JUNIPER NETWORKS | Engineering Simplicity

Juniper Mist Wireless Assurance Configuration Guide

Published
2026-01-06

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

Juniper Mist Wireless Assurance Configuration Guide

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

1

CHAPTER

Get Started

IN THIS CHAPTER

Juniper Mist™ makes it easy to get started with your wireless network. This chapter provides an introduction to Juniper Mist Wi-Fi Assurance, along with information and links to help you select your hardware, deploy your access points, and start configuring your wireless network.

NOTE: Start setting up your wireless network *after* setting up your Juniper Mist organization and sites (as described in the Juniper Mist Management Guide).

Overview of Juniper Mist Wi-Fi Assurance

SUMMARY

Juniper Mist™ Wi-Fi Assurance is a cloud service based on machine learning (ML) and driven by Mist AI™. It replaces manual troubleshooting tasks with automated wireless operations to make Wi-Fi predictable, reliable, and measurable. Juniper Mist Wi-Fi Assurance provides network administrators full visibility into the user experience on their wireless networks.

IN THIS SECTION

Video: Wi-Fi with Assurance

Juniper Mist™ Wi-Fi Assurance helps you keep the focus on your users' network experience, with built-in machine-learning (ML) features that tune the network for the best possible user experience. Network administrators can set service thresholds for time to connect, wireless coverage, throughput, and more. When user experience doesn't match these service-level expectations (SLEs), Juniper Mist tells you why. When problems arise, our AI-driven virtual network assistant, Marvis, shows you the root cause and often suggests action to fix the problem.

Juniper Mist Wi-Fi Assurance includes access points (APs), Mist Edges, wireless LANs (WLANs), radio management, security, network segmentation, and a lot of automation.

Scalable Cloud-Based Architecture

The Juniper Mist platform is built on a modern microservices cloud architecture, which offers the scalability to meet your network needs. The architecture supports multitenancy and scales with the elasticity of the cloud. Thus, a managed service provider (MSP) can operate wireless sites and networks for dozens of client organizations. A large retailer can accommodate various site-specific requirements yet manage the organization centrally, with a single login per cloud. Other features and benefits include:

- **Microservices**—The Juniper Mist cloud is built on a microservices architecture that brings agility and scale to network management and operations. On-demand network upgrades and patches take minutes instead of months. Services are designed independently of one another. These features lay the foundation for a flexible, scalable, resilient, programmable, and agile network. See What Is a Cloud Microservice for more information.
- **Programmability through open APIs**—Juniper Mist is 100% programmable with all functions available through open APIs. Every task you can perform in the Mist GUI you can perform through an API call. For a complete, searchable list of APIs that you can try out for yourself, see the Mist API Reference.
- **Controllerless management**—Wi-Fi assurance runs in the cloud. You don't have any on-premises controllers to install or manage, so your network scales easily.
- **Centralized data path**—When an organization needs to retain a centralized data path architecture for security in campus or branch deployments, the Juniper Mist Edge solution provides that data path. The use of the centralized data path enables Juniper Mist to operate like a controller-based solution, in that the on-site data paths are secure. The tunneling functions of Juniper Mist Edges let Juniper Mist keep control and management functions securely in the Juniper Mist cloud.
- **Performance optimization and regulatory compliance**—To comply with data residency regulations and optimize performance, we deploy Juniper Mist cloud instances worldwide. Server locations include Europe, Asia, and Australia. In the United States of America (USA), we have servers on the east and west coasts as well as a USA federal cloud.

Video: Cloud-Based Architecture

Centralized Configuration and Operations

The Juniper Mist portal is entirely API driven and provides configuration options for every aspect of your wireless network. You can perform a wide range of tasks on the Juniper Mist portal:

- Create users
- Define and apply policies

- Define and apply WLAN templates to your sites
- Define and apply device profiles that can override template settings
- Set up sites within your organization
- Investigate and solve problems with the help of AI

With APIs behind every function, you can programmatically control every aspect of your network. If you are GUI-minded, you can use the Juniper Mist portal. For the automation experts and application integrators, there's the Mist API Reference.

Templates and Device Profiles

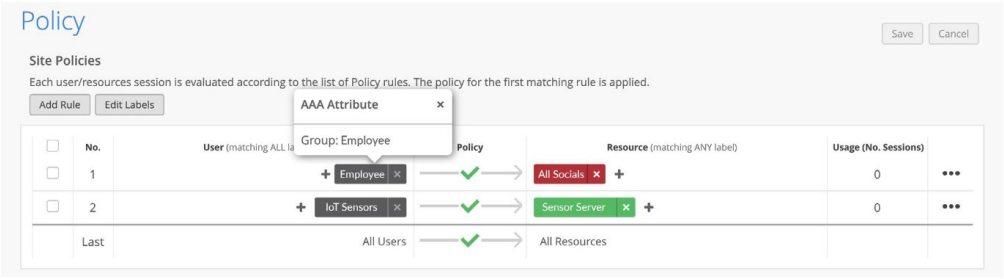
In the Juniper Mist portal, you'll often find that you can make the same configuration settings in different places. For example, you can configure radio resource management (RRM) and other radio settings directly on the Juniper access points (APs), in a device profile, or an RF template. The modular design makes it easy to scale configurations across different AP groupings or quickly assemble any combination of APs, WLANs, access policies, and radio frequency (RF) configurations.

NOTE: We recommend that you use templates, device profiles, and other group configuration options to simplify the management of your devices and networks in the Juniper Mist portal. Using these configuration aids prevents direct device or network configuration, which can be error-prone and difficult to track.

For details, see: "Configure a WLAN Template" on page 231 and "RRM Configuration Options" on page 351.

WxLAN Policies

The Wireless extensible LAN (WxLAN) policies in Juniper Mist allow you to define organization and site-level labels. You can apply these labels to many types of objects, including users, WLANs, APs, IP addresses, IP subnets, applications, and so on. You can easily apply WxLAN policies to endpoints, regardless of their authentication or authorization method. With labeling and visual policy design, you replace multiple lines of CLI syntax with easy-to-read graphic policy displays.



As shown in the image above, WxLAN policies allow for granular configuration of the rules within the policy. Juniper Mist processes the rules from the top down. Juniper Mist applies the first rule that matches the traffic and does not process any more rules. See "WxLAN Access Policies" on page 220 for more details.

Flexible and Secure Guest Wi-Fi Access

Guest access is an important consideration for any enterprise WLAN. Juniper Mist provides options to customize your WLAN for guest access, including:

- **Scalable guest access solution**—Your guest access solution can incorporate flexible options including multiple language support, customizable branding, social login, external captive portal integration, and RADIUS integration. See "WLAN Guest Portal" on page 285.
- **WLAN segmentation**—Segment your guest WLAN by using multiple preshared keys (PSKs) and making each PSK a personal WLAN. There's no connectivity between devices with different PSKs.
- **Guest traffic**—You can locally bridge guest traffic, tie it to a dedicated guest Ethernet port, or tunnel it to a centralized concentrator from your APs.

See "Compare WLAN Guest Portal Options" on page 286 for more details.

Proactive Optimization of Wireless Performance

Juniper Mist-managed WLANs undergo periodic optimization as part of our radio resource management (RRM) implementation. Juniper Mist uses a once-daily RRM optimization based on machine learning (ML) data and applies this optimization to all access points (APs) in a site. You can also trigger individual frequency band optimization at any time, or when you make changes to certain settings.

Juniper Mist offers the following services to improve wireless performance:

- **Customizable wireless service levels**—You can set and monitor service-level expectation (SLE) metrics for key performance areas. Juniper Mist gathers these metrics from all client devices. The SLEs

determine what constitutes success in your network, including connection times, throughput, and more. The Wireless Capacity SLE plays a key role in the RRM optimizations mentioned above. See "Wireless SLEs" on page 375.

- **AI-driven RRM**—Juniper Mist applies data science and reinforcement learning strategies to the aggregate SLE performance data to:
  - Optimize radio settings.
  - Assure network performance.
  - Adapt to radio interference.
  - Respond to environmental issues.

  Juniper Mist applies the previous actions, as appropriate, to all sites within your organization.

  For more information, see "Radio Management" on page 342.

- **Marvis Virtual Network Assistant (VNA)**—The Marvis VNA proactively identifies issues, interprets the scope and magnitude of the impact, identifies the root causes, and recommends fixes. In some cases, Marvis can take action to correct issues without your intervention.

- **Marvis Minis**—Marvis Minis are network digital twins that validate network and application services for your network even when no clients are connected to the network. Marvis Minis detect issues and assess the impact of those issues. So, they'll tell you if the problem impacts a switch, an AP, a WLAN, or a server.

- **Digital transformation with network insights**—The Juniper Mist Wi-Fi Assurance cloud service includes base capabilities for analyzing up to 7 days of data, simplifying the process of extracting network insights from data across your enterprise.

Wireless Service-Level Expectations

Juniper Mist service-level expectations (SLEs) help you understand a user's wireless network experience. Here's the typical SLE workflow:

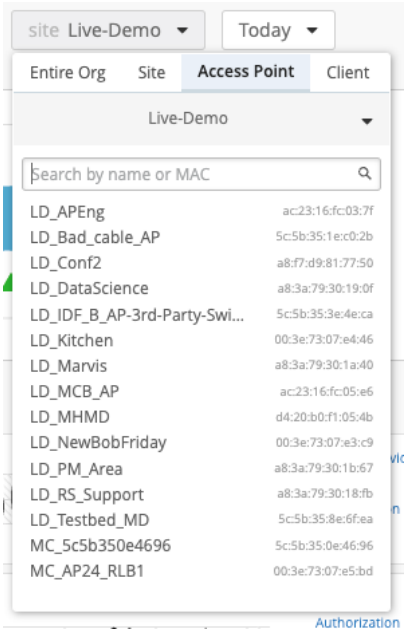
1. Juniper access points (APs) collect key data about every user's wireless experience and upload it to the Juniper Mist cloud.
2. The Juniper Mist portal normalizes the data to a user-minute metric.
3. Juniper Mist applies machine learning (ML) to create measurable, actionable information about successful connections, time to connect, wireless throughput, and more.

This process helps determine whether the user experience was good or bad during the last user minute. And, if it was bad, it identifies the SLE that was not met."

At any time, you can see how your network is performing against the wireless SLEs with deep visibility into impacted users, applications, and devices. From the various Juniper Mist dashboards, you can visualize this information across the entire organization, individual sites, or even individual clients.

From the dashboard, you can visualize the data for the entire organization, individual sites, or even individual clients.

As you can see in the preceding image, the filter is currently set to show Wireless SLE metrics for today on the Live Demo site. You can also configure the scope of the visualization for a single site, an entire organization, and specific APs or clients as shown below.



For more information, see "Wireless SLEs" on page 375.

Troubleshooting

When questions or problems arise, Juniper Mist provides you with the following automated tools that help answer your questions or solve your problems.

- **Dynamic packet capture**—The Juniper Mist Wi-Fi Assurance cloud service automatically starts capturing packets when it detects specific anomalies. Juniper Mist captures more than 150 state changes for each client device and access point every few seconds. With this record, you can rewind in time to see what, exactly, was going on when the event occurred. This eliminates hours of guesswork or time spent trying to reproduce an issue. See "Dynamic and Manual Packet Captures" on page 425 for more information.

- **Marvis Actions**—Use the predictive recommendations and automated workflows in Marvis Actions to quickly solve problems or prevent them from occurring.

- **Root-cause identification**—Using data science and machine learning, the Proactive Analytics and Correlation Engine (PACE) aids in the root-cause identification of problems so you can quickly identify and fix them.

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 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	Before you can configure your wireless network or onboard your devices, you need to complete these tasks in the Juniper Mist™ portal: • Create your organization. • Set up at least one site, and activate your subscriptions. • Configure your firewall to allow outbound Juniper Mist traffic. Recommended, but not required before you can configure your wireless network: • 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.	• Juniper Mist Quick Start • Firewall Configuration: Juniper Mist IP Addresses and Ports • Security Options
Device Installation	Claim your devices into your organization.	• 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	Set up your WLAN templates and WLANs. Configure settings such as security, radio frequency, rate limits, QoS, and more. 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.	• "Configure a WLAN Template" on page 231 • "Adding a WLAN" on page 234 • "WLAN Options" on page 235
RF Templates and Device Profiles	If you have multiple sites and device types, you can use RF templates and device profiles to streamline configuration and deployment. By doing so, you ensure consistent settings across sites. As with WLAN templates, Juniper Mist applies any changes across all associated sites and devices.	"RRM Configuration Options" on page 351
Auto-Provisioning	For large deployments, consider enabling auto-provisioning. Juniper Mist can automatically assign device profiles, names, and sites to your APs as you onboard them.	"Auto-Provision Device Names, Sites, and Device Profiles" on page 90

Explore Juniper Mist Features

SUMMARY

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.

IN THIS SECTION

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 Automatic Firmware Upgrade" on page 82.

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 384.
  - For in-depth insight into monitoring, see the Juniper Mist AI-Native Operations 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 AI-Native Operations Guide.

2

CHAPTER

Access Points

SUMMARY

Use the information in this chapter to select your access points (APs), onboard them to your organization, and enable the features that you need to support your business and your users.

IN THIS CHAPTER

Video: AP Page Tour

What Do You Want to Do?

Table 2: Top Tasks

If you want to...	Use these resources:
Install APs at your site *Use datasheets to compare models. Use quick start guides and deployment guides to install your APs.*	Juniper Mist Supported Hardware - Wireless Access Points
Add APs to your Juniper Mist organization *Onboard your APs, assign them to your sites, and position them on your floorplans.*	• "Claim a Juniper AP" on page 42 • "Assign APs to Sites" on page 45 • "Adding APs to a Floorplan" on page 61
Get the latest AP firmware *Upgrade the firmware to the latest release.*	"Upgrade the Firmware on a Juniper AP" on page 79
Reset an AP to Factory Default Settings *You might need to do this when the AP is unresponsive or the current configuration fails and the AP cannot connect to the Juniper Mist cloud.*	"Reset an AP to the Factory-Default Configuration" on page 421
Optimize WPA2/WPA3 authentication by enabling fast roaming *Fast roaming is a great feature to enable when using WPA2/WPA3.*	"Enable Fast Roaming" on page 161

Table 2: Top Tasks *(Continued)*

If you want to...	Use these resources:
Enable your AP's vBLE array to support location services *If your use cases include indoor wayfinding, access tracking, and other location-based features, you need to enable BLE settings.*	"BLE Settings" on page 90 Juniper Mist Location Services Guide
Set up a mesh network *Use APs in a mesh to simplify wireless AP deployment and expand coverage.*	"Wireless Mesh Network Configuration" on page 97
Set up geofencing to prevent unauthorized access from nearby clients *Set an RSSI threshold to detect outside devices that are trying to gain access your network.*	"Enable Geofencing" on page 253
Streamline AP onboarding and configuration with device profiles *Save common configurations in device profiles and apply them to dozens or hundreds of APs at once.*	"Device Profiles Overview" on page 127

Overview of Juniper APs

SUMMARY

Get familiar with the features and benefits of Juniper access points (APs).

Juniper® Series of High-Performance Access Points 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 1: 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: Juniper Mist Supported Hardware.

Juniper AP Ports and Their Usage

SUMMARY

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

IN THIS SECTION

Table 3 on page 19 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 7	AP47	Eth0: PoE 802.3bt in + data in Eth1: PoE 802.3bt in + data in	–
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	Eth0: PoE 802.3bt 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.	–
	AP64	Eth0: PoE 802.3at/ 802.3bt in + data in	–
Wi-Fi 6	AP12	Eth0: PoE 802.3at in + data in Eth1: Data out 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. Eth2 and Eth3: Data out	–
	AP32	Eth0: PoE 802.3at in + data in Eth1: Data out	–

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	Eth0: PoE 802.3at in + data in Eth1: Data Out If the PoE Passthrough feature is enabled, the Eth1 port can provide PoE out. **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.	–
	AP41	Eth0: PoE 802.3at in + data in Eth1: Data out	Supports digital inputs (0 to +5V), digital outputs (0 to +5V), and analog inputs (0 to +5V)
	AP61	Eth0: PoE 802.3at in + data in Eth1: Data out The Eth1 port does not support PoE out.	–

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

Wireless Standard	AP Model	Ports	
		Ethernet	IoT
Other	BT11	Eth0: PoE 802.3at in + data in Eth1: Data out If the PoE Passthrough feature is enabled, the Eth1 port can provide PoE out. **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.	–

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.

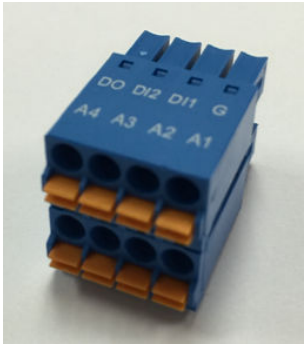


Table 4: IoT Port Connector Pins

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 APs

SUMMARY

Understand the Power over Ethernet (PoE) requirements to ensure that your access points (APs) receive sufficient power.

IN THIS SECTION

The following table lists the power over Ethernet (PoE) requirements for Juniper Mist Access Points (APs). The notes below the table provide additional information for understanding the dynamic power mode available with most Juniper APs.

Table 5: PoE Requirements for Juniper APs

Generation	Model	Minimum Power	Full Wi-Fi*
Wi-Fi 7	AP36	802.3at	29.3 watts
	AP37	802.3at	29.3 watts
	AP47/D/E	802.3at/bt	29.3 watts
	AP66	dynamic	25.5 watts
Wi-Fi 6E	AP64	802.3af	13 watts
	AP45/45E	dynamic	29.3 watts

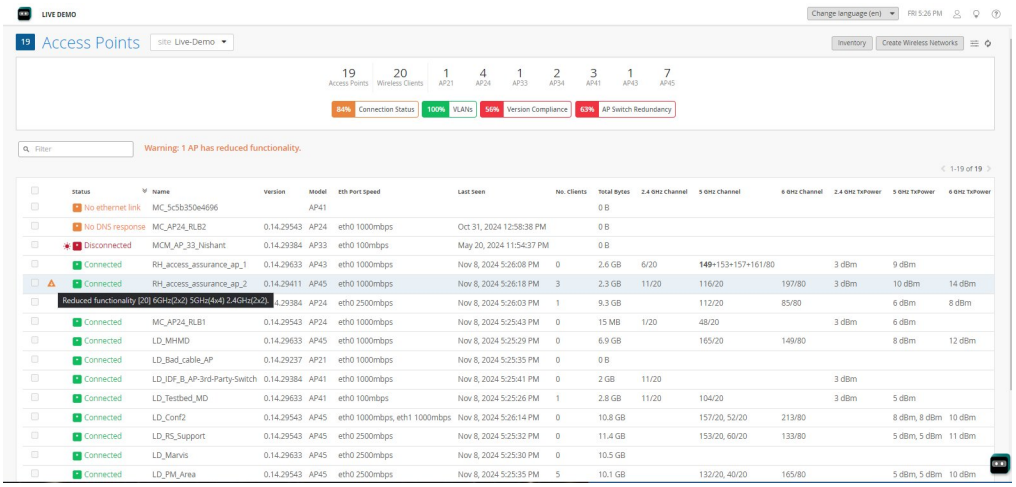
Table 5: PoE Requirements for Juniper APs *(Continued)*

Generation	Model	Minimum Power	Full Wi-Fi*
	AP34	dynamic	20.9 watts
	AP24	802.3af	13 watts
Wi-Fi 6	AP63	802.3at	25.2 watts
	AP43	802.3at	25.5 watts
	AP33	802.3af	19.5 watts
	AP32	802.3af	19.5 watts
	AP12	802.3af	12.9 watts
Wi-Fi 5	AP61	802.3at	19.5 watts
	AP41	802.3at	19.5 watts
	AP21	802.3af	12.9 watts
Other	BT11	802.3af	5.5 watts
* Power required at the power device to support all Wi-Fi radios and all spatial streams.			

Full Power, Reduced Functionality, and Insufficient Power

Although you may be able to power up an AP from any given PoE interface, if the interface does not meet the requirement for full power, the performance of the AP will be unpredictable. In this case, a warning appears on the Access Points dashboard, indicating either that the AP is running with reduced functionality (dynamic power mode), or that the AP is only able to connect to the cloud.

Figure 2: Reduced PoE Power



To see the exact power required, power requested, and power allocated for a given AP, click the AP name in the Access Point list, and in the screen that appears, scroll down to the Power Mode section.

Dynamic Power Mode

Many Juniper Mist APs can leverage a dynamic power mode which allows them to automatically reduce their operating capabilities according to the power available, for example by reducing from 4x4:4 spatial streams to 2x2:2 spatial streams.

- **AP47**—The AP47 has two 10 multi-gigabit Ethernet ports, both of which support power over Ethernet (PoE) in. Either port, or both ports, can be used to power the AP. It requires 802.3bt power (approximately 29 watts at the PD) for full Wi-Fi functionality and to power the USB port.
    - - Single 802.3bt in—Full functionality
        - Both 802.3bt in—Full functionality. When both ports are connected, LLDP details and PoE statistics for the active and standby ports are available in the **Connected Switch Properties** section of the AP details page.
    - On 802.3at power, the AP will operate with reduced functionality. If all three Wi-Fi radios are enabled, they will operate at 2x2:2. If only two Wi-Fi radios are enabled, they will operate at 4x4:4 The scanning radio, BLE radios, GPS and UWB are always enabled regardless of power source.
        - Single 802.3at in—Reduced Wi-Fi functionality—tri 2x2 or two 4x4
        - Both 802.3at in—Full functionality

    - Mixed Power Source
        - One 802.3bt in and one 802.3at in—Full functionality

- Note: Regarding the failover behavior of AP47 when both Ethernet ports are used for uplink. There is full Ethernet and PoE redundancy support when the AP is powered by two 802.3bt sources. When the AP is powered by two 802.3at sources this is considered as power sharing—the power from both ports is combined for full functionality. In this case, there is full Ethernet redundancy, however the AP may brownout or reboot in the event one of the power sources fails. In lab testing this is a rare occurrence, however we want to call out for the highest redundancy, please ensure 802.3bt power sources are used.

  Please ensure 802.3bt or 802.3at compliant PoE switches or injectors are used to power the AP47

- **AP45 or AP45E**—Requires 802.3bt for full functionality. The dedicated scanning radio and BLE are always active regardless of power.
    - At 802.3at power, with any two data radios enabled, both will operate in 4×4 mode. In order to provide power to the USB with 802.3at power, only one radio can be enabled at start-up. With all three data radios enabled, the 2.4 GHz radio will run in 2×2 mode, the 5 GHz radio will run in 4×4 mode, and the 6 GHz radio will run in 2×2 mode. With all three data radios enabled and 5 GHz dual band also enabled, one 5 GHz radio will run in 2x2 mode and the other will run in 4×4 mode. For 5 GHz and 6 GHz dual band, both radios will run in 4×4 mode.
    - At 802.3af, an AP45 or AP45E can connect to the cloud, but only to let you know it needs more power.
- **AP61 or AP61E, AP63 or AP63E**—Always require 802.3at or PoE+ (because these APs consume a maximum of 25.5W).
- **AP41 or AP41E, AP43 or AP43E**—Always require 802.3at or PoE+ (because these APs consume a maximum of 25.5W).
- **AP34**—At 802.3af, the AP can connect to the cloud, but only to let you know it needs more power.
- **AP33/32**—At 802.3af power, the 5-GHz radio operates in 2×2 mode instead of 4×4 mode. Eth0 port operates at a maximum speed of 1 Gbps Eth1 port is disabled.
- **AP24 and AP64**—Always require 802.3af.
- **AP12** —Only requires 802.3at if using PoE out; otherwise, 802.3af power is sufficient.

More Information

PoE injects DC power onto a standard twisted pair Ethernet cable without disturbing the data traffic being transmitted over the same cable. The power sourcing equipment (PSE), such as a supported Juniper switch, supplies the power and the powered device (PD), such as a Juniper Mist AP, gets its power from the switch. Because Ethernet is an isolated network, each twisted pair connects to a different data transformer.

- The IEEE *802.3bt* PoE standard provides for Ethernet cables to carry up to 90 watts of DC power for connected devices (by means of 4 twisted pairs).
- The IEEE *802.3at*-2009 PoE+ PoE standard provides for up to 25.5 watts.
- The IEEE *802.3af*-2003 PoE standard provides for up to 15.4 watts (by means of 2 twisted pairs).

When connecting to either an *802.3at* or *802.3af* interface, most Juniper Mist APs use hardware detection to determine the PoE interface type. AP45, AP43, and AP34 series will also detect BT power. After the hardware detection, the APs use LLDP, when available, to negotiate their specific power requirements.

Note that for most Cisco switches, LLDP is disabled by default so you must enable it on the interface before connecting an AP that requires 802.3at or higher, otherwise the interface will support 802.3af only.

AP Dashboard

IN THIS SECTION

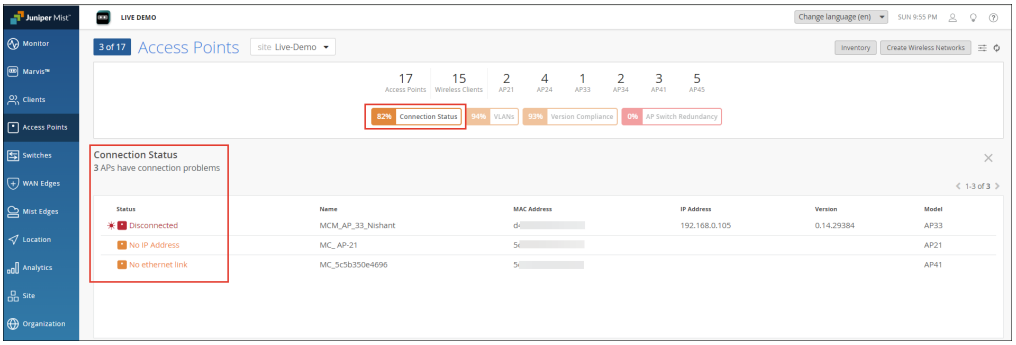
AP Metrics

SUMMARY

Proactively monitor the performance of the access points (APs) at your site and quickly identify and troubleshoot connectivity and firmware compliance issues.

You can see the overall operational health of the APs on the Access Points page, which shows a score for connectivity status, VLANs, version compliance and AP switch redundancy. Green indicates 98.5% or higher compliance, orange means 80% to 98.5% compliance, and red means that 80% or fewer APs are meeting the standard. Click one of the orange or red scores to see which devices have a problem and why, as shown in Figure 1.

Figure 3: Access Point Status



- **Connection Status**—Shows the percentage of APs that are online at your site. Click this metric to see the list of APs that are offline and the reason, for example, **No IP Address** or **No Ethernet Link**. You can also check the LED blink pattern on the AP itself, as described here: "What Does the AP Status LED Indicate?" on page 392

- **VLANs**—Shows the percentage of APs where all wired VLANs are active. Click this metric to see APs with inactive VLANs and find the VLAN IDs. Users connected to an inactive, or incorrectly configured VLAN won't be able to get an IP address or connect to the network.

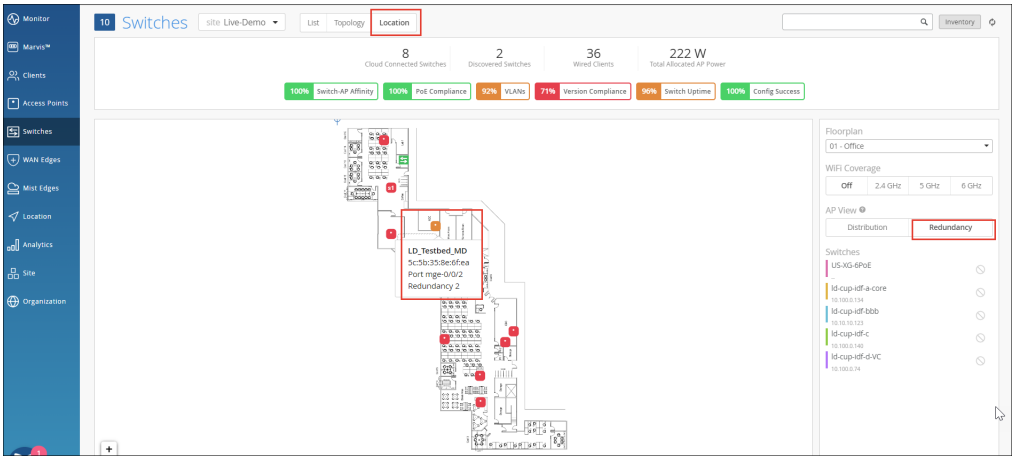
- **Version Compliance**—Shows the percentage of APs, by model, that are using the expected firmware version. The values shown here can have different meaning depending on whether or not you've enabled Auto Update for the firmware. If this feature is enabled, the value reflects the percentage of APs running the version specified in the configuration. Otherwise, the value is relative to the predominant version, per AP model. For example, if three AP41s are running version 0.7.20383 and

two are running version 0.5.17445, version 0.7.20383 is considered the compliant version (and in this case, 40%, or 2 of the 5 total APs, will be shown as non-compliant). For help with the Auto Update feature, see "Enable Automatic Firmware Upgrade" on page 82.

- **AP Switch Redundancy**—Shows how many APs, that are also RF neighbors, as measured by RSSI strength, are connected to the same switch (or VC stack member).
  - 1—No redundancy, that is, all the top RF neighbors are connected to the same uplink switch or stack member.
  - 2—Good redundancy, that is, at least one of the top RF neighbors is connected to a different uplink switch or stack member.
  - 3 and greater—Excellent redundancy, that is, two or more top RF neighbors are connected to two or more different uplink switches.

  You can also view your AP switch redundancy according to the site floorplan by selecting **Switches** from the main menu and then opening the **Location** tab, as shown in Figure 2.

Figure 4: Switch Redundancy Map

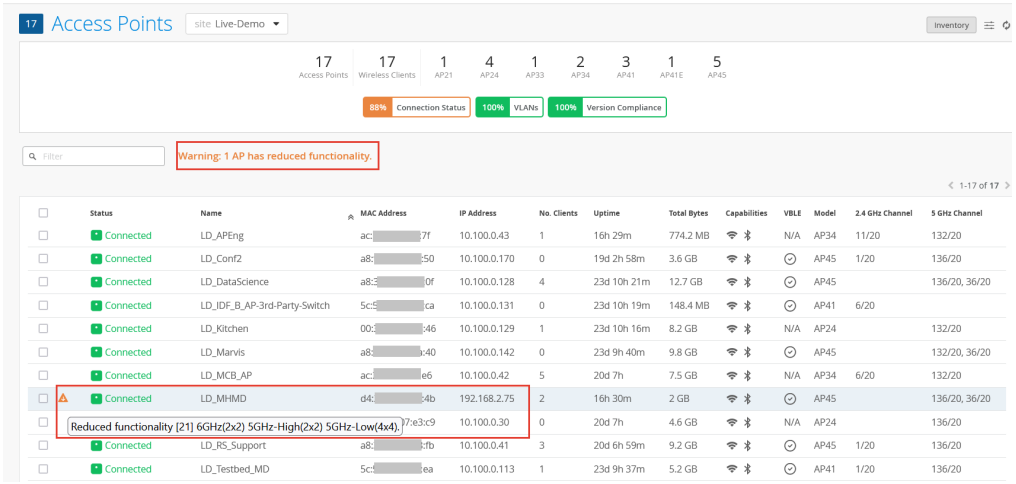


AP Status and Warnings

The Access Points page shows the status of each AP in the site, as well as any warnings associated with the AP. Warning messages are typically shown when an AP is operating in a "reduced functionality mode" on page 28, such as when an AP43 is being used to supply power to an attached USB peripheral.

If an AP in the list shows **Stale Configuration**, it means that the AP was automatically rolled back to a its last known good configuration, typically because there was a config error that caused it to disconnect from the Mist cloud. This warning is associated with the "Automatically Revert Configuration" on page 126 setting for APs site-wide.

Figure 5: Access Point Status and Warnings



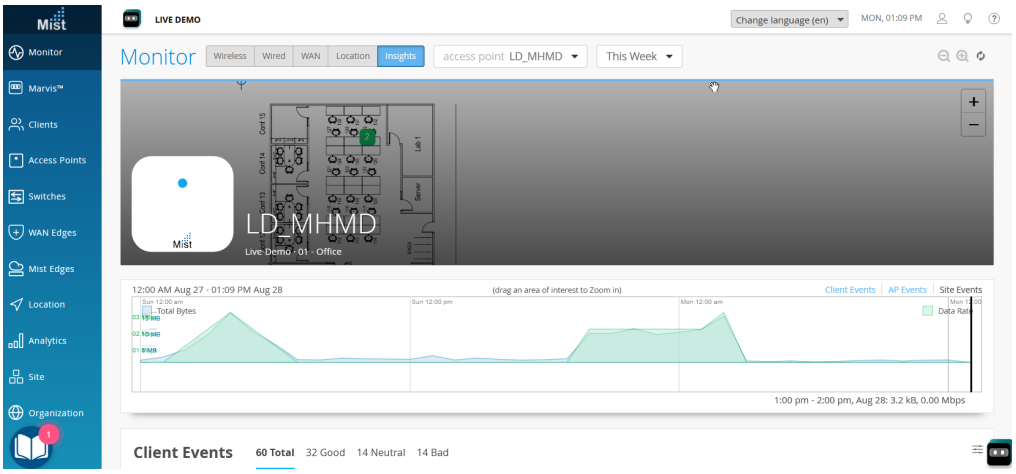
AP Insights

SUMMARY

View information about your access points (APs) and network events.

In the Mist portal, on the AP Insights page, you can see a list of AP events that occurred on the selected site during the selected time frame, as shown in Figure 1.

Figure 6: 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.

AP Utilities

SUMMARY

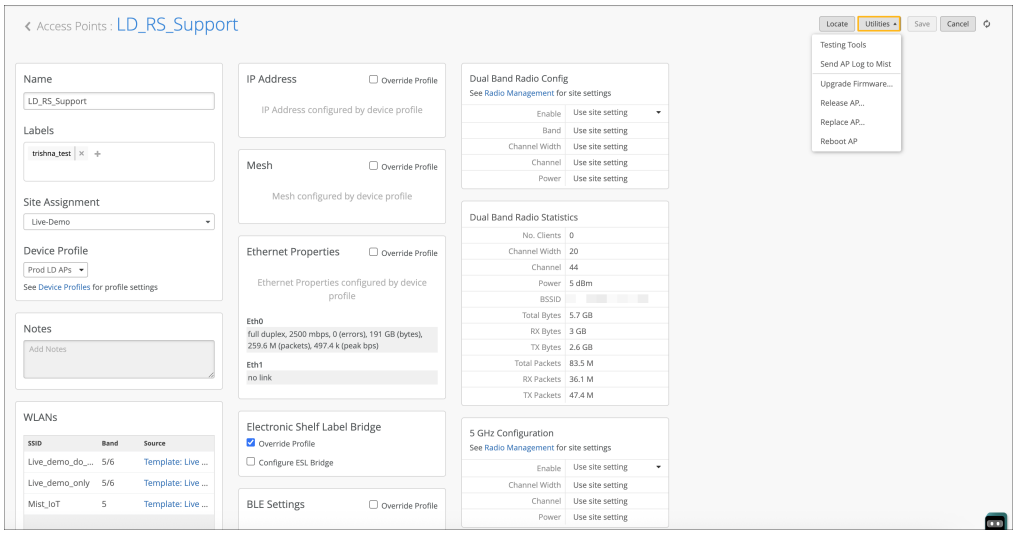
Use utilities to troubleshoot and manage your access points (APs).

Use the **Utilities** option on the AP details page to run tests to monitor the AP and your network. You also can reboot, replace, upgrade, and even release an AP. With these options available on a single page, it becomes easier to manage and troubleshoot your AP.

You can access these options under **Utilities** on the AP details page.

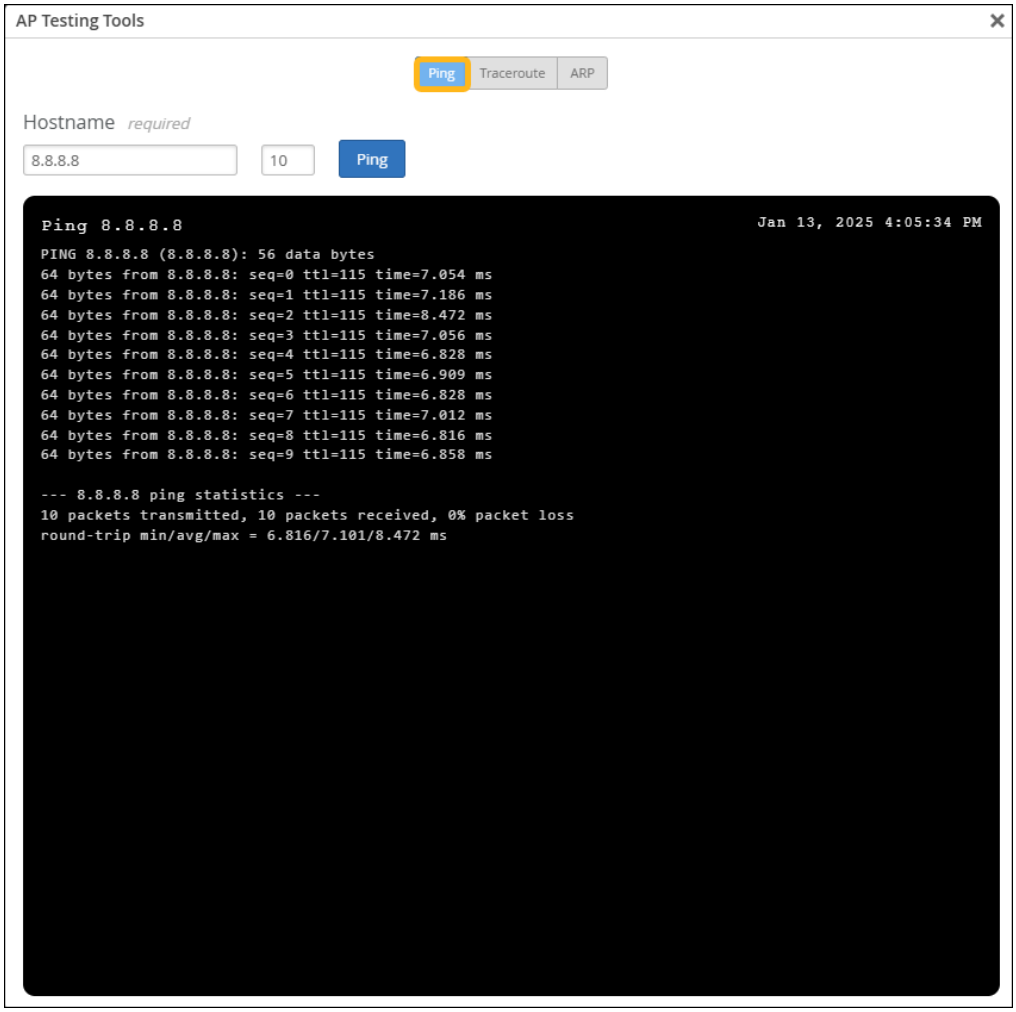
1. On the Juniper Mist portal, click **Access Points** on the left pane.
2. Click an AP from the list to open the AP details page.

3. Select the utility or tool from the **Utilities** drop-down list on the upper-right of the page.



Here are the options that you can access from the **Utilities** list:

- **Testing Tools**—Use the following testing tools to check the AP connectivity and monitor the traffic.
  - **Ping**—Enables you to check the reachability of an IP address or domain. To run the test, specify the IP address or domain name and click **Ping**. You can also enter the number of ping requests to send. The number can range from 1 through 100, with the default being 10.



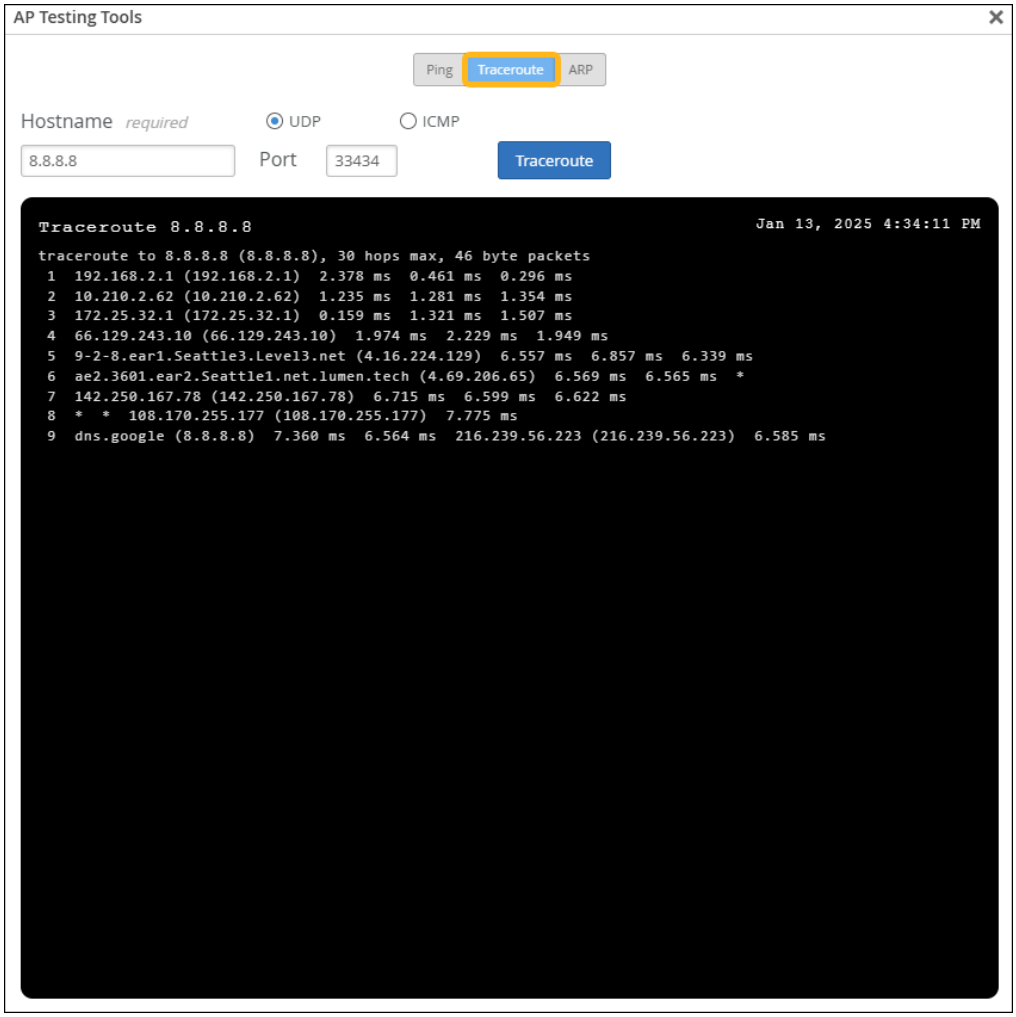
- **Traceroute**—Helps you to analyze the route that packets take to a specified host or domain, and transit delays of these packets. You can choose between the UDP or ICMP protocol.

  You can use ICMP to test network connectivity. ICMP error messages provide information about networking errors, which can help diagnose connectivity issues.

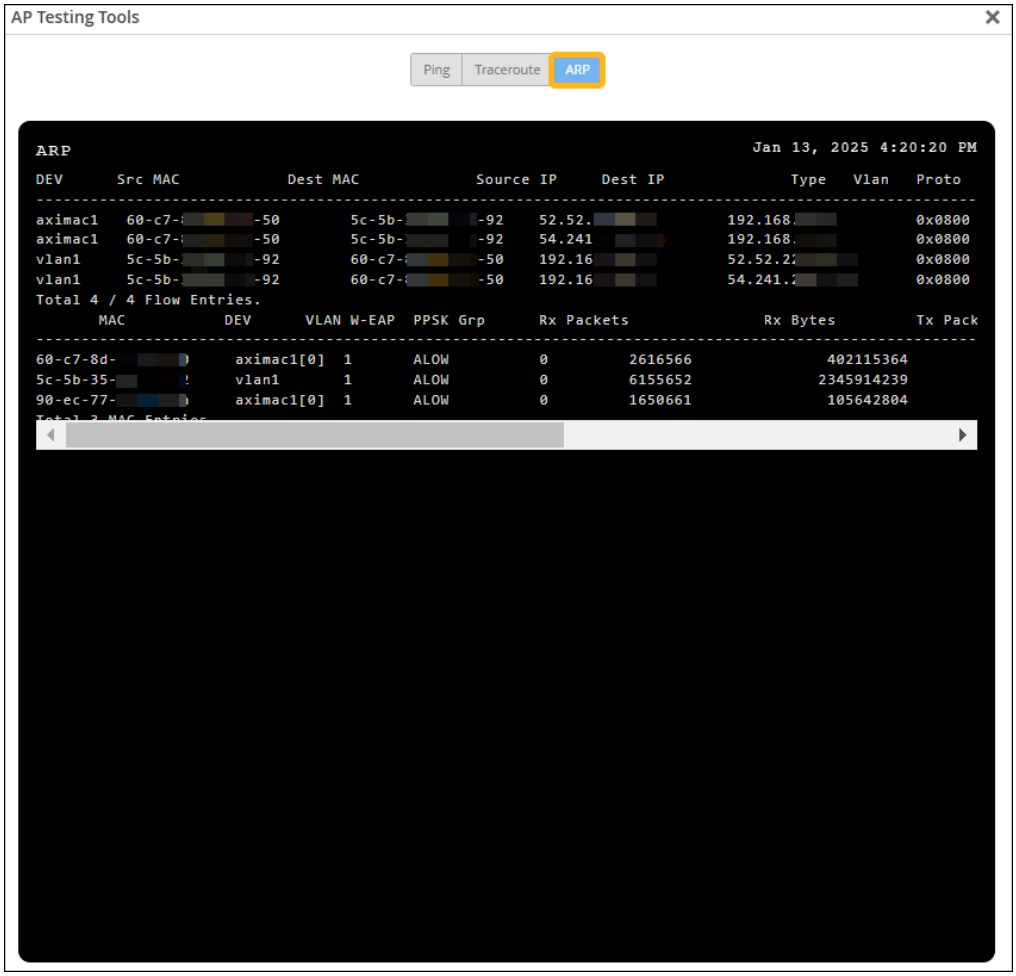
  UDP can be used for time-sensitive applications such as voice and video playback to diagnose application connectivity issues. The default port used for UDP is 33434, but you can set a port number if you want to.

  Note that firewall policies might treat UDP or TCP traffic differently based on certain factors—for example, source or destination ports. As a result, traffic might be routed to different paths. The Traceroute tool enables you to identify such instances.

  To run the test, specify the host, select the protocol, and then click **Traceroute**.



- **ARP**—Lists the ARP entries that you can analyze to identify any network problems. The AP functions as a Layer 2 device and learns the MAC-IP bindings for all sessions through unicast flows. Unlike switches that maintain the ARP entries for only the active sessions on an L3 interface, the AP maintains an ARP entry for the default gateway for every outbound session. These ARP entries are the MAC-IP bindings that the AP is utilizing to forward the traffic on the wired and wireless interfaces.



- **Send AP Log to Mist**—Enables you to send the AP logs securely to Juniper Mist when you experience an issue with your AP. The logs contain real-time status information about the AP and its configuration. The support team uses these logs to understand the issue and provide troubleshooting support.

  It takes at least 30 seconds to 1 minute to send the logs. Do not reboot your device in that interval. If you want to reboot the AP, click **Send AP Log to Mist** first and wait for at least 1 minute before rebooting the AP.

  > **NOTE**: You will not be able to send the logs if the AP is not connected to the Juniper Mist cloud.

  APs have limited onboard log storage, so Juniper Mist uses log rotation to manage device memory efficiently. The retention of logs depends on the number of connected clients and the events they generate. A high volume of client events, even with low client density, increases the likelihood of previous logs being overwritten. If you need to send logs to the Juniper Mist support team, we recommend that you send them within two hours of the occurrence of the issue.

- **Upgrade Firmware**—Manually upgrade or downgrade the firmware on an AP from the AP details page. Note that you can upgrade or downgrade only a single AP from the AP details page. If you need to upgrade multiple APs or perform a peer-to-peer upgrade, then you'll need to use the Upgrade APs option on the **Organization** > **Access Points** page.

- **Release AP**—Release an AP if you no longer want to include it in your organization. An AP must be released if you want to move the AP into another organization or replace it. When you release an AP, the AP is no longer managed by Juniper Mist. See Release an Access Point from Inventory.

  NOTE: Releasing an AP results in the removal of all configuration related to the AP (such as local configurations, profiles, labels, and SSID) and can result in the AP losing wireless connectivity.

- **Replace AP**—Replace an AP seamlessly from the AP details page. The new or replacement AP must be in the **Unassigned** state (that is, the AP is not assigned to a site). Juniper Mist copies the entire AP configuration onto the replacement AP. Depending on the AP model, certain configurations might not be copied to the new AP. See Replace an Access Point

- **Reboot AP**—Use this option if you want to reboot the AP—for example, after a configuration change.

Onboarding

IN THIS SECTION

Request Help with a New Deployment

SUMMARY

If you need help with a new deployment of Juniper Mist™ devices, follow these steps to submit your request.

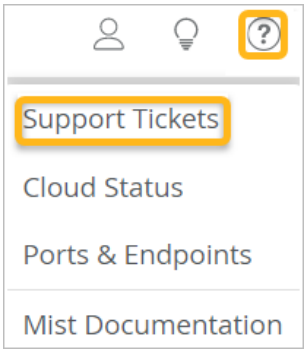
The Juniper Mist Support team provides onboarding assistance to help customers with new deployments. You'll get assistance with initial setup, configuration, and basic troubleshooting.

NOTE:

- These services do not include network design.
- Submit your request at least 48 hours in advance of your preferred appointment time.
- Available only for wireless, switching, and SD-WAN deployments.

To request help with a new deployment:

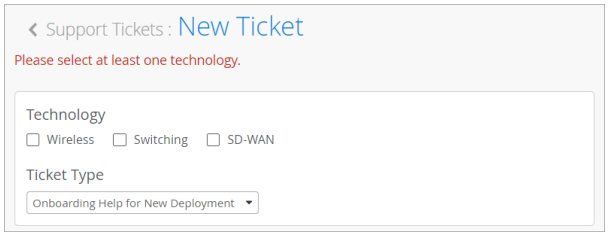
1. Click the question icon near the top-right corner of the Juniper Mist portal, and then click **Support Tickets**.



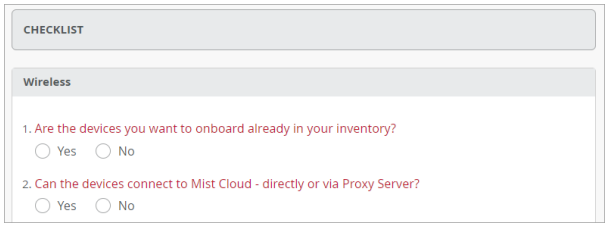
2. Click **Create a Ticket**.
3. For **Technology**, select the technologies that are applicable to your network and are included in the onboarding support program.

NOTE: Onboarding help is available only for wireless, switching, and SD-WAN deployments.

4. For **Ticket Type**, select **Onboarding Help for New Deployment**.



5. Enter a short **Ticket Summary** and a detailed **Description**.
6. Under **Checklist**, answer all the questions.



> **NOTE**: The checklist includes each technology that you selected at the top. Complete all questions in all sections that appear.
>
> As you complete the checklist, you can use suggested hyperlinks for self-help. If you find your answers in these links, you can cancel submitting this ticket.

7. Under **Schedule**, select the date, time, and time zone for your onboarding help session.

> **NOTE**: If you need to change your appointment after you submit your ticket, you can go to your list of open tickets, select this ticket, and reschedule.

8. Click **Submit** at the top right corner of the page.

   If this button is unavailable, ensure that you've entered all required information. Required fields have red labels.

The support team will contact you to conduct the help session.

Claim a Juniper AP

SUMMARY

You need to claim an access point (AP) to be able to manage it from the Juniper Mist cloud.

IN THIS SECTION

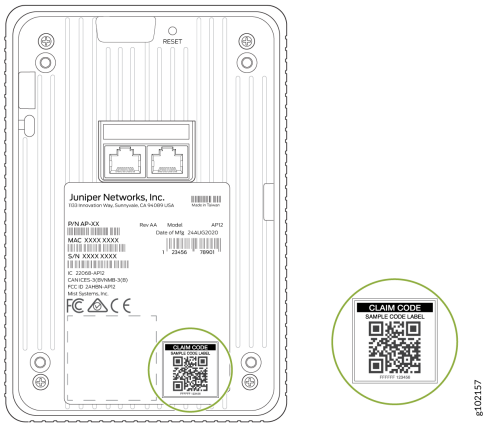
You'll need either a claim code or an activation code to claim an AP. With either, you can claim an AP by using one of the following methods:

- 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

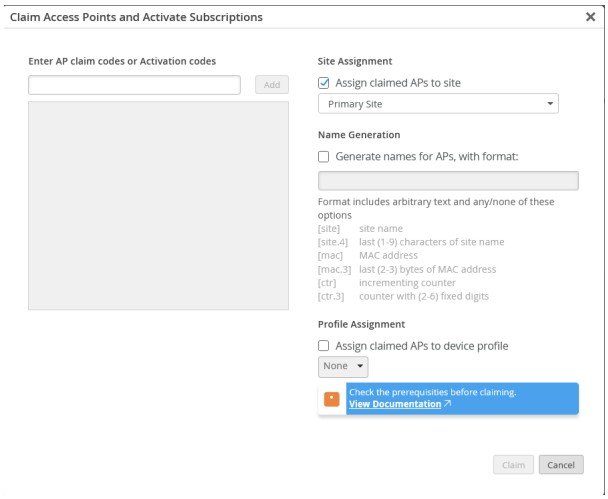
You can onboard a single AP or multiple APs using a Web browser. If you're onboarding a single AP, use the claim code or QR code located on the rear of the AP. If you're onboarding multiple APs, use the activation code that is listed in your purchase order.

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.

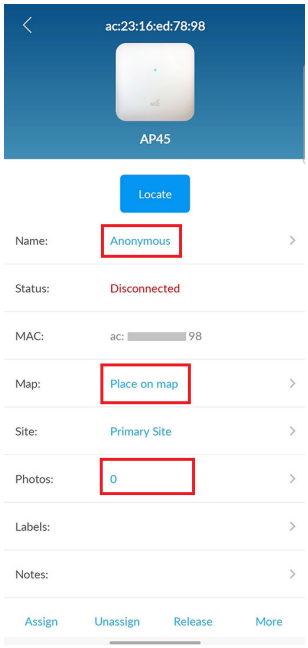
   You can also choose to rename and assign an AP to a site after you claim the AP.
6. (Optional) Select the **Assign claimed APs to device profile** check box and select a device profile from the drop-down list. For information about device profiles, see "Device Profiles Overview" on page 127.
7. Click **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:

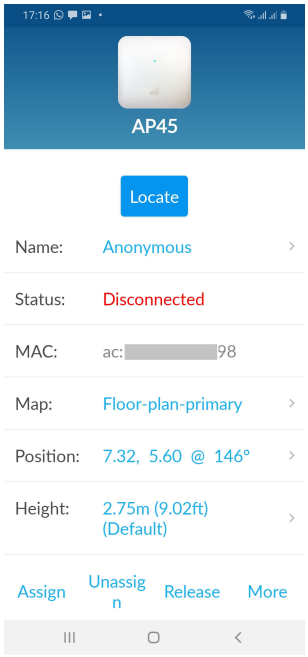
1. Download and install the Mist AI app from the Google Play Store or Apple App Store.
2. Open the Mist AI app and log in using your account credentials.

   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 APs to Sites

SUMMARY

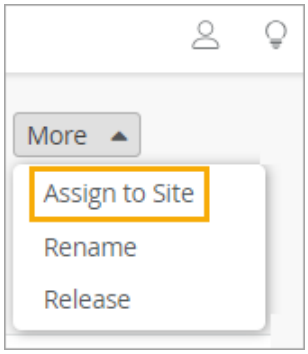
Ensure that all access points (APs) in your organization are assigned to a site.

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:

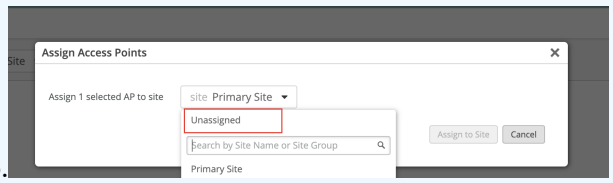
1. From the left menu of the Juniper Mist™ portal, select **Organization** > **Inventory**.
2. Click the **Access Points** button at the top of the page.
3. Select the check box for one or more APs.

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

SUMMARY

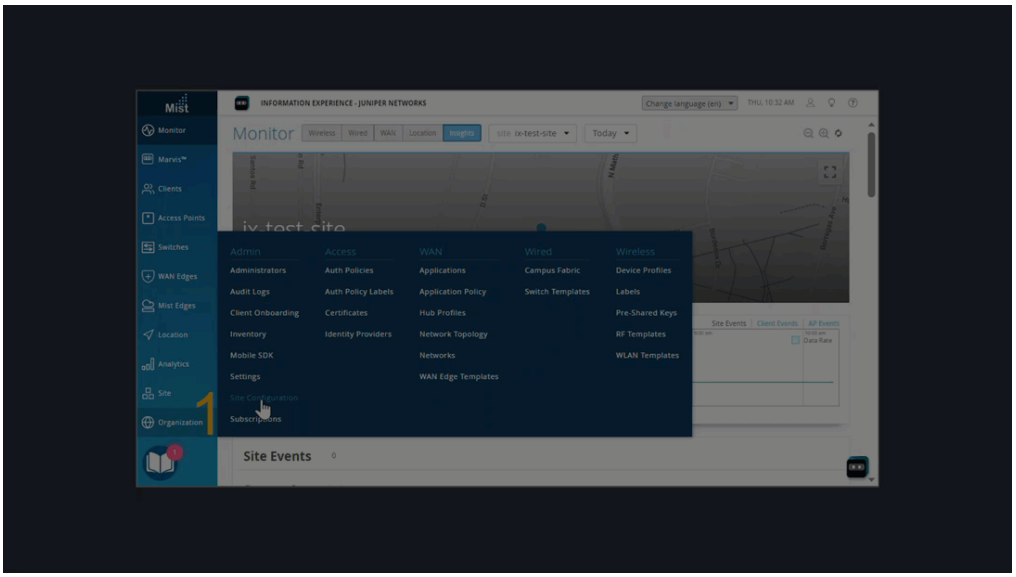
To ensure access point (AP) stability, you can enable configuration persistence.

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.

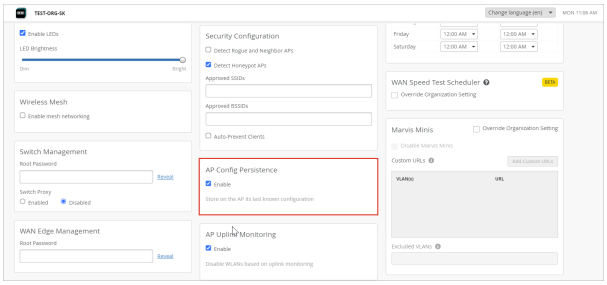
You'll need to enable configuration persistence if you want to use an AP in survey mode. See "Configure an AP for Survey Mode" on page 113.

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**.

Floorplans

SUMMARY

Floorplans are a useful tool and are especially important for Location Services. You can manually upload it or import it. Be sure to scale and validate it to ensure accuracy.

IN THIS SECTION

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.

What Do You Want to Do?

Table 6: Top Tasks

If you want to...	Use these resources:
Upload a floorplan and set it up manually	"Manually Upload Your Floorplan" on page 49
Import a floorplan from another tool	"Import a Floorplan" on page 50
Ensure that the floorplan is properly scaled for your site	"Scale a Floorplan" on page 58
Check your floorplan for accuracy	"Validate Your Floorplan" on page 59

Manually Upload Your Floorplan

SUMMARY

Upload an image file to use as your floorplan.

IN THIS SECTION

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 58
- "Manually Place an AP on a Floorplan" on page 61
- "Validate Your Floorplan" on page 59

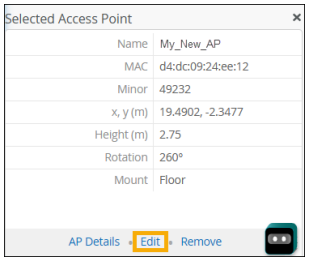
Import a Floorplan

SUMMARY

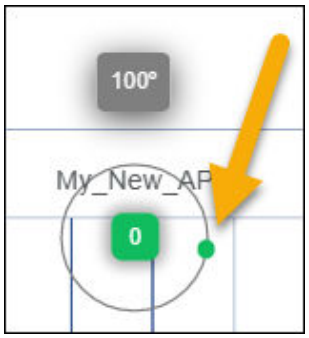
Import a floorplan that you've created in software such as Ekahau or iBwave.

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**.



- 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 58
- "Manually Place an AP on a Floorplan" on page 61
- "Validate Your Floorplan" on page 59

Deploy Mist with Ease using Wireless Design Tools

SUMMARY

Read this topic to learn how you can use wireless design tools to easily import floorplans and related attributes into the Juniper Mist™ portal.

IN THIS SECTION

You can manually import a floorplan and related attributes into the Juniper Mist™ portal simply by importing the files you already created in wireless design tools such as Ekahau Pro, iBwave, and Hamina. Wireless design tools provide a one-stop-shop for all of your floorplan and building design needs. They enable you to design your floorplan and related aspects such as access point (AP) placement, AP orientation, channel settings, and more. Importing the resulting files saves you time, as the design work you have already done in your project within the design tool automatically carries over when you import the file into Mist. Using these completed floorplan maps reduces duplication of effort.

Hamina also offers an integration with the Mist cloud API that enables automatic import of floorplan designs into Mist. Once you provide your Mist API key, simply export your floorplan designs from the third-party tool and they carry over automatically to Mist. Hamina uses the export function to drive the automatic floorplan import to Mist.

This topic demonstrates the following (in sequential order):

- **Manual Import:** How to export design files from wireless design tools and how to manually import those files into Mist.
- **Automatic Import (with integrations):** How to export design files from wireless design tools for automatic import to Mist.

Each of the wireless design tools is introduced in their own sections of this topic.

As part of the *manual* file import, Mist automatically:

- Imports floorplan images from the file.
- Sets the scale of the floorplan for you.
- Imports any APs from the file along with their associated settings, as long as you have completed "AP Matching" on page 54.

- Assigns the AP's x,y coordinates, height, and orientation.
- Assigns the AP to a site if it has not already assigned to one. This requires Super User or Org Network Admin privilege.
- Places the AP on a floorplan if it has not already been placed on a floorplan.
- Names the AP if it has not already been named in the wireless design tool. Otherwise, the name given in the design tool is carried over as part of the import.

NOTE: The import action in Mist never changes an AP's assigned site, name, or floorplan if one has already been assigned in the design tool.

Mist currently allows you to import a floorplan using the following file types:

- Ekahau (`.esx` files)
- iBwave (`.mist.ibwc` files)
- Hamina (there is no file type necessary for importing Hamina floorplans into Mist, as the items you select and export in Hamina are imported directly to Mist as part of the integration).

The *automatic* file import from wireless network tools into Mist (via API integrations) includes the following:

- Hamina:
  - Uploads the floorplan to Mist
  - Matches simulated APs from the Hamina project to the APs in Mist
  - Assesses Wi-Fi coverage needs
  - Scales the floorplan
  - Places the APs on the floorplan
  - Assigns APs to the site
  - Assigns AP names, height, orientation, MAC addresses, location, transmit power, channel, and channel width settings
  - Deploys new sites in Mist

Requirements and Considerations

To import a floorplan into Mist from a third-party project file, you must follow these requirements and keep the following information in mind:

- • iBwave—You must use a minimum version of iBwave Wi-Fi 14.2 or a later.
  - Ekahau Pro—Survey data is *not* supported for *file import*. All survey data must be deleted from the project prior to importing into Mist.
  - Floorplan image size—The size of the floorplan file you import to Mist must be less than 8 MB (less than 1 MB is recommended).
  - You must "Match APs in the Project Files to Your Physical Mist APs" on page 54.

Match APs in the Project Files to Your Physical Mist APs

Prior to using the Import Floorplan feature in Mist, you must match the simulated APs in the project files to your physical Mist APs. There are several ways to accomplish this:

- • Match via MAC address—Within the project file, use the `<apname> - <apmac>` notation to name APs.
  - This is useful if you manually allocate APs ahead of time.
  - Alternatively, you can simply enter the MAC address of the AP name in the project file. This is demonstrated in the Ekahau video below. Use this method if you don't want to name APs in Mist.
  - Match via AP name—Name the AP in the project file so that is matches the exact name of the AP within Mist.
    - This method is most commonly used in conjunction with the Mist AI Mobile App. The advantage is you can pick any AP at random out of the box, and then use the application to scan the QR code and enter a name at the time of installation. You do not need to pre-allocate APs. See "Claim an AP Using the Mist AI Mobile App" on page 44.
  - Match via CSV file—Name the AP in the project file, and also import a CSV file with AP name to MAC address mapping.
    - This is the most flexible and scalable method. It's especially useful when third-party contactors are used to install the APs, as they typically provide a spreadsheet with AP and serial number or mac address.
  - Manually match APs when you ingest the project files.
    - This method is only recommended for small deployments, as it is the most time consuming method.

Export Ekahau Design Files and Import them to Mist

Ekahau is a tool you can use to design your floorplan with granularity for network optimization. It enables you to design your floorplan and related devices so that it mirrors the real-world setup. You can export your Ekahau floorplan designs from within the tool and then manually import them into Mist.

1. In Ekahau Pro, navigate to **File** > **Save** and save the `.esx` file which you will import to Mist in an upcoming step to a location on your local drive.
2. df
3. On the Mist portal, navigate to **Location** > **Live View** > **Import Floorplan**.
4. On the Import Floorplans window, drag and drop the `.esx` file you want to import and select any AP settings you want to include under **More Options**. See step 4 in "Import a Floorplan" on page 50 for more details about what these options do.
5. Click **Import**.
6. To complete "AP Matching" on page 54, select the **Match APs** button, or click **Finish** if you are done. You should now see your floorplans have been imported along with any associated settings.

   The following videos provide a start-to-finish look at how to design and plan your network using Ekahau.

Video: Create Your Floorplan Design in Ekahau

Video: AP Placement in Ekahau for Indoor Location Wayfinding

Video: AP Height and Orientation Considerations in Ekahau

Video: RRM Planning in Ekahau

Video: Import Your Ekahau Floorplan Design into Mist

Export Hamina Design Files for Automatic Import to Mist

The Hamina Planner is a web-based planning and design tool. It is integrated with Juniper Mist so that, when you export your floorplan design from Hamina, it is automatically imported to Mist. This is accomplished through Hamina's integration with the Mist cloud API.

Prior to exporting your Hamina design files, ensure the following:

- Your design includes:
  - Background map

  - Scaled layout
  - AP locations
  - AP model and type
  - BLE directionality
  - Height settings
  - Walls and attenuating objects
  - Scope zones
- AP naming is consistent:
  - Helps Mist match APs more easily during import
  - Optional: Preload MAC addresses if known

1. In Hamina, select your project name from the drop-down menu in the top left corner, then select **Export**.
2. Under the Juniper Mist section of the Export window, make the appropriate selections in the **Region** and **Choose credentials** fields. The credentials field is where you select your Mist API credentials. Or, you can click the three dots to the right of the field to enter a new API key. Refer to Create API Tokens if you need to obtain your Mist API Key.

   NOTE: The Mist API enables Hamina floorplan designs and AP settings to be brought over automatically to Mist.

3. Select the appropriate Organization, Site, Floorplans, and APs to export, then click **Export**. This action sends all of the selections over to Mist.

   To see the export steps in action, watch the video under the **Import & Export, Reimagined** section of this blog.
4. On the Mist portal, navigate to **Location** > **Live View**. You should see your floorplan imported from Hamina.

   NOTE: Additionally, when you create a new project in Hamina, you can choose Connect Infrastructure, then choose Juniper Mist and select your region and credentials. This automatically brings the floorplan you selected to the Live View page of the Mist portal along with any APs and related information.

   Watch the video below for a closer look into the power of the Juniper Mist and Hamina integration.

Video: Future of Wi-Fi Tools

Automatically Import Mist Floorplans to Hamina

On the flip side, you can import Juniper Mist floorplans and associated inventory into Hamina. Follow the instructions outlined in Import From Juniper Mist to Hamina to see how this is done.

If you wish to make changes to a Mist floorplan you imported to Hamina, you can push those changes back to Mist by following the export steps in the section above.

You can also see the steps for importing Mist Floorplans to Hamina in the second half of the video under the **Import & Export, Reimagined** section of this blog.

Export iBwave Design Files and Import them to Mist

iBwave is a wireless network design software that enables you to design floorplans and related aspects, ensuring an exceptional wireless experience in your buildings. You can export your iBwave floorplan designs from within the tool and then manually import into Mist.

1. Complete the steps outlined in iBwave's Quick Start Guide to create a project in iBwave Express.
2. In iBwave Express, navigate to **File** > **Export** > **Export to MIST**.
3. Save the file to a location on your local drive.
4. On the Mist portal, navigate to **Location** > **Live View** > **Import Floorplan**.
5. On the Import Floorplans window, select the `.mist.ibwc` file you want to import and select any AP settings you want to be included under **More Options**. See step 4 in "Import a Floorplan" on page 50 for more details about what these options do.
6. Click **Import**.
7. To complete AP matching, select the **Match APs** button, or click **Finish** if you are done.
   You should now see your floorplans have been imported.

   The following videos provide a start-to-finish look at how to design and plan your network using iBwave.

Video: Create Your Floorplan Design in iBwave

Video: Place APs on a Floorplan in iBwave

Video: RRM Planning in iBwave

Video: Import Your iBwave Floorplan Design into Mist

SEE ALSO

Import a Floorplan | 50

https://docs.hamina.com/planner/import-export/juniper-mist

https://blog.hamina.com/hamina-wireless-x-juniper-integration-brings-network-design-and-operations-together

https://support.ekahau.com/hc/en-us/articles/20294597049883-Ekahau-Juniper-Mist-Dashboard-Integration-How-To-Guide

Scale a Floorplan

SUMMARY

To ensure location accuracy, scale your floorplan.

IN THIS SECTION

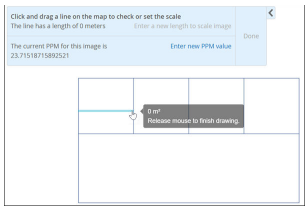
After you "upload" on page 49 or "import" on page 50 your floorplan, you need to set the scale.

Video Overview

Video: Scale a Floorplan

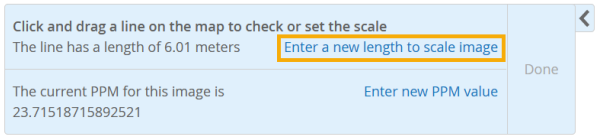
1. From the left menu of the Juniper Mist portal, select **Location** > **Live View**.
2. Select the site and the floorplan.
3. Click **Set Up Floorplan**.
4. Click **Set Scale** (near the top left corner of the floorplan).
5. Drag a line between two points on the floorplan.

   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.

Now you're ready to add access points to the floorplan.

Validate Your Floorplan

SUMMARY

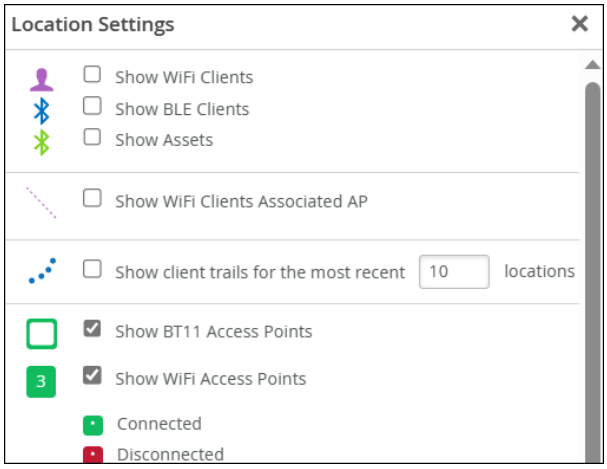
Double-check everything to ensure that your floorplan is valid.

Most issues with location can be traced to floorplan inaccuracies. To enable the AP to generate accurate location estimates, the position information in the Juniper Mist portal must match the AP's actual position at your site.

1. From the left menu of the Juniper Mist portal, select **Location** > **Live View**.
2. Select the site and the floorplan.
3. If APs are not visible 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.



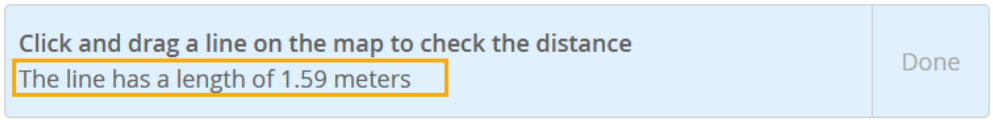
c. Close the **Location Settings** window.

4. Check the scale to ensure that distances on the floorplan match the actual distances at the site.

   a. Click **Ruler**.

   b. Draw a line between two points on the floorplan, such as two walls of a room.

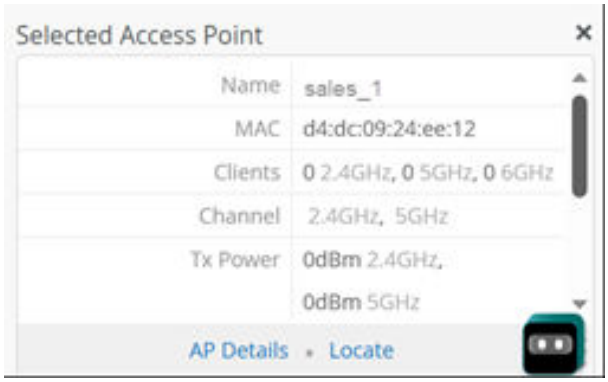
   c. Verify that the line length in the blue box matches the actual measurement at the site.



   d. Click **Done** to put away the ruler.

   If you need to change the scale, click **Setup Floorplan**, and then make the changes. For help, review the other topics in this chapter.

5. Click each AP, and verify the information in the **Selected Access Point** area of the page.



- The MAC address shown on the floorplan must match the MAC address of the corresponding AP at the site. If the MAC addresses don't match, then Juniper Mist has inaccurate information about the location of the AP, and the location estimates will be incorrect.

- The position, height, and orientation must be accurate to enable Juniper Mist to generate correct location estimates.

If you need to make changes, click **Setup Floorplan**. Make changes by dragging the AP or by editing the position details. For help, review the other topics in this chapter.

Adding APs to a Floorplan

SUMMARY

Adding Juniper Mist™ Access Points (APs) to the floorplan provides a helpful visualization for your deployment. For Location Services deployments, correctly positioning your APs is critical for location accuracy.

IN THIS SECTION

You can add APs in these ways:

- "Manually Place an AP on a Floorplan" on page 61
- "Autoplacement: Position New APs" on page 69

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 "Autoplacement: Verify AP Positions for an Existing Site" on page 64.

Manually Place an AP on a Floorplan

SUMMARY

If you're not using autoplacement, manually position your access points (APs) on your floorplan.

IN THIS SECTION

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.

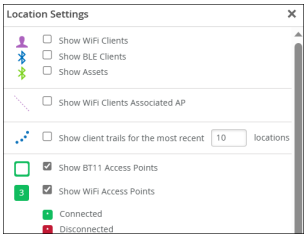
  The following figure shows the location of the LED on an AP.

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).

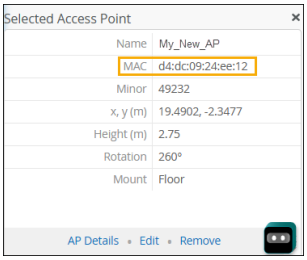
   b. Select the check boxes to show BT11 and Wi-Fi APs.



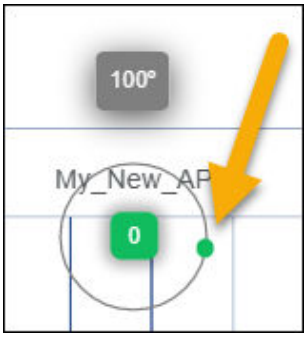
c. Close the **Location Settings** window.

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.



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.

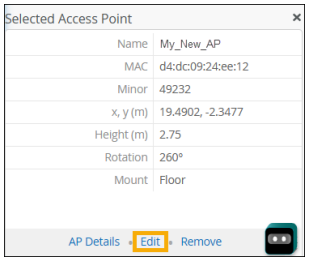


NOTE: In the "Before You Begin" on page 61 section, we imagined drawing a line from the Juniper Mist logo through the LED to an endpoint on the north wall. Here, we drag the green dot so that it aligns with that imaginary path.

9. Set the AP height:

   a. Click the AP.

b. Click **Edit** in the **Selected Access Point** section.



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 Your Floorplan" on page 59.

Autoplacement: Verify AP Positions for an Existing Site

SUMMARY

If you've manually placed access points (APs) on your floorplan, you can verify their positions by using autoplacement. For Location Services deployments, correct positions on the floorplan are critical to ensure location accuracy.

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.

You will receive a message warning you that the action causes a disturbance in your Wi-Fi network(s) and user(s) will be impacted.

NOTE: The above statement does not display if you are performing autoplacement on a floorplan that contains all AP47s, as the AP47 is an Ultra-Wideband (UWB) supported AP and is non-disruptive to Wi-Fi.

Requirements for using autoplacement:

- The supported AP models for autoplacement are AP24, AP32, AP33, AP34, AP43, AP45, and AP47.

- The minimum required firmware version for autoplacement is version 14.28310.

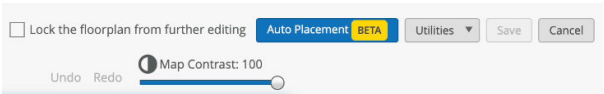
Before you use the autoplacement feature in an existing deployment, ensure that:

- 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.

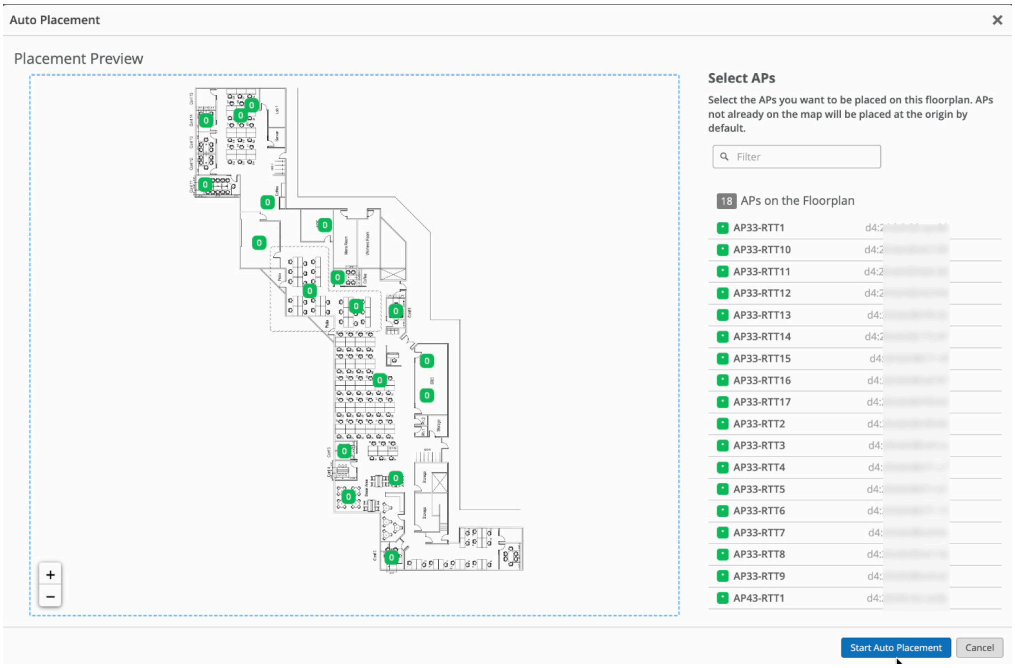
> **NOTE**: If the preceding description doesn't fit your situation, see "Autoplacement: Position New APs" on page 69.

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.

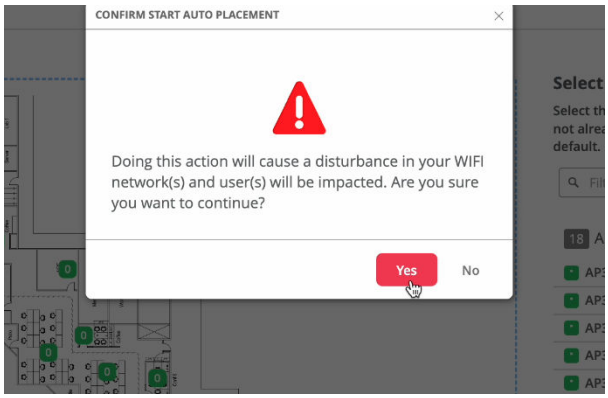


5. On the list of APs in the Floorplan section on the right side of the page, select the APs for which you want to verify the floorplan position.

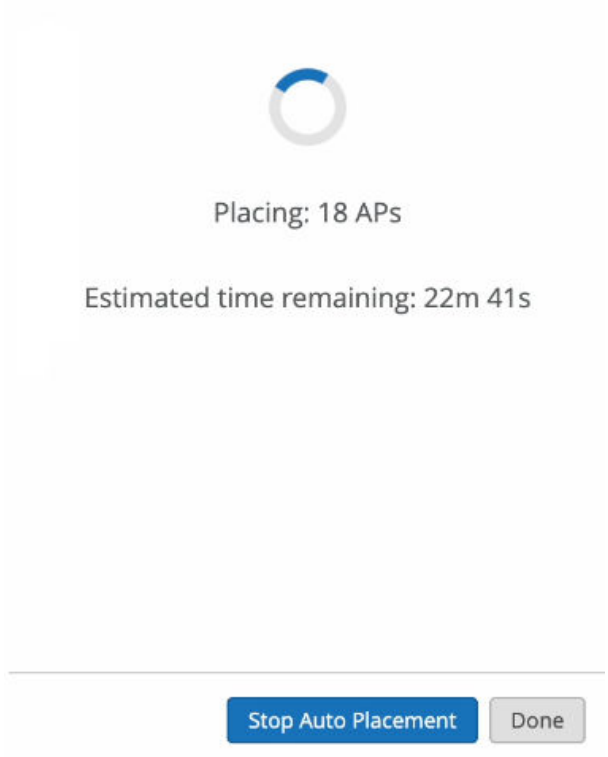


> **NOTE**: Optionally, you also can select APs from the **Available APs** list. The APs on this list have not yet been placed on the floorplan. Juniper Mist will add them to the floorplan during this process.

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.



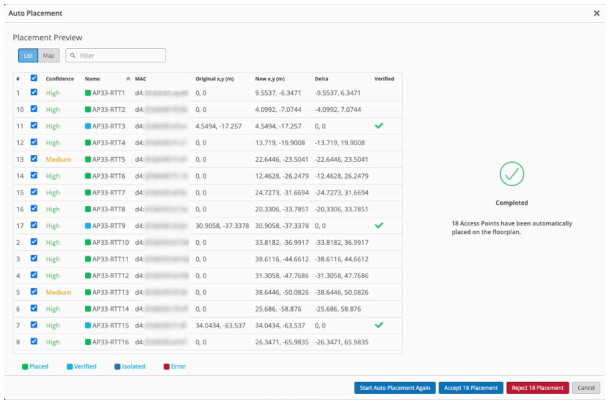
8. On the right side of the page, view the progress and final status message:

- 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.

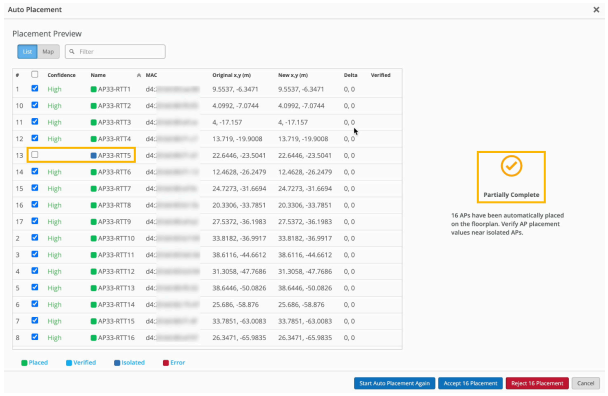
Evaluate the Results in the List View

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

Example: Placement Preview with Completed Status



Example: Partially Complete Autoplacement



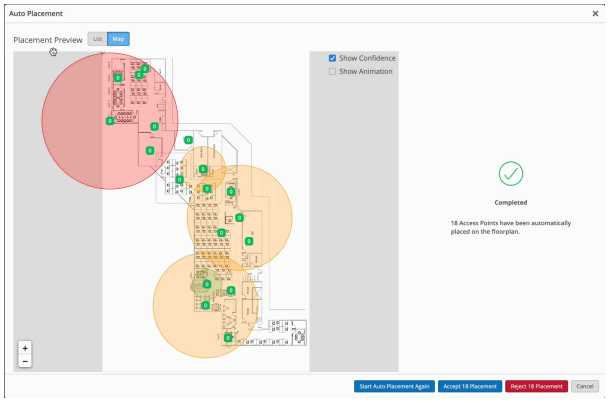
Icons

- 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.

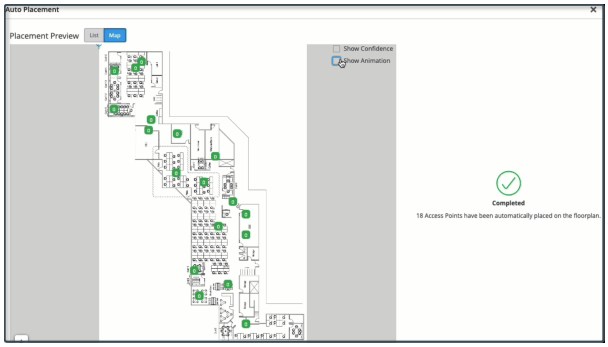
- A low confidence level (red) is associated with a larger radius area and indicates low certainty about the actual location of the APs. If Mist indicates a low confidence level, then you'll need to manually place the APs on your floorplan within the radius predicted by Mist. Note that Mist cannot place 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 autoplaced, 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 APs

SUMMARY

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.

You should only attempt autoplacement during a maintenance window. During the autoplacement process, wireless clients cannot connect to Access Points (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. Also see the requirements listed below.

Requirements for using autoplacement:

- The supported AP models for autoplacement are AP24, AP32, AP33, AP34, AP43, AP45, and AP47.
- The minimum required firmware version for autoplacement is version 14.28310.

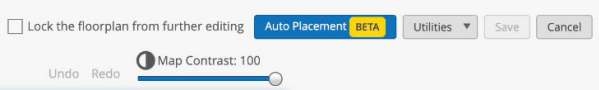
Before you use the autoplacement feature in a new deployment, ensure that:

- 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.

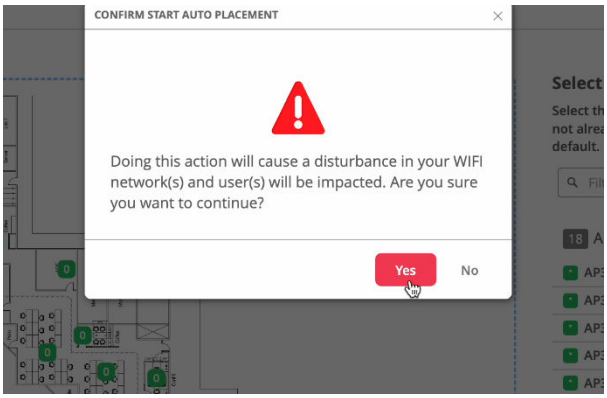
NOTE: If the preceding description doesn't fit your situation, see "Autoplacement: Verify AP Positions for an Existing Site" on page 64.

To place access points on a floorplan automatically:

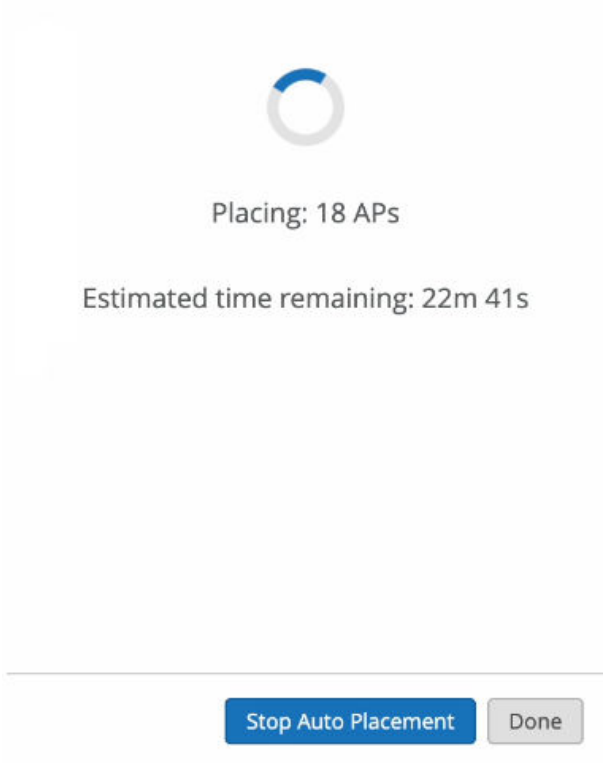
1. From the left menu of the Juniper Mist portal, select **Location** > **Live View**.
2. Select the site and the floorplan.
3. Click **Setup Floorplan**.
4. Click the **Auto Placement** button near the top right corner of the page.



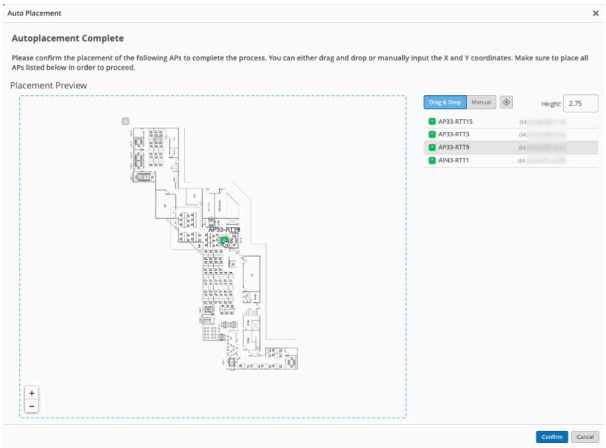
5. Select the APs that you want to place on the floorplan.
6. Click **Start Auto Placement**.
7. When the warning appears, read the information, and then click **Yes** to continue or **No** to cancel.



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:

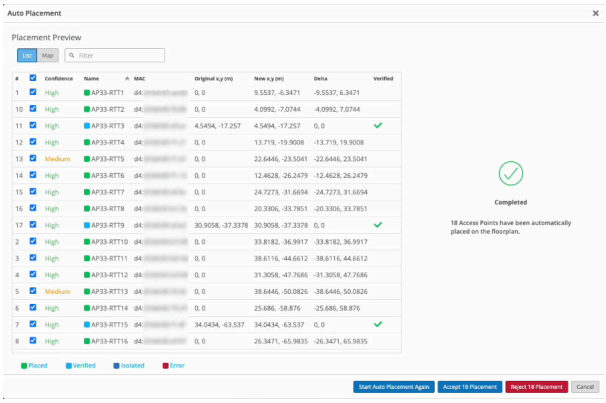
    - If you see the Placement Preview and a large check mark on the right side of the page, it indicates that the autoplacement process is complete. You can review the results and either accept or reject the results. See the Evaluate the Results section below.

    - 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.

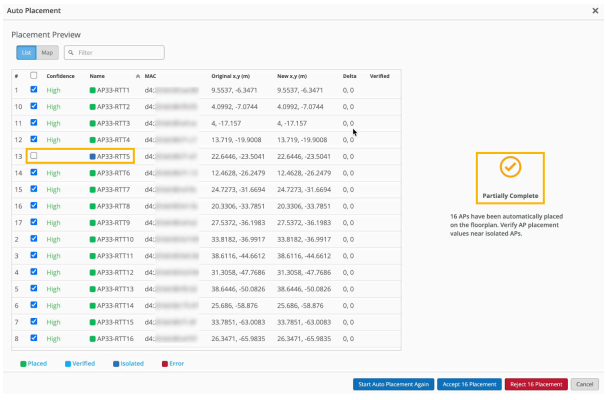
Evaluate the Results in the List View

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

Example: Placement Preview with Completed Status



Example: Partially Complete Autoplacement



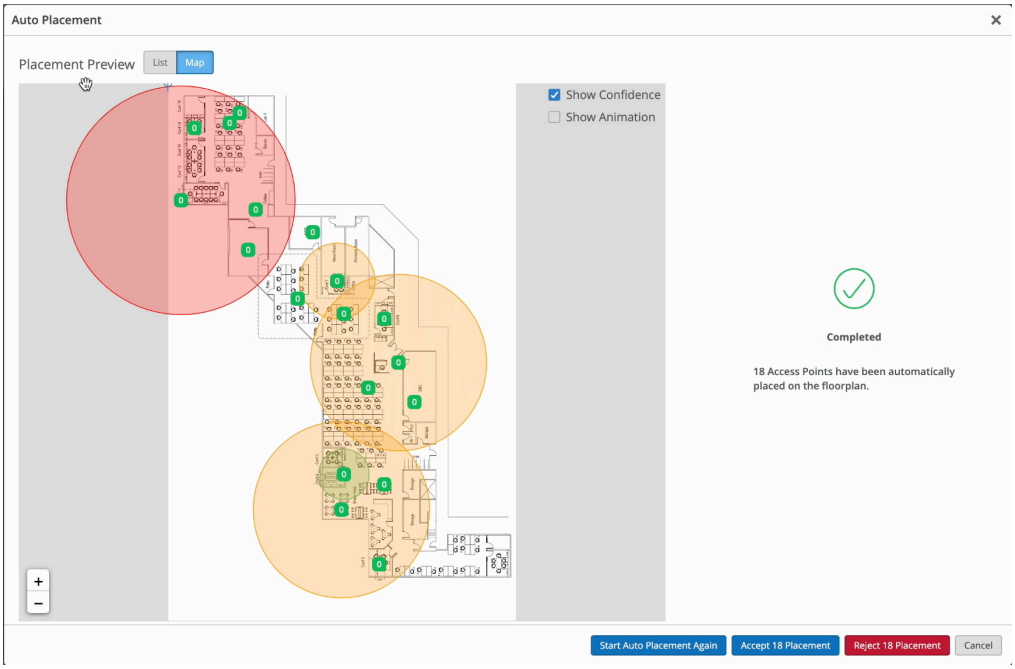
Icons

- 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.

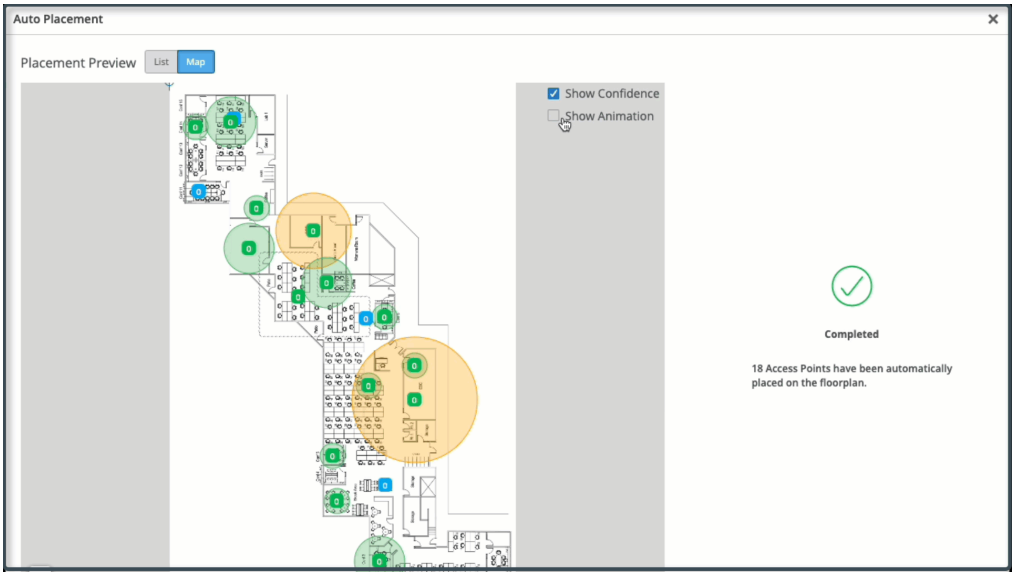
- A low confidence level (red) is associated with a larger radius area and indicates low certainty about the actual location of the APs. If Mist indicates a low confidence level, then you'll need to manually place the APs on your floorplan within the radius predicted by Mist. Note that Mist

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, select 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 APs

SUMMARY

After placing access points (APs) on your floorplan, ensure that they have the correct orientation to ensure location accuracy.

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 0.14.28310 or higher, and is only supported by the following AP models: AP24, AP32, AP33, AP34, AP43, AP45, and AP47.

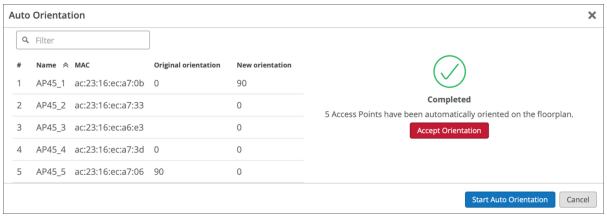
Before you use the Auto-Orientation feature, ensure that you have:

- 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 69 ***(optional)***.

To use Auto-Orientation:

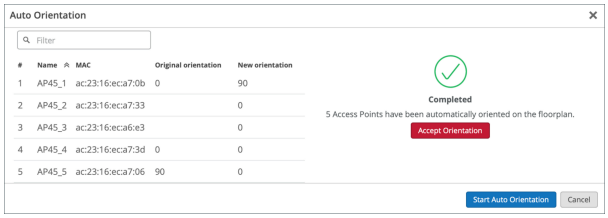
1. On the Juniper Mist portal, navigate to **Location** > **Live View.**
2. Select the applicable floorplan.
3. Select the **Setup Floorplan** button.
4. Select the **Auto Orientation** button.

5. Select **Start Auto Orientation**.



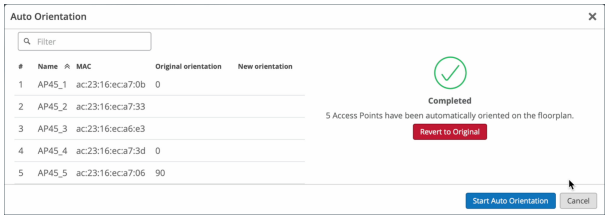
   Back on the Floorplan Setup section, you will see an “In Progress” status just below the Auto Orientation button. It will take 24 hours before you are returned with the rotation in degrees of the AP(s).

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.



RELATED DOCUMENTATION

Autoplacement: Position New APs | 69

Autoplacement: Verify AP Positions for an Existing Site | 64

Rename a Juniper AP

SUMMARY

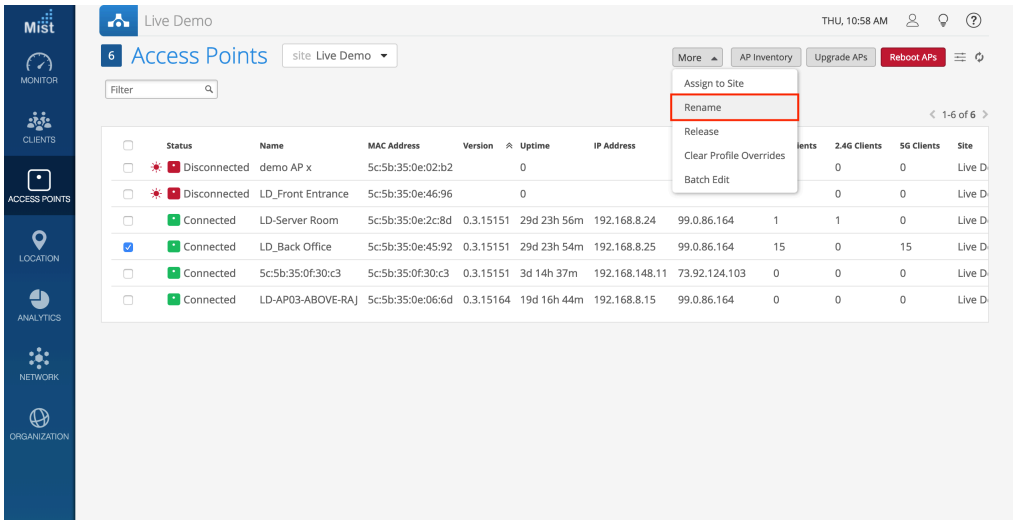
You can rename the access points (APs) on your network for easy identification. You can also use the Juniper Mist™ portal to automate the naming of APs by using variable fields in the name format.

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.

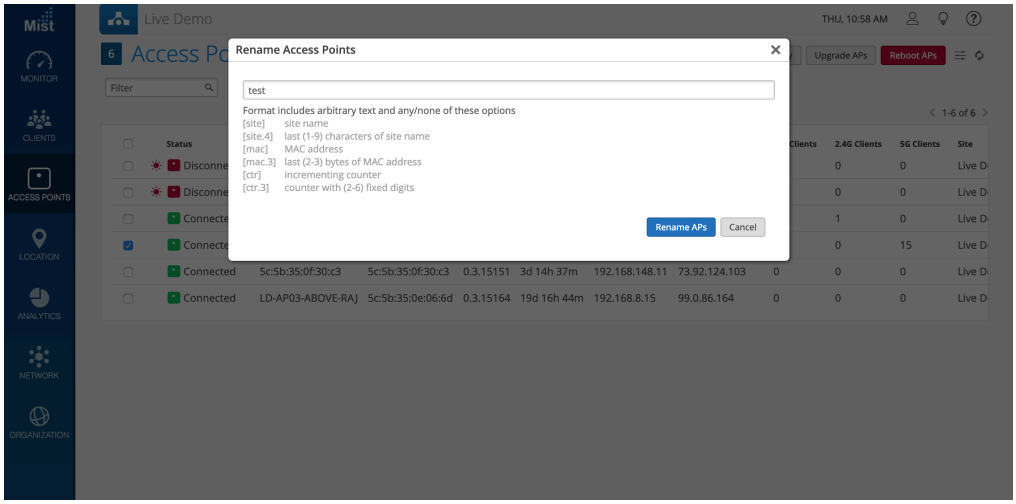
You can rename multiple APs at once. To rename APs in the Mist portal:

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**.

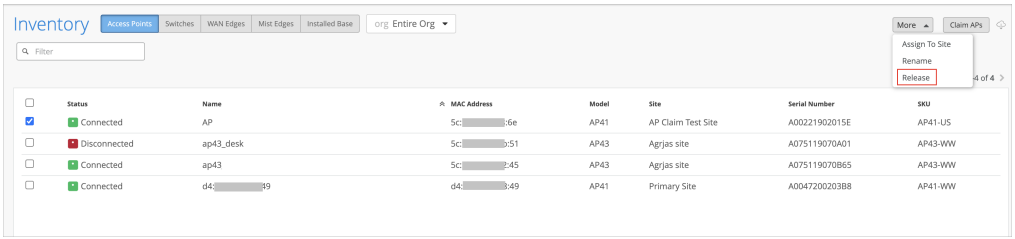
Release an AP from Inventory

SUMMARY

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

To release an AP from 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.

   The device configuration is deleted.

Upgrade the Firmware on a Juniper AP

SUMMARY

To ensure best performance, regularly upgrade your firmware. You can upgrade the firmware on a Juniper access point (AP) either manually or automatically.

IN THIS SECTION

With the automatic upgrade method, you can only upgrade the firmware, whereas you can use the manual process to upgrade or downgrade the firmware.

What Do You Want to Do?

Table 7: Top Tasks

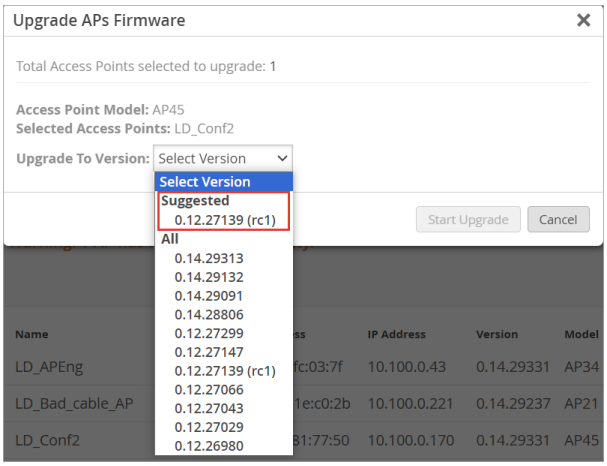
If you want to...	Use these resources:
Learn about Juniper version tags	"Firmware Version Tags for Juniper Mist Access Points" on page 80

Table 7: Top Tasks *(Continued)*

If you want to...	Use these resources:
See what updates are available	"Check for AP Firmware Updates" on page 81
Schedule regular updates to keep up with new releases	"Enable Automatic Firmware Upgrade" on page 82
Manually update the firmware yourself	"Manually Upgrade the Firmware on an AP" on page 85
Allow APs to get firmware updates from peers instead of the Cloud	"Enable Peer-to-Peer AP Firmware Upgrade" on page 88

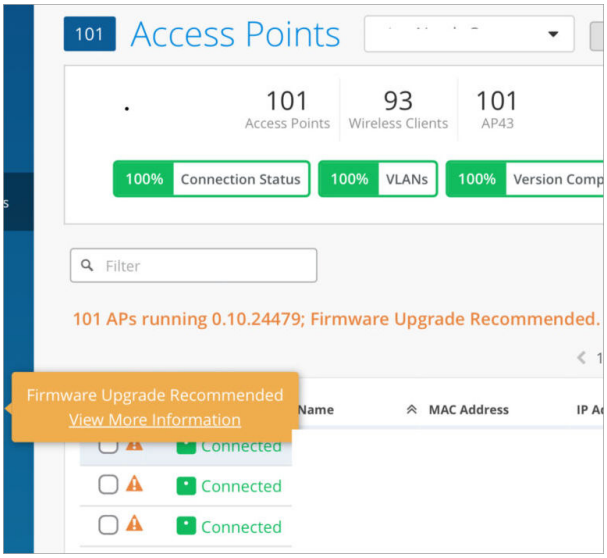
Firmware Version Tags for Juniper Mist Access Points

TheJuniper Mist™ portal displays the firmware versions that are supported on a specific AP model. Higher-numbered firmware versions contain all the fixes and features from the lower-numbered versions. Mist uses the rc1 tag to indicate a recommended firmware release for a specific AP model. Here's an example:



Untagged firmware versions are intended for demos and proof-of- concept purposes, allowing you to evaluate certain features or functionalities. These firmware versions have more recent bug fixes and functionalities than the rc1 firmware.

If an AP is running an obsolete firmware version, you'll see a notification on the Access Points page as shown in the following example:



For information on obsolete firmware and recommended firmware versions, see Firmware.

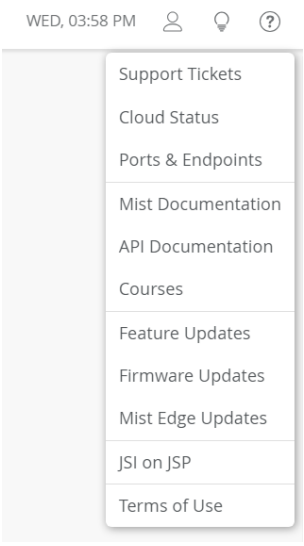
Check for AP Firmware Updates

SUMMARY

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 Automatic Firmware Upgrade

SUMMARY

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

IN THIS SECTION

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

Note that the auto upgrade process upgrades the firmware only if the specified firmware version is higher than the current version running on the AP.

You can configure auto upgrades as follows:

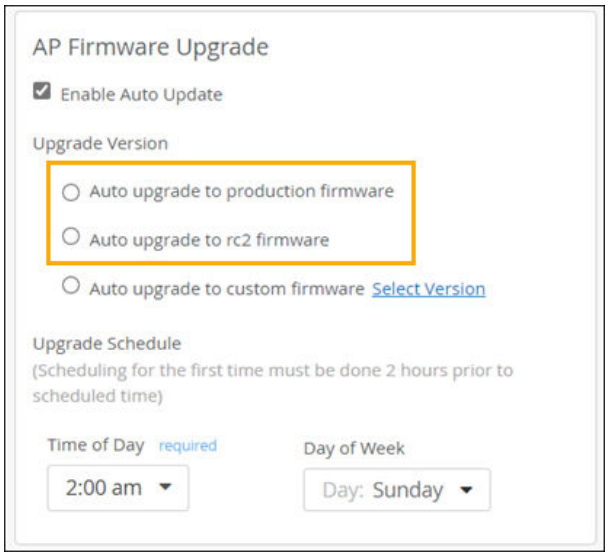
- Apply the latest production or beta firmware to all APs
- Apply a specific firmware to specific AP models

Apply the Latest Production or Beta Firmware to All APs

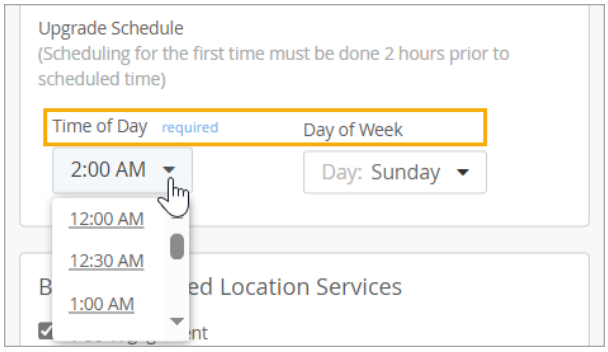
With this option, Juniper Mist will check weekly for available updates and apply them to all APs. You determine whether to install the latest production firmware or the latest beta release.

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

1. From the left menu of the Juniper Mist portal, select **Organization** > **Site Configuration**.
2. Select the site.
3. On the Site Configuration page, under AP Firmware Upgrade, select the check box for **Enable Auto Update**.
4. 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.



5. Under **Upgrade Schedule**, select the time and day when you want the upgrade to run, or select **Daily** as the **Day of Week** to run upgrades every day.



> **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.

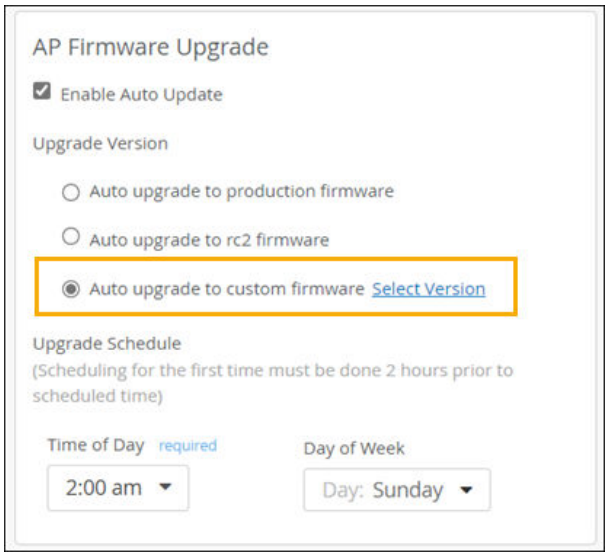
6. Click **Save** near the top-right corner of the page.

Apply Specific Firmware to Specific Models

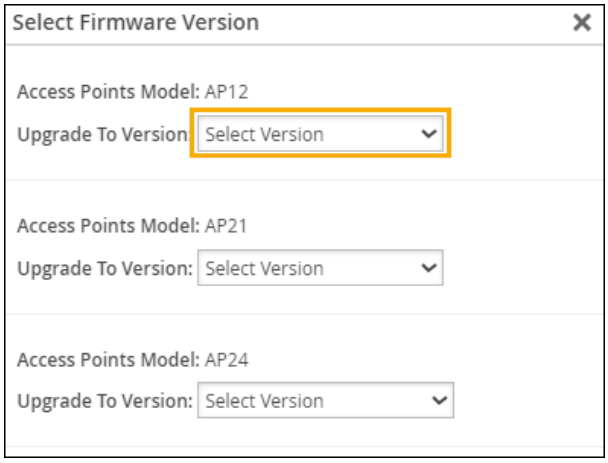
With this option, Juniper Mist will check the specified models in your AP inventory to see if they need to be upgraded to the firmware version that you specify.

To configure an auto upgrade to apply specific firmware to specific models:

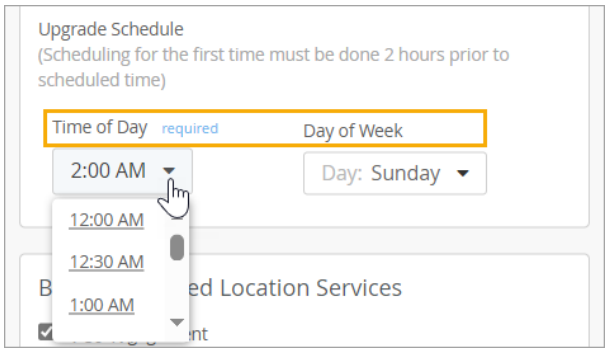
1. From the left menu of the Juniper Mist portal, select **Organization > Site Configuration**.
2. Under AP Firmware Upgrade, select the check box for **Enable Auto Update**.
3. Click **Auto upgrade to custom firmware**, and then click **Select Version**.



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



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.



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.

Manually Upgrade the Firmware on an AP

SUMMARY

For efficiency and to keep up with new releases, you'll typically use automatic upgrades. But when needed, you can upgrade the firmware 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.

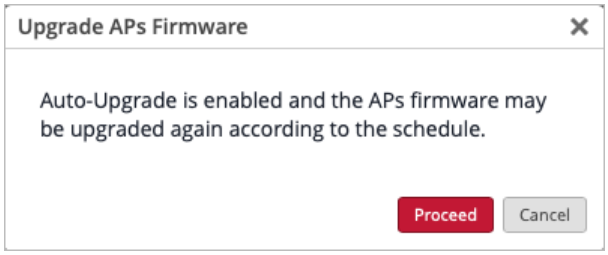
If your AP is part of a site that has auto updates enabled:

- You can either upgrade or downgrade the firmware version manually irrespective of the version configured for auto upgrade.
- If you manually upgrade the firmware to a version that is higher than the version configured for auto upgrade, then Mist will not run an auto update on the AP (as this would downgrade the firmware version on the AP).
- If you manually upgrade or downgrade the firmware to a version that is lower than the version configured for auto upgrade, then Mist will run the auto update process and upgrade the firmware version on the AP.

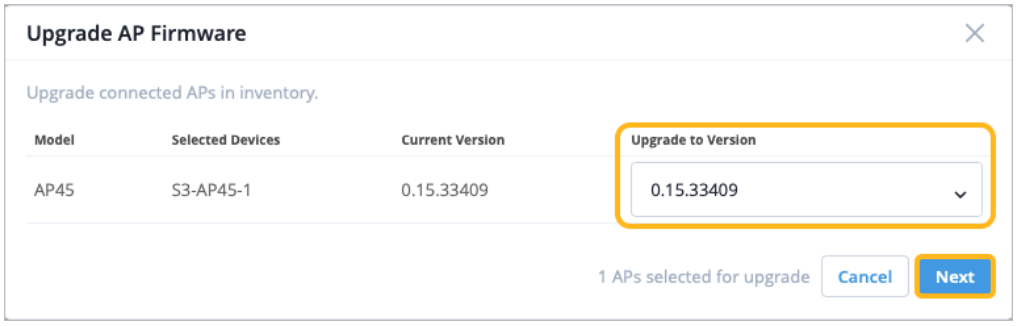
To manually upgrade the AP firmware:

1. From the left menu, select **Access Points**.
2. Use the Filter box to narrow down the list to show only the APs that you want to upgrade.

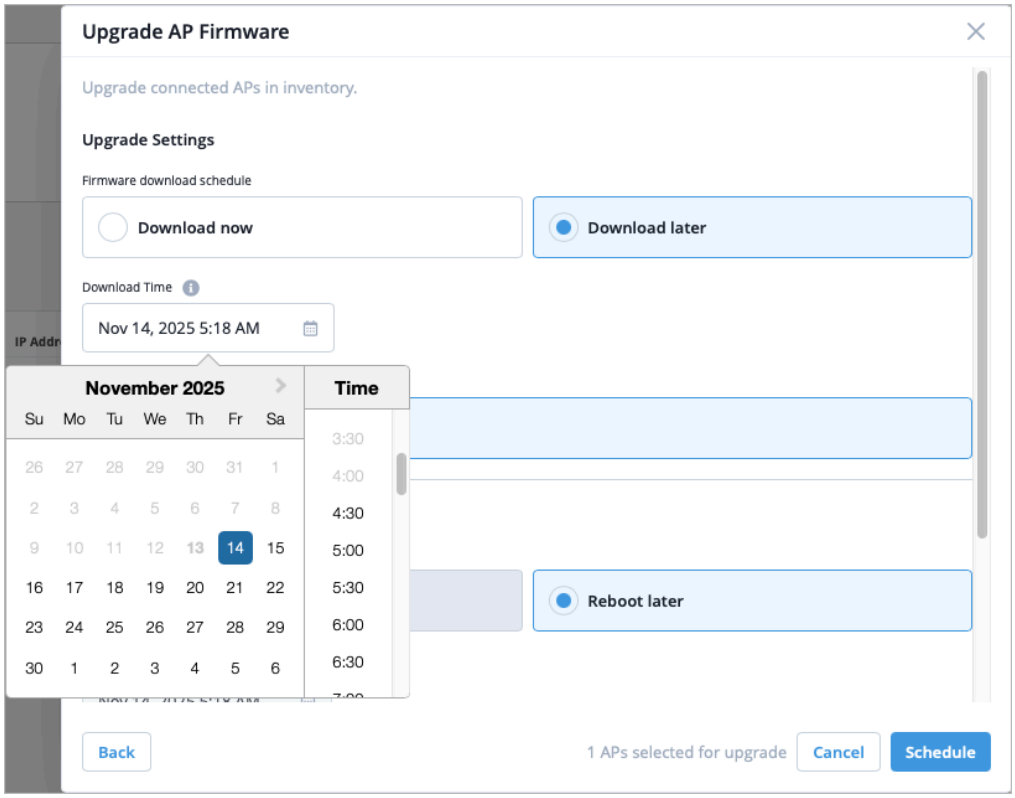
   For example, filter by entering tags, version number, or any of the fields listed in the table.
3. Select the APs that you want to update.
4. Click the **Upgrade APs** button in the top-right corner of the **Access Points** page.
5. The **Upgrade APs Firmware** window appears. Click **Proceed**.



6. Select the firmware version to upgrade to, then click **Next**.



7. In the **Upgrade Settings** section of the window, you can choose **Download now** or **Download later.**.
   a. If you select **Download now**, the Reboot schedule will be set to **Reboot now**, but you can optionally choose **Reboot later**.
   b. Choosing **Download later** prompts you to set a date and time for the firmware download to occur. This will automatically select the **Reboot later** option in the Reboot Settings section of the window. The **Reboot Time** is set to the same date and time you chose for the Download time.



8. Click **Schedule**.
   You will see a blue banner appear at the top of your screen stating that the firmware download has started.

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

Enable Peer-to-Peer AP Firmware Upgrade

SUMMARY

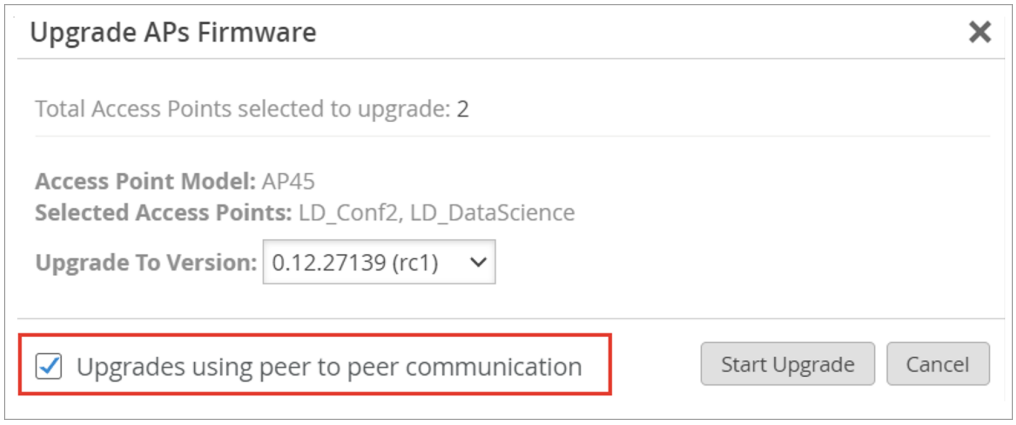
When doing manual upgrades, you might find it convenient and time-saving to allow APs to get their firmware from peer APs instead of going to the cloud.

This is a useful option when you need to upgrade many APs of the same model.
Juniper 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.



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.

Configuration

IN THIS SECTION

Auto-Provision Device Names, Sites, and Device Profiles

SUMMARY

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.

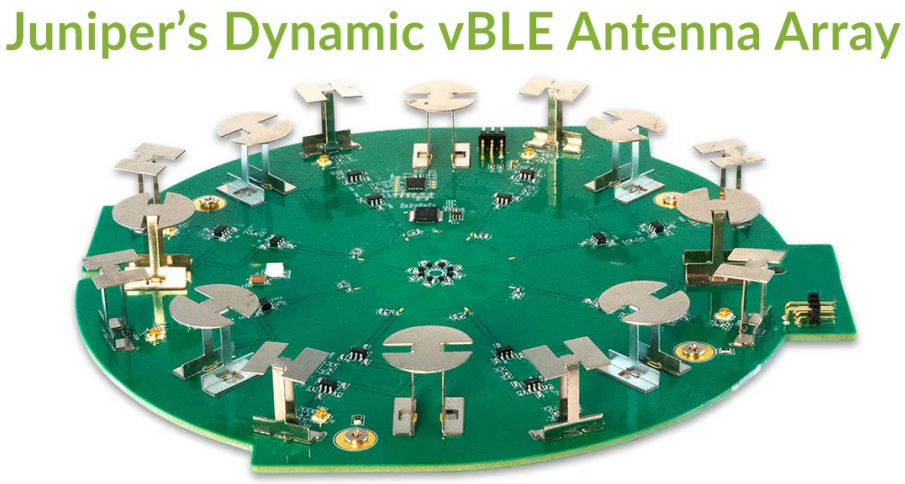
BLE Settings

SUMMARY

Understand the benefits and uses of virtual Bluetooth Low Energy (vBLE). Adjust the settings to support your organization's use cases.

Most Juniper APs have built-in 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 7: vBLE Antenna Array



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).

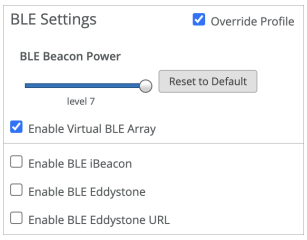
You can use device profiles or the device-level configuration page of the AP to configure BLE settings:

- 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.

  - **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.



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

Configure Ethernet Settings in a Device Profile

SUMMARY

Although you typically won't need to configure the Ethernet ports for your Juniper Mist access points (APs), when needed you can enable features such as PoE passthrough and enable or disable interfaces.

IN THIS SECTION

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.

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.

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

Configuration Steps

To configure the Ethernet ports for APs attached to a device profile:

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

NOTE: You can also configure the settings for an individual AP. From the Mist portal, click **Access Points**, click an AP, and scroll down to the **Ethernet Properties** section in 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)

[ ]

[ ] Port VLAN ID (optional)

[ ]

802.1X Supplicant

(!) requires firmware v0.14.x or higher

(•) Enable ( ) Disable

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

2. Enable **PoE Passthrough** if you want to extend power from an AP to its enabled Ethernet ports.

3. Configure the Ethernet ports. Note that 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.

   - **List of VLAN IDs (Eth0 port)**—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.

   - **List of VLAN IDs (Eth1, Eth2, Eth3, and Module ports)**—Enable or disable individual Ethernet ports on the AP, as available. 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. For more information, see Configure Your Access Points as IEEE 802.1X Supplicants

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

The exact Power over Ethernet (PoE), Ethernet port specifications, 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

Hardware for Your Wireless Network | 9

Configure Ethernet Settings in a Device Profile | 92

Configure IP Settings

SUMMARY

Configure the IP settings for your access points (APs) individually (for special use cases) or in the device profiles (for consistent settings across similar devices).

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 willl have to do a factory reset on the AP to get back to VLAN=1.

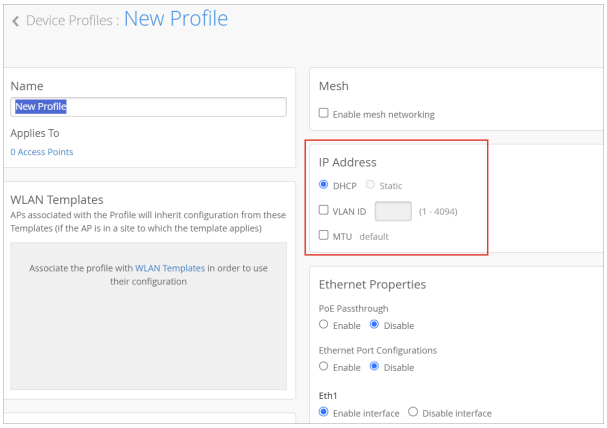
If the AP cannot obtain an IP address, the LED will blink three times. See "What Does the AP Status LED Indicate?" on page 392.

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.



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.

Wireless Mesh Network Configuration

SUMMARY

To cover a wider area than a single AP could do on its own, consider configuring a wireless mesh network.

IN THIS SECTION

A mesh network is a group of connectivity devices, such as APs that act as a single network. With a mesh network, you can have multiple sources of connectivity around your location instead of a single point of access.

Using APs in mesh mode expands the coverage area for your deployment. APs leverage neighboring APs to relay traffic to and from a base AP that is connected to the access switch.

Mist supports single hop mesh—the interconnection between the APs is single, wireless hop, and occurs automatically after setup. In a mesh, APs are classified as a *base* or *relay*. A base has an Ethernet connection to an uplink switch. The relay AP connects to the base AP through a wireless mesh link. If a base AP goes offline, the relay APs can automatically failover to another base AP. You can create mesh groups so that a base AP will only accept failovers from relay APs that are members of a given group.

Mist also supports mesh on Dynamic Frequency Selection (DFS) channels. DFS channels are a group of channels that are located in the UNII-2 and UNII-2-extended bands where Wi-Fi coexists with Doppler weather radar, commonly located in airports. The AP switches to a new channel if it detects radar, in which case it will advertise a Channel Switch Announcement. When switching channels, if the AP selects a non-DFS channel, it begins sending Wi-Fi beacons right away (these beacons advertise the available SSID and data rates). However, if the new channel is another DFS channel, the AP will perform a 60-second channel availability check (CAC) before sending any beacons.

Enable Wireless Mesh

Before you set up a mesh, ensure that all the APs have a wired connection to the Mist cloud so that they can receive the configuration. After that, you can disconnect wired links from the APs.

If you intend to set up wireless mesh at scale, we recommend that you use "device profiles " on page 127 to save time and simplify management. In such as case, you would create one profile for the base APs and another for the relay APs and then attach the various APs to the correct device profile according to role.

To enable wireless mesh:

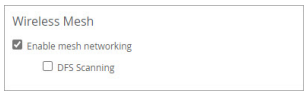
1. Enable mesh networking at the site level:

   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 Wireless Mesh section of the page and select the **Enable mesh networking** check box.

      If you enable DFS scanning, the relay AP will scan for the base APs on both DFS and non-DFS channels.

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

2. Designate the base and relay APs:

   a. From the Mist portal, click **Access Points**.

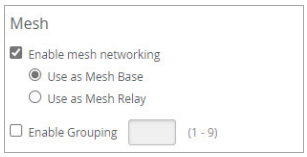
   b. Click an AP.

   c. Scroll down to the **Mesh** section.

   d. Select **Enable mesh networking**.

e. Choose the role you want for the AP, 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).



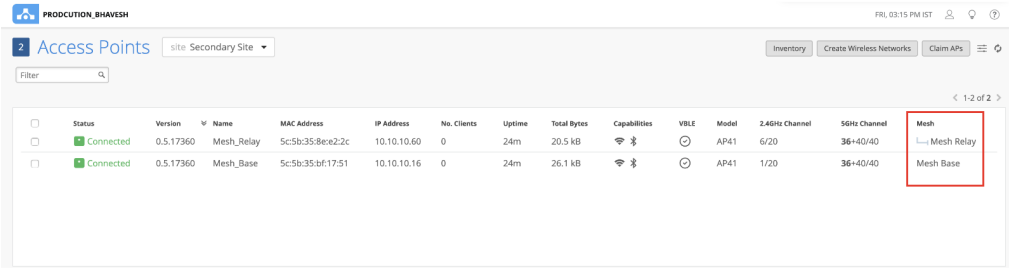
f. (Optional, to control failover with multiple mesh links in a site) Click **Enable Grouping** and enter a group number (1 through 9) to control which relay APs can failover to a given base AP.

You can create mesh groups so that a base AP will only accept failovers from relay APs that are members of a given group. Assign a group number (1 through 9) to the relay APs, and then configure the base AP to only accept failover connections from relay APs with that group number.

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

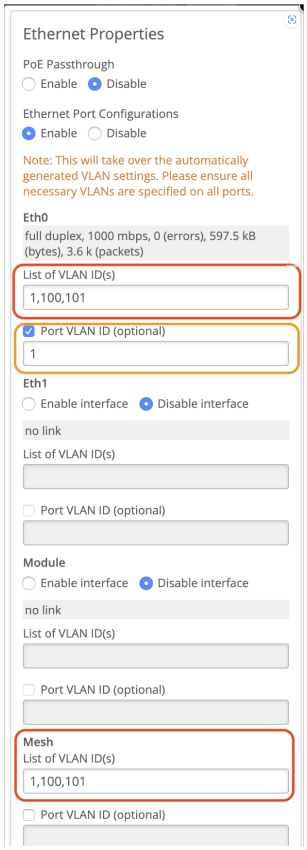
h. After you configure an AP as a relay AP, wait for a few seconds before removing its wired uplink to the switch. Ensure that the relay AP is connected to a power adapter

The relay AP will now be connected to the base AP. In the Access Points page, you can see which of your APs are set as base and relay. You'll need to enable the Mesh column in the display menu.

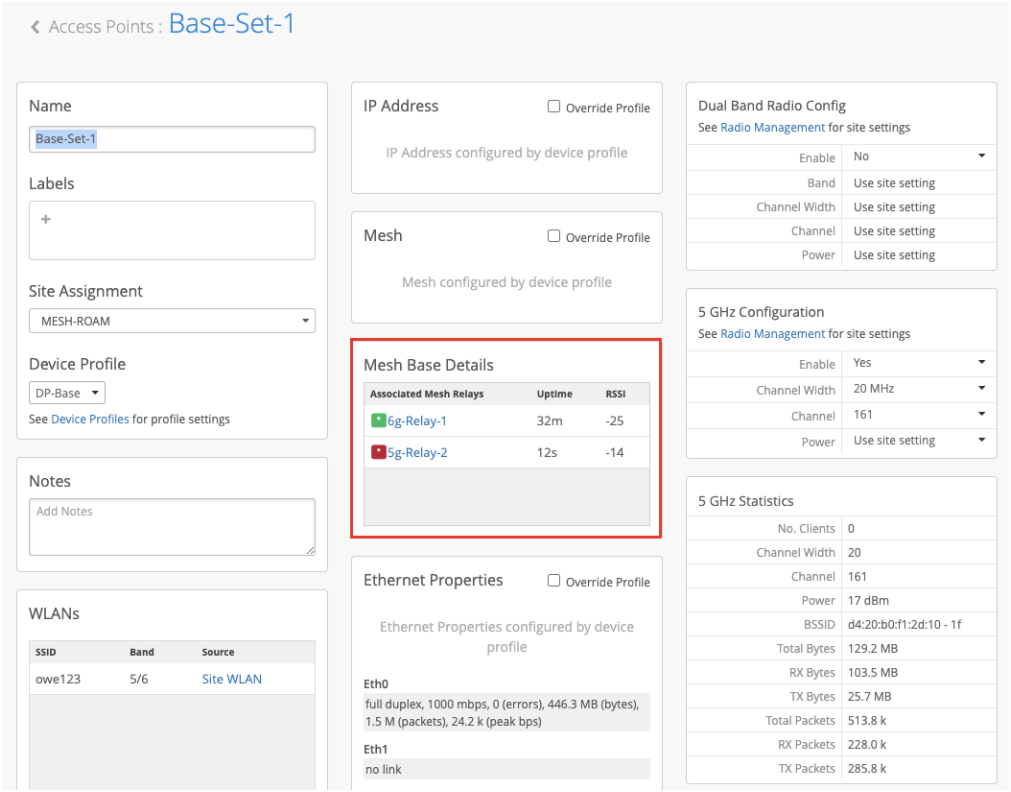


If you have any SSIDs broadcasting on the relay AP but not on the base AP, specify the SSID VLAN ID(s) on the Eth0 or Eth1 port of the base AP in the **Ethernet Properties** section.

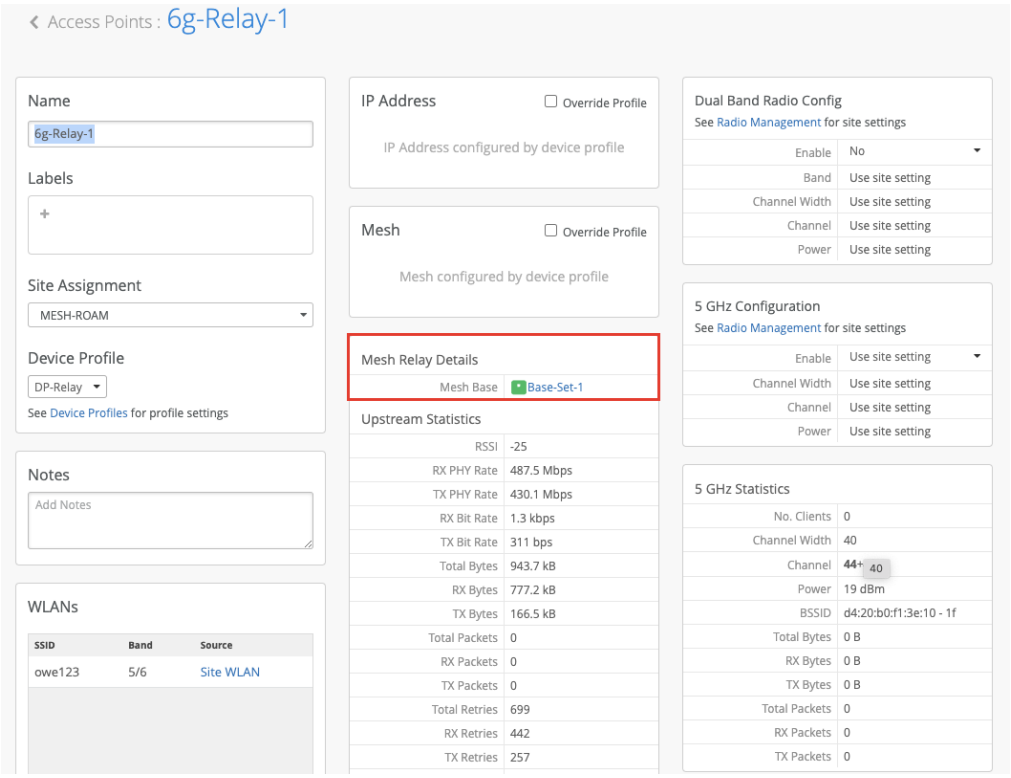
Here's an example that shows the Eth0 settings on the base AP with VLAN IDs 1, 100, and 101. VLAN 1 is the management VLAN of the AP. You must specify this value in the **Port VLAN ID** field or else the AP will disconnect from the cloud. VLAN 100 and VLAN 101 are for tagged SSIDs, which are broadcasting on the relay AP but not on the base AP.



The AP configuration page for the base and relay APs display the mesh details if the mesh is set up correctly. In the following example, you'll see the details of the relay APs on the base AP configuration page.



Similarly, the configuration page for the relay AP will display the details of the base AP that it connects to.



AP Mesh Use Cases

IN THIS SECTION

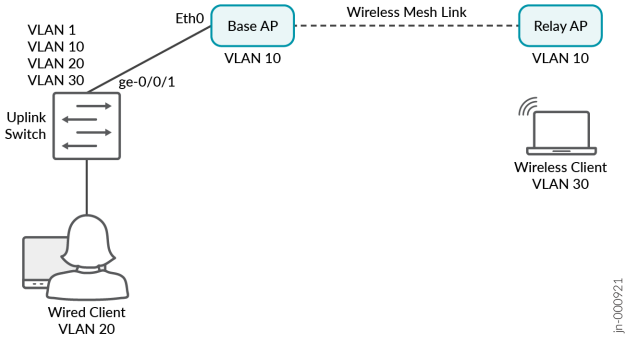
Use Case 1: Extend WLANs over Mesh

IN THIS SECTION

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 the base AP gets connected) = 10,20,30
- Management VLAN (through which the APs will get the IP address)= 10
- Wireless SSID B= tag with VLAN 30
- Wireless client should get an IP address from VLAN 30.
- Both base and relay APs should get an IP from the management VLAN 10.

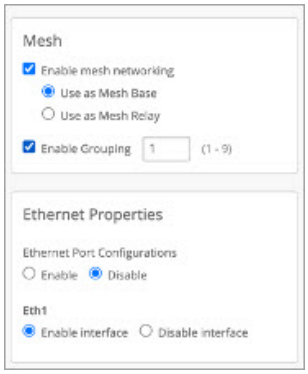
Procedure

1. Configure the uplink switch port by using the following commands:

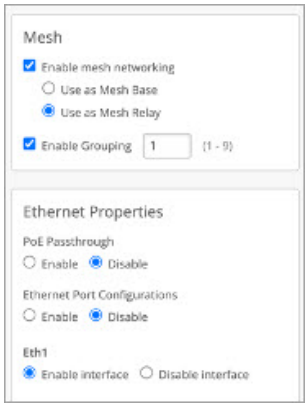
   ```
   set interfaces ge-0/0/1 native-vlan-id 10

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

   See Add or Delete a CLI Configuration for information about adding CLI configurations to a switch from the Mist portal.

2. Designate the base AP in the AP configuration page as shown.



3. Designate the relay AP in the AP configuration page as shown:



4. Configure the WLAN for the wireless clients to connect to the base or relay AP. In this example, the clients will obtain an IP address from VLAN 30.

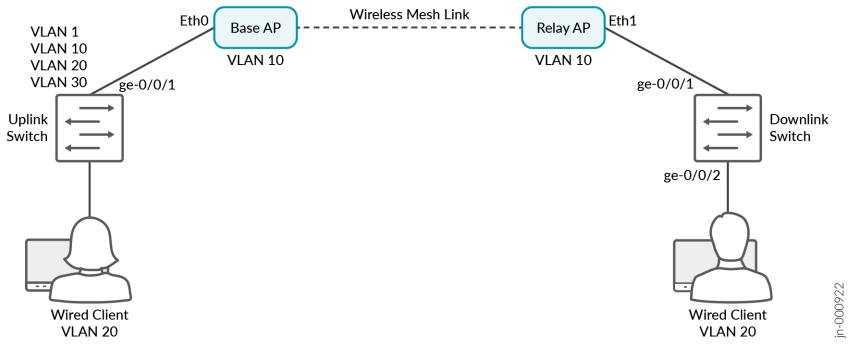
Use Case 2: Connecting a Switch on a Relay AP

IN THIS SECTION

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. 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" on page 102, but we also need to enable the Ethernet port configurations in order to pass VLAN 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.

Procedure

1. Configure the uplink switch ports by using the following commands:

   - 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]`

   See Add or Delete a CLI Configuration for information about adding CLI configurations to a switch from the Mist portal.

2. Configure two ports on the downlink switch port:

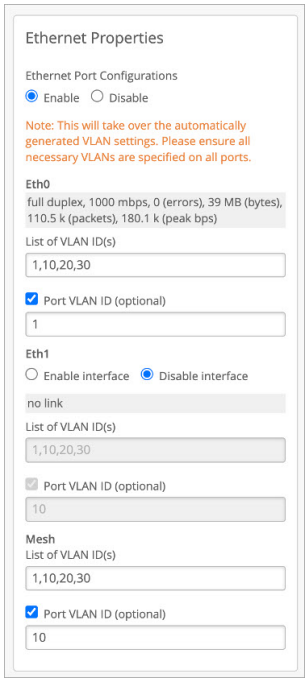
   - ge-0/0/1

     - `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]`

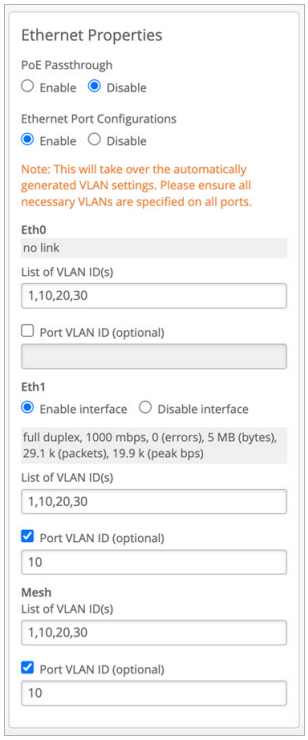
   - ge-0/0/2

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

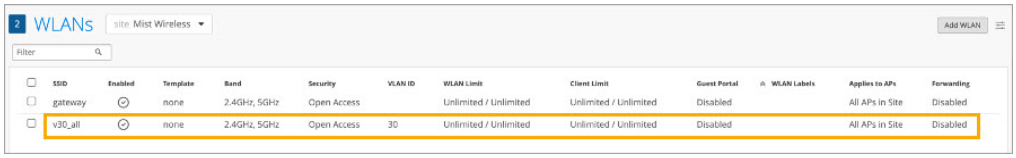
3. Designate the base AP. Enable mesh, as in "Use Case 1" on page 102. Also enable Ethernet port configurations and enter the settings.



4. Designate the relay AP. Enable mesh, as in "Use Case 1" on page 102. Also enable Ethernet port configurations and enter the settings. In this example, you'll see that wired clients connecting to Eth1 on the relay AP will get the IP address on VLAN 10.



5. Configure the WLAN:



FAQs: AP Mesh Configuration

IN THIS SECTION

Can I configure a mesh using different AP models?

Yes.

Can I configure a mesh using APs running different firmware versions?

We recommend that you use APs running the same firmware version.

Can I deploy one mesh relay AP for multiple mesh base APs? If yes, how many mesh base APs can be deployed? Will the mesh base APs support failover?

Yes, it is possible to deploy multiple mesh relay APs on one mesh base AP. We recommend not to exceed 4 mesh relay APs, which we have tested in our environment. A failover from one base AP to another can occur if the signal is weak or if the first base AP goes down.

Will clients connected to a mesh relay AP have a lower throughput than clients connected to a mesh base AP?

If both the mesh and client are on the 5 GHz band, the bandwidth available for the client is shared. Although the bandwidth is shared, it has a minimal impact on the overall throughput. Mist supports only single hop mesh. In multihop mesh, bandwidth is reduced at every mesh hop.

What is the recommended distance between a mesh base AP and a mesh relay AP?

The distance is dependent on the AP models and antenna types.

Enable RTLS Support

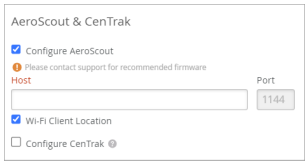
Juniper APs can support Real-Time Location System (RTLS), or asset tracking systems, including AeroScout and Centrak. These systems use Wi-Fi tags to send a proprietary beacon to the Juniper AP, which receives the signal and sends data to the RTLS. You can set this up individually on selected APs, or in a device profile, so that all supported APs attached to the device profile can inherit the settings.

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.

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 AP:

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.

Electronic Shelf Labels

SUMMARY

Understand the requirements to support electronic shelf labels, and enable this feature on supported access points (APs).

IN THIS SECTION

Electronic shelf labels (ESLs) are small, battery-powered electronic paper (e-paper) displays that provide product and pricing information at the shelf edge, replacing paper labels. ESLs use wireless technology to communicate with a central hub to form a dynamic pricing automation network.

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.

Mist supports the following ESL systems:

- ESL supported by USB (version 0.12x and beyond)
  - SES-Imagotag HF USB Dongle (Proprietary technology; up to 15000/min ESL tags)
  - SES-Imagotag BLE USB Dongle (BLE SIG core 5.4; up to 15000/min ESL tags)
  - SoluM USB dongle (Proprietary technology; up to 15000/min ESL tags)
  - Hanshow USB dongle (Proprietary technology; up to 15000/min ESL tags)
- ESL native BLE supported
  - SES-Imagotag BLE (BLE SIG core 5.4; up to 15000/min ESL tags)

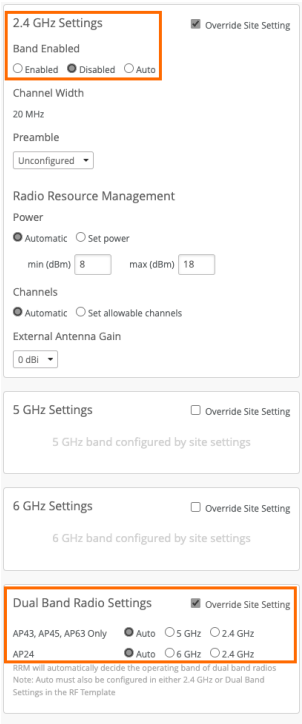
As a general guideline, you can assume each AP can support from 7,000 to 15,000 ESL tags depending on the vendor and AP model. The following AP models support ESL:

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

Requirements

To support ESL, you must be running AP firmware version 0.14x or 0.15x. Depending on the 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 as shown below.

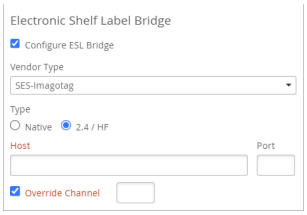


Enable ESL

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 the **Configure ESL Bridge** check box.
3. Select the **Vendor Type**. Mist supports SES-Imagotag, SoluM, and Hanshow.
4. 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.
5. Complete the configuration with the following settings:
   For SES-Imagotag:
   - **Host**
   - **Port**
   - **Override Channel (available only for the 2.4/HF ESL type)**



   For Hanshow and Solum, enter the VLAN for separating traffic.

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

You can also enable ESL for an AP from the Access Points page.

Enabling LEDs on the AP

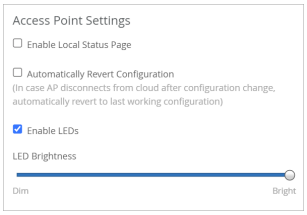
SUMMARY

Configure your site settings to enable access point (AP) LEDs to indicate operational status and help you to 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

Troubleshoot a Juniper Access Point

Configure an AP for Survey Mode

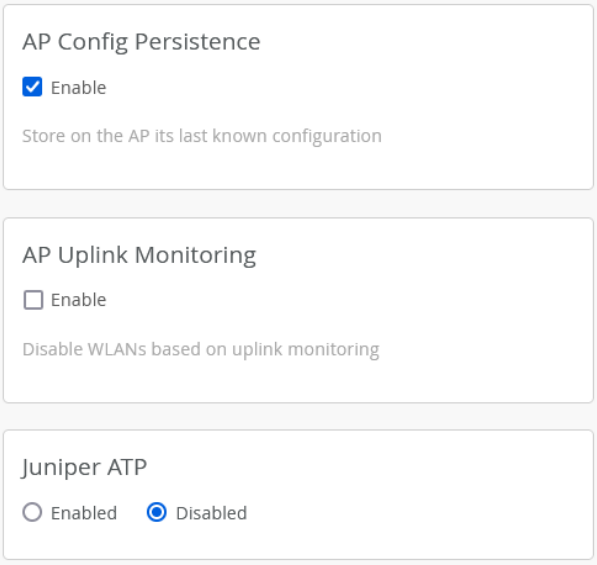
SUMMARY

To plan where to deploy your access points (APs), onboard one AP and enable site survey mode so that you can use this AP to test wireless coverage throughout your site.

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 AP" on page 42 and "Assign APs to Sites" on page 45.
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.

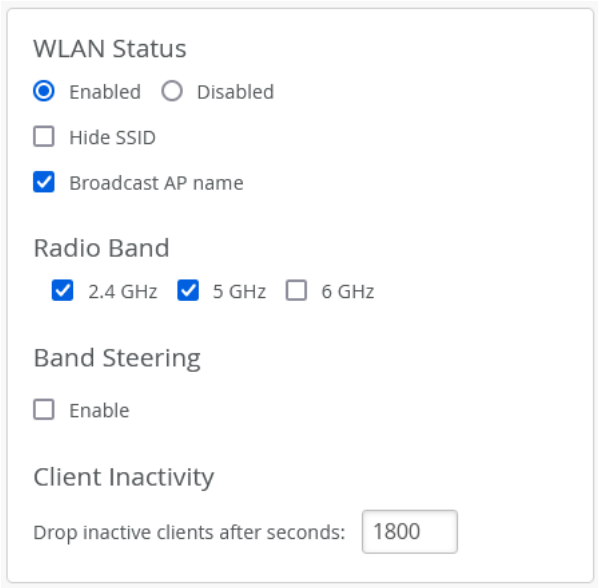


   The AP stores the complete configuration if AP configuration persistence is enabled for your site. When the AP is unable to connect to the Juniper Mist cloud, the AP can reboot from this stored configuration and continue to transmit beacons.

   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 235.

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.



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 APs as IEEE 802.1X Supplicants

SUMMARY

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

IN THIS SECTION

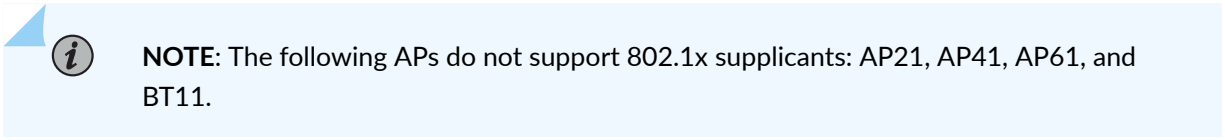
Certain models of Juniper Mist APs can authenticate to their uplink wired switch by using IEEE 802.1X authentication. When 802.1X authentication is implemented, the switch blocks traffic to the AP at the port until its credentials are presented and matched on the authentication server (a RADIUS server).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

To get the 802.1X supplicant feature working on your supported 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.

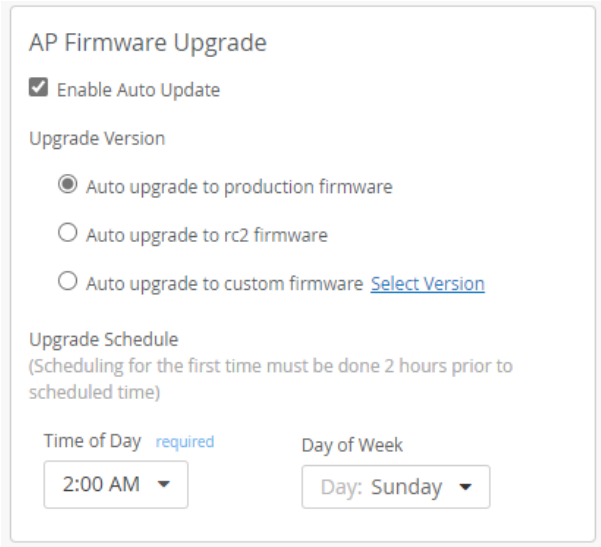


NOTE: The following APs do not support 802.1x supplicants: AP21, AP41, AP61, and BT11.

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.
3. Under AP Firmware Upgrade, select **Enable Auto Update**.
4. Under Upgrade Version, select **Auto upgrade for production firmware** to get the latest firmware.



5. Select the **Time of Day** and **Day of Week** when you want the auto-upgrade to run.

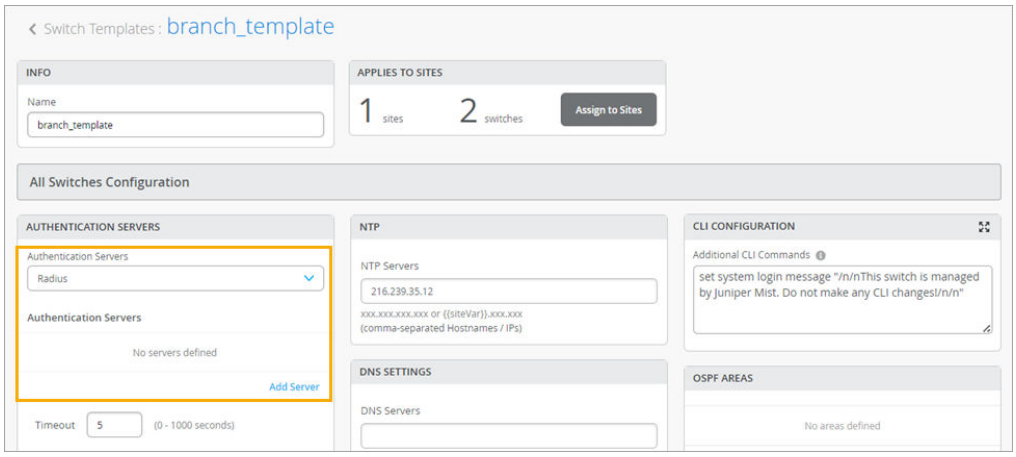
   Allow at least 2 hours for the new settings to take effect. For example, if you are configuring these settings at 2 PM and you want to update your APs today, set the time to 4 PM or later.
6. Click **Save** near the top-right corner of the Site Configuration page.

Enable 802.1X in the Switch Port Profile

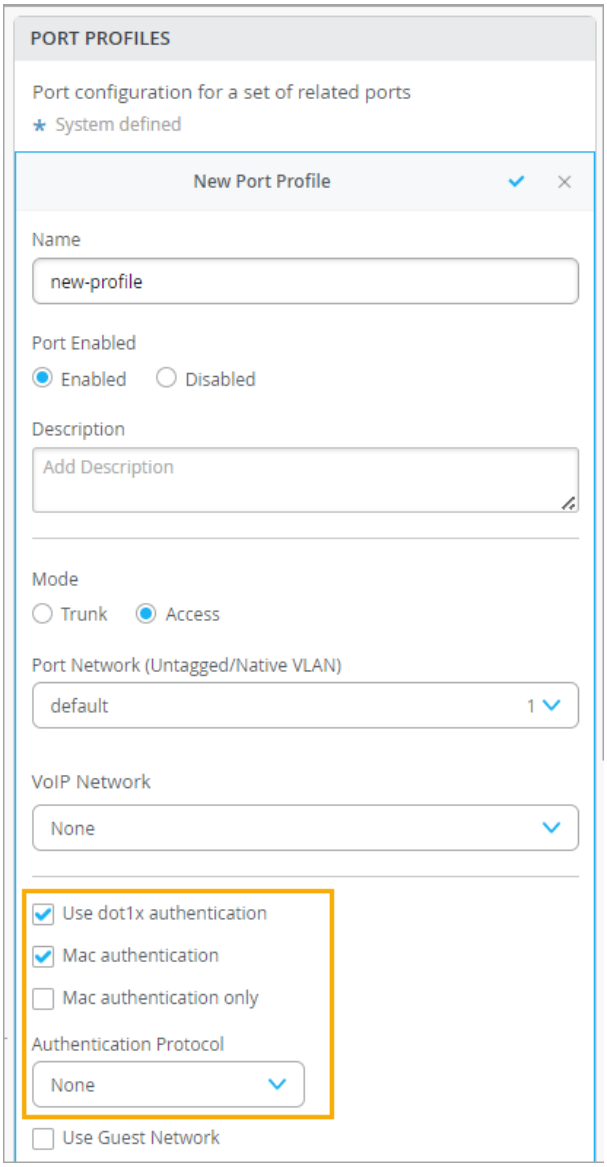
On your switch, enable 802.1X authentication for the ports that your APs connect to. We recommend using a Guest VLAN, server reject VLAN, or MAC auth fallback with a default VLAN that allows AP connectivity to the Mist Cloud, at least for initial deployment of the site. This way, APs can safely connect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

To configure 802.1X in the Port Profile:

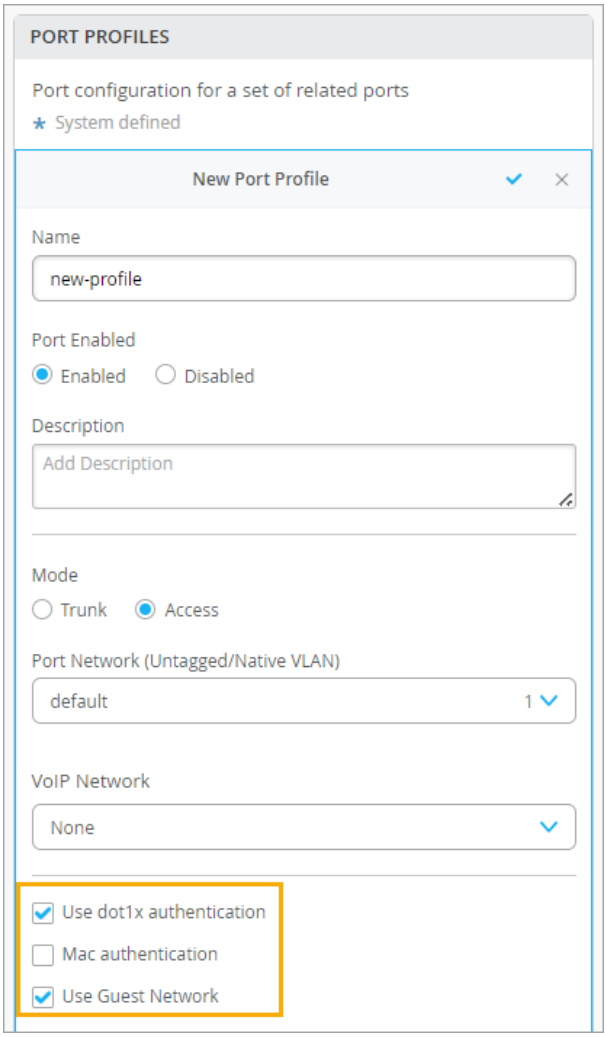
1. Select **Organization** > **Switch Templates**, and then click the switch template that you want to configure.
2. In the **Authentication Servers** section, add your RADIUS servers.



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).



- 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).



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 120.

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:

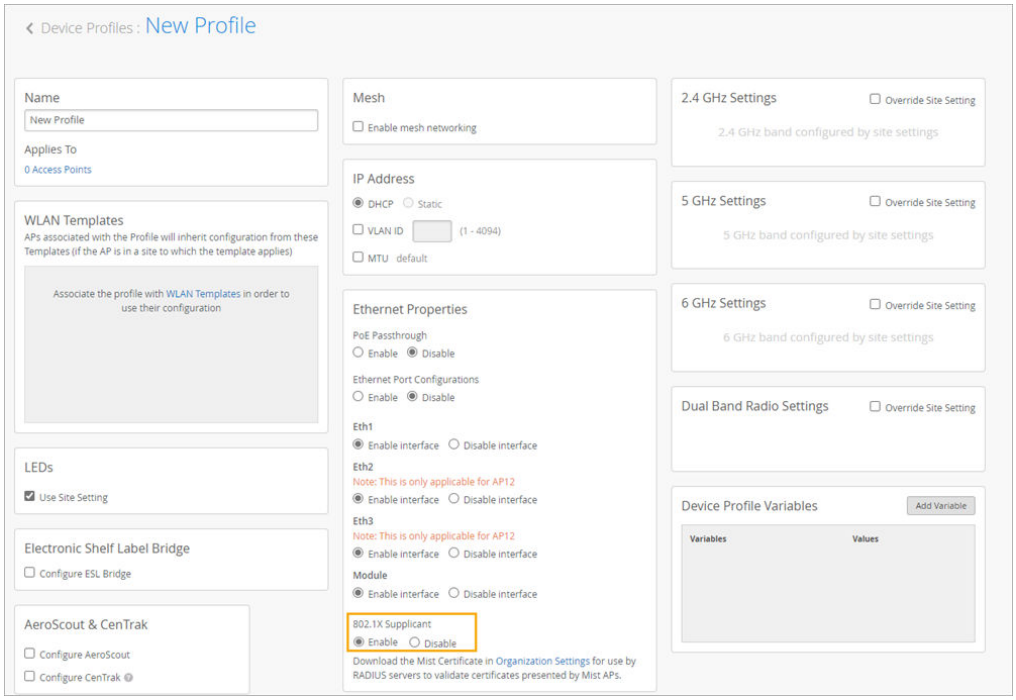
```
001094001144 Cleartext-Password := "001094001144“
      Tunnel-Type = VLAN,
      Tunnel-Medium-Type = IEEE-802,
      Egress-VLAN-Name += 1vlan-2,
      Egress-VLAN-Name += 2vlan-3,
```

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**.

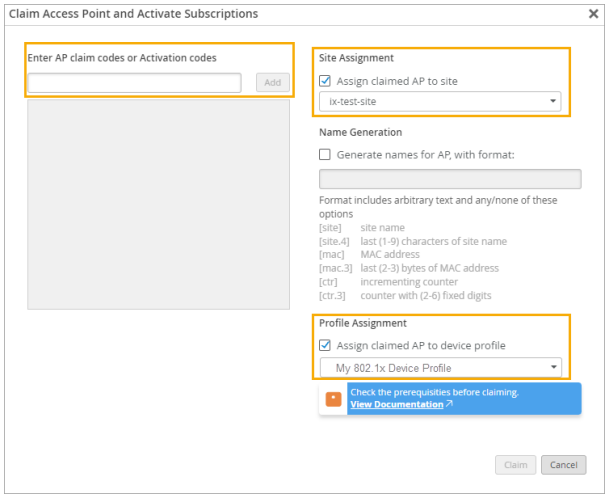


4. Configure any other desired settings for this device profile.
5. Click **Save** near the top-right corner of the Device Profile page.

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.



4. Click **Claim**.

Access Assurance Configuration

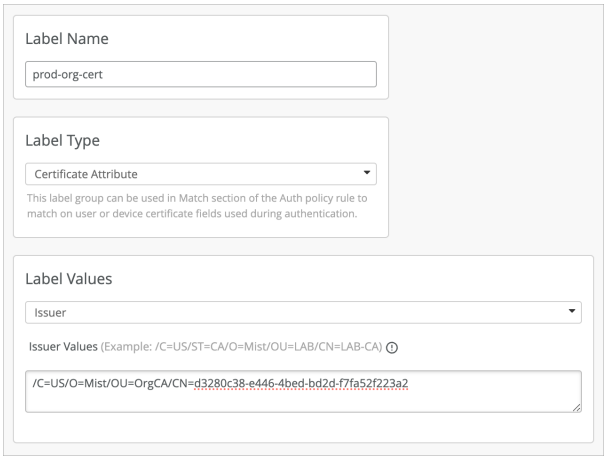
IN THIS SECTION

If you are a Juniper Mist Access Assurance customer, the configuration is extremely simple. You only need to create a label and a policy to match on for the AP authentications and optionally return configuration back to the switch. Juniper Mist Access Assurance automatically knows about the organization's CA, and does not need to be manually added into the certificate store.

Auth Policy Label

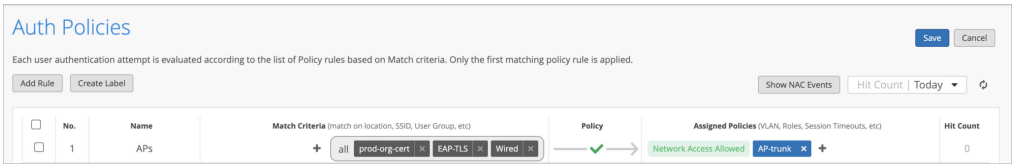
Here is an example label to match the AP authentications. The label type is Certificate Attribute with the value set to Issuer. The value is your Org ID.

```
/C=US/O=Mist/OU=OrgCA/CN=d3280c38-e446-4bed-bd2d-f7fa52f223a2
```



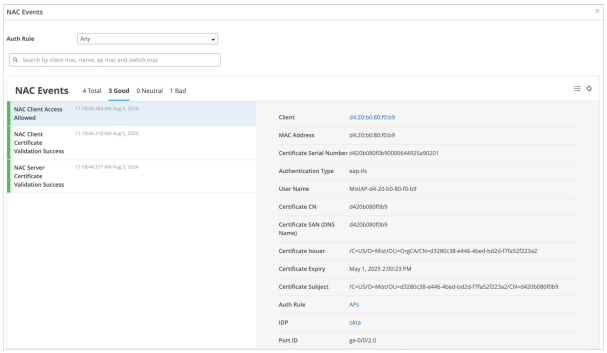
Auth Label

After you make your matching label, you can create your policy. In this example, the rule is to match on the AP certificate, wired authentication, and EAP-TLS. Upon successful authentication, a trunk VLAN configuration is returned to the switch.



Validation

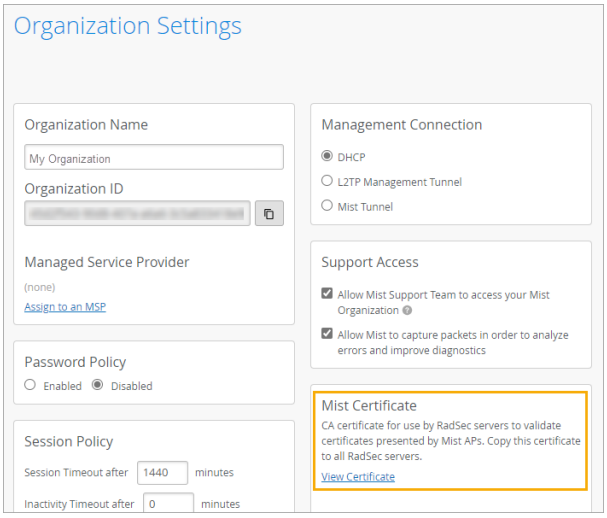
If all goes well, you will see your AP authenticated.



Importing 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.



Enable Local Status Page

SUMMARY

For troubleshooting purposes, configure a local status page where clients can see information about the AP they're connected to.

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

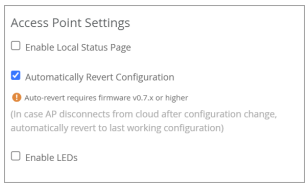
SUMMARY

As a best practice to ensure smooth operations, enable access points (APs) to revert to their last working configuration if they can't connect to the cloud.

For Mist APs running firmware version 0.7.x or newer, you can configure the APs to automatically revert to their last working configuration if the APs lose connectivity to the cloud.

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

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



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

Device Profiles

IN THIS SECTION

Device Profiles Overview

SUMMARY

Device profiles provide uniformity and scale when onboarding and managing Juniper APs at the organization level.

You can use device profiles in the same way as a template to configure and save a collection of settings that will apply to Juniper AP attached to the profile. These including settings such enabling the Bluetooth radio, configuring the default VLAN that the AP will connect to, and various Ethernet port properties for the hardware itself. In addition, you can include one or more WLAN Templates in the profile (which can include user access policies and a further subset of APs), and by extension, WLAN-specific configurations for the SSID such as a security policy.

Device profiles are especially convenient when onboarding new Juniper APs because you can include the APs in the profile and they will automatically receive the configuration when they come online.

When you add or remove a Juniper AP from a device profile, the change takes effect immediately; that is, the configuration settings defined in the profile will be removed from the AP and whatever default or AP-specific settings there are will take effect.

When you change a configuration setting in the device profile, you can push the change to the Juniper APs immediately by clicking the **Optimize Now** button in the Radio Management page. Alternatively, you can wait a few minutes and the update will propagate automatically.

By default, settings made on an individual AP take precedence over conflicting settings configured in a device profile. When creating a device profile, if such a conflict occurs, you will be notified and can choose whether to override the APs settings with those from the device profile.

Device Profile Options

SUMMARY

Get familiar with the various options available on the Device Profiles page, and configure radio settings, ethernet properties, BLE settings, and other features that you want to enable on your access points.

IN THIS SECTION

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

Table 8: Device Profiles

Option	Default	Summary
WLAN Templates	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. See "Create a Device Profile" on page 130.
"LEDs" on page 112	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 110	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 108	none	Defines settings for interoperability with third-party Real-Time Location System (RTLS), or asset tracking systems, including AeroScout and Centrak.

Table 8: Device Profiles *(Continued)*

Option	Default	Summary
"Wireless Mesh Network Configuration" on page 97	not enabled	Defines whether the AP is a relay or base for use in mesh networks.
"IP Settings" on page 95	DHCP	Defines how the AP and clients get an IP address: manually (static) or automatically from a DHCP server.
"Ethernet Properties" on page 92	not enabled	Defines PoE and VLAN settings for the Ethernet ports on the AP.
"BLE Settings" on page 90	not enabled	Enables or disables vBLE for location services on Juniper APs. Also adjusts beacon power.
RF Template Configuration	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 5 GHz Operation	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.
"Device Profile Variables" on page 131	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

SUMMARY

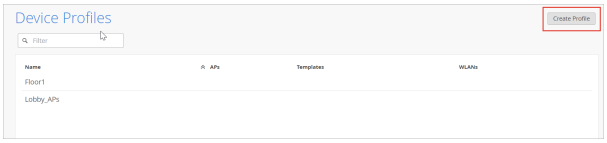
Create device profiles to streamline your configuration process and ensure consistency across similar access points (APs) at your site.

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

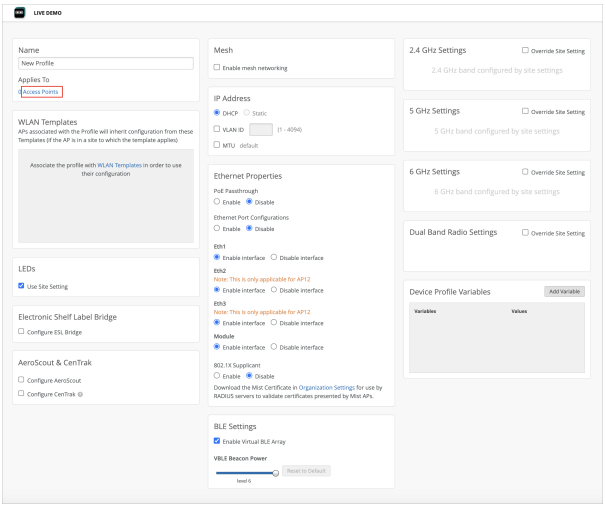
To create a device profile:

1. In the left menu, select **Organization** > **Wireless** > **Device Profiles**.

   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. You can also 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**.

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 128 for an explanation of the settings and associated tasks.
7. Click **Save** at the top of the screen.

Variables in Device Profiles

SUMMARY

By using variables to stand for values such as VLAN IDs or subnets (which vary across WLANs), you can get even more value from your device profiles.

Create and use device profile variables just like you do elsewhere in the Mist portal: first you define *{{key}}, value* pairs in the device profile, and then you reference the key(s) in a WLAN template. In this way, variables make it easy to both scale the configuration and have AP-specific settings that vary according to the WLAN.

Variables are most commonly used in device profiles for WLAN fields including, SSID, passphrase, VLAN, radio bands and RADIUS Authentication / Accounting Server.

Syntax and Rules for Variables

- ***{{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.

Regarding precedence, variables configured directly on the APs are given the highest priority, followed by those configured in a device profile, and then those configured at the Site level.

You can also use the Mist API to view the actual configuration that is being applied, for example, as a way to see exactly which variable is being used: Get Org Device Profile.

Monitor and Manage Access Points

SUMMARY

Use the Access Points page to view information about your APs and to complete maintenance tasks such as renaming and rebooting APs, clearing profile overrides, uploading images, and more.

IN THIS SECTION

Access Points Page Overview

To find this page, select **Access Points** from the left menu.

At the top of the page, you can use various features to get information and customize what you're seeing in the table.

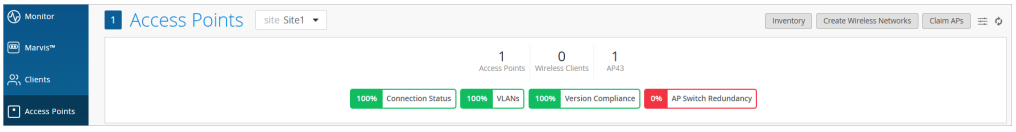


Table 9: Top-of-Page Features

Feature	Description	More Information
Site List	Select the site that you want to view.	

Table 9: Top-of-Page Features *(Continued)*

Feature	Description	More Information
More	This button appears only if you've selected one or more APs in the table. Take various actions to manage selected APs.	• "Reassign an AP to Another Site" on page 134 • "Rename an AP" on page 135 • "Release AP" on page 136 • "Clear Profile Overrides" on page 136 • "Batch Edit Labels, PoE Passthrough, and Radio Configurations" on page 137 • "Upload Images" on page 138 • "Bounce AP Tunnels" on page 138 • "Optimize Radios for Selected APs" on page 138
Inventory Button	Go to the Inventory page to see information for your organization's devices.	Inventory information in the Juniper Mist Management Guide
Create Wireless Networks Button	Go to the WLANs page to add and manage your networks.	"WLANs and WLAN Templates" on page 144
Claim APs Button	Add new APs to your organization.	"Claim a Juniper AP" on page 42
Upgrade APs	This button appears only if you've selected one or more APs in the table. Upgrade the selected APs.	"Upgrade the Firmware on a Juniper AP" on page 79
Reboot APs	This button appears only if you've selected one or more APs in the table. Reboot the selected APs.	

Table 9: Top-of-Page Features *(Continued)*

Feature	Description	More Information
Table Settings Button 	Open the Table Settings window, where you can select the information to show or hide in the table. You also can drag items up or down in the settings window to reorder the columns of the table.	
Refresh Button 	Update the page with the latest data.	
Device Totals	The total number of access points and clients, and the number of each AP model.	
Metrics	Metrics for basic criteria. Click a button to see only the APs with issues.	"AP Metrics" on page 31

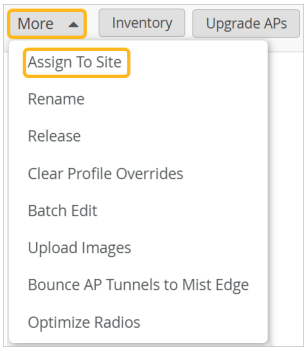
Selecting APs in the Table

Select the site at the top of the Access Points page, and then select one or more APs in the table.

- Individual APs—Use the check boxes in the first column to select individual APs.
- All APs—Use the check box in the header row to select all APs.

Reassign an AP to Another Site

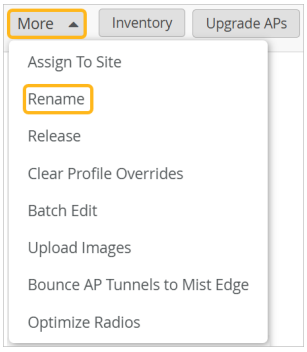
1. "Select the APs" on page 134 to reassign.
2. At the top of the page, click **More** > **Assign to Site**



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

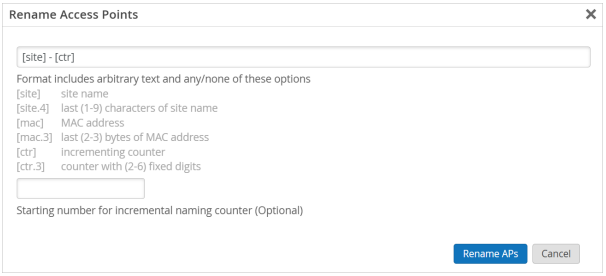
Rename an AP

1. "Select the APs" on page 134 to rename.
2. At the top of the page, click **More** > **Rename**.



3. In the pop-up window, enter text or variables to create the names for the selected APs. OR leave the box blank to reset the APs to an empty name.

   You can enter text, spaces, special characters, and variables. For example, let's say you want the AP name to include the site name, and an integer, such as *Boston - 1*, *Chicago - 2*, and so on. You'd enter *[site] - [ctr]* as shown in the following example.



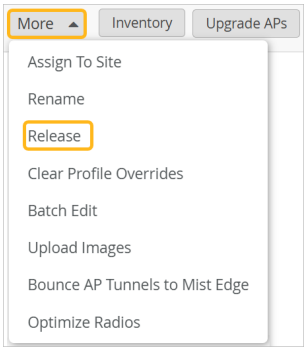
NOTE: If you use a counter variable, you can enter the number that you want to start with. If you leave the starting number field blank, then the numbers start with 1.

4. Click **Rename APs**.

Release AP

Release an AP from your organization's inventory.

1. "Select the APs" on page 134 to release.
2. At the top of the page, click **More** > **Release**

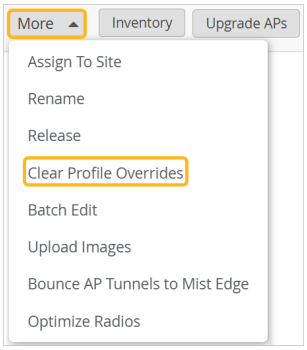


3. Read the warning message, and if you want to continue, click **Yes**.

Clear Profile Overrides

Follow this procedure if you've modified the AP configuration and want to revert to the settings in the device profile.

1. "Select the APs" on page 134to clear overrides for.
2. At the top of the page, click **More** > **Clear Profile Overrides**.



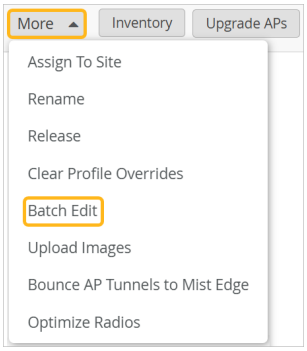
3. Read the warning message, and if you want to continue, click **Clear Overrides**.

Batch Edit Labels, PoE Passthrough, and Radio Configurations

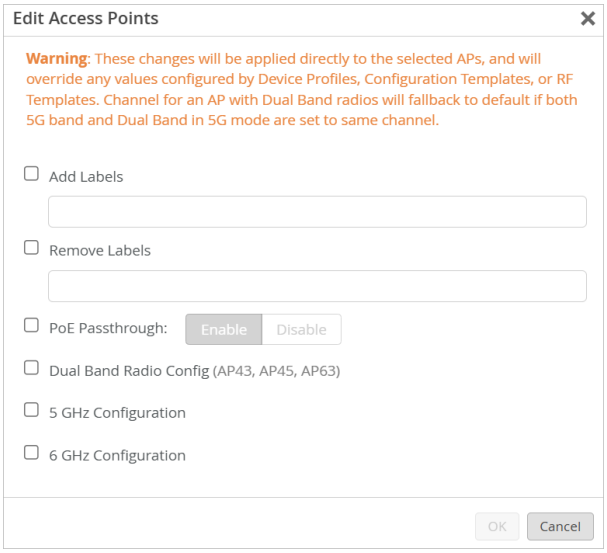
Select multiple access points, and then apply new settings to all of them. You can make these types of changes:

- Add or remove labels.
- Enable or disable PoE passthrough.
- Configure dual band, 5 GHz, or 6 GHz.

1. "Select the APs" on page 134 to edit.
2. At the top of the page, click **More** > **Batch Edit**



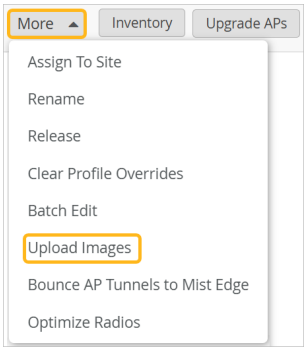
3. Read the warning to understand the impact of these changes.
4. Select the check box for each setting that you want to change, and then enter the new settings.



5. Click **OK**.

Upload Images

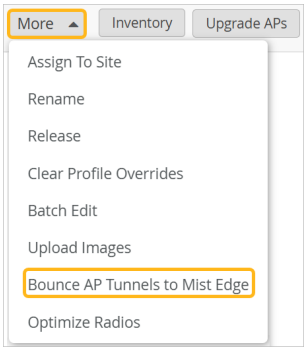
1. "Select the APs" on page 134 to upload images for.
2. At the top of the page, click **More** > **Upload Images**.



3. Add the images, and then click **Save**.

Bounce AP Tunnels

1. "Select the APs" on page 134 to bounce tunnels for.
2. At the top of the page, click **More** > **Bounce AP Tunnels to Mist Edge**.

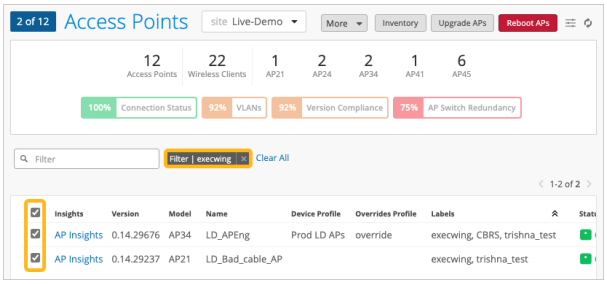


Optimize Radios for Selected APs

You can manage most radio settings automatically, as Radio Resource Management runs periodically to optimize performance. However, in certain situations, you might want to run RRM at will to optimize radios on a single AP or a small subset of APs at your site.

Consider the following examples:

- You need to make a change on a few APs based on their label.



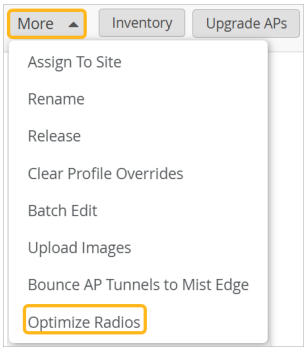
- You've onboarded a few new APs, and you want to immediately optimize their radios.
- In a large, multi-use building, you want to run RRM only on a few APs, without disrupting a heavily used dining hall, conference room, or auditorium.
- In an outdoor setting, you need to change the channel or power settings on a few APs due to environment variations.

With the Optimize Radios feature, you can run RRM only on the radios that need adjustments, without impacting the other APs in your wireless network.

TIP: By default, optimization involves both channel selection and transmit power. However, if you prefer to avoid channel impact, you can optimize transmit power only.

To optimize radios for selected APs:

1. "Select the APs" on page 134 to optimize.
2. At the top of the page, click **More** > **Optimize Radios**.



3. In the pop-up window:,
   - Select the bands to optimize.
   - If you do not want to adjust channel selection, select **Optimize transmit power only**.
4. Click **Optimize Now** at the bottom of the pop-up window.

Access Point FAQ

SUMMARY

Get answers to common questions about installation, configuration, and hardware requirements.

IN THIS SECTION

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 APs" on page 26.

How much bandwidth does AP telemetry to the Mist cloud require?

About 10 Kbps to 20 Kbps per client is typical. For one AP with ten clients, 14.4 Kbps is a typical average. You can also use Mist Edge to aggregate telemetry for individual APs into a single connection.

More Information: Telemetry on the cloud is available to all relevant microservices (that is,., there is no need for each service to separately poll for the data it needs). Mist APs poll the Mist cloud and/or send AP statistics every 2 seconds; if the cloud doesn't receive stats from an AP within 90 seconds, it will show the AP as disconnected in the dashboard and automatically update the status when the connection resumes.

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.

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 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 46.

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.

How do I reset an AP?

For help resetting an AP to its factory default settings, see "Reset an AP to the Factory-Default Configuration" on page 421.

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 80.

3
CHAPTER

WLANs and WLAN Templates

SUMMARY

Use the information in this chapter to configure your WLANs and set up features such as guest portals, integrations, access policies, and more.

IN THIS CHAPTER

What Do You Want to Do?

Table 10: Top Tasks

If you want to...	Use these resources:
Get started with WLANs and WLAN Templates *Explore the benefits of using WLAN templates and get started with the basic configuration steps.*	"Configure a WLAN Template" on page 231
Explore WLAN settings *Learn about all of the options that you can implement, including band steering, geofencing, rate limits, filtering, QoS, security, and more).*	"WLAN Options" on page 235
Enable guest access *Enable guest access to your Internet services while preventing unauthorized access to your devices and resources. Explore options such as adding a custom guest portal, using an external sign-on page, or enabling Single Sign-On.*	"Compare WLAN Guest Portal Options" on page 286
Control users' access to network resources *Set up access policies to control which users can access which resources.*	"WxLAN Access Policies" on page 220

Security

SUMMARY

Use the information in this chapter to get started with security options such as 802.1X, MAC RADIUS authentication, integrations, and access policies.

IN THIS SECTION

What Do You Want to Do?

Table 11: Top Tasks

If you want to...	Use these resources:
Use a RADIUS server to authenticate users *Juniper Mist supports IEEE 802.1X security for WPA2 and WPA3. You can also set up CoA/DM and RadSec.*	"Enable WPA2/WPA3 Enterprise (802.1X) Security on a WLAN" on page 164
Use MAC address authentication *You can use this option with any security type.*	"MAC Address Authentication By RADIUS Lookup" on page 172

Table 11: Top Tasks *(Continued)*

If you want to...	Use these resources:
Use preshared keys to authenticate users *With preshared keys (PSK), clients must present a secure passphrase to connect to the wireless network. You can also leverage PSKs for onboarding users to the SSID.*	"Configure and Manage Pre-Shared Keys" on page 192
Integrate with third-party products *Integrate with Aruba Clearpass, JumpCloud, Cisco ISE, or Hotspot 2.0.*	"Integrations" on page 267
Configure access policies *Set up rules to allow or deny access to resources on the network.*	"WxLAN Access Policies" on page 220
Monitor and remove potential security threats *Juniper Mist detects rogue, neighbor, and honeypot APs. These are unauthorized devices operating on or near your network, often with the goal of stealing data or monitoring communications.*	"Rogue, Neighbor, and Honeypot Access Points" on page 205
Use Juniper Mist Access Assurance for secure network access control for your wired and wireless networks.	Juniper Mist Access Assurance Guide

Configure AP Threat Protection

SUMMARY

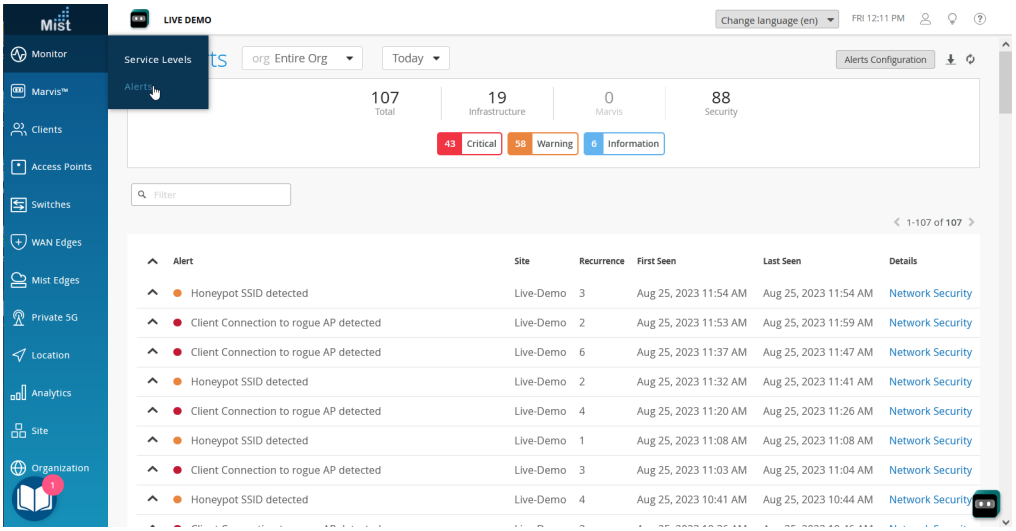
To protect your network, enable Juniper Mist™ to detect unauthorized access points (APs) across your site.

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 "Rogue, Neighbor, and Honeypot Access Points" on page 205.

When threat protection is enabled, you'll see the detected APs on the Monitor > Alerts page, as shown below.

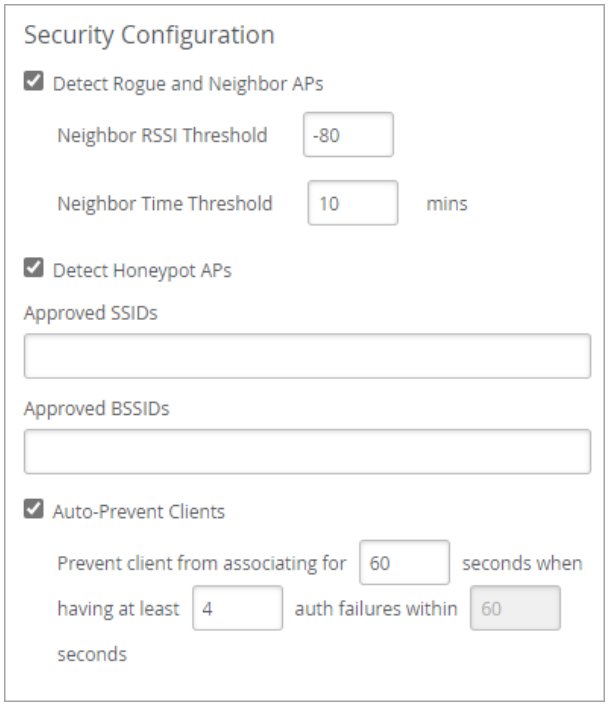
Figure 8: Viewing Alerts for Rogues, Honeypots, and Neighbor APs



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.



- **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.

Self-provisioning for IoT and Personal Devices

SUMMARY

Automate client onboarding at scale, for personal devices and IoT, with secure self provisioning.

IN THIS SECTION

Wireless users in environments like dormitories can securely self-provision their personal devices such as Xboxes, Apple TV, and Roku. Likewise, unattended IoT devices can securely and automatically join a specified VLAN, or network segment. We call this the Personal Network Experience. And because it eliminates the need for client MAC address registration and IT intervention, it is an ideal solution for providing Wi-Fi access at scale.

Self provisioning with the Personal Network Experience works by connecting a SAML-compliant identity provider (IDP), for example, Microsoft Entra ID, to the Mist Active Assurance portal. Users log on to the WLAN, where they are redirected to the single-sign-on service for authentication and authorization. Mist assigns authenticated users a personal preshared key (PSK) that is specific to both the individual user and/or the SSID. Using personal PSKs also enables micro-segmentation, which means you can have users connect to a specific VLAN according to their role or profile. The same is true for IoT devices; they can be automatically connected to a specific VLAN, a best practice for protecting against IoT take-over attacks.

In the Mist console, you can configure both the complexity of the required passphrase, and the frequency of key rotation.

Figure 9: Self-Provisioning Logon Screen

During self-provisioning, laptop users can generate a unique passphrase, then copy and paste it into the portal when prompted. Or, if working from a mobile device, they can have the passphrase emailed to them. Generated passphrases expire after 24 hours.

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 help with WLAN configuration, see the Juniper Mist Wireless Assurance Configuration Guide.
- 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.

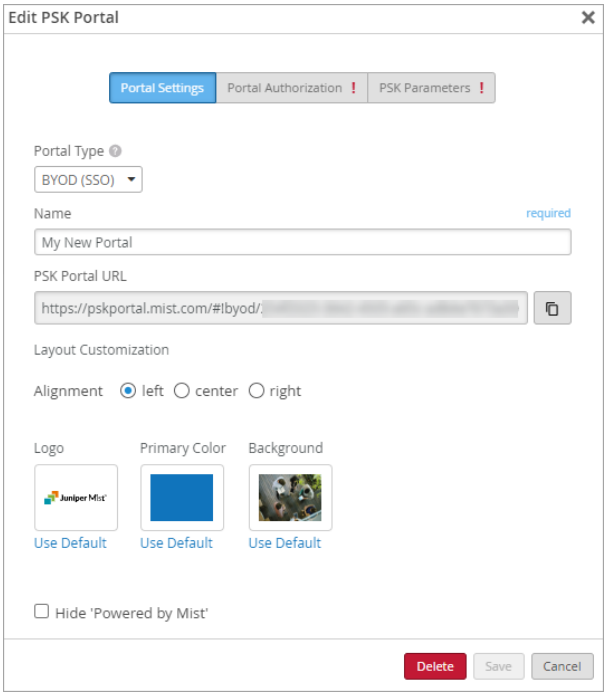
  Copy the following information from your SAML 2.0 app integration, and save it so that you can use it to set up your PSK portal in Juniper Mist.

  - Signing Algorithm
  - Issuer ID (this key may vary, for example, in Okta, this value is called *Identity Provider Issuer* and in Azure, it's called *Azure AD Identifier*.
  - SSO URL (this key may vary, for example, in Okta, this value is called *Identity Provider Single Sign-On URL* and 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.

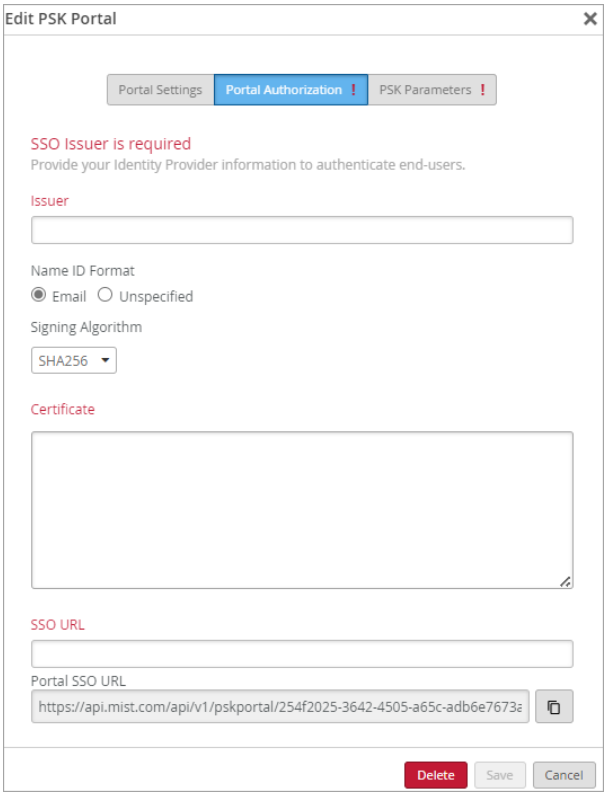
Configure Self-Provisioning

To set up client onboarding with a BYOD PSK Portal:

1. From the left menu of the Juniper Mist portal, select **Organization** > **Access** > **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**.
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.



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**.



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.

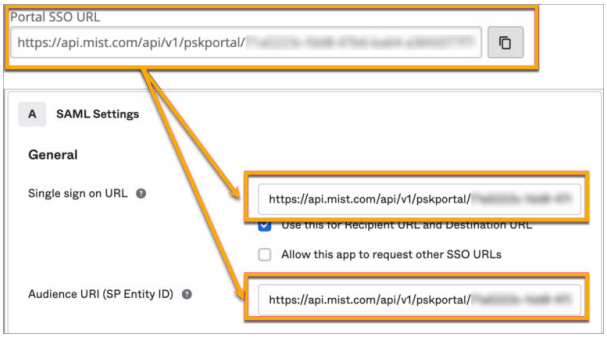
   c. Enter the copied value into the appropriate field to identify your Juniper Mist PSK portal to your IdP. For help, see your IdP documentation.

   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.

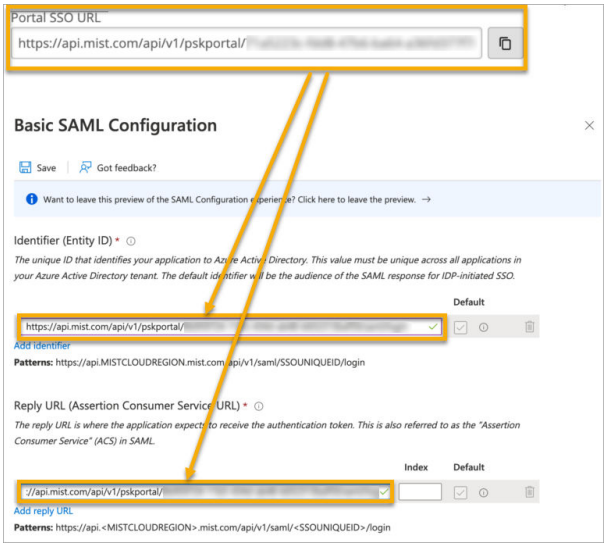
   Okta Example

   In this example, the **Portal SSO URL** from Juniper Mist is copied into the appropriate fields in the Okta Admin Console.



Microsoft Azure Example

In this example, the **Portal SSO URL** from Juniper Mist is copied into the appropriate fields in the Azure Admin Console.



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:
     - 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.
     - Set the **Passphrase Settings** to enforce your policies for password complexity.

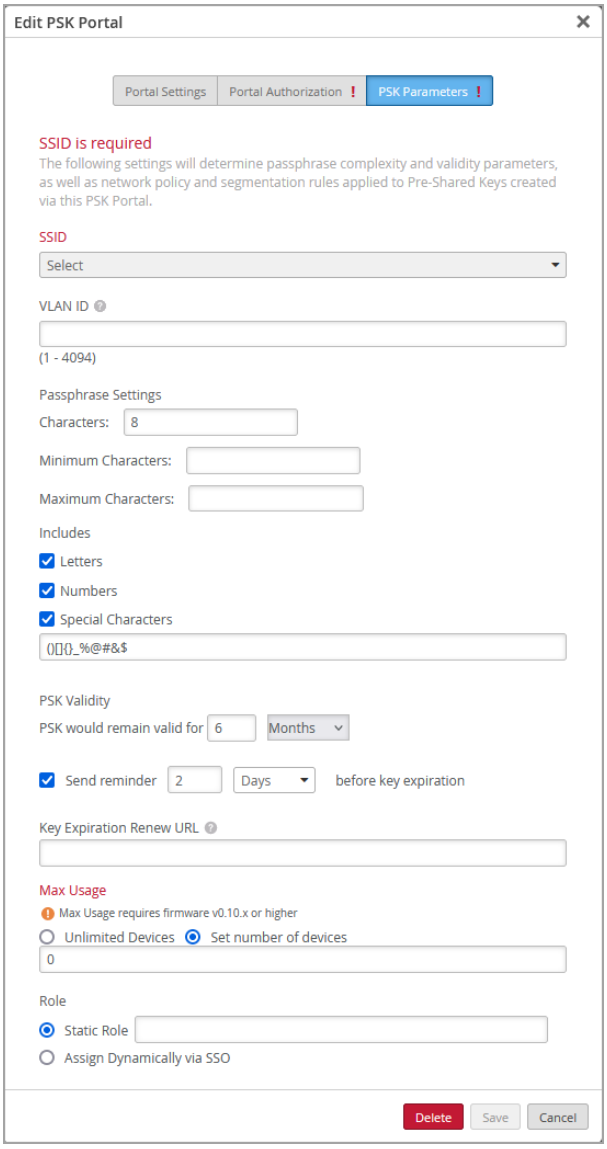
- Adjust the **PSK Validity** options to set the expiration period and to send reminders before key expiration.

  If you enable the option to send reminders, Juniper Mist sends users an email when their PSK is about to expire.

  The email includes either the default reauthentication URL or your **Key Expiration Renew URL** (if you enter one). This is typically an single sign-on URL (for example, using your corporate identity provider URL through Okta or Microsoft Azure).

- 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).



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.

Users can follow the on-screen text to onboard their devices.

Personal WLANs

SUMMARY

Set up personal WLANs to enable communication between clients who share a preshared key (PSK) or RADIUS-based SSID.

IN THIS SECTION

Personal WLANs are secure micro-segmented networks within a WLAN for a group of users.

You can use personal WLANs in a couple of ways:

- Use personal WLANs with **multi passphrase WLANs (MPSK SSIDs)**, forming groups per PSK. Clients within a key can talk to other clients in the same key, but clients can't talk to other clients in different keys. The personal WLAN groups are automatically formed using the PSK.
- Use personal WLANs across multiple SSIDs that use **RADIUS-based SSIDs**. This can be helpful in a dormitory or university campus, where students bring their own devices and connect to MPSK-based SSID, while their laptops are on 802.1X enabled Eduroam network. When personal WLAN is enabled, clients with the same username are placed in the same group, regardless of the SSID they are connected to. These clients can communicate only with other clients that have the same username. There is no connectivity between devices with different usernames.

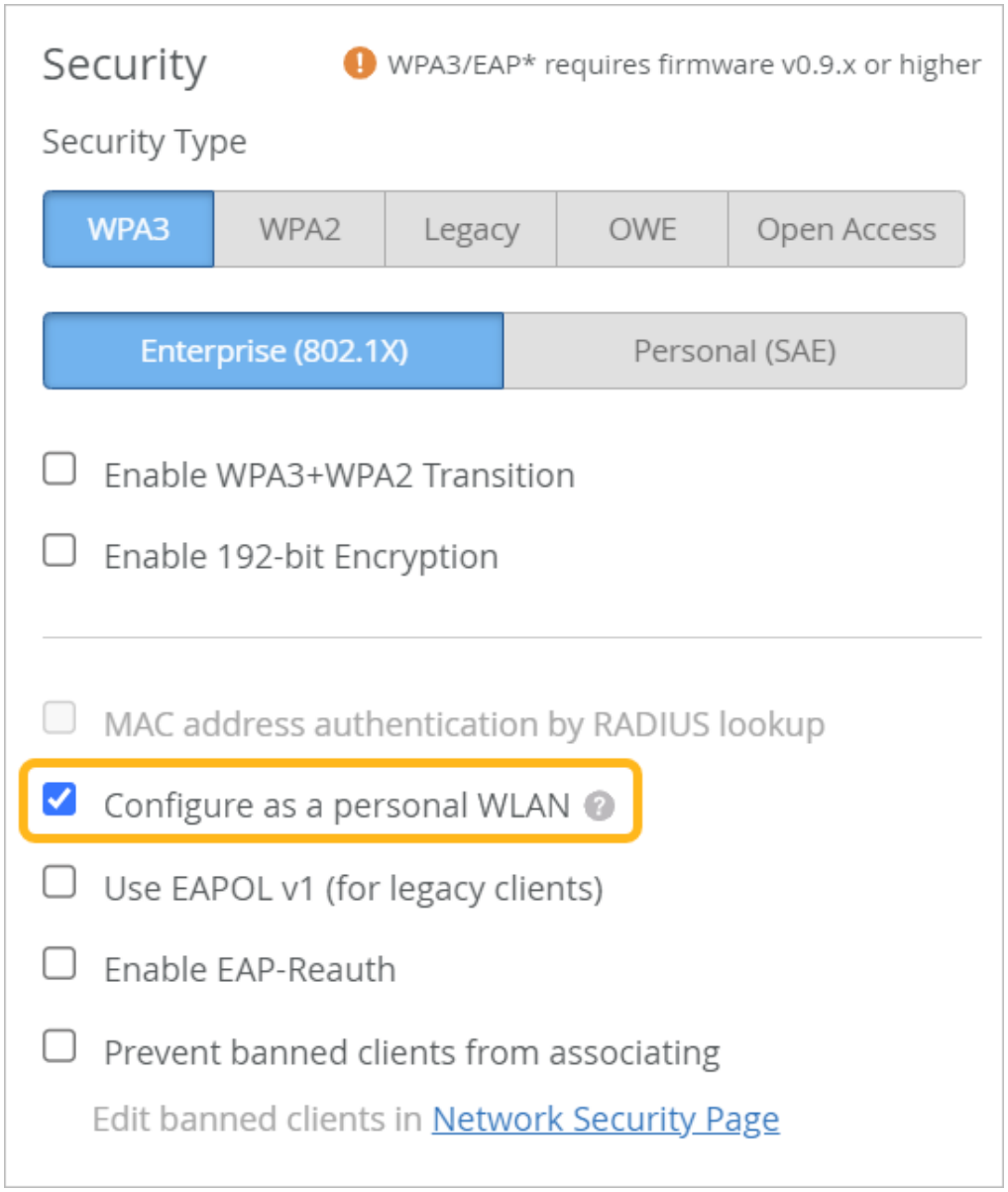
NOTE: To use personal WLANs with RADIUS-based SSIDs, your access points need firmware version 0.14.x or later.

Personal WLAN works across SSIDs and security types:

- WPA2 or WPA3 + Enterprise (802.1X)
- WPA2 or WPA3 + RADIUS PSK
- Open Access + MAC address authentication by RADIUS lookup
- OWE + MAC address authentication by RADIUS lookup

How to Configure Personal WLANs

When adding or editing a WLAN, select a supported security type, and then select **Configure as a personal WLAN**.



RELATED DOCUMENTATION

Configure and Manage Pre-Shared Keys | 192

RSSI, Roaming, and Fast Roaming

SUMMARY

Understand the importance of RSSI and the impact of poor RSSI on throughput. Enable fast roaming, and view roaming history to troubleshoot client issues.

IN THIS SECTION

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 fast roaming option becomes available when you select WPA3 or WPA2 as your security type. With WPA3 selected the available methods for fast roaming are, *Default*, *Opportunistic Key Caching (OKC)* and *.11r*. With WPA2 selected, only *Default* and *.11r* are available. For both these methods, there is no need to send access request packets to the RADIUS server.

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.

.11r (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. Select this option to enable support for the Fast BSS Transition 802.11r protocol.

- **Zebra Compatibility**—This option changes how Mist APs advertise fast roaming, which was necessary for interoperability with certain legacy Zebra mobile devices. There is no need to enable this option if your Mist APs and Zebra mobile devices are running firmware that is up to date, and in fact, incorrect

configuration can introduce problems. This option enables *FT-over-the-DS* (Fast Transition over the Distribution System), which is a method within the IEEE 802.11r standard for fast roaming wherein fast transition handshakes occur through the wired network (the Distribution System) without the need for full re-authentication.

- For more information on the joint solution for combining Juniper's AI-Native Networking with Zebra's advanced mobile computing, see:
  - Juniper Mist for Zebra Delivers Intelligence at the Edge Solution Brief
  - Marvis Zebra integration
  - Marvis Android Client

The table below summarized the roaming options and RADIUS interactions for different security types.

Table 12: 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 160 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. Marvis uses this information to provide a visual representation of your device's roaming history. See Client Roaming Visualization for more information.

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.

   Here's an example that shows how Marvis depicts the roaming information for a client.

Figure 10: Track and Troubleshoot Client Roaming

RADIUS

IN THIS SECTION

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

These topics guide you through the basic steps of enabling 802.1x security and adding your RADIUS server, with additional information about various options.

Set the WLAN Security Type and Add Your RADIUS Server

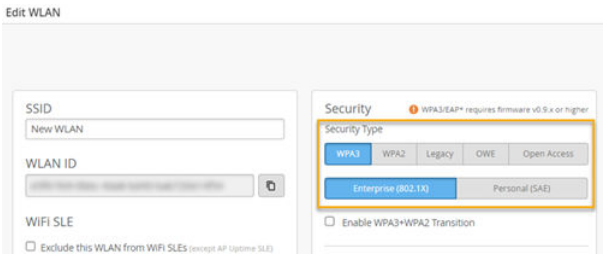
Juniper Mist supports IEEE 802.1X security for WPA2 and WPA3.

NOTE: WPA3 or OWE are mandatory in 6 GHz. 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:
   a. Click **WPA3** or **WPA2**.
   b. Click **Enterprise (802.1X)**.

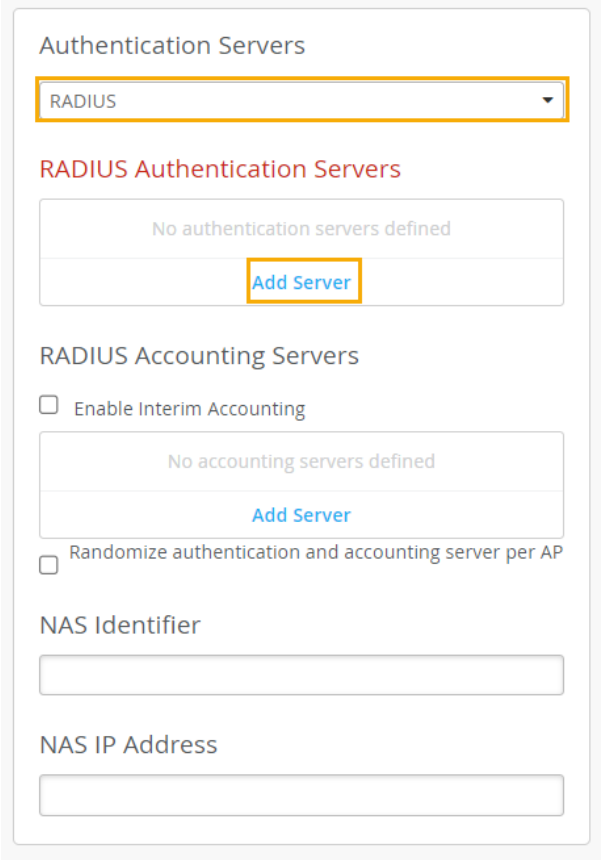
   RADIUS authentication is available only when you've selected WPA2/WPA3 and Enterprise (802.1X) in the Security section.



3. In the **Authentication Servers** section, add your server.

   a. Select RADIUS as the server type.

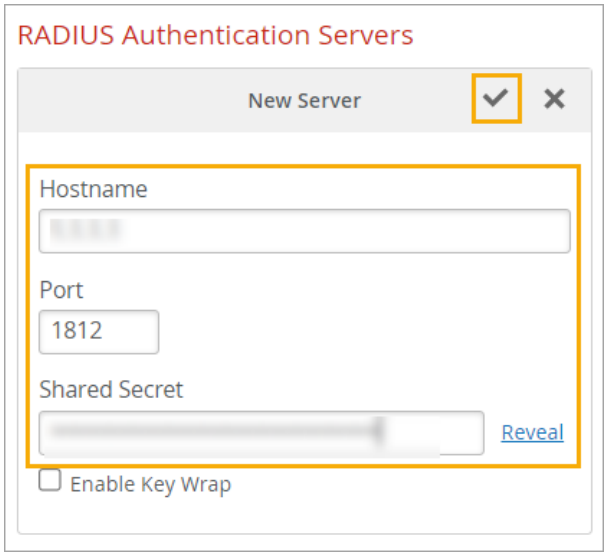
   b. Click **Add Server**.



   c. Enter the **Hostname** and the **Shared Secret**.

> **NOTE**: You can use site variables instead of entering the hostname. See "(Optional) Use Site Variables to Add a Server" on page 166.

   d. Click the check mark button.



4. (Optional) Configure additional options for your WLAN if needed (as described in the remaining sections of this document).
5. Save the WLAN configuration, and save the template changes (if the WLAN is part of a WLAN template).

(Optional) Use Site Variables to Add a Server

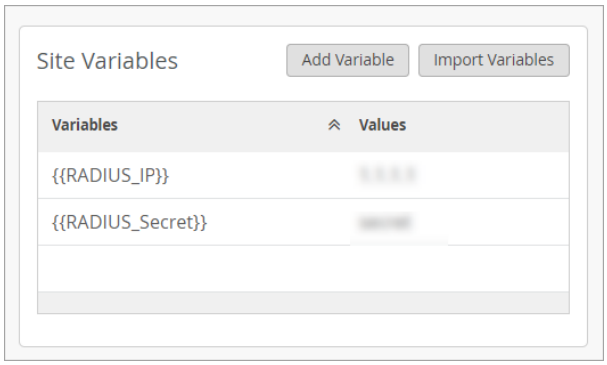
By using site variables to identify your RADIUS server, you can easily apply the same WLAN configuration to APs at different sites even though certain attributes are different. In this scenario, imagine that Site A and Site B use different RADIUS servers. You'll use variables to add the RADIUS server 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**.

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.



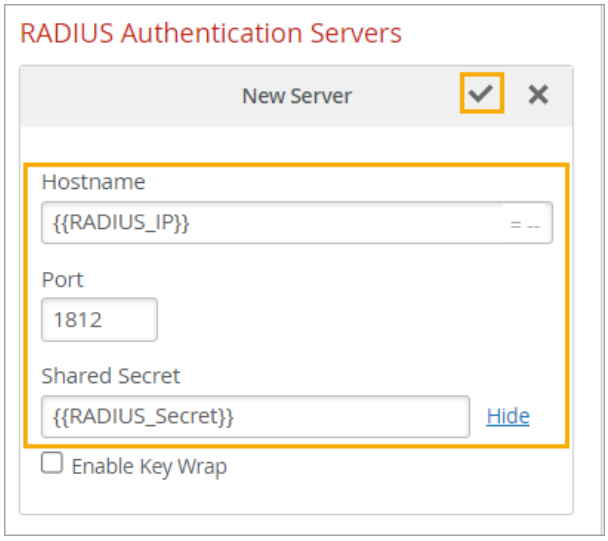
2. Add the same variables to the next site (Site B), and enter the correct values for that site's RADIUS server.

   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 164, 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}}.



5. Save the WLAN settings.

(Optional) Add a 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.

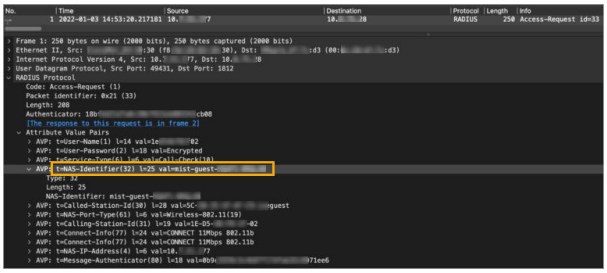
If you leave the NAS Identifier field blank, the WLAN ID is used as the NAS ID.

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.

As shown below, when an AP on this WLAN sends an Access-Request, the variables are transformed to identify the AP.



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.

(Optional) Add a CoA/DM Server

When you're enabling 802.1X security on a WLAN, you also can add a CoA/DM server.

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.

NOTE: For more information, see "Change of Authorization (CoA)" on page 188.

(Optional) Enable 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.

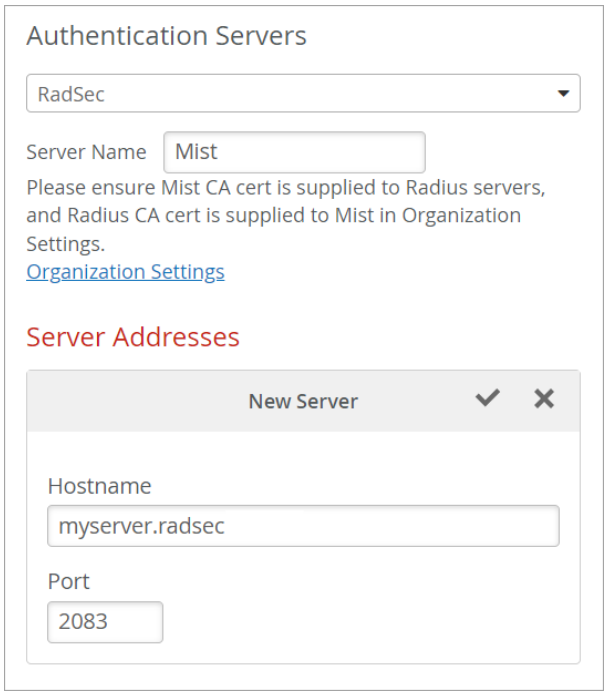
To enable RadSec and install the certificates:

1. After you "Set the WLAN Security Type and Add Your RADIUS Server" on page 164, 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**.



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.

SEE ALSO

Juniper Mist RADIUS Attributes | 176

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.

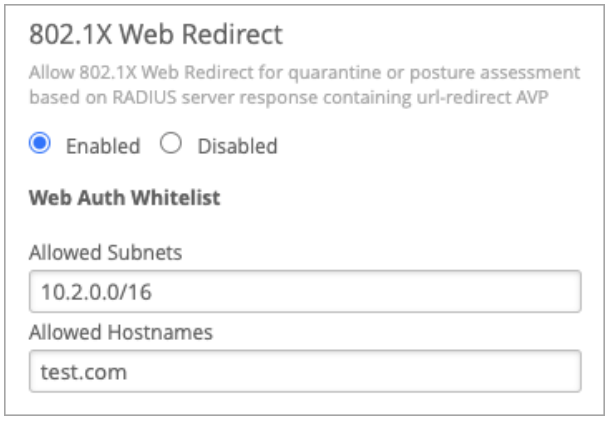
This feature enables you to perform compliance checks on clients with agents installed. During a client authentication, the RADIUS server sends an Access-Accept message containing a URL-redirect RADIUS Attribute Value Pair (AVP) to point the client to a quarantined portal for remediation.

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.



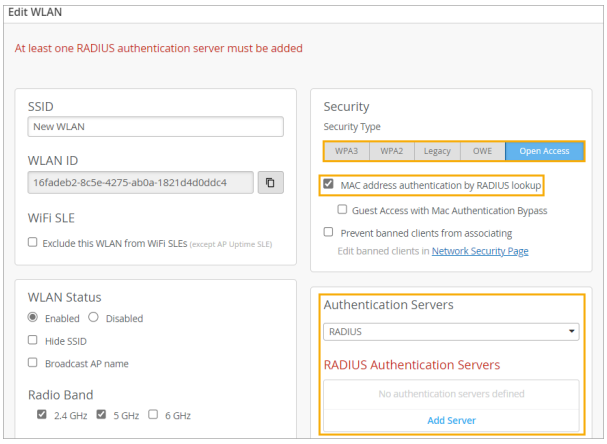
4. Save the changes.

MAC Address Authentication By RADIUS Lookup

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.



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 173.

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

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.

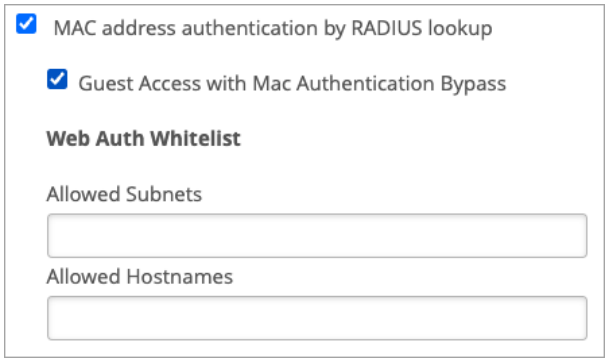
6. Traffic is intercepted and is responded with the redirect URL that was sent by RADIUS server.
7. The client is redirected to the specified URL. Based on your configured policy, it might be a sponsored portal, a self-registration portal, or a hotspot portal.
8. After the client provides the necessary 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 231.
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**.



3. (Optional) Use the **Allowed Subnets** and **Allowed Hostnames** fields to specify resources that guests can access in the redirect state.

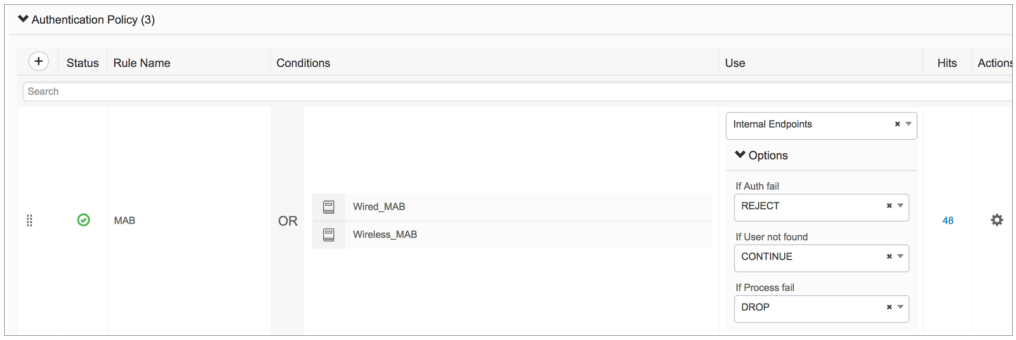
   If these fields are left blank, the RADIUS server is the only IP address that guests can access.
4. Add your RADIUS server, as described in "Enable WPA2/WPA3 Enterprise (802.1X) Security on a WLAN" on page 164.

Complete the additional RADIUS configuration tasks below.

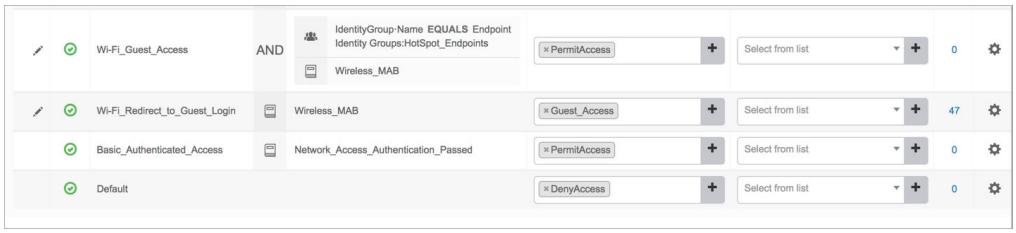
RADIUS Configuration

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.

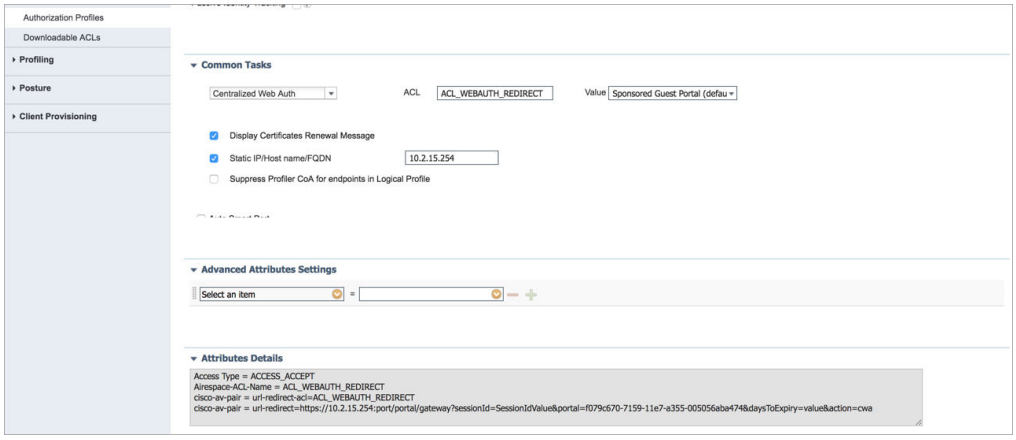


2. Authorization Policies: Configure two policies that will be hit during the process of the guest access flow.



- 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.



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

IN THIS SECTION

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 13: IETF Standard Authentication Attributes

Attribute Name	Type	RFC	Description
User-Name	1	RFC 2865	The *User-Name* attribute is forwarded in the *Access-Request* and indicates the name of the user to be authenticated.
User-Password	2	RFC 2865	The *User-Password* attribute is forwarded in the *Access-Request*. It indicates the password of the user to be authenticated, or the user's input following an Access-Challenge.
NAS-IP-Address	4	RFC 2865	The *NAS-IP-Address* attribute is forwarded in the *Access-Request* and indicates the IP Address of the AP requesting user authentication. You can configure this attribute in the RADIUS settings for a WLAN. All APs on a WLAN send the configured value.
Service-Type	6	RFC 2865	The *Service-Type* attribute is forwarded in the *Access-Request* 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 *Framed-User* by the AP for 802.1X/EAP WLANs or to *Call-Check* for the MAC-Auth enabled WLANs.
Framed-MTU	12	RFC 2865	The *Framed-MTU* attribute is forwarded in the *Access-Request* and indicates the Maximum Transmission Unit (MTU) to be configured for the user. The attribute value is always set to *1200* by the AP.
State	24	RFC 2865	The *State* attribute is available to be forwarded in the *Access-Challenge*. It must be sent unmodified from the client to the server in the *Access-Request* reply to that challenge, if any.

Table 13: IETF Standard Authentication Attributes *(Continued)*

Attribute Name	Type	RFC	Description
Called-Station-Id	30	RFC 2865	The *Called-Station-Id* attribute is forwarded in the *Access-Request* 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: *XX-XX-XX-XX-XX-XX:ESSID*.
Calling-Station-Id	31	RFC 2865	The *Calling-Station-Id* attribute is forwarded in the *Access-Request* and indicates the MAC address of the authenticating user. It is only used in Access-Request packets. The Access Point will forward the attribute value using the following formatting: *XX-XX-XX-XX-XX-XX*.
NAS-Identifier	32	RFC 2865	The *NAS-Identifier* attribute is forwarded in the *Access-Request*. You can configure this attribute in the RADIUS settings for a WLAN. All access points on a WLAN send the configured value. You can use variables to send the device name, model, MAC address, and site name. The variables are: {{DEVICE_NAME}} {{DEVICE_MODEL}} {{DEVICE_MAC}} {{SITE_NAME}}
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 *NAS-Port-Type* attribute is forwarded in the *Access-Request* and indicates the type of physical connection for the authenticating user. The attribute value is always set to *Wireless-802.11* by the Access Point.
Connection-Info	77	RFC 2869	The *Connection-Info* attribute is forwarded in the *Access-Request* and indicates the data-rate and radio type of the authenticating user. The Access Point will forward the attribute value using the following formatting: *CONNECT XXMbps 802.11X*.
EAP-Message	79	RFC 2869	The *EAP-Message* attribute is forwarded in *the Access-Request*, Access-Challenge, Access-Accept and Access-Reject and encapsulates Extended Access Protocol (EAP) packets.

Table 13: IETF Standard Authentication Attributes *(Continued)*

Attribute Name	Type	RFC	Description
Message-Authenticator	80	RFC 2869	The *Message-Authenticator* attribute is forwarded in the *Access-Request* and may be used to prevent spoofing of CHAP, ARAP or EAP Access-Request packets.
Tunnel-Private-Group-ID	81	RFC 2868	The *Tunnel-Private-Group-ID* attribute is forwarded in the *Access-Accept* 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.
Filter-Id	11	RFC 2865	The *Filter-Id* attribute may be forwarded in the *Access-Accept* and indicates user role client will be associated with. User Groups are used by the Mist WxLAN policy framework to assign network firewall rules. Format: Group-Name Example: employee

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 14: Supported Vendor-Specific Attributes

Attribute Name	Type	Vendor ID	Attribute Number	Formatting	Description
Airespace-Interface-Name	26	14179	5	String	The *Airespace-Interface-Name* attribute may be forwarded in the *Access-Accept* to indicate the dynamic VLAN membership of an 802.1X or RADIUS MAC authenticated user. Returned attribute value is always a string formatted name of the VLAN. VLAN Name to VLAN ID translation must be configured under WLAN using VLAN IDs or Variables. Format: VLAN-Name Example: employee-vlan

Table 14: Supported Vendor-Specific Attributes *(Continued)*

Attribute Name	Type	Vendor ID	Attribute Number	Formatting	Description
Airespace-ACL-name	26	14179	6	String	The *Airespace-ACL-Name* attribute may be forwarded in the *Access-Accept* and indicates user role client will be associated with. User Groups are used by Mist WxLAN policy framework to assign granular network resource restrictions. Format: Group-Name Example: employee
Aruba-User-Role	26	14823	1	String	The *Aruba-User-Role* attribute may be forwarded in the *Access-Accept* and indicates user role client will be associated with. User Groups are used by Mist WxLAN policy framework to assign granular network resource restrictions. Format: Group-Name Example: employee

Table 14: Supported Vendor-Specific Attributes *(Continued)*

Attribute Name	Type	Vendor ID	Attribute Number	Formatting	Description
Cisco-AVPair	26	9	1	String	The *Cisco-AVPair* attribute may be forwarded in the *Access-Accept* to indicate to 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. **AVPair URL Redirect** Format: url-redirect=<URL value> Example: url-redirect=https://ise28.89mistilbs.org:8443/portal/gateway?sessionId=0a004b1c/Jtf4peiJ5A8nPreloHRRITWvmhDCbnH3qXQ8MngtoA&portal=71984f36-f55e-4439-ba6e-903d9f77c216&action=cwa&token=1f7dca2cc907b1ad56ee4880e1cfa1ae **AVPair PSK** The *Cisco-AVPair* attribute may also contain PSK attribute, indicating to the Mist 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 another AVPair providing the actual Pre-Shared Key value. Format: psk-mode=ascii & psk=<passphrase>

Table 14: Supported Vendor-Specific Attributes *(Continued)*

Attribute Name	Type	Vendor ID	Attribute Number	Formatting	Description
Eleven-Authentication-Find-Key	26	52970	3	TLV	The *Eleven-Authentication-Find-Key* attribute is used to supply additional information to the supported RADIUS servers to simplify wireless client PSK lookup via RADIUS, removing the need to pre-associate a wireless client MAC with a particular PSK ahead of time. This attribute is a TLV according to the 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 by 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 by 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 *xxxxxxxxxxxx* format
Eleven-EAPOL-STMAC (sub-attribute)			5	Octets	Eleven-EAPOL-STMAC sub-attribute contains wireless client MAC address in *xxxxxxxxxxxx* 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 15: Supported Accounting Attributes

Attribute Name	Type	RFC	Description
User-Name	1	RFC 2865	The *User-Name* attribute is forwarded in the *Accounting-Request* and indicates the name of the user.
NAS-IP-Address	4	RFC 2865	The *NAS-IP-Address* attribute is forwarded in the *Accounting-Request* and indicates the IP Address of the Access Point.

Table 15: Supported Accounting Attributes *(Continued)*

Attribute Name	Type	RFC	Description
Framed-IP-Address	8	RFC 2865	The *Framed-IP-Address* 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. **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.
Class	25	RFC 2865	The *Class* attribute is optionally forwarded in the *Access-Accept* and should be sent unmodified by the client to the accounting server as part of the *Accounting-Request* packet if accounting is enabled. Mist Access Points support sending multiple Class attributes for each client.
Called-Station-Id	30	RFC 2865	The *Called-Station-Id* attribute is forwarded in the *Accounting-Request* and indicates the BSSID and ESSID that the user is associated with. The Access Point will forward the attribute value using the following formatting: *XX-XX-XX-XX-XX-XX:ESSID*.
Calling-Station-Id	31	RFC 2865	The *Calling-Station-Id* attribute is forwarded in the *Accounting-Request* and indicates the MAC address of the user. The Access Point will forward the attribute value using the following formatting: *XX-XX-XX-XX-XX-XX*.
NAS-Identifier	32	RFC 2865	The *NAS-Identifier* attribute is forwarded in the *Accounting-Request* and indicates the user defined identifier configured under WLAN settings.
Acct-Status-Type	40	RFC 2866	The *Acct-Status-Type* attribute is forwarded in the *Accounting-Request* and indicates whether the *Accounting-Request* marks the status of the accounting update. Supported values include *Start*, *Stop* and *Interim-Update*.

Table 15: Supported Accounting Attributes *(Continued)*

Attribute Name	Type	RFC	Description
Acct-Delay-Time	41	RFC 2866	The *Acct-Delay-Time* attribute is forwarded in the *Accounting-Request* 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 *Accounting-Request*.
Acct-Input-Octets	42	RFC 2866	The *Acct-Input-Octets* attribute is forwarded in the *Accounting-Request* and indicates how many octets have been received from the user over the course of the connection. This attribute may only be present in *Accounting-Request* records where the *Acct-Status-Type* is set to *Stop*.
Acct-Output-Octets	43	RFC 2866	The *Acct-Output-Octets* attribute is forwarded in the *Accounting-Request* and indicates how many octets have been forwarded to the user over the course of the connection. This attribute may only be present in *Accounting-Request* records where the *Acct-Status-Type* is set to *Stop*.
Acct-Session-Id	44	RFC 2866	The *Acct-Session-Id* attribute is forwarded in the *Accounting-Request* and provides a unique identifier to make it easy to match *start*, *stop* and *interim* records in an accounting log file.
Account-Authentic	45	RFC 2866	The *Account-Authentic* attribute is forwarded in the *Accounting-Request* and indicates how the user was authenticated. When RADIUS accounting is enabled the Access Point will set this value to *RADIUS*.
Acct-Session-Time	46	RFC 2866	The *Acct-Session-Time* attribute is forwarded in the *Accounting-Request* and indicates how many seconds the user has received service for. This attribute may only be present in *Accounting-Request* records where the *Acct-Status-Type* is set to *Stop*.

Table 15: Supported Accounting Attributes *(Continued)*

Attribute Name	Type	RFC	Description
Acct-Input-Packets	47	RFC 2866	The *Acct-Input-Packets* attribute is forwarded in the *Accounting-Request* and indicates how many packets have been received from the user over the course of the connection. This attribute may only be present in *Accounting-Request* records where the *Acct-Status-Type* is set to *Stop*.
Acct-Output-Packets	48	RFC 2866	The *Acct-Output-Packets* attribute is forwarded in the *Accounting-Request* and indicates how many packets have been forwarded to the user over the course of the connection. This attribute may only be present in *Accounting-Request* records where the *Acct-Status-Type* is set to *Stop*.
Acct-Terminate-Cause	49	RFC 2866	The *Acct-Terminate-Cause* attribute is forwarded in the *Accounting-Request* and indicates how the session was terminated. This attribute may only be present in *Accounting-Request* records where the *Acct-Status-Type* is set to *Stop*.
Event-Timestamp	55	RFC 2869	The *Event-Timestamp* attribute is forwarded in the *Accounting-Request* and indicates the time that the accounting event occurred on the Access Point.
NAS-Port-Type	61	RFC 2865	The *NAS-Port-Type* attribute is forwarded in the *Accounting-Request* and indicates the type of physical connection for the user. This attribute value is always set to *Wireless-802.11* by the Mist Access Point.

Dynamic Authorization Extensions

IN THIS SECTION

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 16: 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.*Event-Timestamp attribute validation can be optionally disabled under WLAN configuration.*
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).

NOTE: For more information about CoA, see ."Change of Authorization (CoA)" on page 188

Table 17: 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.*Event-Timestamp attribute validation can be optionally disabled under WLAN configuration*
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

Change of Authorization (CoA)

SUMMARY

Explore the benefits of adding a Change of Authorization (CoA) server to your WLAN.

IN THIS SECTION

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.

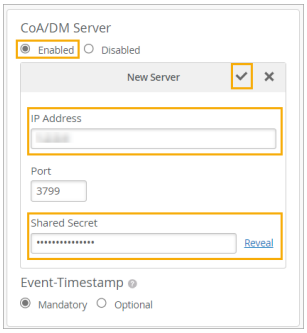
Benefits of Change of Authorization (CoA) in RADIUS

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.

Enabling CoA in the WLAN Settings

In the WLAN settings, go to the **CoA/DM Server** section to enable this feature. Enter the **IP Address** and **Shared Secret**. You can keep the default **Port** value or specify a port.



NOTE: For more help with WLAN settings, see "Configure a WLAN Template" on page 231 and "WLAN Options" on page 235.

How CoA Works

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:

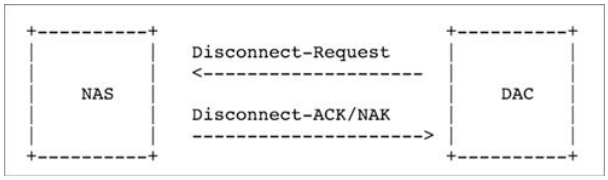
- Enable RADIUS servers to actively modify sessions after authentication, overcoming the constraints of the standard protocol.
- Utilize two key message types (Disconnect and CoA Re-Auth) to manage different session scenarios effectively.
- Address various use cases, such as administrator-initiated session 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

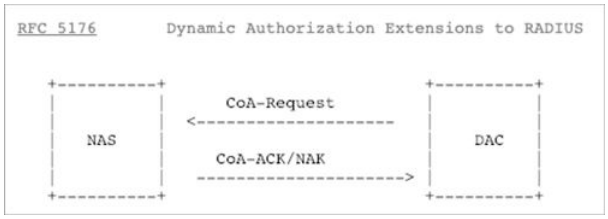
1. Disconnect Message: Session Termination
    - AVP: Acct-Terminate-Cuase

- 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 10:46:49.000000000 PST
        Type: 55
        Length: 6
        Event-Timestamp: Nov 20, 2018 10:46:49.000000000 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




```
3888 2018-12-13 21:27:13.578009    10.2.15.254    10.2.10.13     RADIUS    271 CoA-Request id=37
3889 2018-12-13 21:27:13.583400    10.2.10.13     10.2.15.254    RADIUS     86 CoA-ACK id=37
3890 2018-12-13 21:27:13.585375    10.2.10.13     10.2.15.254    RADIUS    205 Access-Request id=1
3892 2018-12-13 21:27:13.599993    10.2.15.254    10.2.10.13     RADIUS    286 Access-Accept id=1

▸ Frame 3888: 271 bytes on wire (2168 bits), 271 bytes captured (2168 bits)
▸ Ethernet II, Src: Microsof_b2:e8:0e (00:15:5d:b2:e8:0e), Dst: Mist_3e:d2:28 (5c:5b:35:3e:d2:28)
▸ Internet Protocol Version 4, Src: 10.2.15.254, Dst: 10.2.10.13
▸ User Datagram Protocol, Src Port: 21779, Dst Port: 3799
▾ RADIUS Protocol
    Code: CoA-Request (43)
    Packet identifier: 0x25 (37)
    Length: 229
    Authenticator: 8224d751dab908cccc8fe58124fd140d
    [The response to this request is in frame 3889]
  ▾ Attribute Value Pairs
    ▸ AVP: t=NAS-IP-Address(4) l=6 val=10.2.10.13
    ▸ AVP: t=Calling-Station-Id(31) l=19 val=F0-18-98-57-5D-E4
    ▸ AVP: t=Event-Timestamp(55) l=6 val=Dec 13, 2018 13:27:13.000000000 PST
    ▸ AVP: t=Message-Authenticator(80) l=18 val=27bc61454f9bcc5339beb12f16e43ded
    ▾ AVP: t=Vendor-Specific(26) l=43 vnd=ciscoSystems(9)
        Type: 26
        Length: 43
        Vendor ID: ciscoSystems (9)
      ▸ VSA: t=Cisco-AVPair(1) l=37 val=subscriber:reauthenticate-type=last
    ▾ AVP: t=Vendor-Specific(26) l=41 vnd=ciscoSystems(9)
        Type: 26
        Length: 41
        Vendor ID: ciscoSystems (9)
      ▸ VSA: t=Cisco-AVPair(1) l=35 val=subscriber:command=reauthenticate
    ▾ AVP: t=Vendor-Specific(26) l=76 vnd=ciscoSystems(9)
        Type: 26
        Length: 76
        Vendor ID: ciscoSystems (9)
      ▸ VSA: t=Cisco-AVPair(1) l=70 val=audit-session-id=0a020ffeCTLnZbHwvQwBBLHh606hq/tfezmNVnP9NWDx8Deke64
```

- 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

RELATED DOCUMENTATION

Juniper Mist RADIUS Attributes | 176

Preshared Keys

IN THIS SECTION

Configure and Manage Pre-Shared Keys

SUMMARY

Understand the benefits of pre-shared keys, add them to your WLAN, and refresh them periodically.

IN THIS SECTION

What Are Pre-Shared Keys (PSKs)?

Juniper APs support pre-shared keys (PSKs) to provide secure-channel encryption without an additional authentication server. When enabled for a WLAN, clients must present the secure PSK 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. You can assign PSKs individually, per user, or by groups, to

multiple users via Multi-Pre-Shared Key (MPSK). You also can limit a given PSK to a set number of devices (requires firmware version 0.10 or later).

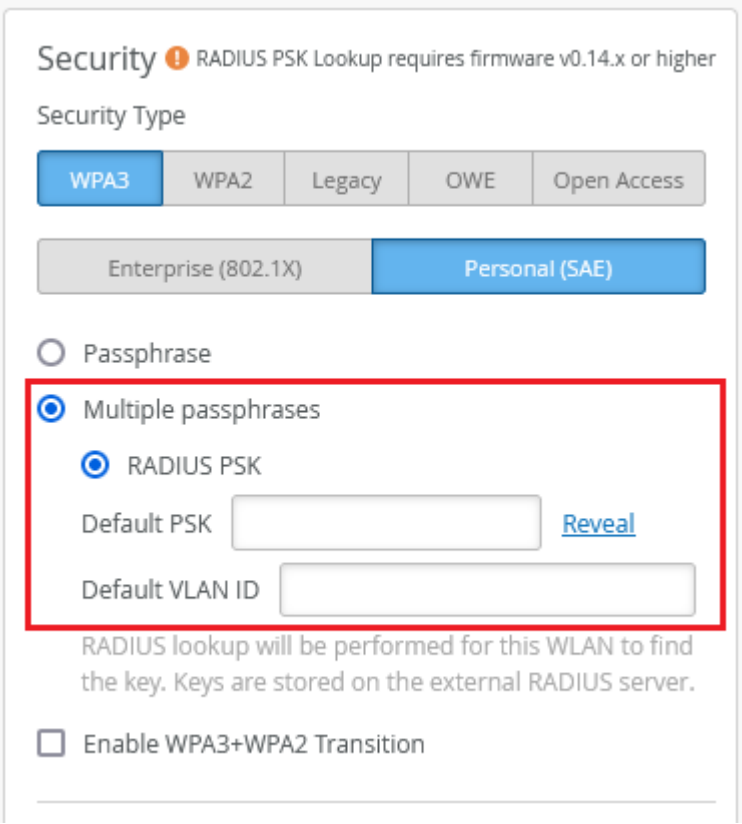
Each PSK in the Mist platform gets its own key name, which is essentially an identity that can be leveraged for user-level accountability for WxLAN policies, key rotation, and visibility in the Mist dashboard. For example, you can assign PSKs individually to corresponding VLANs for dynamic network segmentation 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.

WLAN Security and PSK

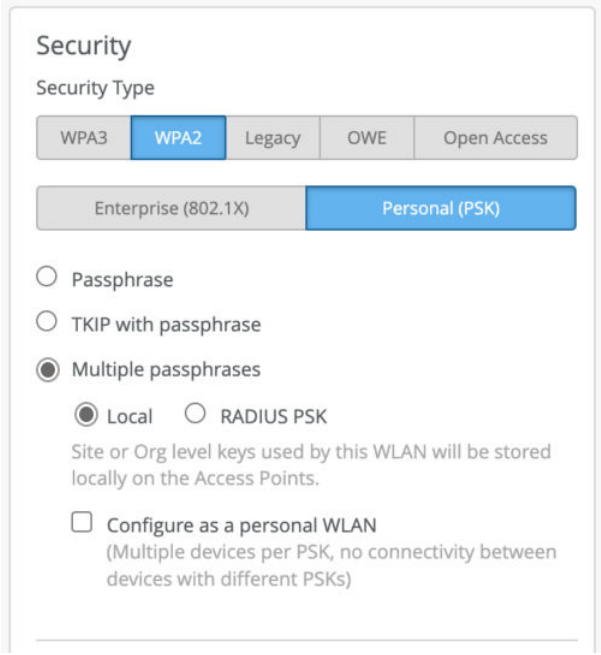
Consider the following options when setting up your WLAN.

- WPA3/802.1X WPA3 (Wi-Fi Protected Access 3) PSK requires AP firmware v0.9.x or later.
- WPA3/SAE requires AP firmware v0.8.x or later.

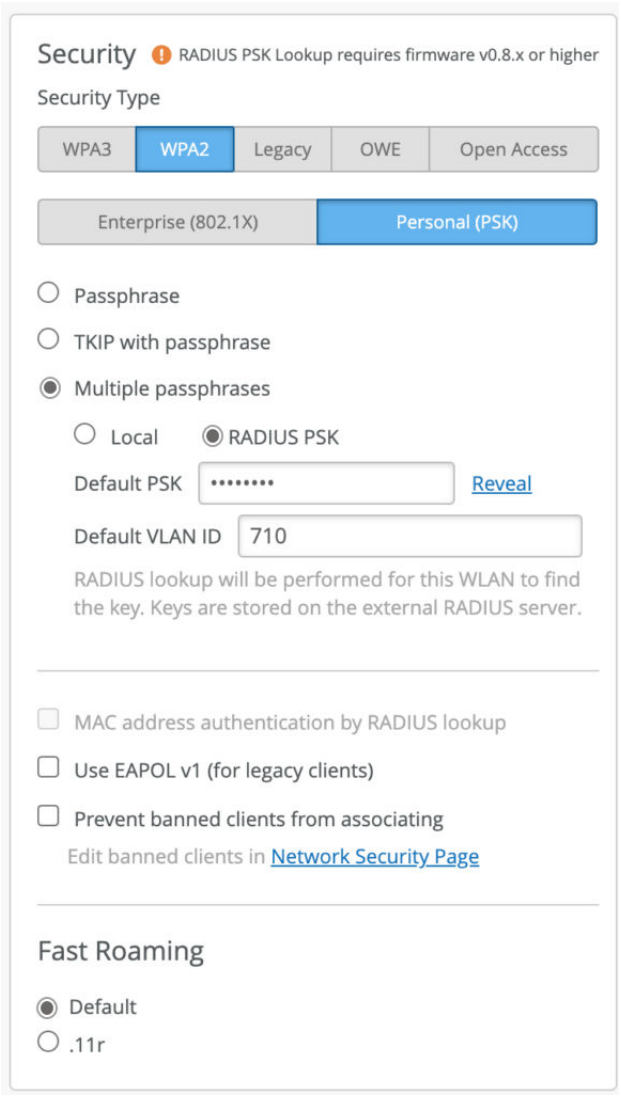
  For the sake of backward compatibility with legacy devices, Juniper Mist also supports (but does not recommend) WPA-PSK and Temporal Key Integrity Protocol (TKIP), the Wi-Fi Protected Access (WPA) security protocol, and Wired Equivalent Privacy (WEP), all of which have known vulnerabilities. These Legacy 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.
- To configure the multiple passphrase option with WPA3, you need AP firmware version 0.14 or higher.



- 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.



- (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.



Additional Options with Access Assurance

Access Assurance for Additional Features

If you have an Access Assurance subscription, you can enable additional MPSK features, including:

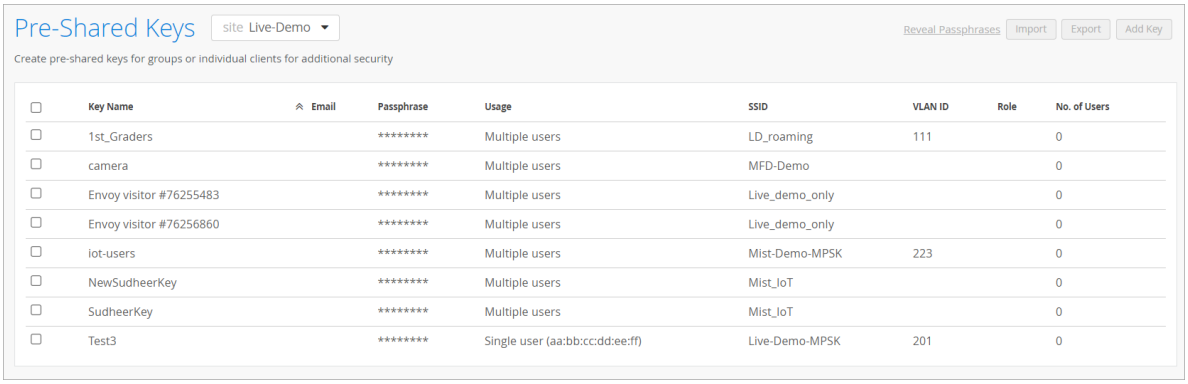
- Cloud-based PSK lookup.
- Support for more than 5000 PSKs at the organization level.
- Automatic client onboarding, and PSK portals.
- Features of the PSK life-cycle management, including PSK expiration, rotation, and per-PSK accounting and visibility (on the Wi-Fi Clients page of the Mist portal).

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).

Configure PSKs

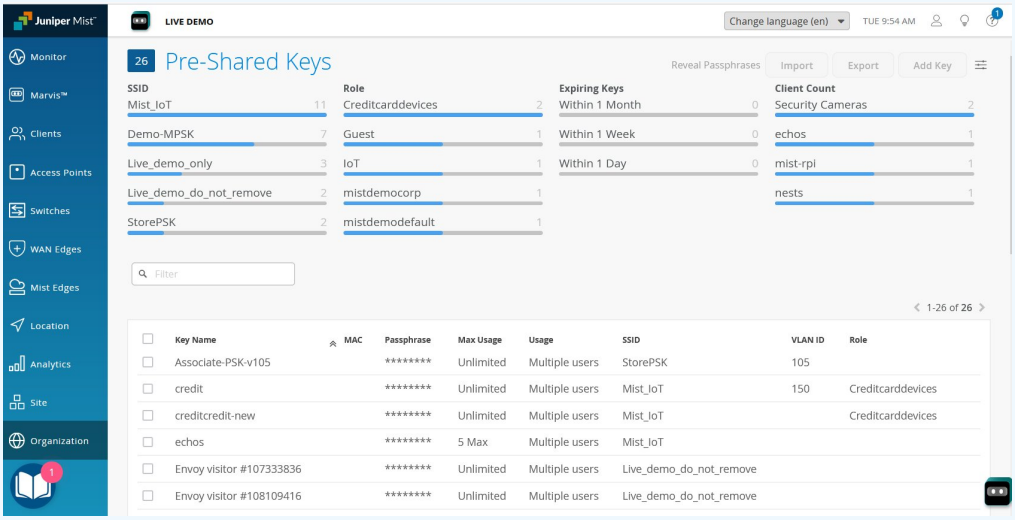
You can add, view, modify pre-shared keys on the WLAN Settings page, the Pre-Shared Keys page, and the Wifi Clients page.

- **WLAN Settings Page**—Navigate to your WLAN or create a new one (see "Adding a WLAN" on page 234).
  - **Security Type**—Select **WPA3** with **Personal (SAE)** or select **WPA2** with **Personal (PSK)**.
  - Enter the **Passphrase** or enable **Multiple Passphrases**.
- **Pre-Shared Keys Page**—From the left menu, select **Site** >**Wireless** > **Pre-Shared Keys**.



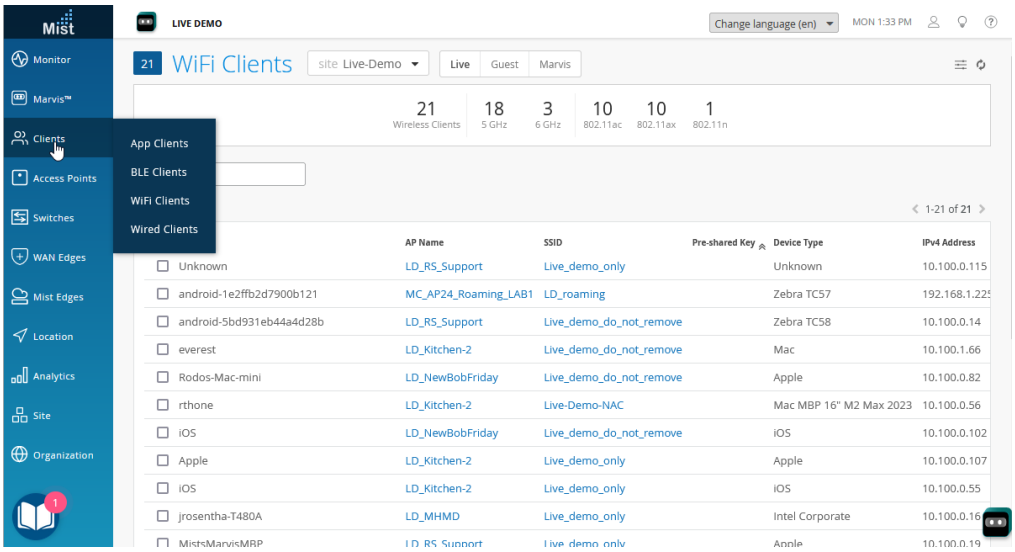
  - To view keys for a site—Select a site at the top of the page.

NOTE: With an Access Assurance subscription, you also can view pre-shared keys at the organization level.



- To change a key's passphrase, role, VLAN, or other properties—Click the key that you want to change. Make your changes, and then click **Save**.
- To add or remove keys—Use the buttons at the top-right corner of the page: **Import**, **Export**, **Add Key**, and **Delete Key**.

- **Wifi Clients Page**—From the left menu, select **Clients** > **WiFi Clients**.



- To view keys for a site or WLAN—Select a site at the top of the page, or enter an SSID in the **Filter** box.

- To change the passphrase—Click the SSID to go to the WLAN page. Under **Security**, enter a new PSK. Then click Save at the top-right corner of the page.

As a best practice, refresh the PSK weekly.

TIP: You can automate the rotation process via email. See "Rotating PSKs" on page 199.

Rotating PSKs

SUMMARY

Rotating PSKs is a best practice to reduce network exposure in the event that a key is compromised. Use this information to understand the benefits of PSK rotation and the steps involved to rotate keys.

IN THIS SECTION

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 "Additional Options with Access Assurance" on page 196 for details.

PSK Rotation

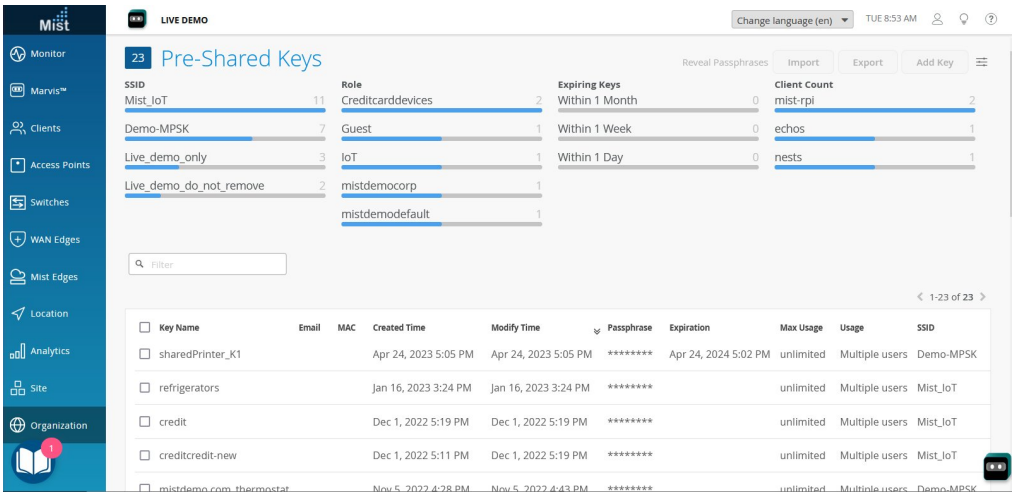
PSK rotation is available for both users and devices. When a key rotation occurs, only the key itself will change. There is no disruption to the existing connection for IoT devices, and any VLANs, roles, and so on that are associated with the PSK will remain the same.

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.

You can also enable e-mail notifications for users when a PSK is created or updated. Do so 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 11: PSK Status and Rotation



Manually Rotate A PSK

PSK rotation is transparent to users. For manual PSK rotation, start by duplicating the old key (which includes all the existing properties and associations), and then switching the users over to the duplicate. When done, remove the original PSK so it can no longer be used.

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

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.

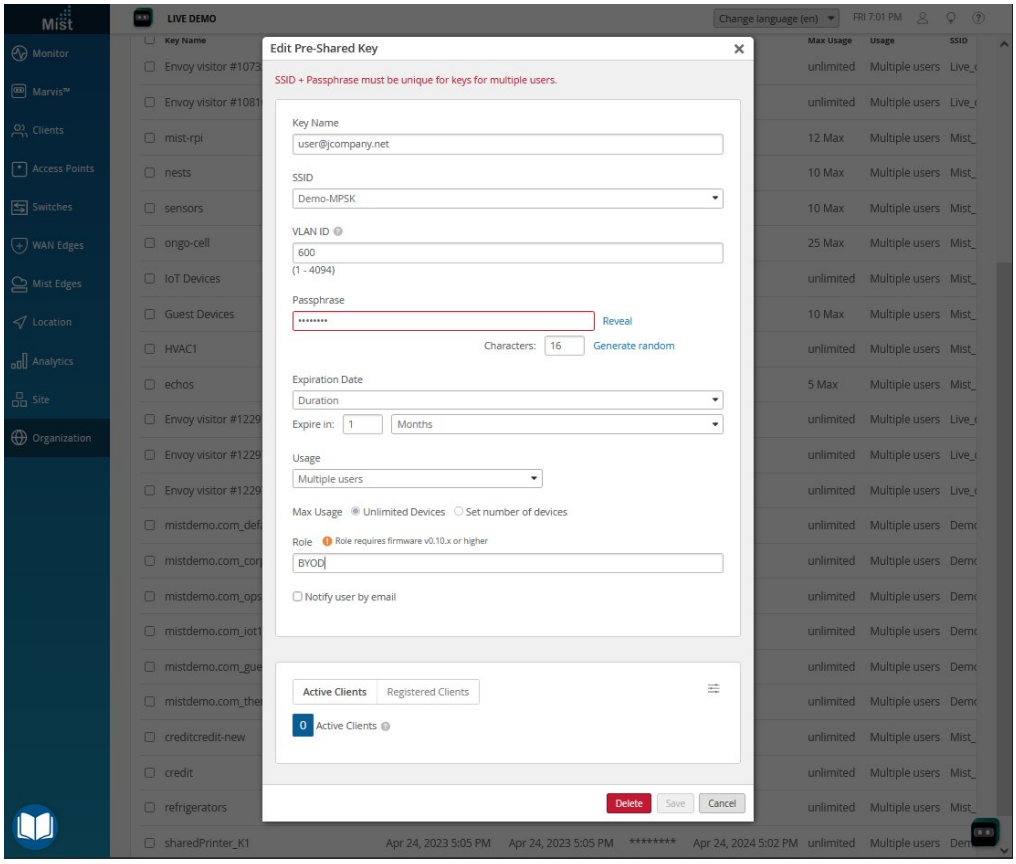
In this use case, you'll use a role to allow BYOD devices to access the internet while blocking them from accessing your private networks.

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**.



NOTE: For more information, see "Configure and Manage Pre-Shared Keys" on page 192.

4. Click **Save**.

Create Labels for the PSK Role and Resources

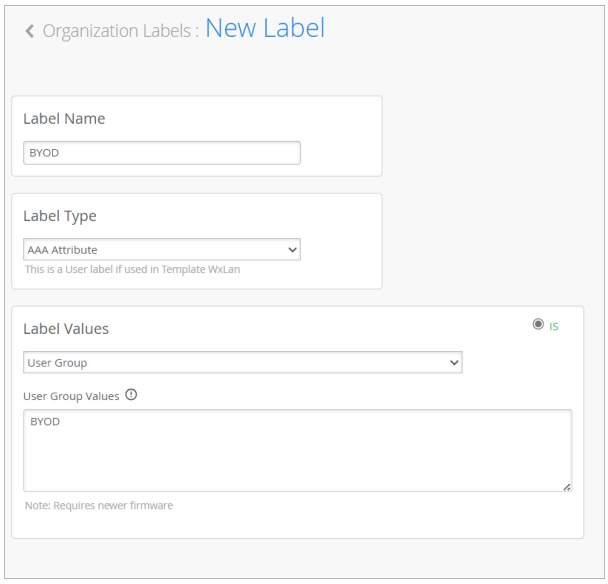
In this use case, you'll create three labels to define the role and resources:

- 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 .

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:



   - **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.

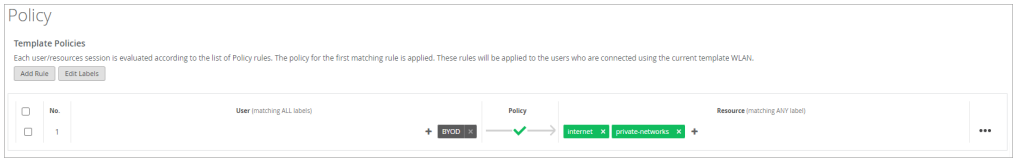
To create a WxLAN policy:

1. From the left menu of the Juniper Mist portal, navigate to the WLAN template where you want to add the rule.

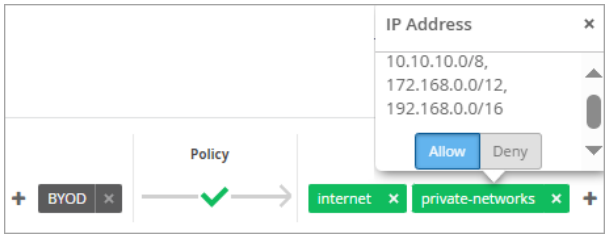
   > **NOTE**: To find out more about access policies, see "WxLAN Access Policies" on page 220.

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.

Rogue, Neighbor, and Honeypot Access Points

SUMMARY

Understand the threat posed by unauthorized access points on or near your site. Learn how to view the list of detected APs, and take action to address these threats.

IN THIS SECTION

What are Rogue, Neighbor, and Honeypot Access Points?

Rogue, neighbor, and honeypot access points (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.

- *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.

- *Neighbor APs* are not connected to your network, but Juniper Mist detects them in the vicinity. Because these nearby APs typically have a strong signal, clients might connect to the neighbor AP, assuming that it's yours and is 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.

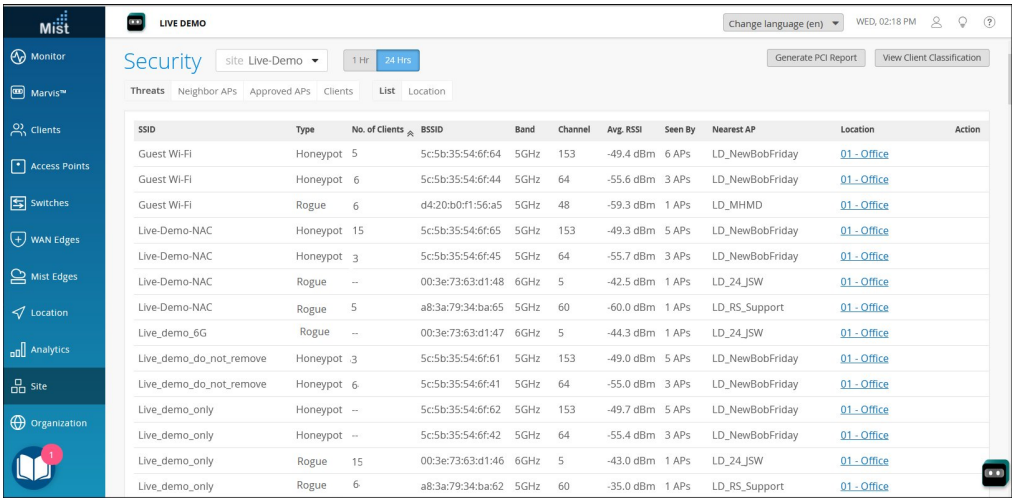
- *Honeypots*, also known as *Evil Twins*, are unauthorized APs that advertise your SSID, typically with the goal of capturing client login credentials. Here, a bad actor may copy or approximate your Wi-Fi hotspot, spoof your organization's login screen, and then collect the username and password of 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.

Dectection of Anomalous Devices

Juniper APs include a dedicated scanning radio to detect and potentially malicious APs and their clients. The dedicated scanning radios operate on 2.4, 5 and 6 GHz Wi-Fi bands. They provide data for real-time performance adjustments on the AP, as well as streaming telemetry that Juniper Mist uses for site-wide optimizations.

In the Juniper Mist portal, the **Site** > **Wireless**> **Security** page provides a list of all the anomalous APs that have been detected. You can drill down on any item to find the physical location, Ethernet connection, and rogue clients connected to the AP. Click on non-zero entries in **No. of Clients** column to open a Rogue Clients List pop-up for clients associated with that device.

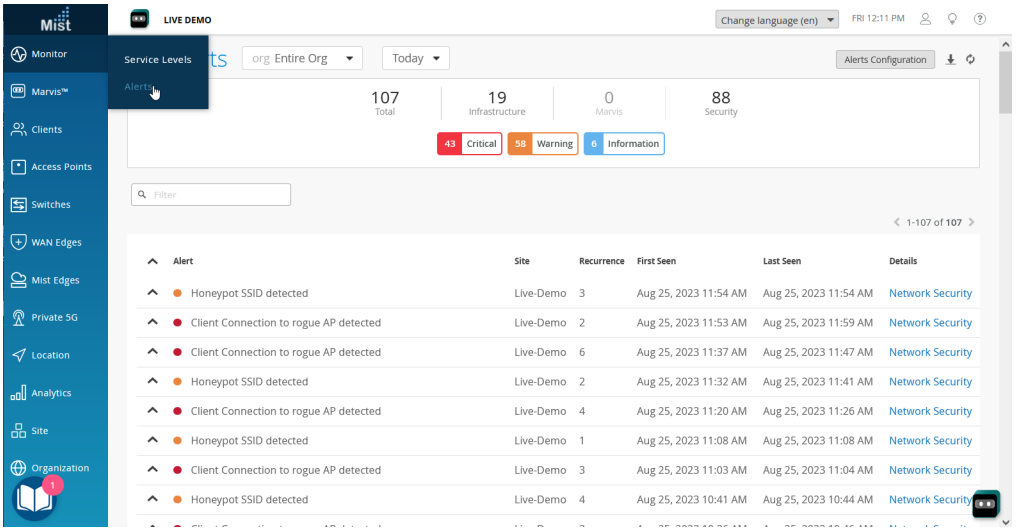
Figure 12: Security Page



The Threats tab on the Security page shows a list of Rogue and Honeypot APs. You can see the lists of **Neighbor APs**, **Approved APs**, and **Clients** by clicking on the appropriate tab above the list.

NOTE: To see this information on this page, you must configure alerts for honeypot and rogue APs for the site or the entire organization.

Figure 13: Alerts Page

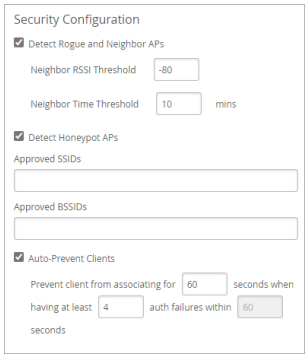


Configure AP Threat Protection

In your site settings, you can enable or disable detection of rogue, neighbor, and honeypot APs. You also can adjust the settings to prevent known APs from being misclassified as threats.

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. Under **Security Configuration**, adjust the settings as needed.



- **Detect Rogue and Neighbor APs**Select this option to enable Rogue and Neighbour detection. You can then configure alerts by going to **Monitor** > **Alerts** and selecting the required alert types.

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**—Select this option to enable detection of honeypot APs (option is selected by default). To configure alerts for detected honeypots, go to **Monitor** > **Alerts** and select the alerts that you want to receive.
- **Approved SSIDs and Approved BSSIDs**—To prevent unnecessary detection of known APs in your vicinity, enter their SSIDs or BSSIDs, 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.

Find and Remove Rogues

You can discover and remove rogue clients from your network on the **Site** > **Wireless** > **Security** page of the Juniper Mist™ portal.

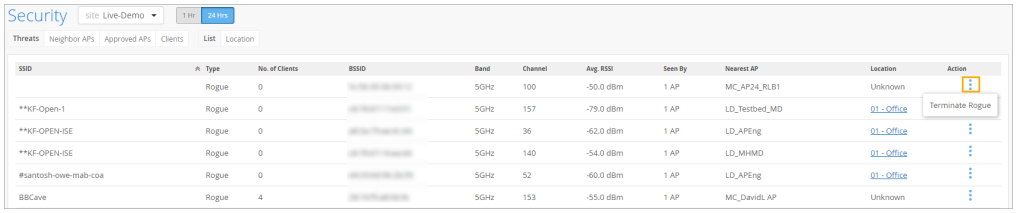
The following animation shows how to find rogue APs and remove them. Basically, when you click the **Terminate** button, nearby Juniper APs will send deauthentication frames to the rogue clients, which are identified by their MAC addresses through their association with the rogue AP. The deauthentication frame is a notification, not a request, and the rogue client will be dropped.

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. 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. For help, see "Classify, Approve, and Ban Designated Wireless Clients" on page 209.

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**.



Classify, Approve, and Ban Designated Wireless Clients

SUMMARY

To protect your network, use this feature to allow or ban access points based on their MAC addresses.

To simplify wireless security and control, you can identify wireless clients that you want to ban or approve.

With AP firmware version 0.9.x or later, clients can be banned or approved from a specific site or from the entire organization.

Classification limitations:

- Firmware version 0.14.x and later—Up to 512 client classifications for a given SSID can be stored locally, on the relevant APs, (Any more than 512 are stored only on the cloud.)
- Earlier firmware versions—Client classifications are stored on the Mist cloud. The AP must be connected to the cloud to reference and enforce the classification.

1. Identify the MAC addresses of the clients that you want to approve or ban.

   TIP: First, go through this procedure for clients that you want to approve. Then repeat the procedure for clients that you want to ban.

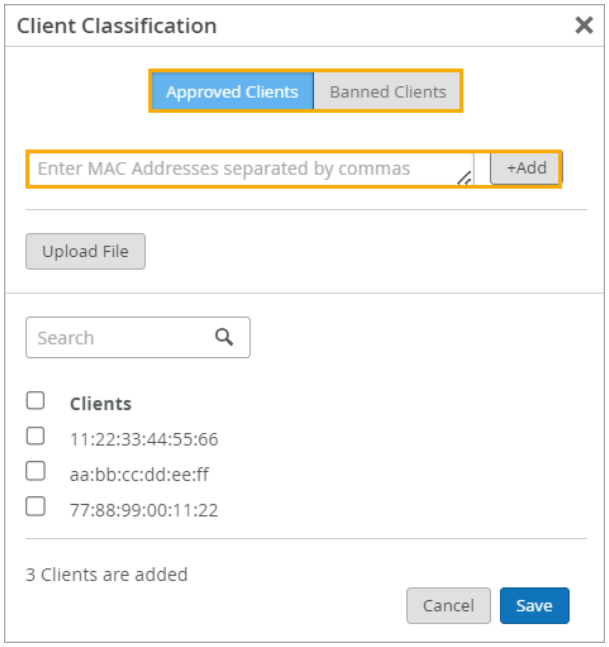
   To find MAC addresses in the Mist portal, use *one* of these methods:

   - Go to **Clients** > **WiFi Clients**, click the client's MAC address, and then copy it.
   - Go to **Site** > **WirelessSecurity**, find the rogue client, and click the client count number. When the Rogue Clients List appears, copy the MAC addresses.

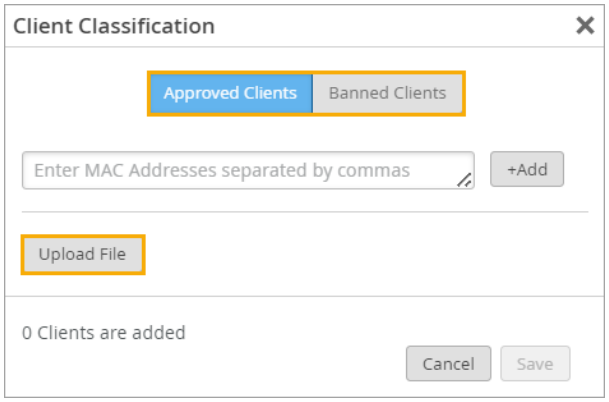
   TIP: If you need to classify multiple addresses, paste them into a text file. Use commas or line breaks to separate the addresses. Save the file as with a CSV file extension.

2. Go to **Site** > **Wireless** > **Security**, and click the **View Client Classification** button in the top-right corner of the page.
3. Click the **Approved** tab or the **Banned** tab.
   - Banned clients—Clients that you want to prevent from connecting to your network. These clients will not be able to join, even if they try through a valid AP. If you choose this option, also complete the additional steps to configure banning.

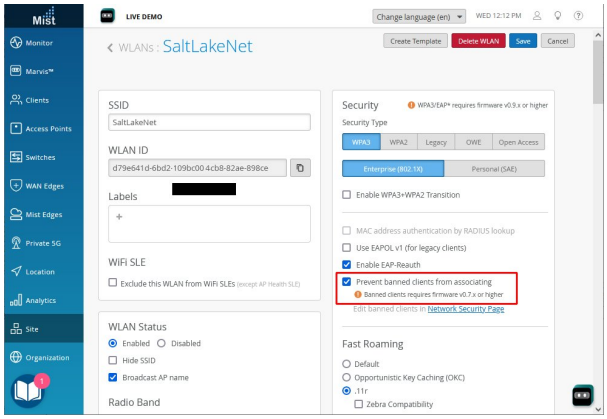
     Approved clients—Clients that you want to allow onto your network. This feature is useful if a legitimate client previously connected through a rogue AP and lost access when the rogue was removed. When you *approve* a legitimate client, they can rejoin the network by reconnecting through a valid AP.
4. Enter the MAC address(es):
   - To enter addresses individually, paste or type a MAC address into the field and then click **+Add**. Repeat this step if needed. The addresses appear in a list at the bottom of the pop-up window. When finished, click **Save**.



- Addresses in a CSV File—Click **Upload File**, select or drag-and-drop the file, and then click **Upload**.



5. If you entered a list of banned clients, also complete these steps to prevent them from associating with your APs.
   a. From the left menu, select **Site** > **Wireless** > **WLANs**.
   b. Select the WLAN.
   c. Under **Security**, select **Prevent banned clients from associating**.
   d. Click **Save** at the bottom of the Edit WLAN window.



CAUTION: Banning rogue clients from an SSID should be considered in the larger context of *client blocking*. Consult applicable regulations, such as the U.S. Federal Communications Commission prohibition against Wi-Fi blocking.

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.

IN THIS SECTION

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 security policies and best practices, PCI DSS enables security personnel and network administrators to effectively thwart various threats to payment data. PCI DSS 4.0 went into effect for assessments in March 2022.

The network is a critical cornerstone of PCI DSS compliance because 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. PCI DSS requirements also ensure that the organization defines traceable well-structured policies, procedures, and practices that can be audited.

The wireless network is especially important to retail environments because business operations and digital engagement technologies rely on 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. PCI DSS compliance for wireless networks specifies two types of requirements:

- **Generally applicable wireless**—These requirements 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 requirements are 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 the system with compliant software, and monitoring access.

PCI DSS 4.0 Attestation of Compliance (AOC)

The Juniper Mist solution has been assessed by an independent PCI DSS security assessor to meet PCI DSS 4.0 Attestation of Compliance (AOC).

Cloud Security

The Juniper Mist cloud is outside the CDE environment because 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 security, processing integrity, and availability as listed here:

- Uses SOC2 Type 2/ISO 27001/ PCI cloud data.
- Maintains an information security policy.
- Uses network application firewalls / access control lists.
- Uses Intrusion Detection System (IDS) / Intrusion Protection System (IPS).
- Uses industry standard encryption at various levels.
- Obfuscates data stored in the cloud.
- Integrates security with development cycles, and pen tests are performed to detect vulnerabilities at the network and application.
- Performs regularly scheduled internal and external vulnerability scans.
- Implements annual security awareness training for all in-scope employees.
- Performs an annual risk assessment.

- Includes incident response plan.
- Subscribes to an annual PCI DSS Attestation of Compliance (AOC) by independent PCI DSS security assessor.

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 safe without access control policies between VLANs.
- **Firewall separation**—If the WLAN 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 4.0 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 through 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.

To ensure that the wireless network complies with the generally applicable requirements for PCI DSS, retailers need to pay special attention to the following:

- **Rogue Devices**—These are accidental or malicious APs 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 APs that masquerade as sanctioned APs sending the retailer's AP beacon.
- **Non-compliant and unsanctioned APs**—This category includes sanctioned APs that are out of compliance and running old firmware without critical security. It also includes APs that are neighbors or causing inadvertent interference to the wireless operations inside a retail store or warehouse.

Wireless IDP is required to handle these external devices to monitor the RF environment and isolate APs not used for cardholder data. Traditionally there have been two main ways that WLAN vendors have addressed the requirements for WIDS/WIPS compliance:

- **Part-time**—When not serving clients, APs scan the spectrum for rogue devices. This approach is similar to having a security solution that only works some of the time, not 24x7.

- **Dedicated APs**—These APs provide 24x7 security monitoring of the wireless network. While this approach ensures continuous protection, it explodes the deployment cost for additional APs plus the associated cost of installing PoE cable 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. This approach can cause nightmares in channel planning and can result in insufficient coverage. Some vendors, while offering a tri-radio AP solution with a dedicated third radio, deploy complete overlay monitoring solutions that are orthogonal to the rest of the wireless infrastructure and controller solution. They use isolated islands of data sources, databases, visualization, and even separate controls for radio configuration, control, and provisioning.

Mist APs provide continuous 24x7 scanning of the spectrum alongside 2.4 GHz, 5 GHz, and 6 GHz client access. With this approach, Mist continually scans the spectrum for rogues, honeypots, interference, and anomalies such as unsuccessful connection attempts at a site (which might be a source for a DDoS attack).

The Mist platform maintains a baseline on key metrics for all APs, clients, locations, sites, and site-groups. Mist's AI-powered infrastructure identifies unusual activity at every level of the network. 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. Alerts are generated when key postures change, such as a 4x4 client device appearing as a 2x2 device, or a client device sanctioned for a California location accessing the network from New York.

Securing Wireless in the Cardholder Data Environment (CDE)

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. It helps you remediate the vulnerabilities on the wireless network and enforce policies on the wireless management system.

Table 18: Juniper Mist PCI DSS compliance

PCI DSS REQUIREMENTS 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.

Table 18: Juniper Mist PCI DSS compliance *(Continued)*

PCI DSS REQUIREMENTS FOR WIRELESS	MIST CONFORMS	MIST VALUE PROPOSITION
1.2.3 An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	√	Network diagram includes WLAN SSID and AP inventory.
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. *Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*	√	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 18: Juniper Mist PCI DSS compliance *(Continued)*

PCI DSS REQUIREMENTS 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: • 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).
8.2.8 If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.	√	Authentication parameters are set to meet these requirements.
8.3.4 Invalid authentication attempts are limited by: • Locking out the user ID after not more than 10 attempts. • Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.	√	Authentication parameters are set to meet these requirements.

Table 18: Juniper Mist PCI DSS compliance *(Continued)*

PCI DSS REQUIREMENTS FOR WIRELESS	MIST CONFORMS	MIST VALUE PROPOSITION
8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). • Contain both numeric and alphabetic characters.	√	Authentication parameters are set to meet these requirements.
9.1.3 Restrict physical access to APs, 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 AP 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 that is hosted in a SOC 2 Type 2 Data Center.
11.1 Implement processes to test for the presence of APs (802.11), and detect and identify all authorized and unauthorized APs on a quarterly basis. *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.*	√	Mist WIDS/WIPS allows detection of authorized and unauthorized APs 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.

Generate a PCI Report

SUMMARY

If your access points (APs) handle cardholder data, you can run a report to check for "compliance" on page 212 with the Payment Card Industry Data Security Standard (PCI DSS).

Before you run a PCI DSS report for a site, ensure that all of the site's access points (APs) are in the Connected state. If APs are in the Disconnected state, the appendix section of the report will display a message indicating that the AP's firmware could not be determined.

How to generate a PCI report:

1. From the left menu, select **Site** > **Wireless** > **Security**.
2. At the top of the Security page, click **Generate PCI Report**.
3. Follow the on-screen prompts to complete the sections of the pop-up window.
   - Included Sites—Select the sites or site groups to include. Then click **Next**.
   - SSIDs Transmitting Cardholder Data—Select the WLANs and specify the VLANs that move cardholder data. Then click **Next**. You must enter at least one VLAN ID to see the Next button for this section.
4. When you see confirmation that all sections are complete, click the **Generate PCI Report** button.
5. When the **View Report** link appears, click it to read the report.

TIP: You can use the printer button to send the report to your printer or PDF maker.

6. Click **Close** to return to the Security page.

RELATED DOCUMENTATION

PCI DSS Compliance | 212

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 options so that you can create WxLAN access policies for your use cases.

IN THIS SECTION

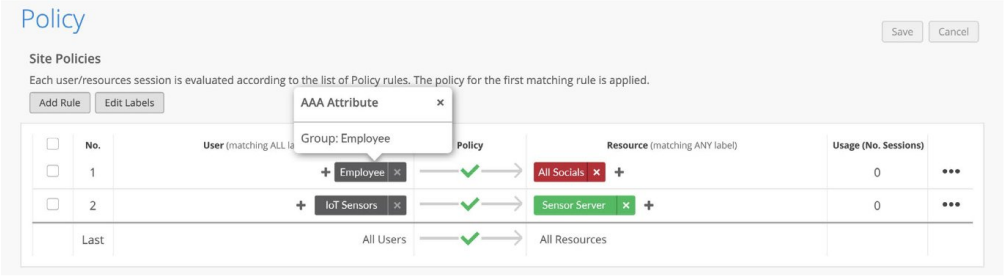
Introduction

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 14: 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

How Policy Rules Are Processed

- When you create an access policy in your WLAN template (an organization-level policy), any user who connects through one of the specified WLANs is first evaluated for the policies in the template. If a user does not satisfy any of these rules, then the user is evaluated for site-level policies.
- 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* resources, then only that resource is allowed for the user and everything else is denied.
- If a rule consists of only *deny* resources, then only that resource is denied for the user and everything else is allowed.

- If a rule consists of *allow* and *deny* resources, then you must explicitly define all allowed and denied resources. There's no default "deny all other traffic" unless you add a rule such as deny 0.0.0.0/0.
- 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 Label to Use in a WxLAN Policy

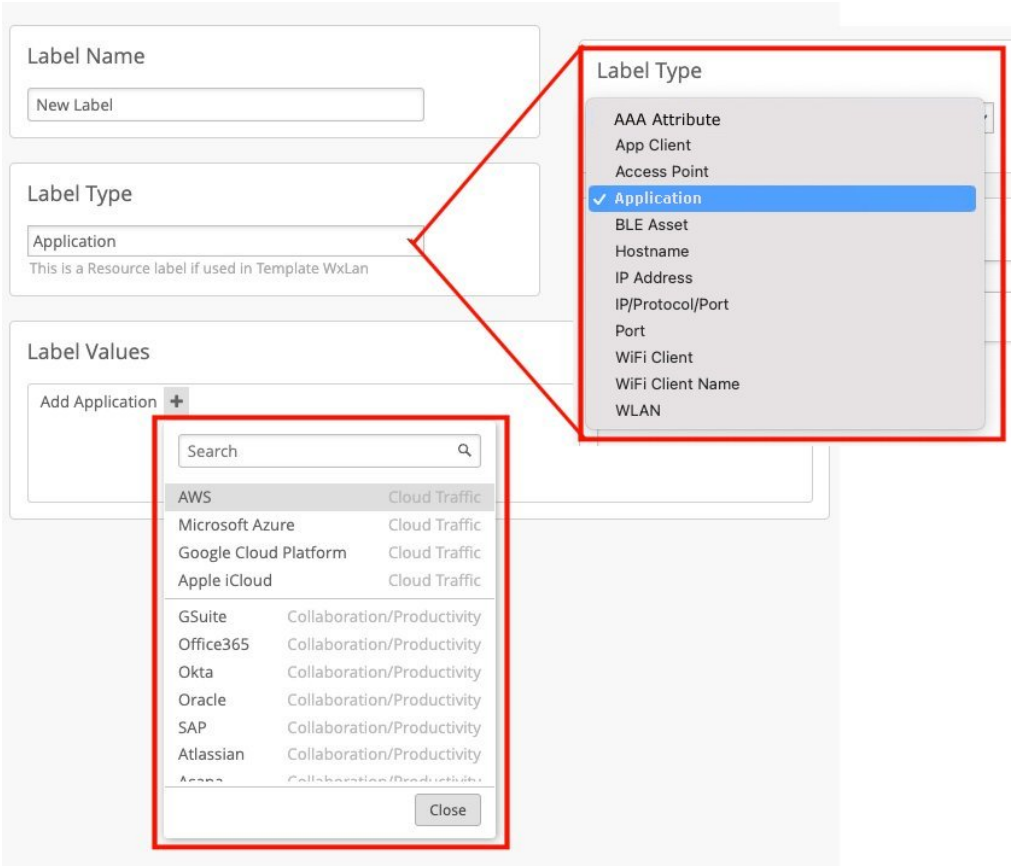
SUMMARY

Optionally, you can use labels to streamline the process of setting up WxLAN policies.

In Juniper Mist™, labels represent a collection of users or resources. (You might compare Mist *labels* to *tags* or *groups* in some other applications.) By using one simple label to represent several related items, you avoid having to specify each item individually when you set up an access policy.

You can create a label at the organization level or the site level. The main difference is where you use these labels. You can use organization-level labels in the policies for WLAN templates. You can use site-level labels in site-level policies.

1. Select the correct menu option for organization-level or site-level labels:
   - Organization-level label—From the left menu of the Juniper Mist portal, select **Organization** > **Wireless** > **Labels**.
   - Site-level label—From the left menu of the Juniper Mist portal, select **Site** > **Wireless** > **Labels**.
2. Click **Add Label** at the top-right corner of the page.
3. Enter a **Label Name**.
4. Select a **Label Type**.



NOTE: Certain label types can only be used for users or resources in WxLAN policies.

- User types—AAA Attribute, Access Point, WiFi Client, WLAN
- Resource types—Application, Hostname, IP Address, Port

5. Enter the **Label Values**.

   The required fields depend on the selected Label Type.
6. Click **Create** at the top-right corner of the page.
7. Create other labels as needed.

Your labels will now be available in the drop-down list when you're selecting Users or Resources for an WxLAN policy.

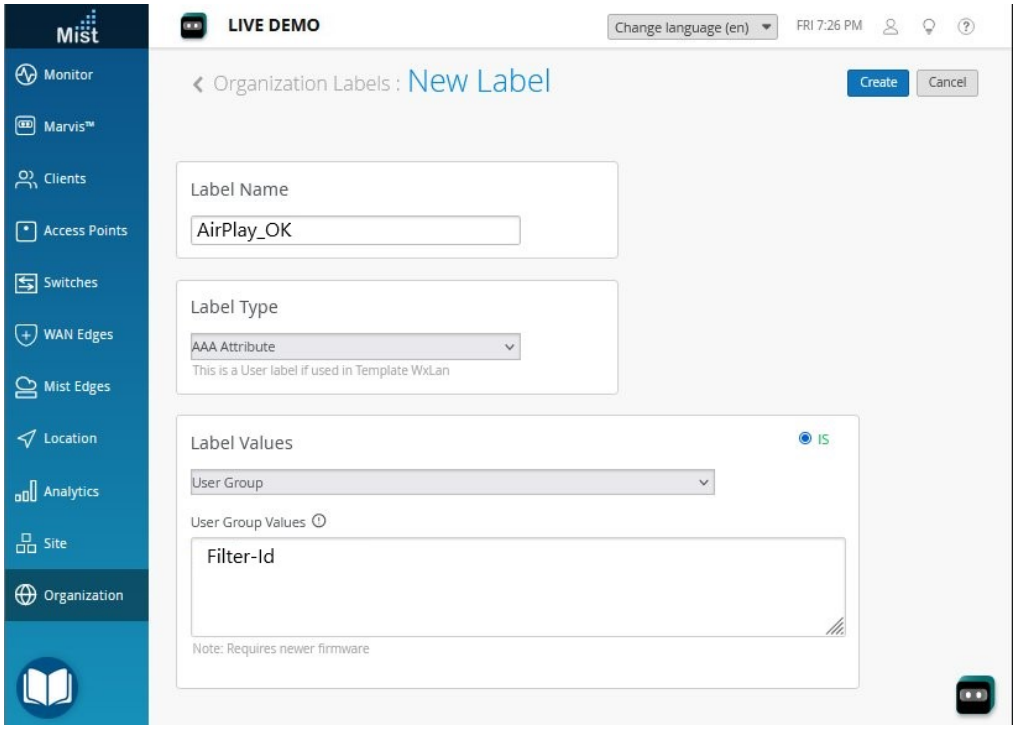
Example: Creating and Applying Labels for Bonjour Filtering

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**.

To create 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 that you want to connect this user role to.



4. Click **Create** at the top of the page.
5. Identify the clients to associate with this label.

   In this animated GIF, you see how to select the clients on the WiFi Clients page and edit the client properties to assign a label that you created earlier.

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

Your labels will now be available in the drop-down list when you're selecting Users or Resources for an WxLAN policy.

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 a Label to Use in a WxLAN Policy" on page 222.

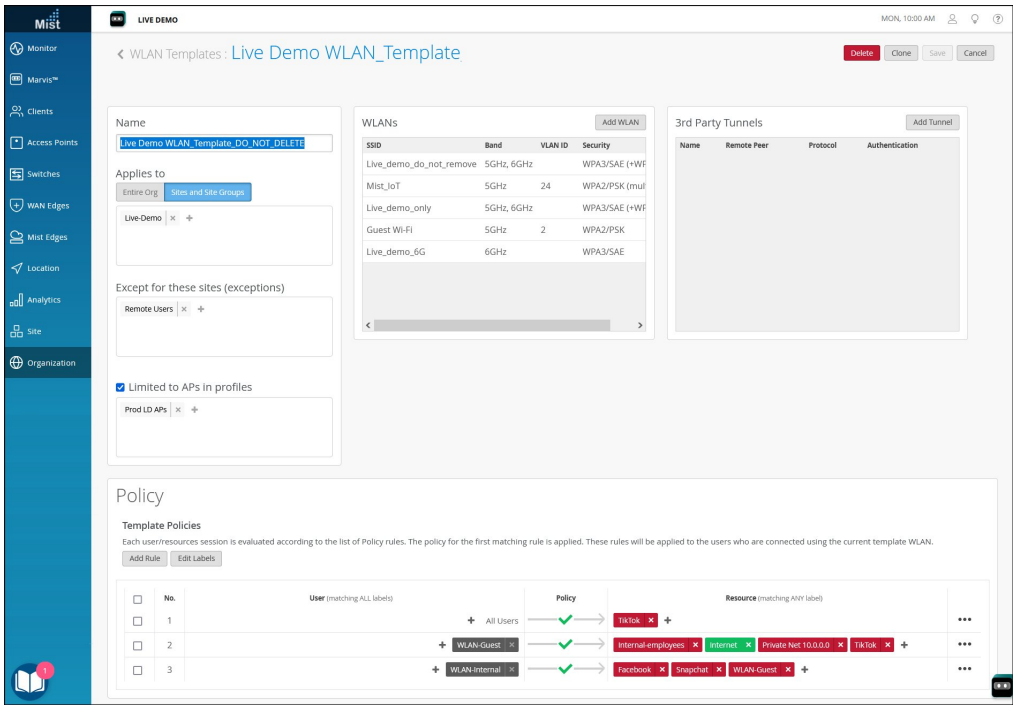
To create a WLAN access policy:

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 or user label from the list that appears.

   NOTE: For help creating user labels, see .
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.

NOTE: For help creating resource labels, see .

In this example, you see a policy with multiple rules and rules with multiple resources.



6. When finished creating and ordering the policy, click **Save** at the top of the screen.

Using Labels in a WxLAN Policy

SUMMARY

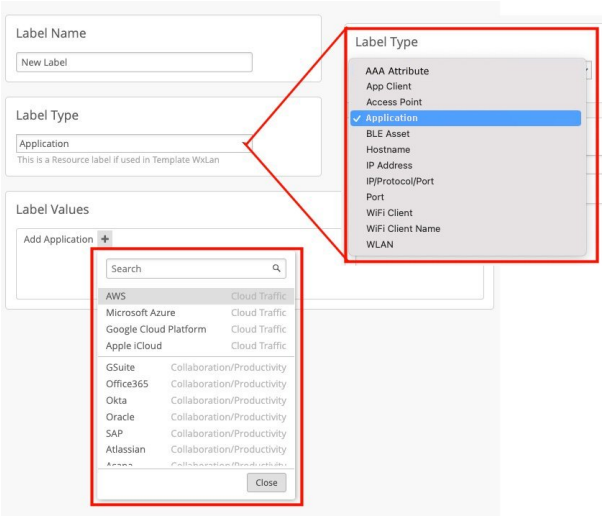
Use labels to identify users and resources in your WxLAN policies.

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 15: Creating Labels



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 top-right corner of the page.

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.

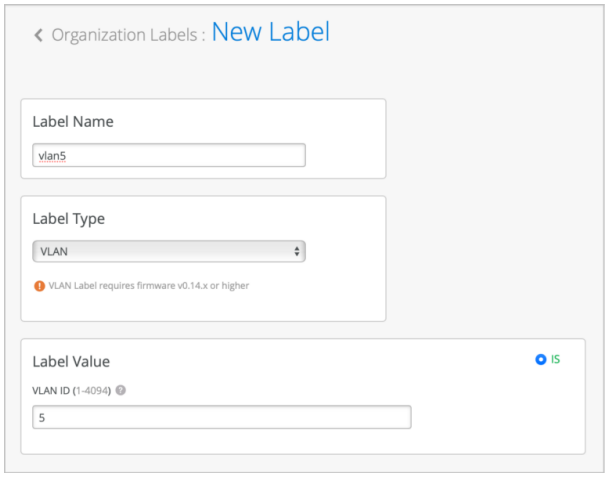
Requirements

- 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.



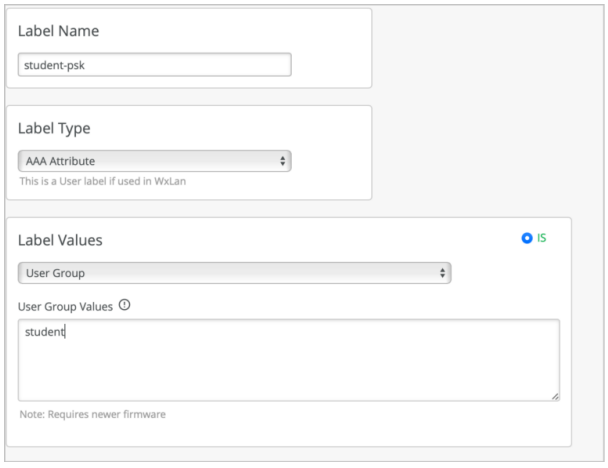
3. Click **Save** to save the new label.
4. Click **Add Label**, and set up the label for the PSK user role that you want to use in your WxLAN policy:

   - **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.



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**.

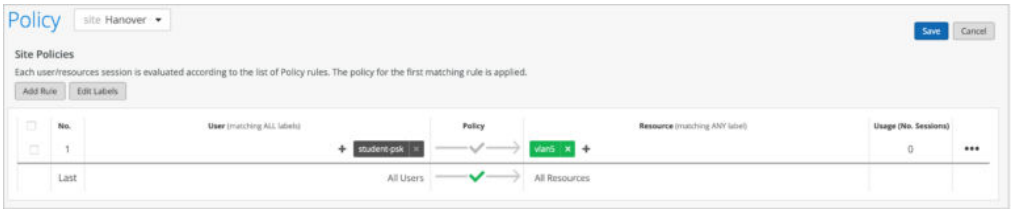
b. Click the template that you want to add the policy to.

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.



f. Click **Save**.

g. Click the ellipsis button (...) to enable the new rule.

Using WLAN Templates in a Device Profile

A WLAN template is a collection of WLAN policies, tunneling policies, and WxLAN policies. Instead of having to repeat a given configuration across multiple SSIDs, with WLAN templates you can set it once and then attach APs to the template to automatically inherit the setting. Both the APs and WLAN must belong to the same site.

- From the main menu, create or modify a WLAN Template from the device profiles page or by clicking **Organization | Wireless > WLAN Templates.**
- From the device profiles page, use the **WLAN Templates** link to open the WLAN Templates screen and create or modify a WLAN template.

Configure a WLAN Template

SUMMARY

Configure and use WLAN templates to streamline the configuration process and ensure consistency across various WLANs in your organization.

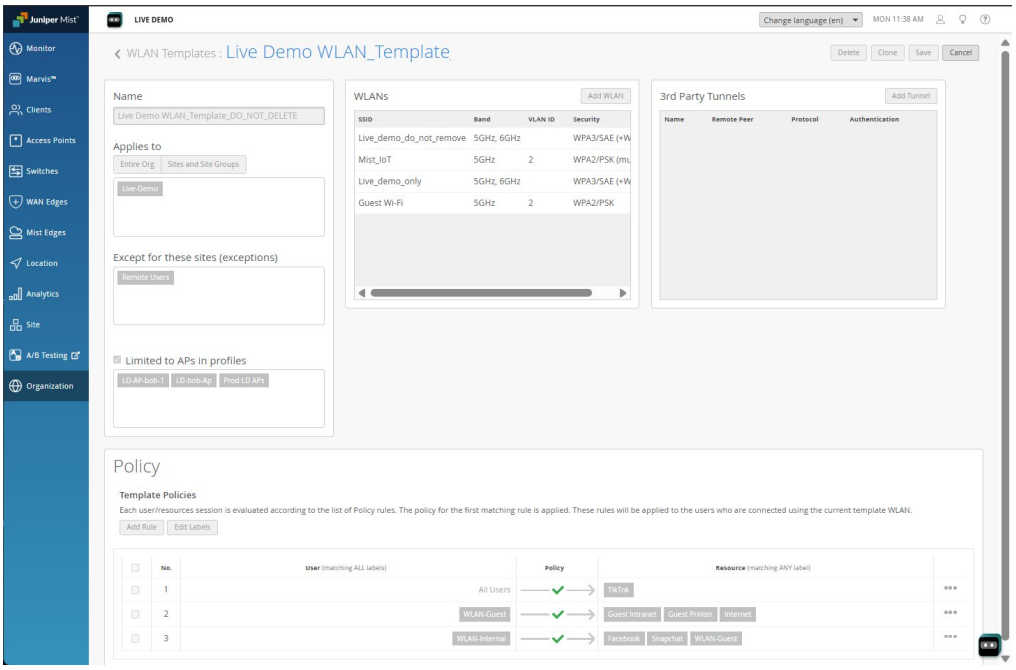
In the Juniper Mist portal, WLAN templates (**Organization > Wireless > WLAN Template**) give you a way to configure uniform user policies, and to selectively apply them to your organization, selected sites, and/or selected WLANs. Policies created in a WLAN template allow you to manage users' access to specified resources, such as social media sites. You can also use them for network segmentation, for example to keep IoT devices off the private network and thus limit exposure in the event of malicious actors gaining access to a device.

In large deployments, we recommend that you create one WLAN template for each WLAN (SSID). To assist with automation, we also recommend that you define all WLANs within WLAN templates. WLAN templates are useful for automation and ensuring policy application to:

- multiple sites
- site groups
- entire organization
- exclude specific sites
- APs within specifi device profiles.
- any combination of the above

See "WxLAN Access Policies" on page 220 for details about how to create and use policies.

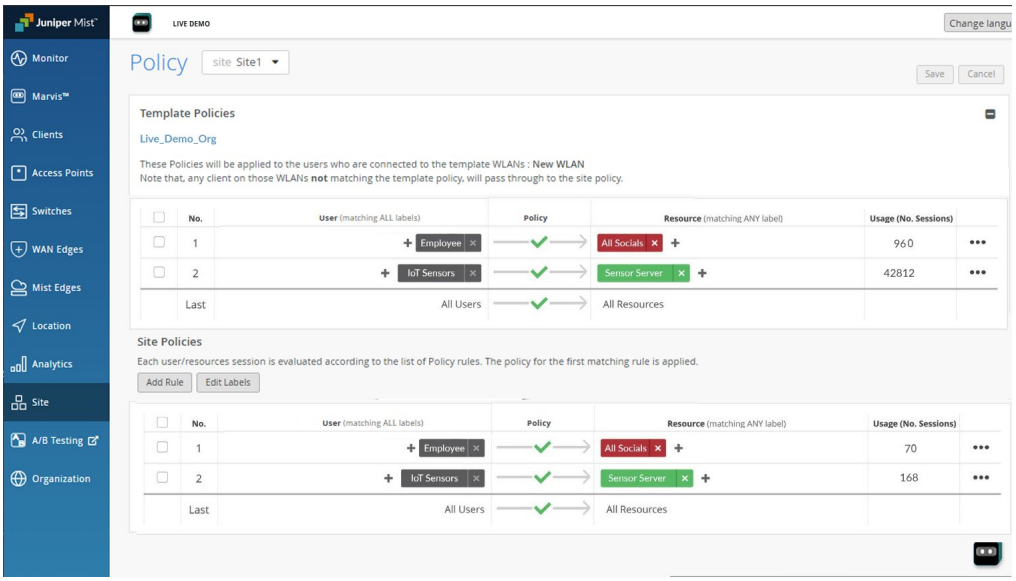
Figure 16: User Policy in a WLAN Template



Note that you can also create site-specific user access policies at the site level: **Site > Wireless | Policy**.

From the site policy page, you can see a policy's usage statistics, that is the hit count, or how many times the policy has been applied, for both site policies and those created as part of a WLAN template.

Figure 17: User Access Policy Summary



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. See "WLAN Options" on page 235 for additional information.

   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.

   We recommend having only one WLAN in each WLAN Template. This makes management and changes easier.
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 one or more policies, and/or include a third-party tunnel (uncommon).

   - "WxLAN Access Policies" on page 220

   - "Configure a Third-Party Tunnel" on page 252
7. Click **Save** at the top right-corner of the template page.

Adding a WLAN

SUMMARY

Configure security, Wi-Fi protocols, radio band, and other features to support your use cases and meet the needs of your WLAN users. 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 231 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: For tips about the various WLAN settings, see "WLAN Options" on page 235.
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 231.

WLAN Options

SUMMARY

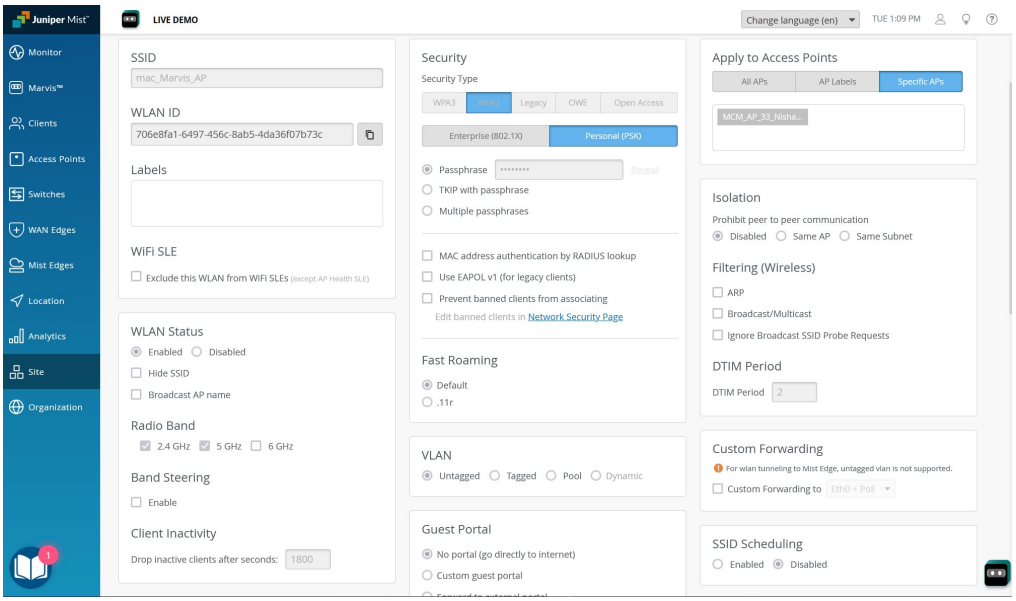
Get familiar with the various options available on the WLAN settings page, and configure features such as security, radio band, geofence, peer-to-peer isolation, and more.

IN THIS SECTION

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 231 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.
- Some changes will reset the radio. See "WLAN Changes That Reset The Radio" on page 260 for more information.

Figure 18: WLAN Settings



WLAN Configuration Settings

Table 19: WLAN Settings

Setting	Summary
SSID	This is the name the WLAN will broadcast for clients to see. 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.
Wi-Fi SLE	Select the check box if you want to mark this WLAN as an "excluded WLAN" for your Wireless Service Level Expectations (SLEs). For example, you might want to exclude a test WLAN or a new WLAN that you're fine-tuning. When viewing the Wireless SLEs dashboard, you can hide or show any excluded WLANs. This exclusion applies to all SLE metrics except AP Health, which includes all WLANs without exception.

Table 19: WLAN Settings *(Continued)*

Setting	Summary
WLAN Status	Use this to set whether an AP broadcasts the WLAN. You can also do the following: • Hide the SSID • Broadcast the AP by name • Set Mist to disable a WLAN when the AP has no IP address or default gateway, or on tunneled WLANs when the Mist Edge tunnel is down. This is meant to prevent dead-ending of clients when the AP doesn't have full network connectivity, or has lost connection to Mist Edge. • Enable band steering. Band Steering technology detects whether a connected client has dual-band (2.4GHz and 5GHz) capabilities. Many devices transmitting on 2.4 band in an overcrowded area can cause noise and interference with your wireless connectivity. Enabling Band Steering mitigates this by encouraging the client to join the 5Ghz band if it has a good signal.
Radio Band	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 therefore, less co-channel interference. The 6-GHz band has still more channels, wider channels, more advanced security options, and greater data rates. See "Radio Resource Management (RRM)" on page 344.
Client Inactivity	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 range for the inactivity timer is between 60 and 86400 seconds. The default time is 1800 seconds.

Table 19: WLAN Settings *(Continued)*

Setting	Summary
Geofence	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. See "Enable Geofencing" on page 253.
Data Rates	Set data rates to prevent clients with slow connections from degrading the overall WLAN performance. The default is **Compatible**, which allows all connections. The other options are: • **No Legacy (2.4G, no 11b)**—Prevents 802.11b devices from joining the WLAN (which, in effect, adds capacity to the network). • **High Density (disable all lower rates)**—Prevents 802.11b and 802.11g clients from joining the network, and also sets a minimum signal level to connect. This setting can affect client roaming. It can also prevent legacy devices from joining the network, which may be desirable from a capacity standpoint, or the opposite, for example, if you have a lot of legacy devices that are cut off. • **Custom Rates**—See "Wi-Fi Data Rate Configuration" on page 254.
Wi-Fi Protocols	Enable or disable various versions of Wi-Fi. When you enable a Wi-Fi version, its features become available on the APs that support that protocol.

Table 19: WLAN Settings *(Continued)*

Setting	Summary
WLAN Rate Limit	Use WLAN rate limits to set uplink and downlink limits for the WLAN bandwidth. You can configure rate limits per AP, per client, and per application. You can also limit the total bandwidth allocation for a given application. The rate limit field also supports site-level variables per WLAN and per client, as an option to hard-coding the values (that is, making them global). This is especially useful in WLAN templates, where you want to configure a core configuration for common use, but also want the flexibility of site-specific differences. You can add variables on the **Organization** > **Admin** > **Site Configuration** page. **NOTE**: Depending on your exact use-case, setting a rate limit may be self-defeating in wireless networks because it can increase the client's airtime consumption. Since airtime is usually the most precious resource in wireless networks, consuming more of it by rate-limiting the comparatively plentiful bandwidth often ends up degrading your overall network performance.
Per-Client Rate Limit	Set the uplink and downlink rate per client. **NOTE**: Mist applies this rate limit to all wireless clients on the selected SSID. There is no way to tune the limits on an individual client basis. The effect of setting values in these fields is to limit each and every wireless client to the uplink and downlink values you set.
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.

Table 19: WLAN Settings *(Continued)*

Setting	Summary
Apply to Access Points	Select the APs you want this WLAN to apply to: All, Specific, or according to the AP label. By default, all APs in a selected site or site group will get the WLAN configuration and beacon the SSID. Based on the use-case or the requirements, you can apply filters to have the WLAN configured only on AP labels or Specific APs. **NOTE**: You can create labels at the organization or site level. From the left menu, select **Organization** > **Wireless** > **Labels** or select **Site** > **Wireless** > **Labels**. 1. Give your label a name. 2. Select a **Label Type** of **Access Point**. 3. Under **Label Values**, click the plus sign to Add Access Point, then select the **Entire Org** tab or the **Site** tab. 4. Select the **AP Name** checkbox at the top to select all APs in the org or site, or you can select the checkboxes next to whichever APs as you would like to include in this label. • The AP selection list includes a search filter which allows you to filter APs by MAC address or AP name. For example, if the APs in the site are named in the strings you filter for, you can then bulk select to apply the label to all APs matching the filtered string. 5. Apply the AP label to your WLAN so that only the APs included in the label get the needed WLAN configuration.

Table 19: WLAN Settings *(Continued)*

Setting	Summary

Security Types	WPA3 is the default security type when you create a new WLAN. Both WPA3 and OWE are required for Wi-Fi 6E and Wi-Fi 7. If you want to use security modes such as WPA2 or Open, you will need to disable both 6 GHz and Wi-Fi 7 in the WLAN.
	• **WPA3** using **Enterprise (802.1X)**—RADIUS-based authentication. With this security type, you also can enable additional options:
	  • **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 459.
	  • **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 459.
	• **Open Access**—Unencrypted, typically used for guest networks.

Table 19: WLAN Settings *(Continued)*

Setting	Summary
Other Security Options	Depending on the selected security type, other options include: • **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.
VLAN	• 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	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.) Subnet isolation requires firmware version 0.12 or later, and clients must have a DHCP address.

Table 19: WLAN Settings *(Continued)*

Setting	Summary

Filtering (Wireless)
• ARP
• Broadcast/Multicast
  • Allow mDNS
  • Allow SSDP
  • Allow IPv6 Neighbor Discovery
• Ignore Broadcast SSID Probe Requests
	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.
	• **ARP**—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.)
	• **Broadcast / Multicast**—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.
	• • 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 19: WLAN Settings *(Continued)*

Setting	Summary

Custom Forwarding	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. You can set custom forwarding to:
	• 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.
	• L2TPv3—Standards-based tunnel. If you use this option, you can also set Mist to disable WLAN when the Mist tunnel goes down.
	• Site Mist Edge—Set custom forwarding to a site level Mist Edge and choose a tunnel. You can also set Mist to disable the WLAN when the tunnel goes down by selecting the **Disable WLAN when Mist Tunnel goes down** check box.
	• Org Mist Edge—If you use this option, you can select multiple tunnels to divide the traffic to multiple Mist Edge clusters using VLAN separation. This means, you can set the WLAN to forward to multiple Mist Edge tunnels, as well as local breakout. Within a WLAN, you can decide the forwarding behavior by VLAN. The per VLAN forwarding control enables extremely high scalability in large environments since the AP can forward to different Mist Edge clusters. Another use is SSID consolidation with flexible forwarding. You must ensure that a VLAN is not duplicated on multiple tunnels. You can also set Mist to:
	  • Disable the WLAN when the Mist tunnel goes down by selecting the **Disable WLAN when Mist Tunnel goes down** check box.
	  • Force clients to reconnect when the APs Mist Edge tunnel fails over to a Mist Edge in a different Mist Edge cluster by selecting the **Reconnect clients when Mist Edge Cluster changes** check box. This will be useful to gracefully disconnect the clients if the same IP subnet is not used across Mist Edge clusters.

Table 19: WLAN Settings *(Continued)*

Setting	Summary
SSID Scheduling	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. SSID scheduling supports multiple time ranges for each day. By default this mode is disabled.
802.1X Web Redirect	Applies to VLANs with security type **Enterprise (802.1X)**. 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 171.
QoS Priority	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. 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: • 0=Background (not used by Juniper APs) • 1=Best Effort • 2=Video • 3=Voice
Multimedia Extensions	When multiple concurrent applications compete for network resources, Juniper APs can use MMEs to define and improve the wireless signal quality and performance. Multimedia extensions (MMEs) are architectural extensions to general-purpose processors to boost the performance of multimedia workloads. Throughput is not guaranteed by WMM.

Table 19: WLAN Settings *(Continued)*

Setting	Summary
AirWatch	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.
Bonjour Gateway	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. The following services are available, but must explicitly enabled to be discoverable: • AirDrop, AirPlay, AirPrint, Apple HomeKit • Amazon Devices, GoogleCast, Roku, Spotify Connect • NFS, Scanner, SleepProxy (Wake-On-Network) See "Add a Bonjour Gateway to a WLAN" on page 248.
Security	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. See: • "Enable WPA2/WPA3 Enterprise (802.1X) Security on a WLAN" on page 164 • "Rogue, Neighbor, and Honeypot Access Points" on page 205 • "Configure and Manage Pre-Shared Keys" on page 192

Table 19: WLAN Settings *(Continued)*

Setting	Summary
"Fast Roaming" on page 159	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. • 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.
VLAN	Required for each WLAN. Specify the type of VLAN the AP will use in the switch connection. • 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. For information about using VLAN Pools with Pre-Shared Keys for segmentation, see "Leveraging Roles in a PSK (Use Case)" on page 201.
Guest Portal	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 285.

Tips for Wi-Fi 6E (Video)

SUMMARY

Wes Purvis, Juniper Mist product management director, offers tips based on a full year's experience with large-scale Wi-Fi 6E deployments (May 2023 presentation).

Video: WiFi 6E Year Two

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

SUMMARY

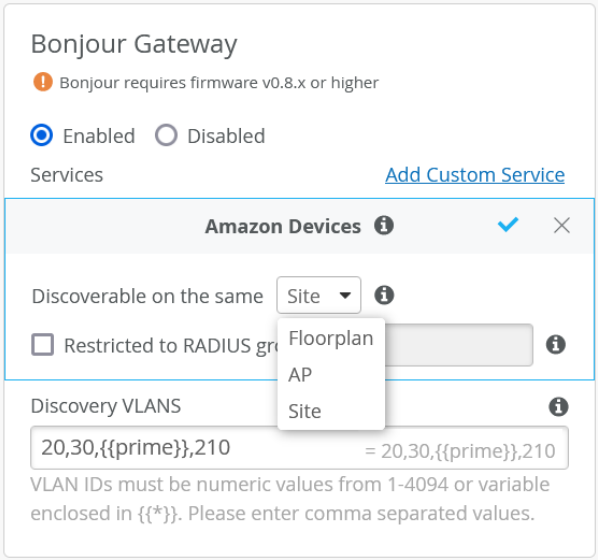
To enable Apple devices and services to discover one another, add a Bonjour gateway to your WLAN.

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 (it can also do so by tunneling through a Mist Edge, for which you should contact Juniper technical support).

Figure 19: Adding a Bonjour Gateway



In Mist, the Bonjour gateway receives discovery queries from eligible clients 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 are forwarded 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. The network here can be the WLAN, a wireless VLAN, or a wired VLAN,

Access Control

When setting up a Bonjour gateway, you can also use it to achieve passive access control by making a given Bonjour service discoverable only to a specified user roles or location. In a classroom setting, for example, you could you could leverage existing RADIUS roles for students and teachers to restrict Apple AirPlay screen casting to teachers only. Students would not see the the service. When setting up wireless printing service, you could leverage the Bonjour gateway so that wireless printers are only discoverable by users located on the same floor as the printer.

Custom Bonjour Services

Bonjour service labels use syntax that include 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 "Example: Creating and Applying Labels for Bonjour Filtering" on page 223.

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:

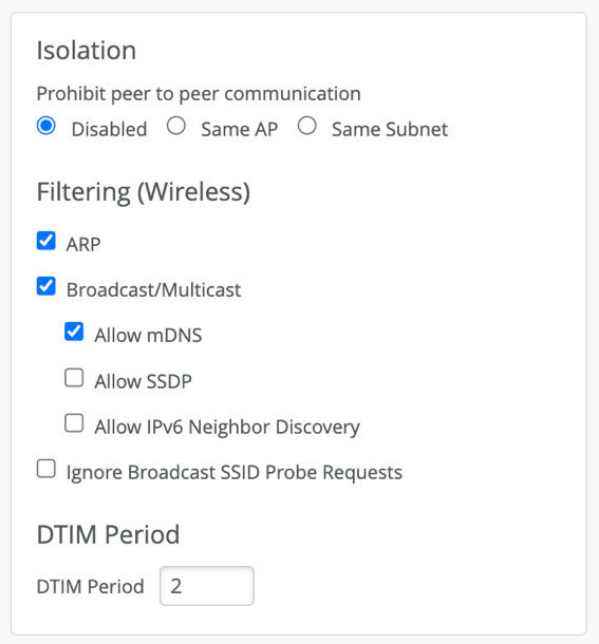
   - If the WLAN is in a WLAN template, select **Organization > Wireless | WLAN Templates**, click the template, and then click the WLAN.
   - For a site-level WLAN, select **Site > Wireless | WLANs**, and then click the WLAN.

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.



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

Configure a Third-Party Tunnel

SUMMARY

Configure a tunnel to connect to VPN concentrators, to aggregate Ethernet interfaces, or implement similar scenarios.

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 Geofencing

SUMMARY

As an extra precaution against unauthorized use of your WLAN, you can enable geofencing.

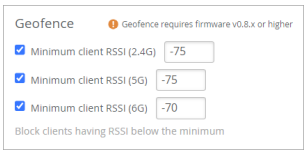
Geofencing is when the AP prevents clients with an RSSI below a set level from connecting to the network, for example to keep users from outside your facility from using your wireless network. Existing clients are not dropped or blocked if their RSSI becomes poor.

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.

Wi-Fi Data Rate Configuration

SUMMARY

Data rate configuration allows you to fine tune the wireless data rates that your WLANs support and enhance wireless performance in multiple network scenarios.

IN THIS SECTION

Overview

Wi-Fi clients and access points (APs) send frames to each other at a particular speed, known as the data rate or transmission rate. Modern clients and APs transmit at speeds of several hundred megabits per second, or even gigabits per second, depending on the client capabilities, AP capabilities, and configuration. However, many of the management and control frames such as beacons, probes, and acknowledgments are sent at legacy rates to maintain backwards compatibility with older devices. Controlling which of these legacy rates are allowed on your network can improve performance and roaming. You'll find the Data Rates configuration block on the **Sites** > **WLANs** page or on the **Create WLAN** pop-up, which you access from **Organization** > **WLAN Templates**.

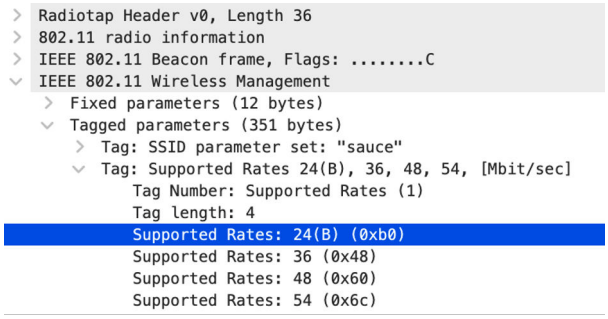
Table 20: Legacy Data Rates

IEEE 802.11 Amendment	Frequency Bands	Data Rates in Mbps
802.11a	5 and 6 GHz	6, 9, 12, 18, 24, 36, 48, and 54
802.11b/g	2.4 GHz	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54

There are arguments for and against disabling low data rates. However, disabling certain lower legacy data rates will help your WLAN perform better. For example, you will experience considerable capacity penalties if you enable the 802.11b 1 Mbps rate on multiple WLANs.

Changing the data rate settings in Mist modifies the supported and basic rates advertised in the beacon frames, probe responses, and association responses per WLAN and frequency band. The minimum basic rate (MBR) is the rate at which beacons, probes, management, control, broadcast and multicast frames are sent. The minimum basic rate is also known as lowest basic rate or mandatory minimum rate. Figure 1 on page 255 below is an example beacon frame that shows four supported data rates with 24 Mbps as the MBR.

Figure 20: Example Beacon Frame

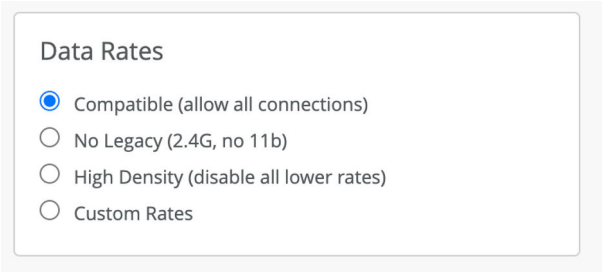


Configuring data rates for Wi-Fi networks is essential for optimizing WLAN performance and ensuring compatibility across various client environments. This feature allows you to enable or disable specific data rates, thereby fine-tuning network performance through four configuration options: Compatible, No Legacy, High Density, and Custom. Each configuration controls the minimum basic rate (MBR) and the supported data rates, which directly influence how management and control frames are transmitted.

Data Rate Configuration Options

With Mist, configuring data rates for Wi-Fi networks involves selecting from four distinct configuration options: Compatible, No Legacy, High Density, and Custom.

Figure 21: Data Rate Configuration Options



- The **Compatible** option:
  - Sets 1 Mbps as the MBR
  - Enables all data rates for maximum compatibility
  - Is ideal for environments with diverse client devices
- The **No Legacy** option:
  - Sets 12 Mbps as the MBR
  - Disables 802.11b and thus the 1, 2, 5.5, and 11 Mbps data rates
  - Is recommended for most scenarios except when your WLAN must support 802.11b clients
- The **High Density** option:
  - Sets 24 Mbps as the MBR
  - Disables all data rates below 24 Mbps
  - Is recommended for environments with high AP density
- Figure 3 on page 257 shows the Basic (Mandatory) and Optional (Supported) data rates for the 2.4, 5, and 6 GHz bands in each of the three predefined data rate configuration options: No Legacy, Compatible, and High Density. For each data rate in each band, **Basic** = basic/mandatory, **Optional** = supported/optional, and **N/A** = not supported.

Figure 22: Predefined Data Rate Groups

No Legacy

2.4GHz Rate Setting		5GHz Rate Setting		6GHz Rate Setting	
1 N/A	12 Optional	6 Basic	24 Basic	6 Basic	24 Basic
2 N/A	18 Optional	9 Optional	36 Optional	9 Optional	36 Optional
5.5 N/A	24 Optional	12 Basic	48 Basic	12 Basic	48 Basic
6 Basic	36 Basic	18 Optional	54 Basic	18 Optional	54 Basic
9 N/A	48 Optional				
11 N/A	54 Optional				

Compatible

2.4GHz Rate Setting		5GHz Rate Setting		6GHz Rate Setting	
1 Basic	12 Optional	6 Basic	24 Basic	6 Basic	24 Basic
2 Basic	18 Optional	9 Optional	36 Optional	9 Optional	36 Optional
5.5 Basic	24 Optional	12 Basic	48 Optional	12 Basic	48 Optional
6 Optional	36 Optional	18 Optional	54 Optional	18 Optional	54 Optional
9 Optional	48 Optional				
11 Basic	54 Optional				
HT + VHT		HT + VHT		HE + EHT	

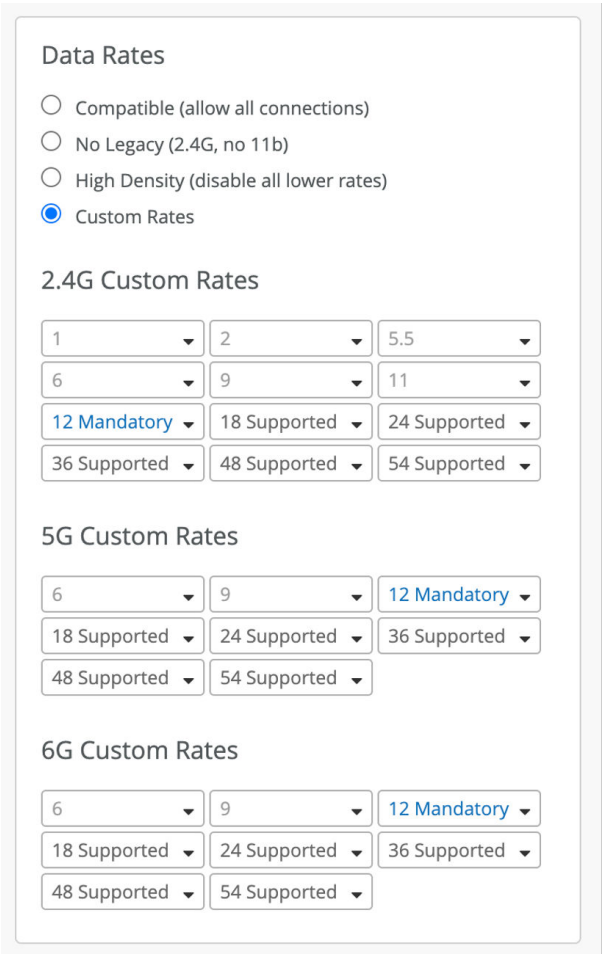
High Density

2.4GHz Rate Setting		5GHz Rate Setting		6GHz Rate Setting	
1 N/A	12 N/A	6 N/A	24 Basic	6 N/A	24 Basic
2 N/A	18 N/A	9 N/A	36 Optional	9 N/A	36 Optional
5.5 N/A	24 Basic	12 N/A	48 Optional	12 N/A	48 Optional
6 N/A	36 Optional	18 N/A	54 Optional	18 N/A	54 Optional
9 N/A	48 Optional				
11 N/A	54 Optional				
HT MCS 3-7, 11-15, 19-23, 27-31	VHT MCS 3-9	HT MCS 3-7, 11-15, 19-23, 27-31	VHT MCS 3-9	HE + EHT	

- The **Custom** data rate configuration:
  - Allows you to manually select which rates are disabled, supported or mandatory
  - Displays only the rate number (in grey text) when the rate is disabled
  - Displays **Supported** when you choose Supported.
  - Displays **Mandatory** when you choose Mandatory. If you select multiple rates as mandatory, Mist sets the lowest mandatory rate as the MBR.

In Figure 4 on page 258 below, we set 12 Mbps as the MBR for all bands and disabled all data rates below 12 Mbps.

Figure 23: Custom Data Rate Configuration



NOTE: When you configure custom data rates, you control the AP transmissions. This has no effect on clients which may still transmit at data rates you have disabled. This will prevent the client from connecting to the WLAN at the disabled rates.

For more information on data rates and deciding which rates to use when designing your network, refer to https://design.mist.com/data-rates/.

DSCP Mapping

SUMMARY

Wi-Fi Multimedia (WMM) and Differentiated Service Code Point (DSCP) mapping in Juniper Mist.

IN THIS SECTION

QoS Priorities

The 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 also align with the QoS traffic prioritization scheme configured for the wired network. For traffic from the Mist AP to the client, Mist uses the default mappings shown in Table 1.

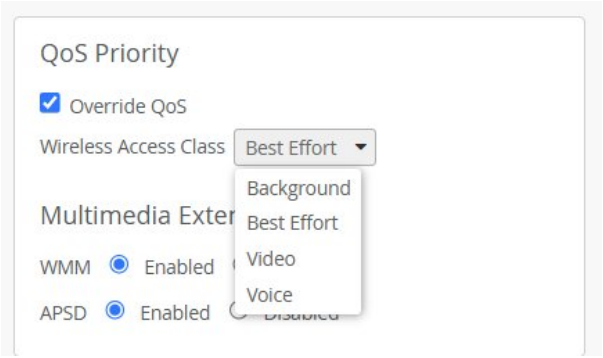
Table 21: DSCP to AC Mapping

DSCP Value	Access Category
DSCP 0 through DSCP 31	AC 1
DSCP 32 through DSCP 47	AC 2
DSCP 48 through DSCP 60	AC 3

Alternatively, you can configure QoS priority for traffic from the Mist AP to clients. Figure 1 shows how you would set a given WLAN to have all downstream client traffic use the **Voice** access class, and thereby override the default DSCP value.

Do this from the WLAN configuration page: click **Site > WLANs** and then select the **wlan** you want to configure.

Figure 24: QoS Priorities



WLAN Changes That Reset The Radio

SUMMARY

By being aware of the changes that reset the access point's radio, you can understand the potential impact on the user experience and plan accordingly.

IN THIS SECTION

WLAN Configuration Changes

Some WLAN configuration changes require the radio to be reset. During this time, clients on the affected APs will be deauthenticated (disconnected from the WLAN), for the minute or two it takes the radio to reset with the new configuration.

The table below shows the WLAN settings that will automatically reset the radio for the given radio band.

Table 22: WLAN Settings Changes and Radio Resets

Change	Effect on Radio
SSID (WLAN name)	Reset (all SSIDs broadcast on the AP)
Selecting specific radio	Reset

Table 22: WLAN Settings Changes and Radio Resets *(Continued)*

Change	Effect on Radio
Data rate	Reset
Broadcast AP name	Reset
Wi-Fi protocols	Reset
Selecting different authentication methods	Reset
Changing shared keys	Reset
Adding, deleting, modifying RADIUS Authentication, Accounting, CoA Servers	Reset
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

Table 22: WLAN Settings Changes and Radio Resets *(Continued)*

Change	Effect on Radio
Application QoS	No Reset
Bonjour gateway	No Reset

4

CHAPTER

Clients

IN THIS CHAPTER

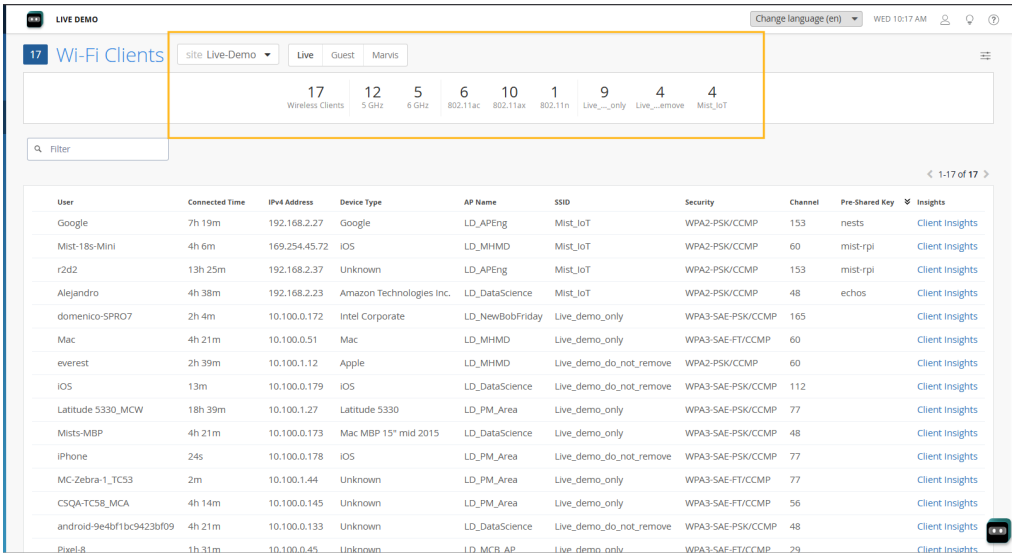
Wireless Clients

SUMMARY

See the wireless clients page for a list of connected clients.

The wireless clients page provides a summary of the Wi-Fi users for a given site, as well as a starting point to drill-down for client-specific information. Quick filters at the top of the page let you select **Live**, **Guest**, or **Marvis** clients, if installed.

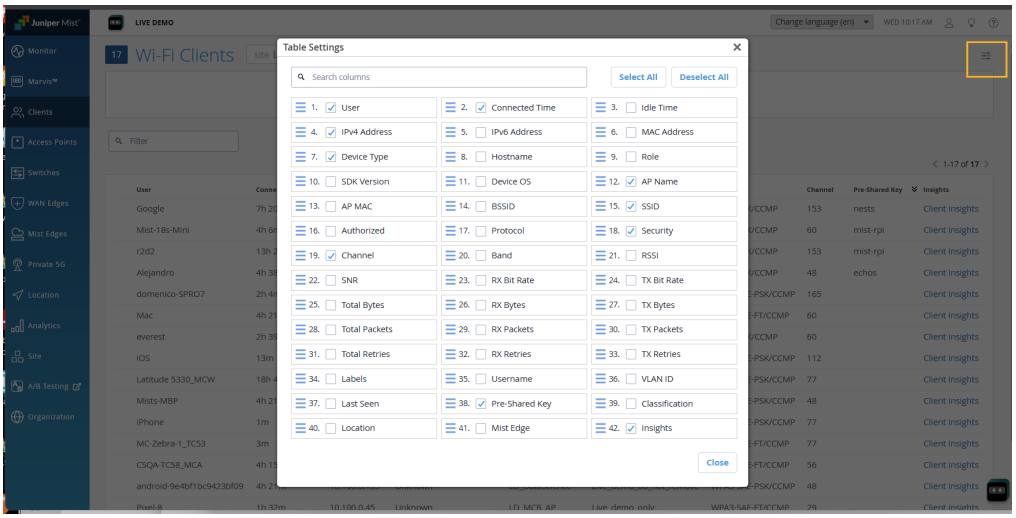
Figure 25: Wi-Fi Client Details



The at-a-glance dashboard along the top shows a summary of the users, the radio bands they are connected on, and the 802.11 protocols being used. You can further filter the list using predefined WLAN filters such as the SSIDs of the top five WLANs by client count, for example, to quickly identify client issues on a specific SSID.

You can choose the properties you want to display in the table by clicking the **Table Settings** icon and adding or removing the columns you are interested in, as shown in Figure 2.

Figure 26: Table Setting Column Options



The following table highlights a few of the fields available for the wireless clients.

Table 23: Selected Wi-Fi Client Details

Column Name	Details
User	Displays the user name of the user device connected to the AP.
IP Address	Displays the IP address of the user device connected to the AP.
MAC Address	Displays the MAC address of the user device connected to the AP.
Device Type	Identifies the device type of the connected device. You can click it to see additional properties such as the location, radio type, and operating system.
AP Name	Shows the name of the AP that the given user is connected to. You can click it to open the configuration page for that AP, as well as see information on the connected switch, radios, power, and connection status.
SSID	Shows the SSID name given to the WLAN the user is connected to. You can click it to open the configuration page for that WLAN or WLAN template.
Pre-Shared Key	Shows the name of the Pre-Shared Key used to connect to the SSID. See "Configure and Manage Pre-Shared Keys" on page 192.

Table 23: Selected Wi-Fi Client Details *(Continued)*

Column Name	Details
Client Insights	Links to the Wireless Clients Insights page for the given client, where you can find client events, pre- and post- connection details, as well as the current status and association of the current client.

You can also download the list for off-line work in a spreadsheet.

5

CHAPTER

Integrations

SUMMARY

Use the information in this section to integrate Juniper Mist with third-party products.

IN THIS CHAPTER

What Do You Want to Do?

Table 24: Top Tasks

If you want to...	Use these resources:
Integrate with Aruba ClearPass	• "Configure Juniper Mist™ as a RADIUS Client in Aruba ClearPass" on page 271 • "Integrate Juniper Mist™ with Aruba ClearPass Guest for Enhanced Access Control" on page 273
Integrate with Cisco ISE	"Integrate Juniper Mist™ with Cisco® ISE for EAP" on page 279
Integrate with Passpoint	"Enable Passpoint on Your WLAN" on page 282

NOTE: For additional information about third-party integrations, see Juniper Mist Access Assurance Guide.

Configuring an OpenRoaming Passpoint

SUMMARY

Use RadSec with Passpoint for Juniper Mist WLANs.

IN THIS SECTION

Juniper Mist supports Wi-Fi certified Passpoint™ (previously called Hotspot 2.0). Passpoint connections are secured with WPA-2/WPA-3-Enterprise for authentication and connectivity, which means Wi-Fi users can connect to Passpoint-configured WLANs as if they were cellular towers. Passpoint supports operator-specific subscriber policies, one of which is network selection, that you can then leverage in Mist when configuring WLANs. Mist also supports OpenRoaming. OpenRoaming uses RadSec, also known as RADIUS over TLS, to securely transfer the RADIUS packets over a public network.

When the RadSec option is enabled in a WLAN, Mist automatically generates a unique CA certificate for the organization, as well as certificates for Juniper APs. The Juniper APs must be running firmware version 0.8x or later to support RadSec, and by extension, be able to implement OpenRoaming. In addition, to complete the set up, you will need to import the Mist CA certificate to your RADIUS server so it can authenticate the certificates presented by the APs in your org.

On the Mist side, you will need to get the RADIUS server certificate and import it to Mist, as described in the following procedure.

Set up the OpenRoaming Certificates

To import an existing RadSec server CA certificate to your org:

1. From the Mist portal, click **Organization > Admin > Settings** and then scroll down to the **RadSec Certificates** section.
2. Click the **Add a RadSec certificate** link to open the **RadSec certificate** window.
3. Copy your RadSec server CA cert and paste it into the RadSec certification window. It should look something like this:

```
-----BEGIN CERTIFICATE-----
HASHHASHA7qgAwIBAgIBATANBgkqhkiG9w0BAQsFADBbMQswCQYDVQQGEwJVUzEN
HASHHASHHASHHASHAgIBATANBgkqhkiG9w0BAQsFADBbMQswCQYDVQQGEwJVUzEN
HASHHASHHASHHASHHASHHASHBgkqhkiG9w0BAQsFADBbMQswCQYDVQQGEwJVUzEN
-----END CERTIFICATE-----
```

4. Click the **Add** button, and then **Save** in the upper right corner of the Mist console.

Create an OpenRoaming WLAN

With all the required the certs configured in your organization, you can create a WLAN that uses OpenRoaming. This can be either site specific (**Site | Wireless > WLANs**) or global (**Organization | Wireless > WLAN Templates > Create Template**).

Note that when updating an existing WLAN to use OpenRoaming, Wi-Fi service on Juniper APs attached to the WLAN template will be interrupted during the update.

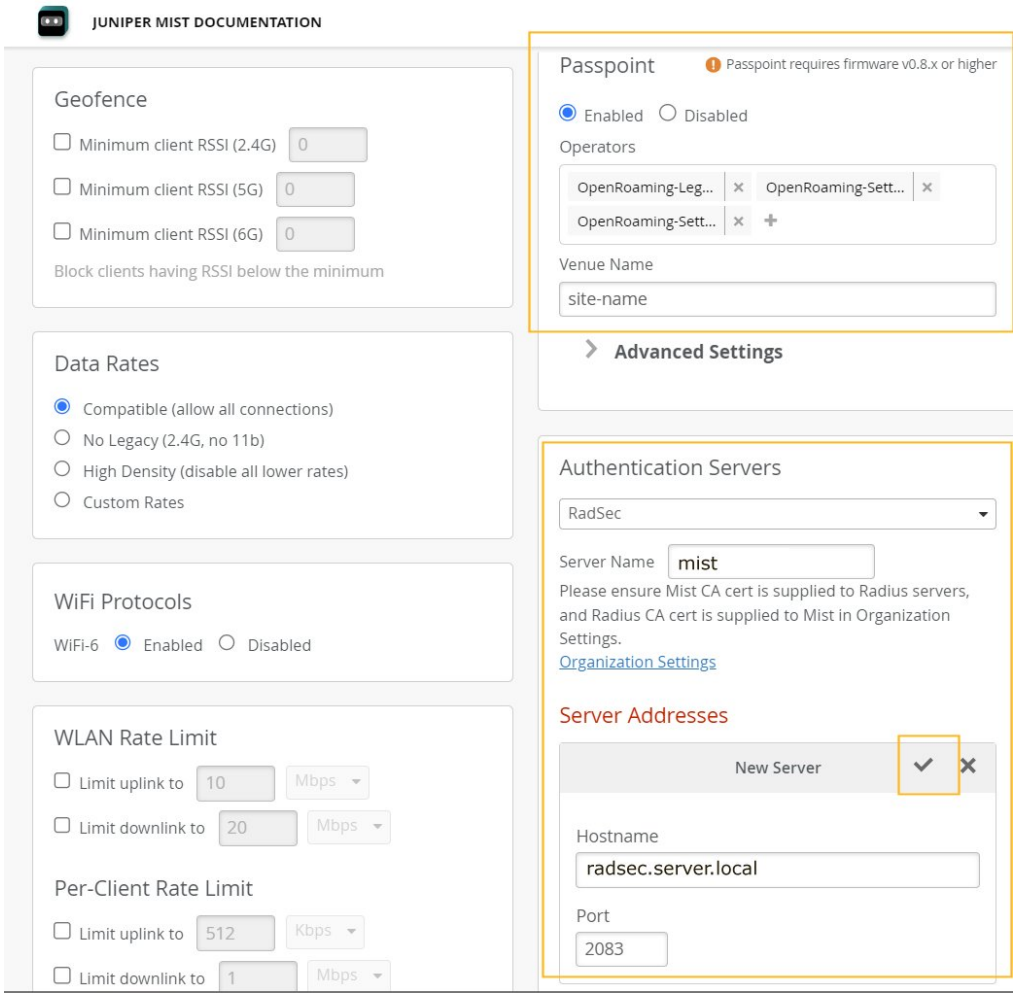
To create a site-level WLAN with OpenRoaming using RadSec:

1. From the Mist portal, click **Site | Wireless > WLANs** and then click the **Add WLAN** button to create a new WLAN.
2. Give the WLAN a name in the SSID field.
3. Scroll down the page to the **Security** section, and choose the following **Security Type**:

- WPA2 or WPA3
- Enterprise (802.1X)

4. As shown in Figure 1, the **Passpoint** section becomes available when you select Enterprise (802.1X).

Figure 27: OpenRoaming Passpoint



Choose **Enable**, and select the following **Operators**:

- OpenRoaming-Legacy
- OpenRoaming-Settled
- OpenRoaming-Settlement-Free

5. In the **Authentication Servers** section, choose **RadSec** from the drop-down.

- For **Server Name**, use the name specified for your RadSec proxy as it appears in the server certificate. Juniper APs will use this name to verify the RadSec server.
- For **Port**, the default is 2083. If you use something else for your RadSec server, specify that.

6. Click the check mark to add the RadSec server configuration.
7. At the top of the configuration page, click the **Create** button to complete the set up.

About RadSec

With RADIUS alone, clients use a trusted network to connect to the RADIUS server, which then authenticates their identity and provides authorization. Part of this handshake involves exchanging IP addresses, in plain text, and uses a shared secret to establish the connection. This sequence repeats each time the client connects or reconnects. There are shortcomings, though, because UDPs are not acknowledged by the receiver, the connection may not be secure, and roaming can interrupt users with the need to re-authenticate.

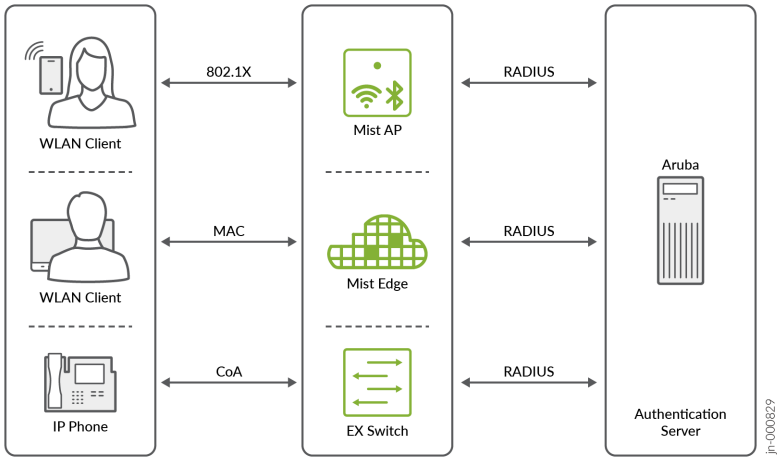
RadSec, on the other hand, forms an encrypted TLS tunnel between the client and server, which allows OpenRoaming traffic to be sent securely over public networks. RadSec also leverages Enterprise Public Key Infrastructure (PKI) and x.509 digital certificates to allow dynamic connections to be created on the fly. The organization issues certificates to both the client and the server, thus allowing each to prove the authenticity of the other (and so prevents man-in-the-middle attacks). Organization-level PKI certificates are also able to provide seamless roaming because the client simply resubmits the certificate at each call for reauthentication. Finally, the RadSec proxy uses OpenRoaming protocols to route authentication requests from roaming users to the correct RADIUS according to their credentials.

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: For help, see Adding and Modifying Roles on the Aruba support site.

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. Configure an enforcement profile.

   NOTE: For help, see:

   - Configuring Enforcement Profiles

6. Configure a service to reflect the profile and policy.

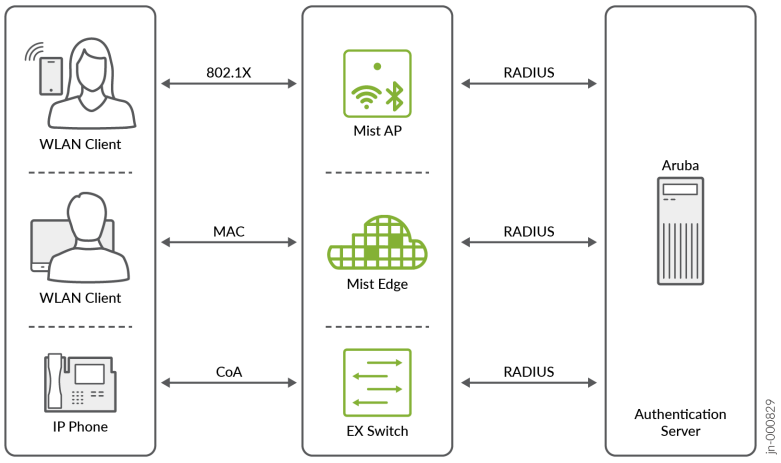
NOTE: For help, see Configuring Services Using Service Templates & Wizards and Configuring Other Policy Manager Services on the Aruba support site.

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 25: 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.

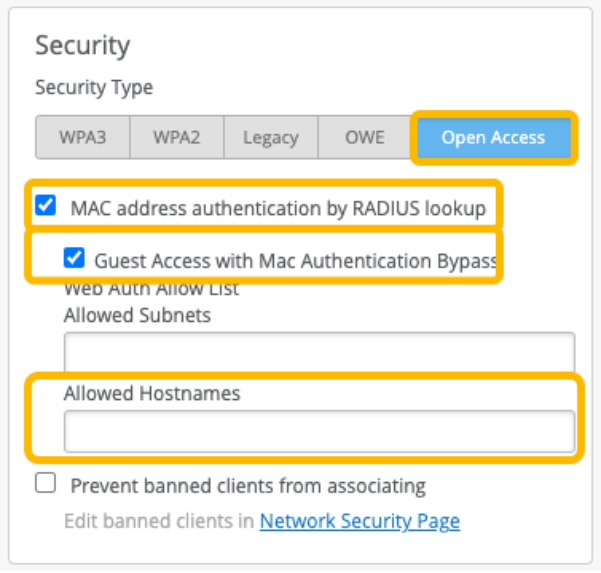
6. Create a new Enforcement Policy to handle guest user authentication through the Captive Portal hosted by ClearPass. For help, go to resources on the Aruba support site, such as Configuring Enforcement Policies.
   a. Set the Enforcement Type as WEBAUTH.
   b. Set the Default Profile as [RADIUS_CoA] [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 231 or "Adding a WLAN" on page 234.

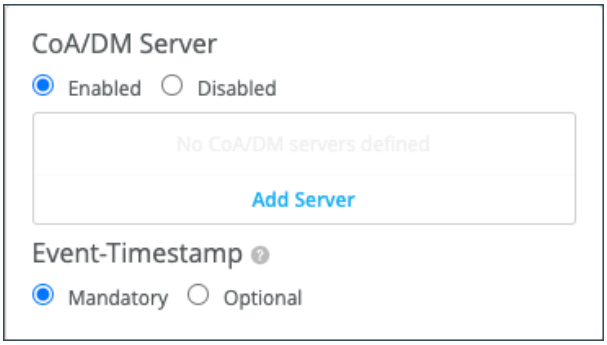
9. Enter the same SSID that you configured in ClearPlass.

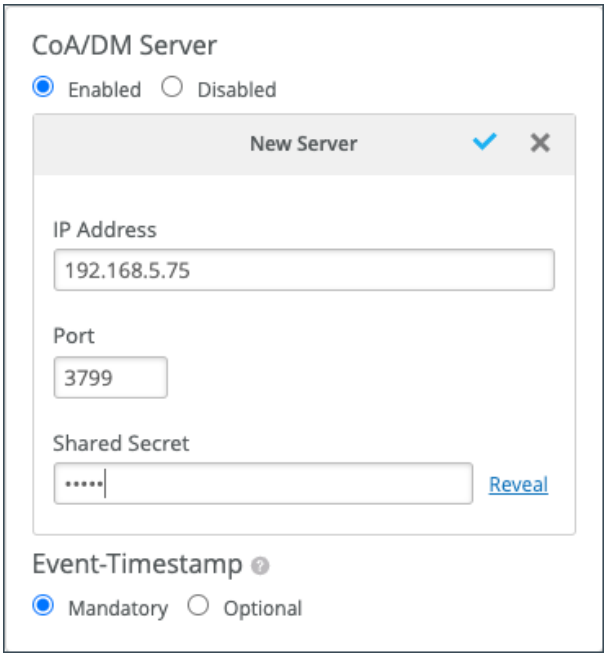
10. In the Security section:

- 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.



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.





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).

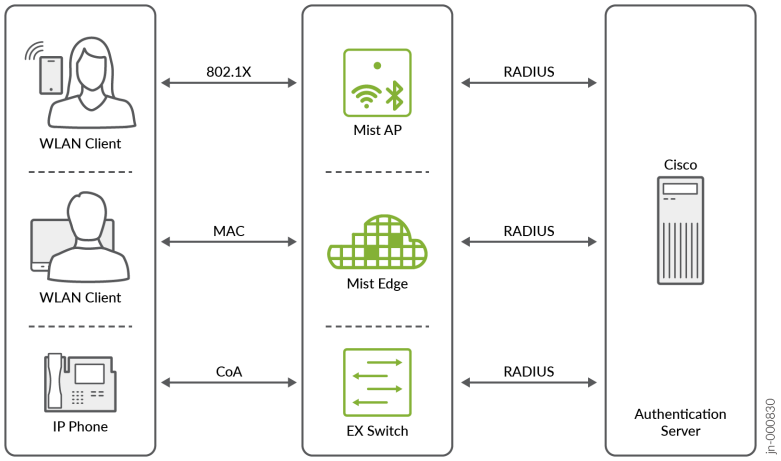
14. Verify that integration was successful by looking at the Access Tracker in the Aruba ClearPass Policy Manager. For help, go to resources on the Aruba support site, such as Live Monitoring: Access Tracker.

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.

You can integrate Juniper Mist™ with Cisco® Identity Services Engine (ISE) to leverage Extensible Authentication Protocol (EAP). This protocol provides a secure way for wireless networks to send identification information for network authentication purposes.

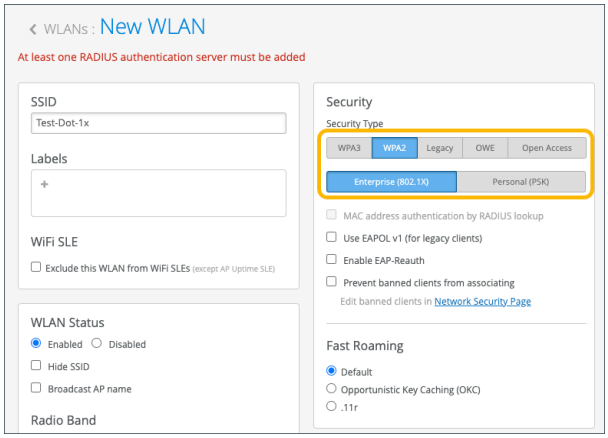


To integrate Juniper Mist with Cisco ISE:

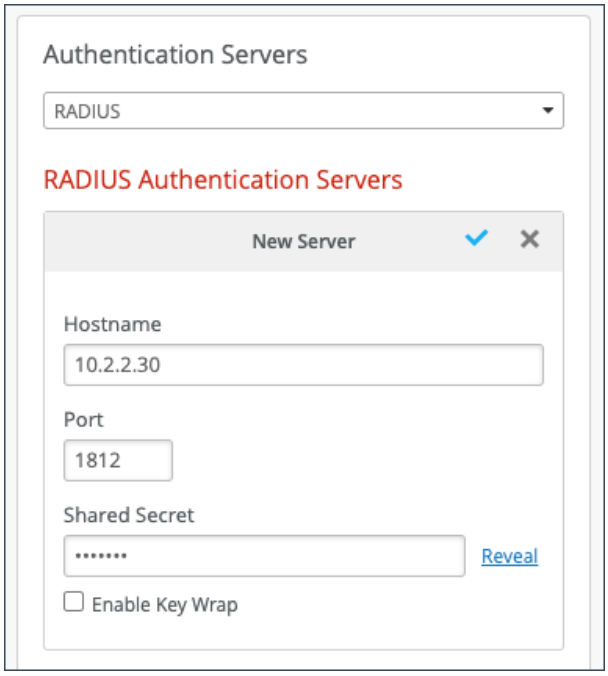
1. In the Juniper Mist portal, navigate to the WLAN or create a new one.

   NOTE: For help, see "Configure a WLAN Template" on page 231 or "Adding a WLAN" on page 234.

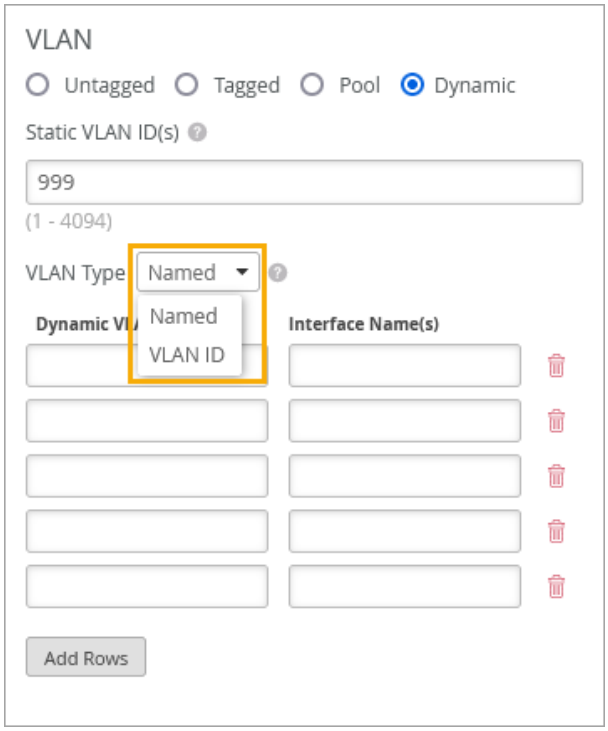
2. For Security Type, select **WPA2** and **Enterprise (802.1X)**.



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.



4. If you need to enable dynamic VLANs:



NOTE:

- **Named VLAN**—This option supports Airespace-Interface-Name or Tunnel-Private-Group-ID RADIUS attributes and can be specified as a single VLAN, a pool of VLANs, or as variables.
- **VLAN ID**—This option supports Tunnel-Private-Group-ID RADIUS Attributes and can be specified as a single VLAN, VLAN range, or as variables.

5. 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).

6. Look up the IP address of the AP that you want to integrate with Cisco ISE:
   a. On the left menu of the Juniper Mist™ portal, select **Access Points (APs)**.
   b. 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. Go to your admin portal for Cisco ISE, add a network device, and enter this information:
   - **Name**—The name of the AP
   - **IP Address**—The IP address of the AP

- **Shared Secret**—The RADIUS Shared Secret

> **NOTE**: For help adding a device in Cisco ISE, go to the Cisco support site: Adding and Editing Devices

Enable Passpoint on Your WLAN

SUMMARY

Follow this procedure to integrate Juniper Mist™ with Passpoint for secure user authentication.

You can integrate Juniper Mist™ with Passpoint® (formerly called Hotspot 2.0), which allows automatic secured connections for mobile devices to support various use-cases, such as public guest networks, carrier Wi-Fi offload, Eduroam services and many more.

> **NOTE**: For more information about Passpoint, see information on the Wi-Fi Alliance site.

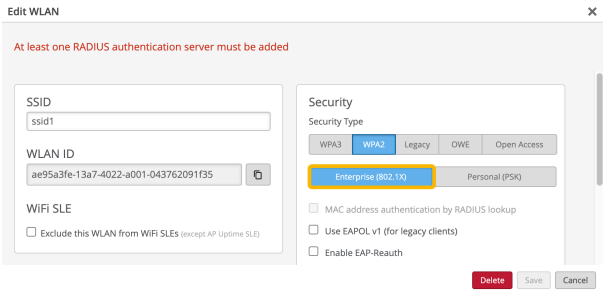
Juniper Mist provides templates for each operator and service provider, removing the complexity that was historically associated with Passpoint configuration. You need only to enable Passpoint on the WLAN and configure your RADIUS or RadSec authentication server according to the guidance from your Passpoint service provider.

To enable Passpoint on your WLAN:

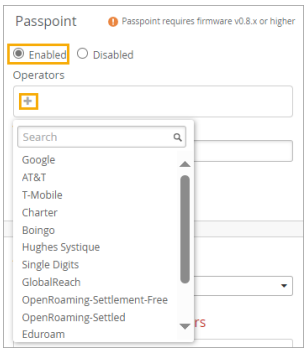
1. In the Juniper Mist portal, navigate to the WLAN or create one.

   > **NOTE**: For help, see "Configure a WLAN Template" on page 231 or "Adding a WLAN" on page 234.

2. In the Security section, select **WPA3** or **WPA2**
3. Select **Enterprise (802.1X)**.



4. In the **Passpoint** section, select **Enabled** and then click **+** to select your **Operators** (service providers).



Selecting an operator loads the 802.11u settings that are required by the service provider.

5. (Optional) Enter a **Venue Name**.

   The access point (AP) uses this value to advertise the location. Leave this field blank, the AP will advertise the site name as the venue.

6. (Optional) Click **Advanced Settings** to customize your settings.

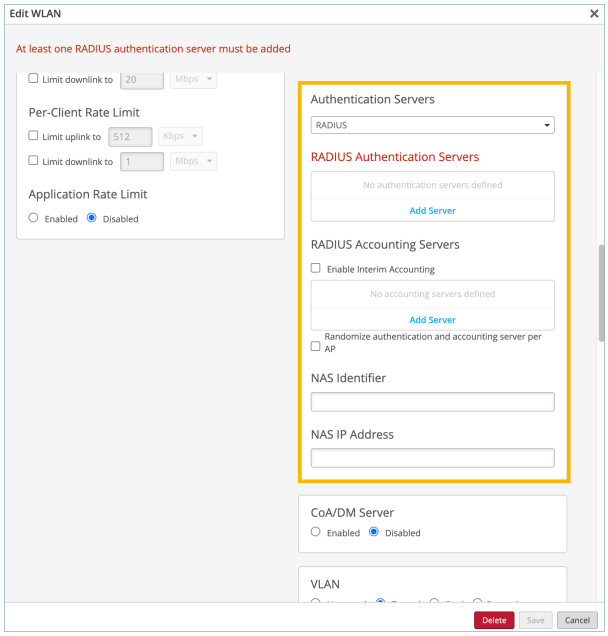
   Enter the following values:

   - 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 that are inherited from the high-level operator template.

7. In the **Authentication Servers** section, click **Add Server**, select the server type (RADIUS or RadSec), then enter the information, and click the checkmark to save the settings.

   Consult with your Passpoint service provider to ensure that you configure the correct RADIUS or RadSec settings.



8. 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).

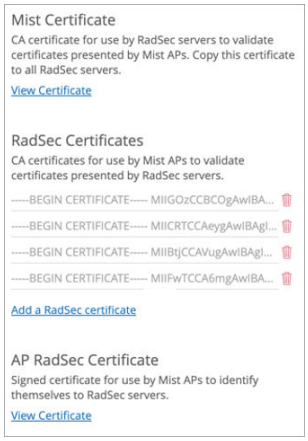
9. If you are using RadSec, manage your certificates as follows:

   a. To obtain your Mist certificate, go to **Organization** > **Admin** > **Settings**. You'll find the certificate under **Mist Certificate**.

   b. Obtain the RadSec certificate from your RadSec server provider.

   c. Obtain the AP certificate from your Passpoint Provider or Authentication Broker.

   d. To add your certificates to Mist, again go to **Organization** > **Admin** > **Settings**. You'll add your certificates under **RadSec Certificates** and **AP RadSec Certificate**.



6
CHAPTER

WLAN Guest Portal

SUMMARY

Use the information in this chapter to get started with the Guest Portal options for your WLAN.

IN THIS CHAPTER

Video Overview

Video: Mist Guest Portal

What Do You Want to Do?

Table 26: Top Tasks

If you want to...	Use these resources:
Compare the options for WLAN Guest Portal.	"Compare WLAN Guest Portal Options" on page 286
Enable a sign-in portal in Juniper Mist and customize it to meet your needs.	"Add a Custom Guest Portal to a WLAN" on page 293
Direct guests to your own full-featured portal.	"Use an External Portal for Guest Access" on page 314
Direct guests to your identity provider's Single Sign-On page.	"Use an Identity Provider for Guest Access" on page 323

NOTE: This chapter 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 173.

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.

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 173.

Table 27: Compare WLAN Guest Portal Options

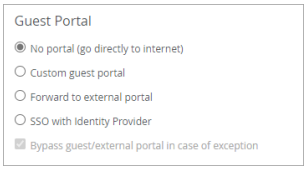
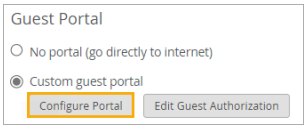
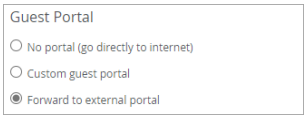
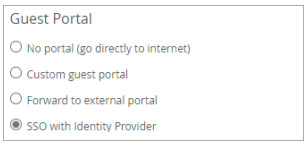
Option	Description	Setup
Direct Access (No Portal)	Guests get immediate internet access without authentication. This is the easiest option unless you have a business need for additional security or you want to collect information about your guests.	No action is needed. This is the default Guest Portal option in WLAN settings. 
Custom Guest Portal	Guests get internet access by completing a simple sign-in form that you set up in Juniper Mist™. This is an easy-to-configure approach that allows you to collect some information from your guests. Optionally, you can enable options such as authorization codes, sponsored guest access, social sign-in, and more.	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.  For help, see "Add a Custom Guest Portal to a WLAN" on page 293.

Table 27: Compare WLAN Guest Portal Options *(Continued)*

Option	Description	Setup
External Portal	Guests get internet access by going to a sign-in portal that you've developed outside Juniper Mist. With this option, you use a sign-in portal that your web developers have specifically designed for your business and your use cases.	Select **Forward to external portal** in the WLAN settings. Then enter your portal URL and configure other optional settings.  For help, see "Use an External Portal for Guest Access" on page 314.
Single Sign-On (SSO) with an Identity Provider	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.)	Select **SSO with Identity Provider** in the WLAN settings. Then enter the settings for your IdP.  For help, see "Use an Identity Provider for Guest Access" on page 323.

Automatic Client VLAN Assignments

IN THIS SECTION

You can set up the WLAN so that users are automatically connected to a given VLAN according to the username/password they enter. You do this by configuring dynamic VLANs in the Mist portal, in conjunction with a RADIUS server. For unknown clients, you can send them to the Guest Network. The RADIUS server should already be connected to you switch. Likewise, your access points (APs) should be connected to the switch, with the correct VLANs configured.

The following VLAN types are supported for dynamic VLANs: *Airespace-Interface-Name* and *Tunnel-Private-Group-ID*.

RADIUS Setup

Although the specific RADIUS-side configuration will vary by provider, in general the idea is to configure a shared secret for encrypting and signing client traffic, to *allow* inbound traffic from the clients IP addresses, and to have a users list that identifies the WLAN clients you want to segment, and their associated VLAN IDs.

Using FreeRADIUS server as an example, you would edit the following files: *clients.conf* and *users*.

Configure the network and a secret for client requests in *clients.conf*, like so:

```
#client WLAN-1
{
# ipaddr= 192.0.2.0/24
# secret= testing123-1
#}
```

Configure the */etc/freeradius/user* file with a list of WLAN users (including their user name, password, and VLAN association) like so:

```
user1
Cleartext-Password := "password1"
User-Name = user1,
Tunnel-Type = VLAN,
Tunnel-Medium-Type = IEEE-802,
Tunnel-Private-Group-ID = 10

user2
Cleartext-Password := "password2"
User-Name = user2,
Tunnel-Type = VLAN,
```

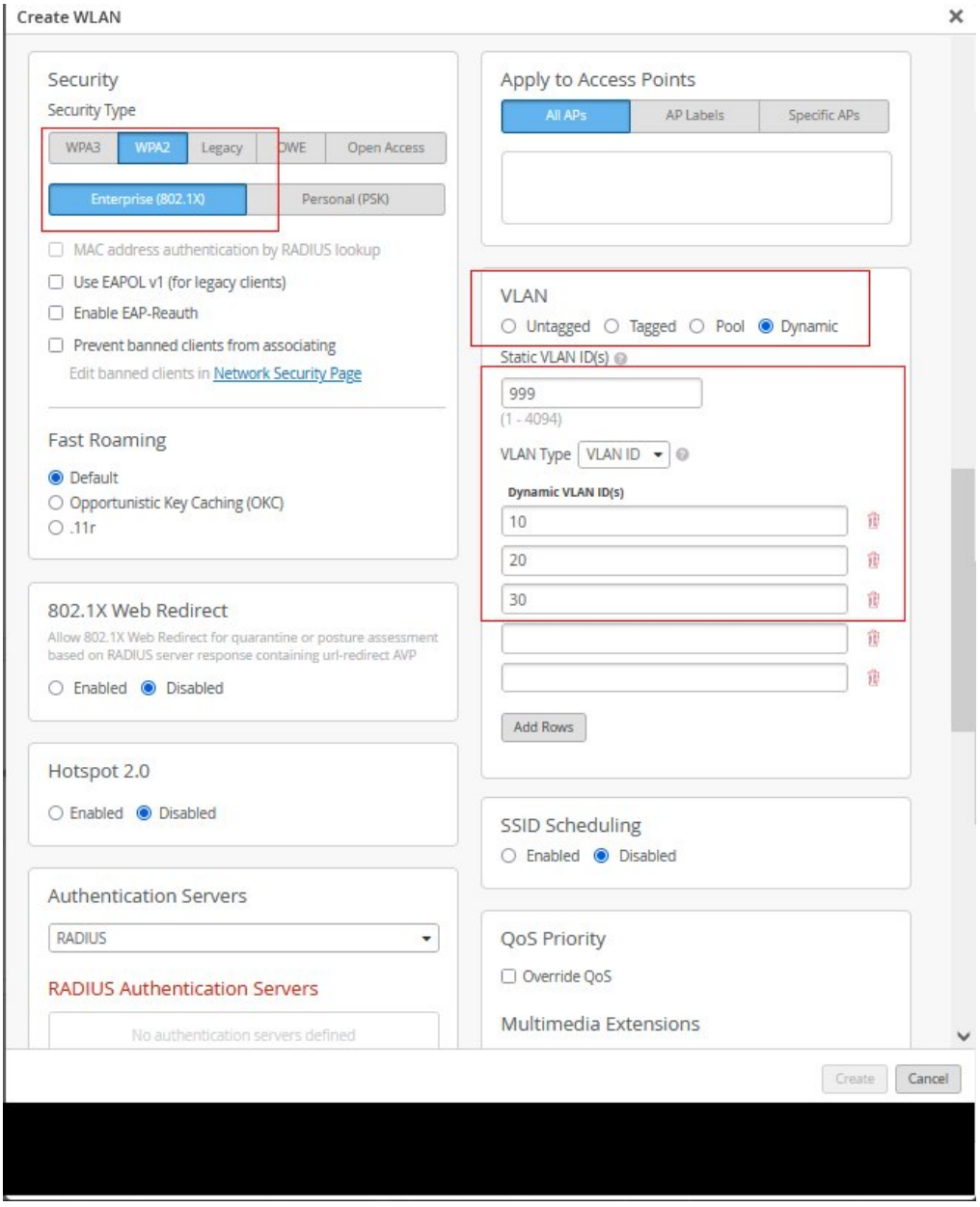
```
Tunnel-Medium-Type = IEEE-802,
Tunnel-Private-Group-ID = 20

user3
Cleartext-Password := "password3"
User-Name = user3,
Tunnel-Type = VLAN,
Tunnel-Medium-Type = IEEE-802,
Tunnel-Private-Group-ID = 30
```

If you are using FreeRADIUS server and it is not returning tunnel attributes in the Access-Accept request, and/or if the user is not being assigned correct IP address (from the VLAN), then you may need to add a line to the `/etc/freeradius/mods-available/eap.conf` file:

```
use_tunneled_reply = yes
```

WLAN Setup

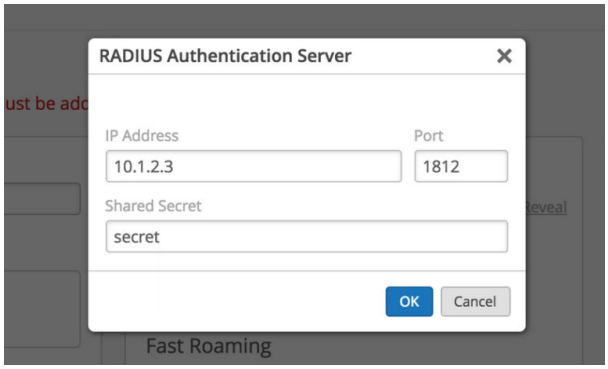
Figure 28: Dynamic VLAN is available with WPA3 and WPA2 Security Types



As noted, you can set up your WLAN so when users log on to it, they are automatically connected to a selected VLAN. In the Mist portal, this is called Dynamic VLANs, and you can enable the feature as follows:

1. In the Juniper Mist portal, click **Organization > Wireless | WLAN Templates**, and on the WLAN Templates page, click **Add WLAN** (or select from the list the WLAN you want to use).

2. Give the SSID a name (or select in from the WLANs section of the template). Typically, the SSID name is the same as the name of the WLAN so that it's easy to find and remember.
3. In the WLAN window, under the **Security** panel, select WPA3 or WPA2 for the **Security Type** and Enterprise (802.1X). This action also unlocks the **Dynamic** option in the **VLAN** section.
4. In the **Authentication Servers** panel, select **RADIUS**.



   - Click **Add Server** and specify the IP address of your RADIUS server.
   - Add the shared secret that is already configured on your RADIUS server.
   - Click the check mark icon when done to post your changes (you still need to click **Save** in the upper right corner when finished with all the steps).
5. In the **VLAN** panel, choose **Dynamic** and then specify the following, as appropriate:
   - **Static VLAN ID(s)**—You can specify static VLANs or VLAN pool IDs (requires AP firmware version 0.14.x or later). Alternatively, you can specify a variable or use both VLAN IDs and variables. Delimit multiple values with a comma, no space.
   - **VLAN Type** supports both Airespace-Interface-Name and Tunnel-Private-Group-ID RADIUS attributes. Note that VLAN Type works on a per-WLAN basis. In other words, you can't use two different types on the same SSID.
     - **VLAN ID**—(also called Standard) This is the Tunnel-Private-Group-ID. Specify the VLAN IDs as configured in your **users** file on your RADIUS server. If entering multiple VLAN IDs and/or ranges on the same line, delimit with a comma (CSV support is for **Standard Tunnel-Private-Group-ID** only).
     - **Named**— This is the Airespace-Interface-Name. Specify the interface names configured in your **users** file, and along side it, the corresponding VLAN ID you want to use.
6. Fill out the rest of the configuration as needed.
7. Click **Save** at the top of the screen when you are done.

Custom Guest Portal

IN THIS SECTION

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 231.

To add a custom guest portal to your WLAN:

1. Navigate to the WLAN.

   NOTE:

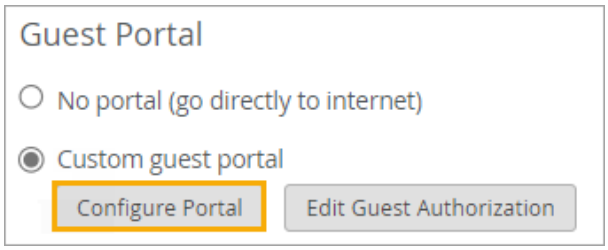
   - If the WLAN is in a WLAN template, select **Organization > Wireless | WLAN Templates**, click the template, and then click the WLAN.

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

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

   a. Click **Custom guest portal**.

   b. Click **Configure Portal**.



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 295.
   - 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 297
   - 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 299
   - 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 302.

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 299.

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.

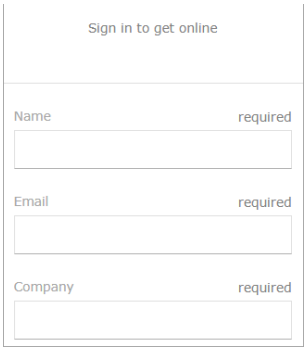
Form Fields for Custom Guest Portal

SUMMARY

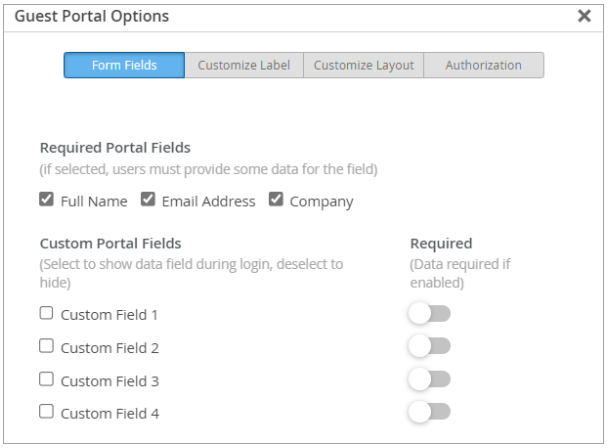
If you've enabled a custom guest portal, you can keep the preset form fields or customize them to collect exactly the information that you want your guests to provide.

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.



You can make changes on the **Form Fields** 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 293.

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

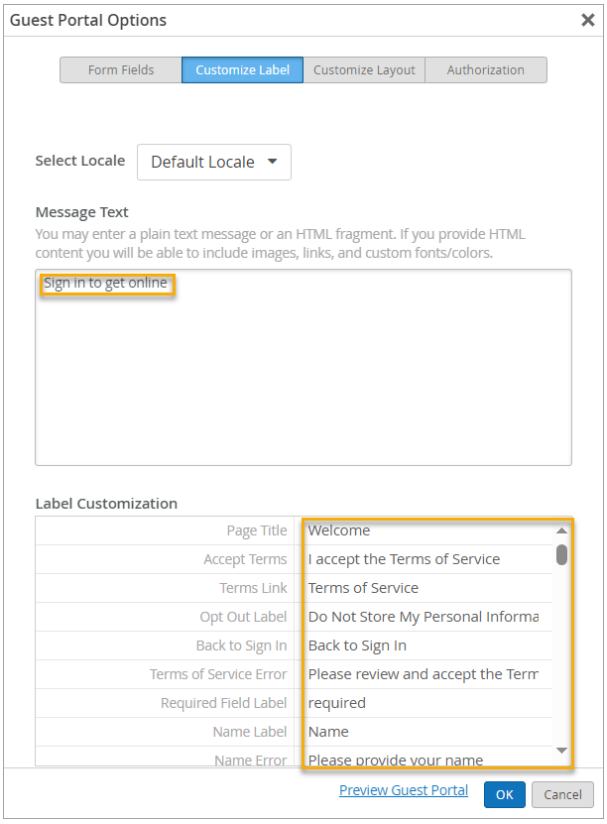
You can change the top-of-page greeting, the form field labels, the button names, and other on-screen text. You can even set up a multi-language portal.

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 293.

Changing the Text

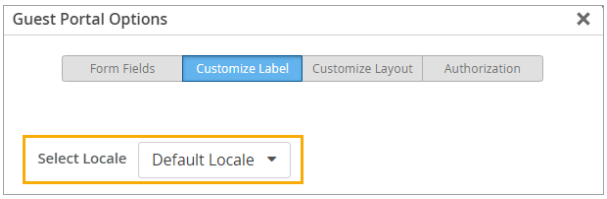
You can see the default text in the **Message Text** box and on the right side of the **Label Customization** section. Read the default text to understand the purpose, and then make your changes by typing in the box.



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.

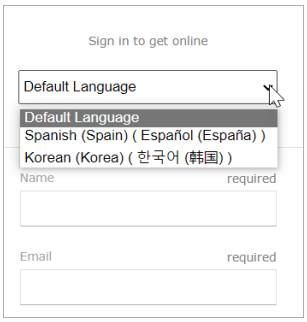
Setting Up Different Sets of Labels for Different Languages

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



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.



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

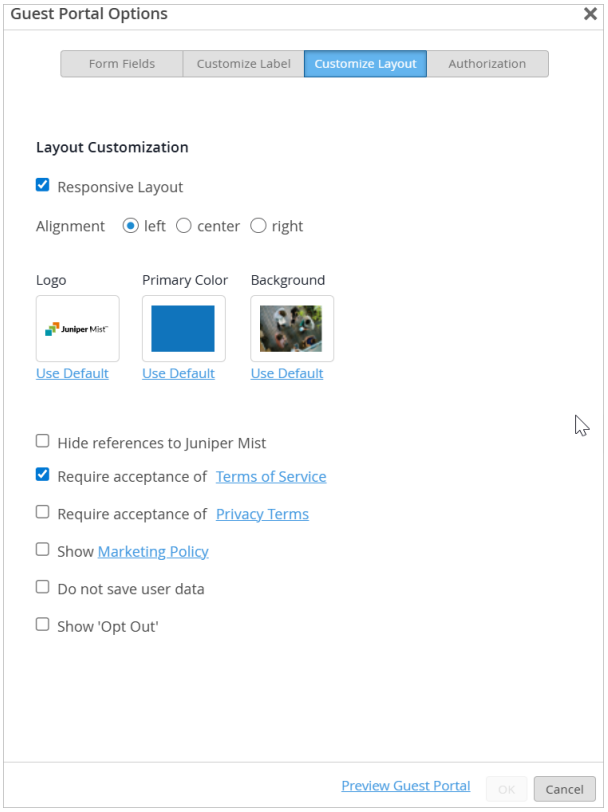
SUMMARY

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.



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 293.

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.

  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.

- **Require acceptance of Privacy Terms**—If you want to require guests to agree to your privacy policy, select the check box. Then click **Privacy Terms**, enter the information that you want users to see, and click **OK** to save the text.
- **Show Marketing Policy**—If you want your guest form to allow guests to opt into marketing communications, select the check box. Then click the link and enter your policy. On the guest form, guests will see a check box to receive marketing communications. The form also will include a link to view your policy.
- **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

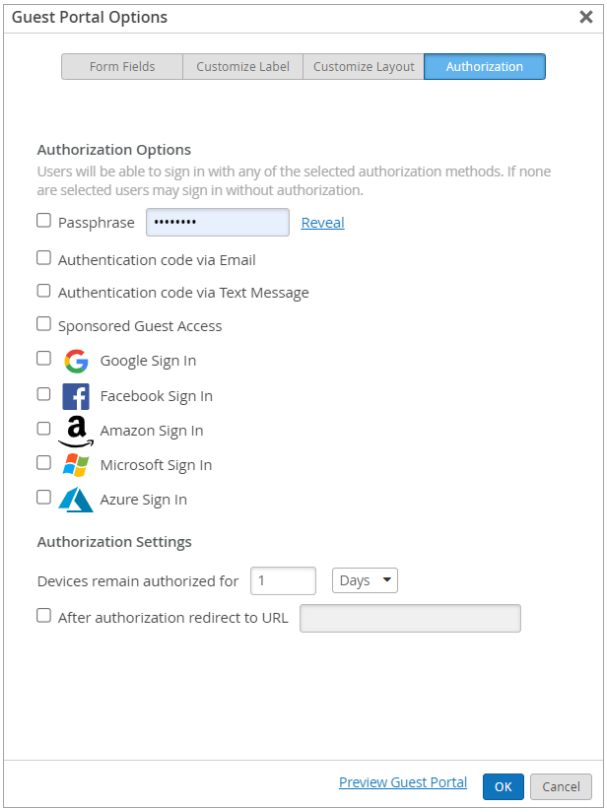
SUMMARY

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

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

You can set up other sign-in options on the **Authorization** 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 293.

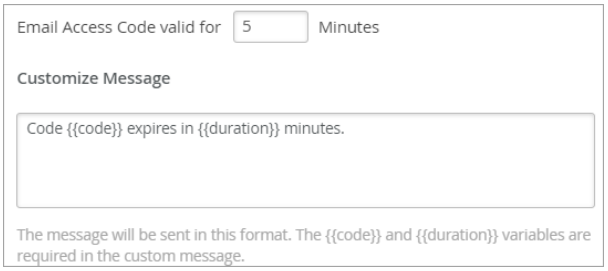
Passphrase

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:

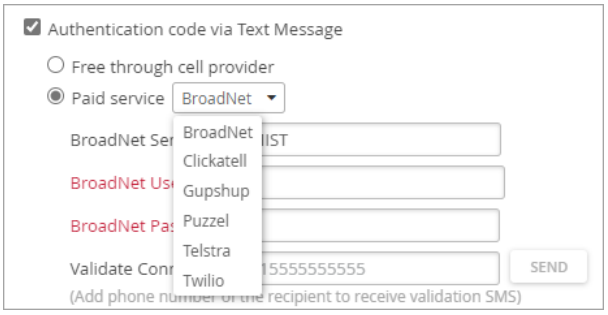


- **Email Access Code valid for**—Enter the amount of time (in minutes) that the code remains valid after the email is sent.
- **Customize Message**—Add any additional text that you want to include in the email message.
  - When the message is sent, the {{code}} variable displays the code that the user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

Authentication Code via Text Message

Select **Authentication code via Text Message** 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.

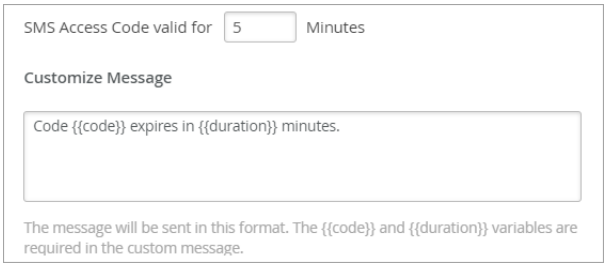
The authentication code can either be sent via a free method via the cell provider, or a paid aggregator. Sending through the cell provider relies upon Email to SMS. The available providers are listed in the **Paid service** drop-down menu. Select a provider, and then enter your account information.



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 Twillio or Broadnet.

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

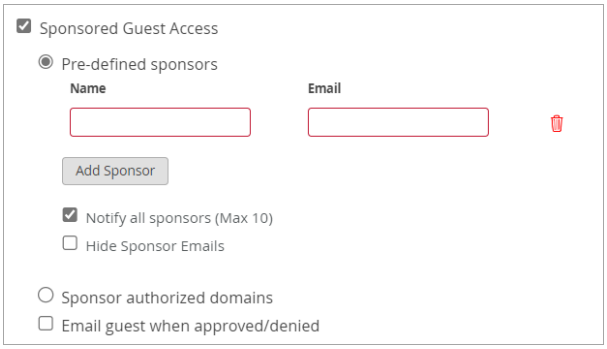


- **SMS Access Code valid for**—Enter the amount of time (in minutes) that the code remains valid after the text message is sent.
- **Customize Message**—Add any additional text that you want to include in the text message. When the message is sent, the {{code}} variable displays the code that the user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

Sponsored Guest Access

Select **Sponsored Guest Access** if you want to require a sponsor to approve guests before they can use your network. To identify the personnel who will receive the guests' access requests, enter pre-defined sponsors or a domain.

- **Pre-defined sponsors**—Create a list of specific sponsors that guests can chose from. Enter the name and email address for each sponsor.



  Additional options for pre-defined sponsors:

  - **Notify all sponsors**—All sponsors will receive all guests' access requests.

- **Sponsor authorized domains**—Select this option if you want guests' access requests to go to everyone on a specified domain. Enter the domain, or enter multiple domains separated by commas.

Select other options as needed:

- **Email guest when approved/denied**—Select this option to send guests an email when the sponsor takes action.

- **Sponsor email request will remain valid for**—You can adjust this time period at the bottom of the Guest Portal Options window. For example, if you enter 60 minutes and no one responds, the request expires.

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. 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.

For help creating custom applications, see:

- "Facebook App Creation" on page 306
- "Enable Guest Portal Social Login with Microsoft® Azure" on page 307

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

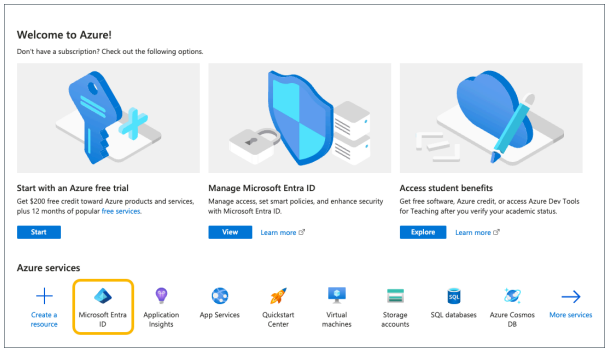
Assign an Application to the Guest User | 313

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.

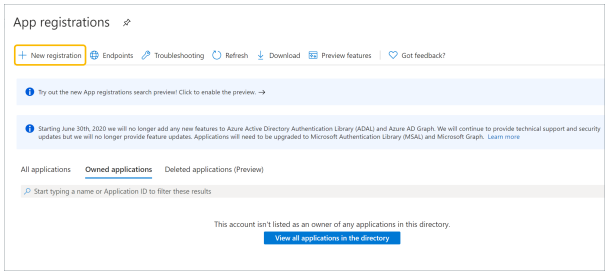
To enable Guest Portal Social Login with Microsoft® Azure:

Create Registration in Microsoft® Azure

1. Register or login to the Azure Portal.
2. On your Azure portal, select **Microsoft Entra ID**.

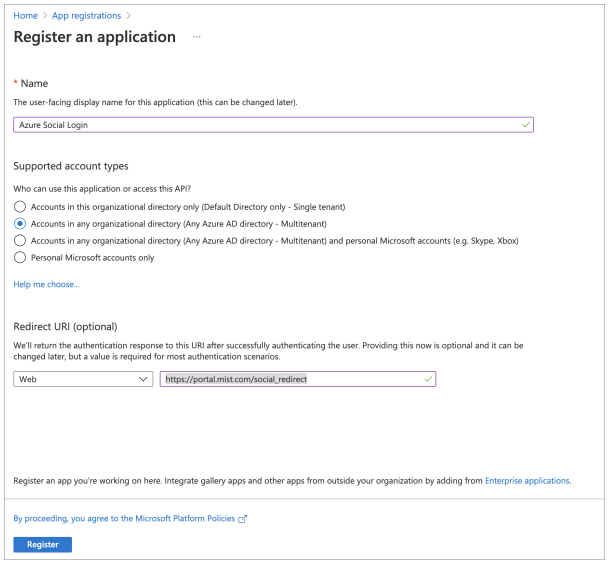


3. Click on **App registrations.** If you cannot find this, click on **More Services** and search for **App registrations**.
4. Select **New Registration**.



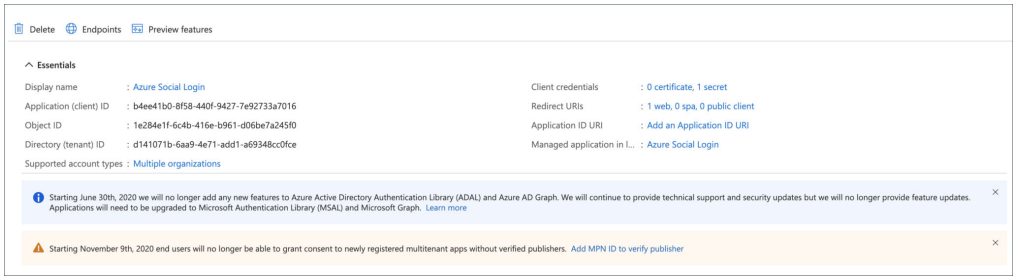
5. Add the name you wish to add for the App.
6. Select any account type.
7. Under **Redirect URI** select **Web**. The web address you enter should be the web address that is listed in the Guest Wi-Fi Portal row for your global region in *Juniper Mist Firewall Ports and IP Addresses for Firewall Configuration*, followed by **/social_redirect**.

NOTE: The following image lists **https://portal.mist.com/social_redirect** as an example, which includes the guest Wi-Fi portal address for the Global 01 region.



8. Click **Register**.

   Once the registration is complete, the following page is displayed:



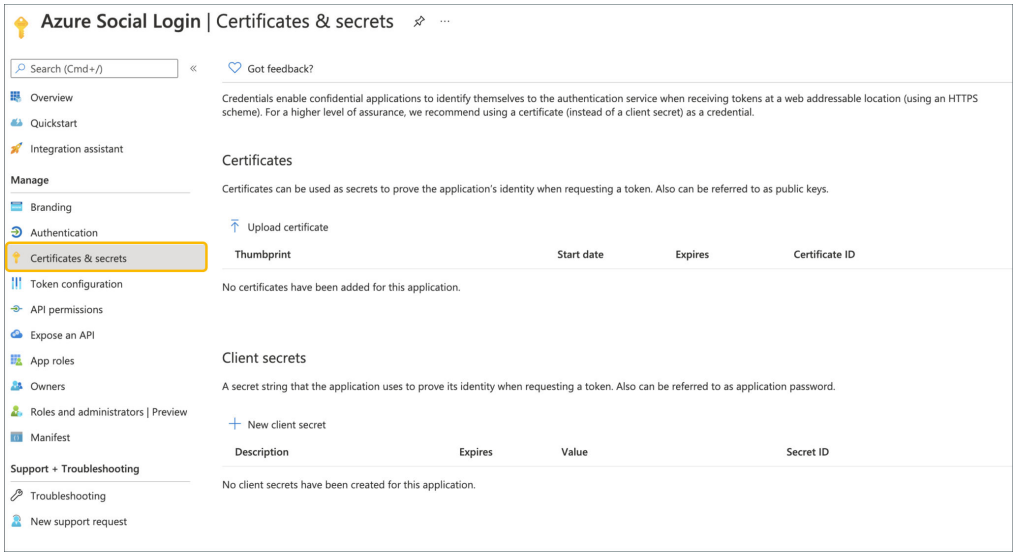
Examples:

- **Application (client) ID** — b4ee41b0-8f58-440f-9427-7e92733a7016
- **Directory (tenant) ID** — d141071b-6aa9-4e71-add1-a69348cc0fce

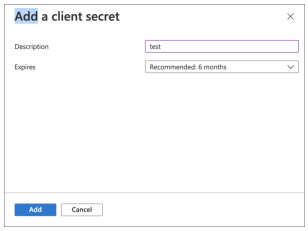
Copy and save the **Application (client) ID** and the **Directory (tenant) ID**. These will be entered into the **Guest Portal Options** window of the Juniper Mist portal in a few moments.

Enter Information About the Mist Portal

1. Next, to generate the Secret ID, click on **Certificates & secrets**.

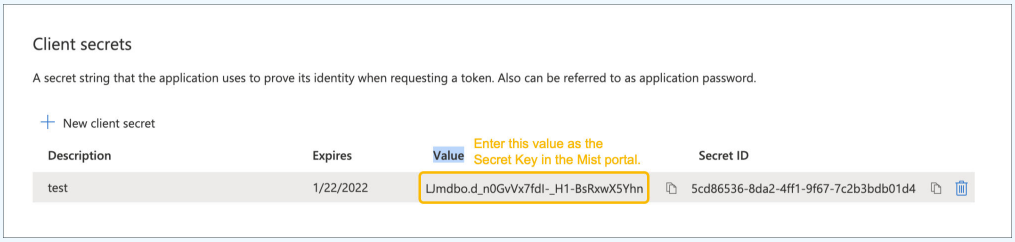


2. Click **New client secret** and enter the **Description** and **Expire** time.

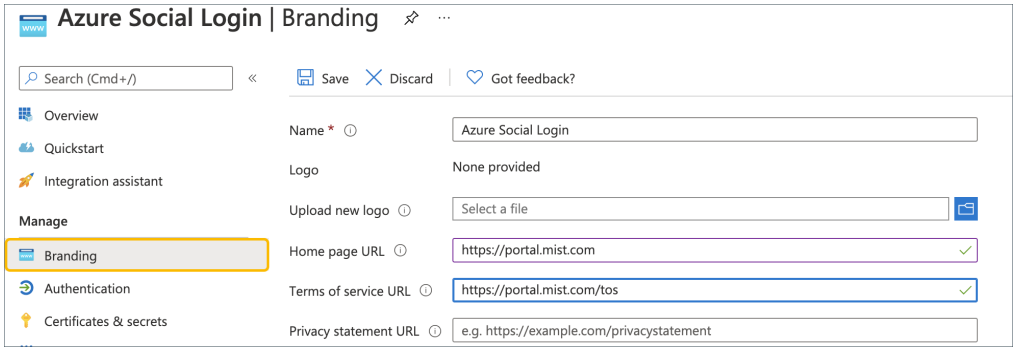


3. Click **Add** and a secret key will be generated.

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.



4. Select **Branding.**
5. For the **Home page URL**, enter **https://portal.mist.com** and for the **Terms of service URL**, enter **https://portal.mist.com/tos**.



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

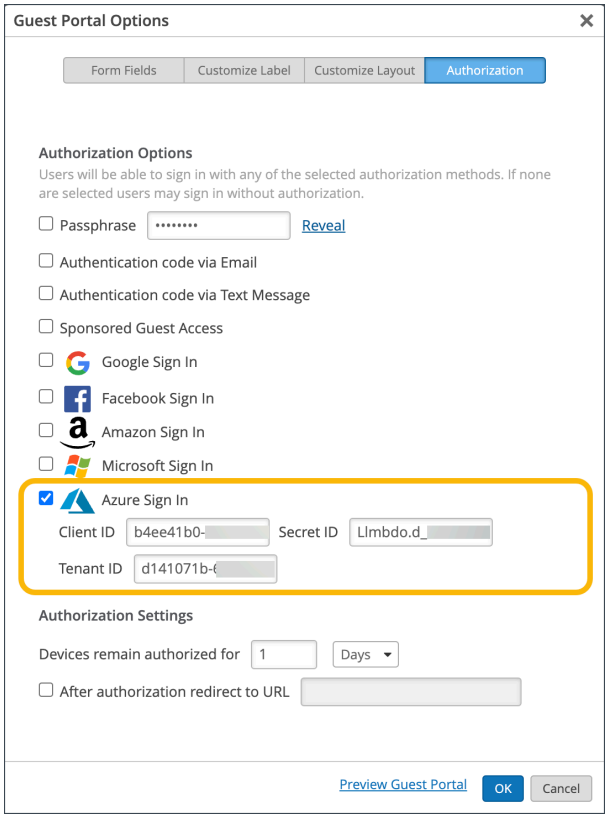
Next, navigate to the Mist portal where you will paste the **Application (client) ID**, **Secret ID** (Value), and **Directory (tenant) ID** that you obtained previously. You need these values to set up the social login for your WLAN.

1. In the Juniper Mist portal, select the WLAN that you want to add the guest portal to.

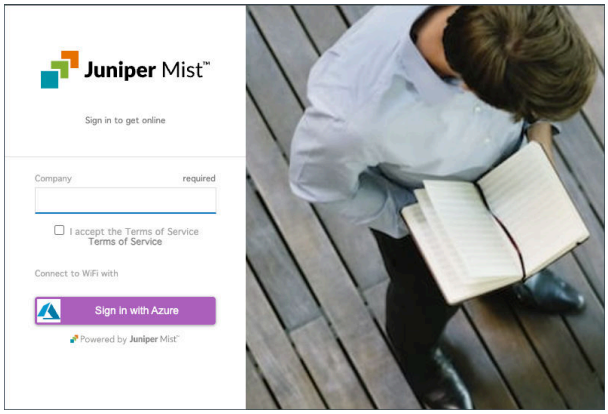
   NOTE:

   - 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.



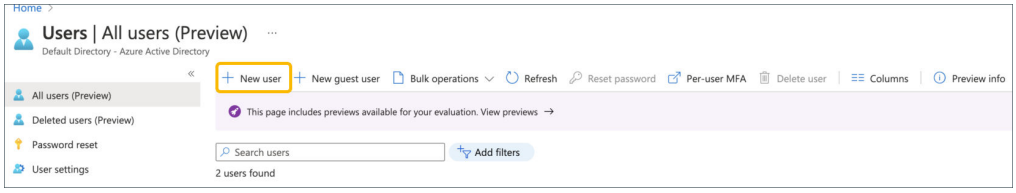
6. Click **OK** on the Guest Portal Options window, then click **Save** on the Edit WLAN window. .
7. You will see this pop up when connecting to the wireless network. **Enter your Company name** to assist with authentication, **accept the terms and conditions**, and then select **Sign in with Azure.**Once 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**.

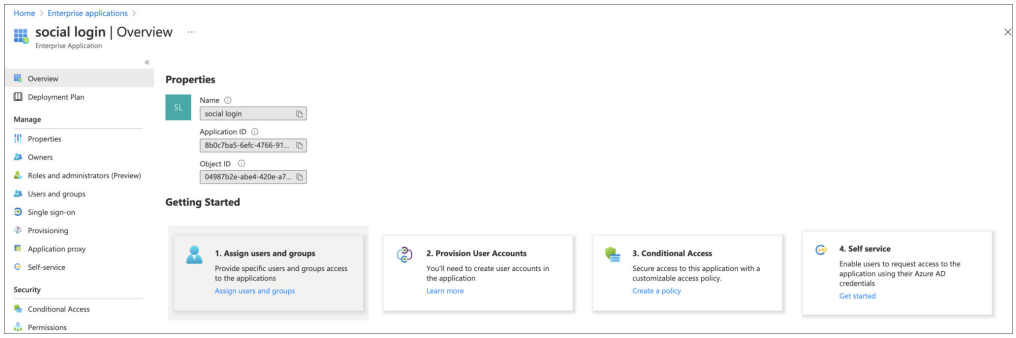


5. On the **New user** page, select **Invite user** and then add the guest user's information.
   - **Name** — This is the first and last name of the guest user.
   - **Email address (required)** — Enter the email address of the guest user.
   - **Personal message (optional)** — Include a personal welcome 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

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.

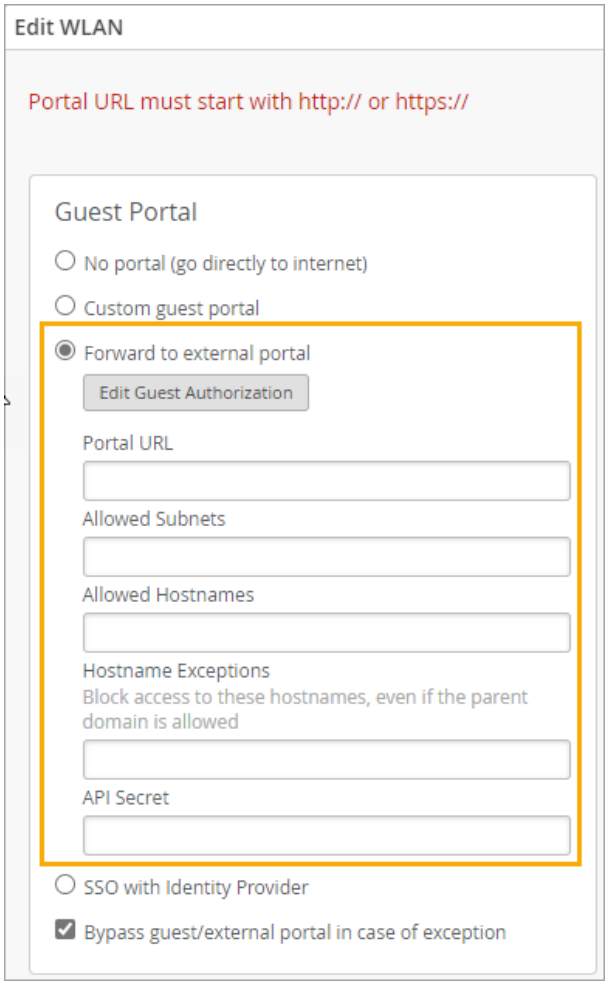
For added security, you can specify authorized users, allowed subnets, and allowed hostnames. You also can enter a list of hostnames to block.

1. Navigate to the WLAN.

NOTE:

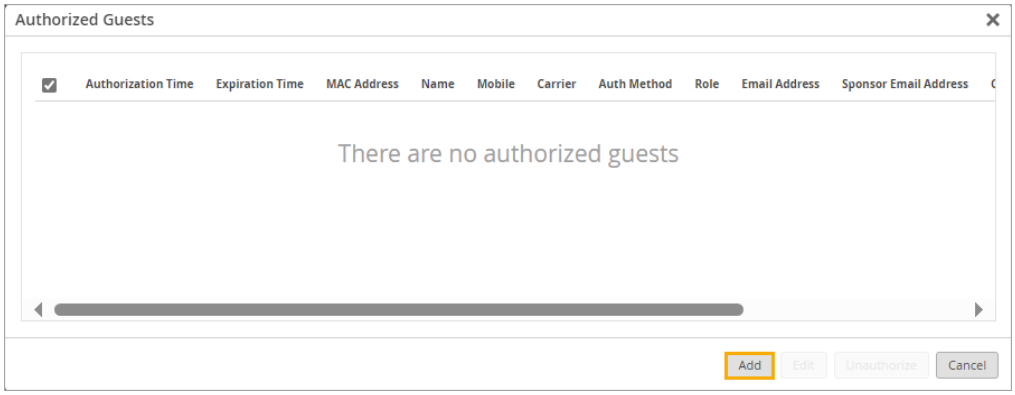
- If the WLAN is in a WLAN template, select **Organization > Wireless | WLAN Templates**, click the template, and then click the WLAN.
- For a site-level WLAN, select **Site > Wireless | WLANs**, and then click the WLAN.

2. In the Edit WLAN window, under **Guest Portal**, click **Forward to external portal**.

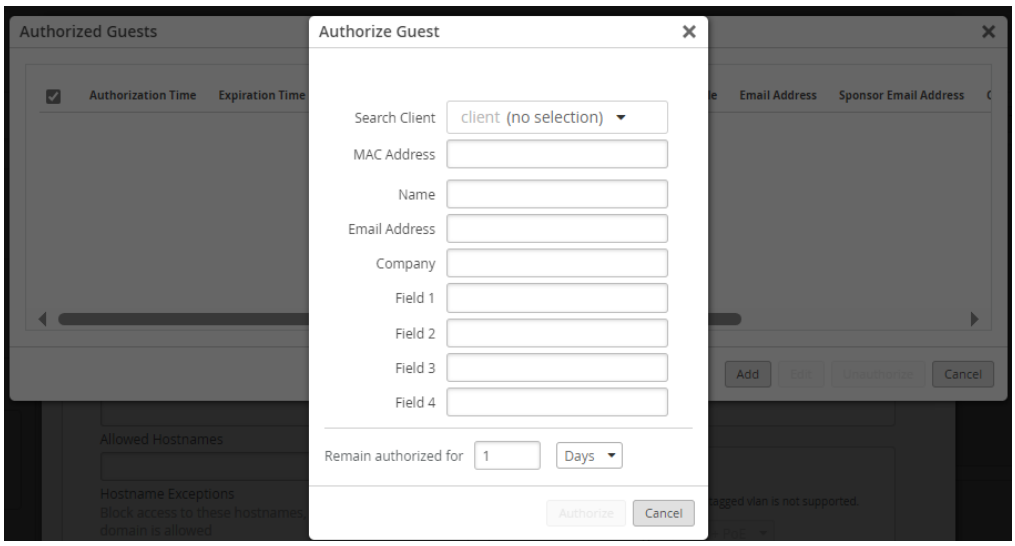


3. (Optional) Click the **Edit Guest Authorization** button if you want to limit access to specific users. Then complete these steps:

   a. In the Authorized Guests window, click **Add**.



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>
                <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)
    $context = sprintf('%s/%s/%s/%d/%d/%d/%d',
        $wlan_id, $ap_mac, $client_mac,
        $authorize_min,
    );
    $token = urlencode(base64_encode($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")) =

YmUyMmJiYTctOGUyMi1lMWNmLTUxODUtYjg4MDgxNmZlMmNmLzVjNWIzNTAwMTIzNC9kNThmNmJiNGM5ZDgvNDgwLzAvMC
8w
expires   : 1768587994
forward    : urlencode("http://www.mist.com")
             http%3A%2F%2Fwww.mist.com%2F
payload-to-sign:
expires=1768587994&token=YmUyMmJiYTctOGUyMi1lMWNmLTUxODUtYjg4MDgxNmZlMmNmLzVjNWIzNTAwMTIzNC9kN
ThmNmJiNGM5ZDgvNDgwLzAvMC8w&forward=http%3A%2F%2Fwww.mist.com%2F
```

```
secret    : test-secret (only used by /authorize-test for testing purpose)
signature : J7VJlf2Zlcs%2BOxhVxCf8hL0XYC0%3D

final URL : http://portal.mist.com/authorize-test?signature=J7VJlf2Zlcs
%2BOxhVxCf8hL0XYC0%3D&expires=1768587994&token=YmUyMmJiYTctOGUyMi1lMWNmLTUxODUtYjg4MDgxNmZlMmN
mLzVjNWIzNTAwMTIzNC9kNThmNmJiNGM5ZDgvNDgwLzAvMC8w&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.eyJhdXRob3JpemVfb25seSI6ZmFsc2UsImV4cGlyZXMiOjE3Njg1ODc5OTQsImFwX21hYyI6IjVjNWIzNTAwMTIzNCIsImZvcndhcmQiOiJodHRwOi8vd3d3Lm1pc3QuY29tIiwiY2xpZW50X21hYyI6ImQ1OGY2YmI0YzlkOCIsIm1pbnV0ZXMiOjQ4MCwid2xhbl9pZCI6ImJlMjJiYmE3LThlMjItZTFjZi01MTg1LWI4ODA4MTZmZTJjZiJ9.msBloHe05XzbzaMEqjsi8XSNWa_3uc--4wucKz3dQGk
final URL : http://portal.mist.com/authorize-test?jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdXRob3JpemVfb25seSI6ZmFsc2UsImV4cGlyZXMiOjE3Njg1ODc5OTQsImFwX21hYyI6IjVjNWIzNTAwMTIzNCIsImZvcndhcmQiOiJodHRwOi8vd3d3Lm1pc3QuY29tIiwiY2xpZW50X21hYyI6ImQ1OGY2YmI0YzlkOCIsIm1pbnV0ZXMiOjQ4MCwid2xhbl9pZCI6ImJlMjJiYmE3LThlMjItZTFjZi01MTg1LWI4ODA4MTZmZTJjZiJ9.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%2BOxhVxCf8hL0XYC0%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=J7VJlf2Zlcs%2BOxhVxCf8hL0XYC0%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

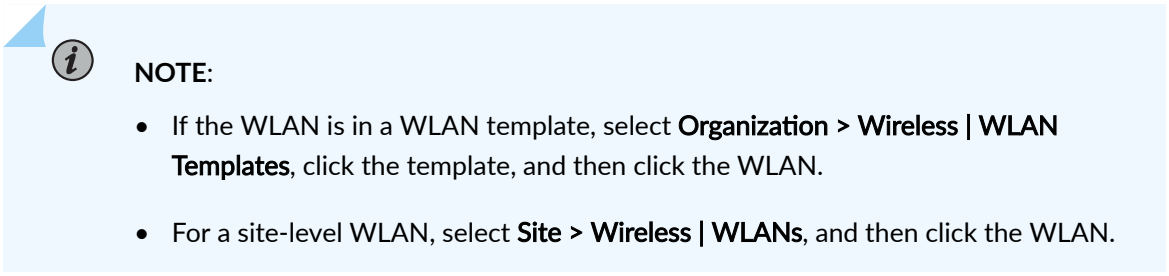
To use an Identity Provider for guest access:

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.

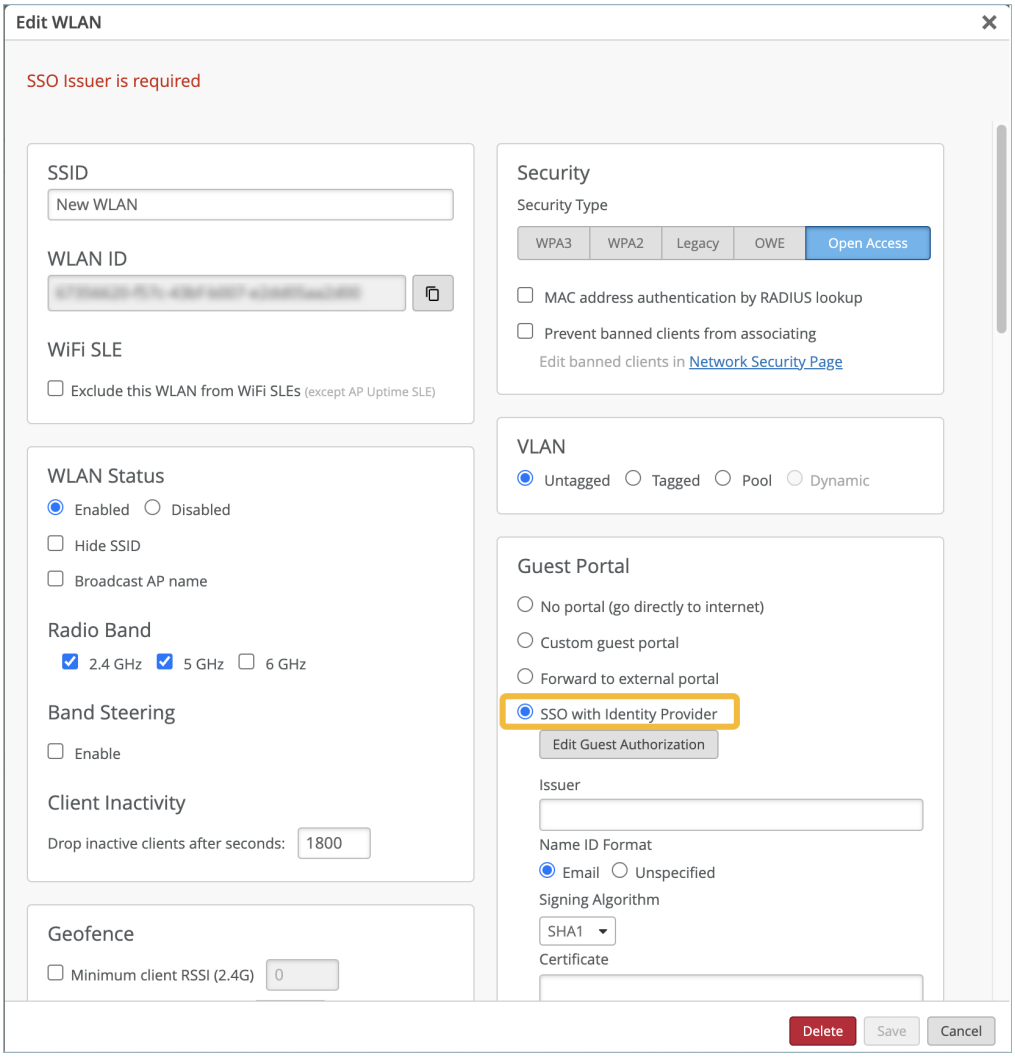
2. Navigate to the WLAN.



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.

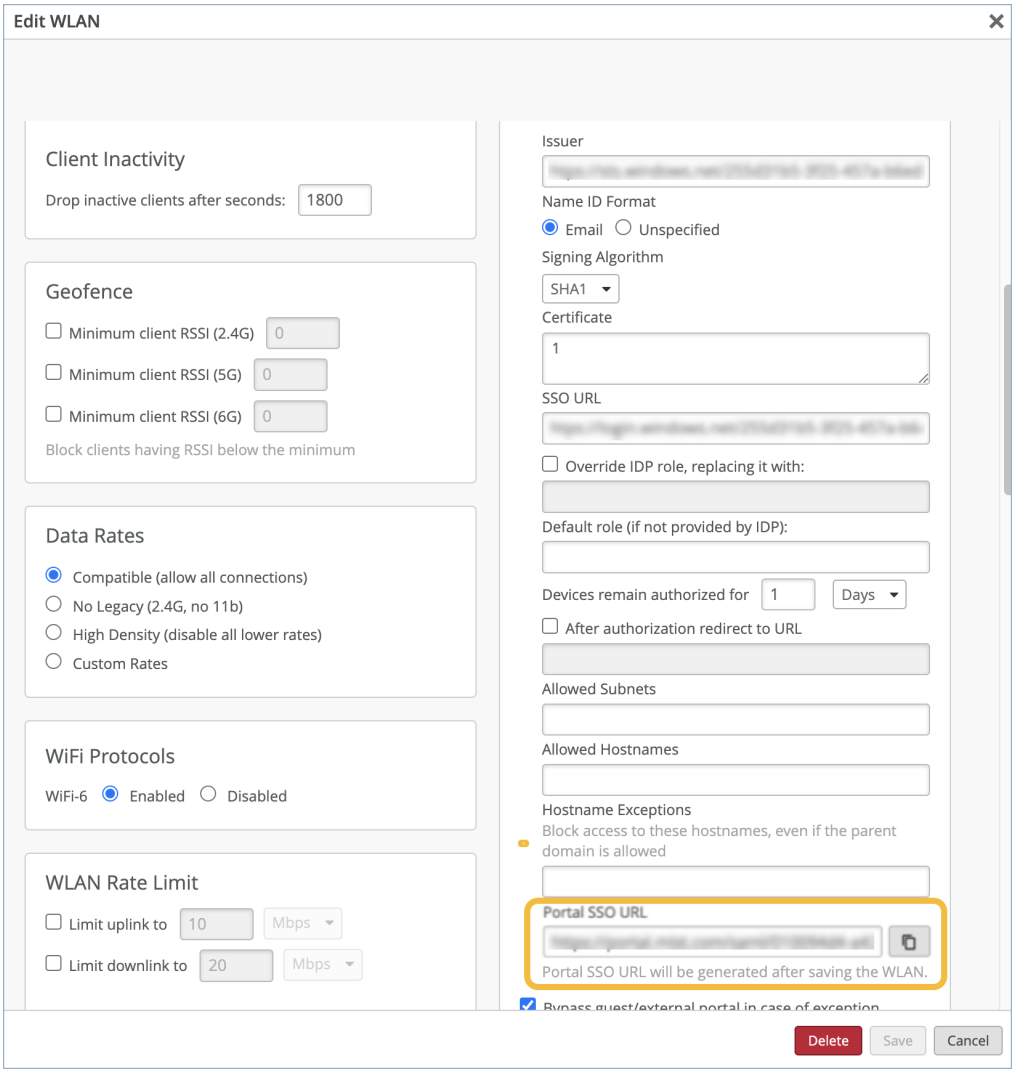
   - **Issuer**—Enter your application's identifier (such as application ID or issuer URL).
   - **SSO URL**—Enter your application's URL/endpoint.
   - **Certificate**—Enter some placeholder text, such as the word *certificate*. Later in this procedure, you'll enter your application's actual certificate.

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.

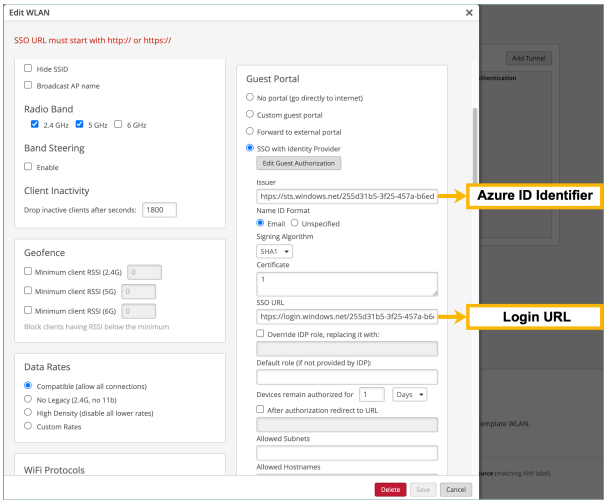
Set up your application in Microsoft Entra ID (previously Azure Active Directory):

- 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.

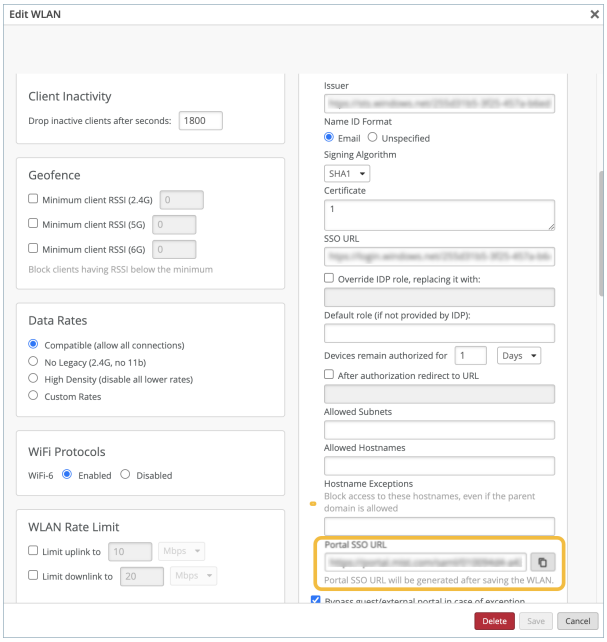
To set up your guest portal SSO with Azure:

1. In your WLAN configuration, select **SSO with Identity Provider**, as described in "Use an Identity Provider for Guest Access" on page 323.
2. Enter the information you obtained from Microsoft Entra in the **Issuer** and **SSO URL** fields.



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.



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**".

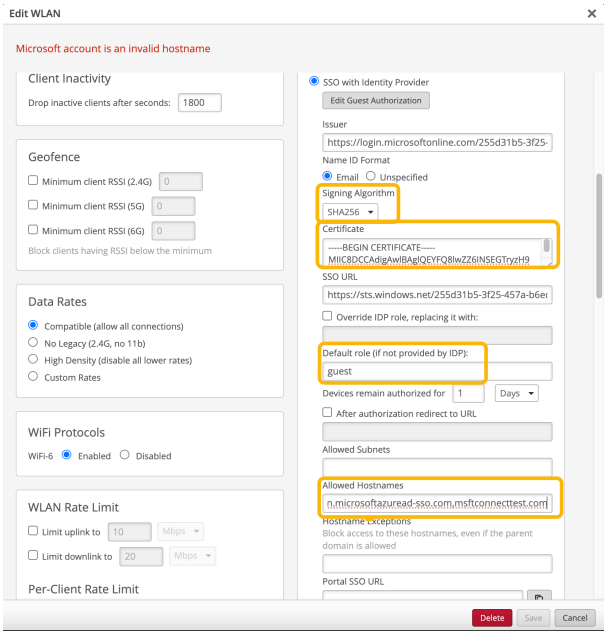
- Edit the “**givenname**” claim. Clear the contents of the **Namespace** field, then change the **Name** field to “FirstName”.
- Edit the “**surname**” claim. Clear the contents of the **Namespace** field, then change the **Name** field to “LastName”.

- 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.

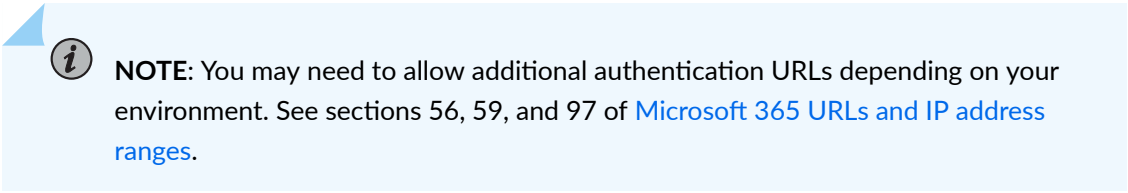
7. In the Juniper Mist portal, navigate to the WLAN.

> **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.



For a complete list of the necessary Microsoft FQDNs, refer to your Microsoft documentation. Suggested Microsoft FQDNs include:

- **login.microsoftonline.com**
- ***.aadcdn.msftauth.net**
- ***.aadcdn.msftauthimages.net**
- ***.aadcdn.msauthimages.net**
- ***.logincdn.msftauth.net**
- **login.live.com**
- ***.msauth.net**
- ***.aadcdn.microsoftonline-p.com**
- ***.microsoftonline-p.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.

Juniper Mist supports SAML 2.0 for device authentication onto the network. As such, you can set up a Single Sign-On (SSO) WLAN for guest access using OneLogin™ as the Identity Provider (IdP). SAML SSO allows users to log on once to their identity provider, and then seamlessly access multiple other web applications without having to log in again. Both Juniper Mist guest portal and OneLogin support RADIUS EAP-TTLS/PAP and EAP-PEAP/MSCHAPv2 authentication methods.

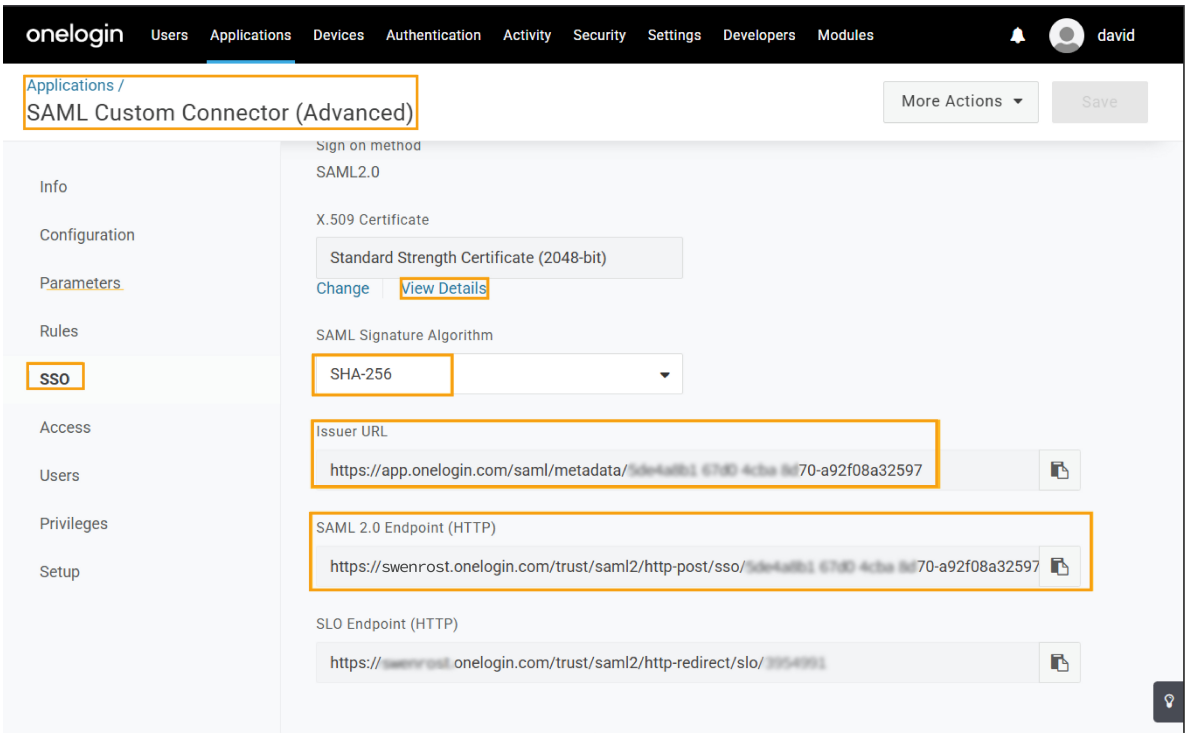
Before you begin setting up the Guest Portal, you should have admin credentials for your OneLogin portal and already have a SAML application (or be ready to create one) that your Mist clients can access (see: Configuring SSO for SAML-Enabled Applications for instructions).

You'll need the following information from the OneLogin SAML application (Figure 1) to configure the OneLogin SSO in the Juniper Mist portal (Figure 2).

In addition, you'll need to copy the **Portal SSO URL** from the Mist portal to your OneLogin application to complete that side of the setup (the Portal SSO URL doesn't get created until after you save the initial WLAN configuration, so you actually loop back to the WLAN configuration page).

- For the OneLogin application, the Signature Algorithm should be set to **SHA-256**. At the same time as you make this change, you can copy and save the **X.509 Certificate** for later use in the Juniper Mist portal. The x.509 certificate is the public certificate that establishes trust between OneLogin and your Juniper Mist Guest Portal.
- Also from your OneLogin application, copy and save the values shown for **Issuer URL** and **SAML 2.0 Endpoint**.

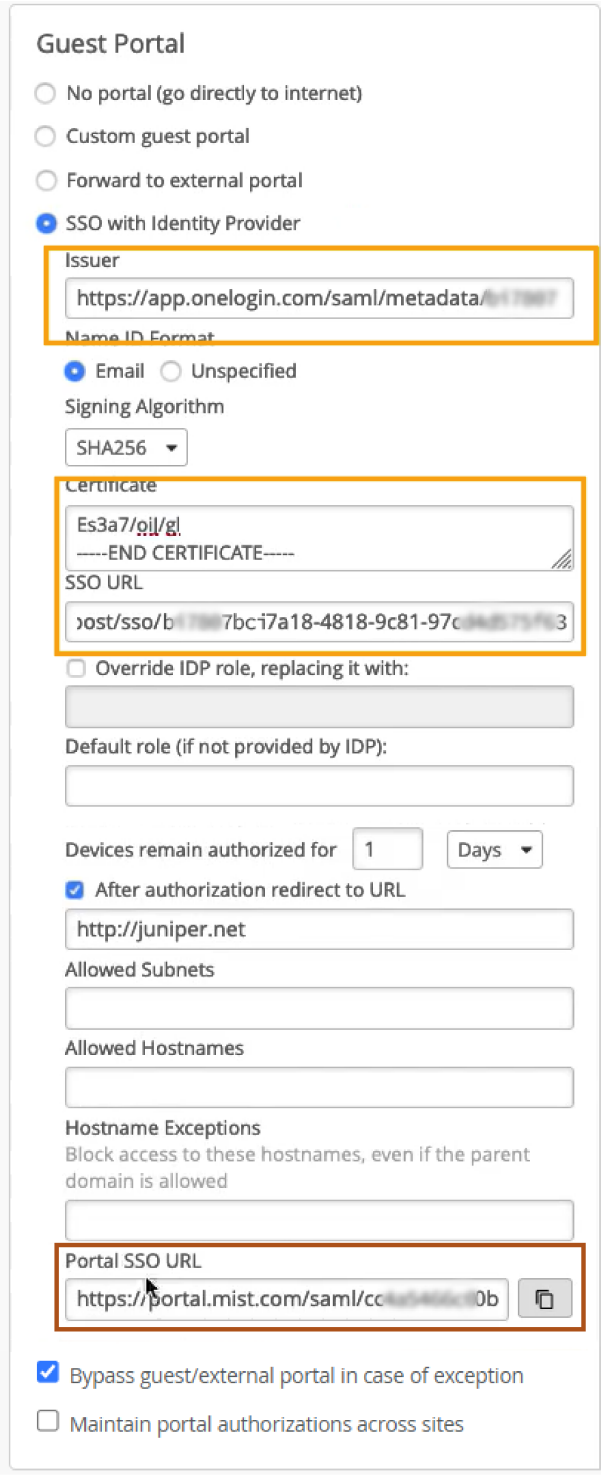
Figure 29: OneLogin SAML App SSO Configuration Screen



To set up a WLAN with SSO access from OneLogin:

1. From the Juniper Mist menu, click **Site | Wireless > WLAN** and then either select an existing WLAN from the list that appears or click the **Add WLAN** button to create a new one.

Figure 30: Configuration Details for OneLogin Interoperation



2. Scroll to the **Guest Portal** section of the WLAN configuration page, and then select **SSO with Identity Provider**.

3. In the fields that appear, use the information you gathered from your OneLogin SAML application, (Figure 1), to fill in the following:
   - **Issuer**—Enter the **issuer URL** from your OneLogin application.
   - **SSO URL**—Enter the **SAML 2.0 Endpoint** from your OneLogin application.
   - **Certificate**—Paste the **X.509 Certificate** for your OneLogin application.
4. (Optional) You can limit how long clients can stay on the network before having to log in again. To do so, select a time from the **Devices remain authorized for __** field.
5. (Optional) After a client logs in, you can redirect them to a given URL or home page. To do so, type that URL in the **After authorization redirect to URL** field.
6. Click the **Create** or **Save** button, as the case may be, to upload the configuration to the Mist cloud and generate the **Portal SSO URL** , which you will need to enter in the OneLogin SAML application so it can recognize requests from the Guest Portal.
7. Reopen the WLAN configuration page for your WLAN, and then **Copy** the **Portal SSO URL**.
8. For detailed instructions, see Advanced SAML Custom Connector. Otherwise, you can go to the OneLogin Application Details page and paste the **Portal SSO URL** you just copied into the following fields:
   - **RelayState**
   - **Audience (EntityID)**
   - **Recipient**
   - **ACS (Consumer) URL Validator**
   - **ACS (Consumer) URL**
   - **Login URL**

   On the same page in the OneLogin App configuration, you can you can include a **SAML Signature Element** for assertions and the responses. Select **Both**.

   With regards to setting up the OneLogin application for interoperation with the Juniper Mist Guest Portal, the above is the only configuration you need. However, you will also need to specify which users you want the application to appear for.
9. To have the OneLogin login page open correctly when redirected by the Guest Portal, you may need to specify various hostnames to cover the domain. Do this in the **Allowed Hostnames** field on the Juniper Mist WLAN configuration page. Use this page from OneLogin, or a packet capture to monitor port 53 and see what the domain resolves to.
10. When the **Bypass guest/external portal in case of exception** option is enabled, if an AP cannot reach the portal or OneLogin service, it will automatically authorize the client to connect to the WLAN.
11. Click **Save** to complete the OneLogin SSO for your Guest Portal.

To verify that everything is working correctly, log out of the OneLogin portal and then log in at the WLAN you just created. You will be redirected to the OneLogin page where you can enter your login credentials, and then redirected to the Juniper Networks homepage (or whatever URL you specified).

Authorize, Reauthorize, and Reconnect Guest Clients

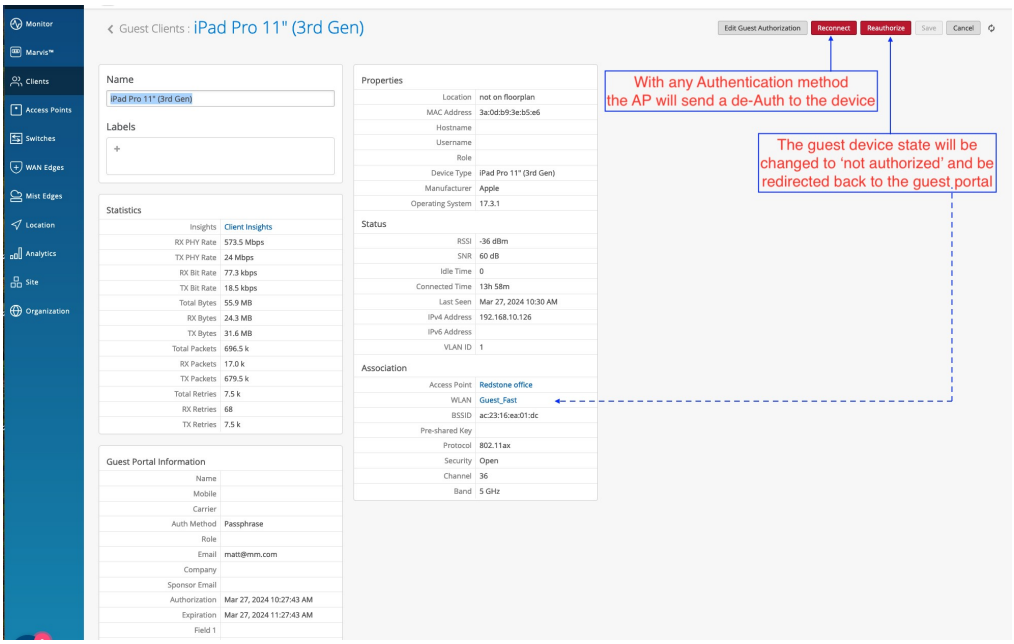
SUMMARY

Use this procedure when you want to force a client to roam to a different AP, require reauthentication with a newly updated passphrase, or deauthorize a device that shouldn't be on your network.

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.

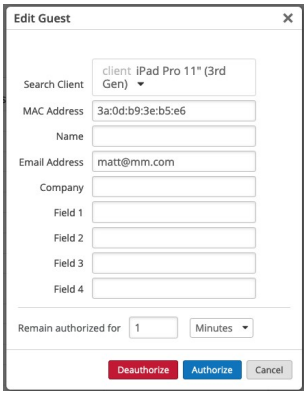
- **Reconnect**—Have the AP send a deauthentication frame to the selected clients, thereby removing them from the client list and triggering a reconnect. This is typically used to nudge the device to roam to another AP.
- **Reauthorize**—Log selected clients off the guest portal, thereby forcing them 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 31: Reconnect and Reauthorize**



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.

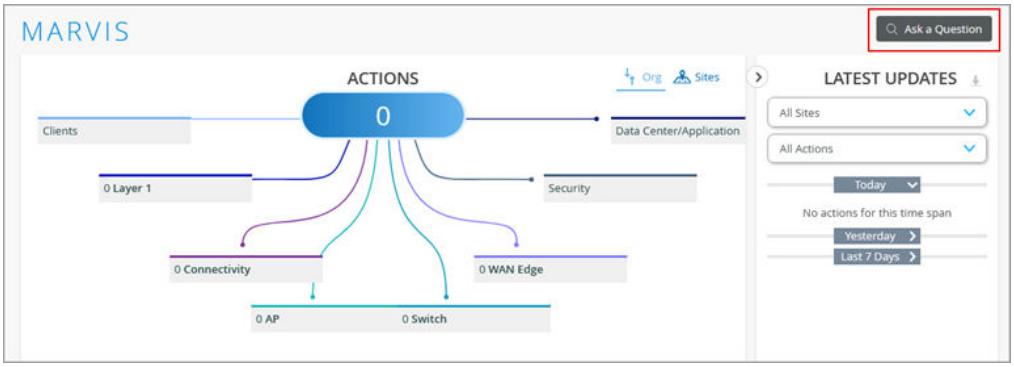


Troubleshoot a Guest Network That Doesn't Work

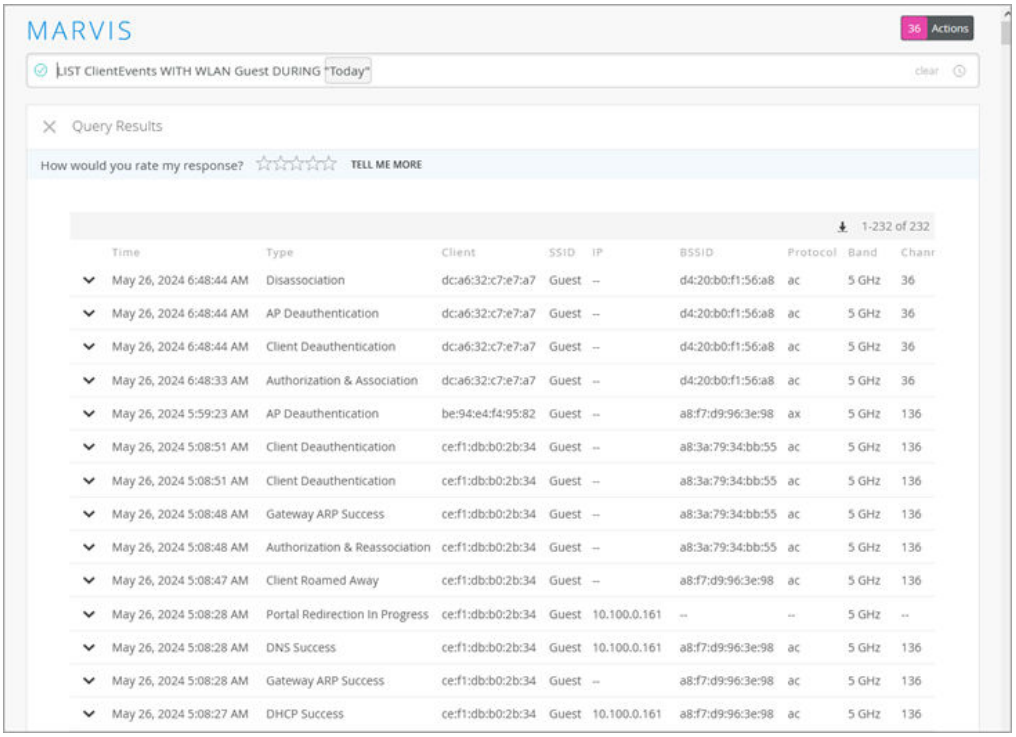
SUMMARY

If your guest network isn't working, use this information to help identify the issues and address the root causes.

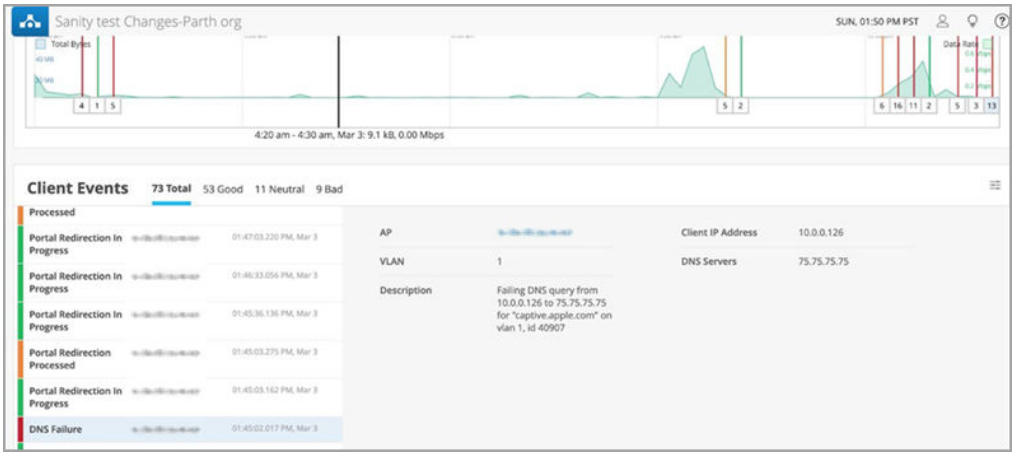
If your guest network is not working, you can use Marvis to identify the issues that are causing the problem. You can search for the client events associated with the guest WLAN by using the **Ask a Question** feature on the Marvis Actions page (**Marvis** > **Marvis Actions**).



Marvis can give a detailed description of all the events including the redirect URL, VLAN tag, AP BSSID. The redirect URL is shown in the case of an external portal. The following example shows events associated with a Mist guest portal.



You can find more details in the Client Events section under Client Insights for a failing client. Typically, if the issue is with DNS not being able to resolve the external portal redirect URL, you will see DNS failures under Client Events for the failing client. Also, if the DNS server is not able to resolve the URL after Mist successfully redirects the client to the URL, you will see a 'Portal redirection' event; but you will not see any 'Portal authorization' event.



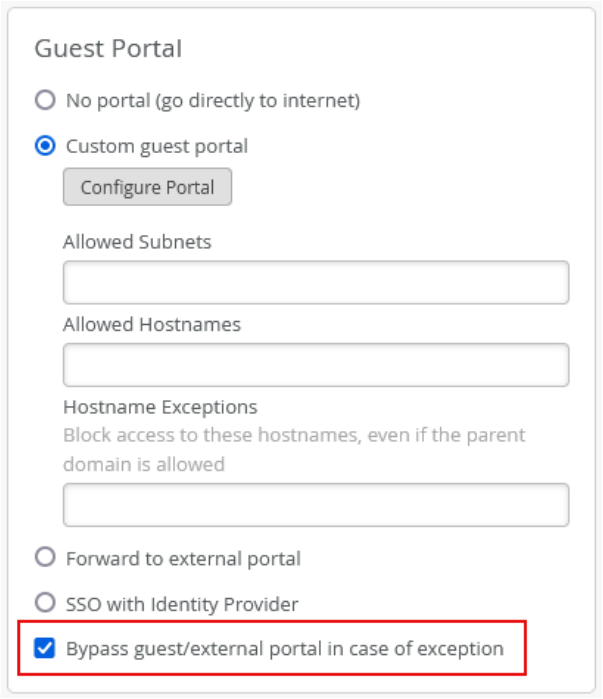
If multiple clients report this issue, you will see a 'DNS server failing' warning on the **Analytics** > **Events** page.

For the event “Portal Redirection in Progress”, you can see the redirect URL link in the event details section. In case of an external portal, you can use the following link to verify and check if all the necessary information has been included: http://portal.mist.com/authorize-howto

If you see a portal redirection event in Client Insights but do not see any captive portal (CNA) pop-up on your device, enter an HTTP URL such as http://neverssl.com in a browser, provided that the client has an IP address. If you see redirection to the portal on your browser, you can use the guest authorization method and see a 'Portal Auth Success' event for the client.

Additionally, check if the AP has cloud connectivity or not. For guest authorization, the AP queries the cloud to get authorization information about the client. If the AP cannot establish a connection to the cloud, Guest authorization information regarding the client cannot be retrieved.

To tackle this scenario, select the **Bypass portal in case of exception** check box in the Guest Portal section on the New WLAN configuration page (**Site** > **WLANs** > **Add WLAN**) as shown below.



FAQs: Guest Portal

SUMMARY

Get answers to common questions about guest portals.

IN THIS SECTION

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 for your regional cloud instance (such as http://portal.mist.com , http://portal.eu.mist.com, and so on) is permitted through the firewall. For FQDN and port details for all cloud instances, 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: "Troubleshoot a Guest Network That Doesn't Work" on page 337.

Guest Portal Redirects Not Working

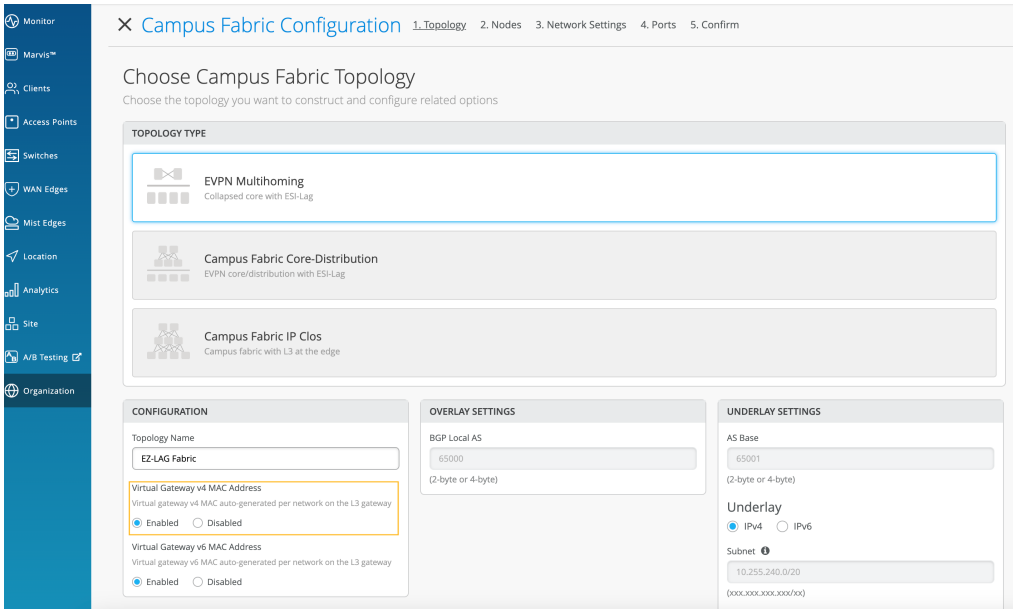
If you configured Campus Fabric EVPN Multihoming or Core Distribution with a CRB sub-type topology in the Juniper Mist portal, you may need to go back and edit your fabric configuration to enable the

Virtual Gateway v4 MAC Address or **Virtual Gateway v6 MAC Address** option. This assigns a MAC address to the switch IRB interface port that is used for the virtual gateway and will prevent a problem with Guest Portal redirects to a Identity Services Engine (ISE) or other server.

To enable a virtual gateway MAC address,

1. From the Mist portal menu, click **Organization | Wired > Campus Fabric** and then select the Site and topology that has the switches your APs with the Guest Portal connects to.
2. In the Campus Fabric Topology page, select the fabric you are using, Campus Fabric Core Distribution with a CRB sub-type topology, or Campus Fabric EVPN multihoming.
3. Enable the **Virtual Gateway v4 MAC Address** or **Virtual Gateway v6 MAC Address** option, as shown in Figure 1.
4. Save your changes.

Figure 32: Virtual Gateway MAC Address for Guest Portals



- See Configure Campus Fabric EVPN Multihoming or

  Configure Campus Fabric Core-Distribution for complete instructions.

CHAPTER 7

Radio Management

SUMMARY

Use the information in this chapter to understand how Juniper Mist uses radio resource management (RRM), with minimal human intervention, to optimize the user's network experience across a site.

IN THIS CHAPTER

Video Overview

Video: AI Radio Resource Management

What Do You Want to Do?

Table 28: Top Tasks

If you want to...	Use these resources:
Use RF templates *Learn about RF templates and how you can use them to apply configurations across all APs or model-specific APs in a site*	"RF Template Configuration" on page 352
Explore the Radio Management page *View radio settings, view channel and power distribution, monitor RRM events for your site, and more*	"Monitor RRM" on page 358
See examples of RRM implementation for dual band usage	"RRM Usage Examples" on page 361

Radio Resource Management (RRM)

SUMMARY

Juniper Mist Radio Resource Management (RRM) is an automated, cloud-based system that continuously manages and optimizes the wireless radio environment to improve the user experience.

IN THIS SECTION

RRM uses data collected by the dedicated scanning radio in every Mist Access Point (AP) to measure capacity, interference, and usage patterns throughout the day. It uses reinforcement learning to dynamically adjust radio settings including:

- Channel selection (automatic channel switching)
- Transmit power levels
- Channel width
- Band steering between 2.4 GHz and 5 GHz
- Disabling or converting radios (that is, turning off 2.4 GHz radios on some APs)

Mist APs send radio frequency events and data to the Mist cloud on a continual basis, where the RRM optimization algorithm analyzes the information to identify changes and make adjustments. The amount of data each AP sends to the Mist cloud is small, on the order of kilobytes rather than megabytes or gigabytes.

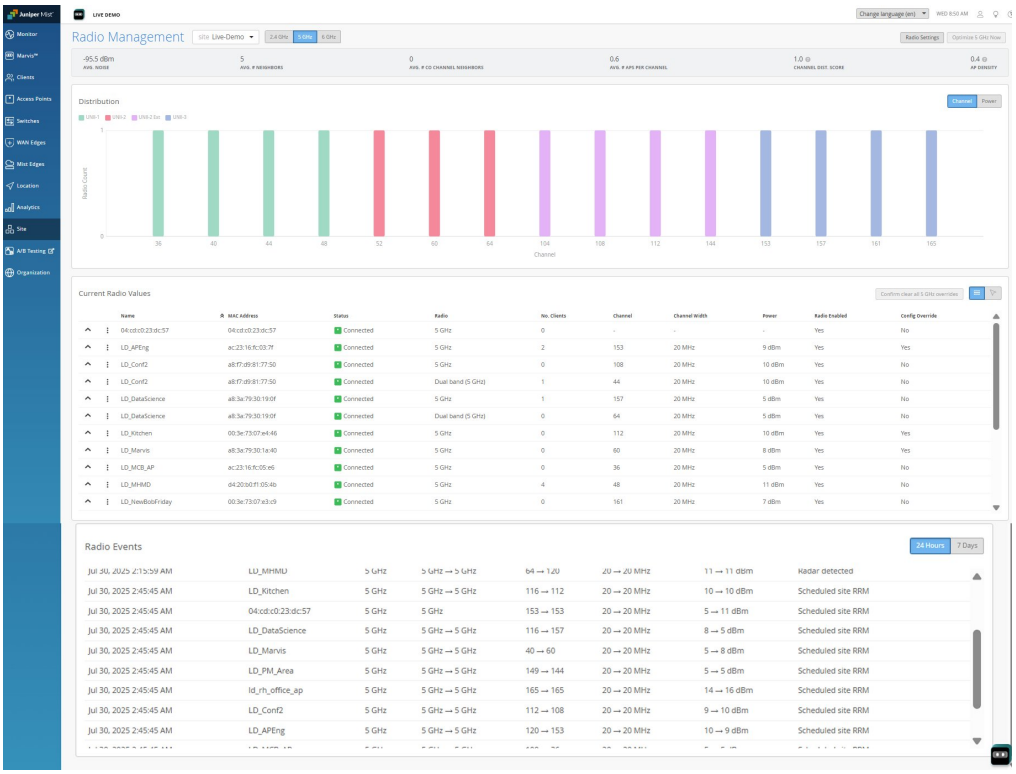
On the Mist cloud, RRM also aggregates historical data for the sites from the past 30 days to identify long-term trends. The Mist portal sends updates back to the relevant APs nightly, at around 3:00 a.m. (the exact time varies; the update is automatic, and not configurable). Mist's system of continuous reinforcement learning dynamically adjusts the radio settings to keep the user experience at ideal conditions. You do not need to manually rebalance your Wi-Fi network, for example, to address the common problem of drift.

Note that some radio adjustments on an AP are local and made immediately in response to an acute event. These include changing channels for radar detection, adjusting for Wi-Fi and non-Wi-Fi interference, and increasing signal strength in response to a neighbor AP going off line. Although these

changes are AP specific and occur in real-time, a record of the triggering event is still sent to the Mist cloud as part of the daily data. These events are included in the long-term pattern analysis to prevent periodic but recurrent issues.

You can see a snapshot of your wireless network, shown in Figure 1, as well as the list of AP events, from the Radio Management dashboard in the Mist portal (**Site > Radio Management**):

Figure 33: The Radio Management Dashboard



To improve coverage and optimize capacity, RRM takes into account key factors from the the Wireless Capacity SLE, including client count, client usage, and interference. Mist RRM can automatically adjust AP power or change wireless channels when the capacity SLE is not met. After applying any updates, Mist will continue to monitor the capacity SLE to determine whether its changes produced measurable improvements. For more information, see "Wireless SLEs" on page 375.

You also have the option at any time to optimize the radios manually. At the top of the Radio Management page, select the site and the band, and then click the optimize button at the top-right corner of the page. The button label includes the selected band: **Optimize 2.4 GHz Now**, **Optimize 5 GHz Now**, or **Optimize 6 GHz Now**.

Video: Whiteboard Technical Series: Reinforcement Learning

Without RRM, a wireless network would be almost unmanageable:

- WiFi and non-WiFi interference (radio signal interference) causes clients and APs to pause transmissions for indefinite periods of time.
- Unmanaged AP transmit power could cause coverage gaps, decreased signal-to-noise ratios (SNR), reduced bandwidth, or increased co-channel interference.
- Unmanaged channel width could cause increased co-channel interference and decreased SNR in high-density environments. This results in lower signal quality and thus, poor performance.

How Juniper Mist RRM Works

Using the dedicated scanning radio built into every Juniper Mist Access Point (AP), Mist RRM measures and calculates capacity, usage, and interference factors all day, every day. RRM uses these calculations and measurements as references to the users' network experience, also known as user minutes. RRM stores up to 30 days of this data which creates a long-term trend baseline. Using the Wireless Site Maintenance Aggregator and manual corrections, RRM can adjust to shortcomings or leverage enhancement opportunities in the wireless environment by:

- Using automatic channel switching (ACS) to respond to overcrowded or interference-prone channels
- Using automatic power adjustments to increase or decrease the AP power output (based on client experience)
- Increasing or decreasing channel width to improve throughput
- Using auto-cancellation to disable the 2.4 GHz radio on certain APs in the network
- Using auto-conversion to convert dual-band capable radios from 2.4 GHz operation to 5 GHz operation

Mist RRM—Events and environmental data in a site's wireless network are sent by the site APs to the Mist cloud for evaluation. Mist compiles long-term, cloud-based trend data from the received information and compares it against the No Link Title for the site. The comparison helps determine if a change to a site's wireless band configuration will be beneficial. Mist band control capabilities allow for automatic changes to:

- AP channel assignments
- Dynamic Frequency Selection (DFS)
- AP broadcast power settings
- Band control

When Mist RRM changes channels, it does so based not only on the current environment, but on historical knowledge. Even if the current environment makes the use of a certain channel look good, Mist remembers if it has seen co-channel interference, or other problems, on that channel. If so, RRM reduces the priority of that channel and chooses a different channel for the affected AP.

If an AP detects a radar signal, the AP immediately jumps to a different channel. This is known as DFS and is intended to reduce interference with radar signals by other wireless (5 GHz) transmitters. The channel change is disruptive to wireless clients and can lead to overcrowding on the channels to which the APs jump.

To help reduce the effects of DFS, APs send all radar events to the Mist cloud. The cloud stores the event data including the channel on which the AP saw the radar signal. Over time, RRM learns which APs see the most radar and on which channels. Based on this learning, RRM restricts the most impacted APs in a site from operating on channels that have the most radar hits. This is known as DFS punishment because the site now operates on a DFS optimized channel distribution rather than on a uniformity-optimized channel distribution. Because of DFS punishment, some overcrowding may occur.

Juniper Mist RRM can adjust the power output of the AP's radios. RRM might increase the broadcast power on neighboring APs to compensate for the loss of a neighbor AP. RRM only reduces power on an AP if that reduction does not affect coverage.

RRM can adjust the channel width for the 5 and 6 GHz radio bands. 2.4 GHz radios can only operate on 20 MHz wide channels. Using channel bonding, 5 GHz radios can operate on 20, 40, or 80 MHz wide channels; And 6 GHz radios can operate on 20, 40, 80, 160, or 320 MHz wide channels (depending on the country). The wider the channel, the more potential throughput is available.

The cloud-based **Wireless Site Maintenance Aggregator** leverages site traffic data, including active client minutes and traffic metrics (transmitted and received), to identify the hours at each wireless site when traffic is lowest. This allows for catered scheduling of network maintenance or policy updates, at your site, during these low-traffic periods. The aggregator uses a combination of statistical methods to calculate predictions, ensuring efficient site maintenance.

The aggregator performs the following functions:

- **Makes Predictions Based on Historical Data**: The aggregator uses a moving window of 14 days of historical traffic data to predict the least active hours at each site.
- **Aggregates Data at Scale**: The solution processes data at scale, aggregating metrics like active client minutes, transmitted bytes, and received bytes across thousands of wireless sites. The medians are then normalized by site to account for variations in traffic patterns between sites.
- **Predicts the Hours of Lowest Activity**: A weighted activity score is generated using the normalized medians, which is a combination of active client minutes, transmitted bytes, and received bytes. The lowest activity hour (based on the weighted activity score) is identified for each site.
- **Confidence Scoring**: Confidence scores are calculated to determine the reliability of predictions. Sites with strong daily seasonality (predictable traffic patterns) will have higher confidence.

- **Stores Site Activity Predictions:** The predicted local hour for each site is stored in the Juniper Mist cloud to enable quick access by the scheduling system.

Channel assignments for 6 GHz bands

By default, RRM assigns 6GHz radio bands with preferred scanning channels (PSCs) and non-PSC, unless a subset is manually selected. In fact, our experience shows that clients are quite able to discover non-PSCs using out of band mechanisms such as reduced neighbor reports or 11k neighbor reports.

The channel default assignment logic in 6 GHz bands for different channel widths is as follows:

- For 20 MHz and 40 MHz width, all allowed channels (PSC and non-PSC) are used as the primary channel.
- For 80 MHz and 160 MHz width, PSC channels are used as primary channels.

RRM can control the network band by turning off unneeded 2.4 GHz radios to reduce co-channel interference. Again, RRM uses its knowledge of the site's radio spectrum to determine when and if turning off a 2.4 GHz radio will result in better user experience.

Mist RRM never makes changes for the sake of making changes. If the Capacity SLE for a particular site is 90% or above, there's not much to be gained by making changes, so RRM doesn't make changes. Additionally, if a change is warranted but RRM can't make a positive change, there might be something in the environment that needs further investigation.

Auto Cancellation and Auto Conversion

There are two additional RRM-related features you should know about: Table 29 on page 348.

Table 29: Auto Cancellation and Auto Conversion

Auto Cancellation	Auto Conversion
Automatically disables 2.4 GHz radios.	Automatically converts dual-band capable radios to 5 GHz operation
Reduces co-channel interference in the 2.4 GHz band by reducing the number of broadcasting radios.	Reduces co-channel interference in 2.4 GHz spectrum by reducing the number of broadcasting radios.

Table 29: Auto Cancellation and Auto Conversion *(Continued)*

Auto Cancellation	Auto Conversion
Improves performance on the 2.4 GHz band.	Improves performance on the 2.4 GHz band.
Turns off 2.4 GHz radios only if the removal of that radio will not cause neighboring APs to increase transmit power to compensate.	Converts 2.4 GHz radios only if the removal of that radio from the 2.4 GHz network will not cause neighboring APs to increase transmit power to compensate.
Typical cancellation rate for 2.4 GHz radios is roughly 40%. Auto cancellation never removes more than 50% of 2.4 GHz radios in a given site.	Typical conversion rate for 2.4 GHz radios is roughly 40%. Auto conversion never removes more than 50% of 2.4 GHz radios in a given site.
Supported on all Juniper Mist APs	Supported only on AP43, AP45, and AP63 models
	Increases coverage in the 5 GHz band with the addition of another broadcasting radio

You might want to consider auto cancellation or auto conversion in primarily 5 GHz networks where the important devices are managed and their roaming profiles are well known. In schools or other environments where you don't care about the guest network or the variety of client devices that might show up, these features can be very beneficial.

On the other hand, you might want to disable these features in less densely covered environments where a lot of mission critical devices run only on 2.4 GHz.

Dual 5 GHz Operation

When the AP43, AP45, AP47, or AP63 are operating in Dual 5 GHz mode, the radios split the 5 GHz band and are locked to a specific range of channels. See Table 30 on page 349.

Table 30: Radio Operations and Usable Channels

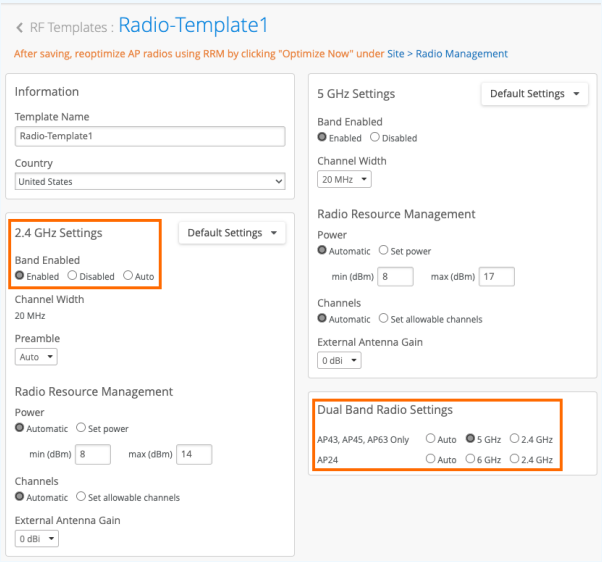
Wireless Mode	Dual Band Radio (2.4 GHz)	Dual Band Radio (5 GHz)	5 GHz Radio
Dual Band Mode	All 2.4 GHz channels	N/A	All 5 GHz channels

Table 30: Radio Operations and Usable Channels *(Continued)*

Wireless Mode	Dual Band Radio (2.4 GHz)	Dual Band Radio (5 GHz)	5 GHz Radio
Dual 5 GHz Mode (AP43 and AP63)	N/A	Channels 100-165	Channels 36-64
Dual 5 GHz Mode (AP45 and AP47)	N/A	Channels 36-64	Channels 100-165

NOTE: We recommend setting the 5 GHz channel width to 20 MHz when using auto-conversion or dual 5 GHz. Using the 20 MHz width helps maximize the number of 5 GHz radios in use while minimizing co-channel interference.

If you want to use operate Dual 5 GHz radios in 5 GHz mode, configure **Dual Band Settings** to **5 GHz** and set the **2.4 GHz Settings** to **enabled**.



RRM Configuration Options

IN THIS SECTION

Configuration Hierarchy

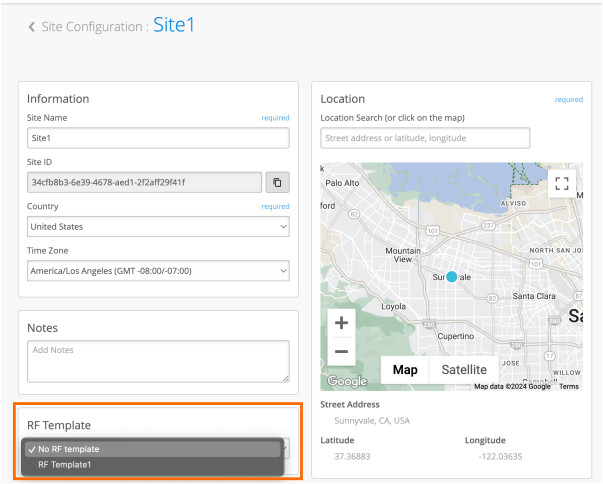
Juniper Mist provides a flexible configuration hierarchy that allow you to manage RRM configuration through the use of RF templates, device profiles, or directly on the APs themselves.

In terms of which settings take precedence, both RF templates and device profiles are optional elements. If you do not configure either, then you must configure radio management options on each AP individually. This is, obviously, a difficult task in a large org with a lot of APs. To clarify, RRM configuration settings can be applied through:

- "RF Templates" on page 352—are configured at the org level (*Organization* > *RF Templates*) and applied at the Site configuration level (*Organization* > *Site Configuration* > Select the site to configure.) RF templates have the widest scope of application, but can be overridden by both device profiles and direct AP configuration.
- "Device Profiles" on page 354—are configured at the org level (*Organization* > *Device Profiles*), but are applied only to specific devices selected in the profile. Device profile settings can override RF template settings but can be overridden by settings made directly on the APs.
- "Direct Device Level Configuration" on page 356—has the highest precedence of the three configuration options. Settings made directly on the APs (*Access Points* > Click AP name) override RF templates and device profiles.

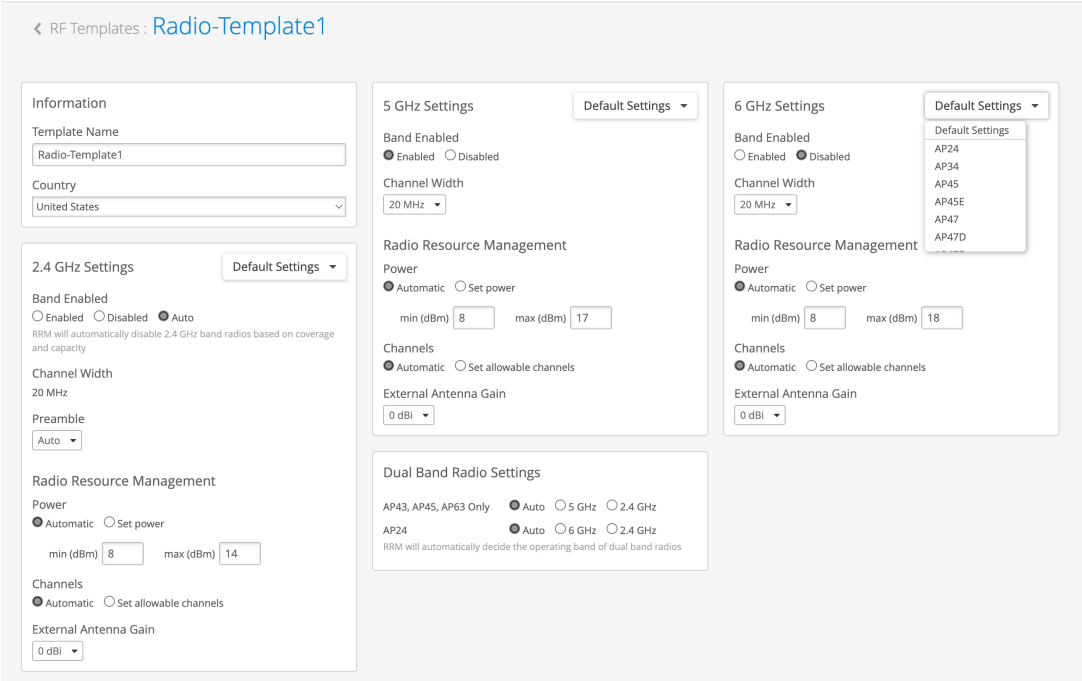
RF Template Configuration

Every site should have an RF template assigned. The RF template is where you begin configuring the constraints for RRM. Configuration performed at the RF template level applies to all APs in the assigned site unless overridden with a device profile or direct device configuration. You apply the RF template to the site by selecting the template on the Site Configuration page (Organization > Site Configuration > Select a site to configure.)



All the band specific settings in the template apply to all devices in the site unless you change settings for specific device types in the **Default Settings** menu.

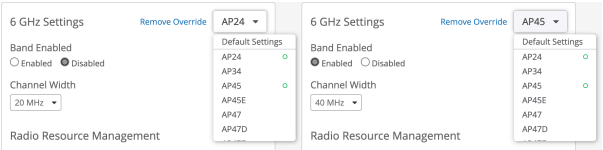
Figure 34: RF Template



In the Figure 34 on page 353 configuration page, shown above, you can configure all three frequency bands. Each band contains a Default Settings pull-down menu. Changes you make to any band settings without changing the Default Settings menu apply to all APs in the assigned site regardless of AP model.

You can customize the RF template settings in a given band to apply to specific models of APs by selecting the model name from the Default Settings menu, as shown in the 6 GHz settings block above. Any 6 GHz settings apply only to the selected device model.

You can make settings for multiple device models within a single RF template. For example you could disable the 6 GHz radio band on all your AP24s but leave it enabled on all your AP45s. The template maintains that distinction as shown below.



In the Figure 34 on page 353 image above, you can see that the 2.4 GHz band is set to Auto which allows for auto-cancellation on any model AP. The Dual Band Radio Settings section is also set to Auto, which allows for auto conversion on dual-band radio APs.

Dual and tri band radio settings also apply to all dual-band or tri-band capable APs in the site.

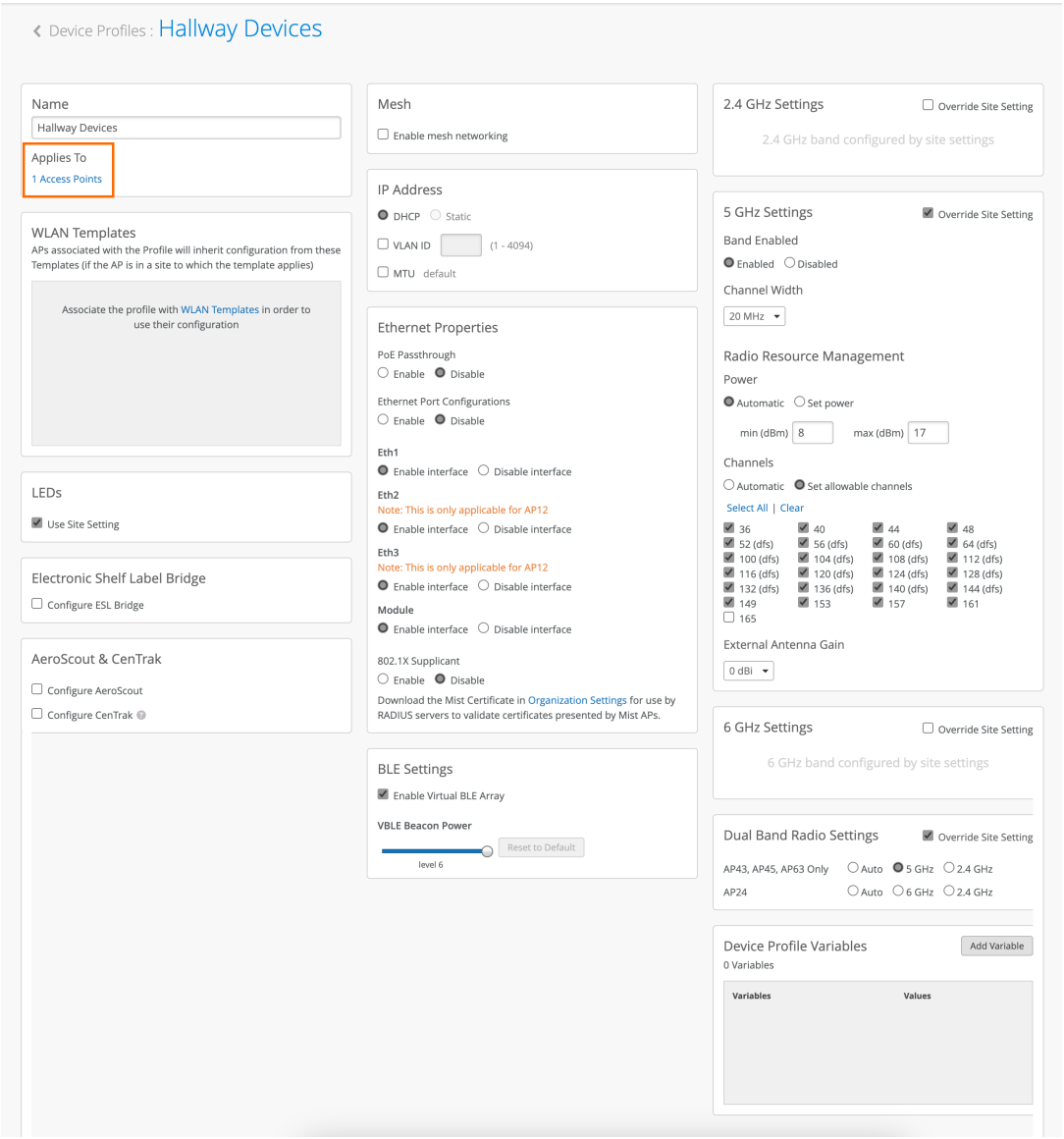
NOTE: If you do not select Auto in the 2.4 GHz *Band Enabled* section, the *Dual Band Radio Settings*, or the *Tri Band Radio Settings* section in the RF Template, then you will not be able to choose Auto for either device profile level or device level.

Device Profile Configuration

Device profiles are used for advanced use cases to apply specific configuration on a subset of APs.

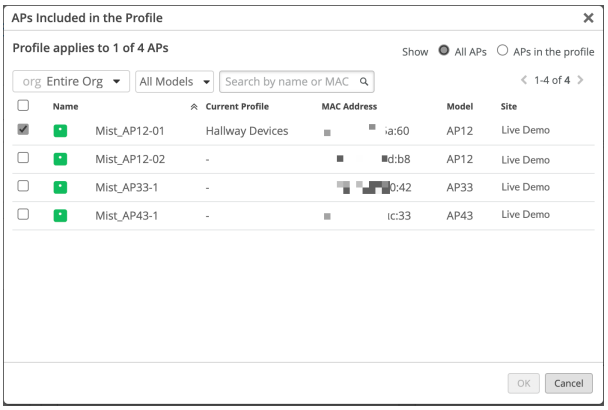
Configuration performed at the device profile level applies to specific devices or device groups as highlighted in the Figure 35 on page 355 image below. Within a device profile, you can override the RF template (site) settings on a per-band basis. This *Hallway Devices* profile overrides the settings for the 5 GHz band and for the Dual Band Radio Settings.

Figure 35: Device Profiles



To choose which APs inherit the settings from your device profile, click the link in the *Applies To* section. When you click the link, a window appears in which you can select the APs to which the profile is applied. See Figure 3 on page 356.

Figure 36: Access Point Selection



This particular site has 4 APs, one of which is selected. That AP is the only one that will inherit the settings from the device profile.

Direct Device Level Configuration

Device level configuration can be useful for specific override configuration such as overriding the bandwidth on one AP.

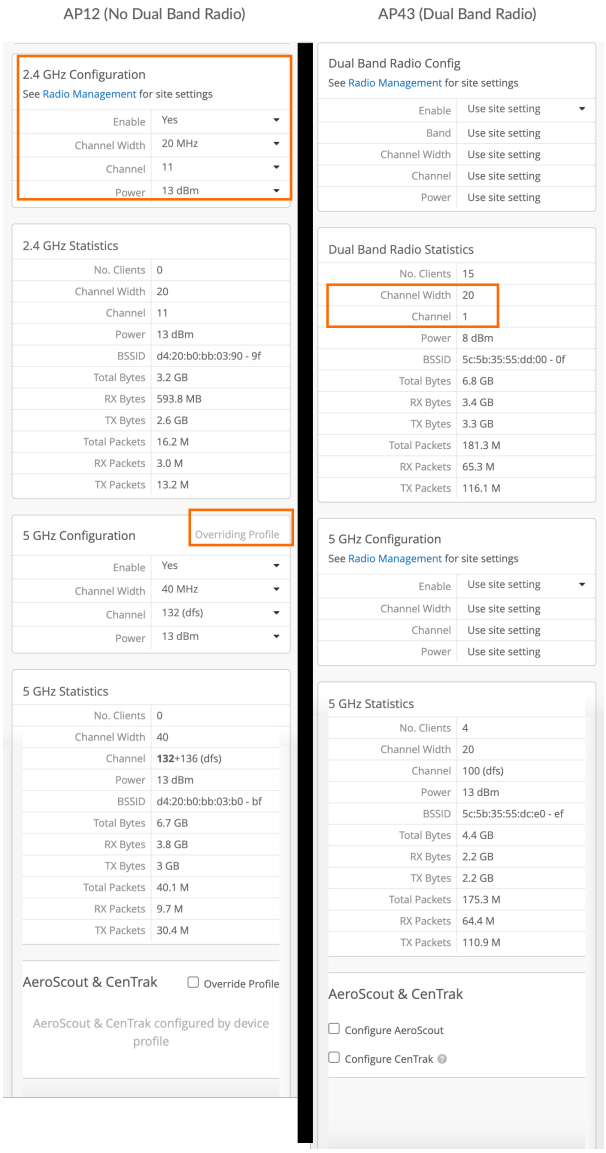
In scenarios where you need to configure RRM options directly on an AP, you can navigate to **Access Points** and click on the name of the AP you want to configure.

You can determine which settings are configured directly on the AP:

- Settings that are inherited from the assigned RF template say "Use site setting."
- Settings that are configured directly on the device have specific values shown.
- Settings that override an applied device profile have specific values shown and contain the text "Overriding Profile."

Figure 4 on page 357 shows the radio settings of two different APs as seen on their AP configuration page.

Figure 37: Direct AP Config - Single Band and Dual Band Radios



The left side shows an AP12 configuration. The AP12 contains 2 single-band radios. Note in the 2.4 GHz band, we have overridden the site (RF Template) settings. In the 5 GHz band on the same AP, we have overridden the Device Profile settings.

The right side shows an AP43 configuration. The AP43 contains a dual-band radio. From these settings, you can see that we use the RF Template settings for the dual-band radio. The Dual Band Radio Statistics shows that the radio is operating in 2.4 GHz mode (20 MHz channel width and using channel 1.) The 5 GHz band is also using RF Template settings. The template specifies 20 MHz channel width to allow for efficient auto conversion if needed.

NOTE: Any RRM settings you configure directly on an AP will override the inherited settings. All other RRM settings will take effect from the inherited options from the RF Template or Device Profile.

Monitor RRM

SUMMARY

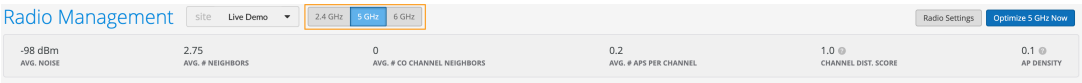
Learn about radio resource management (RRM) monitoring so you can see the effects of RRM on your wireless network.

IN THIS SECTION

What Mist RRM Shows You

In the Juniper Mist GUI, you can see the status of, and interact with RRM by navigating to Site > Radio Management. At the top of the page, the site summary displays statistics about the current RF environment by frequency band. The site summary presents a quick look at the health of RRM for the selected site and radio band.

Figure 38: Radio Management Site Summary



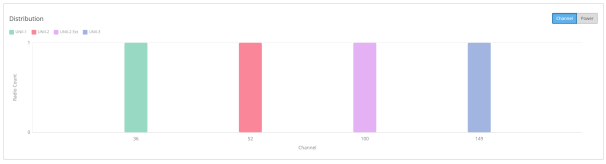
The band selector is highlighted in the image above. The data within the site summary is:

- AVG. NOISE—The average noise floor of all the APs on the selected band. AVG. NOISE, when calculated with the signal strength of a radio on a given channel, gives the signal to noise ratio. Smaller numbers are better for AVG. NOISE.
- AVG. # NEIGHBORS—This is the number of devices (other APs) assigned to the site and within range of a given AP. Higher numbers indicate a denser network. The potential benefits of dense networks are increased routing options in mesh networks and enhanced network connectivity. On of the potential downsides of dense networks is higher power consumption.

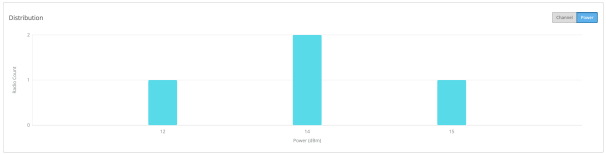
- AVG. # CO-CHANNEL NEIGHBORS—This is the number of neighbor AP radios assigned to the site that are occupying the same channel. Higher numbers here could indicate poor throughput.
- AVG. # APS PER CHANNEL—This is the average number of APs on a given channel. For 2.4 GHz networks where there are fewer channels to choose from, this number tends to be higher. On 5 GHz networks, this number tends to be lower because there are more channels to choose from. The higher the number of APs per channel, the more likely you are to encounter interference in the network, poor throughput, and increased power usage.
- CHANNEL DIST. SCORE—This number refers to the distribution of occupied channels across APs. The number ranges from 0 to 1. 0 (bad) indicates uneven channel distribution with varying numbers of APs occupying each channel. 1 (good) indicates uniform channel distribution with channels occupied by a similar number of APs.
- AP DENSITY—This number indicates how well the APs can hear each other. 0 means no APs can hear each other and 1 means all APs can hear each other. Lower numbers mean decreased potential for interference but increased potential for connectivity gaps, throughput and roaming problems. Higher numbers mean denser, more complete coverage, and better throughput, but may present increased risk of co-channel interference

The **Distribution** block shows the number of radios broadcasting on a given channel or the power settings for those radios on the selected band.

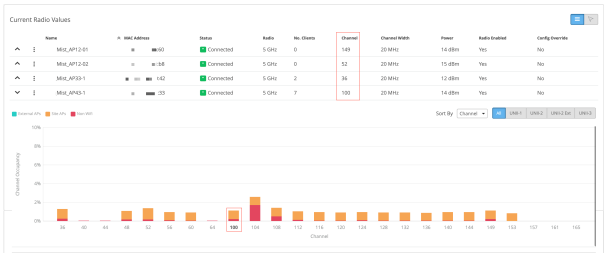
In the image below, we can see that each of four radios are occupying only one 5 GHz channel in this network. If the radio count was higher on any channel, it could be an indication of possible co-channel interference.



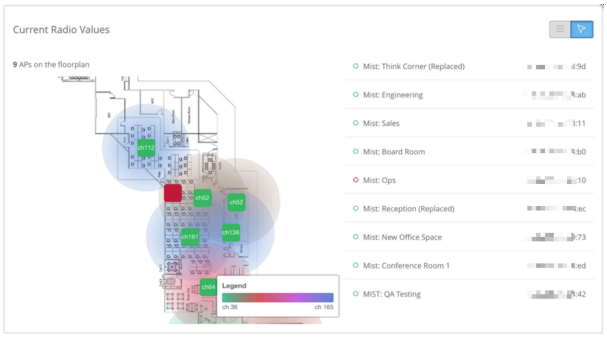
The next image shows the same four AP's power distribution. In this case 2 radios in the 5 GHz band are transmitting at 14 dBm, one at 12 dBm, and one at 15 dBm. In this case, these power settings are automatically controlled by RRM.



The **Current Radio Values** block initially shows a collapsed view of each APs radio settings for the selected band. On the left side, the up-arrow indicates a collapsed view for that particular AP. When the arrow points down, you can see channel occupancy from the perspective of the selected AP. This expanded view shows all the channels available on the selected band. The channel that the selected AP is broadcasting on is shown in bold.

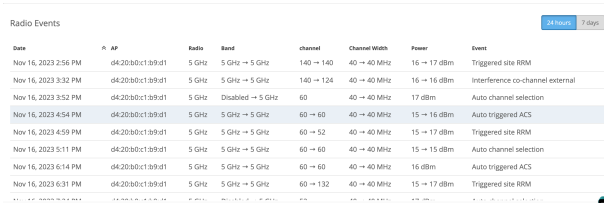


Optionally, you can display the same current radio value information on a location map by clicking the left-pointing arrow at the upper right side of the Current Radio Values block:



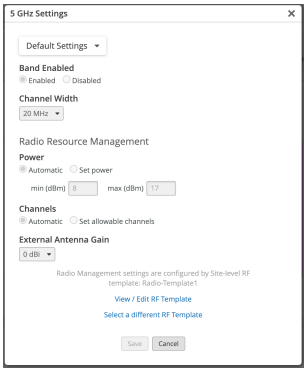
NOTE: You must have your location information, including a map with AP placement, entered into the Mist portal for your site before you can see the location-based radio values information. The location-based radio values image shown above is from the Mist offices and shows a different set of APs than the previous images.

The **Radio Events** block shows you RRM events for the last 24 hours or the last 7 days. Here you can see the channel, bandwidth, and power of your APs as well as what triggered any change. Shown under the Events column, change triggers range from Scheduled site RRM, Triggered site RRM, Radar detected, co-channel interference, etc. The image below shows several radio events in the last 7 days.

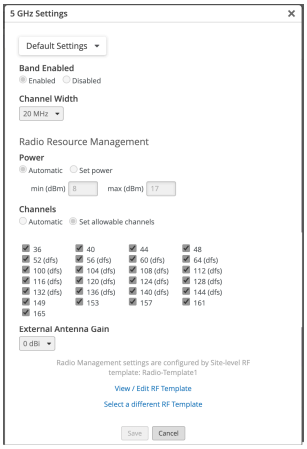


See "RRM Configuration Options" on page 351 for configuration options and hierarchies.

You can see the radio settings for the selected band by clicking the **Radio Management** button at the top right of the page, as shown in the Figure 38 on page 358 image.



At the bottom of the pop-up window, you can see which Site-level RF Template manages band enablement, channel width, power, and channel settings for this site. In this case, Radio Template1 has everything set to auto. This means that RRM is free to manage all of the settings as needed. If any of the template settings were set to manual, you would see different options in the Radio Management settings window:



RRM Usage Examples

IN THIS SECTION

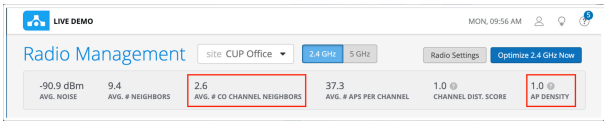
Dual band technology allows a single radio to transmit on either 2.4 or 5-GHz. Mist RRM can turn off surplus 2.4-GHz radios and configure the radio to transmit on 5-GHz instead, which is especially useful for high-density environments. See "Radio Resource Management (RRM)" on page 344.

The following use cases can help illustrate how RRM works.

Carpeted Enterprise

Let's consider a typical, carpeted enterprise, where the goal is to provide 5 GHz WiFi for the high capacity it provides.

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.



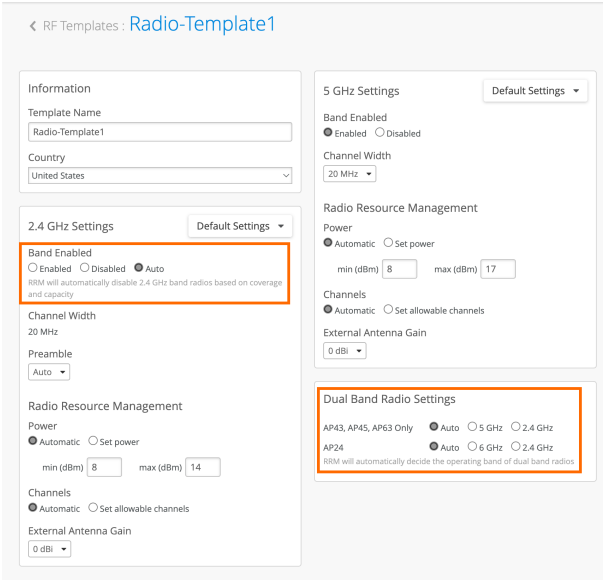
The APs have an average of 2.6 co-channel neighbors, which means that more than 2 neighboring APs are using the same 2.4 GHz channel, which can cause co-channel interference. The AP Density metric is 1.0, which means the APs are uniformly distributed across the site. We can conclude that this site is a great candidate for Mist RRM to auto cancellation or auto conversion.

To enable auto cancellation for the 2.4-GHz radio:

1. In the menu, select **Organization** > **Wireless** > **RF Templates**.
2. Choose an existing template or create a new one using the **Create Template** button.
3. In the 2.4 GHz Settings section, under *Band Enabled*, select **Auto**.

   This enables auto cancellation for all APs in the site.
4. In the Dual Band Radio Settings section select **Auto**.

   This enables auto conversion for dual-band radio equipped APs in the site.



5. Click **Save** to apply your changes.

When you apply this template to a site, RRM will be able to perform both auto cancellation and auto conversion for APs in the site.

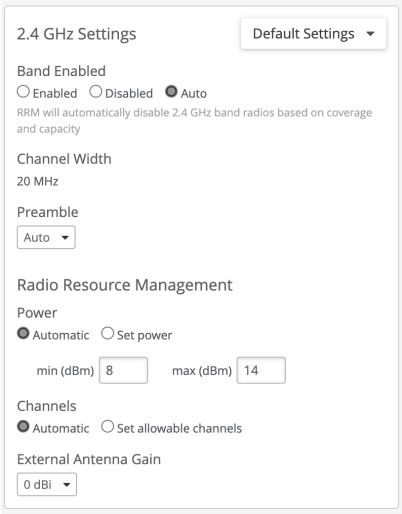
College Dormitories

College dormitories are also a good use case for RRM auto-management. Individual rooms typically have their own AP and are considered the primary means of coverage for residents. Dormitory hallways often use a different AP model with different radio settings and are considered secondary for coverage. Juniper AP12s are common in dorm rooms, 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 RRM to be able to use auto cancellation on the 2.4-GHz radios. And for the dorm rooms, you want to prevent auto cancellation.

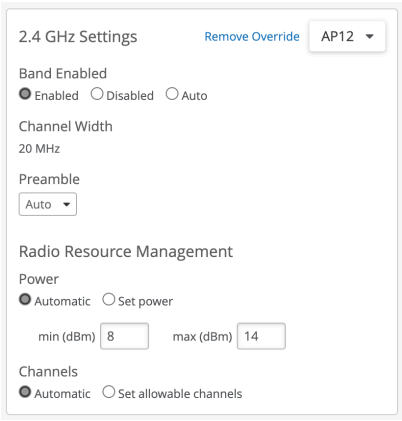
To configure these settings in the same template:

1. In the Mist menu, select **Organization** > **Wireless > RF Templates**.
2. Choose an existing template or create a new one with the **Create Template** button.
3. In the 2.4 GHz Settings section, under Band Enabled, select **Auto**.



4. In the same 2.4 GHz Settings section, click the **Default Settings** pull-down menu and select AP12

.



5. Click **Save** to apply your changes.

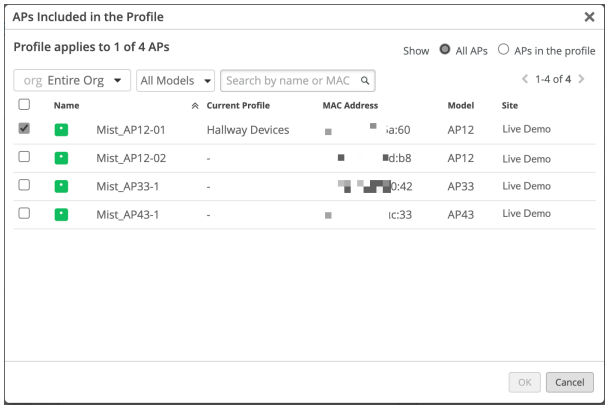
When you set *Band Enabled* to Auto while leaving the **Default Settings** alone, you allow auto cancellation on all APs in the site. When you also set *Band Enabled* to **Enabled** with **Default Settings** set to **AP12**, you prevent auto cancellation on the AP12s in the site.

Conference Rooms and Auditoriums

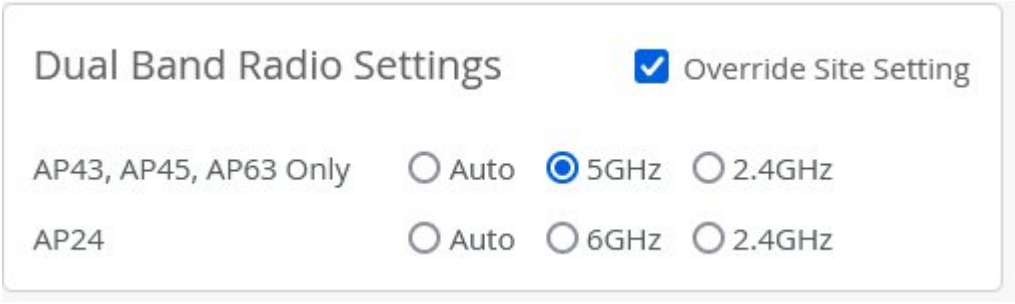
For areas where high client density is expected, you may want to control certain APs explicitly, for example, to enable dual band 5 GHz. For other areas, you may want to broadcast both 2.4-GHz and 5-GHz. You can use device profiles to accomplish both goals.

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 the Access Points link under **Applies To**.
4. In the pop-up window, select the APs on which you want to allow auto conversion. You can select from all APs in the org, site, or by name or MAC address.



5. Click **OK** to close the window.
6. In the *Dual Band Radio Settings* section select **5GHz**.



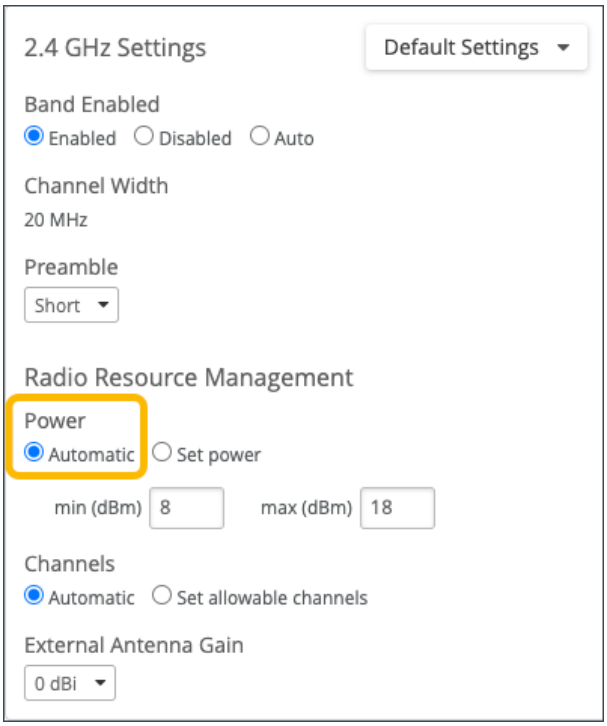
7. Click **Create** to save the Device Profile and apply the settings to the selected APs.

Set Power for all APs in a Site

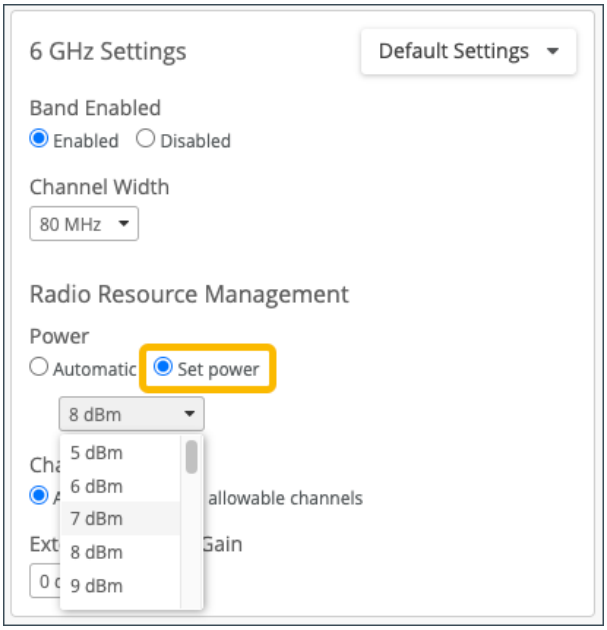
There are use cases where it is necessary to configure a custom power range for your APs. For example, in environments where walls need to be penetrated and max coverage must be ensured. On the other hand, there are environments that a specific power level works well for, and with RRM you can set your APs to that specified power level.

In either case, you could configure power settings under Radio Resource Management at the RF Template level, for example, to apply the power settings to all APs in a site. When you apply the RF Template to a site, RRM will ensure that all APs in the site inherit that power setting.

When the Power setting under **Radio Resource Management** is set to **Automatic** (which is the default), this gives you the option to adjust the minimum and maximum power values to set a custom power range. This can be configured in either the 2.4 GHz, 5 GHz, or 6 GHz Settings sections.



There are also certain environments where it is useful to set the power to a particular level. In this case, you would choose the **Set power** option, then select the power level from the dropdown menu. This can be configured in either the 2.4 GHz, 5 GHz, or 6 GHz Settings sections



Setting the RRM configuration at the RF template level applies the power setting to all APs in the assigned site (unless overridden with a device profile or direct device configuration). As always when configuring RRM, make note of the "Configuration Hierarchy" on page 351.

Also see "RRM Configuration Options" on page 351

Transmit Power Notation for Juniper APs

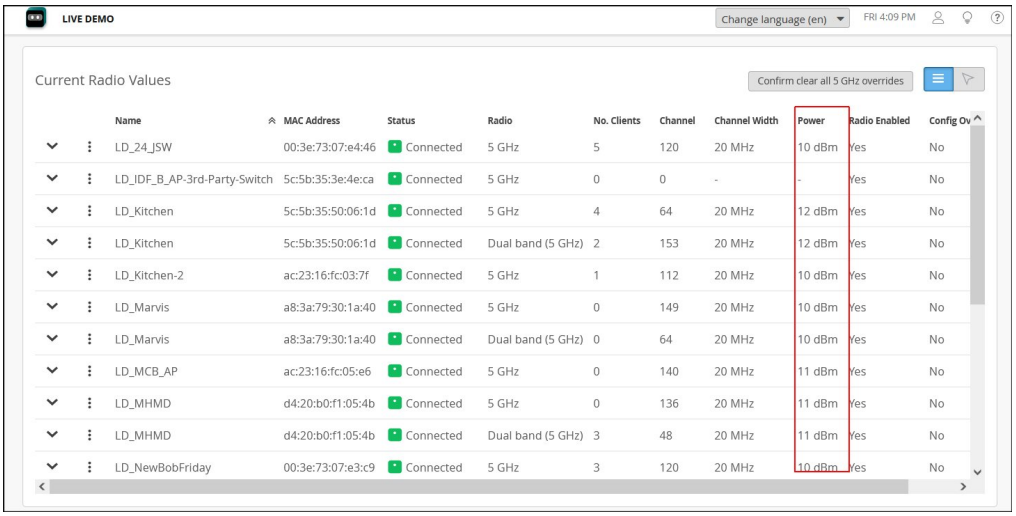
IN THIS SECTION

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 Resource Management (RRM)" on page 344. 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 Juniper Mist, the power values used are for the *total AP transmit power of the entire transmit (Tx) chain*.
- Transmit power for the 6-GHz band 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 transmit power, when using multiple-input multiple-output (MIMO) gains from a wireless design tool, you may need to adjust those values before using them in the Mist portal. Both the reason and the adjustment are explained in the *Working with Wireless Design Tools* section at the end of this topic.

Figure 39: Power Levels in Current Radio Values



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

Table 31: AP Radio Gains

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* = Tx power per chain + 10log (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 + antenna gain - 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 channel width settings, such as 80 MHz, can yield higher EIRP than narrow channel width settings like 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 + 10log (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 32: 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 Wireless Design Tools

Some wireless design tools consider 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 the transmit power from one of those tools to Mist transmit power, you must subtract the MIMO gain.

For example, say that you see a value of **14 dBm** for the simulated transmit power of a Mist AP43. When setting power in the Mist portal, you would set **8 dBm** (14 dBm TPO - 6 dBm MIMO gain.)

In another example, consider two simulated APs, 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 a design tool, 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.

8
CHAPTER

Troubleshooting

SUMMARY

Use the information in this chapter to understand how you can troubleshoot issues on your wireless network.

IN THIS CHAPTER

What Do You Want to Do?

Table 33: Top Tasks

If you want to...	Use these resources:
Explore the various options to troubleshoot your wireless network *Troubleshoot wireless issues using SLEs, Insights, and Marvis.*	"Troubleshooting Wireless Issues" on page 422
Use the status LED to troubleshoot your AP *Understand what the status LED indicates. Learn how to identify issues with your AP using the LED blink patterns.*	"What Does the AP Status LED Indicate?" on page 392
Reset an AP to Factory Default Settings *You might need to do this when the AP is unresponsive or the current configuration fails and the AP cannot connect to the Juniper Mist cloud.*	"Reset an AP to the Factory-Default Configuration" on page 421
Use packet captures to troubleshoot connectivity failures between the client and AP *Identify the cause of failures between the client and AP using dynamic and manual packet captures.*	"Dynamic and Manual Packet Captures" on page 425
Replace an AP *Copy the existing configuration to the new AP through the Mist portal or Mist AI app.*	"Replace an AP" on page 417

Wireless SLEs

SUMMARY

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

IN THIS SECTION

Overview

IN THIS SECTION

Wireless SLEs Video Overview

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

Video: Wireless Service Level Expectations

Finding the Wireless SLEs

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

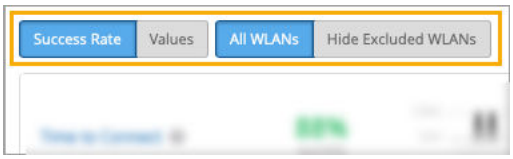
NOTE:

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

SLE Filter Buttons

Filter buttons appear above the SLE blocks.

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



Success Threshold Settings

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

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

Wireless SLEs Video Deep Dive

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

Video: SLE v2

Wireless SLE Blocks

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

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

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

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

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

Table 34: Wireless SLE Descriptions

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
Time to Connect	Time to Connect is the number of seconds that elapse between the point when a client sends an association packet and the moment when the client can successfully move data. You can click the **Settings** button to set the number of seconds to use as the threshold for this SLE.	Authorization	Connection attempts that took significantly longer than the average to pass the authentication state.
		Association	Connection attempts that took significantly longer than the average to pass the association state.
		Internet Services	Connection attempts that took significantly longer than the average to access Internet resources.

Table 34: Wireless SLE Descriptions *(Continued)*

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

Table 34: Wireless SLE Descriptions *(Continued)*

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

Table 34: Wireless SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
Roaming	Juniper Mist tracks the percentage of successful roams between access points and assigns a quality score from 1 to 5. A score of 1 indicates excellent roaming, and a score of 5 indicates poor roaming. You don't need to set this threshold. It's assumed that you want very good to excellent roaming, so this threshold is set to 2 and cannot be changed.	Latency	Excessive roaming time due to latency. Sub-Classifiers: • **Slow 11r Roams**—Fast (802.11r) roaming time exceeding 400 ms • **Slow Standard Roams**—Standard roaming time exceeding 2 seconds • **Slow OKC Roams**—Opportunistic Key Caching (OKC) roaming time exceeding 2 seconds
		Stability	User minutes affected by instability of fast roaming (802.11r). This classifier applies when both the client and the SSID are capable of fast roaming but the client experiences slow roaming for more than 2 seconds. This classifier contains one sub-classifier: **Failed to fast Roam**.

Table 34: Wireless SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions

		Signal Quality	Roaming events affected by weak signal strength
			
			Sub-Classifiers:
			
			• **Interband Roam**—Weak RSSI when clients roam between bands
			
			• **Suboptimal Roam**—Weak RSSI when clients roam to an AP:
			
			  • With more than 6 dBm decrease in RSSI compared to the client's RSSI in the previous AP
			
			  • If the RSSI in the new connection is worse than the configured coverage SLE threshold. Note that the default coverage SLE threshold is 72 dBm.
			
			• **Sticky Client**—Weak RSSI when client remains connected to an AP even when more roaming options are available to improve the RSSI by more than 6 dBm.

Table 34: Wireless SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
Throughput	Juniper Mist calculates the estimated throughput on a per-client basis for the entire site. This calculation is done for every client every minute. The estimator considers effects such as AP bandwidth, load, interference events, the type of wireless device, signal strength, and wired bandwidth, to arrive at the probabilistic throughput. You can click the **Settings** button to set the number of Mbps to use as the success threshold for this SLE.	Network Issues	Low throughput due to the capacity of the wired network
		Coverage	Low throughput due to weak signal strength
		Device Capability	Low throughput due to issues with the device capability. For example, throughput issues can occur if a device only supports 20 MHz wide channels, one spatial stream, or a lower version of Wi-Fi (802.11 g/ 802.11 n).
		Capacity	Low throughput due to either excessive load on the AP or interference on the channel. Sub-Classifiers: • High Bandwidth Utilization • Non Wi-Fi Interference • Excessive Client Load • Wi-Fi Interference
Capacity	Juniper Mist monitors the percentage of the total RF channel capacity that is available to clients.	Non-Wi-Fi Interference	Low capacity due to interference from non-Wi-Fi sources
		Client Usage	Low capacity due to a high client load

Table 34: Wireless SLE Descriptions *(Continued)*

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

Table 34: Wireless SLE Descriptions *(Continued)*

SLEs	SLE Descriptions	Classifiers	Classifier Descriptions
		Ethernet	Ethernet connectivity issues due to one of these issues: • Speed Mismatch—Juniper Mist detected a speed or duplex mismatch between an upstream device and an AP. • Ethernet Errors—Juniper Mist detected cyclic redundancy check (CRC) errors on the Ethernet interface of the AP.
		Network	Network-related issues due to round-trip time, packet loss, and Mist Edge tunnel unreachability. Sub-Classifiers: • Latency • Jitter • Tunnel Down

Using SLEs for Troubleshooting

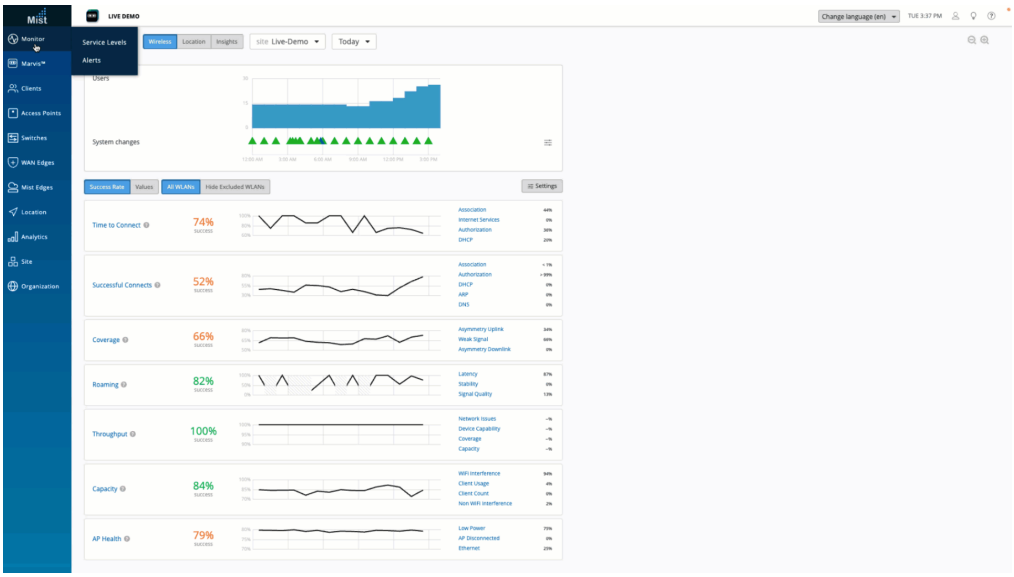
SUMMARY

Learn how to use wireless SLEs to find the root cause of an issue and get details about scope, affected users, and more.

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 40: 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

SUMMARY

Understand the reason codes that are sent when a wireless connection closes, and use these codes to troubleshoot issues.

IN THIS SECTION

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 35: 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

SUMMARY

Get started troubleshooting access point issues with a few basic steps.

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 392.
- 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 399.

For issues related to AP disconnection, see "Troubleshoot AP Disconnection Issues" on page 400.

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?

SUMMARY

Is your Juniper access point (AP) booting? Does it have enough power? Is it having trouble getting an IP address or reaching the proxy server? Correctly interpret the various LED colors and patterns that a Juniper AP uses to indicate its status.

IN THIS SECTION

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
	Blinking red for 3 seconds	The AP is starting to boot.
	Blinking green-off-yellow-off for 12 seconds	The AP is booting.
	Blinking green and yellow for 30–40 seconds	The AP is connecting to the Juniper Mist cloud.
	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
	2 yellow	**No ethernet link**	The AP does not have an Ethernet link. This error is usually seen if you did not connect the AP to a switch when using a power injector.
	3 yellow	**No IP Address**	There is no IP address in the static configuration or through the DHCP lease.
	4 yellow	**No default gateway**	Neither the static configuration nor the DHCP lease has a default gateway.
	5 yellow	**Default gateway unreachable**	The AP does not receive an ARP response from the default gateway.
	6 yellow	**No DNS**	Neither the static configuration nor the DHCP lease has a DNS server.
	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.

(Continued)

LEDs	Blink Pattern	Error	Description
	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 ep-terminator.
	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).

(Continued)

LEDs	Blink Pattern	Error	Description
	2 yellow, pause, 5 yellow	**L2TP mgmt tunnel stopped**	The L2TP management server sent a StopCCN and terminated the tunnel.
	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.
	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 36: 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.
	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.

(Continued)

LEDs	Blink Pattern	Error	Description
	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.
	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: AP Status LED Video Demo

Troubleshoot AP Claiming Issues

SUMMARY

Understand and resolve the error messages that can appear when you're trying to claim an access point (AP) into your organization.

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 37 on page 401 lists the LED behavior for some of the common issues that cause an AP to disconnect from the network.

IN THIS SECTION

Table 37: Troubleshoot AP Disconnection Issues

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
○	Off	The AP is not receiving power.	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. **NOTE**: If your APs are already installed and you cannot swap any AP, skip this step.

Table 37: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
	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.	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/test and see if it resolves the host. Your output should look like this: `Welcome to MIST` 3. Check the firewall logs to see whether any policy is blocking access.

Table 37: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
	Blinking yellow two times	The switch or AP is experiencing a Layer 2 issue.	1. Run a cable test to verify that the cable connected to the AP is working correctly. 2. Check whether the switch port connected to the AP learns the MAC address of the AP. 3. Check for any eth0 errors on the switch port. 4. Change the cable and switch port and verify that the AP powers on. 5. If you have a working AP, swap it with the faulty AP. Check whether the issue persists. **NOTE**: If your APs are already installed and you cannot swap any AP, skip this step.

Table 37: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
	Blinking yellow three times	The AP is unable to obtain an IP address.	The AP can obtain an IP address either through DHCP or through a static configuration. Troubleshooting steps for DHCP: 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. • 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 37: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
			DHCP Discover, Offer, Request, Acknowledgment (DORA) process is failing. • 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. Troubleshooting steps for static configuration: 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: 1. 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. 2. Correct the configuration on the switch port.

Table 37: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
			3. Reset the AP to the factory-default configuration. See "Reset an AP to the Factory-Default Configuration" on page 421. 4. Power on the AP.

Table 37: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
	Blinking yellow four times	No default gateway IP address found in the DHCP lease or static configuration.	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: 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 AP to the Factory-Default Configuration" on page 421. d. Power on the AP.

Table 37: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
			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. • 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 37: 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.	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: 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 AP to the

Table 37: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
			Factory-Default Configuration" on page 421. **d.** Power on the AP. If the configuration is correct and the LED still blinks yellow five times, follow these steps: **a.** Connect a laptop on the same VLAN, network, or switch port to which the AP was connected. **b.** Ping the default gateway. Use the `ipconfig /all` command to get the default gateway information. If the ping fails, contact your network administrator to check for issues on the wired side. If the ping succeeds but the AP still fails to connect, contact Juniper Mist support.

Table 37: 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.	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. If the DNS server is not configured correctly, follow these steps: 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 AP to the Factory-Default Configuration" on page 421. d. Power on the AP.

Table 37: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot
			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. • 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 37: Troubleshoot AP Disconnection Issues *(Continued)*

LED Color	Blink Pattern	Issue	Steps to Troubleshoot

	Blinking yellow seven times	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.	• Connect a laptop on the same VLAN or network, and try to resolve the URL `ep-terminator.mistsys.net` to an IP address by executing the `nslookup` command at the command prompt.
			
			`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`
			
			• If the `nslookup` 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 37: 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?

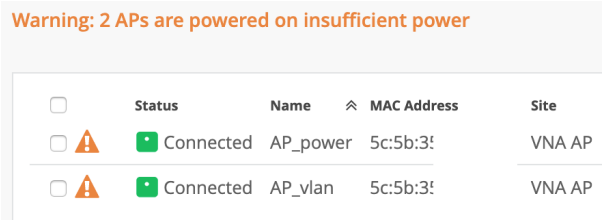
NOTE: If you select the **Allow Mist Support Team to access your Mist Organization** option on the Support Access tile in Organization Settings (**Organization** > **Settings**), the Mist support personnel can see all the device information available through the Mist portal.

Troubleshoot Insufficient Power for an AP

SUMMARY

Follow this procedure if you see an indication that an access point (AP) is not getting enough power.

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:



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 APs" on page 26 for information about the PoE requirements for each AP model.

Troubleshoot AP Reboots

SUMMARY

Resolve various issues that can cause an access point (AP) to reboot.

IN THIS SECTION

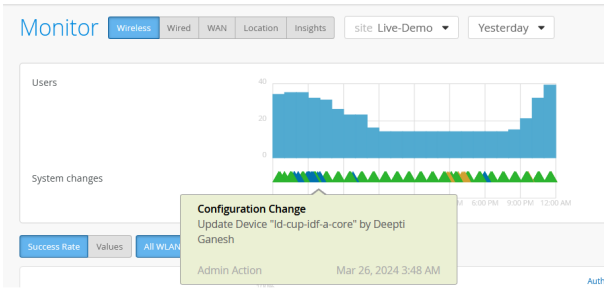
An access point (AP) can reboot owing to various reasons such as configuration changes, power outages, and firmware updates. Here are some of the possible reasons for an AP reboot and troubleshooting steps where applicable.

- 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.

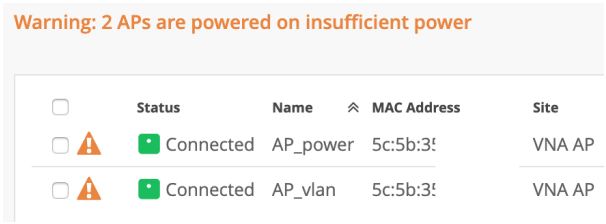
- AP reboot initiated manually.

  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.



  Ensure that you enabled LLDP on your switch or assign the required power to the AP. For more information, see "Troubleshoot Insufficient Power for an AP" on page 415.

- 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 an AP" on page 415.

  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 AP

SUMMARY

Follow this procedure if you need to replace an access point (AP).

IN THIS SECTION

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**.

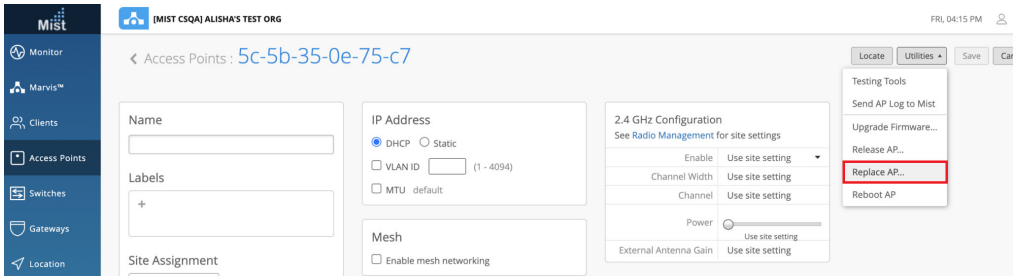
Before you begin, ensure that the new AP is in the **Unassigned** state. You should claim the AP on your organization but should not assign it to any site. You can use either the Juniper Mist portal or the Juniper Mist AI™ AI mobile application to replace an AP.

Replace an AP Using the Juniper Mist Portal

To replace an AP through the Juniper Mist portal:

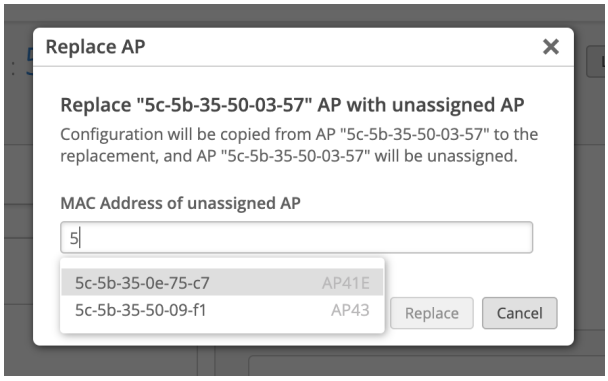
1. Select **Access Points** from the left menu of the Juniper Mist portal. The Access Points page appears.
2. Click the AP that you want to replace.

   The AP settings page appears.
3. Select **Replace AP** from the **Utilities** menu in the top-right corner of the page.

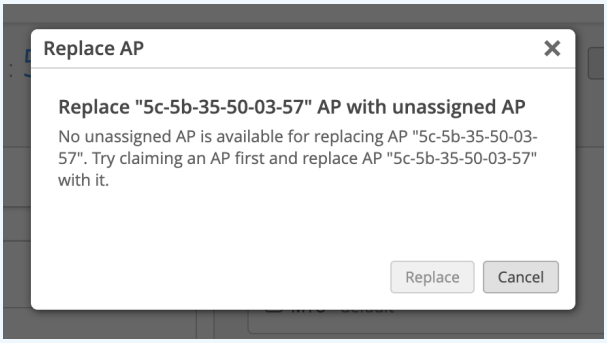


4. Enter the MAC address of the unassigned AP with which you want to replace the existing AP.

   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.

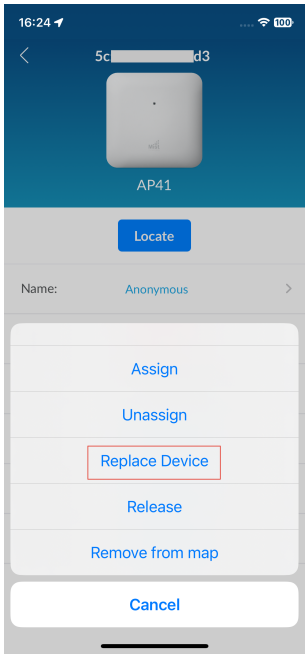
Replace an AP Using the Juniper Mist AI Mobile Application

To replace an AP using the Juniper Mist AI mobile application:

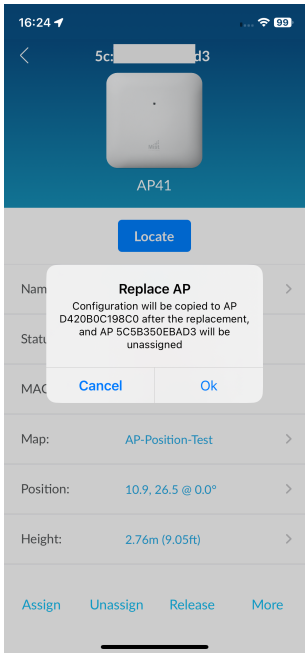
1. Open the Juniper Mist AI application on your mobile phone and log in with your account credentials.
2. Select your organization.
3. Tap **Device Inventory > Access Points**.
4. Tap the AP that you want to replace.

   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 AP to the Factory-Default Configuration

SUMMARY

Follow this procedure if you need to revert an access point (AP) to its factory-default settings.

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

SUMMARY

Follow these guidelines to improve the performance of your wireless network.

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 384 and "View Roaming History" on page 162.

You can also use AP insights to see channel utilization, which should always be less than 50%.

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.
- Make sure you are using RRM on the APs. This will ensure that both power and channel usage are optimized at all times.
- 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 235. For the steps to create a WLAN, see "Adding a WLAN" on page 234.
- 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 159.
- Disable band-steering and force the clients to choose a radio band (5 GHz or 2.4 GHz).

Common Wi-Fi Issues

SUMMARY

Learn more about Wi-Fi issues caused by interference, channel changes, and client load.

Interference

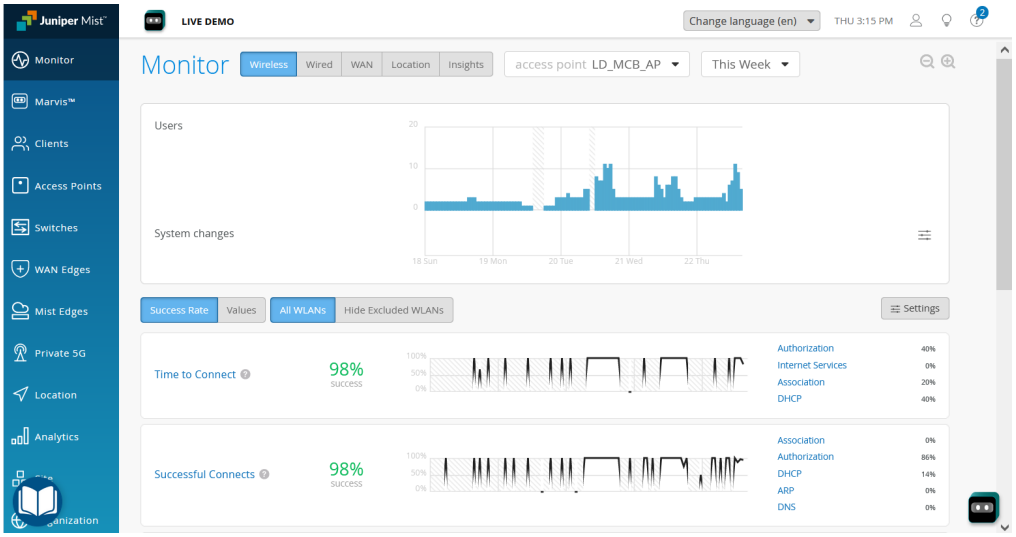
Interference can result in slower network speeds and client disconnections. This can be caused by various wireless signals and devices. For example, any Wi-Fi networks nearby, microwave ovens, or Bluetooth devices could disrupt or weaken your Wi-Fi signals. The most common types of interference are:

- 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.

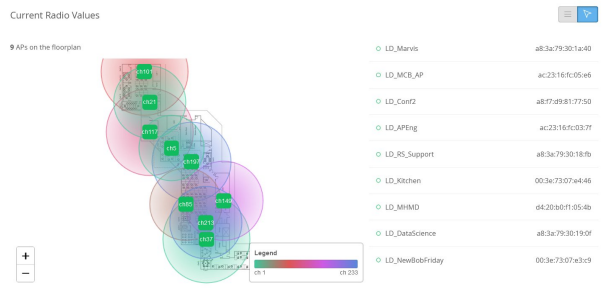
You can view these by clicking **Monitor > Service Levels | Insights** in the main menu, selecting the time period and AP you want, and then scrolling down the page to **Channels** (see Figure 41 on page 424).

Figure 41: 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 42 on page 424).

Figure 42: Floor plan view of Current Radio Values.

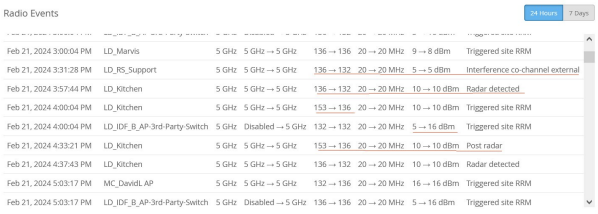


Channel Changes

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 43 on page 425).

Figure 43: Radio Events showing channel changes.



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

When investigating communication failures between the client and the access point (AP), you can use the Juniper Mist™ portal to get dynamic and manual packet captures.

IN THIS SECTION

NOTE: Mist does not collect or store any payload data from packets capture. Only transmission and connection data are used.

Dynamic Packet Captures

IN THIS SECTION

Which Events Trigger Dynamic Packet Captures?

Whenever a connection failure occurs between the wireless client and an AP (AP), it automatically triggers a short-term dynamic packet capture.

These events include:

- DHCP Timeout—When the client sends a broadcast discover packet but does not receive an offer packet from server.
- DHCP Denied—When the server sends a DHCP NAK, indicating that the IP address might already be in use.
- DHCP Terminated—When the Client does not proceed with DHCP request for the offer provided by the server.
- Authorization Failure—This type of failure could be caused due to various reasons. Examples include MIC failure, RADIUS server not responding, Access-Reject from RADIUS server, client failing to complete the auth process, and so on.
- 11r FBT Failure—This type of failure is caused due to client failing 11r roam.
- OKC Auth Failure—This type of failure is caused due to client failing OKC roam.
- Association Failure—This type of failure could be caused due to transmission failures or an invalid PMKID included by the client during association request.

Finding the Packet Captures

Dynamic packet captures are saved to the cloud. You can download these files from the Insights page.

Video Demo

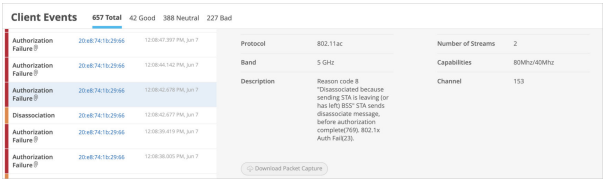
Video: NOW in 60: WAN Assurance - Dynamic Packet Capture

Example

This example shows how easily you can find dynamic packet captures on the Insights page.

1. From the left menu, select **Monitor** > **Service Levels**.
2. Click the **Insights** button to view the Insights page.
3. Scroll down to the **Client Events** section.

   Paperclip icons indicate the events with dynamic packet captures.
4. Click an event to see more details on the right side of the screen.
5. Below the details, click **Download Packet Capture**.



Manual Packet Captures

For manual packet captures, go to **Site** > **Packet Captures**, where you can:

- Choose which network type to capture packets from: wired, wireless, or WAN.

  NOTE: Wired packet capture applies to the wired ports of APs (not the switch ports). The switch must be running a CloudX version of Junos for it to appear in the **Add Switch +** selection window. WAN packet captures support Session Smart Router and SRX WAN edge device ports.

- 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 38 on page 430 for details.

After downloading the packet capture to your computer, follow the steps below to view the data in Wireshark.

Configure IEEE 802.11 on Wireshark

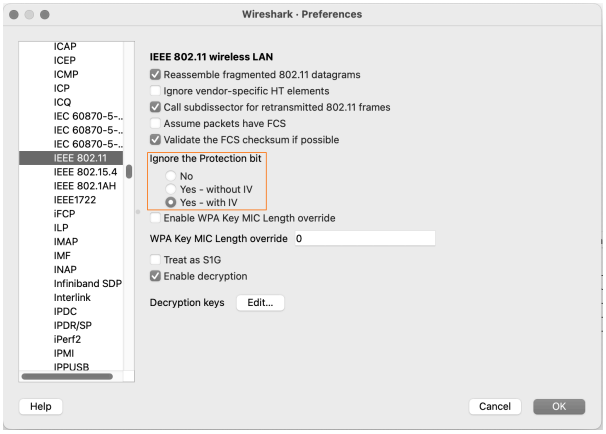
Packet inspection requires Wireshark. See https://www.wireshark.org for the download file and related information.

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 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.

   Wireshark adds a new line called New Column, and the type Number.

   Radiotap headers include wireless packet frames that would otherwise not be displayed. See: https://www.wireshark.org/docs/dfref/r/radiotap.html.

   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 38: Packet Capture Options

Option Name	Option Function	Usage Notes	Firmware Notes
Include Network Headers	This feature includes packet headers with the packet data.	Packet capture works by buffering packets locally on the device, which has limited space available. By default, Mist truncates header data from the captured packets to reduce the size of capture files while still providing the most relevant information.	–
Local Capture	This capture is local only and is not streamed to the Mist portal.	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	These filters are based on the type of packet capture that 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	Use this option to apply your own filters by using `tcpdump` syntax.		0.10.x or later
Expression Builder	This interactive tool builds 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

SUMMARY

To improve the user experience, steer clients to the faster 5-GHz radio band.

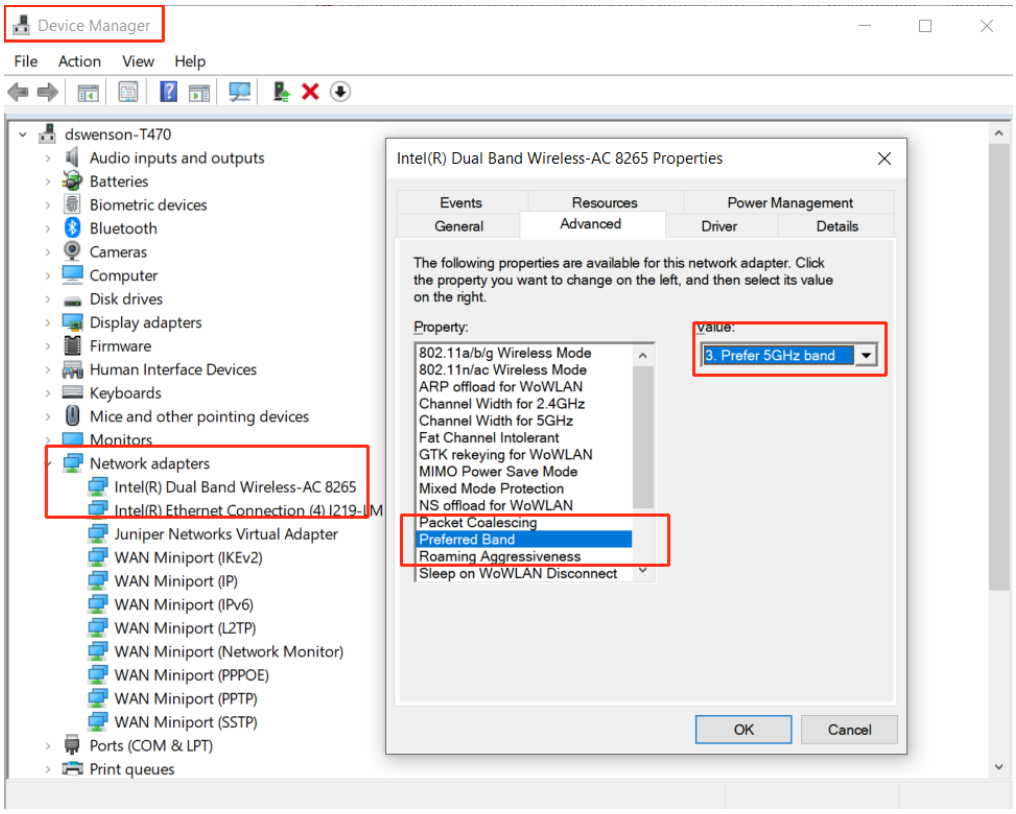
In the Juniper Mist portal, you can see which band your clients are using by clicking **Clients > WiFi Clients** in the menu.

Most Juniper APs support dual band radio setting, which means they can provide client connections on both 2.4 GHz and 5 GHz radio bands... 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 44: 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

SUMMARY

Reduce the overhead traffic on your WLAN by using Bluetooth® Low Energy (BTLE) rather than Bonjour services to support plug-and-play 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 device 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 can 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 248.

LLDP-MED Power Negotiation

SUMMARY

Get familiar with the power negotiation options available in Juniper Mist™.

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

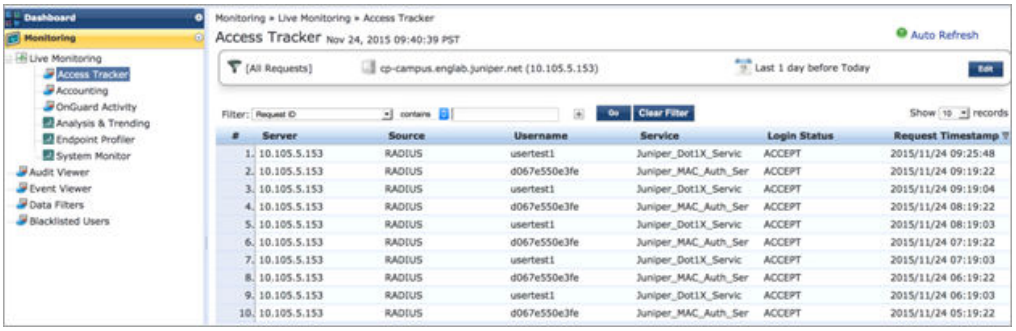
NOTE: This topic provides some tips for troubleshooting in ClearPass. For up-to-date information about ClearPass, see the ClearPass support site.

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 438 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.

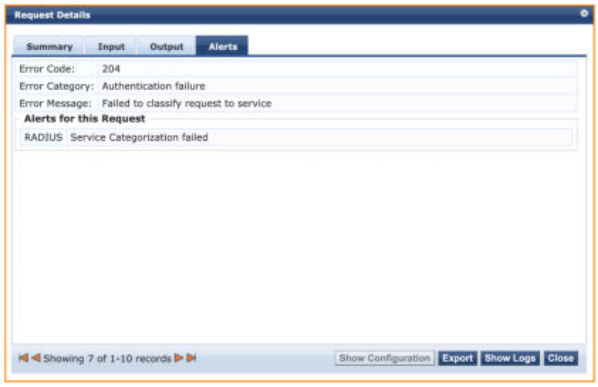


For help with various reject reasons, see the "Reject Reasons" on page 435 section of this topic.

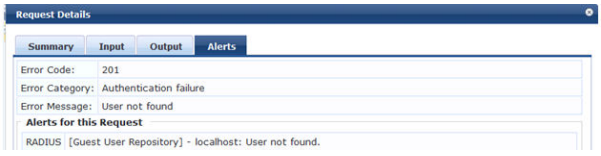
Reject Reasons

The possible reasons for a reject are:

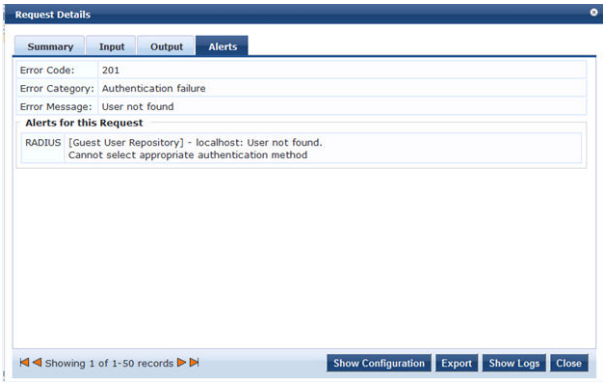
- Service categorization failed—The incoming request on the ClearPass is not categorized under any service that is configured for the SSID that the user is trying to connect to. Make necessary corrections in the service rules under **Configuration** > **Services** > Select the configured service.



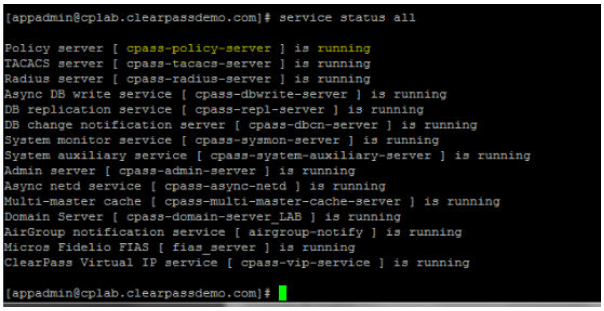
- User not found—This error means that the user is not listed in the configured Authentication Source in the service. See if the appropriate source (Static Host lists, Local User Repository, Guest User Repository, Endpoints Repository, or Active Directory) is added in the service.



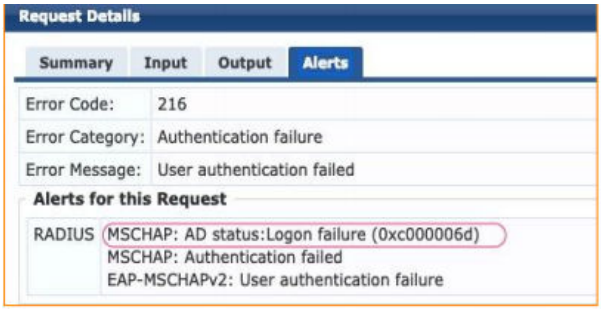
- Cannot select appropriate authentication method—This error appears when the wrong authentication method is added in the service. For MAC authentication, the method should be either [MAC AUTH] or [ALLOW ALL MAC AUTH]. For dot1x, it should be [EAP PEAP], [MSCHAPv2] when username and password are used, [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.



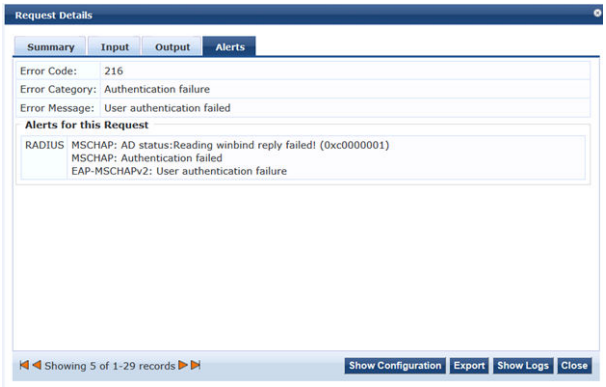
- Cannot send request to policy server—This error appears if the policy service is not running on the server. To check the status, go to the CLI and enter the command `service status all`.



- Logon failure—This error means that the user provided an incorrect password.



- Reading winbind reply failed.



This error can be due to two different reasons:

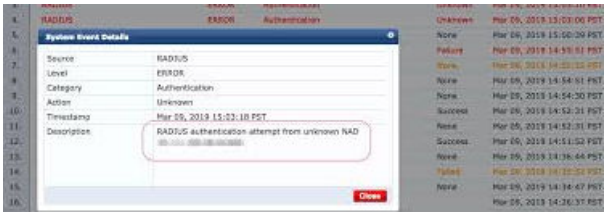
- ClearPass is not added to the AD Domain. Go to **Administration** > **Server Manager** > **Server Configuration**, and then select the server.

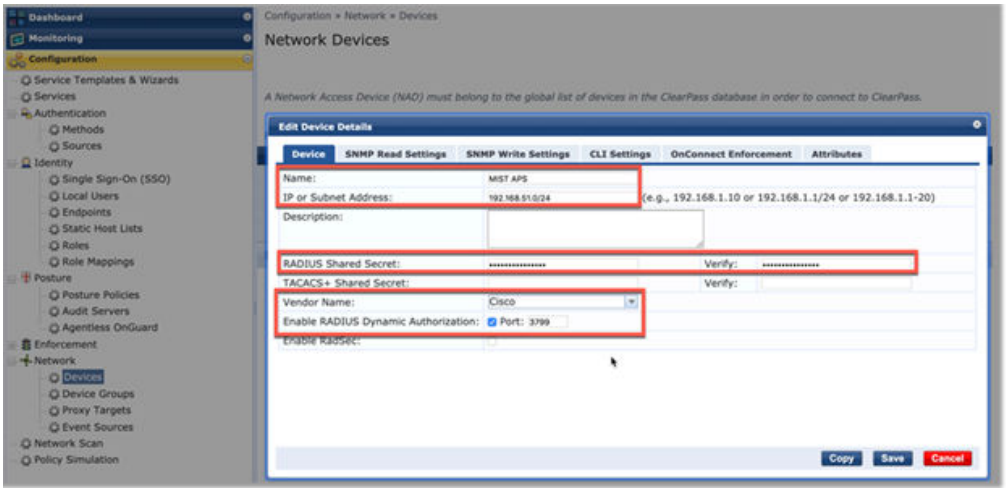
- There is a delay in the response from the AD. This can be verified by clicking the **Show Logs** button on the Access Tracker request. The delay should be less than 500 ms. Check on the AD side to see why there is a delay in sending the response.

Event Viewer: NAD and Shared Secret Errors

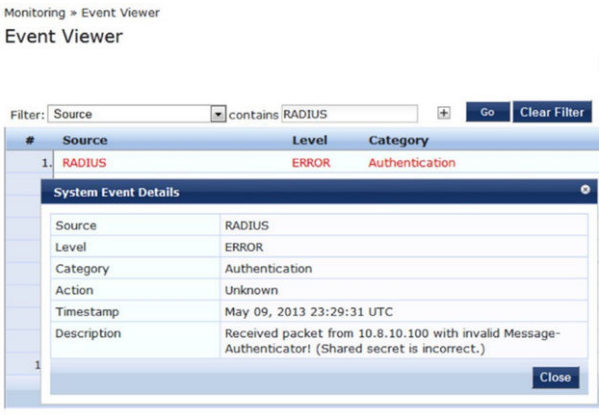
If there is no request in the Access Tracker for the MAC or username, navigate to the Event Viewer and look for any events in the Authentication category. If so, open the errors and investigate further.

- 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.



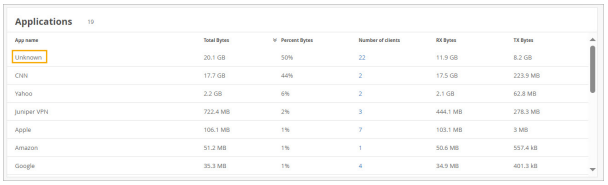
If there are no events in the Event Viewer, check the reachability from the AP to the RADIUS server.

Use Labels to Identify "Unknown" Applications

SUMMARY

One beneficial use of labels is to identify the applications that Juniper Mist is unable to categorize automatically. This way, when you look at the Applications page, you'll see fewer Unknown items and will gain more insight from the data.

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.



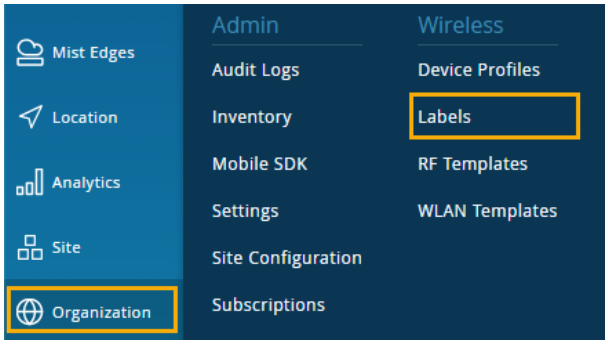
NOTE: To see the complete list of pre-defned applications, go to /api/v1/sites/:site_id/wxtags/apps

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:

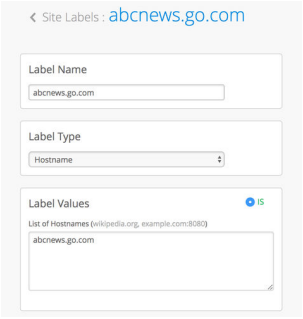
1. Navigate to the Labels page for your organization or site:
   - For organization-level labels, select **Organization** > **Wireless | Labels** from the left menu of the Juniper Mist portal.



- 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.



4. Click **Create**, near the top-right corner of the New Label page.

9
CHAPTER

Technology Reference

IN THIS CHAPTER

Antenna Gains per AP Model

SUMMARY

To choose the right Juniper access points (APs) for your needs, compare antenna gain values for various models.

IN THIS SECTION

Mist AP Antennas

The tables below show the maximum gain for which the Juniper Mist AP, or the AP plus an external antenna, is certified. Note, though, that the maximum *allowable* gain will vary according to the regulatory domain in which the AP is operating. As such, when configuring the gain settings for a given AP, you need to be sure not to exceed the maximum allowed by local regulations.

Take the case of an AP43E with an external directional antenna, for example. The AP supports a gain of up to 8 dBi on the 2.4 GHz radio band, and up to 10 dBi on the 5 GHz radio band. This level of gain will exceed the maximum allowed for some regulatory domains. Thus, although the AP hardware supports it, and you can configure a 10 dBi gain in the software, a setting of 10 dBi would be mistake if your local regulations do not allow it.

Table 39: Indoor Antenna Gains

Model	Antenna Type	2.4 GHz	5 GHz	6 GHz
AP12	Omni	2dBi	5dBi	~
AP21	Omni	3dBi	5dBi	~
AP24	Omni	3dBi	5dBi	5dBi
AP32	Omni	5dBi	6dBi	~
AP33	Omni	5dBi	6dBi	~

Table 39: Indoor Antenna Gains *(Continued)*

Model	Antenna Type	2.4 GHz	5 GHz	6 GHz
AP34	Omni	4dBi	6dBi	6dBi
AP41	Omni	4dBi	5dBi	~
AP43	Omni	4dBi	6dBi	~
AP45	Omni	3dBi	5dBi	5dBi
AP47	Omni	4dBi	6dBi	6dBi
AP47D	Directional	6dBi	8dBi	8dBi
AP61	Omni	4dBi	5dBi	~
AP63	Omni	4dBi	6dBi	~
AP64	Omni	3dBi	5dBi	5dBi

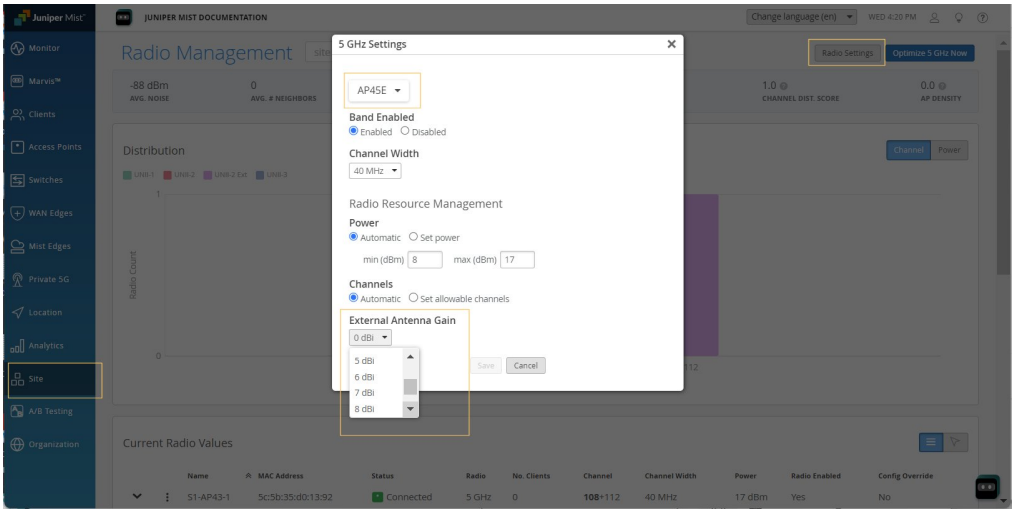
Table 40: Outdoor Antenna Gains

Model	Antenna Type	2.4 GHz	5 GHz	6 GHz
AP47E	Directional	8dBi	10dBi	10dBi
AP45E	Omni Directional	4dBi 8dBi	6dBi 10dBi	6dBi 10dBi
AP43E	Directional	8dBi	10dBi	~
AP41E	Directional	8dBi	8dBi	~

Table 40: Outdoor Antenna Gains *(Continued)*

Model	Antenna Type	2.4 GHz	5 GHz	6 GHz
AP63E	Directional	8dBi	10dBi	~
AP61E	Directional	8dBi	8dBi	~

Figure 45: Configuring Antenna Gain



When configuring a gain of 6 dBi or higher for an external antenna, we recommend that you make the setting in the RF Template, a device profile, or at the level of the individual AP. An example configuration from the **Radio Settings** page (site-level) is shown in Figure 1. Note that the **External Antenna Gain** option does not appear for internal APs.

Wireless Network Design Tutorial

SUMMARY

Get guidance about best practices for designing your wireless network.

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 7

IN THIS SECTION

Deploy Wi-Fi 7 with AP47

SUMMARY

Explore the features and benefits of Wi-Fi 7. Learn about deploying Wi-Fi 7 in your network using the Juniper AP47.

IN THIS SECTION

AP47 Access Point Overview

IN THIS SECTION

The Juniper® AP47 High Performance Access Point is an indoor Wi-Fi 7 access point (AP) that provides virtual Bluetooth® Low Energy (vBLE) for enterprises that require increased channel width and capacity.

The AP47 has three IEEE 802.11be data radios, which deliver up to 4x4 multiple input, multiple output (MIMO) with four spatial streams. The AP47 also has a fourth 802.11be radio that is dedicated for scanning. The AP uses this radio for radio resource management (RRM), wireless security, and analytics.

The AP47 has a vBLE antenna array to enable location services such as asset visibility, wayfinding, and other services without battery-powered beacons. The AP47 includes two 802.15.4 capable radios, a built-in Global Navigation Satellite System/Global Positioning System (GNSS/GPS) radio, as well as Ultra-Wideband (UWB) capabilities.

The AP can operate simultaneously in the 2.4-GHz, 5-GHz, and 6-GHz bands. The AP is backward compatible with the 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax wireless standards.

AP47 Access Point Models

Table 41: AP47 Access Point Models

Model	Antenna
AP47	Internal omnidirectional

Table 41: AP47 Access Point Models *(Continued)*

Model	Antenna
AP47D	Internal directional (60x60)
AP47E	External

Figure 46: Front and Rear View of AP47 and AP47D

Figure 47: Rear View of AP47E

Key Features of AP47 Access Points

- Wi-Fi 7 support—The AP47 supports Wi-Fi 7, which allows for higher throughput and lower interference. Wi-Fi 7 can support 320 MHz wide radio channels in the 6GHz band and offers 4K QAM.
- Dual Ethernet—The AP47 can connect to two Ethernet inputs at the same time, allowing for PoE redundancy and Ethernet failover.
- Three models - AP47, AP47D, AP47E.

- Dual 5 GHz or Dual 6 GHz support.
- Dedicated scan radio.
- U-NII-4 channel support.
- Virtual Bluetooth Low Energy (vBLE) and Ultra-wideband (UWB) technologies for enhanced location use cases.
- Dual 802.15.4-capable, multi-personality IoT radios.
- Multiple sensors including pressure, accelerometer, temperature, and GPS.

For AP47 specifications, see the AP47 Datasheet.

Choose Between AP47, AP47D, and AP47E

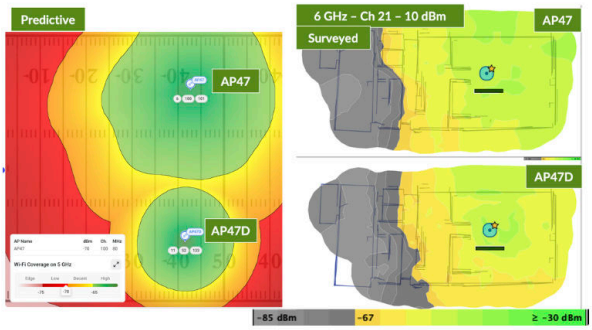
SUMMARY

Learn the differences between the different AP47 models to help you choose the best model for your deployment.

Juniper Networks offers three versions of the AP47:

- The AP47 has traditional integrated omnidirectional antennas. It is the general usage AP in the lineup. It is used for general to high-density deployments for coverage in open areas such as conference rooms, open office spaces, retail spaces, etc.
- The AP47D has 60x60° integrated directional antennas and is meant to be used in everyday deployments where you are looking for higher capacity. In many environments, AP47D can be used instead of AP47 to support higher AP density. For example in carpeted enterprise, education, or any environment where you are running into co-channel contention issues on 5 or 6 GHz due to the density of APs. AP47D provides better signal control and the capacity benefits of directional antennas without the added overhead of external antennas. AP47D is also a great fit for auditoriums, lecture halls or other high density environments that would benefit from a 60x60 pattern.
- The AP47E allows for the use of external antennas and complete customization of the AP's coverage pattern. It is suited for deployment in very high density areas where the direction of the signal needs to be controlled using different types of antennas or you where you may need a different coverage pattern than the 60x60. For example, in large public venues with a high density patch, or high racking warehousing through a warehouse style antenna. The AP47E uses the 14 lead antennas with three pluggable connectors (MPC). Because the AP47E has dual 5 and dual 6 GHz capability, it uses different external antennas than the AP45E.

Figure 48: Comparing the Coverage of AP47 and AP47D



Power Options for the AP47

The AP47 has dual 10 GbE multigigabit Ethernet ports, both of which support power over Ethernet (PoE) in.

The AP47 requires 802.3bt power (Class 6 - 60W) for full functionality. It requires approximately 29 Watts of power at the powered device (PD) for full Wi-Fi functionality. When powered by 802.3at power, the AP operates with reduced functionality. The three Wi-Fi radios operate at 2x2:2, or 4x4:4 with any two Wi-Fi radios enabled. The AP47 keeps the scanning radio, and the BLE, GPS, and UWB radios active at all times, regardless of the power source.

Either or both of the ports can be used to power the AP using PoE. You can see the functionality differences below:

- **802.3bt Power Source**
  - Single 802.3bt in – Full functionality
  - Dual 802.3bt in – Full functionality
- **802.3.at Power Source**

- Single 802.3at in – Reduced Wi-Fi functionality – Three 2x2 or Two 4x4
- Dual 802.3at in – Full functionality

- **Mixed Power Source**
  - One 802.3bt in and one 802.3at in – Full functionality

NOTE: NOTE: When two 802.3bt sources power the AP, the device supports full Ethernet and PoE redundancy. When two 802.3at sources power the AP, a power-sharing configuration is created, where the AP merges power from both ports to ensure full functionality.

In the power-sharing configuration, the AP maintains full Ethernet redundancy; however, it may experience a brownout or reboot if one power source fails. Internal testing has proven that brownouts or reboots are rare occurrences. To ensure maximum redundancy, use 802.3bt power sources.

Ensure you use 802.3bt or 802.3at compliant PoE switches or injectors to power the AP47.

See PoE Requirements for Juniper Mist APs for AP47 power requirements.

Ethernet Redundancy and Connecting the AP47 to the Network

The two 10 Gbps Ethernet ports on the AP47 not only provide PoE redundancy but also support redundant Ethernet links to ensure continued operation during infrastructure outages or upgrades in mission critical environments. The AP47 supports single uplink, dual uplink, individual uplink and downlink, and dual downlink connectivity.

Single Uplink

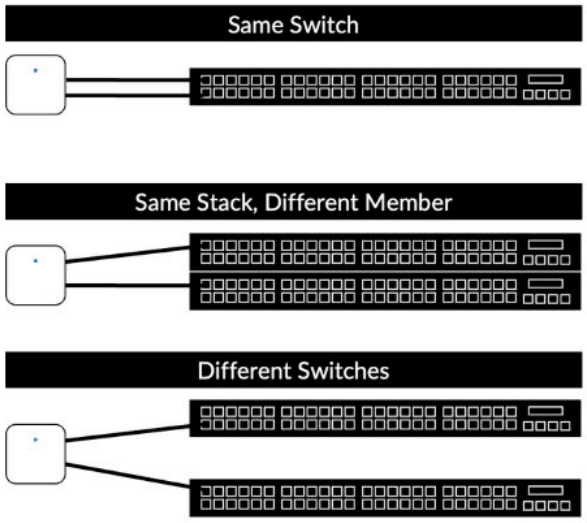
For single uplink we recommend that you connect Eth0 to the network uplink for simplicity and consistency. However, there is no restriction on using Eth1 to connect to the network uplink on an AP47.

If you enforce a MAC limit on your AP switch ports, such as when you tunnel traffic to a Mist Edge, you must configure the MAC limit to two or more.

Dual Uplink

If you leverage dual uplinks, here are a few good things to know:

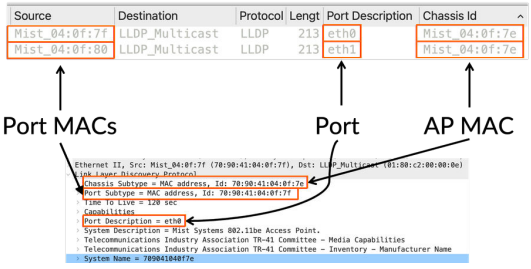
- Connecting the AP47 to the network requires no switch configuration. You can connect the AP to the same switch or different switches. Ensure the L2 VLAN is the same on both switch ports so clients don’t need to obtain new IP addresses if a failover occurs.



- New AP47s arrive configured with dual uplinks in an active-standby configuration.
  - You can configure uplink, downlink and dual downlink (mesh relay) connectivity by manually configuring the port VLANs in the Mist portal.
- The AP47 employs passive failover detection based on link status and activity which results in three to five-second failover.
- The AP47 is capable of non-traffic-impacting (hitless) PoE failover when you use dual 802.3bt power sources.
- If you use two 802.3at or mixed 802.3at and 802.3bt power sources, the AP47 combines the received power for full functionality. The AP may brownout or reboot in the event it needs to reduce functionality due to a single power source failure.

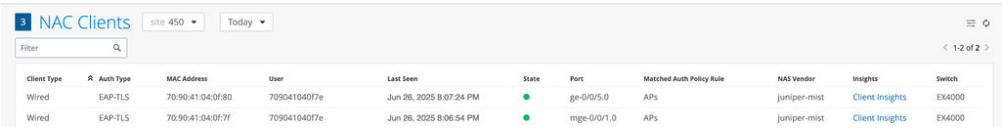
AP47 Ethernet MAC Addresses

AP47 LLDP PCAP



- The AP47 uses three MAC addresses for Ethernet, because it supports multiple uplinks. The MAC address for the AP wireless interface is known as the AP MAC address, then each Ethernet port MAC address is incremented by 1. For example:
  - AP MAC Address = 70:90:41:XX:XX:7E

  - AP Eth0 MAC Address = 70:90:41:XX:XX:7F
  - AP Eth1 MAC Address = 70:90:41:XX:XX:80
- The AP47 uses the AP MAC address for switch virtual interfaces (SVIs) and IP communication, such as DHCP, ARP, DNS, NTP, AP Management, L2TPv3, and RADIUS.
- The AP47 uses the unique Ethernet port MACs for link-local packets, such as LLDP and Dot1x Supplicant.
- Connected switches use the AP47's multiple MAC addresses primarily when you configure switch-side MAC-based policies. For example:
  - To perform MAC authentication bypass (MAB) authentication against the APs, add both the AP MAC address and the port MAC addresses to your switch's MAB database,
  - If you leverage LLDP, the Chassis ID is the AP MAC address.
  - If you enforce a MAC limit on your AP switch ports, such as when tunneling traffic to a Mist Edge, set the MAC limit to two or more: one for the Ethernet MAC and one for the AP MAC.
- If you leverage 802.1X authentication against the APs with dual uplinks, both ports authenticate to the network independently of each other. Thus, two separate auths appear in your RADIUS server.



Wi-Fi 7 Deployment Considerations

The AP47 supports Wi-Fi 7 (IEEE 802.11be Extremely High Throughput), which provides higher throughput and lower interference as compared to other Wi-Fi standards. Wi-Fi 7 also introduces several new features such as 4K Quadrature Amplitude Modulation (QAM), Multi Resource Unit (Multi-RU), and Multi-Link Operation (MLO) among others.

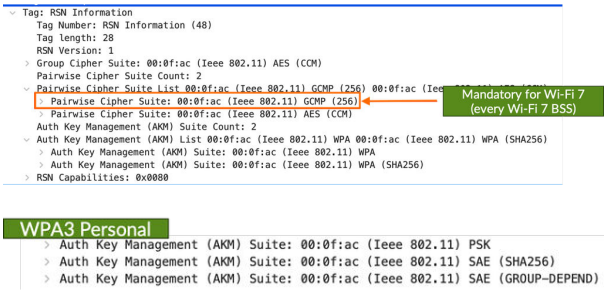
With the introduction of Wi-Fi 6E, the Wi-Fi Alliance enforced the use of WPA3 in the 6 GHz band. With Wi-Fi 7, the use of WPA3 or OWE is mandatory on any WLAN in any band that has Wi-Fi 7 enabled.

The mandatory security items in Wi-Fi 7 are:

- WPA3 or OWE
- Management Frame Protection
- GCMP256 Cipher
- Beacon Protection

- Authentication and Key Management (AKM) type 24 (SAE-GDH) or type 25 (FT+SAE-GDH) with the use of WPA3 Personal

The GCMP256 encryption protocol is mandatory on every Wi-Fi 7 BSS, regardless of the security type.



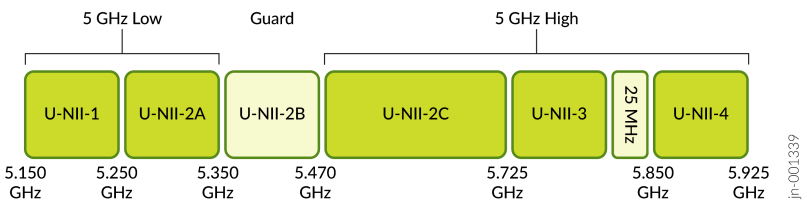
When you create WLANs in the Mist UI, Wi-Fi 7 is enabled by default and Mist automatically enables the mandatory Wi-Fi 7 security features.

For additional information about Wi-Fi 7, see: Wi-Fi (802.11be) Technology.

Tri-Band Radio Operation on the AP47

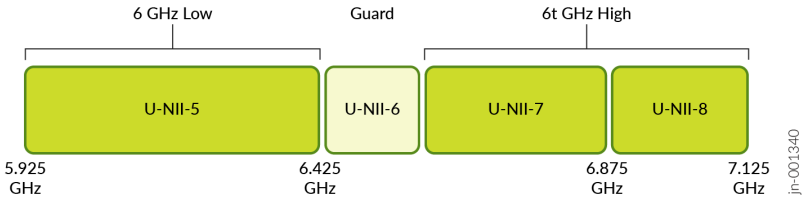
The AP47 has three Wi-Fi 7 data radios and supports the following modes of operation:

- Tri-band mode—This mode operates simultaneously in the 2.4-GHz, 5-GHz, and 6-GHz bands.
  - 2.4 GHz band—channels 1-13
  - 5 GHz band—channels 36-177
  - 6 GHz band—channels 1-233
- Dual 5 GHz mode—This mode splits the 5 GHz band into high channels and low channels.
  - 5 GHz band (low)—U-NII-1 and U-NII-2A (channels 36-64)
  - 5 GHz band (high)— U-NII-2C, U-NII-3, and U-NII-4 (channels 100-177)
  - 6 GHz band—(channels 1-233)



- Dual 6 GHz mode—This mode splits the 6 GHz band into high channels and low channels.

- 5 GHz band—channels (36-177)
- 6 GHz band (low)—U-NII-5 (channels 1-93)
- 6 GHz band (high)—U-NII-7 and U-NII-8 (channels 117-233)



NOTE: Dual 5 and dual 6 GHz mode support varies per country based on the allowed channels in the country.

GPS and GNSS Support on the AP47

The AP47 supports L1 and L5 based Global Navigation Satellite System (GNSS). The reason for including a Global Positioning System (GPS) chip on the AP is to support Standard Power use cases in 6 GHz. These use cases require suppling geolocation information to the Automated Frequency Coordination (AFC) system. However, GNSS reception indoors can be challenging, especially as your AP placement approaches the center of a building..

You will achieve the strongest GNSS reception indoors when you deploy AP47s near the edge of the building or close to exterior windows.

SEE ALSO

AP Placement for Location Services

Wi-Fi 7 (802.11be) Technology

SUMMARY

Explore the features and benefits of Wi-Fi 7 and watch the embedded video to gain insights from our Juniper Mist experts' commentary and recommendations.

IN THIS SECTION

The IEEE 802.11be Extremely High Throughput (EHT) standard, more commonly known as Wi-Fi 7, introduces new features and delivers several major improvements over Wi-Fi 6 and Wi-Fi 6E.

Video Overview

See the following video for more information about Wi-Fi 7.

Video: Introducing the Power and Scale of Wi-Fi 7

Speed

802.11be has a maximum speed of 46 Gbps. Enterprise deployments are unlikely reach or require the theoretical data rates due to the size and power limitations of a 16-spatial stream Access Point (AP). But 8-spatial stream enterprise APs can be expected to reach data rates up to 23 Gbps, with single-client data rates of around 5.6 Gbps for optimally located clients on a 320 MHz wide channel.

Wi-Fi 7 supports the 2.4GHz, 5GHz, and 6GHz radio bands, but it is the 6GHz band that can accommodate 320 MHz wide channels and thus produce the top speeds. Even so, we expect to see enterprises sticking to 20 MHz wide channels in the 2.4GHz band, 40 MHz, or 80 MHz in the 5 GHz band, and 80 MHz (perhaps 160 MHz) wide channels the 6 GHz band.

To leverage the benefits of Wi-Fi 7, both the AP and the client will need to be running 802.11be, and the upstream switch will need to support the bandwidth with multigigabit port speeds. Note that you'll also want to consider your Power over Ethernet (PoE) requirements when upgrading from Wi-Fi 6 or prior standards to allow for the additional 6 GHz radio operation.

Core Features

Core features include:

- 16 spatial streams
- 320 MHz wide channels in the 6GHz radio band

> **NOTE**: 320 MHz channel width may be unavailable in some regions due to regulatory restrictions.

- 4K Quadrature Amplitude Modulation (QAM)
- Multi-RU
  - Preamble puncturing
  - Flexible channel utilization
- Multi-Link Operation

Wi-Fi 7 (802.11be) Details

Wi-Fi 7 promises unprecedented data rates, as well as increased network capacity and efficiency.

- 4096 QAM—Quadrature Amplitude Modulation converts digital data frames into an analog signal for wireless transmission. It improves spectral efficiency by varying the phase and amplitude of radio waves in such a way that more data can be detected from the signal. 4K-QAM (4096-QAM) provides a 20% data rate increase compared to the Wi-Fi 6 (802.11ax) for 1024-QAM.
- Multi-Resource Unit —This feature was optional in Wi-Fi 6e, but is standard in Wi-Fi 7. Essentially, it provides a way make more efficient use of RUs, which are small slices of wireless radio frequency that provide a way to concurrently support multiple users in heavy traffic. Wider channels contain more RUs, and multi-RUs let a single user leverage more than one RU in order to support more clients by providing more granular scaling support with the channels.
- MLO—MLO is a new feature introduced with Wi-Fi 7 (802.11be) which allows simultaneous operation of AP and client across separate bands and channels. Devices listening on multiple channels can monitor for changing channel quality and dynamically change the transmitting channel to improve reliability. MLO also allow for Wi-Fi band aggregation, which is the same idea as link aggregation in Junos for Juniper switches. It can increase throughput by allowing simultaneous transmission across two radio bands, thus providing redundancy. (Prior to Wi-Fi 7, a Wi-Fi connection was limited to a single band at a time.) Note that MLO requires both the AP and the client to operate on multiple bands. While Mist APs do support this, as of 2024, many clients are limited by power and a maximum of two antenna spatial streams.
- Preamble Puncturing—Also known as Punctured Transmission. Preamble puncturing is particularly useful in the 5 GHz and 6 GHz bands, where wider channels are the norm. Essentially, it provides a way for the AP and client to carve out a small section of an occupied channel and give it over for the

exclusive use of an interfering device. In this way, puncturing lets the AP and the client continue to use as much of the remaining channel spectrum as possible instead of having to scale back the entire channel to the smaller width. Preamble puncturing was optional in Wi-Fi 6e, but is standard in Wi-Fi 7.

RELATED DOCUMENTATION

https://design.mist.com/

Wi-Fi 6 (802.11ax) Technology

SUMMARY

Explore the features and benefits of Wi-Fi 6 and watch the embedded video to gain insights from our Juniper Mist expert's commentary and recommendations.

IN THIS SECTION

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: Maximize the Potential of WiFi 6

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 Wi-Fi Assurance | 2

Hardware for Your Wireless Network | 9

https://en.wikipedia.org/wiki/Wi-Fi_6

https://design.mist.com/

Considerations for 6 GHz Wireless

SUMMARY

Before you deploy Wi-Fi 6E with Juniper Mist™, read these guidelines about necessary steps, recommended configurations, and best practices.

IN THIS SECTION

When deploying Wi-Fi 6E, there are practical considerations to keep in mind to ensure successful implementation.

Spectrum Availability

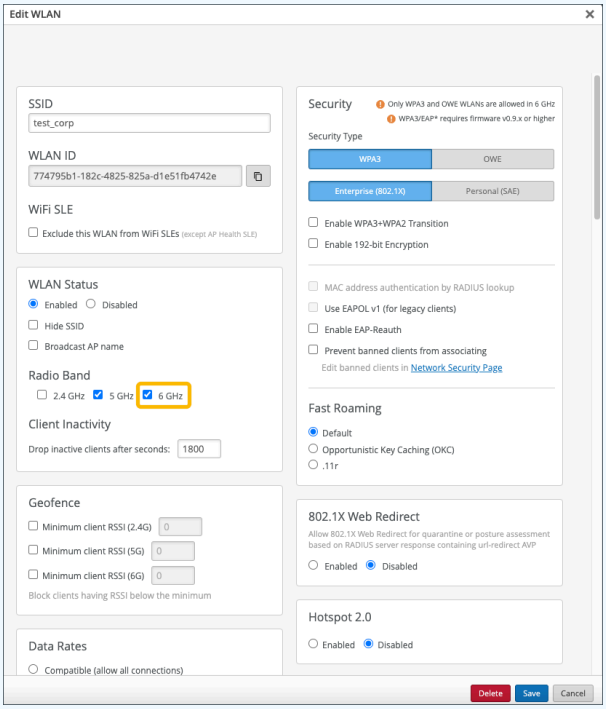
Wi-Fi 6E operates in the 6-GHz frequency band, offering increased bandwidth and reduced interference compared to previous Wi-Fi standards. Before deploying Wi-Fi 6E, it is crucial to verify spectrum availability in your region and ensure that you're complying with regulatory requirements.

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.



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-Enterise 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 42: Client Device Support of WPA3 and OWE

WPA3	OWE
Android • Version 10 and above	Android • Version 10 and above
Apple (iPhone 6, 2013+ MacBook (802.11ac), iPad 5) • 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 • iOS 16, iPadOS 16.1 and above • MacOS 13 and above

Windows
• WPA3 Enterprise – Windows 10 (2004)
  • For Intel NICs: 9260 or newer and driver 21.90.3.X or later
• WPA3 Personal – Windows 10 (1903)
  • For Intel NICs 9260 or newer and driver 21.10.X or later
  • H2E Supported on Windows 10 21H2 or Windows 11
  • W10 Intel Driver = 22.70.x or Later, W11 Intel Driver = 22.100.x or Later
	Windows
	• Windows 10 (2004)
	  • For Intel NICs: 9260 or newer and driver 21.90.3.X or later

ChromeOS • Support added in 2020	ChromeOS • Not Supported

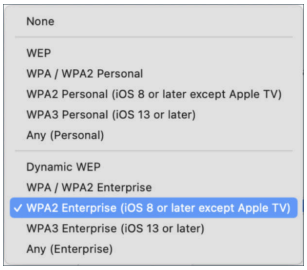
The information in the table above was derived from the intel.com and apple.com support websites.

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.

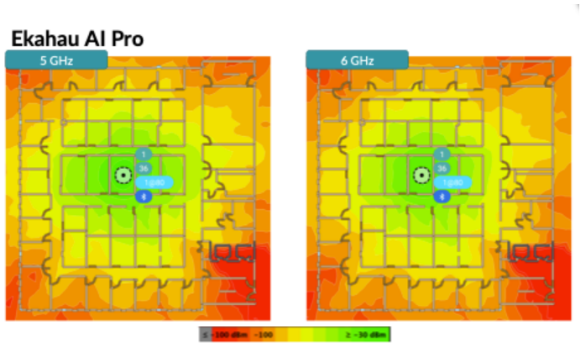
The following depicts selecting the **WPA2 Enterprise** security type from Apple Configurator:

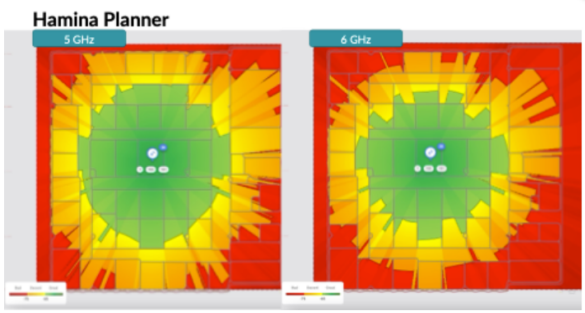


RF Design

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).

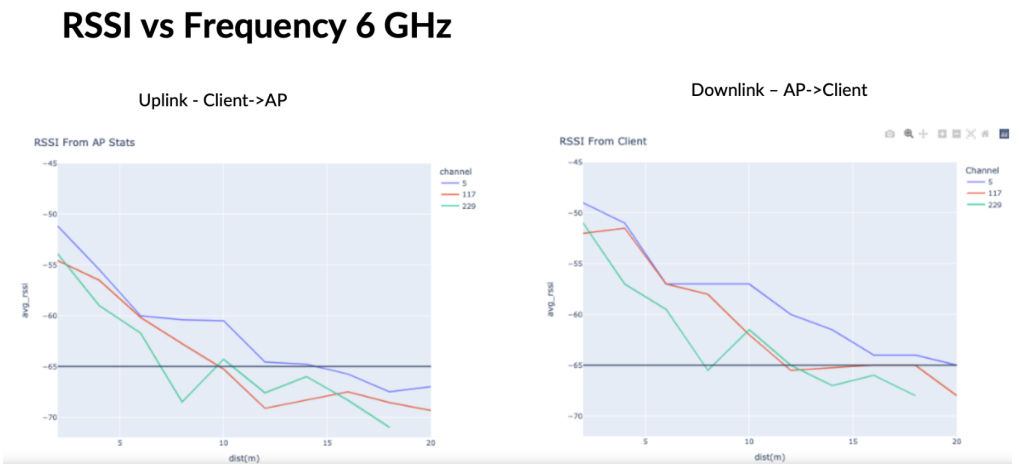
6 GHz requires a slightly higher AP density than 5 GHz. We recommend a proper RF design for 6 GHz. However, in some environments this might not be feasible. If you already have capacity based on 5-GHz designs, you may not need to change much from a density perspective. Based on the material of your walls, 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.



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.

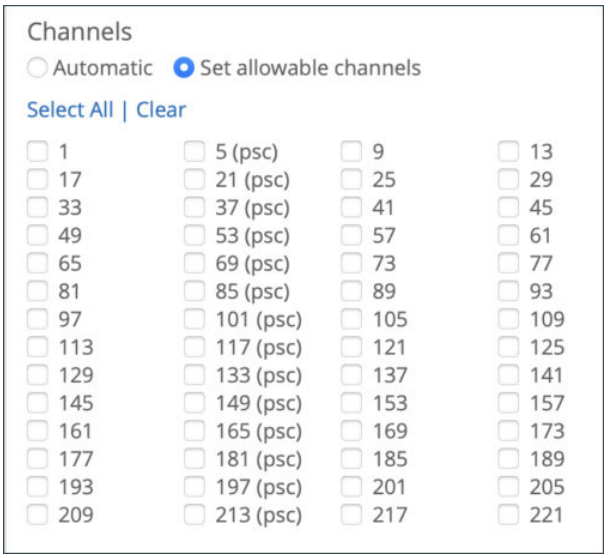
Utilize non-PSCs in environments where you may want to utilize 20 or 40 MHz channel bandwidth, such as in Europe with only 500 MHz of spectrum, or in high density environments.

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.



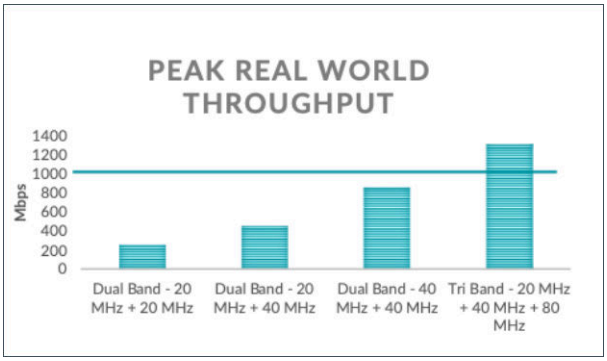
PoE Requirements

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 APs" on page 26.

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.



AFC and 6 GHz Incumbents

SUMMARY

Learn about the benefits of Automated Frequency Control (AFC) and the implications for your wireless deployments.

IN THIS SECTION

Automated Frequency Control (AFC) for standard-power operations reduces the potential for harmful interference to existing licensed users of the spectrum.

The AFC system is designed to protect the tens of thousands of fixed-microwave links in use across the United States from potential harmful interference. Figure 1 shows the number, distribution, and types of active licenses across UNII 5, 6, 7, and 8 spectrum (satellite excluded).

Figure 49: Wi-Fi License Usage

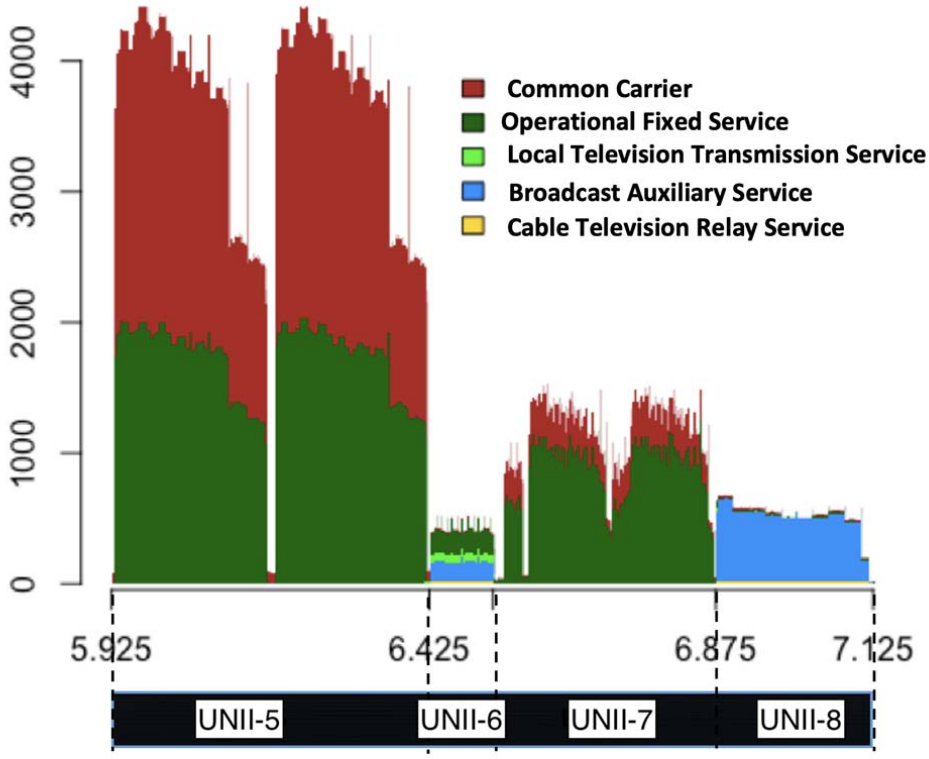


Figure 1. Assignment Density

Source: https://docs.fcc.gov/public/attachments/FCC-18-147A1_Rcd.pdf.

The way AFC works is for an access point (AP), or a central control point acting as proxy for APs under its control, sends the geolocation, including location confidence, antenna height, FCC ID, and device serial number to an AFC operator. The AFC then performs a lookup in the FCC Universal Licensing System (ULS) and then uses an attenuation model based on the distance to the licensed antenna to calculates an interference-to-noise (I/N) power ratio.

The I/N value is used identify allowable frequencies and output powers for the Wi-Fi AP, that is, acceptable operating channel and power. Standard Power APs perform this check with AFC daily.

In the United States, the FCC's universal licensing system is generally the source of data for the AFC operators, except in a few scenarios. To protect radio astronomy from 6650-6675 MHz, the AFC includes and exclusion zones near observatories. The FCC's Universal Licensing System is a good

resource for locating microwave links in your vicinity. You can search by state and county, and filter on active licenses between 5925 MHz to 7125 MHz.

Incumbent Licenses on the 6 GHz spectrum

Band	Allowed Unlicensed Usage	Incumbents
UNII-5	Low Power Indoor	Fixed Service, Satellite Service
UNII-6	Low Power Indoor, Standard Power AP	Satellite Service, TV and Broadcast Services
UNII-7	Low Power Indoor	Fixed Service, Satellite Service
UNII-8	Low Power Indoor, Standard Power AP	Satellite Service, TV and Broadcast Services

- **Fixed Service** is by far the heaviest user group of 6 GHz, usually in the form of fixed microwave links. There are nearly 50,000 registered 6 GHz microwave links in the US. Most links are in the UNII-5 band, followed by UNII-7. Microwave links aren't as common in UNII-8, but they do exist. Fixed microwave links are not allowed in UNII-6 as to prevent overlap with television and broadcast services. Fixed service links are used for a sorts of private and common carrier purposes, such as control and management of public utilities, public safety uses (back-haul for emergency and police dispatch), back-haul for cell towers, long distance telephone links, and many more. Microwave links are regarded as extremely reliable and some are designed to allow less than 30 seconds of downtime in a year. That's 99.999% to 99.9999% reliability.
- **Satellite Service** includes fixed Earth-to-Space which is allowed across UNII-5 through UNII-8, except the upper 150 MHz of UNII-8. It utilizes UNII-5 the most and is part of the "conventional c-band." Common uses include TV and Radio uplink for distribution and back-haul for voice and data communications. Satellite service also includes mobile Space-to-Earth satellite links in portions of UNII-7 and UNII-8.
- **Television and Broadcast Services** predominates in UNII-6 and UNII-8. There are a wide range of uses, from the transmission-and-relay of video signals, to electronic news gathering for broadcast and cable TV entities. For this incumbent, use is also granted in the lower part of UNII-8 for special large scale audio usage by broadcast entities, venue and sounds production companies.
- **Existing unlicensed use** includes Ultra Wide Band across UNII-5, 6, 7, and 8, and was previously allowed unlicensed use of 6 GHz, which is unchanged.

Low Power Operations

Low Power mode is intended for general use such as home and enterprise. It is allowed across the entire 1200 MHz of the 6 GHz spectrum. In addition, the following restrictions are in place to protect incumbents:

- Limiting low power mode APs to a power spectral density of 5 dBm/MHz and -1 dBm/MHz for client devices.
- Requiring a contention based protocol.
- Restricting Low Power mode to indoors operation only (APs much carry a “FCC regulations restrict to indoor use only.” label).
- Allowing only integrated antennas.
- Disallowing weatherizing low power APs.
- Disallowing battery-powered APs.

In 2020, it was still possible to increase the allowed output to 8 dBm/MHz Power Spectral Density (PSD) through a Further Notice of Proposed Rule Making. With the constant PSD, the EIRP doubles with channel bandwidth, which means the highest allowed EIRP with wider bandwidth could be supported. Recall that EIRP is 18 dBm at 20 MHz, 21 dBm at 40 MHz, and 24 dBm at 80 MHz. Thus 18-24 dBm EIRP is well within the typical range for enterprise APs.

Standard Power Operations

For information on 6 GHz Standard Power Frequencies, or 6 GHz Standard Power and Juniper Mist APs, see "Wi-Fi 6E Standard Power and Automated Frequency Coordination" on page 471.

In general, standard power is available to address issues that may arise from Low Power mode, for example, supporting both indoor and outdoor usage, or using a connected external antenna.

Wi-Fi 6E Standard Power and Automated Frequency Coordination

SUMMARY

Standard power is available on certain Juniper APs.

In the United States, the Federal Communications Commission (FCC) allows networks on Wi-Fi 6E to operate under Low Power Indoor (LPI) operating class, which limit operations to indoor only, no external antennas, no weatherproof enclosures. LPI also limits power to 5 dBm/MHz PSD (Power Spectral Density).

The other operating class that the FCC had announced at the same time was Standard Power (SP) which came with a requirement that its operations be coordinated through an AFC or Automated Frequency Coordination service. This was required to prevent interference with incumbent users (legal license holders still using these frequencies) and protect their existing deployments. The AFC provides coordination so that Wi-Fi and other users can both operate without worry of interference. Wi-Fi 6E operating under Standard Power opens up several of the use cases that LPI cannot address. The SP operating class rules:

Indoor and Outdoor operations

Allows the use of external antenna’s

Allows more power with 23 dBm/MHz PSD and max AP EIRP of 36 dBm and Client max *EIRP of 30 dBm

Operations are limited to UNii-5 and UNii-7, with UNii 6 and 8 being protected for Incumbents

*EIRP = Equivalent Isotropic Radiated Power or radio geek for what comes out of the antennas.

SP operating Class in Wi-Fi 6E in the US?

Different Juniper APs support different power modes (standard and low power indoor), different radio bands (2.4 GHz, 5 GHz, and/or 6Ghz), and vary in whether or not they include GPS.

For the 6 GHzGPS is needed for a precise geolocation, which Mist uses to perform its cloud-based AFC optimizations for the 6 GHz radio spectrum. . If the AP itself does not have GPS, it can leverage the GPS from a nearby AP

Table 1 shows GPS and power modes for the 6 GHz APs. For example, the Juniper AP45E does not include GPS. So, for the 6 GHz radio band to work, you need to deploy the AP45E in the same site (or within the radio frequency vicinity) as an AP that does have an inboard GPS so the AP45E can get it's location from that AP.

- The AFC system (database driven) provides the maximum permissible power to 6g APs based on the info provided by the FCC (U.S. Federal Communications Commission) regulations.
- Based on the AP's data (geographic location coordinates - latitudes/longitudes, antenna height above ground level (AGL) or above mean sea level (AMSL), manufacturer's serial number, etc), the AFC system will dynamically send the power info (EIRP/PSD values) for channel-based/frequency-based combinations, which in-turn will be used by AP during frame transmission.
- AFC systems allow SP (Standard Power) APs to transmit at a higher power, while avoiding interference between the users within the band.

For APs that support standard power only, it is enabled automatically when you configure the 6 GHz radio on the WLAN. For APs that support both low power indoor (LPI) and standard power, however, the default power mode is LPI. For these APs, you need to enable standard power when you enable the 6 GHz radio, for example as part of a dual band configuration on an AP64.

6 GHz standard power requires GPS for geolocation. For Juniper APs without GPS, they can get a geolocation from any neighboring Juniper AP that does have GPS.

Table 43: Power Modes for Juniper APs with 6 GHz Radios

Juniper APs with 6 GHz Radio	GPS	Low Power Indoor	Standard Power
AP66/D	yes	no	planned
AP47/D	yes	default	yes
AP47E	yes	no	yes
AP36/AP37	yes	default	planned
*AP36M	yes	default	planned
AP64	yes	no	default
AP45	**no	default	planned
AP45E	**no	no	planned

AP34	**no	default	planned
AP24	**no	default	planned

*AP36M defaults to the integrated directional antenna and LPI.

** These APs require a nearby Juniper AP with GPS for their geolocation.

In the United States, the FCC requires standard power for weatherized APs and APs with external antennas, even if they are deployed indoors. For indoor-rated APs, standard power is optional, for example, in a deployment where high AP and/or client transmit power is required.

Automated Frequency Control (AFC) for standard-power operations reduces the potential for harmful interference to existing licensed users of the spectrum.