rogue Devices:** These are accidental or malicious AP on the wired network that can be used to violate internal networks with access to all network resources.
- **Honeypot devices:** these are accidental or malicious AP that masquerade as sanctioned AP sending the retailer's AP beacon.
- **Non-compliant and unsanctioned APs:** These range for APs that may be sanctioned APs but out of compliance running old firmware without critical security. Similarly, these may also include APs that are neighbors as well as those causing inadvertent interference to the wireless operations inside the four walls of a retail store or warehouse.

Two activities are required for handling these external devices, often referred to as Wireless Intrusion Detection and Prevention (WIDS/ WIPS):

- Monitor the RF environment to find and analyze the existence of
- Isolate any Wi-Fi APs not used to transmit or receive cardholder

Traditionally there have been several ways in which WLAN vendors have addressed the above requirements for WIDS/WIPS compliance:

- **Part-time** In this mode, APs when not serving clients scan the spectrum for rogue devices. This is almost akin to having a security solution that only works some of the time – not 24×7.

- **Dedicated APs** provide 24×7 security monitoring of the wireless. While this does protect the network all the time, it explodes the deployment cost for additional APs with associated installation cost of PoE cable runs to the IDF/MDF to power up the sensors.
- Some vendors use dual-banded radios in APs and steal a radio within an AP for sensor implementation leading to nightmares in channel planning and insufficient coverage for clients in the
- Some vendors, while offering a tri-radio AP solution with a dedicated third radio, deploy a complete overlay monitoring solutions orthogonal to the rest of the Wireless infrastructure and Controller solution with isolated islands of data sources, databases, visualization and even separate controls for radio configuration, control, and provisioning.

Mist APs provide continuous 24×7 scanning of the spectrum alongside 2.4Ghz, 5Ghz, and 6Ghz client access. This allows Mist to continually scan the spectrum for rogues, honeypots, interference, and for anomalies such as unsuccessful connection attempts at a site (which may be a source for a DDOS attack).

In addition, unlike traditional vendors, the Mist platform maintains a state machine and a baseline on key metrics for every physical device (AP, clients) and logical entity (location, site, site-groups) that complements flow information and a rich elastic cloud data store. Mist's AI powered infrastructure identifies unusual activity at every level of the network and this way the Mist platform can detect existing and zero-day threats. In addition, Mist's location technology can be used to accurately locate accidental or malicious rogue devices and

provide location-based access to resources. Mist's Machine Learning framework can be extended to behavioral analytics whereby client device capabilities can be checked against the "normal" baseline and alerts generated when key postures change (e.g. a 4×4 client device appears as a 2×2 device or a client device sanctioned for a California location appears to access the network from New York).

Securing Wireless in the Cardholder Data Environment (CDE)

As mentioned above, the second set of requirements applies to wireless devices on the same network where credit card data is handled. Mist allows you to conduct a PCI scan for the VLANs and Wireless LANs in scope, and helps you remediate both the vulnerabilities on the wireless network and enforce policies on the wireless management system.

The following is how Mist addresses the main requirements for these "in scope" wireless networks to be PCI DSS compliant:

Table 27: Juniper Mist PCI DSS compliance

PCI DSS REQUIREMENTS V3.1 FOR WIRELESS	MIST CONFORMS	MIST VALUE PROPOSITION
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.	✓	Mist's PCI scan report identifies the list of wireless SSIDs and APs that connect with the CDE.
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	✓	Mist does not have default passwords, encryption keys or SNMP community strings.
2.4 Maintain an inventory of system components that are in scope for PCI DSS. Maintain an inventory of system components that are in scope for PCI DSS.	✓	Mist provides a list of wireless networks and APs that are in scope of PCI DSS.
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.	✓	Mist supports strong encryption standards, including WPA2-PSK, and WPA2-Enterprise with AES encryption. As part of its PCI scan report, Mist calls out any weak encryption used on SSID in scope of the CDE.
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. <i>Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.</i>	✓	Mist makes available the latest released firmware that includes any critical fix required for the integrity of the wireless network. Mist identifies any AP that has not yet been upgraded to the latest firmware.
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	✓	Wireless network access is restricted to authorized administrators. All authorized administrators are listed on the Mist PCI scan report.

Table 27: Juniper Mist PCI DSS compliance *(Continued)*

PCI DSS REQUIREMENTS V3.1 FOR WIRELESS	MIST CONFORMS	MIST VALUE PROPOSITION
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.	✓	Mist Network Administrators are assigned roles with limited scope of access. Default administrator role is Observer (View-only).
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	✓	Mist's PCI scan report identifies the list of wireless SSIDs and APs that connect with the CDE.
8.2 In addition to assigning a unique ID, ensure proper user- authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: <ul style="list-style-type: none"> • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric 	✓	All Mist administrators are authenticated using either complex passwords or Two-factor authentication (2FA).
9.1.3 Restrict physical access to wireless access points, gateways, hand-held devices, networking/ communications hardware, and telecommunication lines.	✓	Mist APs can be made physically secure with the help of screws and brackets available as part of the access point kit. Additional physical security is supported with the Kensington lock slot on the AP.
10.1 Implement audit trails to link all access to system components to each individual user.	✓	All system access, updates and configuration changes are tracked in an audit log.
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	✓	All event logs are stored in centralized servers in the Mist cloud platform hosted in a SOC 2 Type 2 Data Center.

Table 27: Juniper Mist PCI DSS compliance (Continued)

PCI DSS REQUIREMENTS V3.1 FOR WIRELESS	MIST CONFORMS	MIST VALUE PROPOSITION
<p>11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.</p> <p><i>Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.</i></p>	✓	Mist WIDS/WIPS allows detection of authorized and unauthorized access points on the network, eliminating the need for manually intensive wireless scans. Specifically, rogue AP detection and containment protects the CDE network from being compromised.

Conclusion

As organizations rely more on wireless networks as a key enabler for business services, PCI DSS requires careful attention to WLAN security.

Fortunately, Mist has you covered. By protecting wireless networks from external attack and ensuring data transferred on CDE networks is always secure, the Mist Learning WLAN is a safe choice for mission critical wireless networks in PCI environments. The key difference in the Mist architecture is how the workflows have been streamlined to enable a cohesive experience for network IT, Security Operations Teams, Marketing, and other lines of business. With Mist, access layer connectivity and associated applications is now all about delivering a comprehensive, amazing, and secure experience.

WxLAN Access Policies

SUMMARY

Create WxLAN access control policies to specify who can and can't access resources on your network. After you add these policies to your site or WLAN template, users who connect through the specified WLANs are subject to these rules. Read this topic to learn about the requirements and

IN THIS SECTION

- [Introduction | 330](#)
- [Site-Level and Organization-Level Policies | 331](#)

options so that you can create WxLAN access policies for your use cases.

- [Labels | 331](#)
- [How Policy Rules Are Processed | 331](#)
- [Create a User Access Policy | 332](#)

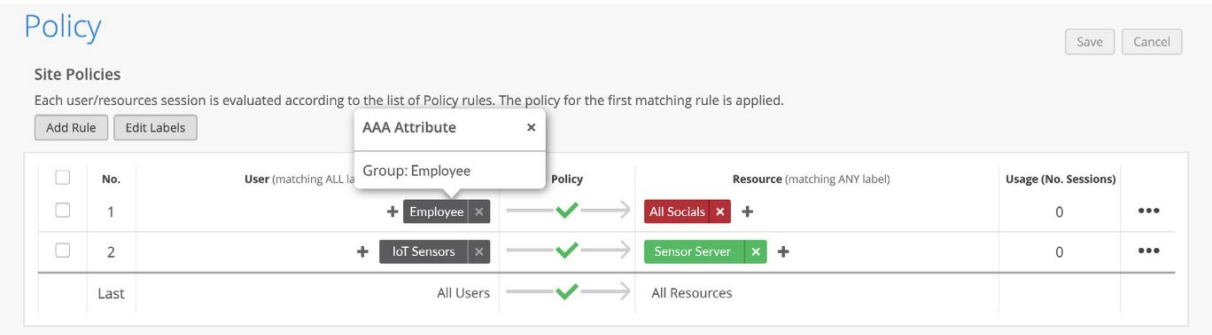
Introduction

Use access policies for a variety of use cases:

- Network segmentation
- Role based policies
- Micro-segmentation
- Least privilege

To get started with policies, you'll first create labels to group and identify users and resources. When you create a policy, you'll match users to the resources that they can or cannot access. The following example shows how easy it is to set up your rules. As shown here, you define users on the left and the resources on the right. Color coding shows which resources are blocked (red) or allowed (green).

Figure 30: Example WxLAN Access Policy



Watch this video to explore a simple use case. Here, the policy allows a user to access the Internet, a printer, and a television on the network, but no other resources.



Video: [Mist WxLAN](#)

Site-Level and Organization-Level Policies

When you create an access policy in your WLAN template, it is only applicable to the WLANs specified in that template. Any user who connects through one of these WLANs is first evaluated for the policies in the template. If user does not satisfy any of these rule, then the user is evaluated for site-level policies.

- Organization-level policies (in a WLAN template)—Select **Organization > Wireless | WLAN Templates**, and then select the template that you want to add the policy to. Scroll down to the Policy section.
- Site-level policies—Select **Site > Wireless | Policy** to open the Policy page.

Labels

You'll create labels to categorize users, groups of users, resources, and groups of resources. You can create labels at the site level or the organization level. Then you'll refer to these labels in your policies.

For help, see ["Labels" on page 135](#) and ["Using Labels in a WxLAN Policy" on page 139](#).

How Policy Rules Are Processed

- The various sets of rules are read from top to bottom in the policy.
- Each rule in a set of rules is read left to right.
- If any policy is applied then for any connecting user, it starts reading from the first rule whether that client satisfies all the user labels or not.
- It keeps reading each rule top to bottom until it finds a rule where all user labels are satisfied for that user.
- It then checks which resources are allowed or blocked for this type of user.
- For each rule, operator is set to allow but resources can either be allowed or denied.
- At the bottom of a site-level policy, there is a final default row that is setup for all users and all resources. It can be either blocked or allowed. Any user not falling under any of the policy rules will fall under this row and either all resources will be allowed or blocked for this user based on applied operation.

- If a rule consists of only allow resource, then only that resource is allowed for the user and everything else is denied.
- If a rule consists of only deny resource, then only that resource is denied for the user and everything else is allowed.
- If a rule consists of few allow and few deny resources, then only allowed resources is allowed while everything else is denied.
- Resources on the right side are displayed alphabetically and applied most specific in the event of overlapping resources. If multiple labels are created for the same host and applied as resources in the same rule, it is suggested to use the ip/port/protocol label type

Create a User Access Policy

Before you begin: If you don't already have user and resource labels for the organization, you need to create them. For more information, see ["Create Labels for a WLAN Access Policy" on page 139](#).

To create a WLAN access policy:

1. Navigate to the site-level or template-level policies:
 - Organization-level policies (in a WLAN template)—Select **Organization > Wireless | WLAN Templates**, and then select the template that you want to add the policy to. Scroll down to the Policy section.
 - Site-level policies—Select **Site > Wireless | Policy** to open the Policy page.
2. Click **Add Rule** to expose the rule line.
3. Click the add icon (+) in the User column and select a user label from the list that appears.
4. In the **Policy** column, click the check mark icon (✓), and then select the action you want to enforce: **Allow** or **Block**.
5. Click the add icon (+) in the **Resources** column and select one or more predefined applications from the list. You can also define a new resource if you prefer, and these will appear at the top of the list. In this example, you see a policy with multiple rules and rules with multiple resources.

Mist **LIVE DEMO** MON, 10:00 AM

< WLAN Templates: **Live Demo WLAN_Template** Delete Clone Save Cancel

Name

Live Demo WLAN_Template.DO_NOT_DELETE

Applies to

Entire Org Sites and Site Groups

Live-Demo x +

Except for these sites (exceptions)

Remote Users x +

☒ Limited to APs in profiles

Prod LD APs x +

WLANs Add WLAN

SSID	Band	VLAN ID	Security
Live_demo_do_not_remove	5GHz, 6GHz		WPA3/SAE (+WF
Mist_IoT	5GHz	24	WPA2/PSK (mul
Live_demo_only	5GHz, 6GHz		WPA3/SAE (+WF
Guest Wi-Fi	5GHz	2	WPA2/PSK
Live_demo_6G	6GHz		WPA3/SAE

3rd Party Tunnels Add Tunnel

Name	Remote Peer	Protocol	Authentication
------	-------------	----------	----------------

Policy

Template Policies

Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied. These rules will be applied to the users who are connected using the current template WLAN.

Add Rule Edit Labels

No.	User (matching ALL labels)	Policy	Resource (matching ANY label)
1	+ All Users	✓	TikTok x +
2	+ WLAN-Guest x	✓	Internal-employees x Internet x Private Net 10.0.0.0 x TikTok x +
3	+ WLAN-Internal x	✓	Facebook x Snapchat x WLAN-Guest x +

6. When finished creating and ordering the policy, click **Save** at the top of the screen.

7

CHAPTER

Wireless SLEs

Service Level Expectations (SLE) | 335

Wireless SLEs Overview | 344

Time to Connect SLE | 345

Wireless Successful Connects SLE | 347

Coverage SLE | 349

Roaming SLE | 351

Wireless Throughput SLE | 353

Capacity SLE | 355

AP Health SLE | 357

Service Level Expectations (SLE)

SUMMARY

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

IN THIS SECTION

- [What Are Service Level Expectations \(SLEs\)? | 335](#)
- [Finding the SLE Dashboard | 336](#)
- [Selecting the Context and Time Period | 336](#)
- [Using the System Changes Timeline | 338](#)
- [Setting the SLE Thresholds | 339](#)
- [Adjusting the SLE Display Options | 340](#)
- [Understanding the SLE Blocks | 341](#)
- [Sample SLE Block | 342](#)
- [Viewing the Root Cause Analysis Page | 342](#)

What Are Service Level Expectations (SLEs)?

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



Video:

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

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

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

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

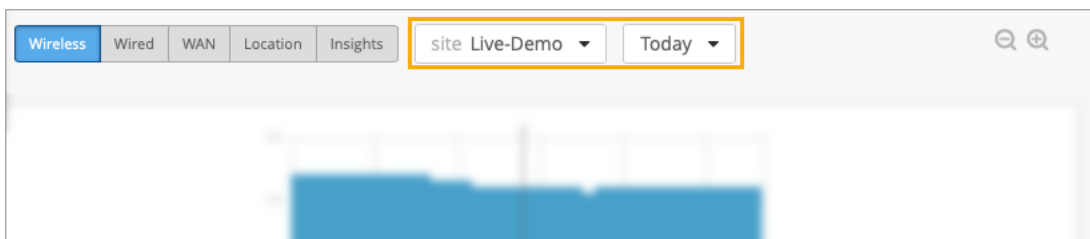
Finding the SLE Dashboard

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

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

Selecting the Context and Time Period

At the top of the Monitor page, select the context, which can be an entire organization, an access point, or a client. In addition, select a time period, such the last 60 minutes, the last 7 days, or a date range.



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

Context Example: Organization

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

Site	Avg AP Count	Avg Client Count	Overall Service	Time to Connect	Successful Connect	Coverage	Roaming	Throughput	Capacity	AP Health
Live-Demo	15	11	85%	96%	62%	93%	98%	100%	55%	92%
Westford	1	1	> 99%	100%	100%	100%	--	100%	> 99%	100%

(includes up to 100 sites, excludes sites with no data for the selected Service Level)

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

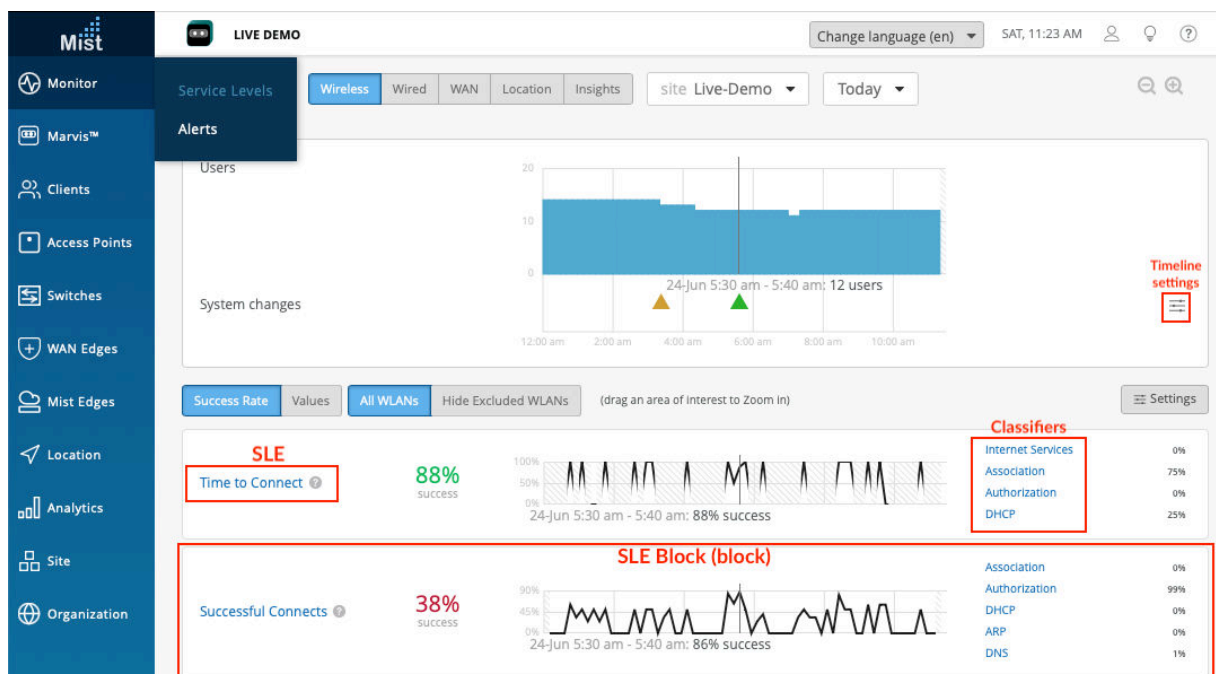
- **Overall Service**—This is the default view when you select Entire Org as the context. You can compare the overall user experience at each site.
- **SLE filter buttons**—Zoom in on a single SLE by using the SLE buttons above the table. The button options vary, depending on which page you're on (Wireless,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

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

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

Context Example: Site

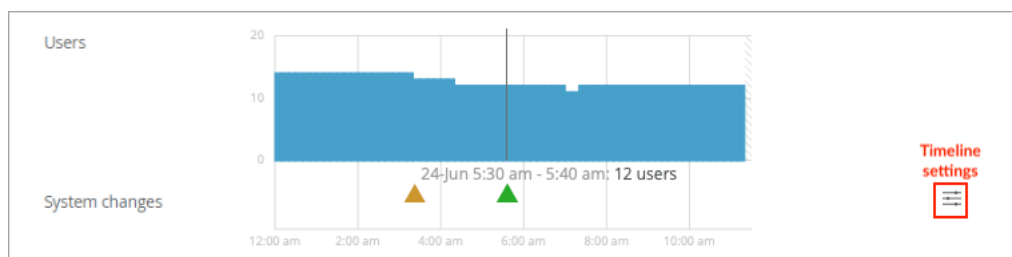
To compare all SLEs for one site, select the site as the context.



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

Using the System Changes Timeline

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



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

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

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



In the System Changes window, select or deselect check boxes for each event that you want to include or exclude.

System changes

×

Choose which system changes to display:

- ▲

AP Health
- ☑

AP Disconnected
- ☑

AP Reboot
- ☑

AP Recovery
- ☑

CPU Issues (Load/Mem/Temp)
- ☑

Ethernet Errors
- ☑

PoE Power Issue
- ☑

Radio Issue
- ☑

Software Panic
- ▲

Radio Management (RRM)
- ☑

Automatic Channel Selection
- ☑

Interference Management
- ☑

Periodic Optimization
- ▲

Admin Actions
- ☑

Configuration Change
- ☑

Firmware Upgrade
- ☑

Manual Access Point Reboot

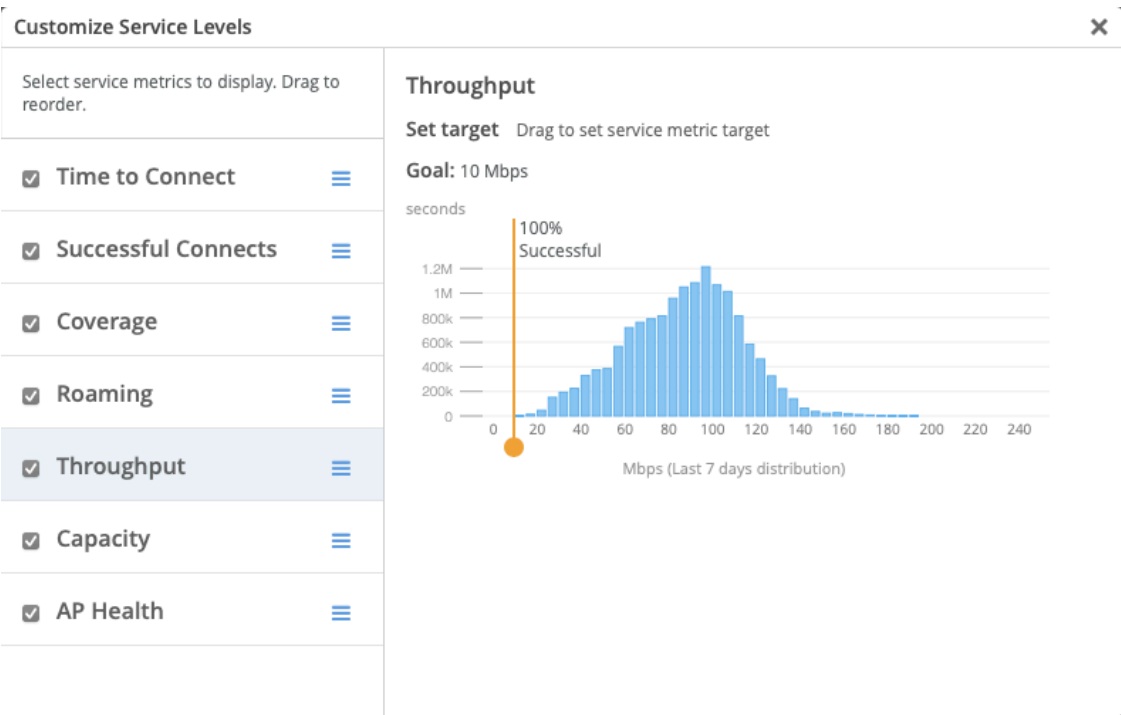
Setting the SLE Thresholds

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

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

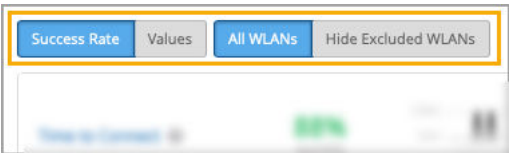


In the Customize Service Levels window, you can modify the thresholds as needed to ensure that the SLE settings meet your goals for your network.



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

Adjusting the SLE Display Options



You can adjust the SLE dashboard display as follows:

- Show success rates or values.

- Include all WLANs or hide excluded WLANs.

Understanding the SLE Blocks

Each SLE is represented by a separate block (sub-section) on the dashboard.

In each block, you'll see:

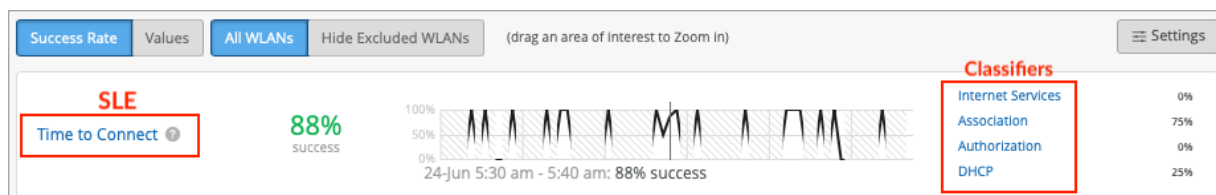
- **Overall Service Level.** On the left side of each SLE block, you'll see the overall service level for the selected site and time period.
 - Click **Success Rate** to see the *percentage* of user experiences that met the SLE success threshold.
 - Click **Values** to see the *number* of user experiences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

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

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

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

Sample SLE Block



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

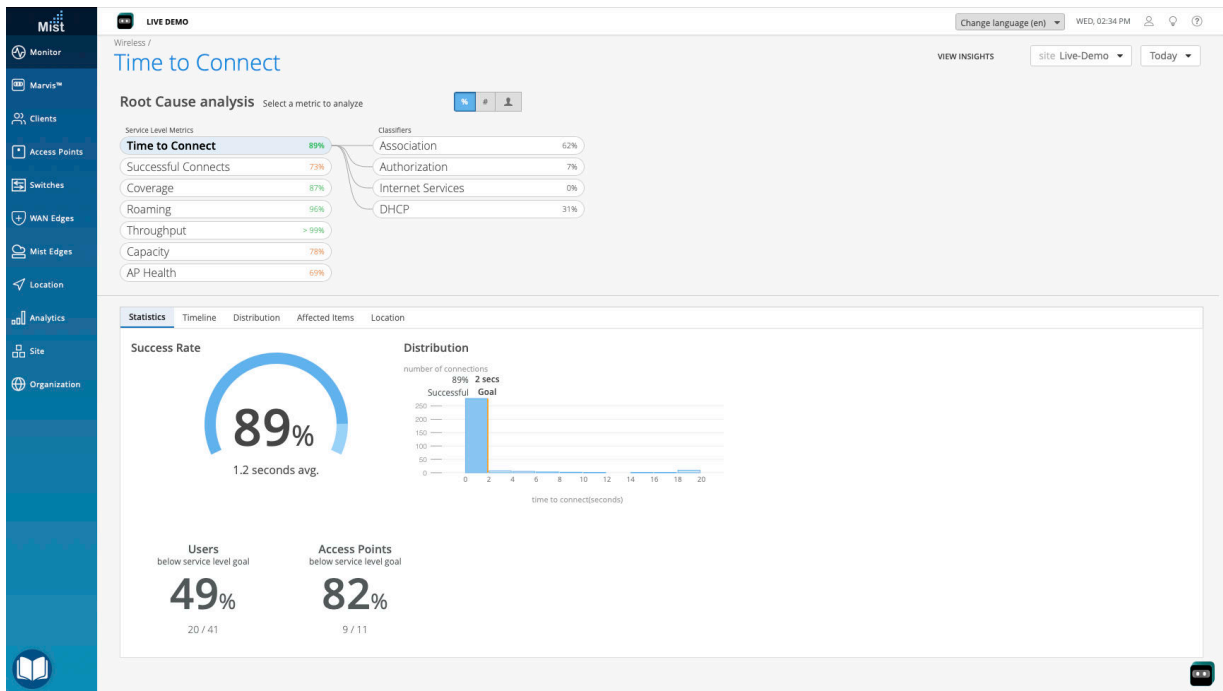
- On the left, you see that the overall success rate for the selected site and time period was 88 percent.
- In the middle, the timeline caption shows that the mouse is hovering over 24-Jun 5:30 am - 5:40 am. At that point, the success rate was 88 percent.

On the right, you see that 75 percent of the SLE-lowering issues occurred in the Association process and 25 percent occurred in the DHCP process. Together, these classifiers account for 100 percent of the user experiences that failed to meet the threshold. The other classifiers show 0 percent, meaning that they did not have any impact on this SLE.

Viewing the Root Cause Analysis Page

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

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



Tips:

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

Affected Items				
Specific Items that failed to meet the service level goal				
Users 9 Access Points 6		Q Filter		
Name	Overall Impact	Failure Rate	✕	MAC Address
hal	10.00%	100%		dc:a6:32:c7:e7:e6
denali	20.00%	100%		50:32:37:ea:c3:c2
ac:67:84:0e:d4:74	10.00%	100%		ac:67:84:0e:d4:74
abhiramms-mbp	10.00%	50%		88:66:5a:18:2d:1f
prajendir-P16	10.00%	50%		30:89:4a:df:ec:6f
satishj-mbp	10.00%	33%		bc:d0:74:59:bd:c2
svadi-mbpm1	10.00%	33%		bc:d0:74:15:82:54
rdandamudi-mbp	10.00%	25%		bc:d0:74:7e:14:7a
fe:29:6e:cc:16:ac	10.00%	13%		fe:29:6e:cc:16:ac

Wireless SLEs Overview

SUMMARY

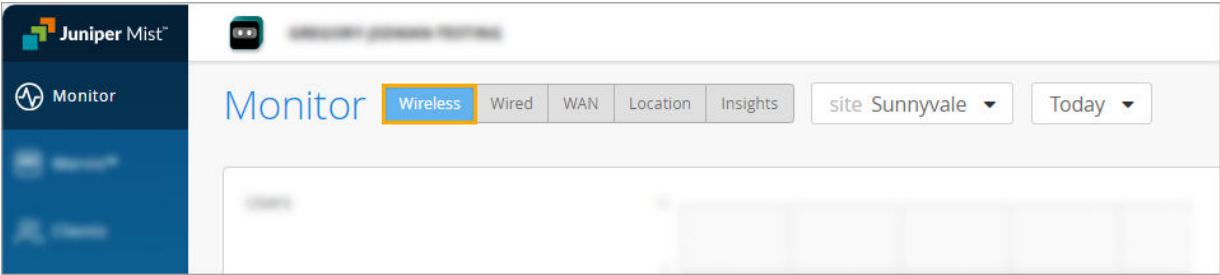
Get started using the wireless service-level experience (SLE) dashboard to assess the service levels for user-impacting factors such as throughput, signal strength, roaming, and more.

IN THIS SECTION

- Finding the Wireless SLEs Dashboard | 344
- Wireless SLEs Video Deep Dive | 345
- Using the Wireless SLEs Dashboard | 345

Finding the Wireless SLEs Dashboard

Select **Monitor** > **Service Levels** from the left menu of the Juniper Mist™ portal, and then select the **Wireless** button.



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

Wireless SLEs Video Deep Dive

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



Video:

Using the Wireless SLEs Dashboard

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

Time to Connect SLE

SUMMARY

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

IN THIS SECTION

- [What Does the Time to Connect SLE Measure? | 346](#)
- [Classifiers | 347](#)

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

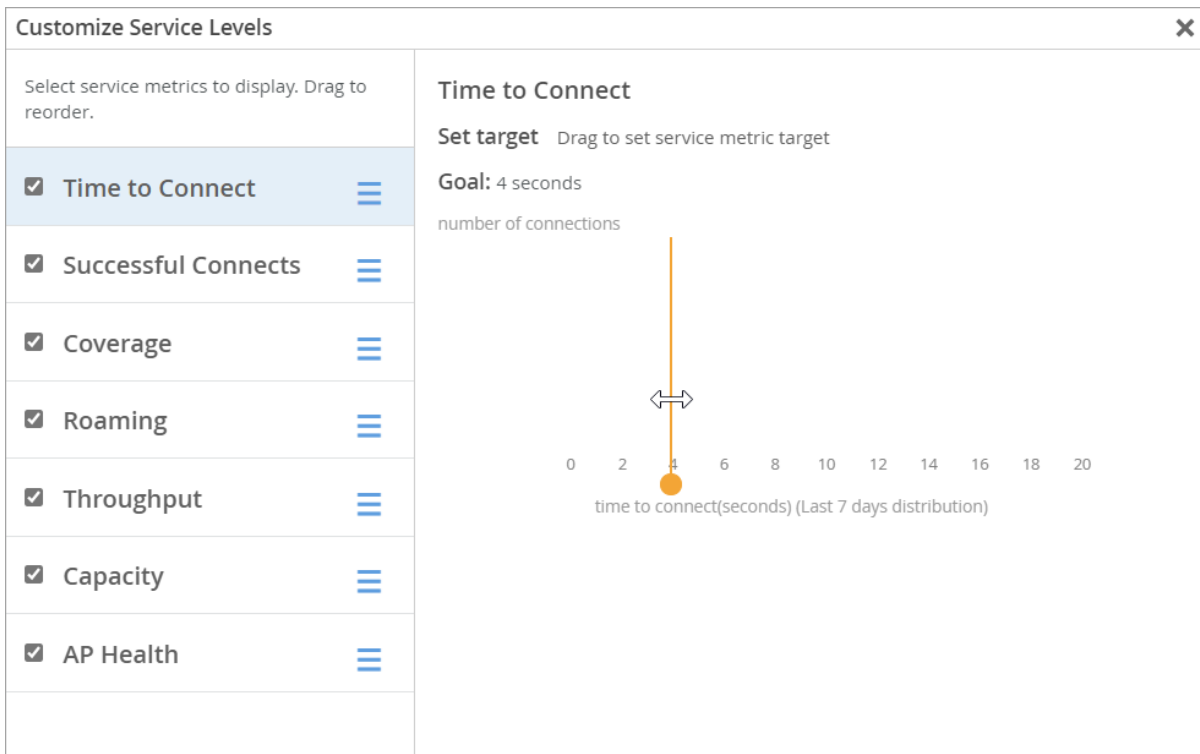


NOTE: To find the Wireless SLEs dashboard, select **Monitor** > **Service Levels** from the left menu of the Juniper Mist™ portal, and then select the **Wireless** button.

What Does the Time to Connect SLE Measure?

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

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



Classifiers

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



- **Authorization**—The time to go past the authentication state was more than 2 sigma from the average authentication latency for this site.
- **Association**—The time to go past the association state was more than 2 sigma from the average association latency for this site.
- **Internet Services** —The time to access external networks was more than 2 sigma from the moving average for this site.
- **DHCP**—(DCHP timeouts) The time to connect to Dynamic Host Configuration Protocol (DHCP) was more than 2 sigma from the average time for fully completed successful connections for this site.

Sub-Classifiers for DHCP:

- Stuck
- Nack
- Unresponsive

Wireless Successful Connects SLE

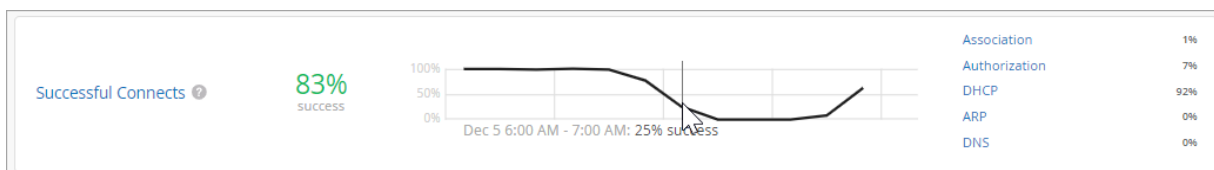
SUMMARY

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

IN THIS SECTION

- [What Does the Wireless Successful Connects SLE Measure? | 348](#)
- [Classifiers | 348](#)

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



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

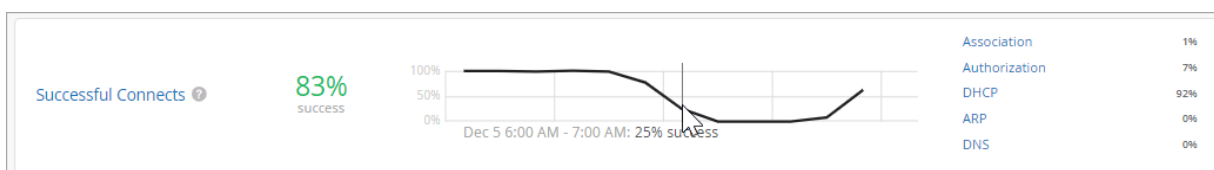
What Does the Wireless Successful Connects SLE Measure?

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

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

Classifiers

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



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

The DHCP classifier has four sub-classifiers:

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

Coverage SLE

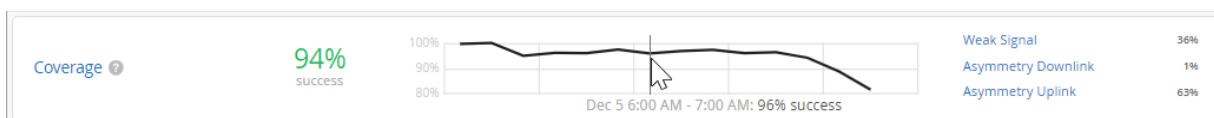
SUMMARY

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

IN THIS SECTION

- What Does the Coverage SLE Measure? | 350
- Classifiers | 350

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

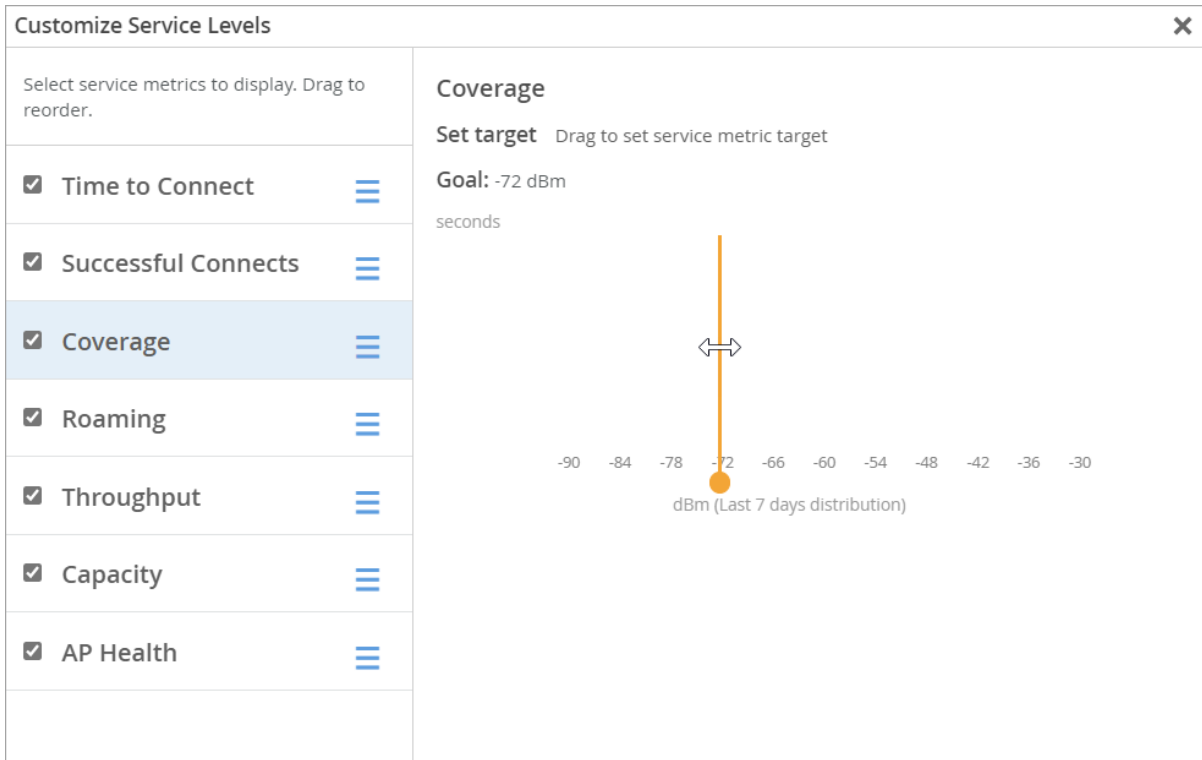


NOTE: To find the Wireless SLEs dashboard, select **Monitor** > **Service Levels** from the left menu of the Juniper Mist™ portal, and then select the **Wireless** button.

What Does the Coverage SLE Measure?

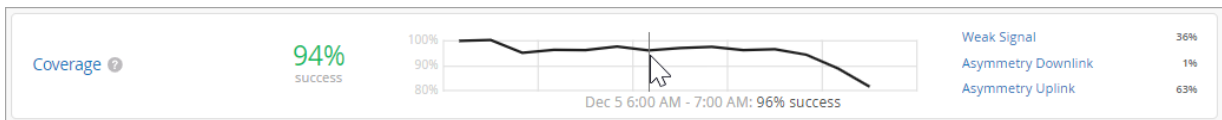
Juniper Mist tracks active clients' Received Signal Strength Indicator (RSSI), as measured by the access point. Use this SLE to determine if you have enough access points.

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



Classifiers

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



- **Weak Signal**—Clients received a weak signal due to other factors.

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

Roaming SLE

SUMMARY

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

IN THIS SECTION

- [What Does the Roaming SLE Measure? | 351](#)
- [Classifiers | 352](#)

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



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

What Does the Roaming SLE Measure?

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

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

Classifiers

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



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

Latency has different sub-classifiers for different roaming options:

- **Slow 11r Roams**—This classifier applies to fast roaming as defined by 802.11r. The roaming time exceeded 400 ms.
- **Slow Standard Roams**—This classifier applies to standard roaming. The roaming time exceeded 2 seconds.
- **Slow OKC Roams**—This classifier applies to clients using RADIUS-based authentication with Opportunistic Key Caching (OKC). The roaming time exceeded 2 seconds.
- **Stability**—This classifier tracks the consistency of AP choice and 11r usage during client roams. Juniper Mist assigns this classifier if a user capable of fast roaming on a fast- roaming enabled SSID experiences slow roaming for more than 2 seconds. This classifier contains one sub-classifier: **Failed to fast Roam**.
- **Signal Quality**—This classifier tracks the RSSI of clients during a roaming event.
- **Interband Roam**—This sub-classifier tracks when clients roam between bands.
- **Suboptimal Roam**—This sub-classifier tracks when clients roam to an AP:
 - With more than 6 dBm decrease in RSSI compared to the client's RSSI in the previous AP
 - If the RSSI in the new connection is worse than the configured coverage SLE threshold. Note that the default coverage SLE threshold is 72 dBm.
- **Sticky Client**—This sub-classifier tracks the events when a client remains connected to an AP even when more roaming options are available to improve the RSSI by more than 6 dBm.

Wireless Throughput SLE

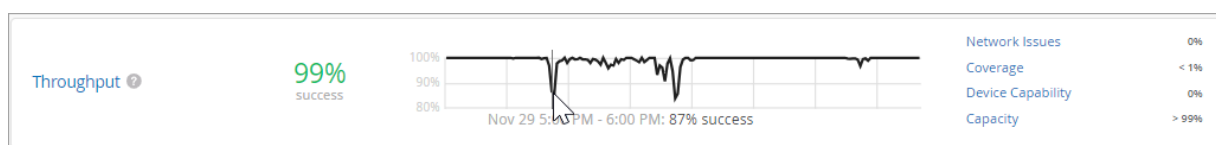
SUMMARY

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

IN THIS SECTION

- [What Does the Wireless Throughput SLE Measure? | 353](#)
- [Classifiers | 354](#)

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

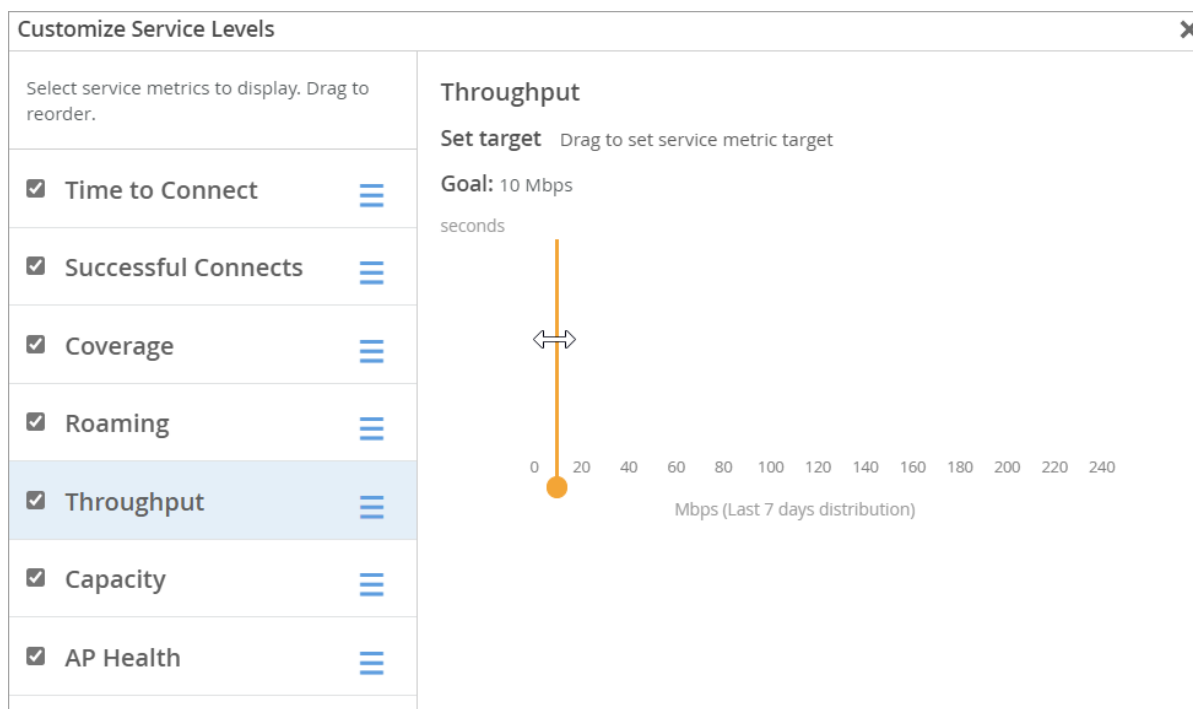


NOTE: To find the Wireless SLEs dashboard, select **Monitor** > **Service Levels** from the left menu of the Juniper Mist™ portal, and then select the **Wireless** button.

What Does the Wireless Throughput SLE Measure?

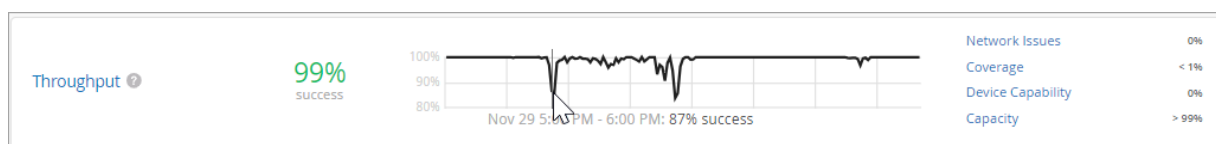
Juniper Mist calculates the estimated throughput on a per-client basis for the entire site. This calculation is done for every client every minute. The estimator considers effects such as AP bandwidth, load, interference events, the type of wireless device, signal strength, and wired bandwidth, to arrive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

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



Classifiers

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



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

The capacity classifier has four sub-classifiers:

- High Bandwidth Utilization

- Non Wi-Fi Interference
- Excessive Client Load
- Wi-Fi Interference

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

Capacity SLE

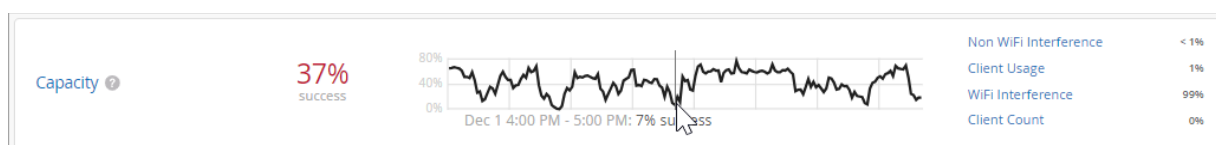
SUMMARY

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

IN THIS SECTION

- [What Does the Capacity SLE Measure? | 355](#)
- [Classifiers | 356](#)

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

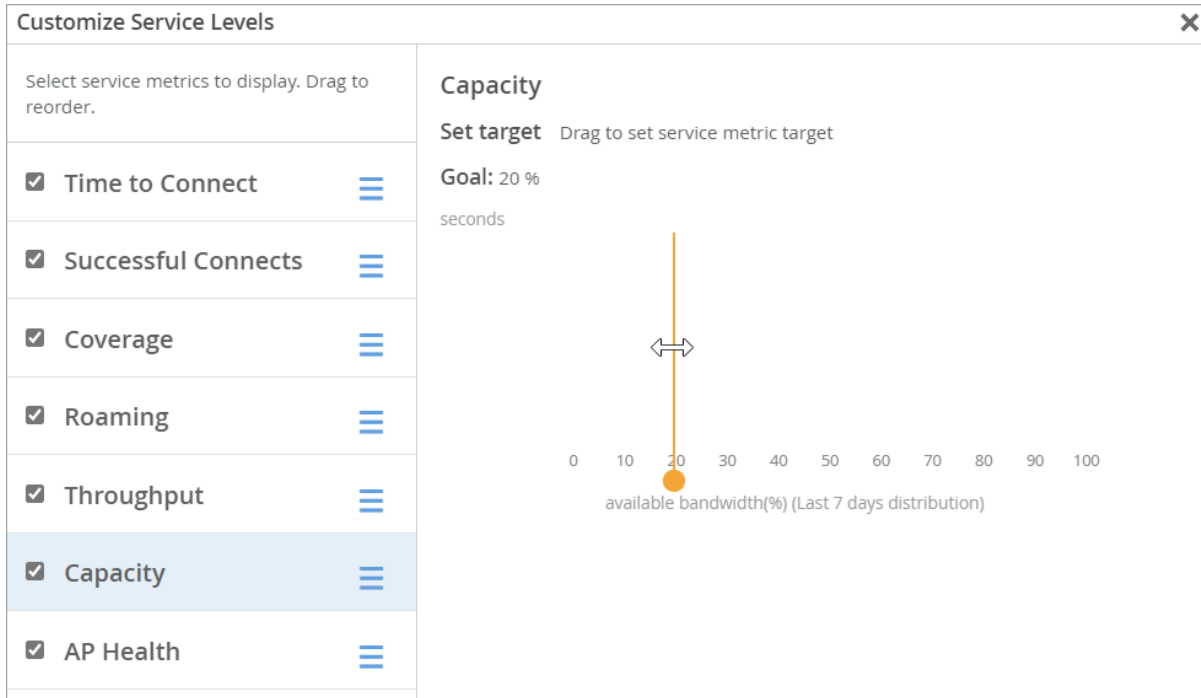


NOTE: To find the Wireless SLEs dashboard, select **Monitor > Service Levels** from the left menu of the Juniper Mist™ portal, and then select the **Wireless** button.

What Does the Capacity SLE Measure?

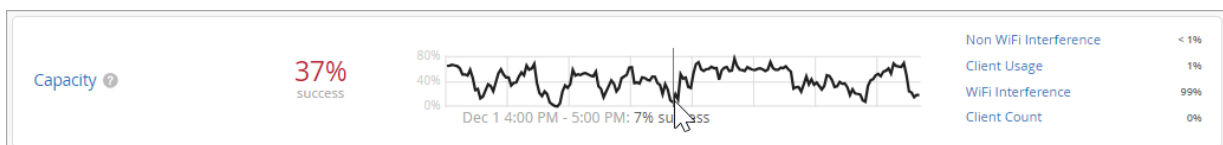
Juniper Mist monitors the percentage of the total RF channel capacity that is available to clients.

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



Classifiers

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



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

AP Health SLE

SUMMARY

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

IN THIS SECTION

- What Does the AP Health SLE Measure? | 357
- Classifiers | 357

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



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

What Does the AP Health SLE Measure?

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

Classifiers

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



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

8

CHAPTER

Troubleshooting

Using SLEs for Troubleshooting | 360

Wi-Fi Reason Codes | 361

Troubleshooting an Access Point | 366

Replace an Access Point | 396

Reset an Access Point to the Factory-Default Configuration | 401

Troubleshooting Wireless Issues | 402

Common Wi-Fi Issues | 403

Dynamic and Manual Packet Captures | 406

Steer Clients to the 5-GHz Band | 411

Bonjour and Bluetooth Devices | 413

LLDP-MED Power Negotiation | 413

Troubleshoot Your Integration with Aruba ClearPass | 414

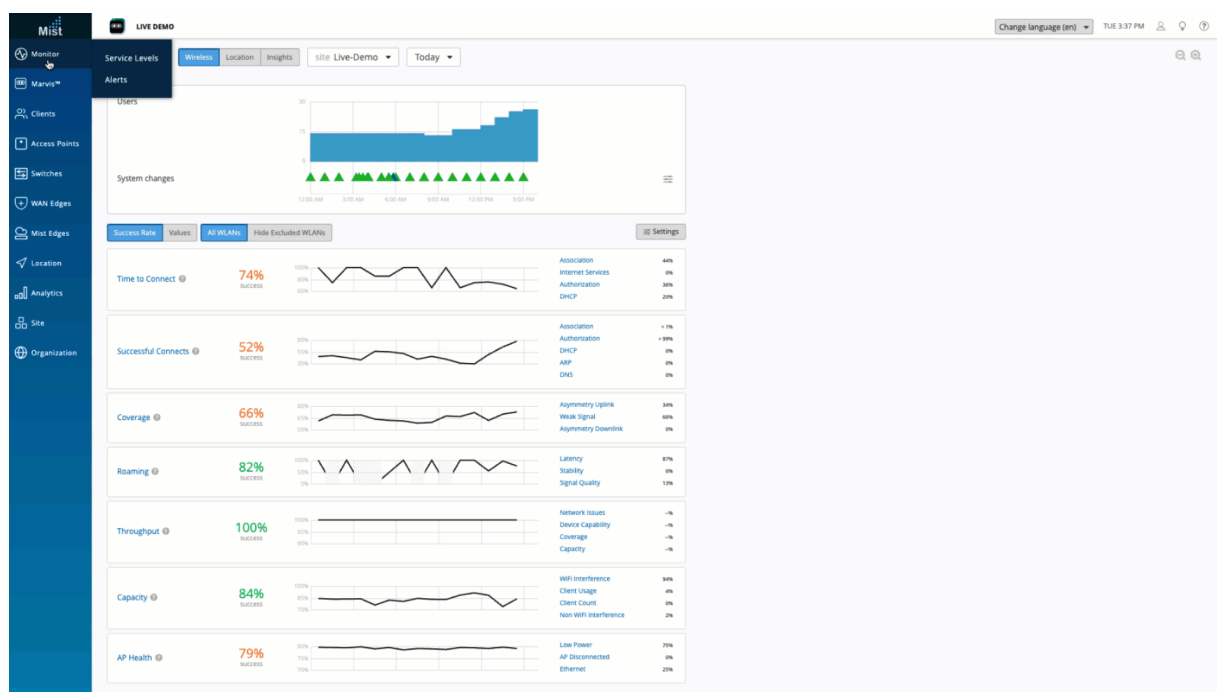
Use Labels to Identify "Unknown" Applications | 419

Using SLEs for Troubleshooting

Service Level Expectations (SLEs) provide metrics that represent users' network experience. In addition, the SLEs are a powerful troubleshooting tool that you can use to drill-down to the root cause and fix the issue, not just the symptom.

The following figure shows how you can use SLEs and their classifiers (explained below) to troubleshoot an issue. This walk-through represents just one of the many ways you can use service levels and classifiers. The Juniper Mist portal provides dozens of different service level metrics and classifiers that you can use to investigate and understand your users' network experience.

Figure 31: Using SLEs to Find Root Cause



In this example, each SLE block displays the success rate as a percentage. Take the Time to Connect SLE, for example. The 74% success rate means that 74% of the connection attempts were successful. The remaining 26% of the connection attempts did not succeed. On the right side of each SLE block, you see the percentage of unsuccessful attempts that were attributed to each classifier.

Click an SLE or classifier for additional troubleshooting details such as statistics, distribution, affected items, and so on.

Wi-Fi Reason Codes

IN THIS SECTION

- Deauthentication Reason Codes | 361

Deauthentication Reason Codes

Both the client and the AP can send a deauthentication frame to let the other side know that the connection is closed. Since it is a notification, not a request, the frame cannot normally be refused. You can use the deauthentication frame and the accompanying reason code in conjunction with Marvis, Insights, or Wireshark to troubleshoot Wi-Fi issues. IEEE 802.11-2012 Section 8.4.1.7 provides the technical standard for wireless device communication, including standard reason codes.

On the Mist portal, you can see these codes in the Client Events section on the Site Insights page (**Monitor > Service Levels | Insights**). When you select a failure event from the Client Events section, the reason code is displayed on the event details view.

In Wireshark, use a filter such as: subtype 10 management frames (disassociation) or subtype 12 management frames (deauthentication) to find the frame with the reason code.

For additional Wi-Fi frame types and subtypes, see: https://en.wikipedia.org/wiki/802.11_frame_types. For DHCPv6 Option and Status codes, see [Status Codes](#).

The reason codes are provided in the table below:

Table 30: Reason Codes

Reason Code	Meaning
1	Unspecified reason
2	Previous authentication no longer valid
3	Deauthenticated because sending STA is leaving (or has left) IBSS or ESS

4	Disassociated due to inactivity
5	Disassociated because AP is unable to handle all currently associated STAs
6	Class 2 frame received from nonauthenticated STA
7	Class 3 frame received from nonassociated STA
8	Disassociated because sending STA is leaving (or has left) BSS
9	STA requesting (re)association is not authenticated with responding STA.
10	Disassociated because the information in the Power Capability element is unacceptable
11	Disassociated because the information in the Supported Channels element is unacceptable
12	Disassociated due to BSS Transition Management
13	Invalid element, that is, an element defined in this standard for which the content does not meet the specifications in Clause 8.
14	Message integrity code (MIC) failure
15	4-Way Handshake timeout
16	Group Key Handshake timeout
17	Element in 4-Way Handshake is different from (Re)Association Request/Probe Response/Beacon frame.
18	Invalid group cipher
19	Invalid pairwise cipher

20	Invalid AKMP
21	Unsupported RSNE version
22	Invalid RSNE capabilities
23	IEEE 802.1X authentication failed
24	Cipher suite rejected because of the security policy
25	TDLS direct-link teardown because TDLS peer STA is unreachable via the TDLS direct link
26	TDLS direct-link teardown for unspecified reason
27	Disassociated because the session is terminated by SSP request
28	Disassociated because of the lack of SSP roaming agreement
29	Requested service rejected because of SSP cipher suite or AKM requirement
30	Requested service not authorized in this location
31	TS was deleted because QoS AP lacks sufficient bandwidth for this QoS STA due to a change in BSS service characteristics or operational mode (example: an HT BSS change from 40 MHz channel to 20 MHz channel).
32	Disassociated for unspecified, QoS-related reason
33	Disassociated because QoS AP lacks sufficient bandwidth for this QoS STA
34	Disassociated because excessive number of frames need to be acknowledged, but are not acknowledged because of AP transmissions or poor channel conditions

35	Disassociated because STA is transmitting outside the limits of its TXOPs
36	STA_LEAVING requested from peer STA as the STA is leaving the BSS (or resetting)
37	Requested from peer STA as it does not want to use the mechanism
38	Requested from peer STA as the STA received frames using the mechanism for which a setup is required
39	Requested from peer STA due to timeout
45	Peer STA does not support the requested cipher suite.
46	In a DLS teardown frame: The teardown was initiated by the DLS peer. In a Disassociation frame: Disassociated because authorized access limit reached
47	In a DLS teardown frame: The teardown was initiated by the AP. In a Disassociation frame: Disassociated due to external service requirements
48	Invalid FT Action frame count
49	Invalid pairwise master key identifier (PMKI)
50	Invalid MDE
51	Invalid FTE
52	SME cancels the mesh peering instance with the reason other than reaching the maximum number of peer mesh STAs.
53	The mesh STA has reached the supported maximum number of peer mesh STAs.
54	The received information violates the Mesh Configuration policy configured in the mesh STA profile.

55	The mesh STA has received a Mesh Peering Close message requesting to close the mesh peering.
56	The mesh STA has resent dot11MeshMaxRetries Mesh Peering Open messages, without receiving a Mesh Peering Confirm message.
57	The confirmTimer for the mesh peering instance times out
58	The mesh STA fails to unwrap the GTK or the values in the wrapped contents do not match.
59	The mesh STA receives inconsistent information about the mesh parameters between Mesh Peering Management frames.
60	The mesh STA fails the authenticated mesh peering exchange because of a failure in selecting either the pairwise ciphersuite or group ciphersuite.
61	The mesh STA does not have proxy information for this external destination.
62	The mesh STA does not have forwarding information for this destination.
63	The mesh STA determines that the link to the next hop of an active path in its forwarding information is no longer usable.
64	The deauthentication frame was sent because the MAC address of the STA already exists in the mesh BSS. See 10.3.6.
65	The mesh STA performs channel switch to meet regulatory requirements.
66	The mesh STA performs channel switch with unspecified reason.
67–65535	Reserved

Troubleshooting an Access Point

IN THIS SECTION

- [AP Troubleshooting Overview | 366](#)
- [What Does the AP Status LED Indicate? | 367](#)
- [Troubleshoot AP Claiming Issues | 378](#)
- [Troubleshoot AP Disconnection Issues | 379](#)
- [Troubleshoot Insufficient Power for Access Points | 393](#)
- [Troubleshoot AP Reboots | 394](#)

AP Troubleshooting Overview

Read the topics in this section to learn how you can troubleshoot issues on your access point (AP) without opening a support ticket. You can use the status LED on your AP to determine some of the issues—for example, connectivity issues.

Here are some basic steps that you can perform to troubleshoot the AP:

- Check the LED blinking pattern to identify possible errors. See ["What Does the AP Status LED Indicate?" on page 367](#).
- Check whether the AP is receiving power from the switch.
- Check whether the connected switch can learn the MAC address of the AP.
- Check whether the AP works correctly by using a different cable and different switch port.
- Verify that the required ports are open on the firewall. See [Firewall Configuration](#).

For issues related to claiming an AP, see ["Troubleshoot AP Claiming Issues" on page 378](#).

For issues related to AP disconnection, see ["Troubleshoot AP Disconnection Issues" on page 379](#).

If you are still unable to resolve the issue, raise a support ticket. See [Create a Support Ticket](#) for instructions on how to raise a support ticket.

What Does the AP Status LED Indicate?

IN THIS SECTION

- [LED Blink Patterns for AP States | 367](#)
- [LED Blink Patterns for Network Connectivity Errors | 369](#)
- [LED Blink Patterns for Cloud Connectivity Errors | 370](#)
- [LED Blink Patterns for Layer 2 Tunneling Protocol \(L2TP\) Management Errors | 373](#)
- [LED Blink Patterns for L2TP Connectivity Errors | 374](#)
- [LED Blink Patterns for Boot Configuration Errors | 375](#)
- [LED Blink Patterns for Firmware and Other Errors | 376](#)
- [LED Blink Patterns for Proxy Server Errors | 377](#)
- [AP Status LED Video Demo | 378](#)

LED Blink Patterns for AP States

A Juniper Access Point (AP) has one multicolor status LED that indicates the operational state of the AP. The LED uses a series of blink patterns that help you assess the status of an AP or determine any issues such as network or cloud connectivity issues. Use the information in the following sections to understand what the blink patterns indicate.

LED Color	Blink Pattern	AP Status
<div><div></div><div></div></div>	Blinking red for 3 seconds	The AP is starting to boot.
<div><div></div><div></div><div></div><div></div></div>	Blinking green-off-yellow-off for 12 seconds	The AP is booting.
<div><div></div><div></div></div>	Blinking green and yellow for 30–40 seconds	The AP is connecting to the Juniper Mist cloud.



(Continued)

LED Color	Blink Pattern	AP Status
	White steadily on	The AP is connected to the cloud.
	Green steadily on	The AP is configured by the Juniper Mist cloud.
	Blue steadily on	The AP has at least one wireless client connected to it.
	Blinking orange	The AP is upgrading.
	Blinking green and purple	The status LED blinks green and purple when the user clicks the Locate button in the Access Point details page.
	Red steadily on	The AP has failed.
	Gradually progresses to red	The user is holding down the Reset button.
	White gradually fades to off	The AP is going to reset the configuration to the factory default.
	Green gradually fades to off	The AP is receiving insufficient power.


LED Blink Patterns for Network Connectivity Errors

LEDs	Blink Pattern	Error	Description
<ul style="list-style-type: none"> • • 	2 yellow	No ethernet link	<p>The AP does not have an Ethernet link.</p> <p>This error is usually seen if you did not connect the AP to a switch when using a power injector.</p>
<ul style="list-style-type: none"> • • • 	3 yellow	No IP Address	There is no IP address in the static configuration or through the DHCP lease.
<ul style="list-style-type: none"> • • • 	4 yellow	No default gateway	Neither the static configuration nor the DHCP lease has a default gateway.
<ul style="list-style-type: none"> • • • • • 	5 yellow	Default gateway unreachable	The AP does not receive an ARP response from the default gateway.
<ul style="list-style-type: none"> • • • • • • 	6 yellow	No DNS	Neither the static configuration nor the DHCP lease has a DNS server.




(Continued)

LEDs	Blink Pattern	Error	Description
	7 yellow	No DNS response	The AP did not receive a response to the DNS lookup. The AP receives the DNS server information through DHCP but the AP is unable to reach the Mist cloud.
	8 yellow	Empty DNS response	The AP received an empty DNS response with no address records.
	9 yellow	Duplicate IP Address	The AP has detected a duplicate IP address on the LAN (ARP probes).

LED Blink Patterns for Cloud Connectivity Errors

LEDs	Blink Pattern	Error	Description
	1 yellow, pause, 2 yellow	Cloud unreachable	TCP SYN fails and the AP cannot ping endpoint.

(Continued)

LEDs	Blink Pattern	Error	Description
	1 yellow, pause, 3 yellow	No cloud response	The AP did not receive a response from the cloud.
	1 yellow, pause, 4 yellow	Cloud cert time check failed	NTP Time is not within cert's not-before/not-after times.
	1 yellow, pause, 5 yellow	Cloud cert invalid	The cloud provided an invalid certificate during authentication.
	1 yellow, pause, 6 yellow	Mutual auth failed	Mutual authentication between the AP and the Juniper Mist cloud failed.



(Continued)

LEDs	Blink Pattern	Error	Description
	1 yellow, pause, 7 yellow	Config fetch failed	The Juniper Mist cloud is unable to push the configuration to the AP.
	1 yellow, pause, 8 yellow	Invalid configuration	The Juniper Mist cloud provided an invalid configuration.
	1 yellow, pause, 9 yellow	Boot config save failed	The AP was unable to save or delete the boot configuration.



LED Blink Patterns for Layer 2 Tunneling Protocol (L2TP) Management Errors

LEDs	Blink Pattern	Error	Description
   	2 yellow, pause, 1 yellow	L2TP mgmt tunnel peer unreachable	The start control connection request (SCCRQ) failed and the L2TP management server is unreachable.
     	2 yellow, pause, 3 yellow	No response from L2TP mgmt tunnel peer	The L2TP management server is reachable but it does not send a response to SCCRQ.
      	2 yellow, pause, 4 yellow	L2TP mgmt tunnel config rejected	The L2TP management server credentials failed. The SCCRQ returns a StopCCN message instead of start control connection reply (SCCRP).
       	2 yellow, pause, 5 yellow	L2TP mgmt tunnel stopped	The L2TP management server sent a StopCCN and terminated the tunnel.



(Continued)

LEDs	Blink Pattern	Error	Description
	2 yellow, pause, 6 yellow	L2TP mgmt session config rejected	The L2TP management server sent a CDN in response to ICRQ.
	2 yellow, pause, 7 yellow	L2TP mgmt session shutdown	The L2TP management server sent a CDN and terminated the session.

LED Blink Patterns for L2TP Connectivity Errors

LEDs	Blink Pattern	Error	Description
	3 yellow, pause, 1 yellow	L2TP DHCP no response	The AP did not receive a response to the DHCP discover message over the L2TP tunnel.
	3 yellow, pause, 2 yellow	L2TP default gateway missing	The DHCP offer message does not have a default gateway.

(Continued)

LEDs	Blink Pattern	Error	Description
	3 yellow, pause, 4 yellow	L2TP default gateway unreachable	The default gateway does not send an ARP response.
	3 yellow, pause, 5 yellow	L2TP mgmt DNS missing	The DHCP offer message does not contain any DNS servers.

LED Blink Patterns for Boot Configuration Errors

Table 31: LED Blink Patterns for Boot Configuration Errors






LEDs	Blink Pattern	Error	Description
	4 yellow, pause, 1 yellow	Boot config unreadable	The boot configuration file is unreadable.




Table 31: LED Blink Patterns for Boot Configuration Errors *(Continued)*

LEDs	Blink Pattern	Error	Description
	4 yellow, pause, 2 yellow	Boot config invalid	The boot configuration is invalid.
	4 yellow, pause, 3 yellow	Boot config failed	The boot configuration failed and the AP has lost connection to the cloud.



LED Blink Patterns for Firmware and Other Errors

LEDs	Blink Pattern	Error	Description
	5 yellow, pause, 1 yellow	Firmware corrupt	The firmware image is corrupted.
	5 yellow, pause, 2 yellow	Unexpected failure	An API failed unexpectedly.

LED Blink Patterns for Proxy Server Errors

LEDs	Blink Pattern	Error	Description
	6 yellow, pause, 1 yellow	Proxy config invalid	The proxy configuration is invalid.
	6 yellow, pause, 2 yellow	Empty DNS response to proxy host lookup	The AP received an empty DNS response with no A (address) records for the proxy host.
	6 yellow, pause, 3 yellow	Proxy is unreachable	The proxy server is unreachable.

(Continued)

LEDs	Blink Pattern	Error	Description
	6 yellow, pause, 4 yellow	No proxy server response	The proxy server is reachable but the AP is unable to connect to the proxy TCP port.
	6 yellow, pause, 5 yellow	Proxy Authentication Required	Proxy authentication is required (code 407).

AP Status LED Video Demo

In this demo, you'll see how you can use the LED blink pattern to identify issues.



Video:

Troubleshoot AP Claiming Issues

When claiming your AP, you might see the following error messages:

- Duplicate

This error message indicates that you have already claimed the AP in your organization. If you cannot see the AP listed, verify that you have assigned it to a site. You can see an AP under a site only if you have assigned the AP to that site. To see the APs and the associated sites in an organization, go to the **Access Points** tab on the **Organization > Inventory** page. On this page, you can choose to view the list of APs in the entire organization or in specific sites.

- Invalid code - Belongs to another org

If you see this error message, check whether any of the other organizations has claimed the AP, provided that you have access to the other organization. You need to release the AP from the previous organization before claiming it in the current one.

If you see that none of the organizations have claimed the AP, contact Juniper support and submit a request to release the AP. Provide the following information in the request form:

- A snapshot of the AP
- The MAC address of the AP
- Details of the purchase order for the AP

The support team will release the AP after verifying the details.

- Invalid Code

This error message indicates that you have entered an incorrect claim code.

Troubleshoot AP Disconnection Issues

SUMMARY

Read this topic to understand how you can troubleshoot issues that cause an access point (AP) to disconnect from the cloud. The blink pattern of the LED on the AP can help you identify the problem. [Table 32 on page 380](#) lists the LED behavior for some of the common issues that cause an AP to disconnect from the network.

IN THIS SECTION

- [Need Help? | 393](#)

Table 32: Troubleshoot AP Disconnection Issues

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
○	Off	The AP is not receiving power.	<ol style="list-style-type: none"> 1. Check whether the switch port connected to the AP learns the MAC address of the AP. 2. Check the power logs on the AP to verify that PoE is enabled on the switch port. 3. Check whether the switch is supplying power to the AP. Change the cable and the switch port to see whether the AP powers on. 4. If you have a working AP, swap it with the faulty AP. Check whether the issue persists. <p>NOTE: If your APs are already installed and you cannot swap any AP, skip this step.</p>

Table 32: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
<ul style="list-style-type: none"> • • 	Blinking green and yellow for more than 30 seconds	The AP is trying to connect to the Juniper Mist™ cloud but is unable to connect.	<ol style="list-style-type: none"> 1. Verify that the relevant ports are open on the firewall. See Firewall Configuration. 2. Connect a laptop to the same switch port as the AP. Open https://ep-terminator.mistsys.net/about and see if it resolves the host. Your output should look like this: <pre>{ "version": "0.3.4476", "git-commit": "0db544d97d09c21dd2ea0778c1f6d03465861c9d", "build-time": "2020-03-16_23:45:06_U TC", "go-runtime": "go1.14", "env": "production", "procname": "ep- terminator/ðŸŒŠ/ provider=aws/ env=production/ host=ep- terminator-172-31-16-1 7-762f638f- production.mistsys.net /pid=12226/ user=terminator", "start-time": "2020-03-19T01:32:54Z" , </pre>

Table 32: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
			<pre>"uptime": 707675.367648 }</pre> <p>3. Check the firewall logs to see whether any policy is blocking the https://ep-terminator.mistsys.net/about URL.</p>
<ul style="list-style-type: none"> • • 	Blinking yellow two times	The switch or AP is experiencing a Layer 2 issue.	<p>1. Run a cable test to verify that the cable connected to the AP is working correctly.</p> <p>2. Check whether the switch port connected to the AP learns the MAC address of the AP.</p> <p>3. Check for any eth0 errors on the switch port.</p> <p>4. Change the cable and switch port and verify that the AP powers on.</p> <p>5. If you have a working AP, swap it with the faulty AP. Check whether the issue persists.</p> <p>NOTE: If your APs are already installed and you cannot swap any AP, skip this step.</p>

Table 32: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
<ul style="list-style-type: none"> • • • 	Blinking yellow three times	The AP is unable to obtain an IP address.	<p>The AP can obtain an IP address either through DHCP or through a static configuration.</p> <p>Troubleshooting steps for DHCP:</p> <ol style="list-style-type: none"> 1. Check whether the switch port configuration has the required parameters (such as native VLAN and VLAN ID) configured. 2. Check the DHCP server logs to verify that leases are available in the DHCP pool. 3. Connect a laptop to the switch port to which the AP was connected. Verify that the laptop is able to obtain an IP address from the VLAN management pool. <ul style="list-style-type: none"> • If the laptop is unable to obtain an IP address, contact the DHCP team to fix the DHCP pool. You can port-mirror the switch port to identify which step in the

Table 32: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
			<p>DHCP Discover, Offer, Request, Acknowledgment (DORA) process is failing.</p> <ul style="list-style-type: none"> If your laptop is able to obtain an IP address whereas the AP is unable to obtain an IP address, contact the Juniper support team. <p>Troubleshooting steps for static configuration:</p> <p>If the AP was connected to the Juniper Mist cloud earlier, check the static configuration on the Juniper Mist portal. If the static configuration is incorrect, then the AP will not be able to connect to the Juniper Mist cloud. To correct the static configuration:</p> <ol style="list-style-type: none"> Power off the AP by shutting down the PoE on the switch connected to the AP. Alternatively, you can remove the physical cable that provides power to the AP. Correct the configuration on the switch port.

Table 32: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
			<p>3. Reset the AP to the factory-default configuration. See "Reset an Access Point to the Factory-Default Configuration" on page 401.</p> <p>4. Power on the AP.</p>

Table 32: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
<ul style="list-style-type: none"> • • • • 	Blinking yellow four times	No default gateway IP address found in the DHCP lease or static configuration.	<ol style="list-style-type: none"> 1. Check the DHCP pool configuration to see whether the default gateway is configured. 2. If you've configured a static IP address for the AP, check whether the default gateway is configured correctly. If the default gateway is not configured correctly, follow these steps: <ol style="list-style-type: none"> a. Power off the AP by shutting down the PoE on the switch port to which the AP is connected. Alternatively, you can remove the physical cable that provides power to the AP. b. Correct the configuration on the switch port. c. Reset the AP to the factory-default configuration. See "Reset an Access Point to the Factory-Default Configuration" on page 401.

Table 32: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
			<p>d. Power on the AP.</p> <p>3. Perform port mirroring for the switch port and obtain the packet capture. In the DHCP offer packet from the server, check whether the default gateway field displays an IP address.</p> <ul style="list-style-type: none"> • If the default gateway field does not display an IP address, contact your DHCP server team to fix the configuration on the DHCP server. • If the default gateway field displays an IP address, contact Juniper Mist support to troubleshoot the issue.

Table 32: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
• • • • •	Blinking yellow five times	The default gateway IP address is configured but the AP is unable to connect to the default gateway.	<ol style="list-style-type: none"> 1. Verify that the default gateway IP address is set correctly in all the configurations on the switch port (VLAN, native VLAN) and the DHCP pool configuration. 2. If you've configured a static IP address for the AP, check whether the default gateway is configured correctly. If the default gateway is not configured correctly, follow these steps: <ol style="list-style-type: none"> a. Power off the AP by shutting down the PoE on the switch port to which the AP is connected. Alternatively, you can remove the physical cable that provides power to the AP. b. Correct the configuration on the switch port. c. Reset the AP to the factory-default configuration. See "Reset an Access

Table 32: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
			<p>Point to the Factory-Default Configuration" on page 401.</p> <p>d. Power on the AP.</p> <p>If the configuration is correct and the LED still blinks yellow five times, follow these steps:</p> <p>a. Connect a laptop on the same VLAN, network, or switch port to which the AP was connected.</p> <p>b. Ping the default gateway. Use the <code>ipconfig /all</code> command to get the default gateway information.</p> <p>If the ping fails, contact your network administrator to check for issues on the wired side.</p> <p>If the ping succeeds but the AP still fails to connect, contact Juniper Mist support.</p>

Table 32: Troubleshoot AP Disconnection Issues (*Continued*)

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
• • • • • •	Blinking yellow six times	No DNS IP address found in the DHCP lease or static configuration.	<ol style="list-style-type: none"> 1. Check the DHCP pool configuration to see whether the DNS server is configured. 2. If you've configured a static IP address for the AP, check whether the DNS server is configured correctly. <p>If the DNS server is not configured correctly, follow these steps:</p> <ol style="list-style-type: none"> a. Power off the AP by shutting down the PoE on the switch port to which the AP is connected. Alternatively, you can remove the physical cable that provides power to the AP. b. Correct the configuration on the switch port. c. Reset the AP to the factory-default configuration. See "Reset an Access Point to the Factory-Default Configuration" on page 401.

Table 32: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
			<p>d. Power on the AP.</p> <p>3. Perform port mirroring for the switch port and obtain the packet capture. In the DHCP offer packet from the server, check whether the dns server field displays an IP address.</p> <ul style="list-style-type: none"> • If the dns server field does not display an IP address, contact your DNS server team to fix the configuration on the DNS server. • If the dns server field displays an IP address, contact Juniper Mist support to troubleshoot the issue.

Table 32: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
<ul style="list-style-type: none"> • • • • • • • 	Blinking yellow seven times	<p>The DNS server does not respond to a DNS lookup. The AP receives the DNS server through DHCP but it cannot reach or ping the Juniper Mist™ cloud. When the AP gets an IP address from the DHCP server, the AP tries to reach ep-terminator.mistsys.net. If the DNS server is unable to resolve this URL, the AP cannot connect to the cloud.</p>	<ul style="list-style-type: none"> • Connect a laptop on the same VLAN or network, and try to resolve the URL <code>ep-terminator.mistsys.net</code> to an IP address by executing the <code>nslookup</code> command at the command prompt. <pre> C:\Users \username>nslookup ep-terminator.mistsys.net Server: dns.google Address: 8.8.8.8 Non-authoritative answer: Name: ep-term- production-1584483204-1989267174.us- west-1.elb.amazonaws.com Addresses: 52.9.76.55 13.57.102.113 Aliases: ep-terminator.mistsys.net </pre> • If the <code>nslookup</code> command cannot resolve the URL, explicitly add the URL to your DNS server. • If the issue is still not resolved, check the firewall and proxy logs

Table 32: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
			to see whether the traffic for the URL is getting dropped. You can also take a packet capture to analyze further.

Need Help?

If you're unable to resolve the issue after following the steps listed in the table, contact Juniper support or open a support ticket.

Provide the following details to customer support:





- What is the exact LED blink pattern that you see on the AP? You can also share a short video of the blinking pattern.
- Are you getting the MAC address of the AP on your switch port?
- Is the AP receiving power from the switch?
- Is the AP getting an IP address and pinging on the Layer 3 gateway of your network?
- What are the troubleshooting steps that you followed?
- Are there any additional logs that can help identify the root cause of the issue?

NOTE: If you select the **Allow Mist Support Team to access your Mist Organization** option on the Support Access tile in Organization Settings (**Organization > Settings**), the Mist support personnel can see all the device information available through the Mist portal.

Troubleshoot Insufficient Power for Access Points

If the switch that is connected to your access point (AP) does not provide sufficient power, you'll see a warning message on the Access Points page. Here's an example:

Warning: 2 APs are powered on insufficient power

<input type="checkbox"/>	Status	Name	MAC Address	Site
<input type="checkbox"/> 	 Connected	AP_power	5c:5b:3f	VNA AP
<input type="checkbox"/> 	 Connected	AP_vlan	5c:5b:3f	VNA AP

In such a scenario, you'll need to enable the Link Layer Discovery Protocol (LLDP) on your switch or assign 802.3at power to the AP. Juniper Mist APs do not operate properly with only 802.3af power, and this might impact your wireless services. See ["PoE Requirements for Juniper Mist APs" on page 21](#) for information about the PoE requirements for each AP model.

Troubleshoot AP Reboots

An access point (AP) can reboot owing to various reasons such as configuration changes, power outages, and firmware updates. Here are some of the possible reasons for an AP reboot and troubleshooting steps where applicable.

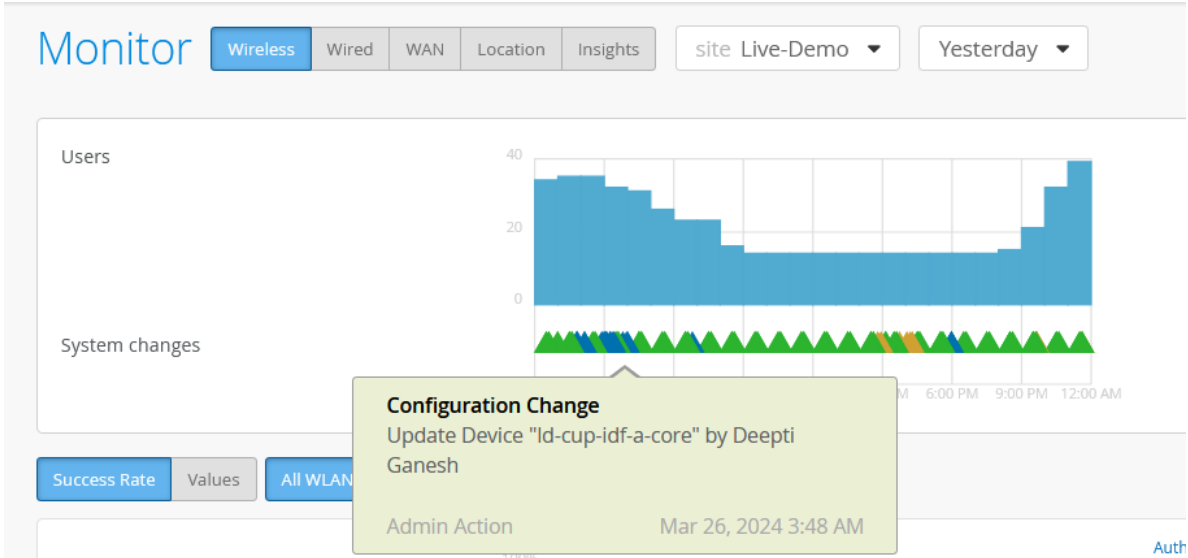
- AP reboots due to a firmware upgrade.

The **Organization > Audit Logs** page lists the firmware upgrade events for a site or organization. You can view details such as the date and time at which the upgrade was initiated and the user who initiated the upgrade.

Audit Logs Today ▾		
Timestamp	Admin Name	Message
10:51:18 AM, Jul 31	Prashanth Epuru prashanth@mistsys.com	Device "5c:5b:35:0e:13:d3" upgrade scheduled (from "0.3.14788" to "0.2.13518")
10:52:50 AM, Jul 31	Prashanth Epuru prashanth@mistsys.com	Device "5c:5b:35:0e:2c:d8" manually restarted

- AP reboot initiated manually.

A user can manually reboot an AP after a configuration change. You can view the details of the configuration change on the Wireless dashboard.



- AP reboots due to PoE issues.

APs need sufficient power to be able to operate normally. You'll see a warning message on the Access Points page highlighting the APs that are not receiving sufficient power.

Warning: 2 APs are powered on insufficient power

<input type="checkbox"/>	Status	Name	MAC Address	Site
<input type="checkbox"/>	Connected	AP_power	5c:5b:3f	VNA AP
<input type="checkbox"/>	Connected	AP_vlan	5c:5b:3f	VNA AP

Ensure that you enabled LLDP on your switch or assign the required power to the AP. For more information, see ["Troubleshoot Insufficient Power for Access Points" on page 393](#).

- AP reboots continuously and is unable to connect to the Juniper Mist cloud.

Continuous reboots might occur because of power issues. Verify that the AP is receiving sufficient power and that LLDP is enabled on the switch that is connected to the AP. See ["Troubleshoot Insufficient Power for Access Points" on page 393](#).

If this step does not resolve the issue, contact the Juniper Mist Support team.

- AP reboots due to a crash.

The APs send crash logs to the Mist cloud. The Juniper Mist team will assess the details in the crash logs, identify the cause for the crash, and fix the issue. In this case, no action is required from you.

Replace an Access Point

IN THIS SECTION

- [Replace an AP Using the Juniper Mist Portal | 397](#)
- [Replace an AP Using the Juniper Mist AI Mobile Application | 398](#)

When you replace an existing access point (AP) in your organization, Mist copies the entire configuration of that AP onto the new replacement AP. The copied configuration includes the AP settings, WLANs, physical locations, AP photos, and so on.

Depending on the AP model, certain configurations of the existing AP might not be copied to the new AP. For example, when a Juniper® BT11 Enterprise-Grade Access Point replaces a Juniper® AP41 High-Performance Access Point, the radio configuration on AP41 is not copied because the BT11 hardware does not support it.

The following configurations might not be copied:

- AP41E to AP41 and vice versa with external antenna gain configured—External antenna gain configuration is not copied to AP41 as AP41 has internal antennas.
- AP41 to AP21 and vice versa with the module port configured—Module port configuration will not be copied to the AP21 as the AP21 does not have a module port.
- AP41 to BT11 and vice versa with radio configuration—The radio configuration will not be copied to the BT11.
- AP43 to AP41 and vice versa with dual band configuration—If the AP43 dual band radio operates at 5 GHz, the replacement AP41 will operate at 2.4 GHz and 5 GHz.

NOTE: If the AP43 that has the radio set up at 5 GHz at the AP level is replaced with AP41, the 2.4 GHz configuration on the AP41 will be set to **Use Site Settings**.

Before you begin, ensure that the new AP is in the **Unassigned** state. You should claim the AP on your organization but should not assign it to any site. You can use either the Juniper Mist portal or the Juniper Mist AI™ AI mobile application to replace an AP.

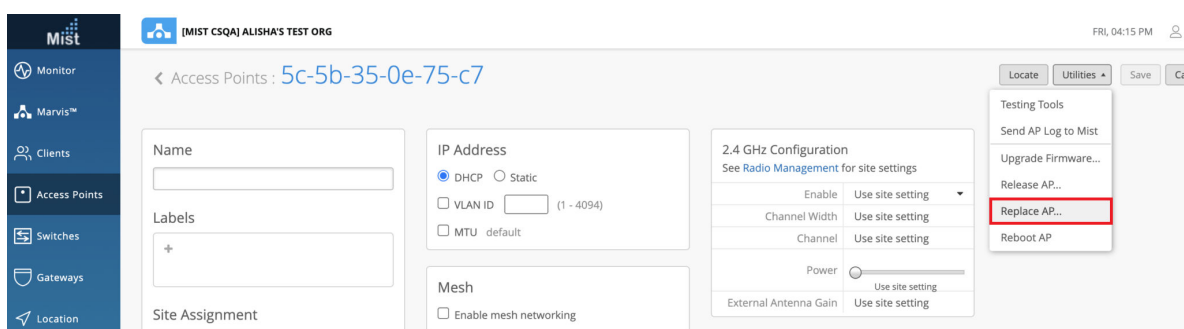
Replace an AP Using the Juniper Mist Portal

To replace an AP through the Juniper Mist portal:

1. Select **Access Points** from the left menu of the Juniper Mist portal. The Access Points page appears.
2. Click the AP that you want to replace.

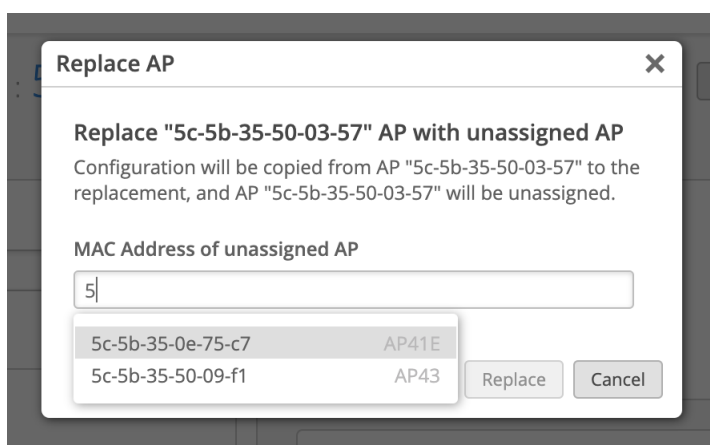
The AP settings page appears.

3. Select **Replace AP** from the **Utilities** menu in the top-right corner of the page.

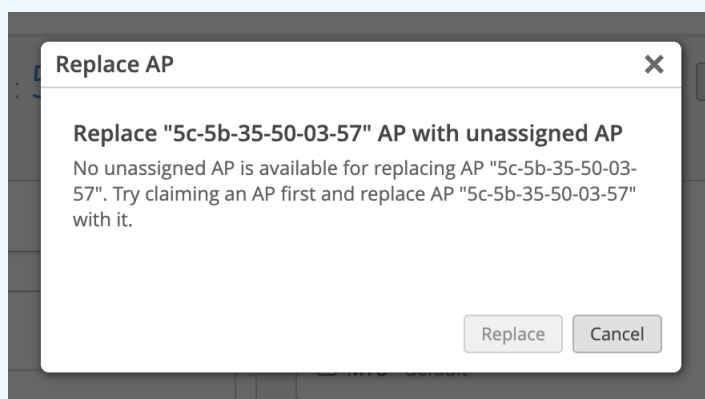


4. Enter the MAC address of the unassigned AP with which you want to replace the existing AP.

When you enter the MAC address, a drop-down list appears, displaying all the available APs, along with their model type. This list does not include switches or gateways.



NOTE: If no unassigned APs are available for replacement, the Replace AP page displays information about the unavailability of a replacement AP.



5. Click **Replace**.

The following API call is made to replace the AP:

```
Request URL: https://api.mist.com/api/v1/<<org_id>>/inventory/replace
Request Method: POST
Request Payload: {"site_id": "<<>>", "mac": "<<>>", "inventory_mac": "<<>>"}
```

The MAC address can be in any of these formats—xxxxxxxxxxxx, xx:xx:xx:xx:xx:xx, or xx-xx-xx-xx-xx-xx. Note that the MAC address must belong to an unassigned AP.

The new AP replaces the existing AP, which is unassigned from the site.

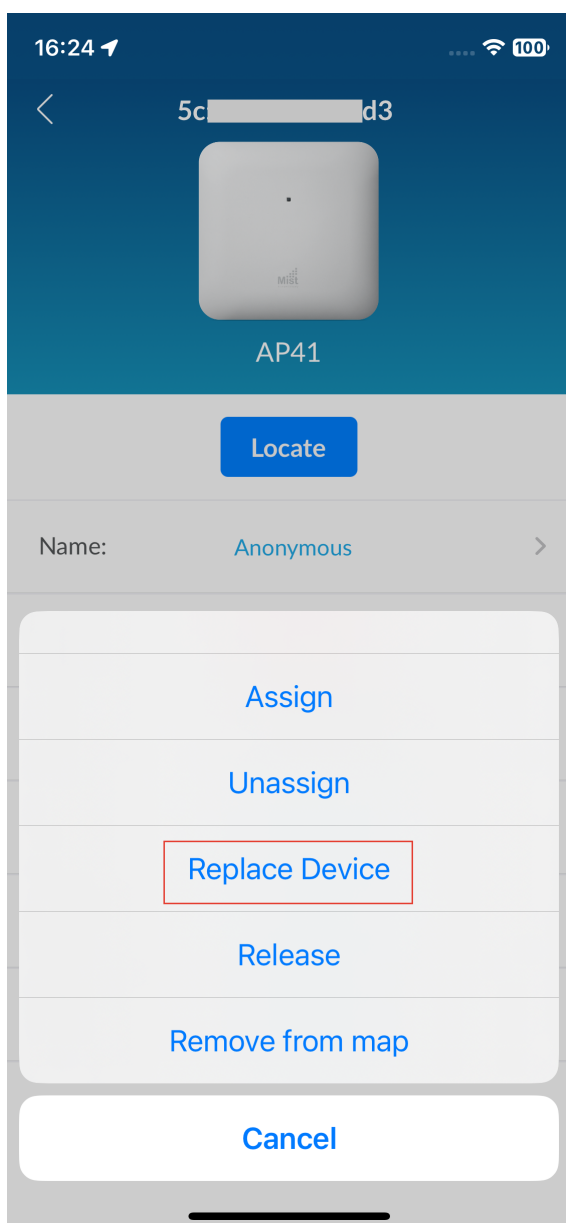
Replace an AP Using the Juniper Mist AI Mobile Application

To replace an AP using the Juniper Mist AI mobile application:

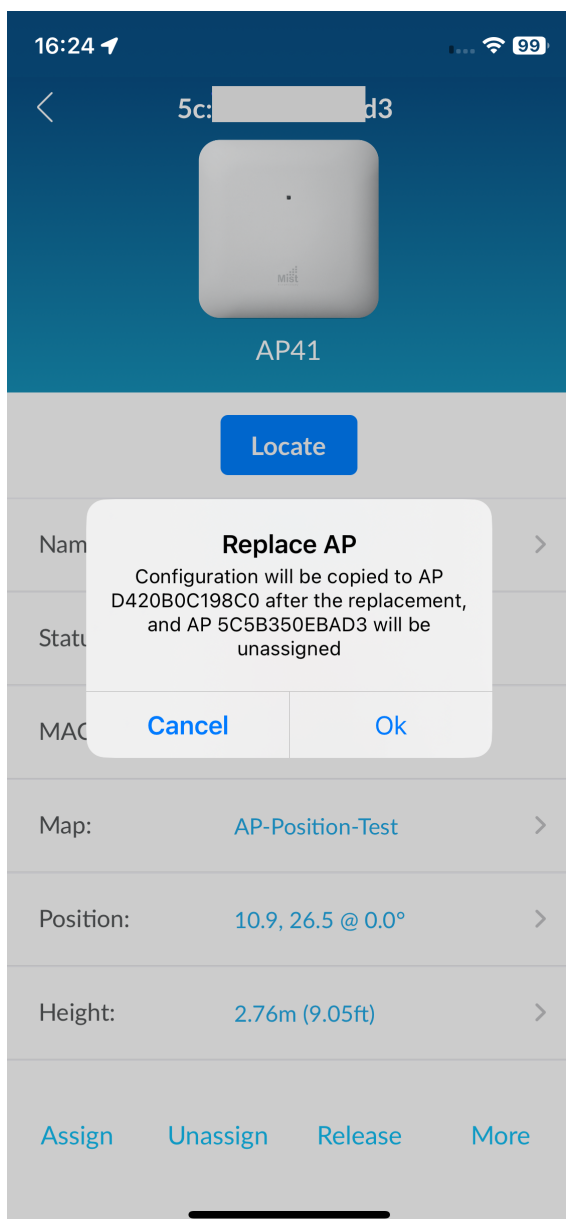
1. Open the Juniper Mist AI application on your mobile phone and log in with your account credentials.
2. Select your organization.
3. Tap **Device Inventory > Access Points**.
4. Tap the AP that you want to replace.

The AP settings page appears.

5. Tap **More > Replace Device**.



6. Enter the claim code or scan the QR code of the new AP. If you have not already claimed the AP, the application automatically claims the AP and assigns the AP to the site. You'll also see a confirmation dialog box that prompts you to confirm the replace operation.



7. Click **OK**.

The configuration from the existing AP is copied to the new AP, which then replaces the existing AP.

Reset an Access Point to the Factory-Default Configuration

You can reset your access point (AP) to the factory-default configuration using the Reset button. You might need to do this when:

- The current configuration on your AP fails and the AP cannot connect to the Juniper Mist cloud.
- The AP is unresponsive.

When you reset an AP, all existing configuration is removed. You must ensure that your AP receives a valid IP address from the DHCP server after resetting so that the AP can connect to the Mist cloud.

Before you reset your AP:

1. In the left menu of the Juniper Mist portal, select **Organization > Access Points**.

The **Access Points** page appears.

2. Click the AP name on the **Access Points** page.

The **AP Details** page appears.

3. Set **IP Address** to **DHCP**.

4. Click **Save**.

To reset your AP to the factory-default configuration:

1. Power off the AP.
2. Using a thin, pointed object, such as a pin, press and hold the Reset button. At the same time, power on the AP.

The LED on the AP blinks red for 3 seconds. This LED behavior indicates that the AP is starting to boot.

-
-

3. Keep the Reset button pressed.

After a pause, the LED gradually turns solid red, and then starts to blink red again. This LED behavior indicates that the AP is reverting to the factory-default configuration.

-
-
-

4. Release the Reset button when the LED starts blinking with the pattern *green-off-yellow-off*.



This LED behavior indicates that the AP has started to boot.

5. When the AP completes booting, the LED starts blinking green and yellow.



This LED behavior indicates that the AP is trying to connect to the Juniper Mist cloud.

The AP resets to the factory-default configuration. Here is a sample video that shows how to reset an AP.



Video: [Factory Reset](#)

Troubleshooting Wireless Issues

When it comes to troubleshooting issues with the wireless network, you always want to be sure that a proper site survey was both conducted and followed. Assuming one was, then you can make the best use of Marvis, Insights, and SLEs. For example, you can use Marvis, the virtual network assistant, to view a client's roaming history to track and discover the root cause of connection drops. See ["Using SLEs for Troubleshooting" on page 360](#) and ["View Roaming History" on page 233](#).

You can also use AP insights to see channel utilization (which should always be less than 50%). See [Figure 1 on page 4](#).

The ["Radio Management \(page\)" on page 207](#) is good place to understand radio coverage and performance site wide.

In addition to these tools, the following principles apply:

- Be sure that the APs are running the recommended firmware (from the Juniper Mist portal, click the Help icon and then **Firmware Updates** for the list of recommended firmware).
- Use the 5 GHz radio band for voice and video in the WLAN. It provides both higher bandwidth and more channels so the performance could be better than 2.4 GHz. Be aware that the environmental variables (such as distance and RF interference) could affect the performance.
- When using 802.11b/g, disable the data rates below 9 Mbps if possible. Similarly, when using 802.11a, disable the 6-Mbps and 9-Mbps data rates if possible. Do be aware, though, that

eliminating the lower data rates will prevent any legacy clients from connecting to the WLAN, so some prior research and experimentation is advisable. See ["Radio Settings \(RF Templates\)" on page 213](#).

- Make sure you are using RRM on the APs. This will ensure that both power and channel usage are optimized at all times. See ["Radio Management " on page 204](#).
- Be sure that QoS is enabled on the WLAN, and that the same QoS settings are reflected on the connected switch and any VLANs. See QoS setting in ["WLAN Options" on page 122](#). For the steps to create a WLAN, see ["Add a WLAN to a Site or a WLAN Template" on page 121](#).
- Make sure that the signal-to-noise ratio (SNR) is at least 25 or greater, and that signal strength is at least -65 dBa for both the client and the AP. See ["RSSI, Roaming, and Fast Roaming" on page 230](#).
- Disable band-steering and force the clients to choose a radio band (5 GHz or 2.4 GHz).

Common Wi-Fi Issues

Periodic Wi-Fi issues are most commonly caused by interference, channel changes, and client load. See ["Radio Management \(page\)" on page 207](#) and ["Radio Management " on page 204](#) for detailed information.

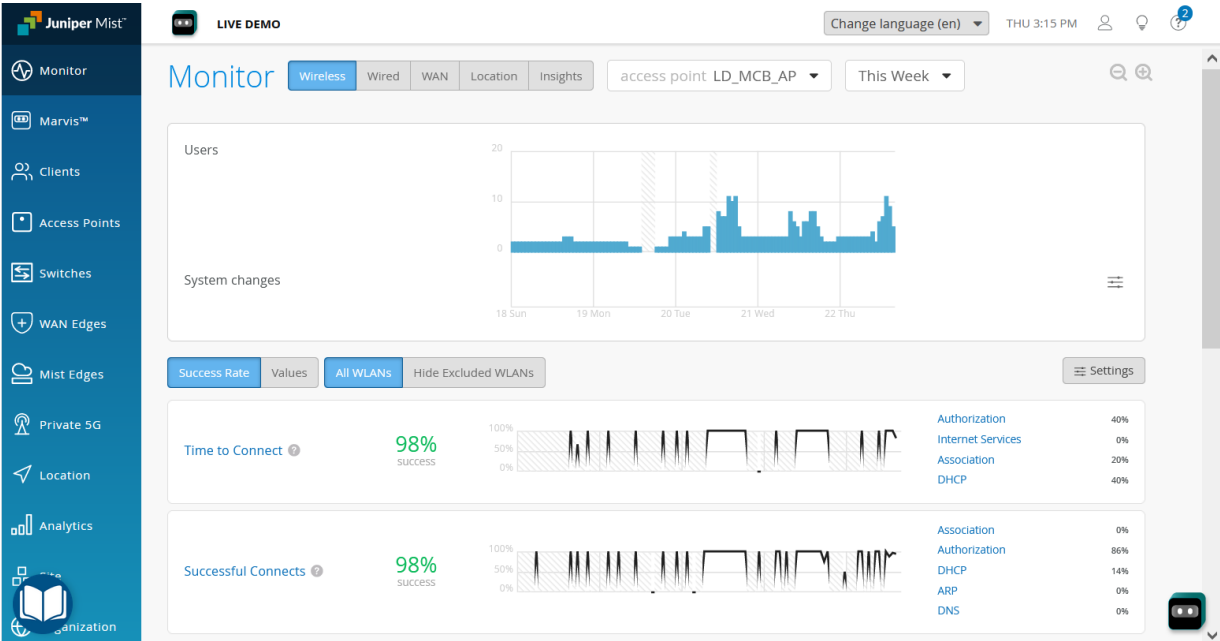
Interference

Interference can result in slower network speeds and client disconnections. This can be caused by various wireless signals and devices. For example, any Wi-Fi networks nearby, microwave ovens, or Bluetooth devices could disrupt or weaken your Wi-Fi signals. The most common types of interference are:

- Adjacent interference, which happens when APs use channels that are close to each other (for example, channels 1 and 2);
- Co-channel interference, which happens when two or more APs are using the same channel;
- Non-Wi-Fi interference, which can be caused by radar from motion detectors, Bluetooth devices, and microwave ovens.

You can view these by clicking **Monitor > Service Levels | Insights** in the main menu, selecting the time period and AP you want, and then scrolling down the page to **Channels** (see [Figure 32 on page 404](#)).

Figure 32: Viewing channel usage

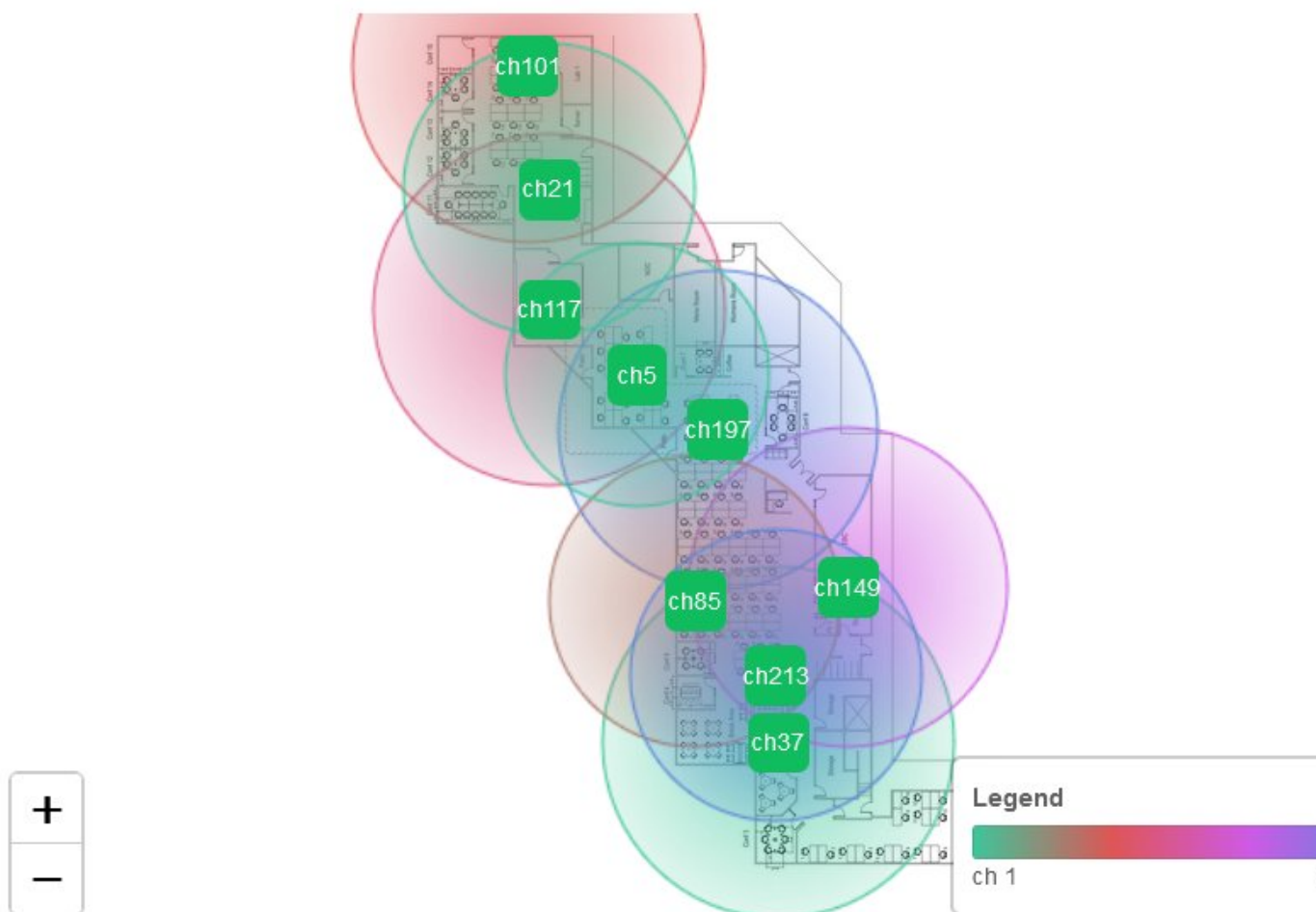


You can check for co-channel and adjacent channel interference by clicking **Site > Radio Management** and then scrolling down to **Current Radio Values** (see [Figure 33 on page 405](#)).

Figure 33: Floor plan view of Current Radio Values.

Current Radio Values

9 APs on the floorplan



Channel Changes

Mist APs will automatically change channel whenever radar is detected on dynamic frequency selection (DFS) channels, or when the current channel encounters interference. During such times, the AP deauthenticates all associated clients and Wi-Fi connection will be briefly interrupted.

You can view these by clicking **Site > Radio Management** and then scrolling down to **Radio Events** (see [Figure 34 on page 406](#)).

Figure 34: Radio Events showing channel changes.

Radio Events					
Time	Radio	Channel	Channel	Channel	Channel
Feb 21, 2024 3:00:04 PM	LD_Marvis	5 GHz	5 GHz → 5 GHz	136	→
Feb 21, 2024 3:31:28 PM	LD_RS_Support	5 GHz	5 GHz → 5 GHz	136	→
Feb 21, 2024 3:57:44 PM	LD_Kitchen	5 GHz	5 GHz → 5 GHz	136	→
Feb 21, 2024 4:00:04 PM	LD_Kitchen	5 GHz	5 GHz → 5 GHz	153	→
Feb 21, 2024 4:00:04 PM	LD_IDF_B_AP-3rd-Party-Switch	5 GHz	Disabled → 5 GHz	132	→
Feb 21, 2024 4:33:21 PM	LD_Kitchen	5 GHz	5 GHz → 5 GHz	153	→
Feb 21, 2024 4:37:43 PM	LD_Kitchen	5 GHz	5 GHz → 5 GHz	136	→
Feb 21, 2024 5:03:17 PM	MC_DavidL AP	5 GHz	5 GHz → 5 GHz	132	→
Feb 21, 2024 5:03:17 PM	LD_IDF_B_AP-3rd-Party-Switch	5 GHz	Disabled → 5 GHz	136	→

Client Load

Client Load and the type of clients can also cause certain issues while passing traffic. If the number of clients is high, the channel contention will also be high. This will affect traffic.

Dynamic and Manual Packet Captures

SUMMARY

The Juniper Mist portal provides both dynamic and manual packet captures to help identify the source

IN THIS SECTION

- Dynamic Packet Captures | 407

of communication failures between the client and AP.

- [Configure IEEE 802.11 on Wireshark | 408](#)
- [View Wireless Packet Captures in Wireshark | 409](#)
- [Manual Packet Capture Options | 410](#)

NOTE: Mist does not collect or store any payload data from packets capture. Only transmission and connection data are used.

Dynamic Packet Captures

Whenever a connection failure event occurs between the wireless client and AP, it automatically triggers a short-term dynamic packet capture. These include DHCP issues (timeout, denied, terminated), authorization failures (RADIUS not responding, Access-Reject, incomplete authorization), and roaming issues (11r FBT and OKC authorization failures).

Packet captures are saved to the cloud, where they are associated with the triggering event in the Juniper Mist portal. You can view or download the packet capture from the events sections (such as Client Events) on the Insights panel.

The following image shows dynamic packet captures stored under Client Events (**Monitor > Service Levels | Insights > Client Events**):

Client Events

36481 Total

2520 Good

16256 Neutral

17705 Bad

Association

AP Deauthentication

sheepy-raspy

2:03:45.376 PM Sep 14, 2023

Authorization Failure ⓘ

sheepy-raspy

2:03:45.376 PM Sep 14, 2023

AP Deauthentication

aconcagua

2:03:41.750 PM Sep 14, 2023

Authorization Failure ⓘ

aconcagua

2:03:41.750 PM Sep 14, 2023

DHCP Timed Out ⓘ

Google

2:03:39.153 PM Sep 14, 2023

AP Deauthentication

sheepy-raspy

2:03:38.926 PM Sep 14, 2023

Authorization Failure ⓘ

sheepy-raspy

2:03:38.919 PM Sep 14, 2023

Protocol

802.11

VLAN

24

Band

5 GHz

Gateway

192.168.1.1

Capabilities

80MHz

Channel

44

Download Packet Capture

Manual Packet Captures

Wired packet capture applies to the wired ports of APs (not the switch ports). WAN packet captures support Session Smart Router and SRX WAN edge device ports.

For manual packet captures, go to **Site > Packet Captures**, where you can:

- Choose which network type to capture packets from: wired, wireless, or WAN.
- Restrict the packet capture to specific clients, WLANs, APs, or wireless bands.
- Configure the number of packets captured, packet size in bytes, and the duration of the capture session.
- Configure other capture parameters such as header inclusion and capture filters. See [Table 33 on page 410](#) for details.

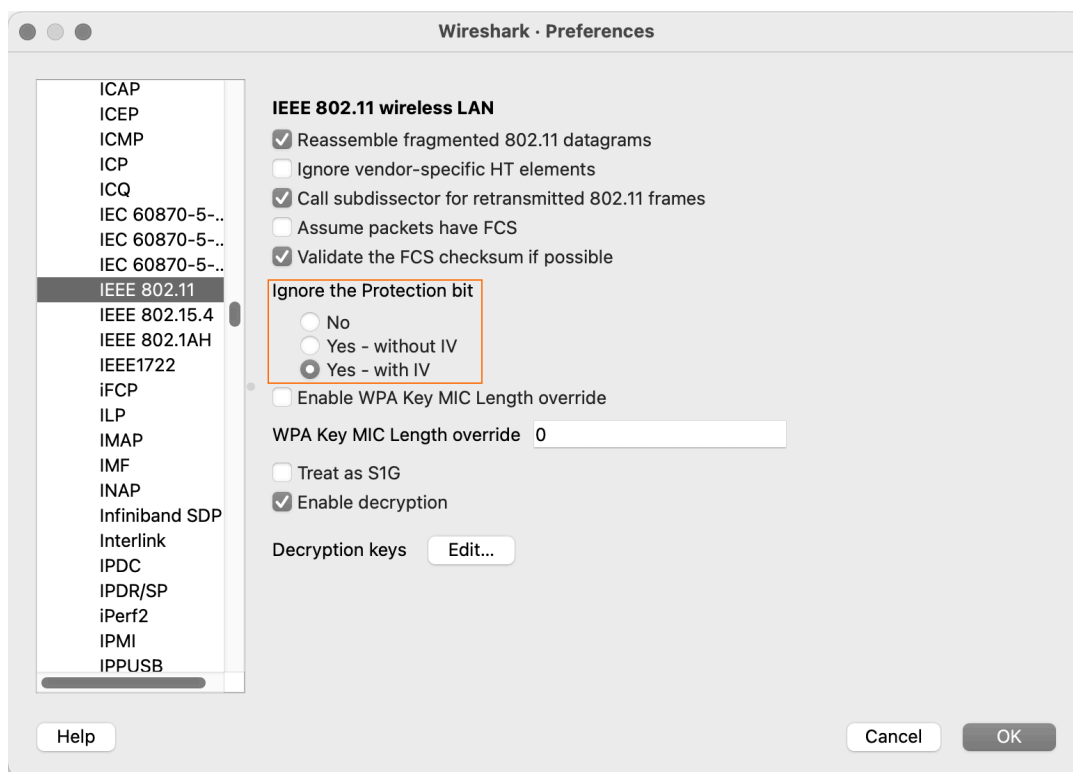
After downloading the packet capture to your computer, follow the steps below to view them in Wireshark.

Configure IEEE 802.11 on Wireshark

Packet inspection requires Wireshark. See <https://www.wireshark.org> for the download file and related information.

To configure Wireshark to view packets captured from the Juniper Mist portal, follow the steps below:

1. Open the Wireshark application on your computer.
2. Open the Wireshark Preferences window:
On a Windows computer, navigate to **Edit > Preferences**.
On a Mac computer, navigate to **Wireshark > Preferences**.
3. In the Preferences window, expand the **Protocols** menu option and scroll down to **IEEE 802.11**.
 - a. Select **Yes - with IV** and then click **OK**, as shown in the following image:



View Wireless Packet Captures in Wireshark

You can capture packets from both your wired and wireless networks. The following configuration regards wireless packet, for which you can see:

- Wireless channel information
- Wireless data rate
- Received signal strength indicator (RSSI)

To accomplish this task, you must download and install the Wireshark application on your computer. In a Web browser, navigate to <https://www.wireshark.org> for Wireshark application downloads and detailed information about Wireshark. For additional information about Wireshark, see <https://www.wireshark.org/docs/>.

This topic provides minimal guidance about how to configure Wireshark for use in examining wireless packet captures gathered from the Juniper Mist portal.

1. Open the Wireshark application on your computer.
2. Open the Wireshark Preferences window:

On a Windows computer, navigate to **Edit > Preferences**.

On a Mac computer, navigate to **Wireshark > Preferences**.

3. In the Preferences window, navigate to **Appearance > Columns**.
4. Click the **Add (+)** button to add a new radiotap column to the Wireshark display (radiotap headers include wireless packet frames that would otherwise not be displayed. See: <https://www.wireshark.org/docs/dfref/r/radiotap.html>).

Wireshark adds a new line called New Column, and the type Number.

- a. Double-click the **New Column** title and type Channel as the title.
 - b. Double-click the **Type** column and select Frequency/Channel from the drop-down menu.
 - c. Leave the **Displayed** column selected.
5. Repeat Step 4 two times
 - a. The first time, use **Data Rate** for the column title and **IEEE 802.11 TX Rate** for the type.
 - b. The second time, use **RSSI** as the column title and **IEEE 802.11 RSSI** for the type.
 6. Click **OK** to save your changes.

Wireshark will display the new columns when you open a packet capture (.pcap) file for viewing.

Manual Packet Capture Options

By default, Juniper Mist streams the packet capture session data, including beacon frames, to the Mist portal. The following table describes the packet capture options that you can use when you create a packet capture session.

Table 33: Packet Capture Options

Option Name	Option Function	Usage Notes	Firmware Notes
Include Network Headers	Include packet headers in addition to the packet data.	Packet capture works by buffering packets locally on the device, meaning there is limited space available for storage. By default, Mist truncates header data from the captured packets to reduce the size of capture files while still providing the most relevant information.	–

Table 33: Packet Capture Options (*Continued*)

Option Name	Option Function	Usage Notes	Firmware Notes
Local Capture	Do not stream the live capture data to the Mist GUI.	Earlier AP firmware did not support live streaming packet captures to the Juniper Mist portal.	Required for AP firmware versions before 0.10.x
Canned Filters	Pre-defined filters that vary based on the type of packet capture you're performing.	The filters available in the list change depending on whether you're capturing wireless, wired, or WAN packets. For example, beacon frames are only available for wireless packet captures.	–
Advanced Filters	Create your own packet filters for the capture session using tcpdump syntax.		0.10.x or later
Expression Builder	Interactive GUI tool to build custom filters in tcpdump syntax for use in the capture session.	You can let the builder start the filter entry and then add to or delete from the entry manually.	0.10.x or later

Steer Clients to the 5-GHz Band

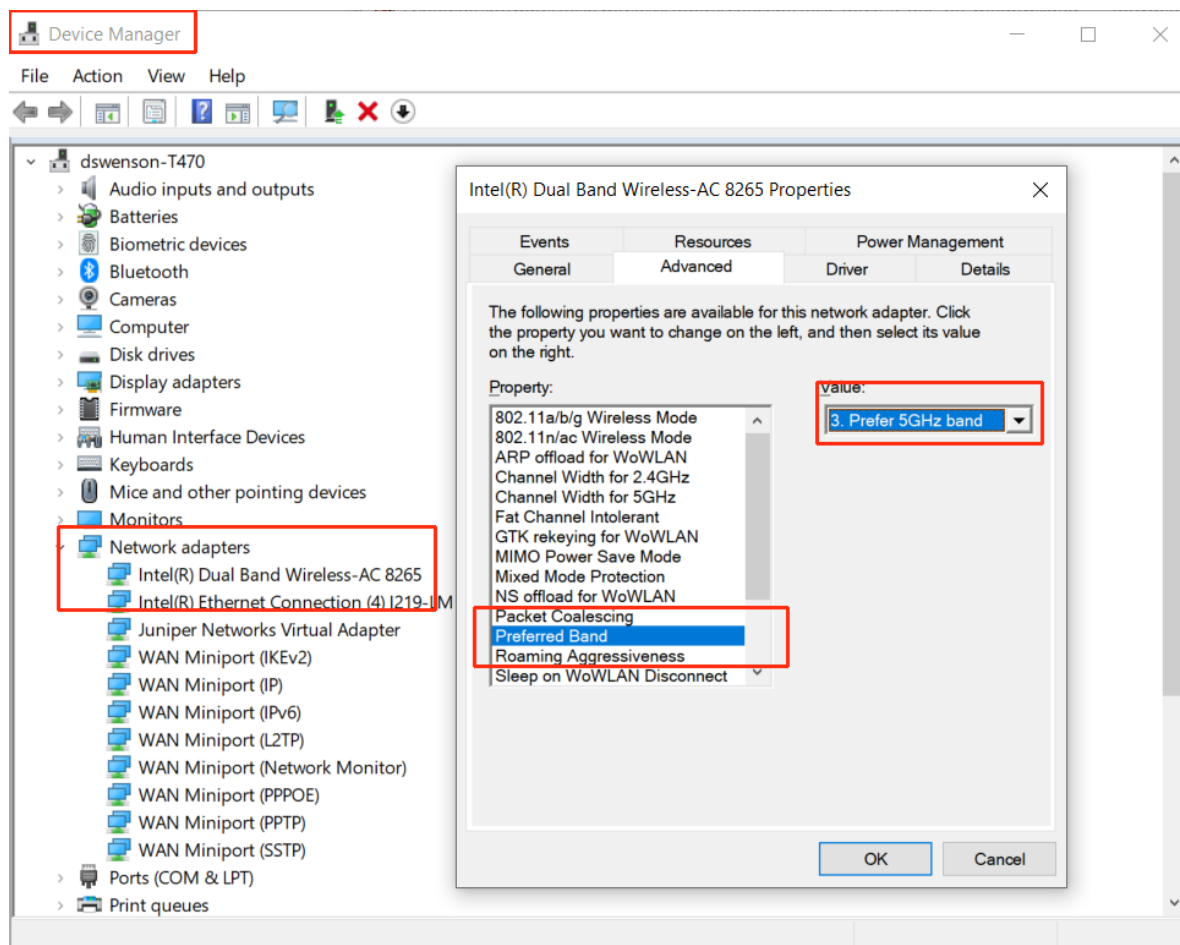
In the Juniper Mist portal, you can see which band your clients are using by clicking **Clients> WiFi Clients** in the menu.

Most Juniper APs support dual band radio setting, which means they can provide both 2.4 GHz and 5 GHz radio connections (see ["Radio Management \(dual-band\)" on page 217](#)). The 5-GHz radio is much faster. Therefore, if you see any clients connecting to the AP on the 2.4-GHz band, or receive user complaints that the Wi-Fi performance is bad, you should check the client device to see if it is statically configured to use the 2.4 GHz band rather than the faster 5-GHz band.

To check or change the radio band preference on Microsoft Windows clients:

1. On the computer of the affected client, right-click the Windows start button and select **Device Manager** from the menu that appears.
2. Double-click **Network adapters** and then in the list that appears, right-click your wireless adapter.
3. Choose **Properties** and then select the **Advanced** tab, as shown.

Figure 35: Have Windows Prefer the 5-GHz Band



4. Select **Preferred Band** from the Property list and set the value to **Prefer 5 GHz band**.
5. Click **OK** and close the various windows.

The Windows client will now connect to the AP using the faster 5-GHz band, unless it is not available.

Bonjour and Bluetooth Devices

Plug-n-play devices, in conjunction with Wi-Fi users' discovering services, can be very chatty and degrade the performance of your wireless network, especially as it grows in scale and spans gateways. To address this issue, you need to first avoid generating multicast Domain Name System (mDNS) frames. You can do that by using Bluetooth® Low Energy (BTLE) rather than Bonjour services to advertise Bonjour devices on a different WLAN or even on a different VLAN (depending on the proximity of those devices).

Using Bluetooth rather than Bonjour works because many Apple TV models and similar devices include the IP address of the Apple TV in their Bluetooth advertisements. Thus supported Apple devices within Bluetooth range of the device (usually about a few thousand square feet) can hear those advertisements and establish an AirPlay session over the Wi-Fi network. The only restriction is that the devices are within Bluetooth range of each other so they can hear the advertisement beacons, and that the beacons are not blocked by a firewall.

In addition to using Bluetooth where possible to avoid creating mDNS traffic, the following best practices can also help limit the amount of packets generated on the Wi-Fi network:

- Pool Bonjour devices into dedicated discovery VLANs.
- Use proximity and role-based discovery policies to limit Bonjour discovery.
- For custom Bonjour applications, test and monitor the service before moving to production.
- ["Add a Bonjour Gateway to a WLAN" on page 132.](#)

LLDP-MED Power Negotiation

Juniper EX Series Switches support both Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED) for sending required DiffServ code point (DSCP) values to connected APs. LLDP is a standards-based protocol for devices to advertise values that include identity, capabilities, and interconnections on IEEE 802 LAN networks. LLDP uses the type-length-value (TLV) format for exchange of information.

Mist supports power negotiation between the LLDP-MED endpoints. The following two power negotiation options are available:

- LLDP Power via MDI TLV IEEE 802.3-2015—Enables advanced power management between LLDP-MED endpoints and network connectivity devices.

- Legacy LLDP Power via MDI TLV IEEE 802.1AB-2009—This is the legacy method.

We recommend LLDP Power through MDI TLV.

See https://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol and https://en.wikipedia.org/wiki/Power_over_Ethernet.

Troubleshoot Your Integration with Aruba ClearPass

SUMMARY

Troubleshoot issues using Aruba ClearPass to handle authentication/authorizations for your network.

IN THIS SECTION

- [Access Tracker | 414](#)
- [Reject Reasons | 415](#)
- [Event Viewer: NAD and Shared Secret Errors | 418](#)

NOTE: This topic provides some tips for troubleshooting in ClearPass. For up-to-date information about ClearPass, see the ClearPass support site.

Access Tracker

In Aruba ClearPass, go to **Monitoring > Access Tracker** and check for authentication failures. Look for authentication requests by using either the username or MAC address, based on the type of authentication that you're using.

If there's no request in the Access Tracker for the MAC Address or username, go to the Event Viewer. See the "[Event Viewer: NAD and Shared Secret Errors](#)" on [page 418](#) section of this topic.

If the MAC Address or username is in the Access Tracker but the Login Status is REJECT, open the request and navigate to the **Alerts** tab to see the reject reason.

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	10.105.5.153	RADIUS	usertest1	Juniper_Dot1X_Servic	ACCEPT	2015/11/24 09:25:48
2.	10.105.5.153	RADIUS	d067e550e3fe	Juniper_MAC_Auth_Ser	ACCEPT	2015/11/24 09:19:22
3.	10.105.5.153	RADIUS	usertest1	Juniper_Dot1X_Servic	ACCEPT	2015/11/24 09:19:04
4.	10.105.5.153	RADIUS	d067e550e3fe	Juniper_MAC_Auth_Ser	ACCEPT	2015/11/24 08:19:22
5.	10.105.5.153	RADIUS	usertest1	Juniper_Dot1X_Servic	ACCEPT	2015/11/24 08:19:03
6.	10.105.5.153	RADIUS	d067e550e3fe	Juniper_MAC_Auth_Ser	ACCEPT	2015/11/24 07:19:22
7.	10.105.5.153	RADIUS	usertest1	Juniper_Dot1X_Servic	ACCEPT	2015/11/24 07:19:03
8.	10.105.5.153	RADIUS	d067e550e3fe	Juniper_MAC_Auth_Ser	ACCEPT	2015/11/24 06:19:22
9.	10.105.5.153	RADIUS	usertest1	Juniper_Dot1X_Servic	ACCEPT	2015/11/24 06:19:03
10.	10.105.5.153	RADIUS	d067e550e3fe	Juniper_MAC_Auth_Ser	ACCEPT	2015/11/24 05:19:22

For help with various reject reasons, see the ["Reject Reasons"](#) on page 415 section of this topic.

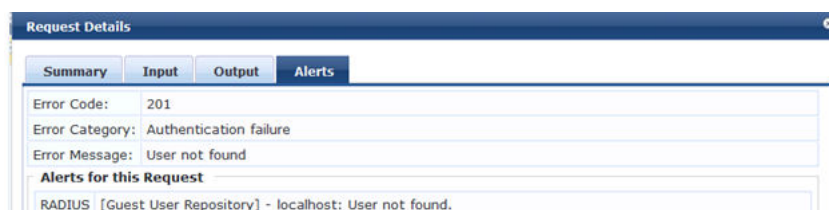
Reject Reasons

The possible reasons for a reject are:

- Service categorization failed—The incoming request on the ClearPass is not categorized under any service that is configured for the SSID that the user is trying to connect to. Make necessary corrections in the service rules under **Configuration > Services** > Select the configured service.



- User not found—This error means that the user is not listed in the configured Authentication Source in the service. See if the appropriate source (Static Host lists, Local User Repository, Guest User Repository, Endpoints Repository, or Active Directory) is added in the service.



Summary	Service	Authentication	Authorization	Roles	Enforcement
<div>Authentication Methods:</div> <div> <div>[Allow All MAC AUTH]</div> <div>Move Up</div> <div>Move Down</div> <div>Remove</div> <div>View Details</div> <div>Modify</div> </div> <div>--Select to Add--</div>					
<div>Authentication Sources:</div> <div> <div>(Guest Device Repository) (Local SQL DB)</div> <div>(Guest User Repository) (Local SQL DB)</div> <div>(Endpoints Repository) (Local SQL DB)</div> <div>(Time Source) (Local SQL DB)</div> <div>Move Up</div> <div>Move Down</div> <div>Remove</div> <div>View Details</div> <div>Modify</div> </div> <div>--Select to Add--</div>					
<div>Strip Username Rules:</div> <div><input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes</div>					

- Cannot select appropriate authentication method—This error appears when the wrong authentication method is added in the service. For MAC authentication, the method should be either [MAC AUTH] or [ALLOW ALL MAC AUTH]. For dot1x, it should be [EAP PEAP], [MSCHAPv2] when username and password are used, [TLS] when certificate based authentication is required, and [PAP] when guest authentication is being performed. Also check the supplicant profile on the client device for dot1x authentications and make sure that it is configured for the correct authentication method and authentication mode.

Request Details	
Summary	Input
Error Code:	201
Error Category:	Authentication failure
Error Message:	User not found
Alerts for this Request	
RADIUS [Guest User Repository] - localhost: User not found. Cannot select appropriate authentication method	
Showing 1 of 1-50 records	
Show Configuration Export Show Logs Close	

Summary	Service	Authentication	Roles	Enforcement
<div>Authentication Methods:</div> <div> <div>[EAP PEAP]</div> <div>[EAP FAST]</div> <div>[EAP TLS]</div> <div>[EAP TTLS]</div> <div>[EAP MSCHAPv2]</div> <div>Move Up</div> <div>Move Down</div> <div>Remove</div> <div>View Details</div> <div>Modify</div> </div>				

- Cannot send request to policy server—This error appears if the policy service is not running on the server. To check the status, go to the CLI and enter the command `service status all`.


```
[appadmin@cplab.clearpassdemo.com]# service status all
Policy server [ cpass-policy-server ] is running
TACACS server [ cpass-tacacs-server ] is running
Radius server [ cpass-radius-server ] is running
Async DB write service [ cpass-dbwrite-server ] is running
DB replication service [ cpass-repl-server ] is running
DB change notification server [ cpass-dbcn-server ] is running
System monitor service [ cpass-sysmon-server ] is running
System auxiliary service [ cpass-system-auxiliary-server ] is running
Admin server [ cpass-admin-server ] is running
Async netd service [ cpass-async-netd ] is running
Multi-master cache [ cpass-multi-master-cache-server ] is running
Domain Server [ cpass-domain-server_LAB ] is running
AirGroup notification service [ airgroup-notify ] is running
Micros Fidelio FIAS [ fias_server ] is running
ClearPass Virtual IP service [ cpass-vip-service ] is running
[appadmin@cplab.clearpassdemo.com]#
```

- Logon failure—This error means that the user provided an incorrect password.

Request Details	
Summary	Alerts
Error Code:	216
Error Category:	Authentication failure
Error Message:	User authentication failed
Alerts for this Request	
RADIUS	MSCHAP: AD status:Logon failure (0xc000006d) MSCHAP: Authentication failed EAP-MSCHAPv2: User authentication failure

- Reading winbind reply failed.

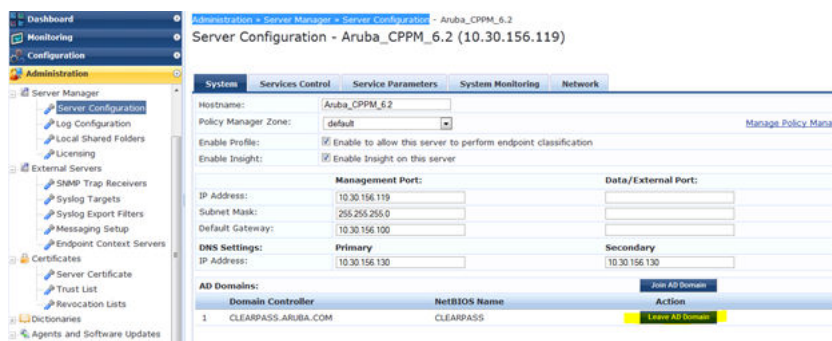
Request Details	
Summary	Alerts
Error Code:	216
Error Category:	Authentication failure
Error Message:	User authentication failed
Alerts for this Request	
RADIUS	MSCHAP: AD status:Reading winbind reply failed! (0xc0000001) MSCHAP: Authentication failed EAP-MSCHAPv2: User authentication failure

Showing 5 of 1-29 records

Show Configuration Export Show Logs Close

This error can be due to two different reasons:

- ClearPass is not added to the AD Domain. Go to **Administration > Server Manager > Server Configuration**, and then select the server.

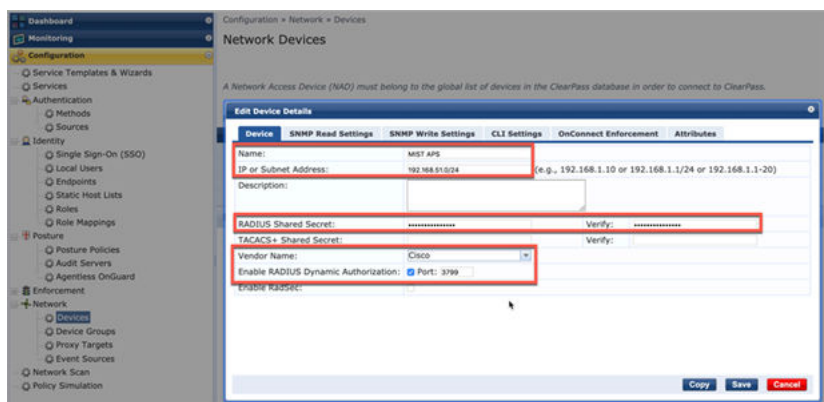


- There is a delay in the response from the AD. This can be verified by clicking the **Show Logs** button on the Access Tracker request. The delay should be less than 500 ms. Check on the AD side to see why there is a delay in sending the response.

Event Viewer: NAD and Shared Secret Errors

If there is no request in the Access Tracker for the MAC or username, navigate to the Event Viewer and look for any events in the Authentication category. If so, open the errors and investigate further.

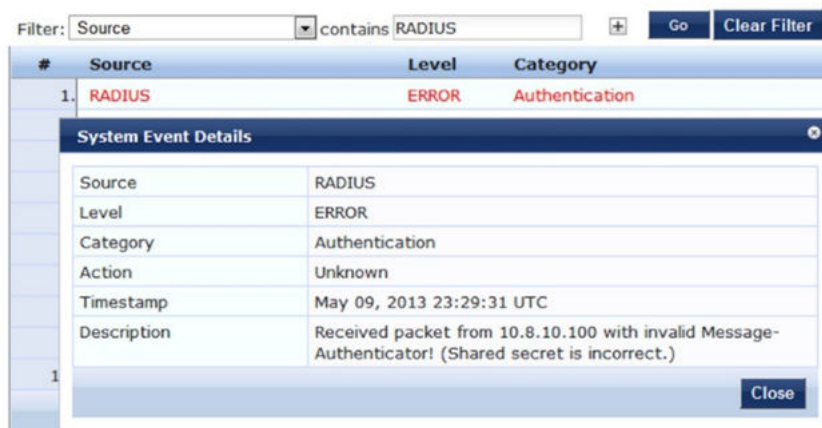
- Request from Unknown NAD—For this error, navigate to **Configuration > Network > Devices** and check if the IP address/subnet or IP range for the APs is added and the correct vendor is selected. Make corrections as needed.



- Shared secret is incorrect—Make sure that the correct shared secret is configured on both the AP and the server.

Monitoring » Event Viewer

Event Viewer



If there are no events in the Event Viewer, check the reachability from the AP to the RADIUS server.

Use Labels to Identify "Unknown" Applications

Juniper Mist™ uses DNS query responses to help populate the Application section of the Insights page. The Application section shows some pre-defined applications as Unknown. This means that Juniper Mist could not categorize or identify this network traffic.

App name	Total Bytes	Percent Bytes	Number of clients	RX Bytes	TX Bytes
Unknown	20.1 GB	50%	22	11.9 GB	8.2 GB
CNN	17.7 GB	44%	2	17.5 GB	223.9 MB
Yahoo	2.2 GB	6%	2	2.1 GB	62.8 MB
Juniper VPN	722.4 MB	2%	3	444.1 MB	278.3 MB
Apple	106.1 MB	1%	7	103.1 MB	3 MB
Amazon	51.2 MB	1%	1	50.6 MB	557.4 kB
Google	35.3 MB	1%	4	34.9 MB	401.3 kB

NOTE: To see the complete list of pre-defined applications, go to `/api/v1/sites/:site_id/wxtags/apps`

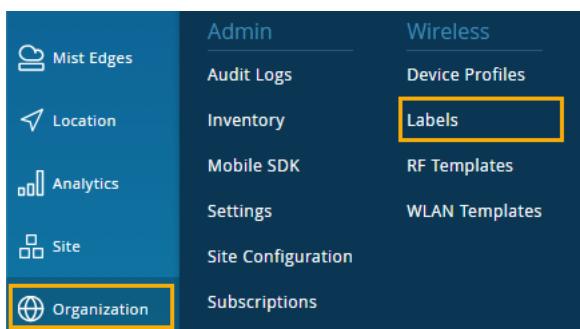
If you want to track any of these applications, you can use labels to identify them. You can configure labels at the organization level or the site level.

NOTE: There is a traffic threshold for applications on the Insights page. Applications appear only if they are responsible for traffic totalling 200KB or more.

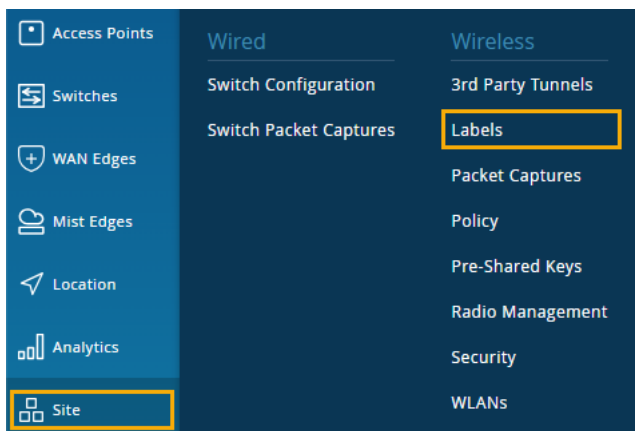
To configure labels for "unknown" applications:

1. Navigate to the Labels page for your organization or site:

- For organization-level labels, select **Organization** > **Wireless** | **Labels** from the left menu of the Juniper Mist portal.



- For site-level labels, select **Site** > **Wireless** | **Labels** from the left menu of the Juniper Mist portal.



2. Click **Add Label** at the top-right corner of the Labels page.

3. Enter the information:

- Label Name—The name that you want to use to identify this application.
- Label Type—Select **Hostname**.
- List of Hostnames—Enter the hostnames whose traffic you want identify with this label.

In this example, traffic from abcnews.go.com will be labeled as abcnews.go.com.

← Site Labels : abcnews.go.com

Label Name

Label Type

Hostname

Label Values • IS

List of Hostnames (wikipedia.org, example.com:8080)

4. Click **Create**, near the top-right corner of the New Label page.

9

CHAPTER

Technology Reference

[Wireless Network Design Tutorial](#) | 423

[Wi-Fi 6 \(802.11ax\) Technology](#) | 423

[Considerations for 6 GHz Wireless](#) | 425

Wireless Network Design Tutorial

To learn how to best design your wireless network, Juniper Mist™ provides a series of videos that walks you through the entire wireless LAN (WLAN) design process. This series includes industry best practices as well as a structured design framework and tested methodologies. Following these design best practices ensures an exceptional user experience on your network.

To begin learning the wireless design process, see [Mist AI Wireless Network Design](#).



Wi-Fi 6 (802.11ax) Technology

IN THIS SECTION

- [Wi-Fi 6 \(802.11ax\) at a Glance](#) | 424

The latest Wi-Fi standard is Wi-Fi 6 (also technically referred to as IEEE 802.11ax), ushers in a new era for wireless communication. The focus of Wi-Fi 6 is on optimizing efficiency and capacity rather than

boosting maximum throughput alone. It is gaining momentum as the future of Wi-Fi technology. For a quick dive into why you should consider Wi-Fi 6 for your network, check out the following video.



Video:

Wi-Fi 6 (802.11ax) at a Glance

Adopting Wi-Fi 6 brings significant improvements for your network capacity, efficiency, and device battery life. Here's what sets Wi-Fi 6 apart:

- **OFDMA**—Orthogonal Frequency-Division Multiple Access (OFDMA) is a critical feature of Wi-Fi 6 that increases efficiency. It divides a wireless channel into a large number of smaller subchannels, each of which carries data intended for a different endpoint. This technique allows the simultaneous transmission of data to multiple clients, reduction in latency, and improvement of bandwidth usage.
- **BSS Coloring**—Basic Service Set (BSS) coloring is a method to improve handling of overlapping BSSs in dense Wi-Fi environments. It assigns different identifiers (colors) to each BSS. This allows access points (APs) and clients to distinguish and ignore transmissions from other BSSs, enhancing overall network efficiency.
- **1024 QAM**—Quadrature Amplitude Modulation (QAM) has been enhanced from the previous Wi-Fi standard of 256 QAM to 1024 QAM with Wi-Fi 6. 1024 QAM allows each signal to carry more data, which improves the overall throughput. However, enabling it requires a higher Signal-to-Noise Ratio (SNR) and might slightly reduce the range.
- **Uplink MU-MIMO**—Wi-Fi 6 introduces Uplink Multi-User Multiple Input Multiple Output (MU-MIMO). While previous Wi-Fi standards allowed simultaneous data transmissions from an AP to multiple clients, Wi-Fi 6 improves this by also supporting simultaneous transmissions from multiple clients to the AP.
- **Target Wake Time**—This feature extends device battery life by scheduling predetermined times for devices to wake up and receive data, allowing them to remain idle (to conserve battery) for longer periods of time.

A migration to Wi-Fi 6 offers considerable enhancements to your network's capacity, efficiency, and the battery life of connected devices.

RELATED DOCUMENTATION

[Overview of Juniper Mist Wireless Assurance | 2](#)

[Hardware for Your Wireless Network | 5](#)

Considerations for 6 GHz Wireless

IN THIS SECTION

- [Spectrum Availability | 425](#)
- [Security | 426](#)
- [Transition Modes | 427](#)
- [Roaming Between Security Types | 428](#)
- [Client Provisioning Considerations | 429](#)
- [RF Design | 430](#)
- [Preferred Scan Channels \(PSCs\) | 432](#)
- [PoE Requirements | 433](#)
- [Multigigabit Considerations | 433](#)

When deploying Wi-Fi 6E, there are practical considerations to keep in mind to ensure successful implementation. This document provides guidance specifically for deploying Wi-Fi 6E using Mist, and focuses on the necessary steps, configurations, and best practices.

Spectrum Availability

Wi-Fi 6E operates in the 6-GHz frequency band, offering increased bandwidth and reduced interference compared to previous Wi-Fi standards. Before deploying Wi-Fi 6E, it is crucial to verify spectrum availability in your region and ensure that you're complying with regulatory requirements.

Configure your wireless LAN (WLAN) to utilize both the 5-GHz and 6-GHz bands. Doing this will ensure that clients can fall back to the 5-GHz band in case of a connection issue on the 6-GHz band.

Security

Use of Wi-Fi Protected Access 3 (WPA3) security or Opportunistic Wireless Encryption (OWE) is mandatory for Wi-Fi 6E deployments. We recommend that you understand the devices and driver versions of the devices on your network before deciding which security type best fits the needs of your environment.

NOTE: In Mist, the 6-GHz band needs to be explicitly enabled on each Wireless LAN (WLAN). It is not enabled on existing WLANs, and is not enabled by default on new WLANs.

Edit WLAN

SSID
test_corp

WLAN ID
774795b1-182c-4825-825a-d1e51fb4742e

WiFi SLE
☐ Exclude this WLAN from WiFi SLEs (except AP Health SLE)

WLAN Status
☒ Enabled ☐ Disabled
☐ Hide SSID
☐ Broadcast AP name

Radio Band
☐ 2.4 GHz ☒ 5 GHz ☒ 6 GHz

Client Inactivity
Drop inactive clients after seconds: 1800

Geofence
☐ Minimum client RSSI (2.4G) 0
☐ Minimum client RSSI (5G) 0
☐ Minimum client RSSI (6G) 0
 Block clients having RSSI below the minimum

Data Rates
☐ Compatible (allow all connections)

Security ❗ Only WPA3 and OWE WLANs are allowed in 6 GHz
❗ WPA3/EAP* requires firmware v0.9.x or higher

Security Type
☒ WPA3 ☐ OWE
☒ Enterprise (802.1X) ☐ Personal (SAE)

☐ Enable WPA3+WPA2 Transition
☐ Enable 192-bit Encryption
☐ MAC address authentication by RADIUS lookup
☐ Use EAPOL v1 (for legacy clients)
☐ Enable EAP-Reauth
☐ Prevent banned clients from associating
 Edit banned clients in [Network Security Page](#)

Fast Roaming
☒ Default
☐ Opportunistic Key Caching (OKC)
☐ .11r

802.1X Web Redirect
 Allow 802.1X Web Redirect for quarantine or posture assessment based on RADIUS server response containing url-redirect AVP
☐ Enabled ☒ Disabled

Hotspot 2.0
☐ Enabled ☒ Disabled

Buttons: Delete Save Cancel

Consider the following points before deciding which security type best fits the needs of your environment:

- **WPA3-Enterprise**—This security type is easy to adopt. It is very similar to WPA2-Enterprise, so it is usually low-risk to adopt WPA3-Enterprise.
- **WPA3-Personal**—Adopting this security type is fairly low-risk when modern devices are involved. You might run into interoperability issues with older devices, in which case, it is best to go with an SSID with WPA2-Personal configured so that older devices can connect to the network without any issue. Built-in downgrade protections prevent roaming back to WPA2. WPA3-Personal is also known as Simultaneous Authentication of Equals (SAE).

In 6-GHz, Hash-to-Element (H2E) is mandatory to mitigate some of the early vulnerabilities found with WPA3-Personal. With H2E, the password undergoes hashing and serves as an element (Password Element [PWE]) in establishing connectivity.

- **Opportunistic Wireless Encryption (OWE)**—This security type has the most recent device support. It is common to deploy OWE Transition for maximum compatibility.

For guest networks, device support of OWE is fairly new; so you will likely need to use OWE Transition if you want to have your guest network on the 6-GHz band.

Transition Modes

Transition modes can help ease adoption to WPA3 or OWE. Transition modes delay the migration to WPA3 by continuing to offer existing security types.

- **WPA3-Enterprise Transition**—This is mostly made up of WPA2-Enterprise and Protected Management Frames (PMF). When you enable WPA3-Enterprise Transition, the same Authentication and Key Management (AKM) (5) is used, but PMF is changed from mandatory to capable. Legacy AKM 1 is dropped with WPA3-Enterprise Transition. Device support of PMF is positive.

Customer feedback has been generally positive around enabling both WPA3-Enterprise and WPA3-Enterprise Transition. This will vary based on the devices and device drivers in your network.

- **WPA3-Personal Transition**—The preshared key (PSK) and Simultaneous Authentication of Equals (SAE) AKMs are advertised.

Older devices (such as Android 9 and older as well as Microsoft Surface devices with Marvell chipsets) have had trouble connecting to WPA3-Personal Transition networks. Therefore, it's important to understand the variety of devices on your networks. You might want to consider using an SSID with WPA2-Personal configured on the 2.4 and 5-GHz bands to support older devices.

- **OWE Transition**—You will need to deploy OWE Transition if you would like to enable your “open” or guest networks on the 6-GHz band. Otherwise, keep these networks on the 2.4 or 5-GHz bands.

OWE Transition creates a second “hidden” SSID. The open network continues to broadcast, and a new information element is added to the beacon to indicate the presence of an OWE SSID, which is broadcast as hidden.

In Mist, when you configure OWE Transition, it automatically creates the hidden OWE SSID, and appends **-OWE** to the end of the SSID name.

NOTE: Mist allows you to configure WPA3 and OWE Transition modes on 6-GHz multiband SSIDs, to ensure easier adoption of transition mode SSIDs. This eliminates the need to create two separate SSIDs, which would break fast roaming if enabled, and would display as two SSIDs with potentially the same name in the UI.

Roaming Between Security Types

In environments with varying device types and device versions, it is important to understand device behavior when roaming between different security types. The following observations have been found in our testing:

BSS1	BSS2	Result
Open	OWE	Fail
OWE Transition	OWE	Fail
WPA2 Personal	WPA3 Personal	Fail
WPA3 Personal Transition	WPA3 Personal	Works if the client is connected via WPA3 on BSS1
WPA2 Enterprise	WPA3 Enterprise	Works both ways
WPA3 Enterprise Transition	WPA3 Enterprise	Works both ways

Table 34: Client Device Support of WPA3 and OWE

WPA3	OWE
<p>Android</p> <ul style="list-style-type: none"> • Version 10 and above 	<p>Android</p> <ul style="list-style-type: none"> • Version 10 and above

Table 34: Client Device Support of WPA3 and OWE (Continued)

WPA3	OWE
Apple (iPhone 6, 2013+ MacBook (802.11ac), iPad 5) <ul style="list-style-type: none"> • iOS 13 and above • MacOS Catalina and above 	Apple (iPhone SE, iPhone 12, iPad mini 6th gen, iPad Air 4th gen, iPad Pro 11 3rd gen, iPad Pro 12 5th gen, Apple Silicon Macs) <ul style="list-style-type: none"> • iOS 16, iPadOS 16.1 and above • MacOS 13 and above
Windows <ul style="list-style-type: none"> • WPA3 Enterprise – Windows 10 (2004) <ul style="list-style-type: none"> • For Intel NICs: 9260 or newer and driver 21.90.3.X or later • WPA3 Personal – Windows 10 (1903) <ul style="list-style-type: none"> • For Intel NICs 9260 or newer and driver 21.10.X or later • H2E Supported on Windows 10 21H2 or Windows 11 <ul style="list-style-type: none"> • W10 Intel Driver = 22.70.x or Later, W11 Intel Driver = 22.100.x or Later 	Windows <ul style="list-style-type: none"> • Windows 10 (2004) <ul style="list-style-type: none"> • For Intel NICs: 9260 or newer and driver 21.90.3.X or later
ChromeOS <ul style="list-style-type: none"> • Support added in 2020 	ChromeOS <ul style="list-style-type: none"> • Not Supported

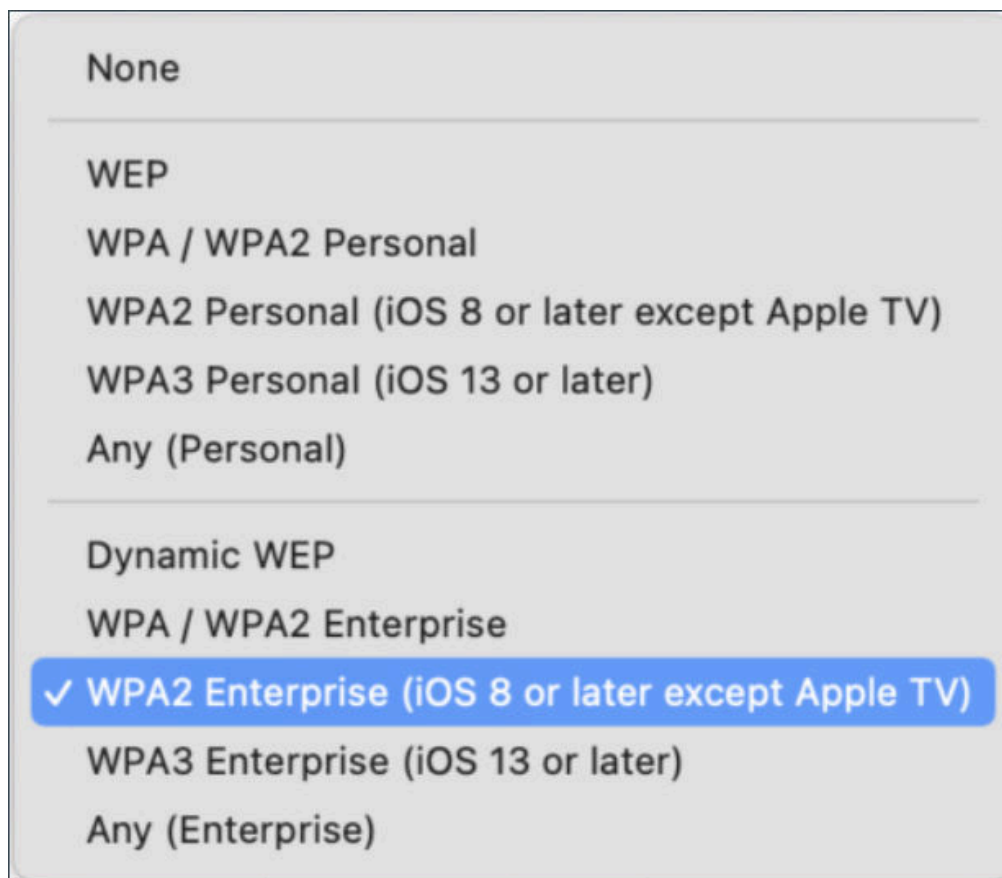
The information in the table above was derived from the intel.com and apple.com support websites.

Client Provisioning Considerations

In larger environments, it's often necessary to rely upon provisioning tools such as MDM, group policy, or other tools which can push configuration profiles to devices. With these tools, you can pre-configure SSIDs, install certificates, and so on. Keep in mind that in the SSID profiles, you need to define the security type.

For secure Enterprise networks, you can define **WPA2-Enterprise** as the security type. This generally enables the device to connect to WPA3-Enterprise networks as well, if the device supports it. On the other hand, if you configure a higher security level and the device does not support it, the profile may fail to install.

The following depicts selecting the **WPA2 Enterprise** security type from Apple Configurator:

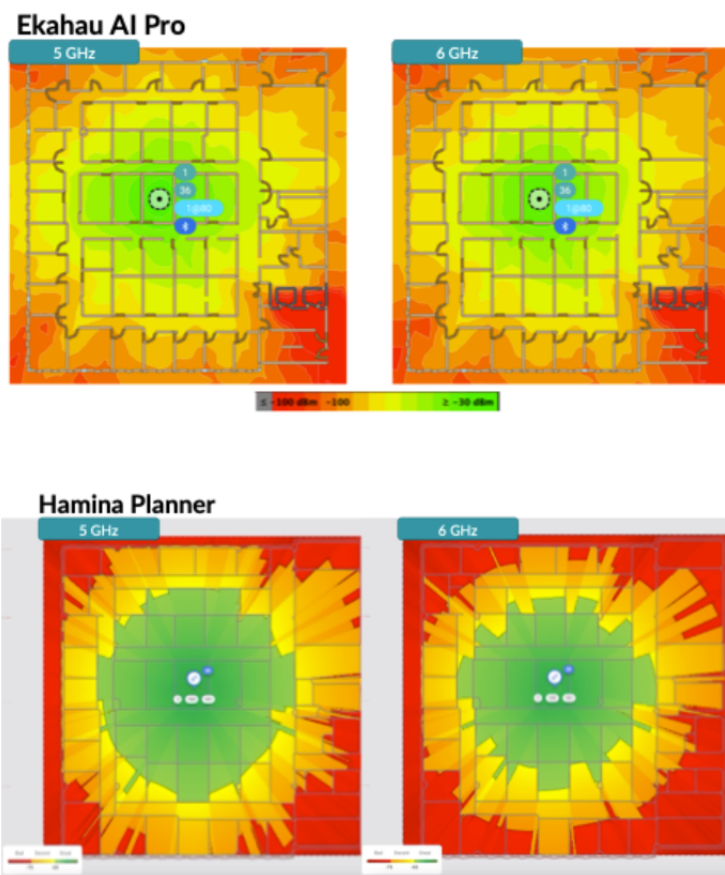


RF Design

Juniper Mist's testing reveals that the biggest difference between 5 GHz and 6 GHz, from a design perspective, is driven from reduced 6-GHz client transmission power. From a free space path loss (FSPL) perspective, 5 GHz and 6 GHz have a 1–2 dB difference depending on which frequencies you are comparing. The difference is that 5 GHz and 6 GHz might attenuate differently through different material types. There may also be max Access Point (AP) Transmission power differences, especially with Low Power Indoor mode (LPI).

6 GHz requires a slightly higher AP density than 5 GHz. We recommend a proper RF design for 6 GHz. However, in some environments this might not be feasible. If you already have capacity based on 5-GHz

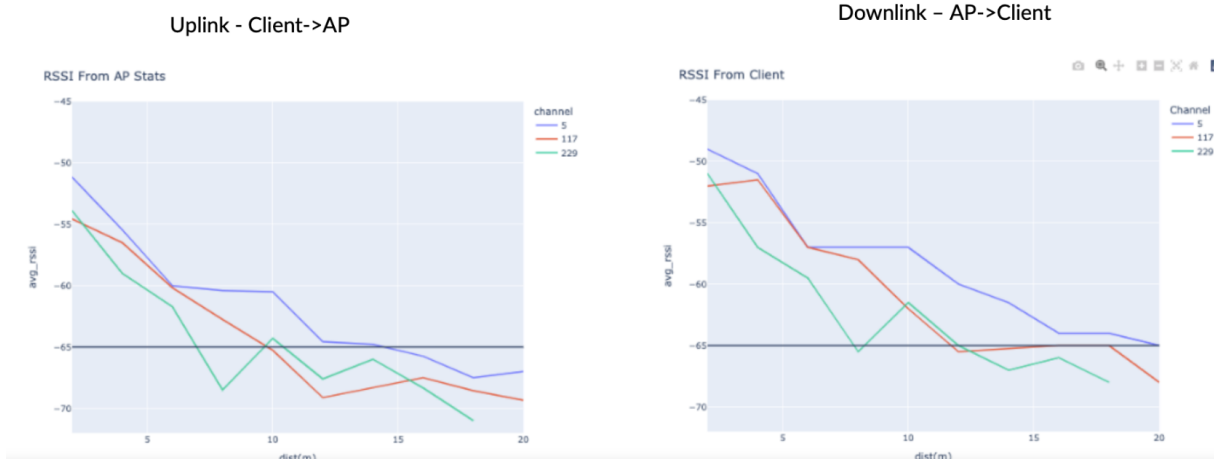
designs, you may not need to change much from a density perspective. Based on the material of your walls, you might find it necessary to add an AP specifically to a conference room where you previously did not have one for 5 GHz. If you look in any of the popular planning tools, you'll notice similar coverage between 5 GHz and 6 GHz.



Client transmission power is limited depending on the regulatory domain.

- In real world tests, we see between 3-10 dB of difference between 5 GHz and 6 GHz.
- In the United States, clients are limited to -1 dBm/MHz.

RSSI vs Frequency 6 GHz



Preferred Scan Channels (PSCs)

Out of the box, Mist defaults to 80 MHz in the 6-GHz band.

80 MHz is recommended because it allows for a higher maximum equivalent isotropic radiated power (EIRP) and it lines up with Primary Scan Channels (PSCs), which clients have an easier time discovering.

Utilize non-PSCs in environments where you may want to utilize 20 or 40 MHz channel bandwidth, such as in Europe with only 500 MHz of spectrum, or in high density environments.

After testing the major client operating systems, the use of non-PSCs as the primary channel is generally OK. Our testing has also shown that Windows, Android, iOS, and MacOS clients connect to APs using non-PSCs and leverage out-of-band discovery mechanisms such as reduced neighbor reports or 802.11k neighbor reports.

In environments where you might need narrow channels, configure your WLAN to utilize both the 5-GHz and 6-GHz bands. This provides the added benefit that if there is ever a 6-GHz discovery issue, clients can fall back to the 5-GHz band.

Mist Radio Resource Management (RRM) uses PSCs by default. When **Automatic** is selected for channels, PSCs will be used as the primary channel. When **Set allowable channels** is selected, whichever channels are selected will be used as primary channels.

For most environments, the **minimum power** for 6 GHz can be kept the same as 5 GHz. For **maximum power**, you generally do not need to restrict the maximum for 6 GHz.

Channels

☐ Automatic
☒ Set allowable channels

Select All | Clear

<input type="checkbox"/> 1	<input type="checkbox"/> 5 (psc)	<input type="checkbox"/> 9	<input type="checkbox"/> 13
<input type="checkbox"/> 17	<input type="checkbox"/> 21 (psc)	<input type="checkbox"/> 25	<input type="checkbox"/> 29
<input type="checkbox"/> 33	<input type="checkbox"/> 37 (psc)	<input type="checkbox"/> 41	<input type="checkbox"/> 45
<input type="checkbox"/> 49	<input type="checkbox"/> 53 (psc)	<input type="checkbox"/> 57	<input type="checkbox"/> 61
<input type="checkbox"/> 65	<input type="checkbox"/> 69 (psc)	<input type="checkbox"/> 73	<input type="checkbox"/> 77
<input type="checkbox"/> 81	<input type="checkbox"/> 85 (psc)	<input type="checkbox"/> 89	<input type="checkbox"/> 93
<input type="checkbox"/> 97	<input type="checkbox"/> 101 (psc)	<input type="checkbox"/> 105	<input type="checkbox"/> 109
<input type="checkbox"/> 113	<input type="checkbox"/> 117 (psc)	<input type="checkbox"/> 121	<input type="checkbox"/> 125
<input type="checkbox"/> 129	<input type="checkbox"/> 133 (psc)	<input type="checkbox"/> 137	<input type="checkbox"/> 141
<input type="checkbox"/> 145	<input type="checkbox"/> 149 (psc)	<input type="checkbox"/> 153	<input type="checkbox"/> 157
<input type="checkbox"/> 161	<input type="checkbox"/> 165 (psc)	<input type="checkbox"/> 169	<input type="checkbox"/> 173
<input type="checkbox"/> 177	<input type="checkbox"/> 181 (psc)	<input type="checkbox"/> 185	<input type="checkbox"/> 189
<input type="checkbox"/> 193	<input type="checkbox"/> 197 (psc)	<input type="checkbox"/> 201	<input type="checkbox"/> 205
<input type="checkbox"/> 209	<input type="checkbox"/> 213 (psc)	<input type="checkbox"/> 217	<input type="checkbox"/> 221

PoE Requirements

For Power over Ethernet (PoE), Mist Wi-Fi 6E APs need a minimum of 802.3at power, but 802.3bt is the general recommendation. For details about the power requirements, see ["PoE Requirements for Juniper Mist APs" on page 21](#).

Multigigabit Considerations

With Wi-Fi 6E, there are real-world situations where you could see more than 1 gigabit per second (Gbps) on a single AP. For these situations, Juniper Mist offers select switches that offer Multigigabit (mGig) speeds for Wi-Fi 6E APs. So, do you need 1 gigabit (Gb) or multigigabit for Wi-Fi 6E APs?

- Generally speaking, you need at least 100 MHz of spectrum to exceed 1 Gbps of throughput.
- With three data radio triband APs, you could have 120-140 MHz of spectrum used by a single AP.

- Select Juniper Switches offer mGig speeds of 2.5 Gigabit Ethernet (GbE), which is necessary for Wi-Fi 6E deployments that surpass 1 Gbps throughput.

