JUNIPER NETWORKS | Engineering Simplicity

Juniper AI-Driven Wired & Wireless Network Deployment Guide Configuration Example (NCE)

Published
2025-11-04

Table of Contents

Juniper AI-Driven Wired & Wireless Network Deployment Guide Configuration Example (NCE)

Juniper Networks Network Configuration Examples (NCEs) describe how to configure and deploy Juniper products in a typical use case scenario. In this NCE, you'll find design and planning suggestions, use case scenarios with Mist GUI configuration information. Read further to plan and optimize your network deployment.

About this Document

This document is designed to guide a user through the many phases of wired and wireless network deployment using the Juniper Mist portal. It provides both concepts and actions that the user would carry out in two different network deployment scenarios: a distributed network and a centralized (tunneled) network. The document starts from a greenfield deployment perspective, so it provides information about onboarding devices into the Juniper Mist cloud and proceeds to switch and access point (AP) configuration using the Mist portal. In several places, there are references to Juniper Mist documentation to provide additional detail as needed.

Introduction

IN THIS SECTION

Purpose of this Guide

- To provide a step-by-step framework for deploying Juniper's AI-Driven wired and wireless solutions in an enterprise environment.
- To provide a focus on best practices for seamless integration, optimal performance, and enhanced security.

Target Audience

- Network Architects, Engineers, and IT Administrators.

Key Benefits of Juniper's AI-Driven Solutions

- Simplified operations with Mist AI.
- Enhanced user experience.
- Proactive troubleshooting and reduced OpEx.
- Robust security with Zero Trust principles.

Planning and Design Phase

IN THIS SECTION

Network Assessment

The Network Assessment phase is foundational for successful Juniper deployment. This involves a detailed evaluation of the current network environment. It includes an inventory and analysis of the wired infrastructure—such as switches and cabling—and the wireless setup, including access points and their coverage. Key considerations during this phase include understanding the specific demands of user density and critical application requirements (for example, real-time voice and video, large data transfers, or the unique needs of IoT devices). A comprehensive review of current security policies and compliance mandates is essential. Existing WAN connectivity and Internet egress points must also be evaluated. This ensures the Juniper solution integrates smoothly, meets performance expectations, and aligns with the organization's security posture.

To help understand the current network infrastructure, ensure your analysis answers the questions in each of the following categories:

- **For Existing Switches**
  - What are the makes, models, and quantities of existing switches at each location?
  - What is the current firmware or OS version running on these switches?
  - What is the age and warranty status of the existing switching infrastructure?
  - Are the switches Layer 2 or Layer 3? If L3, what routing capabilities do they have?
  - What is the current port utilization on key switches (for example, core, aggregation, access)?
  - Are you using any high-availability mechanisms (for example, stacking, MLAG, VRRP)?
  - What is the power over Ethernet (PoE) capabilities of the access switches, and what is the current PoE budget utilization?
  - What is the current network segmentation strategy (for example, VLANs, subnets)?

    - Are you using any network access control (NAC) solutions with the switches?

- **For Existing Access Points (APs):**
    - What are the makes, models, and quantities of existing wireless APs?
    - What Wi-Fi standards do they support (for example, 802.11ac, 802.11ax/Wi-Fi 6, Wi-Fi 6E)?
    - What is the current firmware version of the APs?
    - How are the APs currently powered (PoE or external power)?
    - What is the current wireless controller solution (if any), and is it on-premises or cloud-managed?
    - What are the existing SSIDs, their security configurations (for example, WPA2-Enterprise, PSK), and associated VLANs?
    - Are there any existing wireless site survey reports available?
    - What is the perceived wireless performance and coverage in key areas?
    - Are there known dead spots or performance issues?
    - Are there any location-based services or IoT devices currently utilizing the wireless network?
- **For Existing Cabling:**
    - What type of Ethernet cabling is in place (for example, Cat5e, Cat6, Cat6a, fiber)?
    - What is the age and condition of the existing cabling infrastructure?
    - Are there detailed cabling diagrams or documentation available?
    - What is the current capacity of the backbone cabling between network closets/buildings?
    - Are there any known cabling issues (for example, damaged cables, poorly terminated connections)?
    - Is there sufficient spare cabling capacity for future expansion, especially for new APs or higher speed wired devices?
- **User density and application requirements (voice, video, data, IoT):**
    - What is the peak number of concurrent users expected in different areas (for example, office floors, conference rooms, and common areas)?
    - What is the primary business-critical applications (for example, ERP, CRM, VDI) and their bandwidth/latency requirements?
    - Is there significant use of real-time applications like Voice over IP (VoIP) or video conferencing (for example, Zoom, Microsoft Teams)? What are their QoS requirements?

- What types of IoT devices will be connected to the network (for example, sensors, cameras, smart building controls)? What are their connectivity and security needs?
- What are the typical data transfer patterns and volumes (for example, large file transfers, cloud backups)?
- Are there any specific bandwidth guarantees, or quality of service (QoS) policies required for certain user groups or applications?
- How many devices per user are expected (for example, laptop, smartphone, tablet, wearable)?
- What are the peak usage times for the network?

- **Security policies and compliance requirements:**
  - What are the organization's existing security policies (for example, acceptable use, data classification, access control)?
  - Which industry-specific or regulatory compliance standards must the network adhere to (for example, HIPAA, PCI DSS, GDPR, ISO 27001, NIST)?
  - Are there specific requirements for network segmentation, micro-segmentation, or isolation of sensitive data?
  - What are the current authentication and authorization mechanisms in place (for example, Active Directory, RADIUS, 802.1X)?
  - What are the requirements for guest access, and how is it currently secured and managed?
  - Are there any existing intrusion detection/prevention systems (IDS/IPS), firewalls, or security information and event management (SIEM) solutions?
  - What are the requirements for data encryption, both in transit and at rest?
  - Are there specific policies for BYOD (Bring Your Own Device) or corporate-owned device management?
  - What is the organization's incident response plan, and how does network security integrate with it?
  - Are there any requirements for logging, auditing, and reporting of network security events?
- **Existing WAN connectivity and internet egress points:**
  - What types of WAN connections are currently in use (for example, MPLS, broadband, dedicated internet access, 4G/5G LTE)?
  - What are the bandwidth capacities of each WAN link at each location?
  - What are the current service providers for WAN and internet connectivity?

- Are there any existing SD-WAN solutions in place, and if so, what is their architecture and vendor?
- What are the primary internet egress points for the organization?
- Are there any specific requirements for WAN redundancy or failover?
- What are the current latency and packet loss experienced across WAN links?
- How is traffic prioritized across the WAN today (for example, QoS policies)?
- Are there any direct cloud connections (for example, AWS Direct Connect, Azure ExpressRoute, Google Cloud Interconnect)?
- What are the current costs associated with WAN and internet services?

High-Level Design

The high-level design (HLD) phase translates the assessment findings into a strategic blueprint for the new Juniper network. This involves defining the overall network topology, typically a hierarchical structure with core, aggregation, and access layers, leveraging Juniper EX Series Switches for robust wired connectivity. A comprehensive IP addressing scheme and VLAN planning must be established to ensure efficient traffic flow and logical network segmentation. For the wireless network, detailed coverage and capacity planning, often informed by site surveys, will dictate optimal Juniper Mist AP placement to meet user density and application performance requirements. A key aspect of the HLD is defining security zones to isolate user groups and device types, while integrating with identity systems (for example, RADIUS, Active Directory) and security tools for a unified, secure network.

- Network topology (core, aggregation, access layers).
- IP addressing scheme and VLAN planning.
- Wireless coverage and capacity planning (site surveys, AP placement).
- Security zone segmentation.
- Integration points with existing systems (identity management, security tools).

Juniper has brought true innovation to the networking space with the world's first AI-driven wired and wireless network. The Juniper Mist™ AI platform makes networking predictable, reliable, and measurable with unprecedented visibility into the user experience. Time-consuming manual IT tasks are replaced with AI-driven proactive automation and self-healing capabilities, lowering networking operational costs, and saving substantial time and money. Juniper also brings enterprise-grade Wi-Fi, Bluetooth® Low Energy (BLE), and IoT together so businesses can increase the value of their wireless networks

through personalized location services, such as wayfinding, proximity notifications, and asset location. With the patented virtual BLE (vBLE) technology, no battery beacons or manual calibration are required.

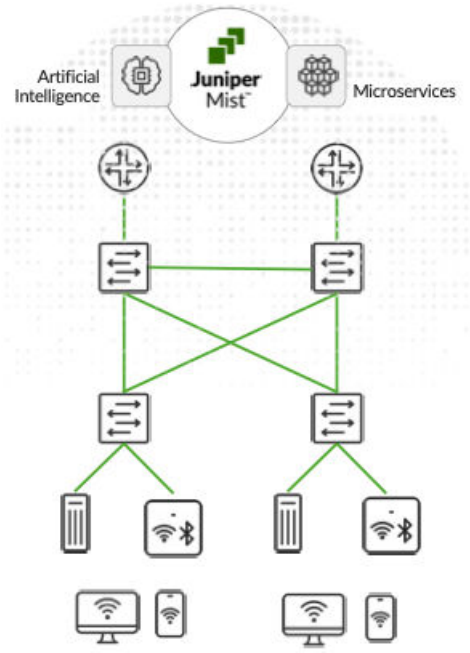
Juniper Mist™ Wired and Wireless Assurance brings cloud management and Mist AI™ to campus fabrics. They set a new standard for network management by moving your campus deployment toward AI-driven operations, which helps deliver better experiences to connected devices. The Juniper Mist cloud streamlines deployment and management of your campus fabric, while Mist AI simplifies operations and improves visibility into the performance of connected devices.

Juniper Mist Edge seamlessly integrates into a Juniper switching and wireless network by serving as a localized extension of the cloud-based Mist architecture. For customers, this means the benefits of a modern, AI-driven network can be achieved without requiring a complete overhaul of their existing infrastructure. The Juniper Mist Edge appliance handles functions that require on-premises processing, such as traffic tunneling from Juniper Wireless APs and acting as a proxy for Juniper switches. This enables secure communication with the Mist Cloud for centralized management and monitoring, even when the devices are located behind firewalls or proxies. This hybrid approach offers advantages such as maintaining a centralized data plane for campus or branch networks (a key factor for organizations transitioning from legacy controller-based architectures), seamless roaming, enhanced traffic isolation and security, and the flexibility to deploy new microservices at the edge as needed. This integration provides customers with increased network flexibility, operational efficiency, and a robust platform for managing wired and wireless networks through a single, intelligent interface.

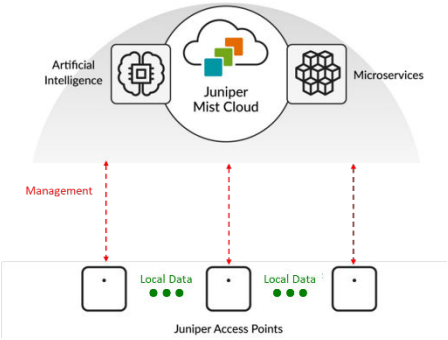
Distributed Approach

Communication between the Juniper Mist Cloud and APs uses HTTPS/TLS with AES-128 encryption, and mutual authentication is provided by a combination of digital certificate and per-AP shared key created during manufacturing. A 4096-bit key is used for the certificate signature. User data traffic is processed and forwarded locally at the Access Point Network Interface utilizing the local network infrastructure. Therefore, SSID to VLAN mapping is configured per SSID, and the switch port connecting to the AP should be configured as a trunk if you use multiple VLANs. The figure below shows the high-level architecture.

Figure 1: High-Level Architecture

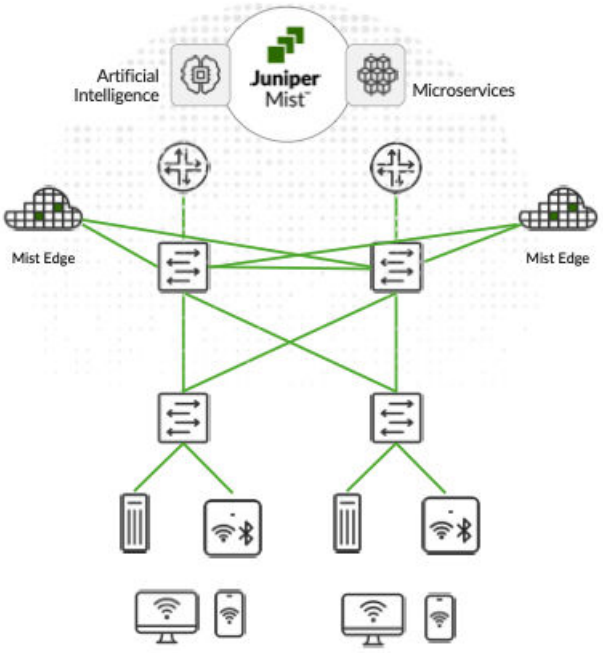


This setup is ideal for any enterprise running up to 1,000 APs in a single roaming domain or up to 2,000 concurrent connected user devices, with the ability to configure switch ports for adapting the local traffic breakout.



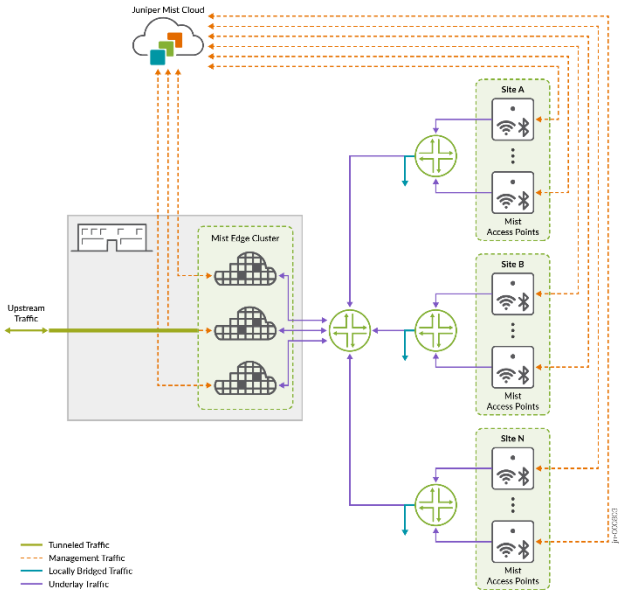
Centralized (Tunneled) Approach

Figure 2: Centralized (Tunneled) Approach



While Juniper Mist can run smoothly without tunneling services as explained in the previous section, in some use cases, you might need to consider tunneling the AP's traffic back to a central location. For that, Juniper extends its microservices to the campus using Mist Edge appliances. Juniper Mist Edge extends AI-native wireless agility and scale to the campus edge without the need for legacy wireless controllers. Juniper Mist Edge allows data centralization, which is useful for organizations limited by legacy network designs, and for those that want seamless wireless mobility for guests and remote access.

Figure 3: Juniper Mist Edge



When using Juniper Mist Edge, organizations gain the advantage of having localized data analyzed by the Juniper Mist microservices cloud and the Marvis AI engine. The unique combination delivers agility, reliability, and operational simplicity while enabling simplified, seamless, large campus roaming and secure IoT with dynamic segmentation. Having a Juniper AI-Native Networking Platform streamlines IT operations with unprecedented automation and insight.

Juniper Mist Edge Use Cases

Juniper Mist Edge solves multiple wireless challenges while increasing network and operational efficiency. We recommend Mist Edge deployments for:

- VXLAN deployment, such as Campus Fabric Core-Distribution or Campus Fabric IP Clos.
- More than 1,000 APs and 2,000 concurrently connected devices in a single roaming domain.
- Deployments exceeding 100K wireless clients—For these large deployments, we recommend configuring multiple Mist Edge tunnels, each carrying AP traffic from different WLANs to two or more Mist Edge clusters that do not share the same L2 VLAN. This tunnel configuration is known as geo-segmentation. The Mist Edges can be housed in the same data center or can be geographically separated.
- Easy migration from a legacy controller architecture to a modern microservices cloud without impacting the existing network design.

- Extending VLANs to distributed branches and telecommuters, thereby replacing remote VPN technology.
- Separating guest access and corporate traffic.
- Providing dynamic traffic segmentation for IoT devices.

Tunneling Microservices

Juniper APs use standards-based L2TPv3 technology, or IPsec in a teleworker scenario, to tunnel traffic to and from the Mist Edge for selected WLANs. This provides flexibility to use a combination of distributed and centralized data planes, where needed, to meet customer requirements. A deployment with Mist Edge can also support locally bridged and tunneled WLANs.

The tunneling service enables you to preserve the VLAN configuration at your edge switches while transitioning to a Mist microservices cloud architecture. You accomplish this by tunneling your traffic through a centralized cluster of Mist Edge devices while maintaining the ability to separate SSIDs and users onto different networks. The tunneling service also supports seamless mobility for devices running latency-sensitive applications, allowing them to maintain performance as they roam across the campus. A Juniper Mist Edge cluster will operate intelligently to deliver scalable and reliable performance by optimizing broadcast and multicast traffic delivery. Configuration of the tunnels is simplified through the power of the Juniper Mist cloud and its zero-touch provisioning capabilities.

Tunneled WLANs and Flexible Traffic Redirection

Many times, Wi-Fi deployments have a requirement to bridge the WLAN locally as well as support separate overlays for guest access and corporate wireless network traffic. The microservices architecture provides the flexibility to form multiple tunnels to different Mist Edge appliances based on the wireless configuration requirements. For instance, at one site, the WLAN could be bridged locally, a guest WLAN could be tunneled to the DMZ using one Mist Edge device, and the corporate SSID could be tunneled to the data center for access to corporate resources using another Mist Edge device.

High Availability and Clustering

Juniper Mist Edge supports elastically scalable clusters, with options for backup clusters, composed of an unlimited number of nodes. The Mist Edge cluster design for the tunneling microservice is guided by

aggregate capacity considerations and based on the number of APs, the number of clients, and throughput expectations.

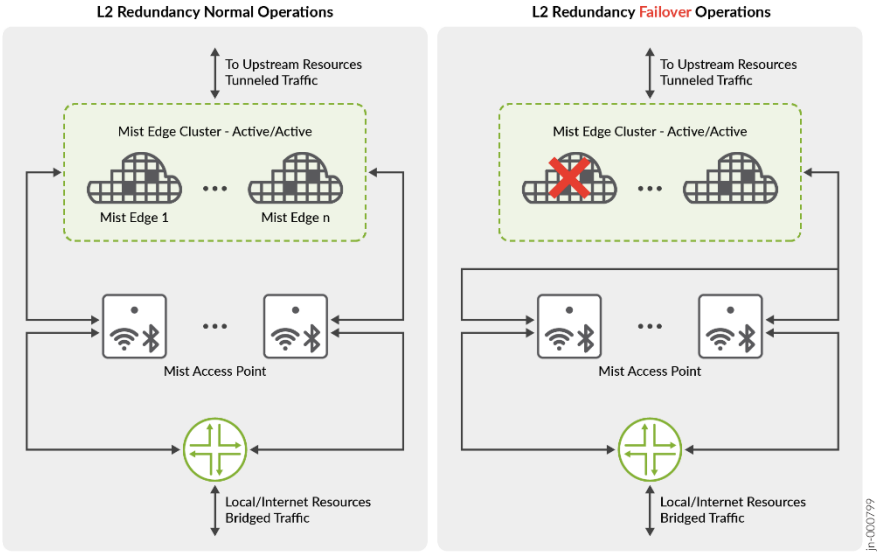
Active/active tunneling clusters deliver higher availability and resiliency than traditional N+1 standby architectures and ensure redundancy while balancing the AP traffic between Mist Edges with zero idle capacity. Mist Edge supports multiple layers of redundancy to ensure WLAN survivability in the event of a catastrophic network failure. Multiple Mist Edge nodes within a cluster allow APs to associate with any surviving node in the event of a failure. If an entire cluster goes offline within a data center, Mist APs can fail over to a different cluster hosted in a different data center to assure network survivability.

Additionally, the Mist Edge architecture allows for the standby cluster for one site to be the Primary cluster for another site, ensuring full utilization of resources and reduced operating costs.

Juniper APs separate the control and management functions from the data plane and will continue to function even if the connection to the Mist Edge goes down.

Design Considerations for L2 Redundancy

Figure 4: Design Considerations for L2 Redundancy



APs located at multiple sites can effectively terminate tunnels to Mist Edges that belong to the primary cluster (active/active), as specified in the Mist Tunnel Configuration. To ensure L2 redundancy, the cluster must consist of a minimum of two Edges. This arrangement provides robust network coverage and enhances overall system reliability. Regardless of the number of Mist Edges in a cluster, all the edges will be active, and the ap tunnels will be load balanced across them. The cloud decides and pushes down

a list of the mist edges for tunnel termination. Each AP receives a list with a different order of edges, the order of the edges determines the preferred edge for the AP.

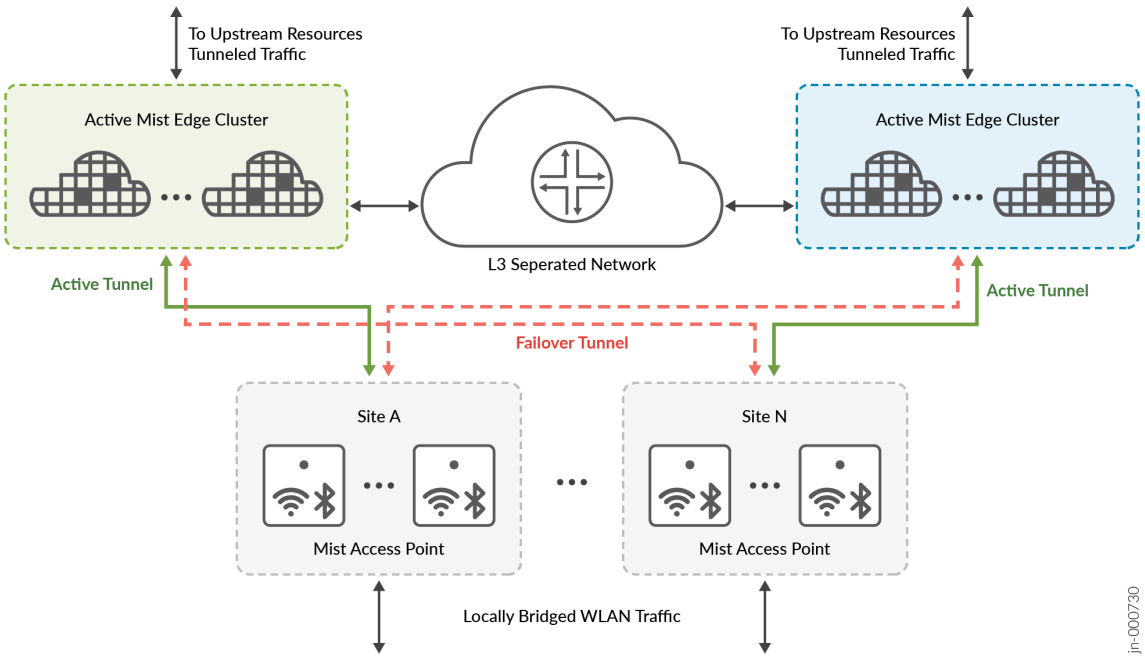
If multiple sites are tunneling traffic to a cluster with more than one edge, apps from within a site may terminate tunnels on different edge. This is the default behavior and recommended, since it achieves optimal load balancing. However, this behavior can be fine-tuned to tunnel traffic from a particular site to terminate on a single edge. This can be configured through the Tunnel Host Selection section under the Mist Clusters in the UI.

If multiple mist edges reside on the same L2 segment in your network, we recommend them to be added to the same cluster in active/active mode. We recommend to design for 80 percent capacity on Mist edge. For ME-X6 SKU, which supports a max of 5000 AP tunnels, we should plan for 4000 AP tunnels which is 80 percent of the max tunnels. In case of multiple Mist Edge loss situation, the tunnel terminator service can be oversubscribed temporarily.

Design Considerations for Data Center Redundancy

When designing data center redundancy or L3 separated networks, Mist Edges should be partitioned into Primary and Secondary clusters. All the Mist Edges that are part of Primary Cluster are active, and the Edges in Secondary Cluster are in a standby mode. Each cluster in the distributed data centers may have one or more mist edges. L3 redundancy can also be achieved with one edge each in Primary and secondary clusters. This will be an active standby deployment.

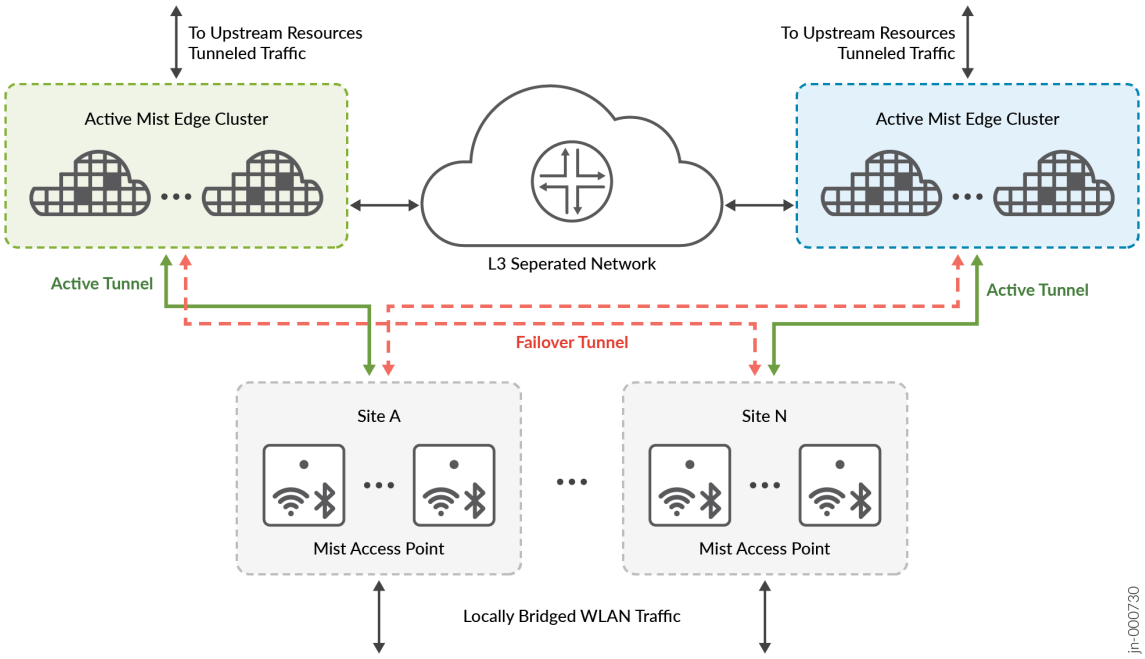
Figure 5: Design Considerations for Data Center Redundancy



The user interface provides the capability to handle up to two cluster failovers, making it an optimal solution for most campus deployments. However, if additional levels of failover protection are necessary, this can easily be accomplished through API integration, allowing for custom configuration to meet specific requirements.

In the case of distributed datacenters, separated geographically, Site A geographically closer to data center A, can be assigned Mist Cluster A as the primary cluster and Mist Cluster B in data center B and the secondary cluster. Site B can be assigned to actively terminate tunnels on cluster B, which serves as primary cluster and uses cluster A as secondary cluster. Refer to the diagram and configuration below.

NOTE: AP does not form concurrent tunnels to a secondary cluster member, dotted lines are for illustration only.



The configuration for the above deployment can be achieved using the UI on the Mist Tunnel page. Select the tunnel and configure the Primary and Secondary cluster options. The same tunnel object can be used for mapping the tunneled WLAN, found in WLAN configuration, at multiple sites which need to have “Mist Cluster A” as the preferred cluster and “Mist Cluster B” for L3 redundancy. Mist APs do not support simultaneous active and standby tunnels.

Details about how to configure Mist Edge cluster/clusters are explained in the centralized deployment section.

Low-Level Design

The low-level design (LLD) phase provides the granular detail necessary for implementation, transforming the high-level blueprint into actionable configurations. This includes specifying the exact Juniper EX Series Switch models for each network layer, along with precise port assignments for connected devices and uplinks. For the wireless component, specific Juniper Access Point (AP) models will be chosen, and their precise mounting details and power requirements (for example, PoE) will be documented. Comprehensive cabling requirements, encompassing Ethernet types (Cat6a for multi-gigabit) and fiber specifications, will be outlined. Detailed VLAN configurations will be defined, along with the selection and configuration of routing protocols such as OSPF, BGP, or advanced EVPN-VXLAN for scalable and flexible campus fabrics. Wireless SSID configurations will cover authentication methods (for example, WPA3-Enterprise), encryption standards, and Quality of Service (QoS) policies to prioritize critical applications. Furthermore, explicit security policy definitions, including firewall rules and access

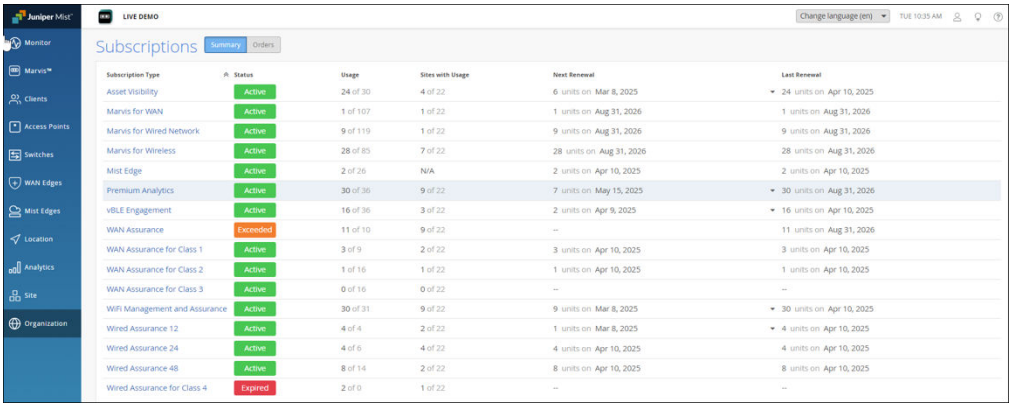
control lists, will be documented. Finally, the LLD will detail high availability and redundancy mechanisms, such as Juniper's Virtual Chassis technology for switches or Easy EVPN LAG (EZ-LAG), to ensure network resilience and uptime.

- Specific Juniper EX Series Switch models and port assignments.
- Juniper Access Point (AP) models and mounting details.
- Cabling requirements (Ethernet, fiber, PoE).
- Detailed VLAN configurations, routing protocols (OSPF, BGP, EVPN-VXLAN).
- Wireless SSID configurations (authentication, encryption, QoS).
- Security policy definitions (firewall rules, access control lists).
- High availability and redundancy mechanisms (Virtual Chassis, EZ-LAG).

Licensing and Subscriptions

This section outlines the necessary Juniper licensing and subscription requirements to enable the full functionality of the AI-Driven wired and wireless solution. It is crucial to identify and procure the appropriate Juniper Mist Cloud subscriptions, which are fundamental for leveraging Mist AI capabilities such as WiFi Management and Assurance, Marvis for Wired Network, Marvis for Wireless, and Location Services. These subscriptions activate the cloud-managed intelligence and automation that are central to Juniper's offering. Additionally, this section covers any specific licenses required for the Juniper EX Series Switches and Juniper Access Points themselves, ensuring all hardware components are properly licensed for operation within the Juniper ecosystem and can fully integrate with the Mist Cloud services. Proper licensing ensures access to features, support, and ongoing updates.

- Juniper Mist Cloud subscriptions
- Switch and AP licenses



https://www.juniper.net/documentation/us/en/software/mist/mist-management/topics/concept/subscription-faq.html

Pre-Deployment Activities

IN THIS SECTION

Site Preparation

Site Preparation is a crucial pre-deployment activity that ensures the physical environment is ready for the new Juniper network infrastructure. This involves meticulously preparing the physical racks where Juniper EX Series Switches will be installed, ensuring adequate space, proper ventilation, and sufficient power outlets are available. Comprehensive cabling installation and testing are paramount, verifying that all Ethernet and fiber runs meet design specifications and are properly terminated and labeled. Furthermore, environmental considerations such as maintaining optimal temperature and humidity levels within network closets and data rooms are vital to ensure longevity and reliable operation of the new Juniper hardware.

- Physical rack and power readiness.
- Cabling installation and testing.
- Environmental considerations (temperature, humidity).

Network Readiness

Network Readiness focuses on preparing the logical and foundational network services essential for the seamless integration and operation of Juniper's AI-Driven solution. A primary concern is ensuring robust Internet connectivity, which is vital for Juniper Mist Cloud access, as the cloud platform manages and orchestrates the wired and wireless infrastructure. You must verify accurate DNS resolution for Juniper

services to allow devices to communicate effectively with the cloud. Furthermore, precise Network Time Protocol (NTP) synchronization across all network devices is critical for consistent logging, troubleshooting, and security event correlation. Finally, the Dynamic Host Configuration Protocol (DHCP) server configuration must be meticulously planned and implemented to ensure proper IP address assignment for all new and existing devices connecting to the network.

- Ensure Internet connection for Mist Portal access
- DNS resolution for Juniper services
- NTP synchronization
- DHCP server configuration for IP address assignment

Account Setup

The Account Setup phase is dedicated to establishing and configuring the necessary accounts within the Juniper Mist Portal, which serves as the central management platform for the entire AI-Driven wired and wireless solution. This involves the initial Juniper Mist Portal account creation and the subsequent setup of the organization within the platform, defining its structure and locations (sites). Equally important is the meticulous configuration of user roles and permissions, ensuring that IT administrators and other personnel have appropriate access levels and privileges to manage, monitor, and troubleshoot the network effectively, adhering to the principle of least privilege for enhanced security.

- List of initial configuration tasks
- Create an account and an Organization
- Configure a site
- Portal user role details
- Add portal user accounts

Core Network Deployment (EX Series Switches)

IN THIS SECTION

Initial Switch Staging

Initial Switch Staging involves the physical preparation and basic connectivity verification of the Juniper EX Series switches before they are integrated into the network. This step starts with carefully unboxing the switches. Securely install them into designated racks, ensuring proper mounting and airflow. Following installation, the switches perform basic power-on procedures to confirm that they receive power and initiate their boot sequence. Crucial connectivity checks involve verifying console access, confirming link lights on ports, and ensuring the switch gets an IP address via DHCP (if configured). These steps establish network communication for Zero-Touch Provisioning (ZTP).

- Unboxing and physical installation.
- Basic power-on and connectivity checks.

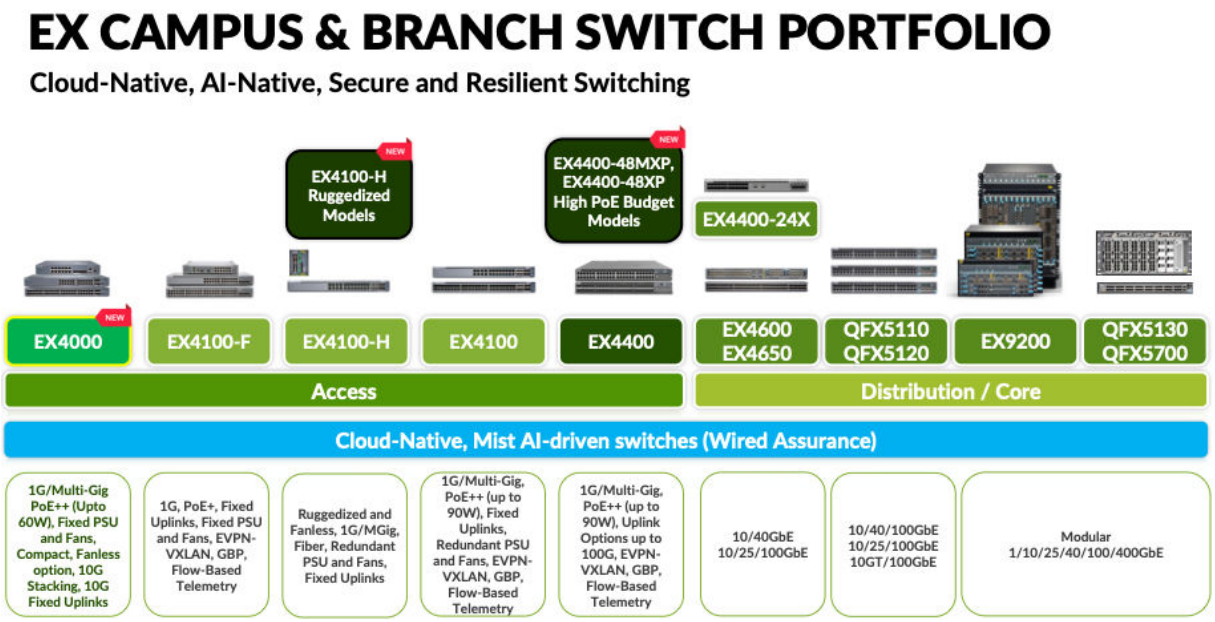
Cloud-Ready Campus Ethernet Switches

Juniper offers an AI-driven, programmable, and open portfolio of cloud-ready access, distribution, and core switches for enterprise campus networks. The access switches are cloud-ready and support Juniper Mist Wired Assurance, bringing AIOps to access layer switching. The switches meet several campus requirements, such as:

- Cloud-ready and managed by the Juniper Mist cloud architecture
- Multigigabit support

- Media Access Control Security (MACsec) AES256
- Power over Ethernet (PoE, PoE+, PoE++)
- Scalable fabric architectures via Virtual Chassis and EVPN-VXLAN
- Multivendor support
- Standards-based micro segmentation using group-based policies (GBP)
- Flow-based telemetry

Figure 6: EX Campus and Branch Switch Portfolio



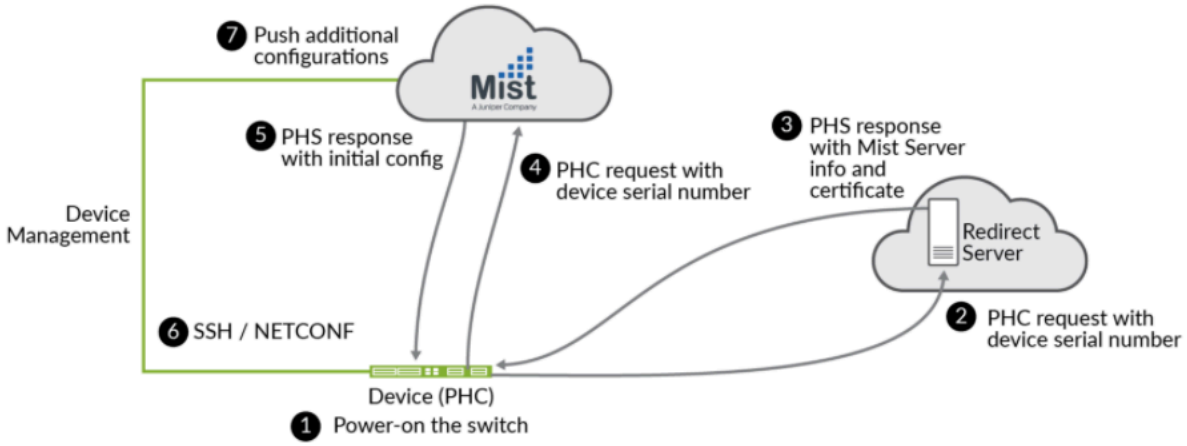
Zero-Touch Provisioning (ZTP) Configuration

Zero-Touch Provisioning (ZTP) is a cornerstone of simplified deployment for Juniper EX-Series switches, enabling rapid and automated onboarding to the Juniper Mist Cloud. Once the switches are physically connected to the network and powered on, they automatically attempt to reach the Mist Cloud. Leveraging ZTP, the switches automatically download their initial configuration templates from the cloud, eliminating the need for manual, per-device configuration. This process significantly accelerates large-scale deployments, minimizes human error, and ensures consistency across the wired infrastructure, seamlessly integrating the switches into the AI-Driven Enterprise environment.

- Ensure the right ports are open in your firewall to allow switch communication with the Mist cloud.

- Connect your switches to the network.
- Onboard your switches to the Juniper Mist cloud.
- Apply initial configuration templates via Mist Cloud.

Figure 7: ZTP Process



Wired Assurance Onboarding

Wired Assurance onboarding extends the power of Mist AI to the wired network, providing unparalleled visibility and automation for Juniper EX-Series switches. This crucial step involves enabling the Wired Assurance service for the EX-Series switches within the Juniper Mist Cloud. Once enabled, IT teams can configure specific Wired Service Level Expectations (SLEs) to define and monitor the desired performance and experience for wired clients and devices. By continuously monitoring wired client experience against these SLEs, the Mist AI engine can proactively detect anomalies, identify root causes of issues, and provide actionable insights, transforming reactive troubleshooting into a proactive and predictive approach for the wired infrastructure.

- Enable Wired Assurance service for EX Series Switches in Mist Cloud.
- Configure wired SLEs and monitor wired client experience.

To create a configuration template for Wired Assurance provisioning of EX switches to the Mist cloud, you need to use the Juniper Mist portal.

- Create a Switch Configuration Template
- Understand Switch Configuration Options

Campus Fabric (EVPN-VXLAN) Implementation (If Applicable)

Campus Fabric implementation, particularly using EVPN-VXLAN, is a critical step for building a scalable, agile, and resilient wired network with Juniper EX Series Switches. This phase involves configuring the spine and leaf switches according to the low-level design and establishing the underlying IP fabric. Next, you'll set up the EVPN-VXLAN overlay to provide efficient network segmentation and simplified routing across the campus. This advanced architecture enables the flexible placement of workloads and devices, supports seamless mobility, and enhances security by allowing for micro-segmentation, all while simplifying the overall network design and operations.

- Configure spine and leaf switches.
- Set up EVPN-VXLAN overlay for network segmentation and simplified routing.

Refer to the following JVDs for details on Campus and Branch Fabric

https://www.juniper.net/documentation/validated-designs/us/en/campus/

Wireless Network Deployment (Juniper APs)

IN THIS SECTION

Access Point Staging

Access Point (AP) staging is the initial physical preparation of Juniper APs before their full deployment and configuration. This process begins with the careful unboxing of each AP, ensuring all components are present and undamaged. Following unboxing, physically mount the APs in their designated locations according to the detailed wireless site survey and low-level design. Address power requirements by connecting the APs to Power over Ethernet (PoE)-enabled ports on the Juniper EX-Series switches. These ports supply both data connectivity and electrical power, eliminating the need for separate power outlets. This streamlined staging ensures that the APs are ready for automated onboarding and configuration via the Mist Cloud.

- Unboxing and physical mounting of APs.
- Power via PoE from EX Switches

Juniper provides a wide range of hardware to support your wireless networking needs. All Juniper APs work in conjunction with the Juniper Mist cloud and Mist AI to deliver premium wireless access capabilities.

To quickly compare different models of APs, see the table below. For more detailed information, refer to https://www.juniper.net/us/en/products/access-points.html.

Table 1: Juniper AP Models

	Wi-Fi 6E (802.11ax)				Wi-Fi 7 (802.11be)			
AP Model	AP24	AP34	AP45/E	AP64	AP36/M	AP37	AP47/D/E	AP66
Deployment	Indoor	Indoor	Indoor	Outdoor	Indoor	Indoor	Indoor	Indoor - Outdoor
MIMO	2x2:2	2x2:2	4x4:4	2x2:2	4x4:4	4x4:4	4x4:4	2.4 GHz:2x2:2
Antenna	2.4/6 + 5GHz	2.4+5+6 GHz	2.4/5/6+ 5+6 GHz	2.4/6 + 5GHz	2.4+5+6 GHz	2.4+5+6 GHz	2.4+5+6 GHz	2.4/6 + 5GHz
Antenna	Internal	Internal	Internal/ External	Internal	Internal/ Directional/ External	Internal	Internal/ Directional/ External	Internal/ Directional
vBLE	No	No	Yes	No	No	Yes	Yes	Yes
Performance	Up to 3.6Gbps	Up to 4.2 Gbps	Up to 9.6 Gbps	Up to 3.6Gbps	Up to 11.53 Gbps	Up to 11.53 Gbps	Up to 28.8 Gbps	Up to 9.38 Gbps
PoE	802.3af PoE	802.3at PoE	802.3bt PoE	802.3at PoE	802.3bt PoE	802.3bt PoE	802.3bt PoE	802.3at PoE

Selecting the Right Access Point

Choosing the right Juniper Mist access point (AP) from the AP36, AP37, and AP47 series depends on your specific environment and requirements for performance, antenna type, and deployment location.

- AP36: This is your go-to for standard indoor Wi-Fi 7 deployments. It offers solid performance with a 2x2 MIMO on the 2.4 GHz band and 4x4 MIMO on the 5 GHz and 6 GHz bands and a dedicated fourth radio for scanning. It's a great balance of essential Wi-Fi 7 features and cost-effectiveness for

environments like offices, retail, and campuses that need reliable connectivity with high performance. The AP36 is designed for efficiency and streamlined deployments.

- AP37: The AP37 is similar to AP36 from a Wi-Fi perspective. It also features advanced location services with vBLE technology which can be used in digital transformation.
- AP47: The AP47 is the top-tier, highest-performance AP in the lineup. It's a four-radio, Wi-Fi 7 AP with 4x4 MIMO on all three bands and a dedicated fourth radio for scanning. The AP47 series is for the most demanding, mission-critical environments that need the absolute best performance, speed, and reliability. This includes large enterprise offices, stadiums, and high-density deployments where every millisecond of latency and gigabit of throughput matter. It also features dual 10 Gbps Ethernet ports for redundancy

Model Specifics (Antenna and Environment)

Once you've chosen the performance tier (AP36/37 or AP47), the suffix (D, E, or M) helps you select the right antenna configuration for your specific physical space.

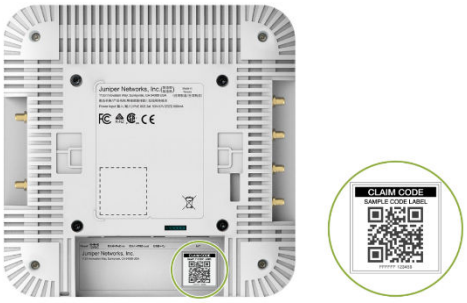
- Standard Models (AP47, AP36, AP37): These are the general-purpose, indoor APs with integrated omnidirectional antennas. They're ideal for open office spaces, conference rooms, and other typical indoor environments where you need broad, uniform coverage. This is the most common choice for most deployments.
- AP47D: The 'D' stands for directional. This model has integrated directional antennas. You should select the AP47D for high-density environments where you need to control the signal and focus capacity in specific directions. Use it in lecture halls, auditoriums, or large meeting rooms where you want to serve a concentrated group of users without causing co-channel interference with other APs nearby.
- AP47E: The 'E' stands for external antennas. This is a flexible model, as it has connectors for external antennas. Choose the AP47E when you need to customize your coverage pattern for unique or challenging environments, such as large public venues, warehouses with high ceilings or high racks where you need to precisely aim the signal.
- AP36M: The 'M' stands for multi-directional. This model is unique to the AP36 series and is designed for indoor environments. It has a built-in directional antenna but can also use external antennas. The AP36M is a versatile option for spaces where you might need to combine omnidirectional coverage with a directional signal, such as warehouses with high ceilings, high racks or large open campus areas.

Onboarding Access Points

If you activated your subscription correctly as described previously, your APs are automatically onboarded into your Mist organization. If you would like to onboard APs individually or you would like to add more APs as an expansion to already claimed APs, then follow the steps: Onboard One AP Using the Mist AI Mobile App or Onboard One or More APs Using a Web Browser.

To perform either onboarding process, you will need to locate the claim code label on the rear panel of your AP. To onboard multiple APs, you can use the activation code that is listed in your purchase order (PO).

Figure 8: Example of a Claim Code Label



Access Point Mounting

You can mount the AP on the ceiling or wall using different methods. For instructions specific to your AP model, see the Mounting Instructions in the Appendix.

All APs ship with a universal mounting bracket that you can use for all mounting options. To mount the AP on a ceiling, you'll need to order an additional adapter based on the type of ceiling.

Table 2: Mounting Bracket Adapters

Part Number	Description
APBR-U	Universal bracket for t-bar and drywall mounting. AP24s ship with the universal bracket APBR-U. If you need other brackets, you must order them separately
APBR-ADP-T58	Bracket adapter for mounting the AP on a 5/8-in. threaded rod

Table 2: Mounting Bracket Adapters *(Continued)*

Part Number	Description
APBR-ADP-M16	Bracket adapter for mounting the AP on a 16 mm threaded rod
APBR-ADP-T12	Bracket adapter for mounting the AP on a 1/2-in. threaded rod
APBR-ADP-CR9	Bracket adapter for mounting the AP on a recessed 9/16-in. T-bar or channel rail
APBR-ADP-RT15	Bracket adapter for mounting the AP on a recessed 15/16-in. T-bar
APBR-ADP-WS15	Bracket adapter for mounting the AP on a recessed 1.5-in. T-bar

Zero-Touch Provisioning for APs

Zero-Touch Provisioning (ZTP) for Juniper Mist Access Points is a key enabler for rapid and efficient wireless network deployment. Once the APs are physically connected and powered on, they automatically attempt to establish a secure connection to the Juniper Mist Cloud. Upon successful connection, the APs are automatically identified and onboarded to the cloud platform. From there, IT administrators can easily assign these APs to specific sites and overlay them onto digital floor maps within the Mist dashboard, streamlining inventory management, simplifying troubleshooting, and enabling location-based services without manual configuration on each device.

- APs automatically connect to the Mist Cloud.
- Assign APs to specific sites and maps.

Connectivity to Mist Cloud

With the initial setup tasks completed, you're now ready to verify that communication between the site and the Mist cloud is functioning properly. Ensure that all necessary network paths are open to allow

seamless connectivity. Juniper APs need the following destination/ports to be enabled at your Internet Gateway or Firewall as below:

Table 3: Connectivity to Mist Cloud

Environment	Destination FQDN/Port
All clouds	ep-terminator.mistsys.net (TCP 443) redirect.mist.com (TCP 443)
Global 01	portal.mist.com (TCP 443)
Global 02	ep-terminator.gc1.mist.com (TCP 443) portal.gc1.mist.com (TCP 443)
Global 03	ep-terminator.ac2.mist.com (TCP 443) portal.ac2.mist.com (TCP 443)
Global 04	ep-terminator.gc2.mist.com (TCP 443) portal.gc2.mist.com (TCP443)
Global 05	ep-terminator.gc4.mist.com (TCP 443) portal.gc4.mist.com (TCP443)
EMEA 01	ep-terminator.eu.mist.com (TCP 443) portal.eu.mist.com (TCP 443
EMEA 02	terminator.gc3.mist.com (TCP 443) portal.gc3.mist.com (TCP 443)
EMEA 03	terminator.ac6.mist.com (TCP 443) portal.ac6.mist.com (TCP

Table 3: Connectivity to Mist Cloud *(Continued)*

Environment	Destination FQDN/Port
EMEA 04	terminator.gc6.mist.com (TCP 443) portal.gc6.mist.com (TCP
APAC 01	ep-terminator.gc7mist.com (TCP 443) portal.gc7.mist.com (TCP 443)
APAC 03	ep-terminator.gc7.mist.com (TCP 443) portal.gc7.mist.com (TCP 443)

Refer to the following document for the exact port details for various cloud instances around the world:

https://www.juniper.net/documentation/us/en/software/mist/mist-management/topics/ref/firewall-ports-to-open.html.

Powering on the Access Point

When you power on an AP and connect it to the network, the AP is automatically onboarded to the Juniper Mist cloud. The AP onboarding process involves the following steps:

- When you power on an AP, the AP obtains an IP address from the DHCP server on the untagged VLAN.
- The AP performs a DNS lookup to resolve the Juniper Mist cloud URL. See Firewall Configuration for the specific cloud URLs.
- The AP establishes an HTTPS session with the Juniper Mist cloud for management.
- The Mist cloud then provisions the AP by pushing the required configuration once the AP is assigned to a site.

To power on your AP, connect an Ethernet cable from a PoE-enabled switch to the Eth0+PoE port on the AP.

An AP can connect to the Mist cloud with 802.3af power. However, most APs require 802.3at power at a minimum, whereas some APs require 802.3bt to operate with full functionality. Generally, 802.3at is

the minimum recommended PoE power for APs. For information about PoE requirements for APs, see the table below:

Table 4: PoE for Juniper APs

AP	Minimum PoE required	Wattage required for full operation
AP12	802.3af	12.9W
AP24	802.3af	13.0 W
AP32	802.3at	19.5W
AP33	802.3at	19.5W
AP34	802.3at	20.9W
AP43	802.3at	25.5W
AP45	802.3at/bt	29.3W
AP63	802.3at	25.5W
AP64	802.3af	13.0 W
AP36	802.3at	29.3W
AP37	802.3at	29.3W
AP47	802.3at/bt	29.3W
AP66	802.3at	25.5W

NOTE: The AP45/47 requires 802.3bt for full functionality. On 802.3at, it has dynamic functionality based on what is configured.

- The AP will do 4×4 on any two data radios, or 2×2 on 2.4 GHz, 4×4 on 5 GHz, and 2×2 on 6 GHz with three data radios enabled. For example:
  - If your WLAN configuration only has two bands configured, the AP will operate as 4×4 on both data radios.

- If WLAN configuration has three bands configured, which means all three data radios are active, then the AP will operate as 2×2 on 2.4 GHz, 4×4 on 5 GHz, and 2×2 on 6 GHz.

You might need to enable the Link Layer Discovery Protocol (LLDP) on the switch for it to deliver 802.3at or 802.3bt power. If the switch that you are connecting the AP to is not PoE capable, use an 802.3at or 802.3bt-capable PoE Power injector. Juniper doesn't carry 802.3bt power injectors in its product list, so we validated the "Phihong POE60U-1BT-5" as an 802.3bt power injector.

The AP should now appear as green (connected) in the Mist portal. You'll also notice that the status LED on the AP turns green, indicating that the AP is connected to the Mist cloud. Congratulations! You've successfully onboarded your AP.

Mist Edge

Juniper® Mist™ Edge extends AI-native wireless agility and scale to the campus edge—without the need for legacy wireless controllers. Juniper Mist Edge allows data centralization, which is useful for organizations limited by legacy network designs, and for those that want seamless wireless mobility for guest and remote access.

When using Juniper Mist Edge, organizations gain the advantage of having localized data analyzed by the Juniper Mist microservices cloud and the Marvis AI engine. The unique combination delivers agility, reliability, and operational simplicity while enabling simplified, seamless, large campus roaming and secure IoT with dynamic segmentation. Having a Juniper AI-Native Networking Platform streamlines IT operations with unprecedented automation and insight.

With Juniper Mist Edge, organizations can deploy new microservices and upgrades easily on campus as the need arises. You can deploy and manage the network services you want, where you want them, in a consistent, seamless, and secure manner.

To quickly compare different models of Mist Edges, see the table below, and for more detailed information, refer to https://www.juniper.net/us/en/products/access-points/juniper-edge-datasheet.html.

Note: Mist Edge ME-VM is not a supported tunnel termination platform for production environments. The ME-VM has different use cases as a proxy for a non-Juniper product with Access Assurance.

Table 5: Juniper Mist Edge Models

	ME-X1-M	ME-X2-M	ME-X6
Max AP	500	2000	5,000

Table 5: Juniper Mist Edge Models *(Continued)*

	ME-X1-M	ME-X2-M	ME-X6
Mac Client	5000	20,000	100,000
Performance	4 Gbps	40 Gbps	100 Gbps
Interfaces	4x1000Base-T	4x10GbE	4x25GBase-X
Optics	N/A	SFP+	SFP28

Wi-Fi Assurance Configuration

Wi-Fi Assurance Configuration is a cornerstone of optimizing wireless user experiences through Juniper's AI-Driven platform. This step involves enabling the WiFi Management and Assurance subscription within your Organization. Once enabled, IT teams can configure specific Wireless Service Level Expectations (SLEs) that align with organizational performance goals, such as connection success rates, throughput, and roaming performance. The Mist AI engine continuously monitors wireless client experience against these defined SLEs, proactively identifying and diagnosing issues, providing actionable insights, and automating troubleshooting to ensure a predictable, reliable, and measurable Wireless network experience for all users.

- Enable WiFi Management and Assurance service in Mist Cloud.
- Configure Wireless SLEs and monitor wireless client experience

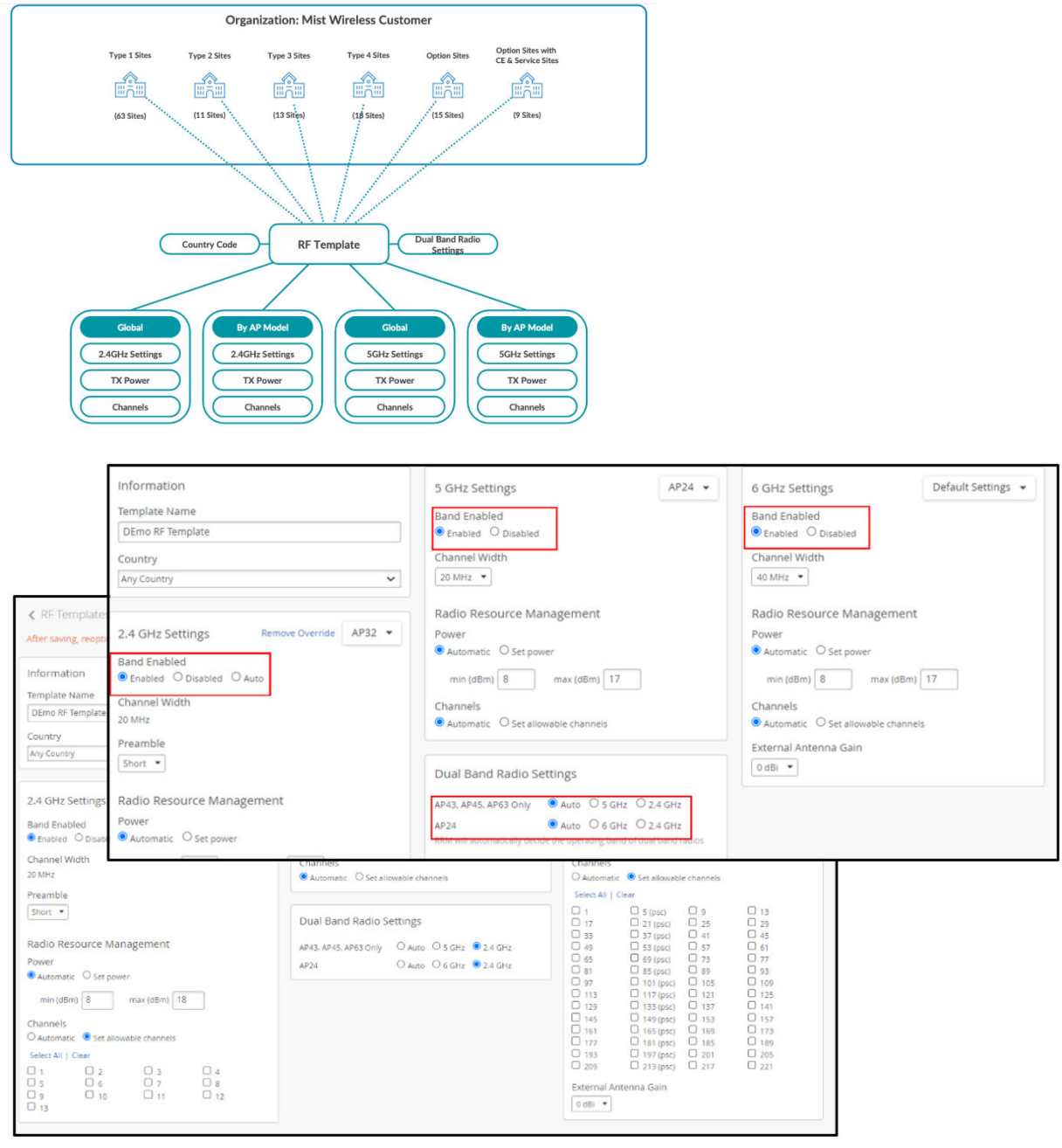
As illustrated in this document, we have two main deployment approaches, distributed and centralized (tunneled). In this section will explain the basic configuration for the distributed approach.

Radio Settings (RF Template)

RF Templates provides a way to make uniform radio configurations that are shared by all APs and sites in your organization. RF Templates do this while simultaneously allowing for model-specific exceptions to cover different use cases that may occur with specific APs or individual sites. Settings include enabling or disabling radio bands, managing channel width, setting transmission power, and configuring AP antenna gain.

AP-specific default settings are available for all AP models when the Default Settings menu is active for each radio band. You can select specific AP models from the Default Settings menu to create model-specific exceptions within the RF Template. In this document, we assume you do one RF template for all APs within the site (Default Settings).

Figure 9: Radio Settings



From the Mist left-nav menu, select **Organization > RF Template** and either choose an existing template from the list that appears or click the **Create Template** button to create a new one.

- Template Name—This is the name that appears in the templates list on the RF Templates page.
- Country—Your selection here determines which radio channels, and which power level defaults are available for configuration. If you keep the country setting on **Any Country**, the power limit and channel availability is dictated by the Country (radio frequency regulatory domain) selected in Organization > Site Settings.
- Enabled/Disabled—Turn on or off the given radio band for all APs in the template.
  - Auto—When enabled for the 2.4 GHz radio band, auto will manage the 2.4 GHz radio band on the AP to maximize performance. For APs that support dual-band, this setting will convert the 2.4 GHz radio to 5 GHz or to 6 GHz based on regularly occurring Radio Resource Management (RRM) analysis. APs that support dual 5GHz are the AP43, AP45, AP63, and AP47. APs that support 6GHz are the AP24 and AP47. RRM can turn off the 2.4 GHz radio on APs that don't support auto-conversion, so the AP offers only the 5 GHz band. If RRM finds that doing so, it will improve network performance.
  - You can select Auto for either the 2.4 GHz band, or for Dual Band Radio Settings in the RF Template configuration page, as shown below.
  - If you enable dual bands, make sure you select narrow channel widths like 20 MHz on the 5GHz band or use directional antennas to avoid high spectrum utilization.
  - The table below describes the modes of AP radio operation when different band settings are combined.

Table 6: Radio Settings

2.4 GHz Mode	Dual Band Setting	Mode of Operation
Enabled	Auto	RRM to decide the band of dual band radios (auto conversion), applies for - AP43, AP45, AP63 (2.4 GHz/5 GHz) - AP24 (2.4 GHz/6 GHz). - AP47 (2.4 GHz/5 GHz or 6 GHz) - AP36 (2.4 GHz/5 GHz or 6 GHz) - AP37 (2.4 GHz/5 GHz or 6 GHz) - AP66 (2.4 GHz/5 GHz or 6 GHz)
Enabled	5GHz	AP36, AP37, AP43, AP45, AP63, AP66 and AP47 will be in Dual 5 GHz mode. Where both radios are operating in 5 GHz band
Enabled	2.4GHz	The radio will be set to 2.4Ghz.
Enabled	6GHz	AP24 will be in 6GHz +5 GHz operating mode AP36, AP37, AP47, and AP66 operate in dual 6 GHz + 5 GHz
Auto	2.4GHz	Allow RRM to decide to enable or disable 2.4 GHz per AP (auto cancellation). Applies to all AP models.

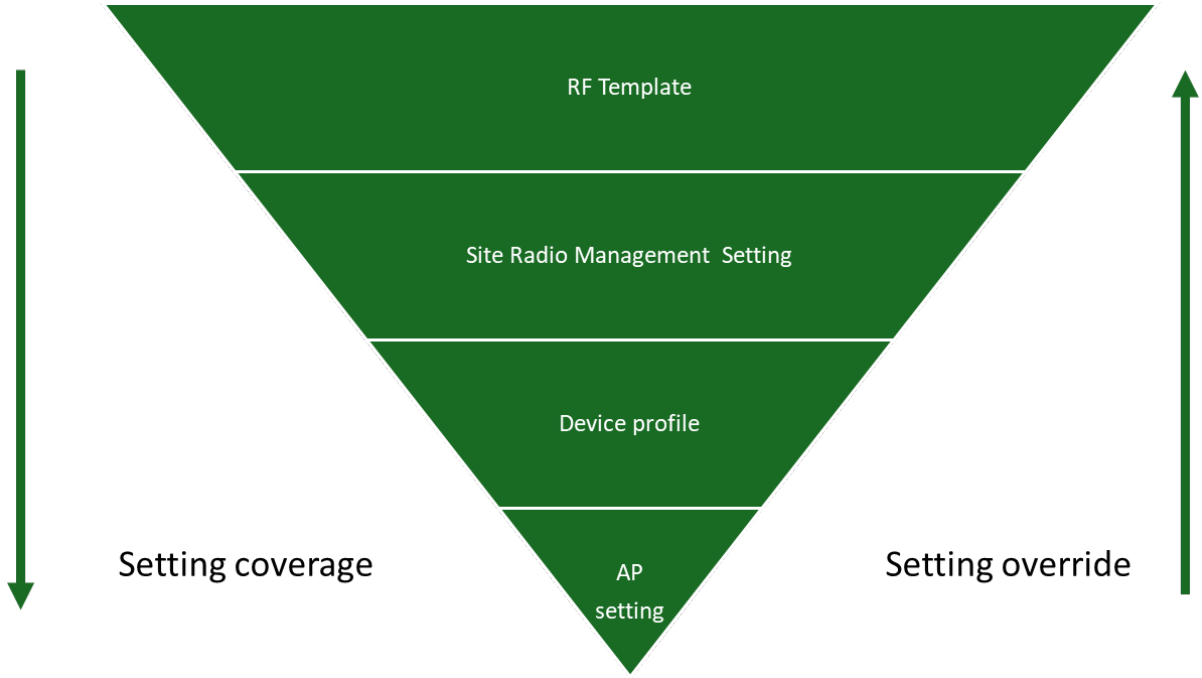
- Channel Width—For the 5 GHz and 6 GHz radio bands, you can set the channel width for all APs in the template. The 2.4 GHz radio band uses a fixed 20 MHz channel width. If required, you can specify which channels the radios can use in each radio band.
- Preamble— A preamble is a set of bits within a packet header sent from an AP to a client that synchronizes transmission signals between the sender and receiver. The options for the Preamble are as follows:
  - Unconfigured — This means the preamble will not be sent from the AP to the client.
  - Short — (Default) This applies to the 2.4 GHz radio band only. This results in faster synchronization but requires clients to have the short preamble bit set in their association requests. Not all client implementations can support this setting. If you see association failures

such as "client does not support short preamble," you can change the preamble that the AP sends to clients.

  - Long — This results in slower synchronization but supports a wider range of clients.
  - Auto — This results in slower synchronization but supports a wider range of clients.

- Power—This is the maximum transmit power allowed for a given data rate per transmit chain. Note that because total power out typically includes any MIMO gain, you should deduct MIMO gain from the total power output (TPO) when configuring transmit power.
  - The TPO for Juniper APs is equal to the transmit power per radio chain, plus MIMO gain.
  - For simplicity, you can use the general rule of thumb for MIMO gain value: 2 spatial streams (2x2) results in 3dB of MIMO gain, and 4 spatial streams (4x4) results in 6dB of MIMO gain.
  - For example, if you configure any Juniper 4x4 Access Point with 17 dBm per chain, you then add 6 dB as the MIMO gain, resulting in a total transmit power of 23 dBm.
- Channels—For the 5 GHz and 6 GHz radio bands, you can set the allowable channels (for your selected country) for all APs. When set to automatic, all allowed channels in the selected country are available. For 6 GHz, the preferred scan channels (PSC) are as defined by the IEEE. The EU, for example, allows half the 6 GHz channels allowed in the USA.
- External Antenna Gain—Mist supports 1 dBm increments (although we recommend using a range of plus or minus 3 dBm from the median value indicated in a site survey predictive design). For example, some external antennas are certified up to a certain level of gain, which depends on the combination of AP and antenna. To prevent the gain from exceeding the maximum allowed for a particular AP model and regulatory domain, you can adjust this setting.

In addition to the RF Templates page described here, you can configure RRM variables and other settings in Organization > Device Profiles, in Site > Radio Management > Radio Settings, and individually on each Juniper AP. To understand the relationship and interaction between settings on these different levels see below.



- RF Template—Configure all APs within a site or sites by leaving the Default Settings menu at Default Settings. Configure specific AP models within a site or sites, by choosing the specific AP model from the Default Settings menu.
- **Site** > **Radio Management** > **Radio Settings**— Configure all APs within the site or specific AP models within the site. Settings made on this page override RF Template settings.
- **Organization** > **Device Profiles**—Configure all APs mapped to the Device Profile and override settings in both the RF Template and **Site** > **Radio Management** > **Radio Settings**.
- Access Point setting—Configure a specific AP and override all other settings.

Juniper RF Template Recommendation

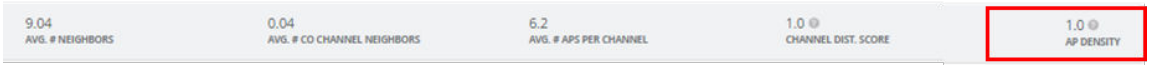
In the RF world, the optimal configuration depends on many variables that affect the installed base, such as interference, AP placement, antenna type, number of users, usage patterns, etc. Juniper recommends following best practices and making certain assumptions. Therefore, after the initial configuration, be sure to review the site Radio Management Site Summary statistics (Site > Radio Management) in addition to the SLEs to monitor the health of your network.

- Country.
  - Select the country where you plan to deploy the AP.
- 2.4GHz settings configuration block:

- Default Settings menu—When Default Settings is selected, the configuration settings you make in the settings block apply to all APs in the organization. To use a different configuration for a specific AP model, select that model from the menu and make your changes in the configuration block. You can make changes to one or more APs using a Device Profile. You can also make changes to individual APs by editing the AP itself from Access Points > AP Name.
- Band Enabled: Enabled.
- Preamble: Short
- Power: Automatic with power range from 5 – 12 dBm
- Channel: Automatic
- External Antenna: add the value of your antenna gain if you are using an external antenna.

- 5 GHz settings configuration block:
  - Default settings option (if you need to make an override configuration for any model type) then you can select the model (change default setting to a specific model) or do it using device profile.
  - Band Enabled: Enabled.
  - Channel Width: 40 MHz.

    NOTE: Monitor the Radio Management Site Summary statistics for 5 GHz as shown in the figure below. If the value of **AP Density** > 0.7 or the **AVG. # Co Channel Neighbors** > 1, change the channel width to 20 MHz. We recommend that you don't use 80 MHz as the channel width in any enterprise deployment.



  - Power: Automatic with a power range from between 5 dBm min to 17 dBm max, depending on the maximum power allowed in the local regulatory domain.

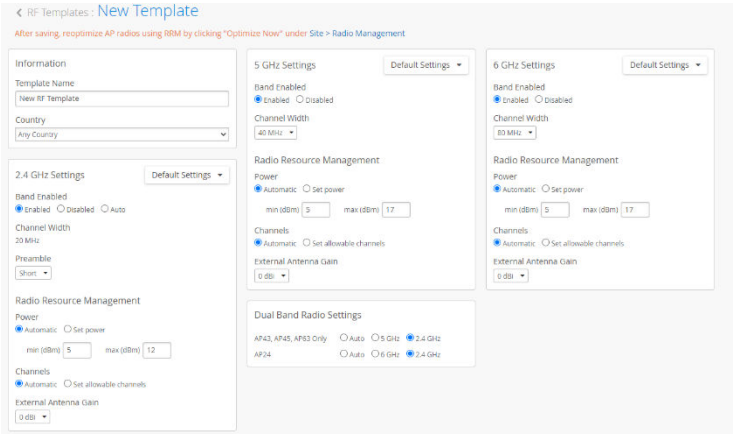
    Note: We highly recommend that you maintain the 5 GHz power setting between 3 to 6 dBm higher than the 2.4GHz power maximum to motivate clients to associate with 5Ghz for better performance.
  - Channel: Automatic.
  - External Antenna: add the value of your antenna gain if you are using an external antenna.

- 6 GHz setting:

- Default Settings menu—When Default Settings is selected, the configuration settings you make in the settings block apply to all APs in the organization. To use a different configuration for a specific AP model, select that model from the menu and make your changes in the configuration block. You can make changes to one or more APs using a Device Profile. You can also make changes to individual APs by editing the AP itself from Access Points > AP Name
- Band Enabled: Enabled
- Channel Width: 80 MHz (in FCC domain) and 40 MHz (in ETSI domain) due to channel availability per domain. Monitor the Radio Management Site Summary statistics, as you would for 5 GHz.
- Power: Automatic with a power range from between 5 dBm min to 17 dBm max, depending on the maximum power allowed in the local regulatory domain.

  Note: We highly recommend that you maintain the 5 GHz power setting between 3 to 6 dBm higher than the 2.4GHz power maximum to motivate clients to associate with 6Ghz for better performance.
- Channel: Automatic.
- External Antenna: Add the value of your antenna gain if you are using an external antenna.

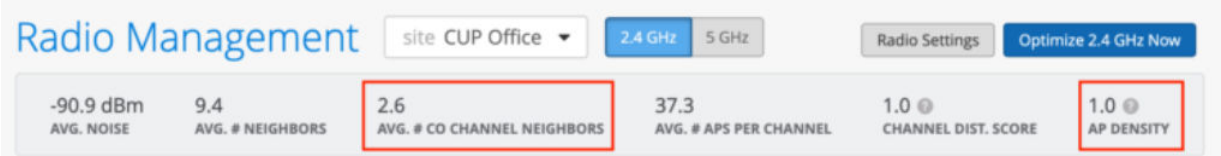
Below is a sample of the RF template that works for most of the use cases.



The following examples show how you can adjust for different use cases:

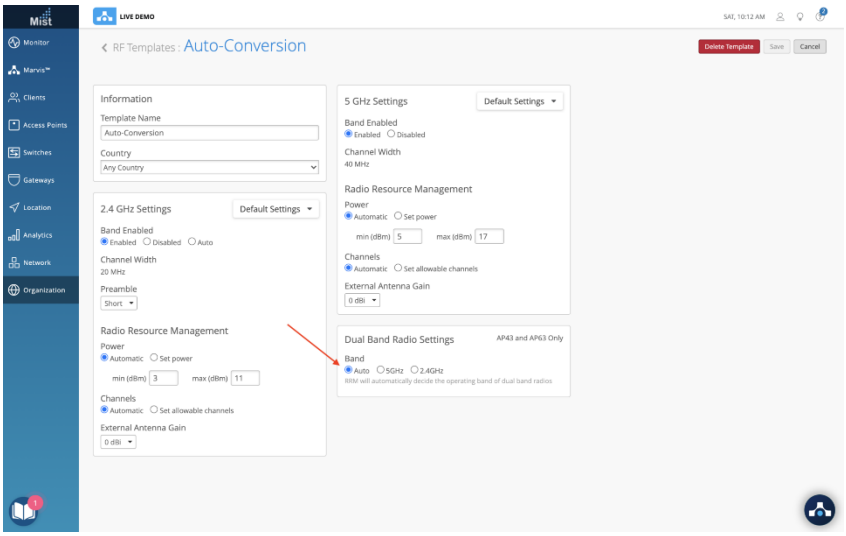
- Enterprise Deployment designed for high-density 5 GHz or 6 GHz

Take a typical enterprise deployment that has been designed for high-capacity 5 GHz or 6 GHz. If we look at the co-channel and density metrics on the Radio Management Site Summary (Site > Radio Management) for 2.4GHz, we see each AP has an average of 2.6 co-channel neighbors. The density metric is 1.0. This site would be a great candidate for auto cancellation or auto conversion.



To enable auto conversion, simply select “auto” under Dual Band Radio Settings in the RF Template and assign the RF Template to a site.

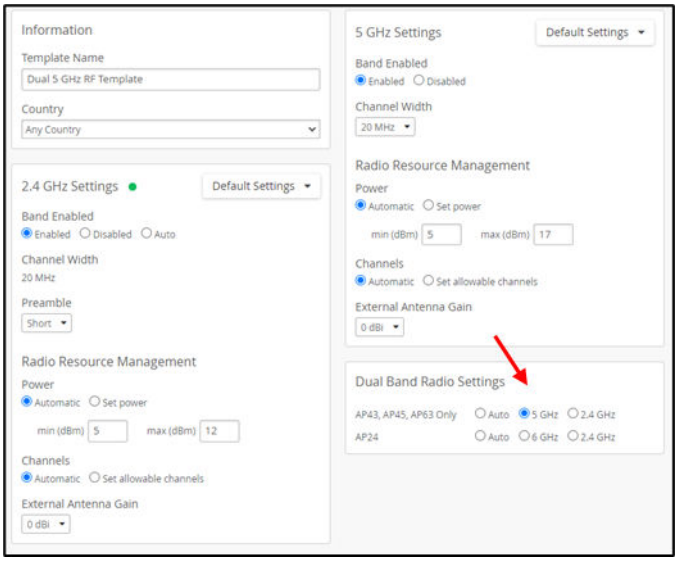
- Auditorium Deployment designed for high-density dual 5 GHz



The final example is an auditorium, conference room, or other area with higher-than-normal client density, where you may want to configure dual 5 GHz on all the APs in the site.

NOTE: If yours is a mixed environment where you want to enable dual 5GHz in some areas but not in others, then you need to leverage the device profile.

To enable dual 5 GHz radios, simply select the 5 GHz radio button in the Dual Band Radio Settings block as shown below.



SSID and Security Policy Configuration

- Service Set Identifier (SSID) and Security Policy Configuration are fundamental aspects of defining the wireless network's accessibility and security posture. This involves creating the various SSIDs that are broadcast by the Juniper Access Points. You can configure separate SSIDs for corporate users, guest access, and dedicated IoT devices. For each SSID, meticulous configuration of authentication methods is required, ranging from robust WPA2/3-Enterprise with RADIUS integration for secure user and device authentication to simpler Pre-Shared Keys (PSK) authentication or open networks for specific use cases. SSID and Security Policy configuration also includes:
  - Create SSIDs (for example, Corporate, Guest, IoT).
  - Configure authentication methods (WPA2/3-Enterprise, PSK, Open).
  - Integrate with RADIUS/Identity Management systems.
  - Implement dynamic VLAN assignment based on user/device roles.

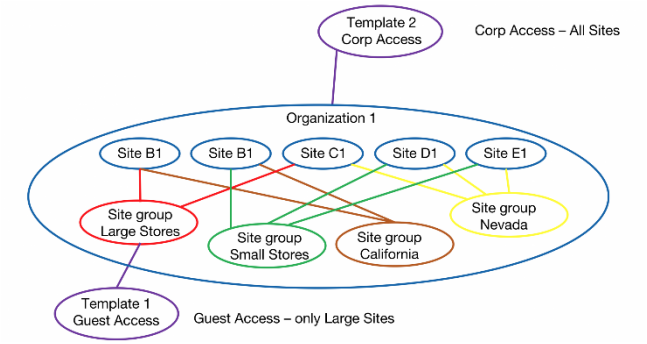
WLAN Templates

In Juniper Mist you can create the WLAN (SSID) either directly from the Site > WLANs page or from the WLAN templates page at Organization > WLAN Templates. The main benefit of using a WLAN Template is that the template can be assigned to one or more sites or an entire organization. This flexibility allows

for consistent, repeatable configuration at scale and enables fast changes to all APs at once. Direct WLAN configuration at the Site > WLANs level only applies to that single site.

Templates are very useful for automation, but not really if there is only 1 site. For example, a guest template could be created with a WLAN, a tunneling policy, and a WxLAN policy and applied to the entire organization. After application, every AP in the organization broadcasts the guest WLAN.

Consider an IoT template. This could, again, contain everything to enable IoT and be tied to a site group called IoT. When a new site is deployed, the IoT devices at that site become part of the site group, and the IoT WLAN is instantly available.

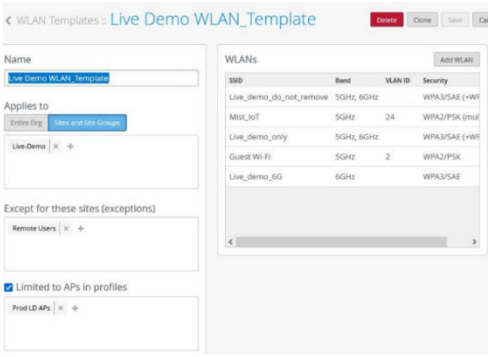


Configure a WLAN template

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

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

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



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

To create a WLAN template, follow the instructions here: Configure a WLAN Template.

See WLAN Options for information about the configuration options in WLANs and WLAN Templates.

Juniper WLAN Template Recommendation

General Guideline

WLAN configuration varies based on multiple factors such as user device compatibility, coverage, interference, capacity, and business requirements. In this section, we provide some examples of WLAN templates and WLAN settings using the best practices. Refer to Wi-Fi Design Fundamentals for considerations and recommendations for wireless band selection and planning.

WLAN Setting Guidelines

Below is the recommended common configuration for a WLAN.

- SSID: Make the name relative to the service you intend to provide (like Guest for guest network or Staff or Employee for employee services). It's not mandatory, but it helps the user connect to the right SSID.
- WLAN Status:**Enabled**—Allow the APs to broadcast the SSID
- Hide SSID:**Unchecked**—Some clients have issues connecting to hidden SSIDs.
- Radio Band: **Select (Check) all three bands if you have AP45s or AP34s that have all three radios available—**Enabling all three radio bands to provide better network capacity. If you have some APs that don't support 6 GHz, then select 2.4 GHz and 5 GHz only.

  Note: Enabling the 6 GHz radio band forces you to choose WPA3 or OWE as the SSID Security Type, thus eliminating the less secure options.

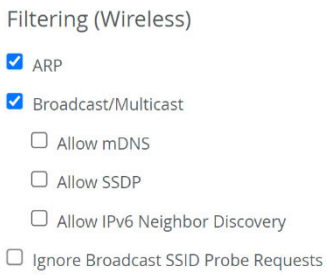
- Band Steering:**Disabled**—Many client devices have issues with band steering.
- Client Inactivity: keep the default value of 1800 because most clients and applications run smoothly with this setting.
- Geofence: For most deployments, keep it disabled except if you need to enable it.
- Data Rates: If you don't have legacy user devices in the network using this WLAN, select the option **High Density (disable all lower rates)**. This setting enhances the WLAN (SSID) utilization, enhances the client roaming experience, and reduces the occurrence of "sticky clients."
- WiFi Protocols: 6 GHz and 7 GHz are disabled by default. To use these protocols, you must have both APs and client devices that support them. Unless you have both APs and clients that support these protocols, leave them disabled.
- WLAN Rate Limit: (Disabled by default) We recommend leaving this disabled unless you have a specific need for it. For example, you could rate limit the entire WLAN, rate limit each client device or limit specific applications on a guest network to prevent guests from overutilizing the services, which could affect other guest users or the network in general.
- Apply to Access Points: This is set to All APs by default. Optionally, you can apply the template only to APs tagged with a specific label, such as lobby, or apply the template to a list of specific APs.
- Security:The setting you chose here is use-case dependent. The list below describes some of the use cases.
  - For staff and registered students, if your network uses an existing IDP or RADIUS for authentication, we strongly recommend configuring **WPA3-Enterprise**. Use **Mist Access Assurance** if available or configure a local RADIUS server.
  - For secure access in small deployments or when no IDP/RADIUS is available, use **WPA3-Personal (SAE)** or **WPA2-Personal (PSK)**. We strongly recommend **WPA3-Personal** for enhanced security, provided all client devices support it.
  - For guest access, use the built-in guest portal for landing and authentication. Set WLAN security to **OWE** or **Open Access**. We recommend **OWE** for stronger security, if supported by guest devices.
  - For IoT and BYOD deployments, use the **Multi-Pre-Shared Key (mPSK)** framework. We support both **WPA2** and **WPA3**:
    - **WPA2-mPSK** supports local AP-level lookup, cloud-based PSK, and RADIUS integration.
    - **WPA3-mPSK** currently supports **RADIUS-based lookup only**.
  - We recommend WPA3 where device compatibility is allowed for stronger encryption and policy enforcement.

    - To enable MAC Authentication Bypass (MAB), configure RADIUS lookup alongside SSID security settings such as **Open**, **OWE**, **WPA2-Personal**, or **WPA3-Personal**.

- VLAN: Juniper recommends assigning a dedicated VLAN per WLAN to minimize Layer 2 broadcast domains and improve performance and security. You can map the WLAN to a tagged VLAN, a VLAN pool, or a dynamic VLAN. Note that dynamic VLANs are supported only with WPA2 or WPA3-Enterprise security.

- Isolation: Isolation is disabled by default. Some use cases require client isolation on either the same AP or on the same Layer 2 subnet.

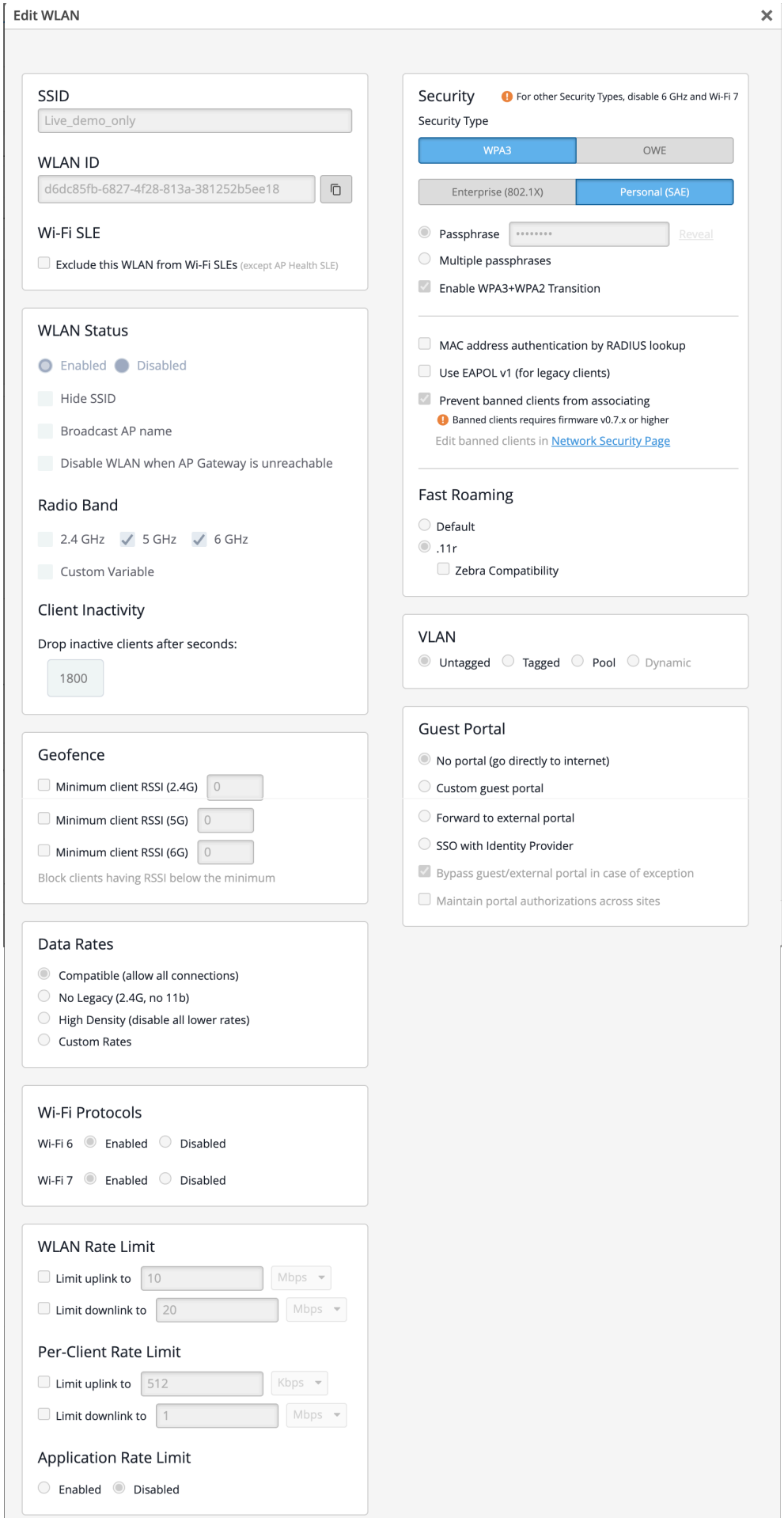
- Filtering: To optimize WLAN performance, enable ARP filtering and Broadcast/Multicast filtering. These settings reduce management frame traffic and free up radio airtime. Disable filtering only if required by specific application use cases.



- Custom Forwarding: By default, tagged or untagged client traffic is forwarded through the primary Ethernet port, Eth0. For distributed AP deployments, no changes are needed. For centralized deployments, alternative forwarding options will be covered in the next chapter.

- QoS Priority: The multimedia extensions, WMM and APSD, are enabled by default and should remain unchanged for most deployments. For specific use cases, you may override QoS settings to map all WLAN traffic to a defined priority level, such as Background, Best Effort, Video, or Voice.

- Bonjour Gateway: By default, this feature is disabled. Enable Bonjour Gateway for use cases like media or printer sharing in schools, or IPTV sharing in hotel rooms. To configure, select the desired service (for example, AirDrop, AirPlay, AirPrint, Amazon devices, GoogleCast, etc.), then define the service scope as AP, Site, or Floorplan.

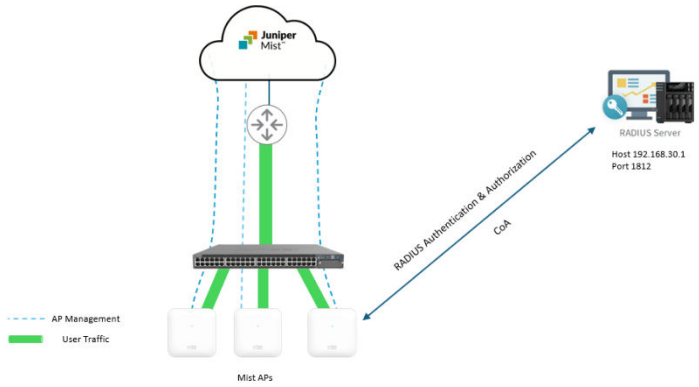

Edit WLAN
SSID
Live_demo_only
WLAN ID
d6dc85fb-6827-4f28-813a-381252b5ee18
Wi-Fi SLE
Exclude this WLAN from Wi-Fi SLEs (except AP Health SLE)
WLAN Status
Enabled
Disabled
Hide SSID
Broadcast AP name
Disable WLAN when AP Gateway is unreachable
Radio Band
2.4 GHz
5 GHz
6 GHz
Custom Variable
Client Inactivity
Drop inactive clients after seconds:
1800
Geofence
Minimum client RSSI (2.4G)
0
Minimum client RSSI (5G)
0
Minimum client RSSI (6G)
0
Block clients having RSSI below the minimum
Data Rates
Compatible (allow all connections)
No Legacy (2.4G, no 11b)
High Density (disable all lower rates)
Custom Rates
Wi-Fi Protocols
Wi-Fi 6
Enabled
Disabled
Wi-Fi 7
Enabled
Disabled
WLAN Rate Limit
Limit uplink to
10
Mbps
Limit downlink to
20
Mbps
Per-Client Rate Limit
Limit uplink to
512
Kbps
Limit downlink to
1
Mbps
Application Rate Limit
Enabled
Disabled
Security
For other Security Types, disable 6 GHz and Wi-Fi 7
Security Type
WPA3
OWE
Enterprise (802.1X)
Personal (SAE)
Passphrase
Reveal
Multiple passphrases
Enable WPA3+WPA2 Transition
MAC address authentication by RADIUS lookup
Use EAPOL v1 (for legacy clients)
Prevent banned clients from associating
Banned clients requires firmware v0.7.x or higher
Edit banned clients in Network Security Page
Fast Roaming
Default
.11r
Zebra Compatibility
VLAN
Untagged
Tagged
Pool
Dynamic
Guest Portal
No portal (go directly to internet)
Custom guest portal
Forward to external portal
SSO with Identity Provider
Bypass guest/external portal in case of exception
Maintain portal authorizations across sites

Juniper WLAN Template Examples

In the previous section, we provided information about template settings, their defaults, and some best practices. In this section, we provide template use case examples to further illustrate best practices in specific scenarios.

Enterprise (802.1x) Based WLAN for Authorized Users

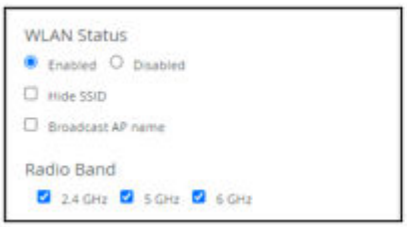
In this example, we configure a WLAN with Juniper best practices and recommendations. We use previously deployed, local RADIUS services. The illustration below explains the network architecture.



First, we apply the best practices settings shown in the list below

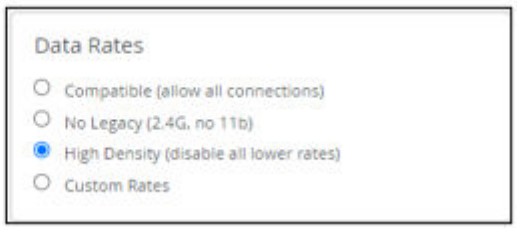
- Create a WLAN Template as explained earlier and add a WLAN to the template.
- In the WLAN settings, set the SSID name to **Staff**.

- Leave the WLAN Status set as **Enabled**.
- Enable all three Radio Bands (2.4, 5 and 6 GHz)

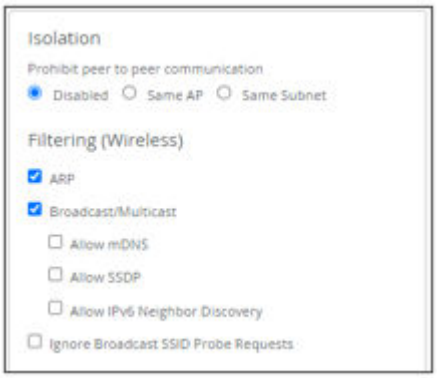


- Ensure all Geofence checkboxes are disabled (not checked).

- Select **High Density (disable all lower rates)** in the Data Rates block to avoid legacy devices and enhance network performance.
- Enable WiFi-6 in the WiFi Protocols block.

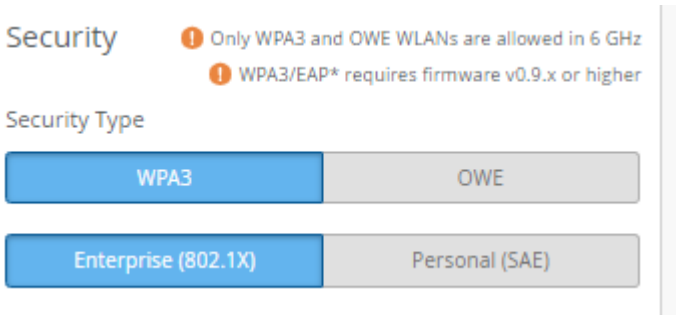


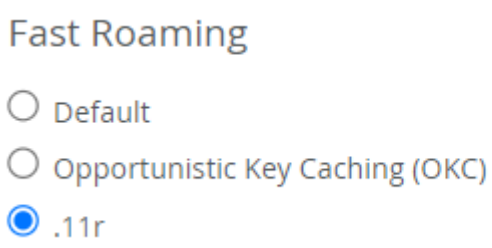
- In the Isolation block, enable the **ARP**, **Broadcast/Multicast**, **and Allow mDNS** checkboxes in the Filtering (Wireless) as shown below:



Leave the rest of the configuration blocks on the left side to set to their default values.

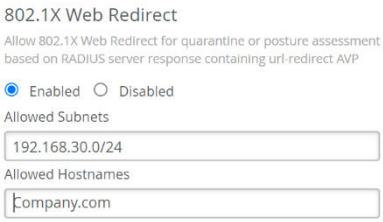
- In the **Security** block of the Create WLAN window:
  - Select **WPA3** as the Security Type
  - Select **Enterprise (802.1X)**
  - In the Fast Roaming section, enable .11r



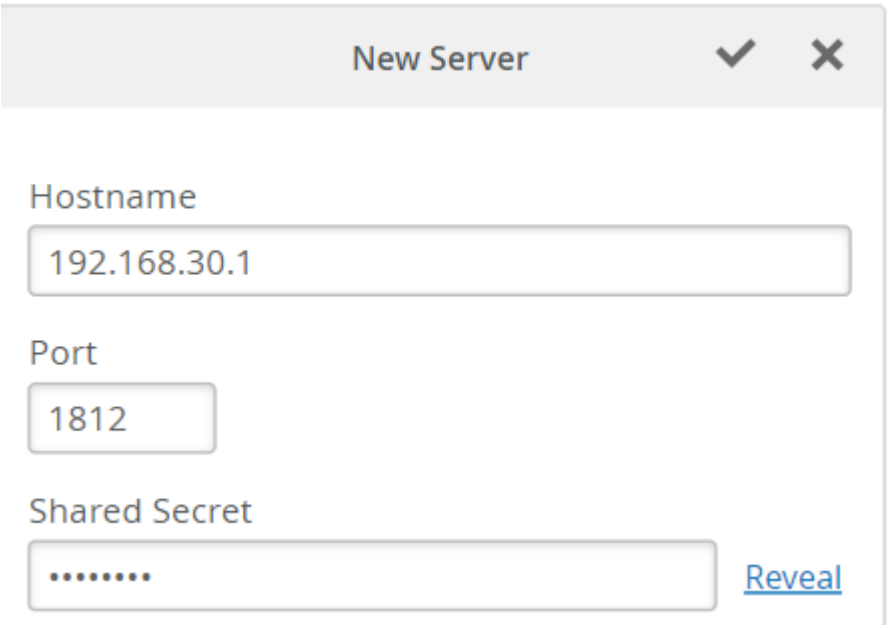


This setting is recommended if all your client devices support it. If not, enable Default.

- In the 802.1X Web Redirect block, you can opt to redirect clients to a webpage, such as a **quarantined portal**, after they complete the 802.1X authentication. Note: The 802.1X Web Redirect box is available only for WLANs with security type Enterprise (802.1X). You can use the web redirect feature to give clients full or partial access to the network. This feature enables you to perform compliance checks on clients with agents installed. During client authentication, the RADIUS server sends an Access-Accept message containing a URL-redirect 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 within the portal, it is fully authorized and allowed to start passing traffic.
    - If you want to use the web redirect feature, select **Enabled** in the 802.1X Web Redirect section. Then, specify the allowed subnets and allowed hostnames accessible to the clients being redirected.

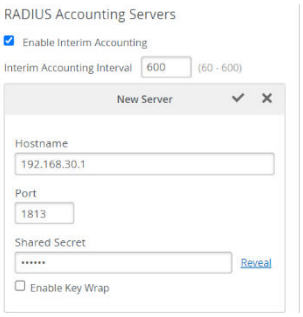


- In the Authentication Servers block, select RADIUS as the server type. Note: The Authentication Servers configuration block is available only when you've selected **WPA3** and **Enterprise (802.1X)** under Security Type.
- Click **Add Server** under RADIUS Authentication Servers.
    - Type the IP address or DNS name of the RADIUS server in the **Hostname** field
    - The port number field defaults to 1812. Change it if needed.
    - Enter a shared secret then click the check mark (√) to save this RADIUS server.

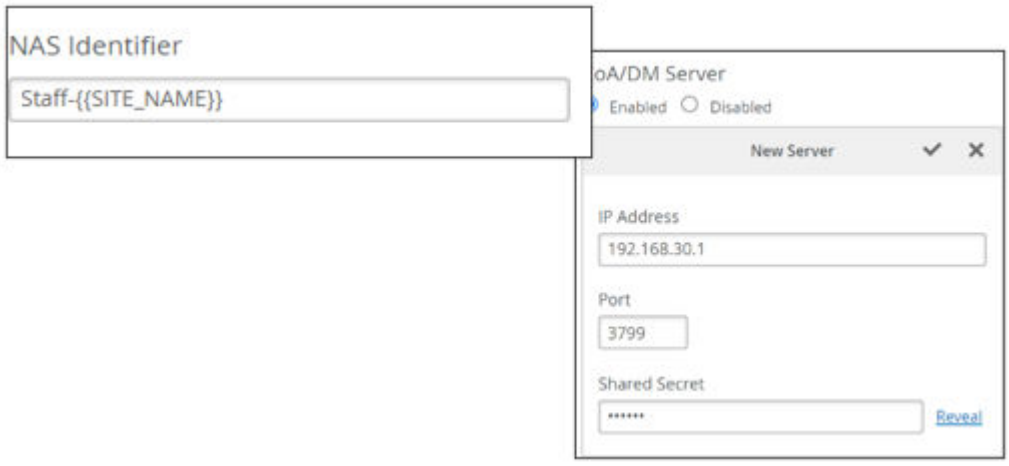


NOTE: You can add multiple RADIUS servers for redundancy.

- Click Add Server under RADIUS Accounting Servers.
  - Add the Accounting Server(s) in the same way you added the authentication server(s). In most cases, the accounting server is the same as the authentication server.
  - Select (check) Enable the Interim Accounting so the AP can send periodic updates to the accounting server during the lifetime of user sessions. If it's not enabled, the AP will send updates only at the start and end of the user sessions.
- Optionally, you can configure the **NAS Identifier** attribute. The NAS-Identifier is a user-configurable attribute value pair (AVP) that could be unique per WLAN configuration. All Mist APs configured with this WLAN send the NAS-Identifier value. Note that Mist Cloud allows dynamic payload configuration, such as sending the current AP hostname, Site name, AP MAC address, or AP model using pre-defined variables. See Configure Site Variables for information about variables. In this example, we set the NAS-Identifier to the name of the WLAN and the assigned Site name, using a variable, as shown below.



- In the CoA/DM Server block, you 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.

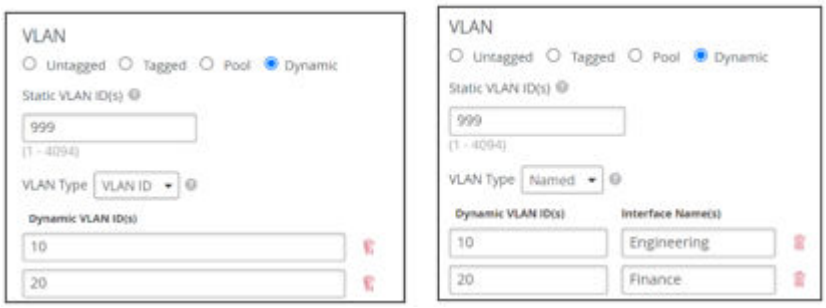


- In the VLAN block, select Tagged (static) or Dynamic. For Dynamic, we support Named VLAN (Airespace-Interface-Name) or VLAN ID. The images below depict example configurations using each method. The best method for your network depends on the capabilities of your RADIUS server.

After applying the above configuration, click **Save** in the Edit WLAN window.

Client Onboarding WLAN

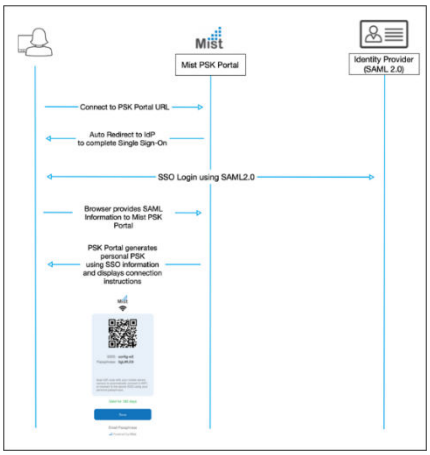
For client onboarding, Juniper Mist provides automation and simplifies the process of secure wireless connectivity by leveraging the mPSK (Multi pre-Shared Key) capabilities provided by BYOD (SSO) using a simple portal to allow clients to provision access without IT involvement.



Benefits from Client onboarding – PSK portal:

- Automate client onboarding with a simple click-and-go flow.
- No legacy on-prem servers or appliances.
- Full control of onboarded clients including role based, validity and number of concurrent devices per PSK.
- Visibility into the usage of each PSK.

The Juniper Mist client onboarding portal allows users to self-provision their devices using multiple PSKs, in a BYOD portal, with simple portal redirection. The portal prompts the user to enter their credentials, and then an automated PSK is generated for that specific user according to configured Organization policy. The diagram below illustrates the workflow of the self-provisioning process.



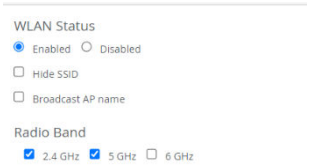
- Prerequisites
  - You must have a Mist Access Assurance subscription if you are planning to use cloud-PSK
    - S-Client-S-Y
    - The Y reflects the number of years in the subscription 1, 3 or 5 years.
  - mPSK ORG level SSID (WLAN) configured.

- SAML 2.0 Identity Provider with SSO

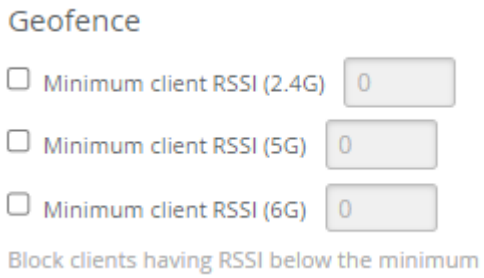
Create the WLAN Template as explained earlier and add a WLAN in the template as shown in the steps below.

- In the SSID block:
  - Name the SSID BYOD. The name is not mandatory, it's easy to remember for this example.

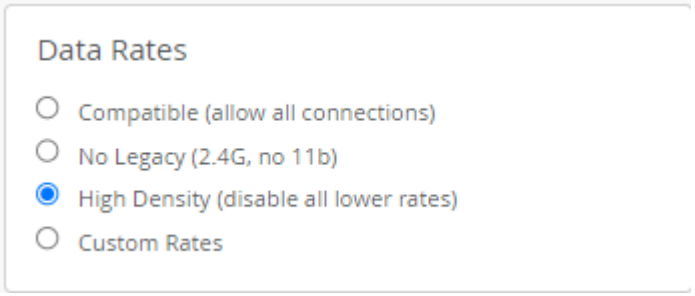
- In the WLAN Status block:
  - Leave the WLAN **Enabled**.
  - Select **2.4 GHz** and **5 GHz** in the Radio Band section.



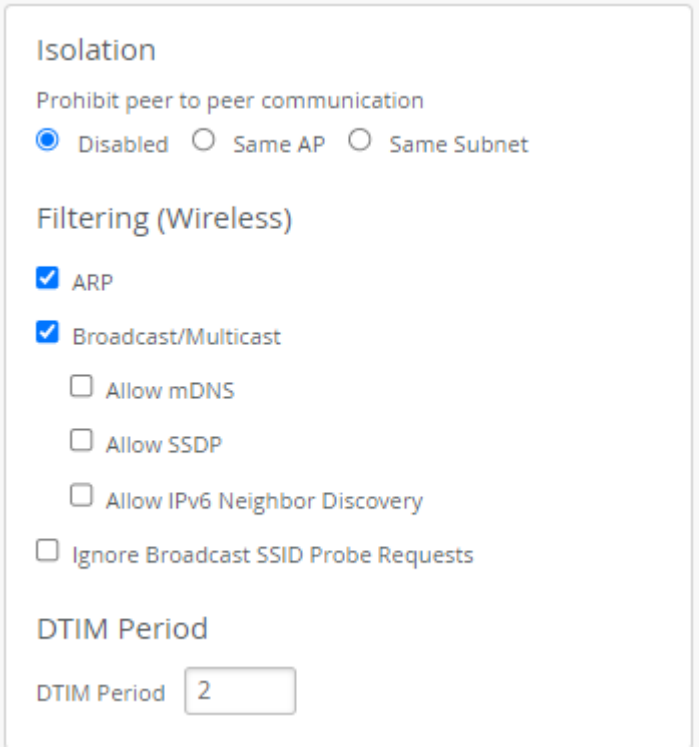
- In the Geofence block:
  - Leave everything disabled (unchecked).



- In the Data Rates block:
  - Enable (select) **High Density (disable all lower rates)**. This excludes legacy devices and enhances network performance.

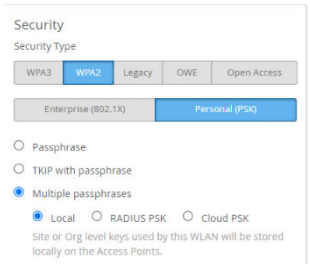


- In the WiFi Protocols block:
  - Leave WiFi-6 and WiFi-7 **Enabled.**
- Leave the WLAN Rate Limit block and Apply to Access Points blocks as-is.
- In the Isolation block set Filtering (Wireless) to:
  - Enable ARP.
  - Enable Broadcast/Multicast.



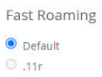
- Leave the remaining blocks down the left side of the Edit WLAN window as-is (keep the default values).
- In the Security block:
  - Select **WPA2**, the supported encryption for mPSK with SSO onboarding).

- Select **Personal (PSK).**
- Select **Multiple passphrases** and **Local**. Local or Cloud PSK would work here. We use Local for this example.



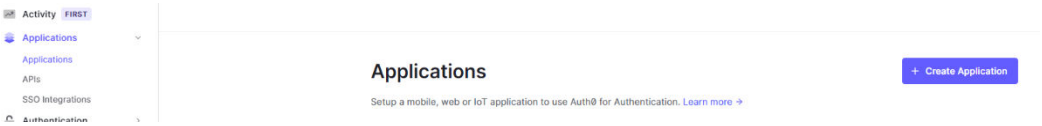
- In the Fast Roaming section, leave **Default** selected.
- In the VLAN block, select **Tagged**.

With those settings complete, you are ready to start the onboarding client configuration process. You must have an account with one of the identity providers that supports SSO and SAML 2.0 with user accounts. To allow users to onboard themselves, they must authenticate using their SSO. In this example we use auth0 as the SSO provider, but you can use any standard SSO provider with SAML 2.0 support.

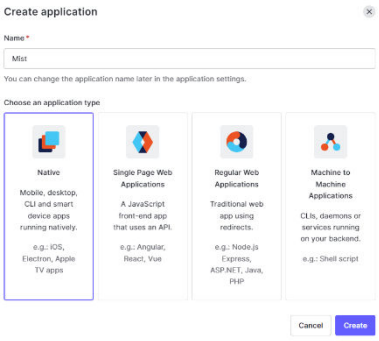


To start, you must have an account with auth0. If you don't have an account, register and create an account at https://auth0.com/signup?place=header&type=button&text=sign%20up.

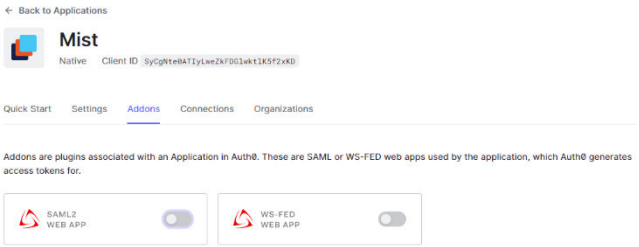
- After you create an account, login to auth0 using the new account.



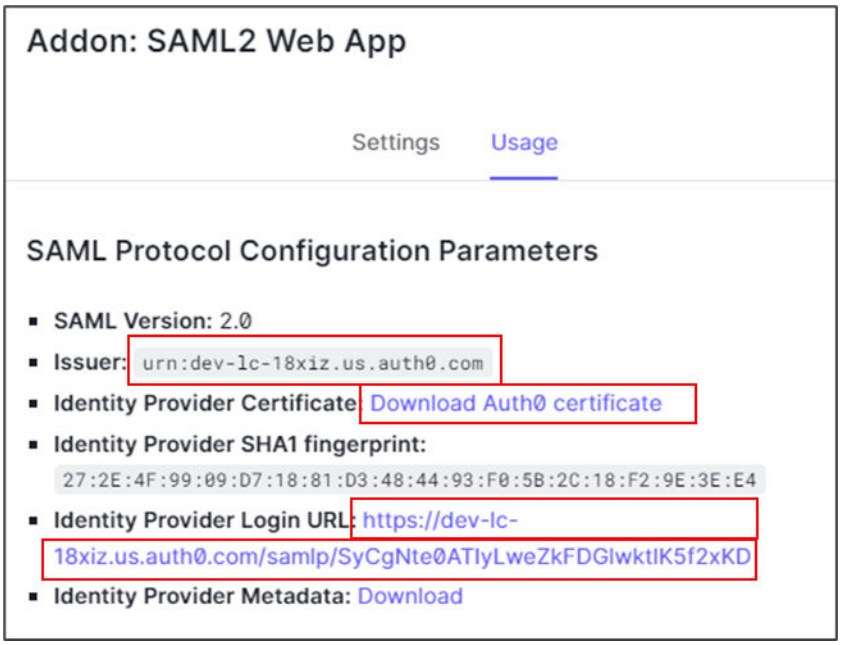
- Select **Applications** > **Applications** from left side main menu
- Create an Application.
- Name your application Mist.



- Select the application you just created and click the Addons tab.
- Enable SAML2 Web App.



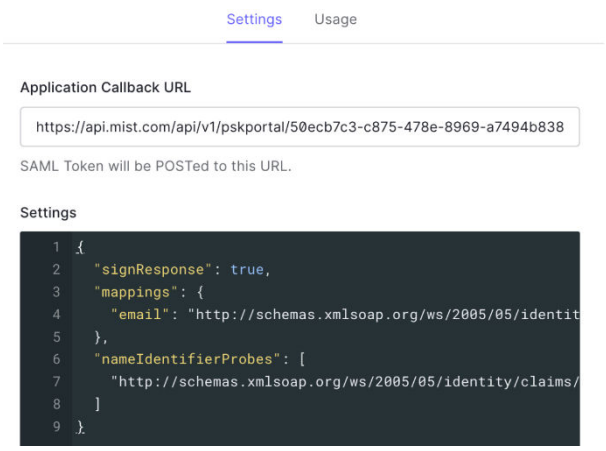
- Under the Usage tab on the Addon page, the SAML2 Web App Parameters display the **Issuer**, **Identity Provider**, and **Identity Provider Login URL**, all of which are required in the Mist portal for onboarding.
- Download and save the Identity Provider Certificate. Keep the other information handy for use in upcoming steps.



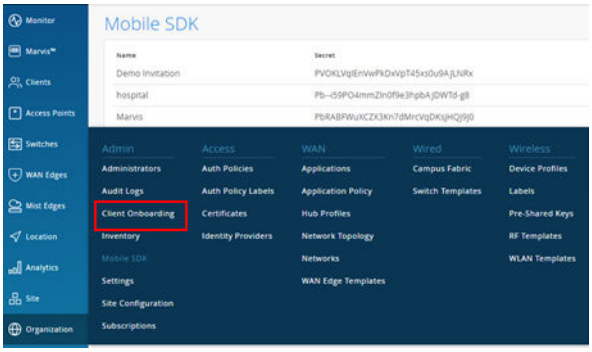
- Select the Settings tab and paste the text below into the Settings window to replace (overwrite) the existing text in the window.

```
{
  "signResponse": true,
  "mappings": {
    "email": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/userEmail"
  },
  "nameIdentifierProbes": [
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/userEmail"
  ]
}
```

The result appears as shown below:

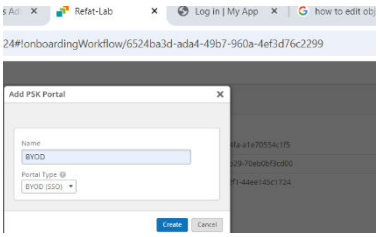


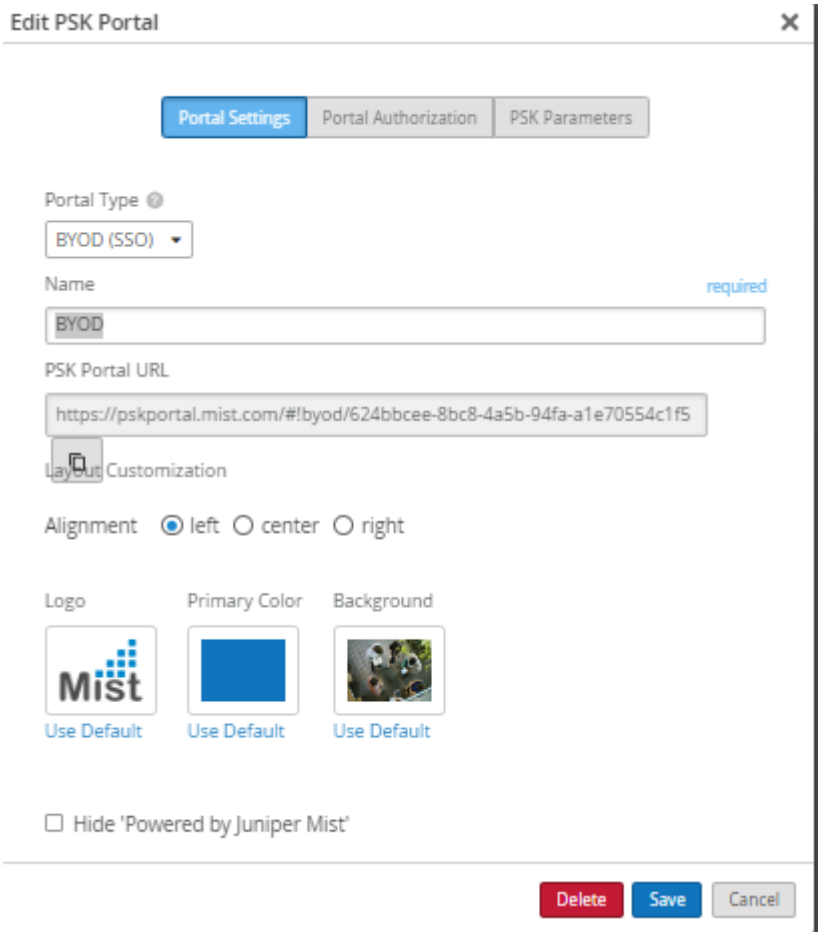
- Open a new tab in your browser and log in to your Mist portal at https://manage.mist.com.
- Go to **Organization** > **Access** > **Client Onboarding**.



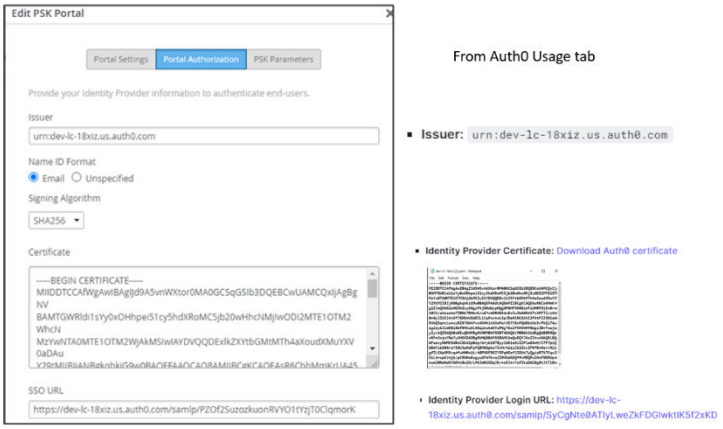
- Click **Add PSK Portal**. The **Edit PSK Portal** window appears.

- On the Portal Settings tab, enter a name for your PSK portal. For this example, call it BYOD and select **BYOD (SSO)** as the Portal Type.

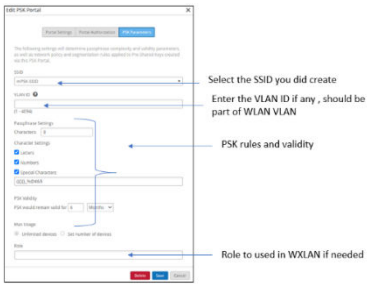




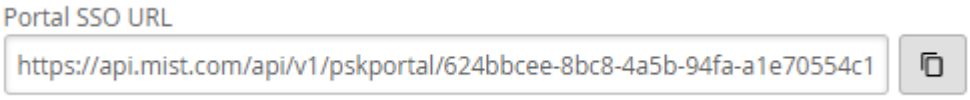
- On the Portal **Authorization** tab, fill in the information as shown below. Use the information saved from the **Auth0** > **Mist App** > **SAML2 Web App Addons** > **Usage** window above.



- Select the **PSK parameters** tab and fill in the information as illustrated in the figure below.



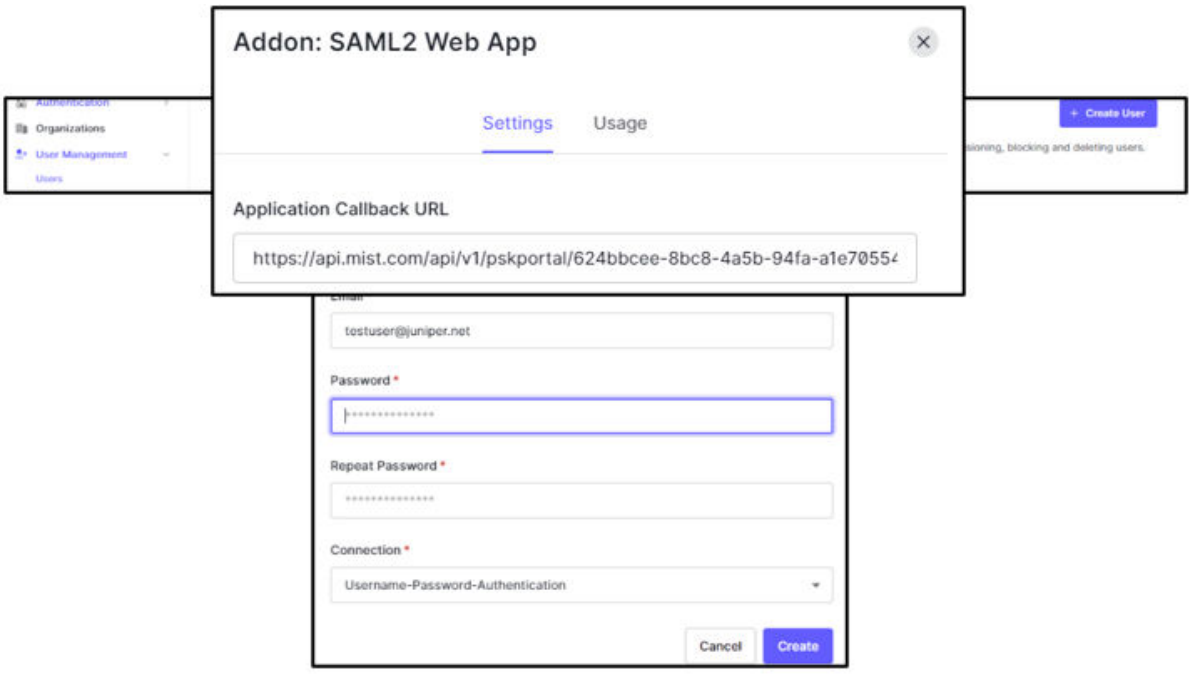
- After this step, save the configuration and open the configuration again, you will notice a new file has been generated. Copy the link as you need it in the next step, now go back to the auth0 tab in your browser from the previous step.



- In the Auth0 application you created previously, select the Settings tab. In the Application callback URL, past the URL link you copied (from the Mist > Client Onboarding > Edit PSK Portal) in the previous step.
- Enable the configuration in Auth0. This takes you back to the main screen where you click Save.

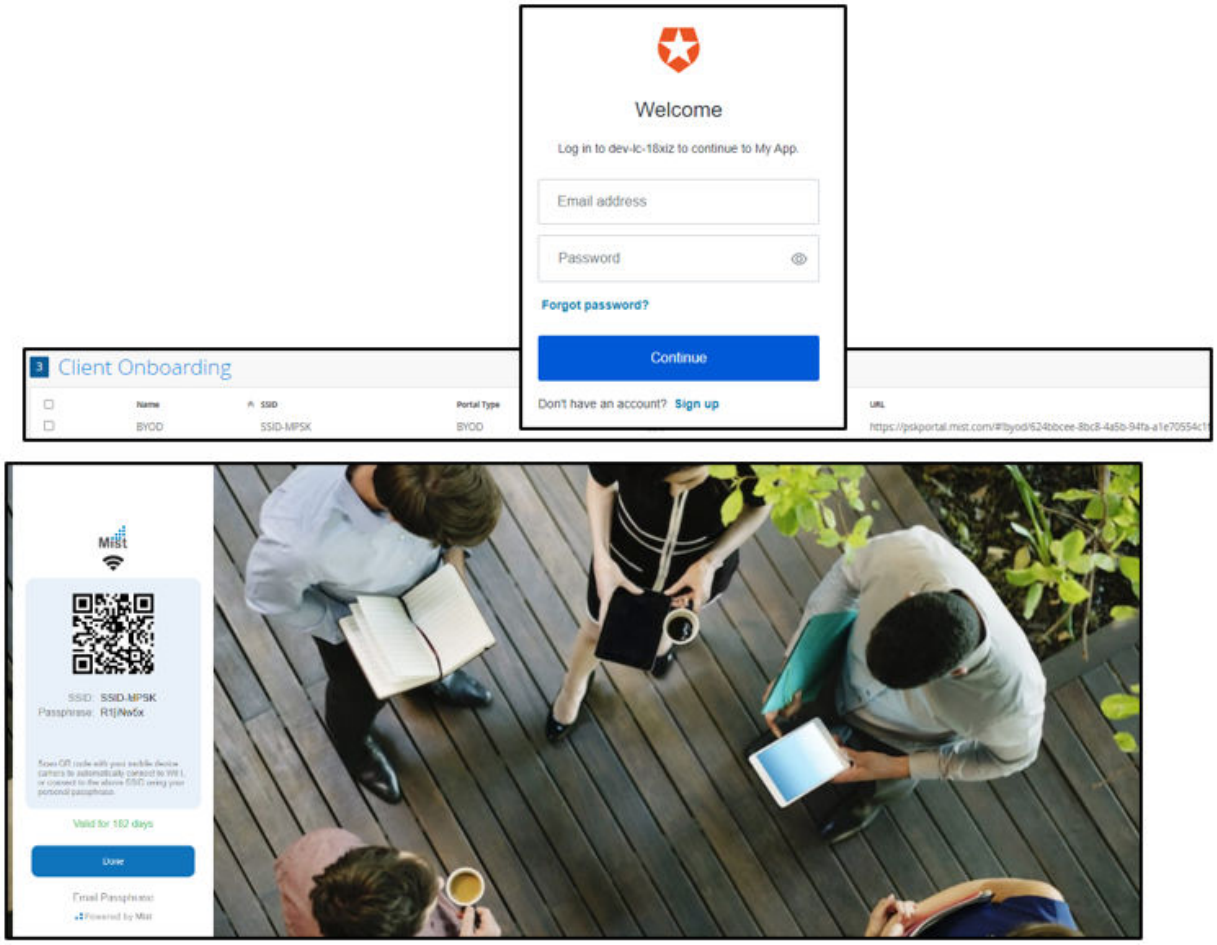
Now, we create a test user in Auth0. If you already have users in Auth0, you can skip this step.

- Select **User Management** > **Users** from the left menu. Click + **Create User**.



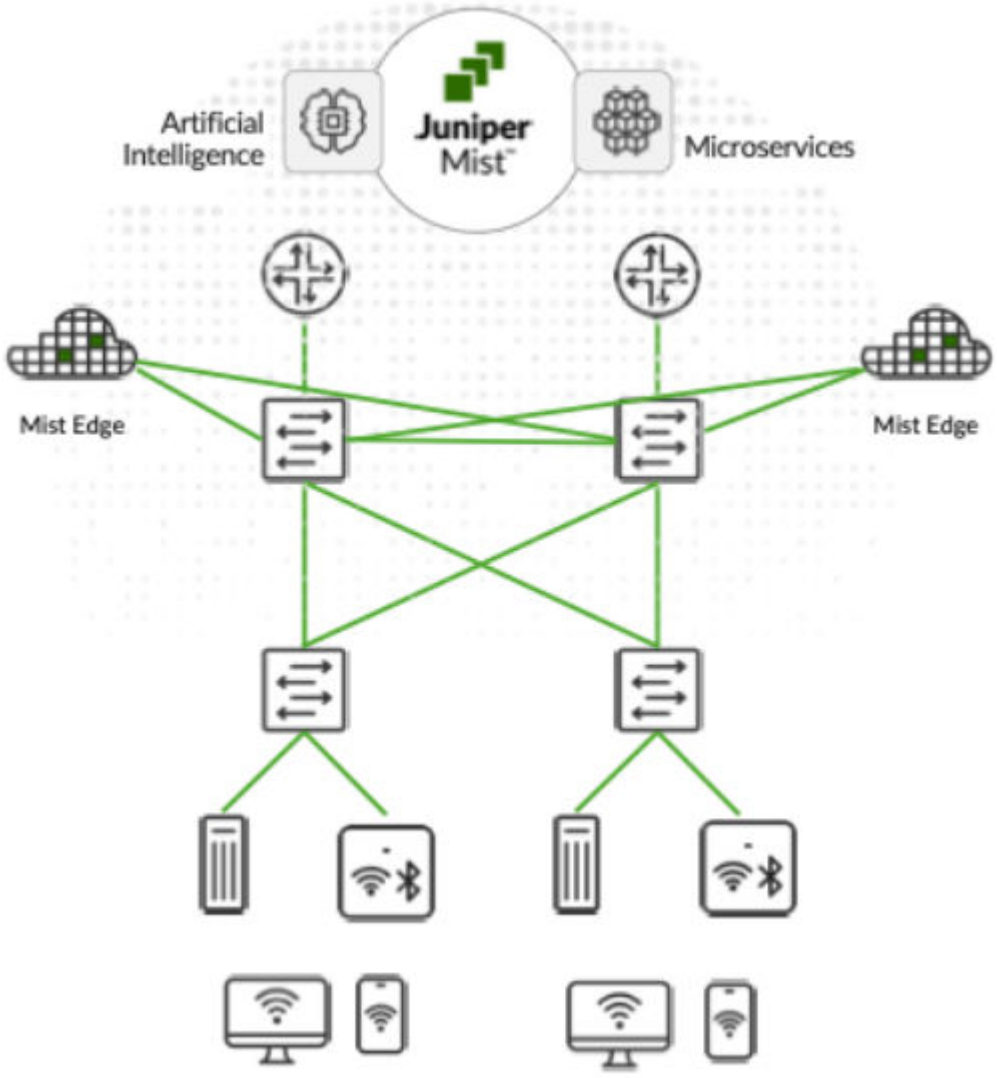
- Enter the **Email** and **Password** of your choice. Confirm the password if needed and click Create.

This completes the required configuration. When you open Mist Client Onboarding, the client list appears similar to the image below. Note that all the fields are filled out.



Upon logging in, the user is directed to the Auth0 SSO page for authentication. Upon successful authentication, the system redirects you to the Mist onboarding portal, where you can scan your code using your mobile and configure the SSID. Optionally, you can copy the information if no barcode scanning is available on your device. An email is sent to the user upon completion.

As mentioned previously, we have two main deployment approaches, distributed and centralized (tunneled). We explained the fundamental configuration for the distributed approach previously. In this section, we explain how to configure the centralized deployment.



The Mist solution leverages Mist Edge devices for cases that need to retain a centralized datapath architecture for Campus and Branch deployments. These tunneled deployments provide the same level of redundancy and access to corporate resources, while extending visibility into user network experience and streamlining IT operations.

Juniper APs can form L2TPv3 tunnels to extend one or more VLANs from one or more Mist Edge devices located in Campus, Datacenter, or DMZ simultaneously. APs can support both local and centralized datapath at the same time.

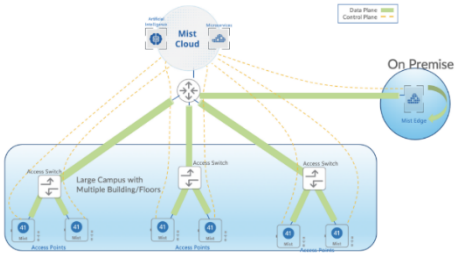
How it works

The centralized solution leverages Mist Edge devices for extending centralized corporate, production, or guest VLANs to APs using L2TPv3 tunnels. The Mist cloud orchestrates the Mist tunnel; the datapath is maintained in the event the Mist Edge's or AP's cloud connectivity to the Mist cloud is lost.

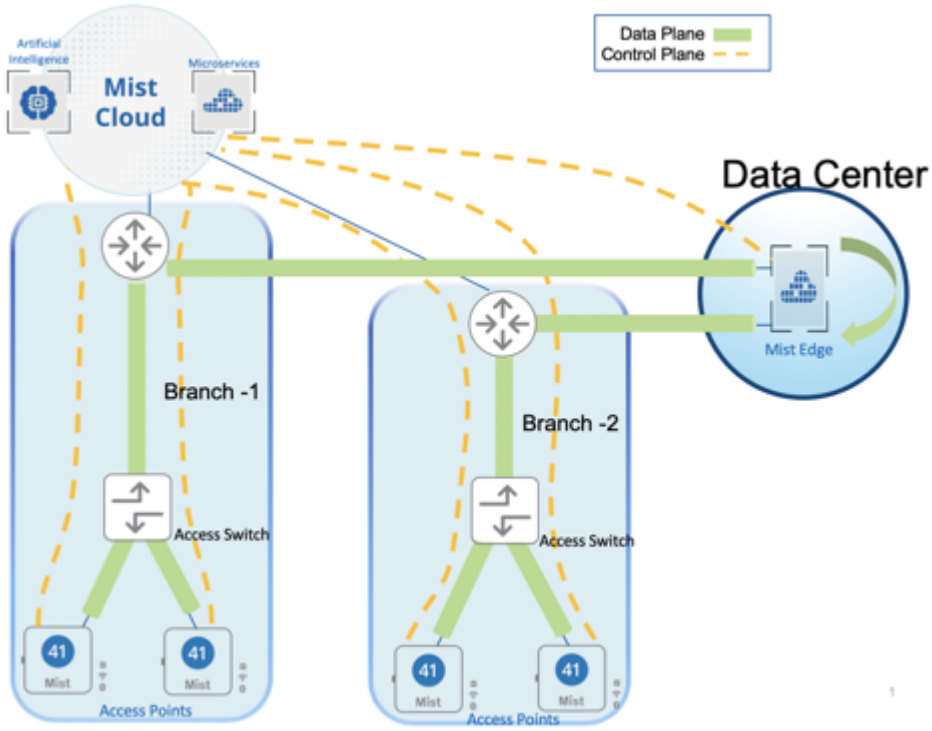
- Mist Edge is based on multi-service architecture, so individual services can be upgraded as and when required with a 3-second downtime, with no need for a reboot.
- AP firmware and Mist Edge service version are decoupled; upgrading a Mist Edge device's firmware does not also require an AP firmware upgrade.
- APs can form multiple tunnels to different Mist Edge clusters in the Site, the DMZ and the datacenter. You can map user traffic to be tunneled or locally bridged based on RADIUS attributes returned for 802.1x authenticated wireless LANs.
- APs can support tunneled and locally-bridged WLANs simultaneously. WLAN types are not mutually exclusive.
- Mist's cloud-driven AI provides unprecedented user-experience visibility through the Service Level Expectations (SLE) framework and the AI-driven Marvis Engine that includes natural language processing for troubleshooting and root cause analysis, along with Marvis Actions. IT teams can leverage these Marvics features for remote troubleshooting of user issues.

In the centralized approach, we can employ either of two different use cases as shown below:

- Enterprise or campus



- Teleworkers and remote offices.



Mist Edge Configuration Components

Mist Edge offers a simple, yet powerful configuration scheme orchestrated by the cloud. The configuration objects needed to deploy Mist Edge in your network are discussed below:

- Mist Edge—Hardware or virtual appliance. Just like Juniper APs, Mist Edge hardware appliances come with a claim code that can be used in the Mist portal or scanned by a mobile app to add Mist Edge devices to an organization's inventory. Within the Mist Edge configuration, you configure the Tunnel IP, which is the IP address or hostname, with which APs will form tunnels.
- Mist Edge Cluster—Mist Edge devices must be a part of a cluster to actively terminate tunnels from APs. A Mist Edge cluster can consist of one or more Mist Edge devices. Under normal operation, the members of a cluster are in active-active mode and load balance all the AP tunnels. The Mist GUI allows you to configure only a primary and secondary cluster. However, using the API, there is no limit to the number of Mist Edge clusters that you can configure.
- Mist Tunnels—The Mist tunnel object contains attributes that determine the tunnel protocol, endpoints, tunneled VLANs, failover timers, and more. The tunnel configuration decides the primary cluster and secondary cluster for AP tunnel termination. APs will load balance across Mist Edges in the primary cluster.

Mist Edge Onboarding

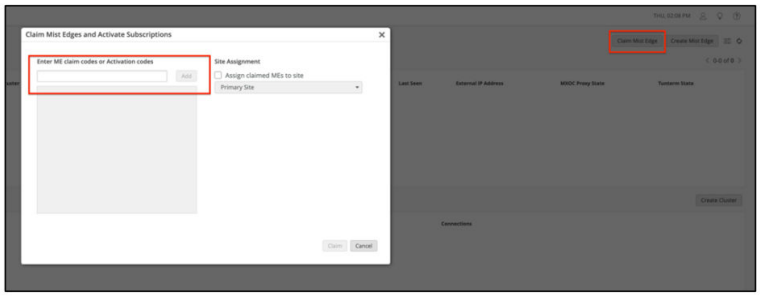
> **NOTE**: Verify your Mist Edge subscription before moving forward with configuring Mist Edge devices to avoid any subscription-related issues. You can verify Mist Edge subscription status by selecting the **Summary** tab on the **Organization** > **Subscriptions** page in the Mist portal. Contact your Juniper Mist partner or representative who can help by getting a quote for adding the Mist Edge subscription or raising a request for trial subscription.Mist Edge subscription is entitled on per AP basis, each AP tunneling requires a Mist Edge subscription.

Mist Edge onboarding is straightforward. There is no need for pre-staging. Mist Edge devices can be shipped directly to the branch or campus, installed, and brought online.

Claim on the Mist Dashboard

From the left-nav menu in the Mist portal, go to **Mist Edges** > **Mist Edges Inventory** > **Claim Mist Edge**.

Enter the claim code, which is provided on the purchase order or can be seen in the appliance pull-out tag. Alternatively, you can scan the QR code using the Mist AI app on Android or Apple mobile phones to claim individual devices.



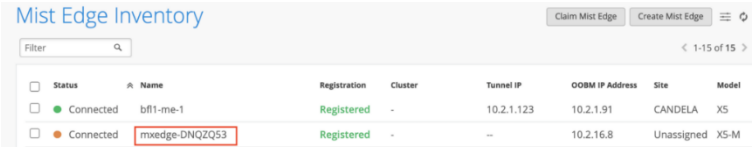
After you claim a Mist Edge device, it shows Disconnected and Registered on the Mist Edges page in the Mist portal.

Setup Mist Edge

Mist Edge devices typically reside in the DMZ, Data Center (DC), or Campus with one arm connected to the Internet, and another arm connected to a trusted network. You must understand the physical port connections of Mist Edge devices before proceeding with configuration.

Physical Port Connections Overview

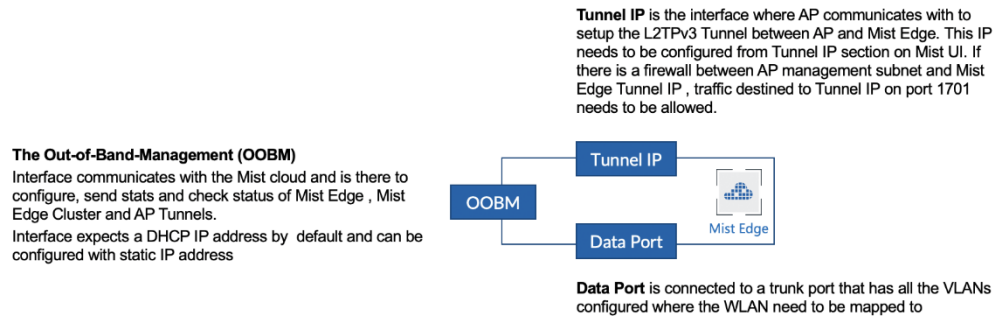
The following illustration shows Mist Edge port configuration requirements:



NOTE: We strongly recommend that you configure the OOBM and the Tunnel Termination IP addresses on different subnets.

Configure OOBM

Connect the Out-Of-Band-Management (OOBM) port of the Mist Edge to an access-mode interface on your switch. Mist Edge devices use the OOBM port to communicate with the Mist cloud for configuration, telemetry, and lifecycle management. The following image shows the OOBM and other ports on a Mist Edge X1 appliance.



NOTE: The OOBM port on the Mist Edge appliance is marked MIST. By default, the OOBM port is configured for DHCP. There are two ways to configure static IP depending on your network.

To configure a static IP, you can configure this from the Mist Dashboard. If your network has DHCP, it is recommended to first connect using DHCP to the cloud and then use the Dashboard to configure the static IP:

Go to **Mist Edges** > **OOBM IP Address**.

For Mist Edge to communicate with the Mist cloud, specific FQDNs and ports must be allowed for the OOBM interface. Refer to this link for the most up-to-date information: https://www.juniper.net/documentation/us/en/software/mist/mist-management/topics/ref/firewall-ports-to-open.html. You must use the region-specific FQDNs listed on that page since the IP addresses will change. Once the OOBM is configured and the firewall rules are in place, Mist Edge displays on the Mist Edge Inventory page as **Connected** (with an Amber dot as shown below).

In case the Mist Edge does not show connected even after 5 minutes, you can SSH to the Mist Edge appliance using the OOBM IP address. Once connected through SSH, you can use the device's CLI to troubleshoot connectivity issues.

Configure Tunnel Termination Services

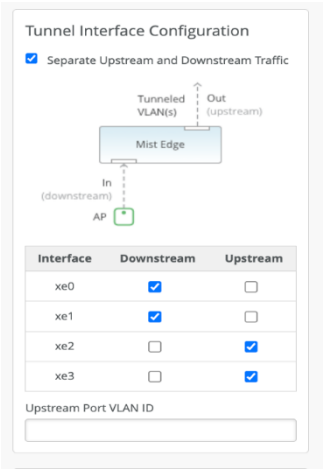
The Tunnel Termination Service listens to APs to request an L2TPv3 tunnel connection. The service is automatically installed once the Mist Edge is fully configured.

To prevent network disruptions, do not enable the switch connections to the Mist Edge data ports until after the Mist Edge device receives a Tunnel IP address, and the tunnel is configured.

Dual Arms

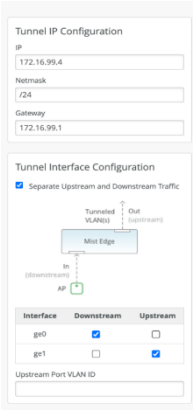
Mist Edge devices have multiple tunnel (data) ports, which you can configure as single-arm or dual-arm connections. When you select **Separate Upstream and Downstream Traffic** on the Mist Edge setting page if you create a dual-arm configuration. Assign the interfaces for upstream and downstream traffic as needed. In the example below, we show a Mist Edge X5-M or X10 on the left and a Mist Edge X1 on the right. The difference in Mist Edge devices appears in the name and number of available interfaces.

You connect interfaces xe0 and xe1 from the X5-M (or ge0 from the X1) to the Downstream (AP, public, or untrusted) side of the Mist Edge. L2TPv3 tunneled VLAN traffic enters the Mist Edge device at these connections from the APs. Interfaces xe2 and xe3 (or ge1) connect to the corporate (trusted) network and carry the tagged VLAN (user) traffic.



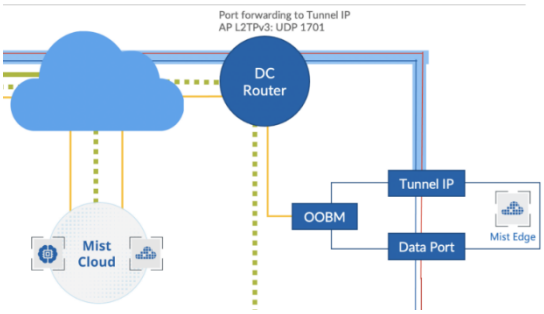
The **Upstream Port VLAN ID** is optional and should only be used when the upstream switch port is configured as an access port with a single, untagged VLAN.

For the tunnel IP configuration, add the IP address, subnet mask, and gateway as shown below. For a campus and branch deployment, the AP must be able to route to the Tunnel IP.

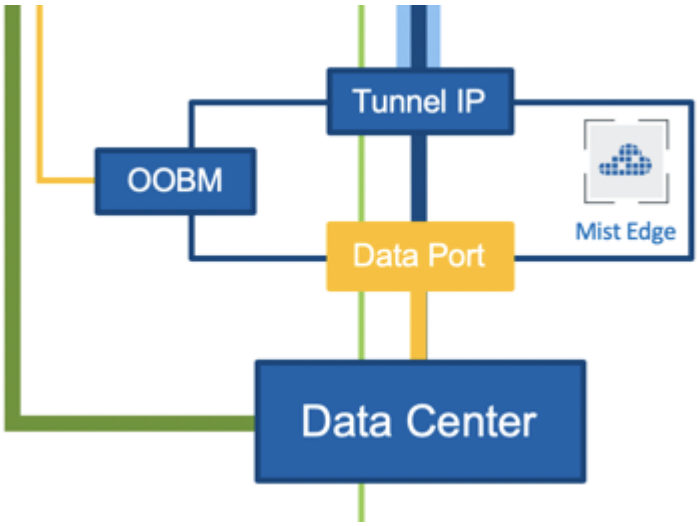


The Tunnel IP SVI on Mist Edge is a protected interface. Even if it is not connected to a firewall, the only open ports are UDP ports 1701 (L2TPv3), UDP 500 (isakmp), and UDP 4500 (IPsec), along with TCP port 2083 (RADSEC).

Mist Edge only uses UDP ports 500 and 4500, along with TCP port 2083 for the remote worker use case. For all other campus and branch use cases, Mist Edge only uses UDP port 1701.



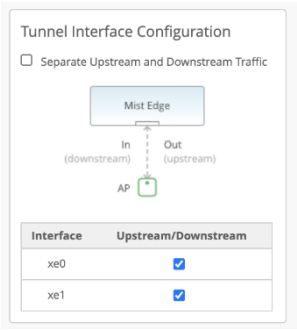
As mentioned previously, upstream ports are connected to the trusted side of the network. These ports typically connect to your core (or aggregation) switch on a trunked port, configured to allow all the necessary user VLANs. Mist Edge carries L2-tagged traffic from the tunnels to here.

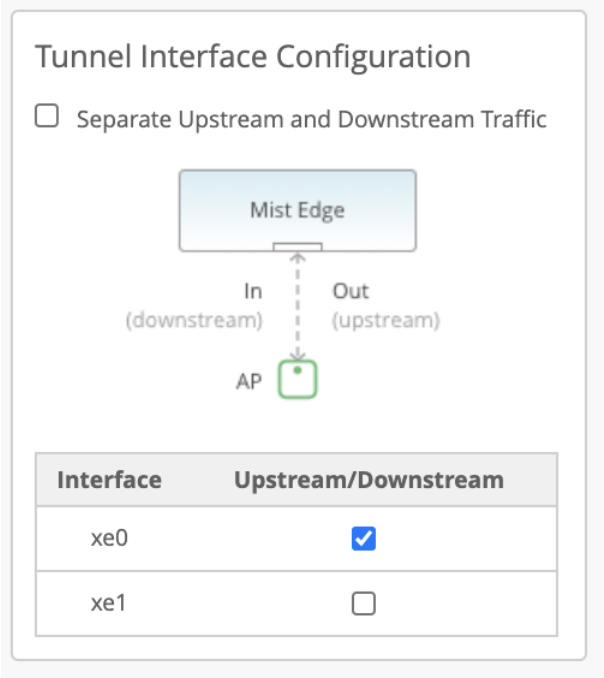


The downstream port is connected to the untrusted side of your network that typically goes to your firewall. The downstream port must be connected to an untagged interface.

Single arm

Instead of a dual-arm configuration, you can also configure Mist Edge devices as single-arm, where either one port or multiple ports are configured in the port channel. In a single-arm arm configuration, the corresponding port on the upstream switch must be configured in trunk mode with the Tunnel IP being on a native or untagged VLAN, the rest of the client VLANs are tagged VLANs. Similar to a dual-arm configuration, you can configure one or more ports to carry the tunneled traffic. If you use multiple ports, they become part of the port channel as shown below.





Port Configurations

- For dual-arm deployments, Juniper Mist Edge automatically configures each upstream data port as a trunk port. Juniper Mist Edge adds the VLANs that you configure for the Juniper Mist Tunnels as tagged VLANs. The downstream port is untagged, and you must connect the port to the tunnel IP network.
- For single-arm deployments, Juniper Mist Edge automatically configures the data port as a trunk with tunnel IP as its untagged or native VLAN. Trunk adds the VLANs that you configure under the Juniper Mist Tunnels as tagged VLANs.

Create Mist Edge Cluster

Depending on your networking needs, you may want to use an org-level Mist Edge or a site-level Mist Edge.

- Org-level: All APs with an SSID configured for tunneling to Mist Edge will be able to form an L2TP tunnel to this Mist Edge, regardless of the AP's site assignment. You must configure a Mist Cluster and a Mist Tunnel

- Site-level: Only APs with an SSID configured for tunneling to the site will be able to form tunnels to Mist Edge devices in the same site. You must configure a Site Mist Tunnel under **Organization** > **Site Configuration** > **Mist Tunnels**.

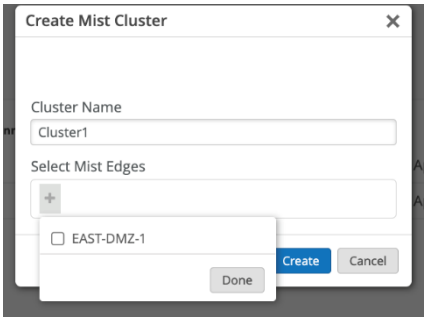
In this document, we explain only the Org level Mist Edge deployment.

- Create a Mist Edge Cluster (Org Level).

Now that all the interface configurations have been done, we can create a Mist Edge Cluster and add Mist Edge devices to the cluster.

- From the left-navigation menu, go to Mist Edges and click Create Cluster in the Mist Edge Cluster section.

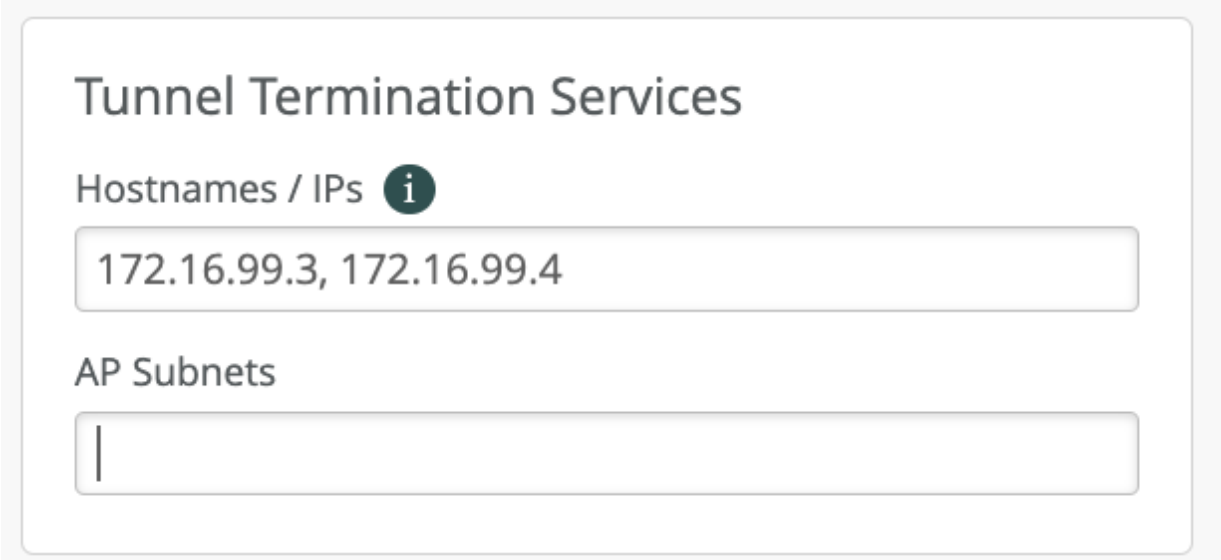
- Enter a name for the cluster and click the plus sign (+) to assign one or more Mist Edge devices from the list of available devices.



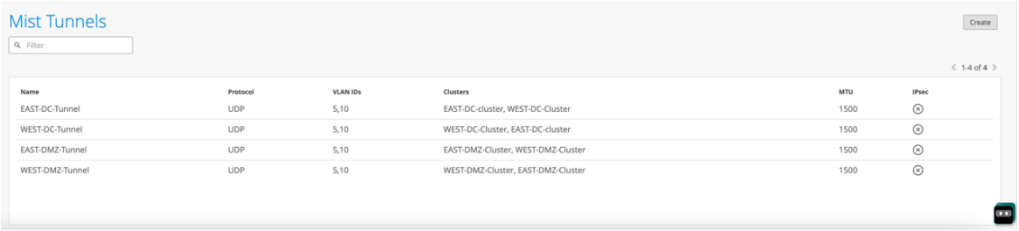
If you add multiple Mist Edge devices to a single cluster, you form an Active-Active configuration for all the devices in that cluster. Mist performs best-effort load balancing among the APs connected to that cluster. In the event one of the Mist Edge devices in the cluster goes down, the APs will failover to the other devices in that cluster. If you require an Active-Standby setup, create a second cluster for the Mist Edge device(s) you want to be on standby. In the event the Primary Cluster devices go down, the AP(s) will fail over to the Secondary Cluster device(s). You designate ca Mist Edge cluster as primary or secondary in the Mist Tunnels section of the Mist Edges page.

- Set Addresses for Tunnel Termination Services:
  - From the left-nav menu, go to **Mist Edges** and click **Create Cluster** above the **Mist Edge Cluster** section. If you already have a cluster defined, you can simply click on its name.
  - On the Cluster configuration page, locate the **Tunnel Termination Services** configuration block. Specify the Hostname or IP address. Use the same address or hostname that you configured for the Mist Edge **Tunnel IP**. If your cluster contains multiple Mist Edge devices, you must enter the IP addresses or hostnames of all cluster members as a comma-separated list.

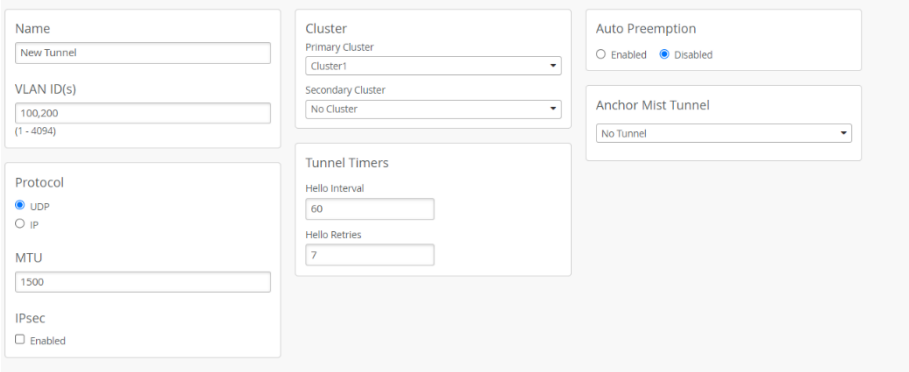
- Click **Save** when finished.



- Setup Tunnel (Org-Level)
  - From the left-nav menu, Go to **Mist Edges** and click **Create Tunnel** above the Mist Tunnels section.



  - On the Mist Tunnel configuration page, enter all user VLAN IDs that you want to extend from your corporate network, through the Mist Edge device(s), to the APs. You can enter Multiple VLAN IDs as a comma-separated list.
  - In the Cluster block, assign the tunnel to the Mist Edge Cluster(s) you created earlier. If you have only configured one cluster, set it as the primary cluster. Otherwise, select the **Primary** and **Secondary Cluster** for this tunnel from the appropriate pull-down list. Leave the rest of the settings on this page in their default settings.

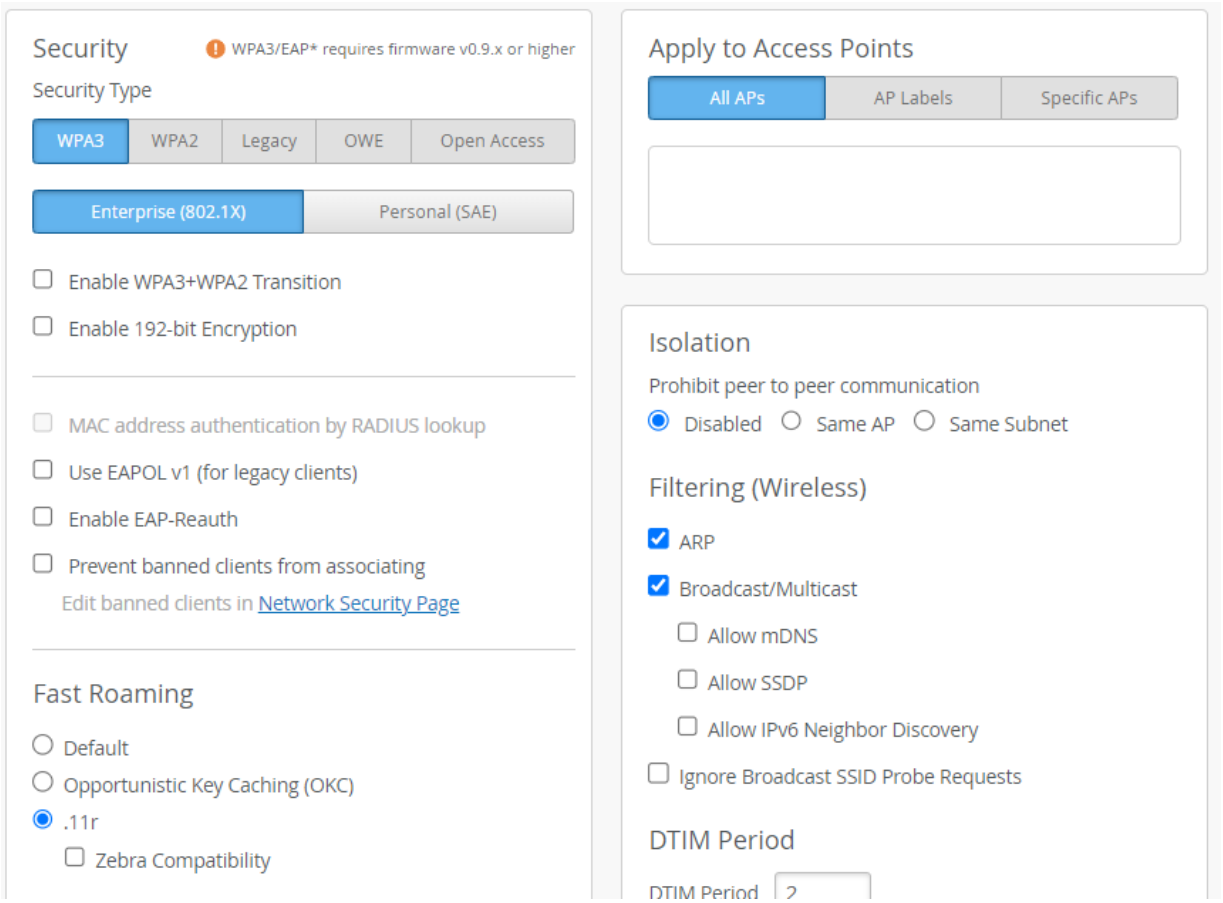


For additional details about the settings on this page, see: Failover Tunnel Timers, Auto Preemption, and Anchor Tunnel.

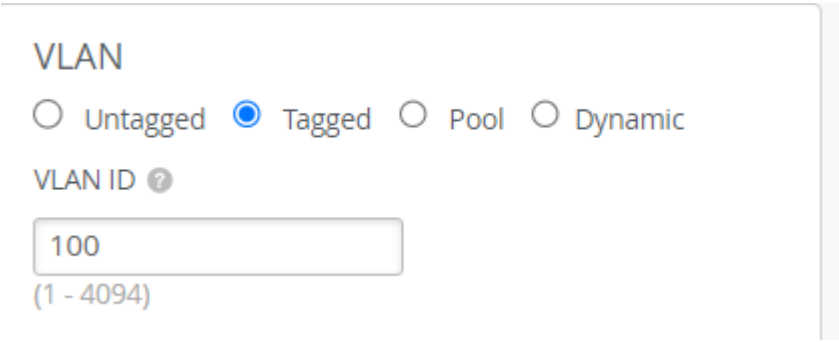
- Configure and prepare the WLAN

As illustrated in the previous chapter on how to create ORG-level WLANs, we follow all the recommendations and in addition we add the tunnel-related setup.

- Navigate to **Organization** > **Wireless** > **WLAN Templates** and create a new WLAN.
- In the Security block, select the following settings
- In the **VLAN** block, select **Tagged.** Mist APs only tunnel WLAN traffic configured with a tagged VLAN.



- For the **VLAN ID**, specify the desired VLAN(s). Use VLAN IDs from the list you defined in the Mist Edge tunnel configuration.
- The VLANs you configure here are tunneled by the AP through the Mist Edge.



- In the Custom Forwarding block, enable (check) **Custom Forwarding** to **Mist**, then select the appropriate tunnel service.

Location Services & Asset Visibility (Optional)

The Location Services & Asset Visibility section, while optional, unlocks powerful capabilities for enterprises leveraging Juniper Mist Access Points with integrated Virtual Bluetooth® Low Energy (vBLE) technology. This involves enabling the vBLE services on the deployed APs within the Mist Cloud. Once activated, IT administrators can configure precise location zones and upload detailed floor maps, allowing for highly accurate indoor positioning. This capability supports various applications, from providing real-time indoor navigation and wayfinding for users to enabling robust asset tracking for critical equipment. By integrating with asset tracking tags or mobile applications, organizations can gain valuable insights into the movement and location of resources, optimizing operations and enhancing efficiency within their physical spaces.

- • Enable vBLE services on APs
  - Add a floorplan (map) to Mist
  - Configure location zones
  - Integrate with asset tracking tags

Security Implementation

IN THIS SECTION

Access Assurance Configuration

Access Assurance Configuration is pivotal for establishing a robust Zero Trust security model that meticulously controls who and what can connect to the network. This involves defining granular

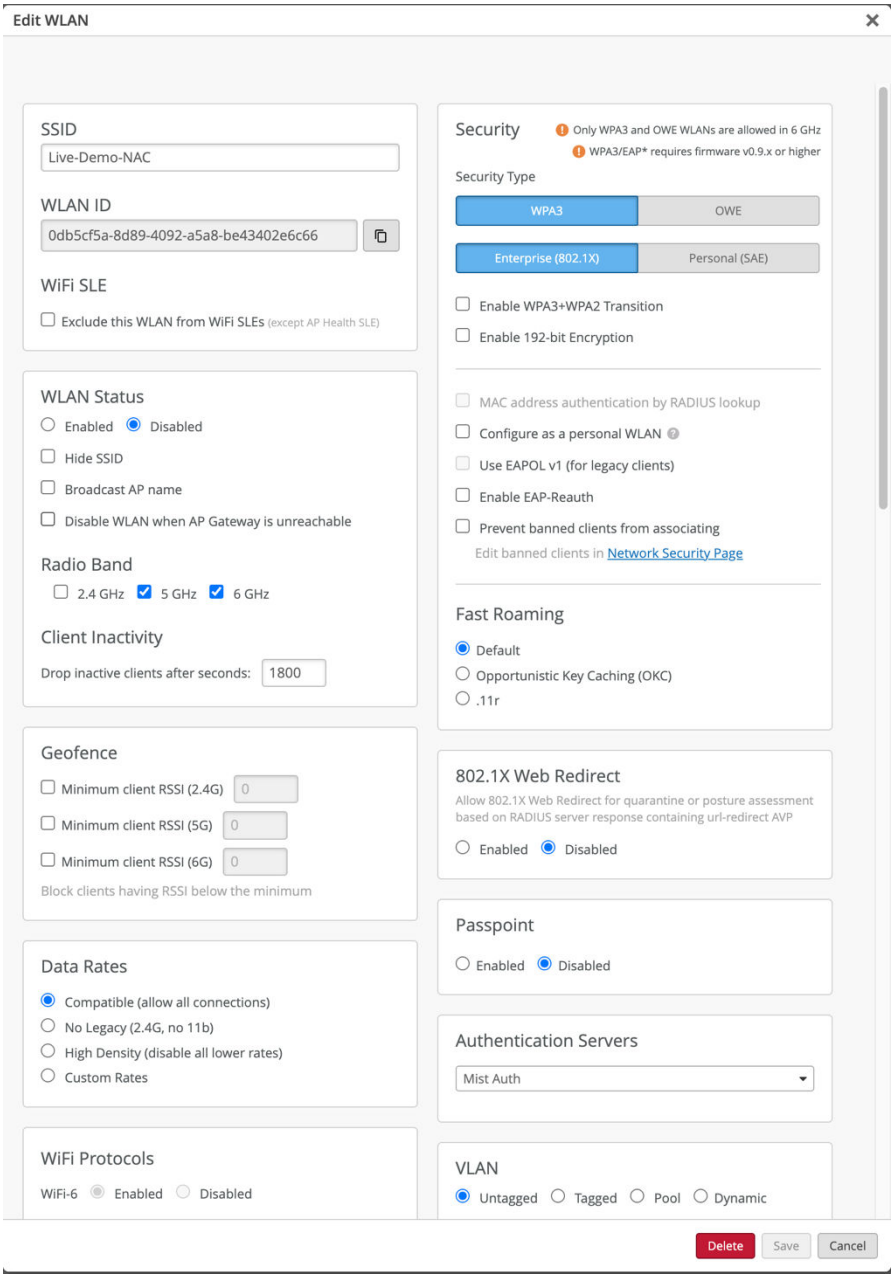
network access policies based on a combination of factors, including user identity (for example, Active Directory groups), device posture (for example, compliance with security updates), and the specific application access. For external or temporary users, configuring secure guest access portals is essential, and allows controlled network entry while maintaining isolation from sensitive internal resources. These policies ensure that only authorized and compliant users and devices gain access to the appropriate network segments.

- Define network access policies based on user identity, device posture, and application
- Configure guest access portals

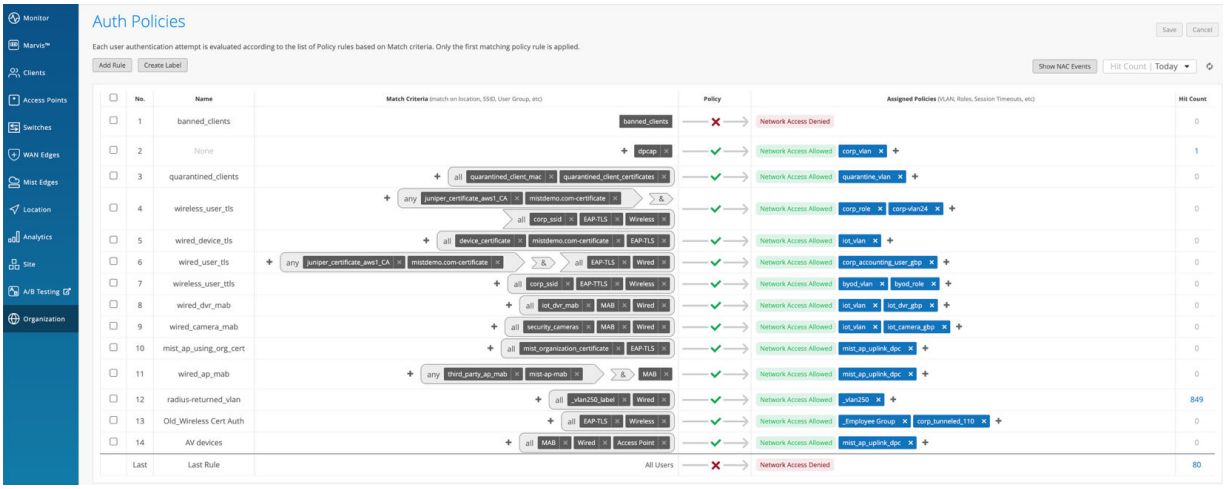
Juniper Mist Access Assurance configuration for both wired and wireless networks involves enabling 802.1X authentication, configuring authentication servers, and creating access policies. For wireless networks, this is done with WLAN templates. For wired networks, it's done with switch templates. Key steps include importing certificate authorities, creating rules for authorized clients, and assigning VLANs.

Wireless Configuration Steps:

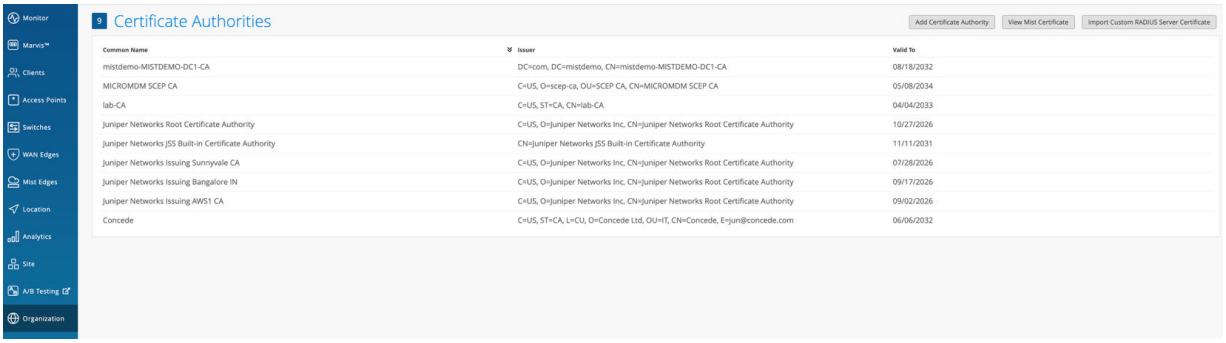
- **Enable 802.1X:** Navigate to Organization > WLAN Templates and select **WPA2** or **WPA3** and **Enterprise (802.1X)** as the **Security Type**
- In the **Authentication Servers** block**,** Select **Mist Auth** as the authentication server



- **Create Authentication Policies:** Define rules based on labels, site, or site group to match client criteria and apply appropriate actions, like VLAN assignment or session timeout.



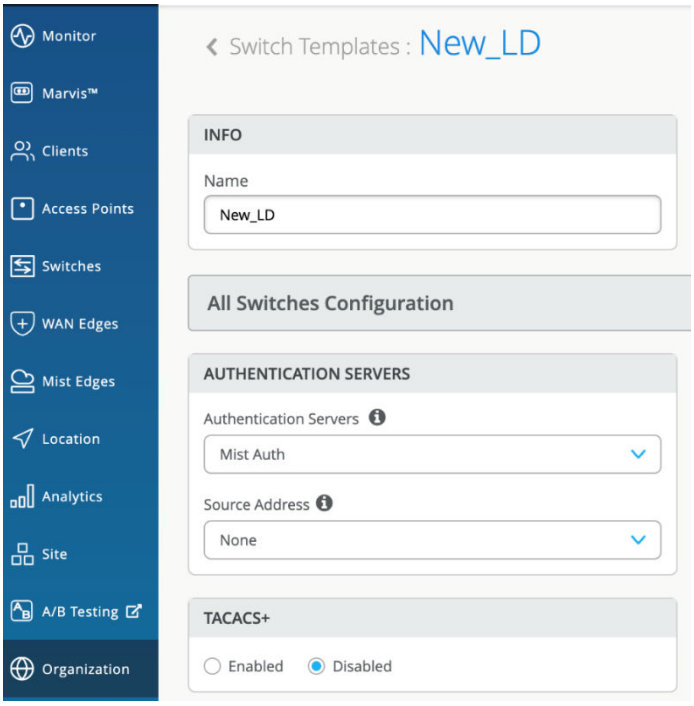
- **Import Certificate Authority:** If you intend to use certificate-based authentication, add your Certificate Authority under Organization > Access > Certificates.



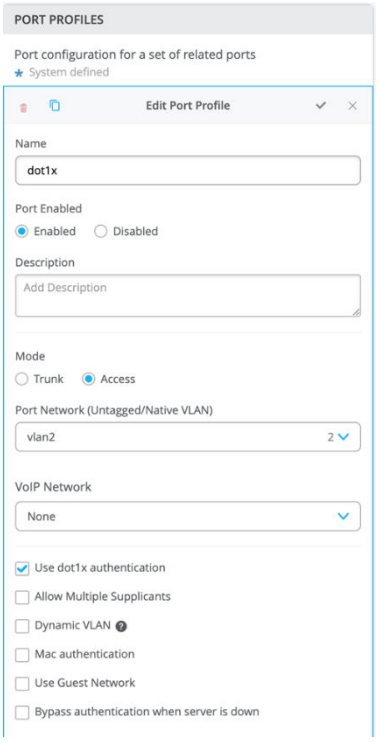
- **Assign VLANs:** Configure VLANs based on your network design. Choose from Untagged, Tagged, Pool, or Dynamic VLAN.

Wired Configuration Steps:

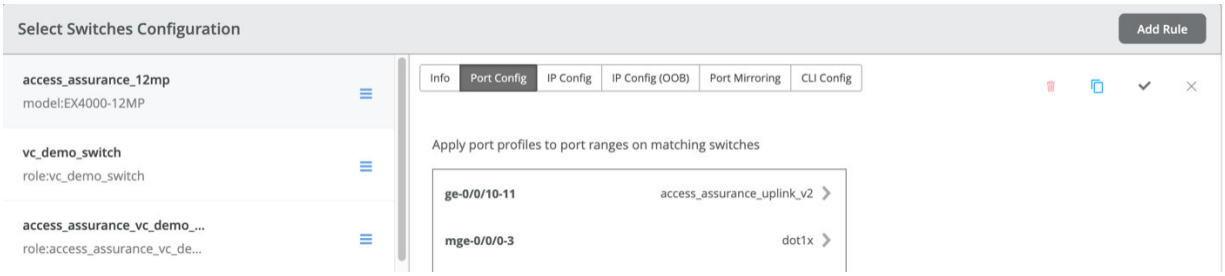
- **Configure Switch Templates:** Navigate to Organization > Wired > Switch Templates and either create a new template or edit an existing one.
- **Enable Authentication Servers:** In the Authentication Servers section, select **Mist Auth** as the authentication server.



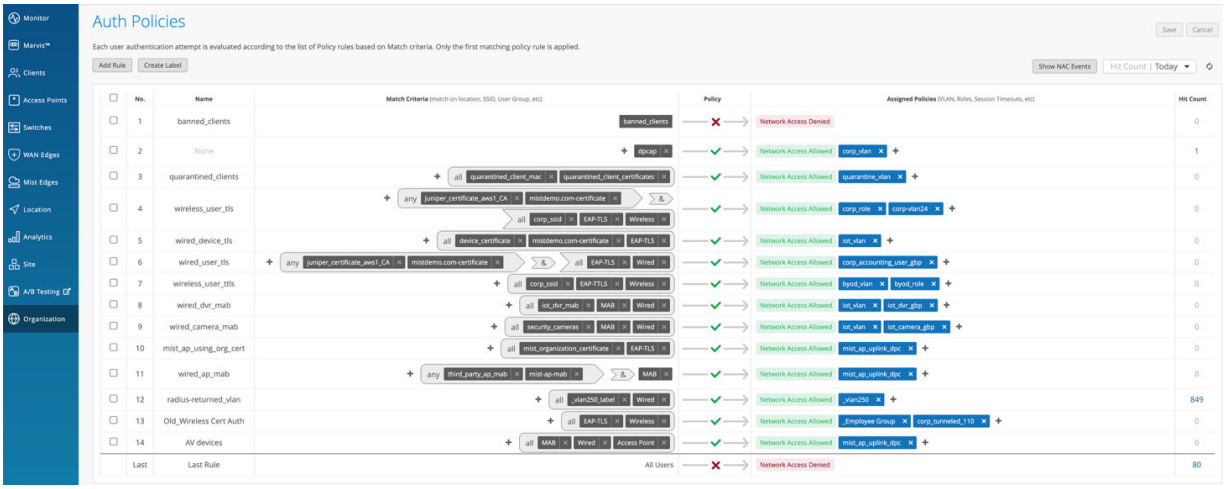
- **Configure Port Profiles:** In the Port Profiles block, set the port mode to **Access** and enable dot1x authentication.



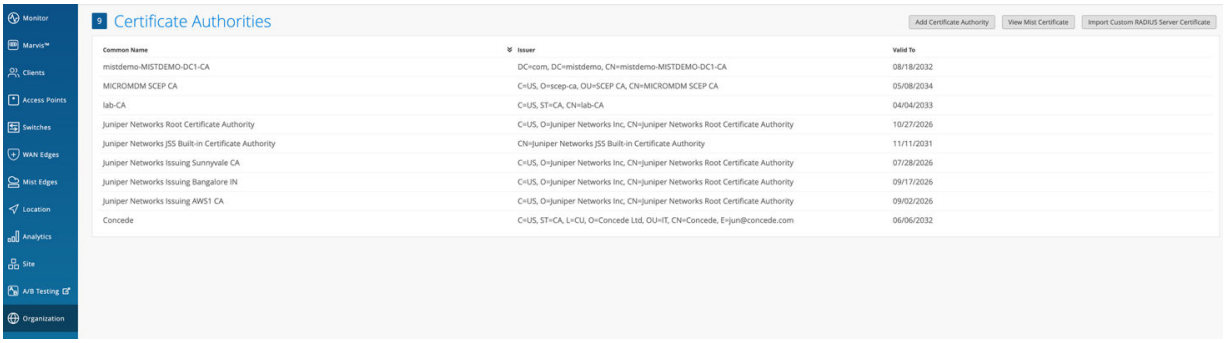
- **Assign Port Profiles:** Associate the created port profile (dot1x) with specific port ranges on the switch.



- **Create Authentication Policies:** Define rules using labels, site, or site groups to match criteria and apply appropriate actions such as VLAN assignment.



- **Import Certificate Authority**: If you intend to use certificates, add your Certificate Authority under **Organization** > **Access** > **Certificates**.



- **Assign VLANs:** Configure VLANs based on your network design.

Firewall Integration (SRX Series)

Firewall Integration, specifically with Juniper SRX Series Firewalls, is essential for providing robust perimeter and internal network security. This involves strategically deploying SRX Series Firewalls at key points, such as the network edge for Internet ingress and egress, or within the data center to protect critical applications and data. The configuration requires that you:

- define comprehensive firewall policies to control traffic flow
- set up Network Address Translation (NAT) rules
- establish secure VPNs for remote access or site-to-site connectivity

Furthermore, integrating the SRX Series with Juniper's Advanced Threat Prevention (ATP) services enhances its capabilities, providing protection against known and unknown threats through features like sandboxing and threat intelligence feeds.

- Deploy SRX Series Firewalls at the network edge or data center.
- Configure firewall policies, NAT, and VPNs.
- Integrate with Advanced Threat Prevention (ATP) services.

Juniper Mist-Based SRX Firewall Configuration for Wired and Wireless Networks

Configuring your Juniper SRX firewall to support both wired and wireless networks managed by Juniper Mist involves a series of steps to onboard the firewall, define networks and WLANs, and apply necessary policies. Here's a breakdown:

- Onboard the SRX Series Firewall to Mist

  NOTE:
  Cloud-Ready SRX Firewalls in Mist

- You can onboard the SRX firewall using either the Mist AI Mobile App or a web browser. Both methods involve claiming the device and assigning it to a site. When using a web browser, you'll also select to manage the configuration with Mist and set a root password. After claiming, verify that the SRX is in your inventory.

Install the SRX Series Firewall in a Rack and Connect to the Network

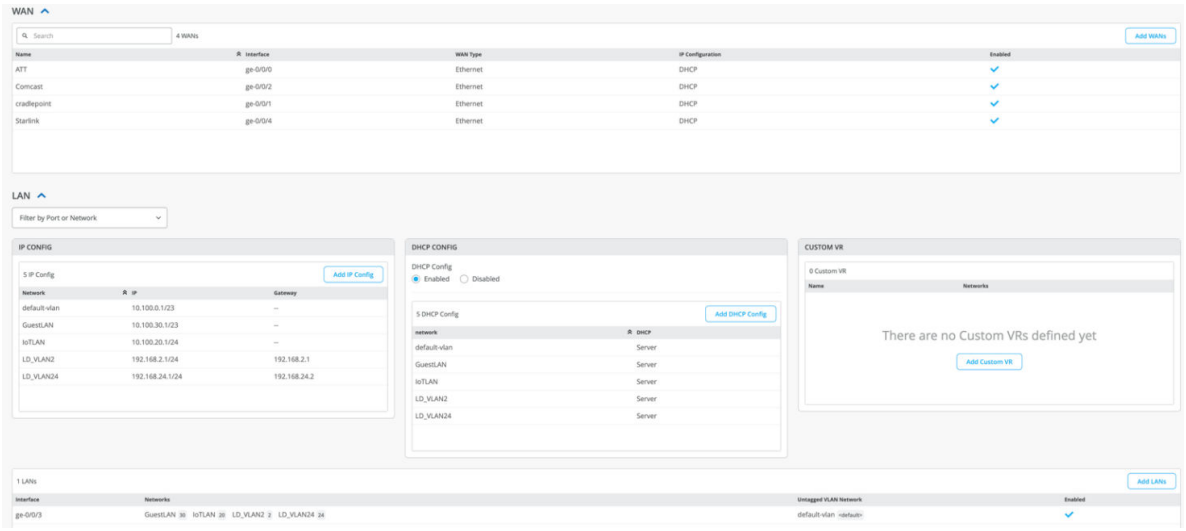
- Install and power on the SRX according to your model's hardware guide. Connect the WAN interface (ge-0/0/0) to the Internet and another interface to your local network. Ensure the necessary outbound ports (like TCP 443, 2200, and 6514) are open on your Internet firewall for communication with the Mist cloud. Power on the device and let it boot.

Configure Networks and VLAN IDs

- In the Juniper Mist portal, navigate to **Organization** > **WAN** > **Networks** and add your L2 networks, defining subnet IP addresses, prefix lengths, and VLAN IDs. If you have variables defined, you can use them in the fields with the VAR designation. We recommend you use variables whenever possible. Select Enable Access to Mist Cloud for the appropriate network(s) so that communication is possible.

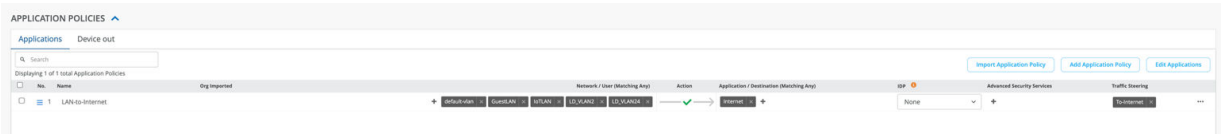
Configure Wireless Networks (WLANs)

- Go to **Site** > **WLANs** in the Mist portal and click Add WLAN. Provide an SSID and choose appropriate security settings. You can configure RADIUS settings for NAC integration and set static or dynamic VLANs.



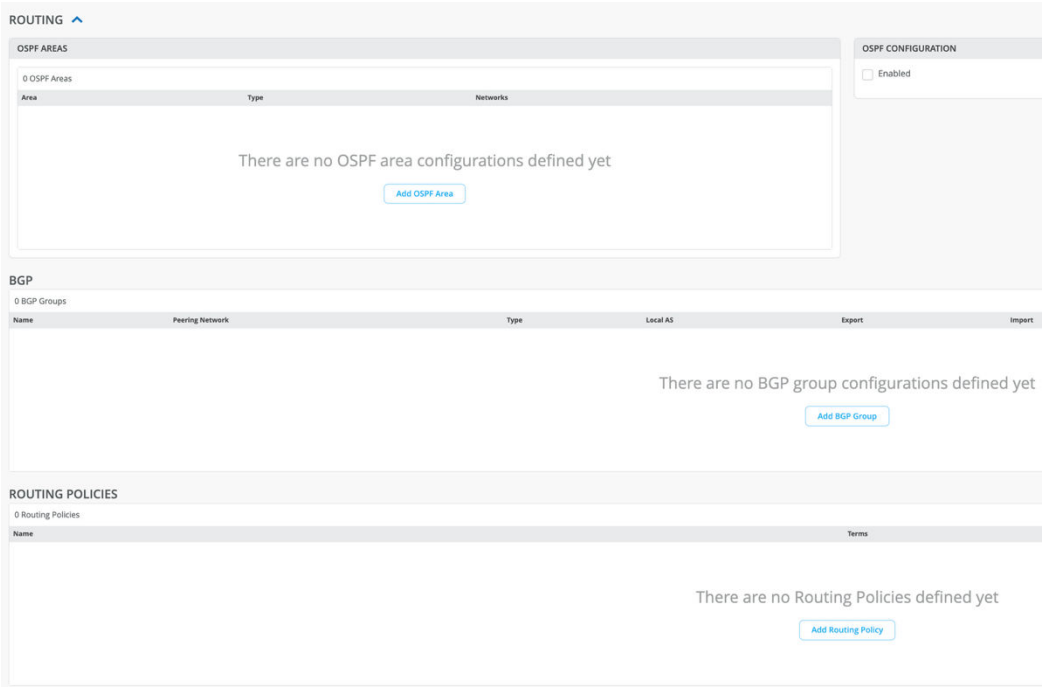
Configure Security Policies

- Define application policies to manage traffic flow. We recommend that you place global policies last. You can configure application policies at the Organization level, within WAN Edge templates, or in Hub profiles.



Configure Routing Protocols

- If you use BGP or OSPF in your networks, go to Organization > WAN > WAN Edge Templates. Configure BGP groups and OSPF areas in the Routing section of any template.



Troubleshooting

- If the SRX appears disconnected in Mist, check the Junos OS version, IP address, gateway, and Internet connectivity, and the ability to resolve oc-term.mistsys.net. Verify that upstream firewalls have TCP ports 2200 or 443 open and that the system time is correct. Also, check the device's ID format and look for MTU issues. For host connectivity issues, check security flow sessions.

These steps provide a general guide. Refer to Juniper documentation for specific details related to your SRX model and configuration needs.

Post-Deployment and Operations

IN THIS SECTION

Verification and Testing

Verification and Testing is a crucial post-deployment phase to confirm the successful implementation and optimal performance of the new Juniper network. This phase involves comprehensive connectivity testing for all devices and users to ensure seamless access to network resources. Rigorous application performance testing validates that critical business applications meet their required bandwidth and latency targets. Security policy enforcement validation is paramount, confirming that all defined access controls, segmentation rules, and threat prevention mechanisms are functioning as intended. Finally, thorough wireless signal strength and coverage validation, often through post-deployment site surveys, will ensure the Wi-Fi network provides ubiquitous and high-quality connectivity across all designated areas.

- Connectivity testing for all devices and users.
- Application performance testing.
- Security policy enforcement validation.
- Wireless signal strength and coverage validation.

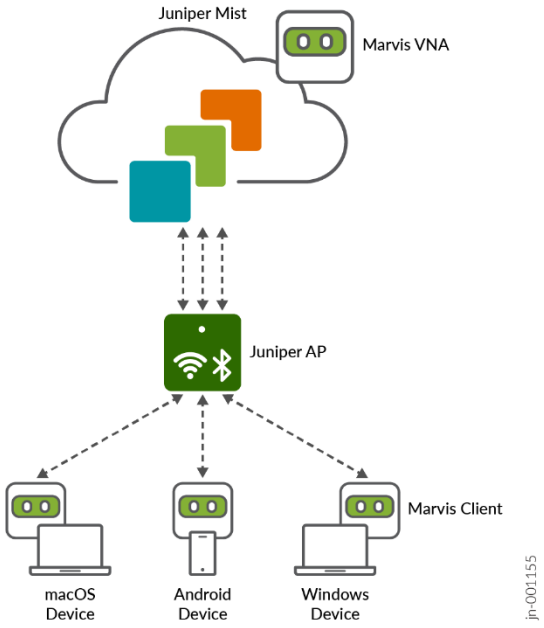
Monitoring and Troubleshooting with Marvis VNA

Monitoring and troubleshooting with Marvis VNA transforms network operations from reactive to proactive, leveraging Juniper's powerful AI engine. This involves actively utilizing Marvis for real-time insights into network health, client experience, and potential issues. Juniper Mist's AIOps capabilities, powered by Marvis, provide unprecedented visibility and automation across the wired and wireless domains. By ingesting vast amounts of network data, Marvis uses AI and machine learning to analyze patterns, detect anomalies, and pinpoint the root cause of issues with high accuracy. Marvis's AI-driven capabilities enable automatic anomaly detection, pinpointing deviations from normal behavior, and providing intelligent root cause analysis across the entire network stack. IT teams can continuously monitor SLEs, allowing them to identify and address problems before they impact end-users. Furthermore, the conversational interface of Marvis VNA simplifies troubleshooting queries, providing quick answers and recommended actions, significantly reducing mean time to resolution.

- Utilize Marvis for real-time insights, anomaly detection, and root cause analysis.

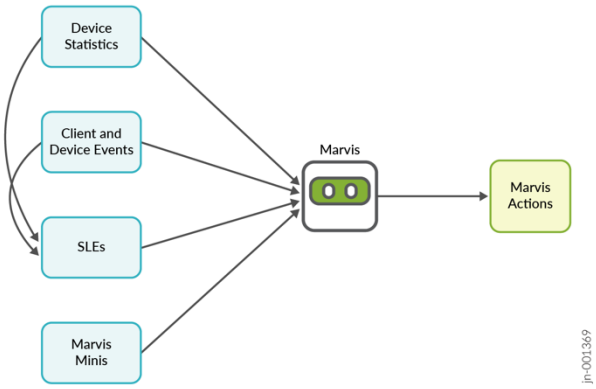
- Monitor SLEs and user experience metrics.
- Leverage Marvis conversational interface for troubleshooting queries.

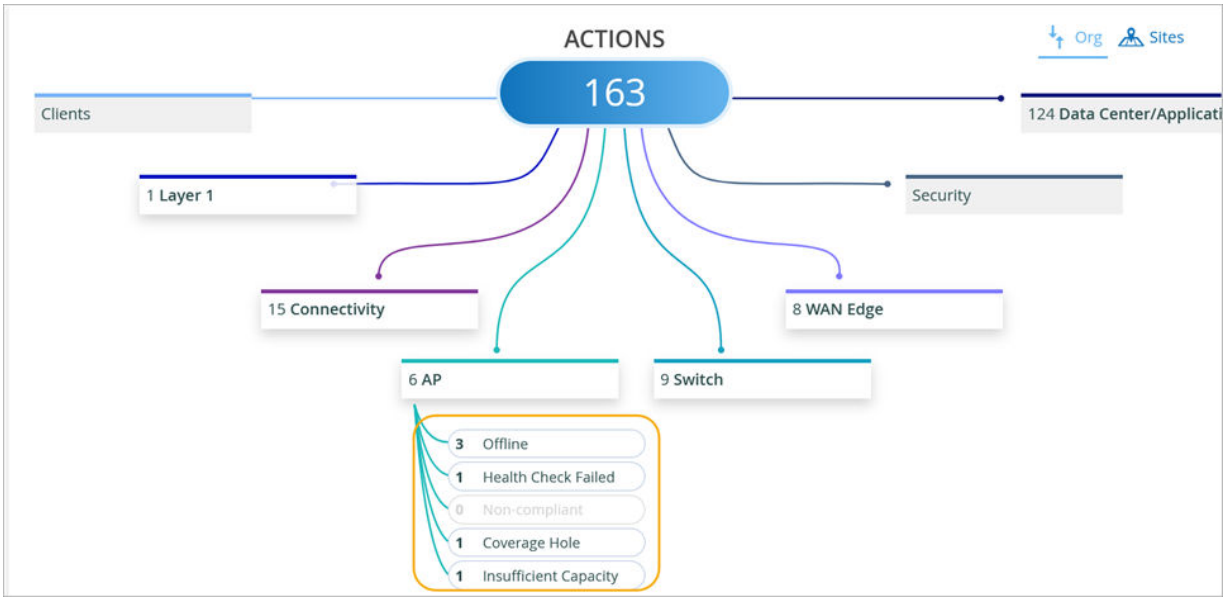
Figure 10: Marvis



You can use Marvis, Juniper Mist's AI engine, to troubleshoot both wired and wireless network issues using its conversational interface and automated analysis. By using natural language queries, users can quickly identify and resolve problems related to clients, devices, and sites. Marvis can also proactively detect issues and recommend actions, streamlining the troubleshooting process.

To ensure optimal network performance and coverage, you must regularly assess the efficiency of the APs in your network. By leveraging the Marvis Actions in the Juniper Mist portal, you can efficiently identify and address any issues affecting your APs.



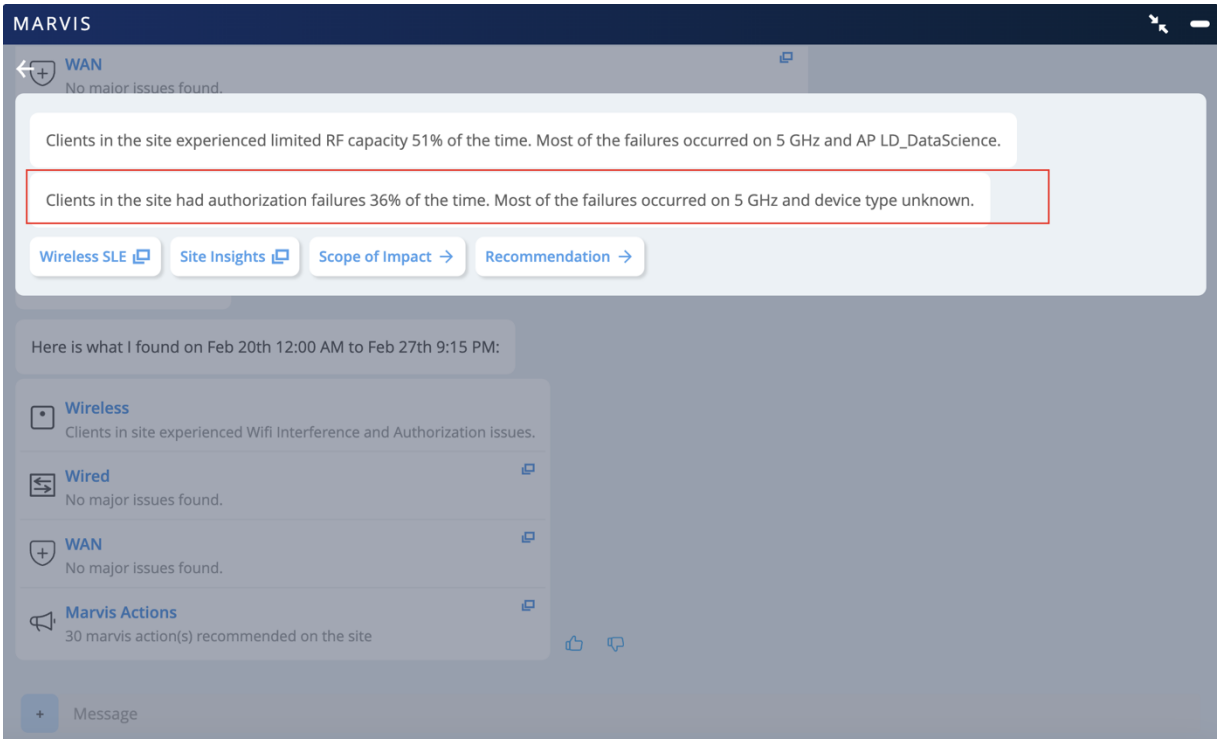


Troubleshooting Wireless Clients:

How can you identify unhappy clients? Ask Marvis questions like "troubleshoot clients" or "unhappy clients" to see a list of clients experiencing issues.

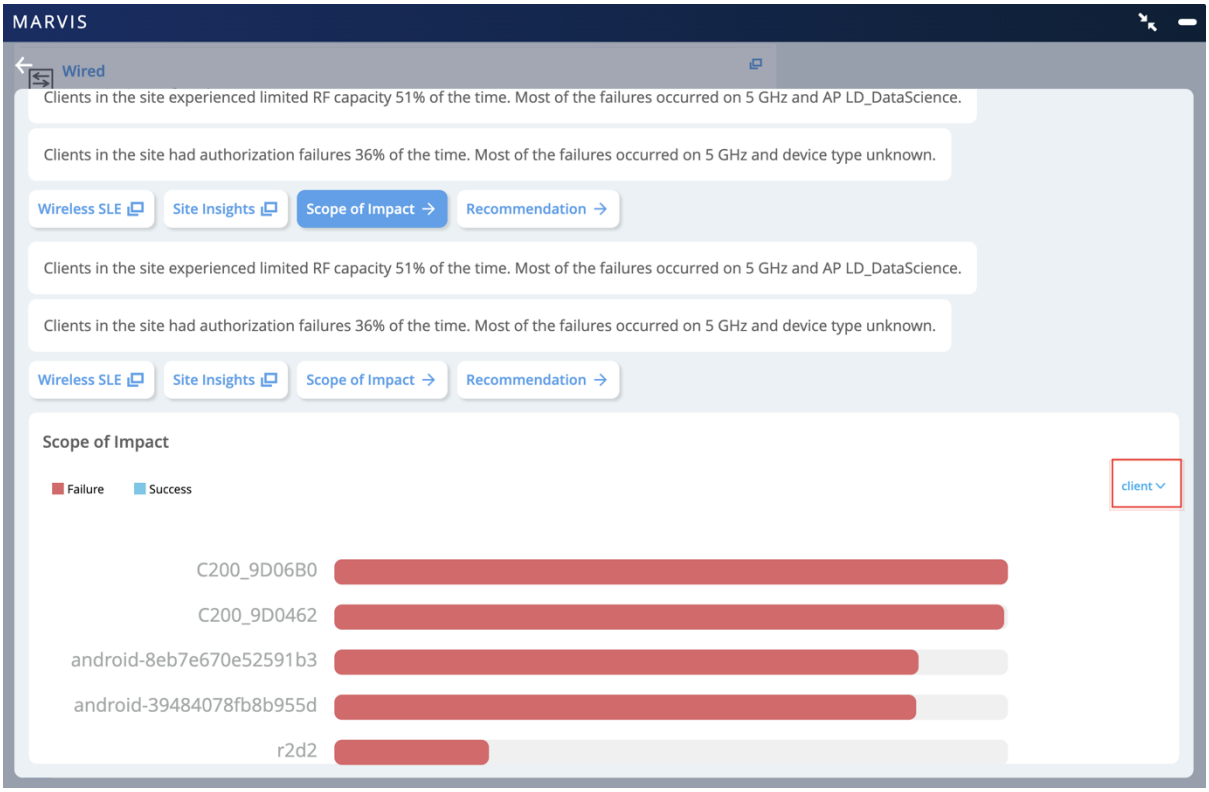
Drill down into specific client issues:

Select a client issue from the list to view detailed troubleshooting information, including connection failures, signal strength, and more.



Understand the Scope of Impact:

Select the Scope of Impact and select the client pull-down on the right to understand which clients were impacted.



Troubleshooting Wired Clients

Identify Wired Client Issues:

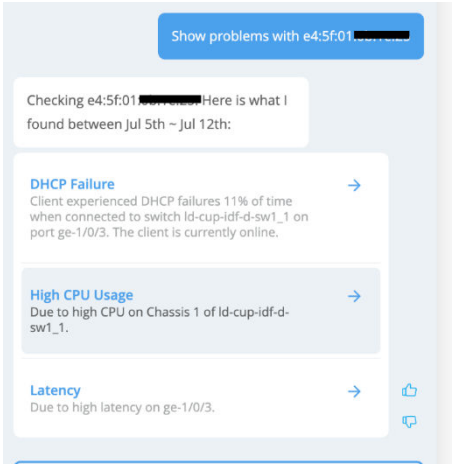
Use queries like "tshoot wired client <mac>" or "troubleshoot client name" to investigate connection problems on the wired network.

View Switch and Interface Health:

Marvis provides insights into switch and interface performance, including potential failures.

Understand Wired Client Connections:

Marvis can show you which switch and port a wired client is connected to, along with other relevant details.



Troubleshooting Devices and Sites

Troubleshoot Devices:

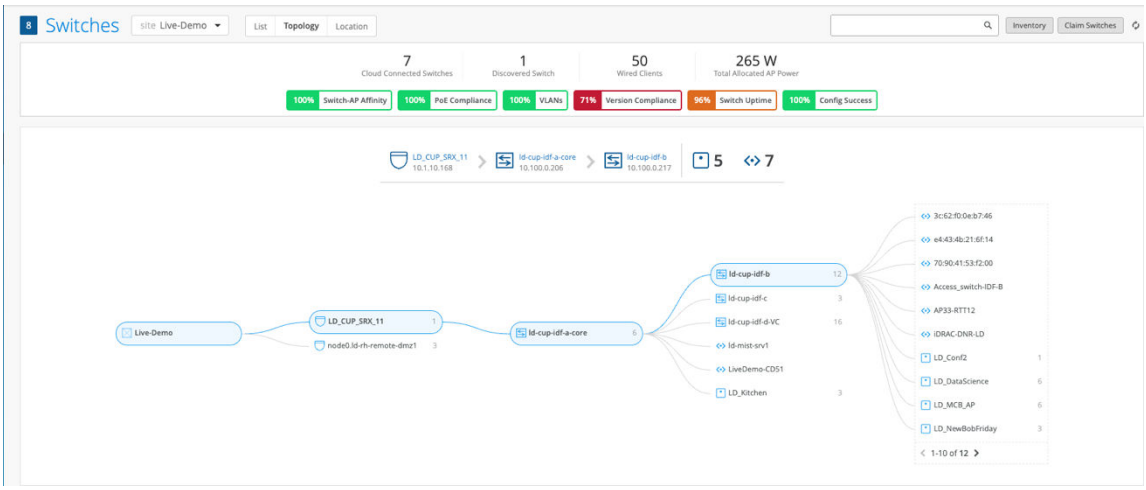
Use queries like "tshoot switch name" or "tshoot device name" to investigate device-specific issues.

Analyze Site-Level Issues:

Marvis can help identify problems impacting an entire site, such as poor coverage or high error rates.

View Site Topology:

Use the topology view to see the relationships between different devices and components within a site.



Marvis Minis

Marvis Minis, part of Juniper's Mist AI-Native Networking platform, is a digital twin that simulates user experiences to proactively identify and resolve network issues before they impact users. It uses AI and machine learning to understand network behavior and automatically fix problems. Marvis Minis acts as a synthetic user, testing network services like DHCP, ARP, DNS, and application reachability. This helps ensure positive user experience by detecting issues from client devices to cloud services.

Digital Twin:

Marvis Minis creates a virtual representation of your network environment, allowing it to simulate user interactions and test network performance without requiring actual users or devices to be connected.

AI-Powered:

Marvis Minis leverages machine learning to analyze network data, learn patterns, and identify potential problems proactively.

Proactive Problem Detection:

Marvis Minis can detect issues like DHCP, ARP, and DNS problems, as well as application connectivity issues, before they affect users.

Automated Issue Resolution:

Marvis Minis can automatically fix some identified problems, reducing the need for manual intervention and minimizing the impact on users.

Client-to-Cloud Visibility:

Marvis Minis provides visibility from client devices to cloud services, helping pinpoint the root cause of issues and enabling faster troubleshooting.

No Additional Hardware:

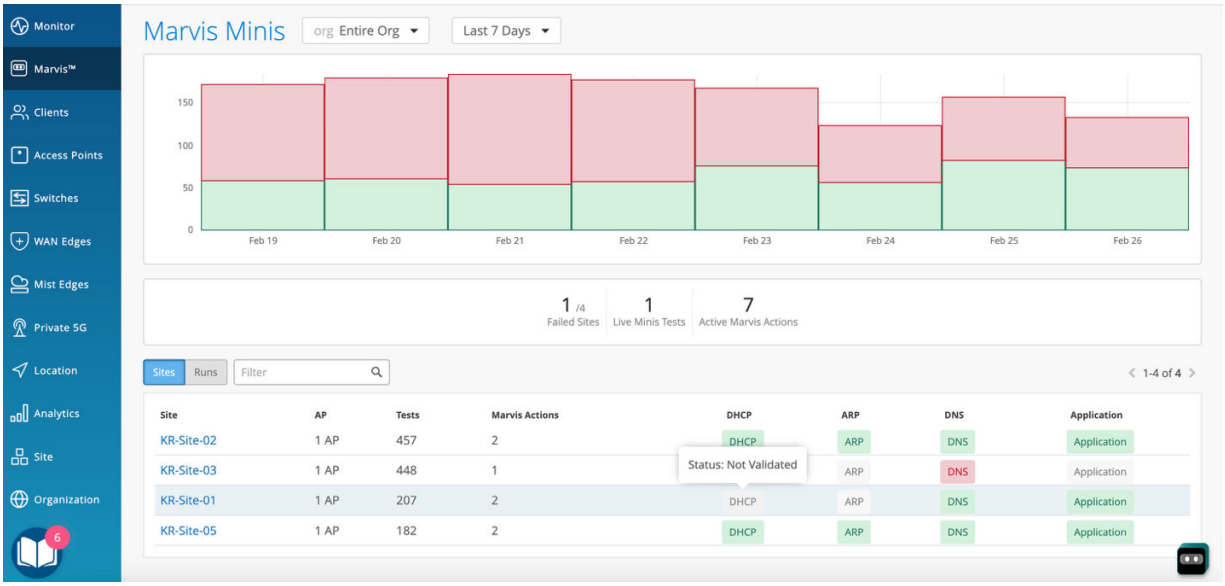
Marvis Minis operates as a cloud-based service, so it doesn't require any additional hardware or sensors to be deployed in the network.

Always On:

Marvis Minis continuously monitors the network, even when users are not actively connected, enabling it to catch potential problems proactively.

Wired and Wireless Support:

Marvis Minis is now extended to wired networks, further enhancing its ability to ensure exceptional user experiences across all network types, according to Juniper Networks.



Ongoing Maintenance and Updates

Ongoing Maintenance and Updates are essential for ensuring the long-term stability, security, and optimal performance of the Juniper network. This includes scheduling and performing regular software updates for both Juniper EX Series Switches and Juniper Mist Access Points. These software updates can be delivered seamlessly via the Mist Cloud, providing access to new features, bug fixes, and security patches. Periodic policy reviews and adjustments are necessary to align network configurations with evolving business needs and security requirements. Continuous performance optimization, guided by insights from Mist AI, ensures the network consistently meets or exceeds SLEs. These optimizations allow the network to adapt to changes in user density, application demands, and traffic patterns.

- Regular software updates for switches and APs via Mist Cloud.
- Policy reviews and adjustments.
- Performance optimization.

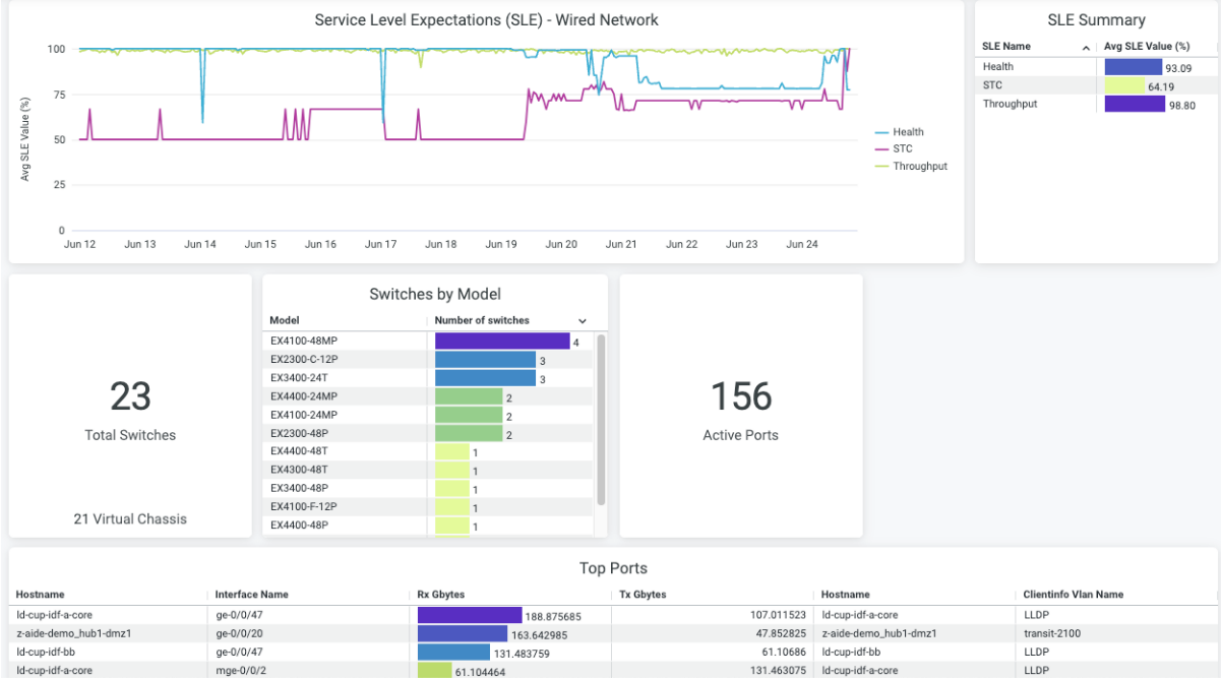
To learn about AP firmware upgrades managed by Mist, see Upgrade the Firmware on a Juniper AP. To learn about switch firmware upgrades managed by Mist, see Upgrade Junos OS on Switches.

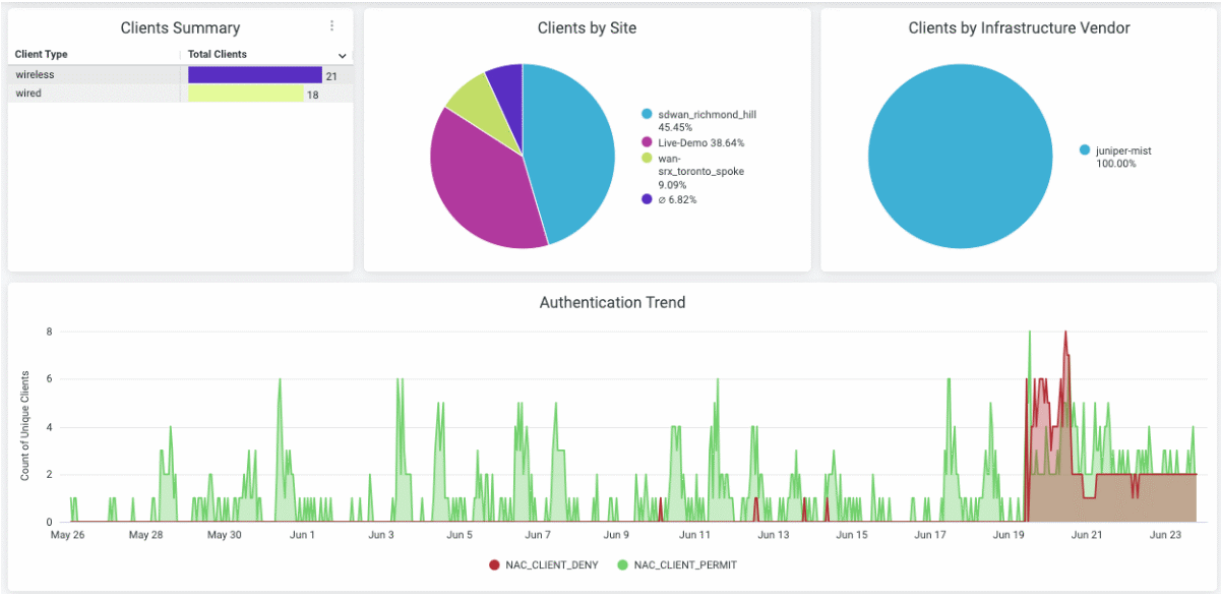
Reporting and Analytics

Reporting and Analytics leverage the rich telemetry collected by the Juniper AI-Driven platform to provide comprehensive visibility into network operations and business intelligence. We utilize the

powerful analytics capabilities within the Juniper Mist Cloud to generate detailed reports on network health, including device performance, connectivity trends, and overall system stability. Insights into usage patterns, such as application resource consumption and client behavior, help optimize resource allocation. Crucially, security insights derived from the analytics platform enable proactive identification of potential threats, compliance adherence, and a deeper understanding of the network's security posture, supporting data-driven decision-making for IT and business leaders.

- Utilize Mist Cloud Analytics for network health, usage patterns, and security insights.



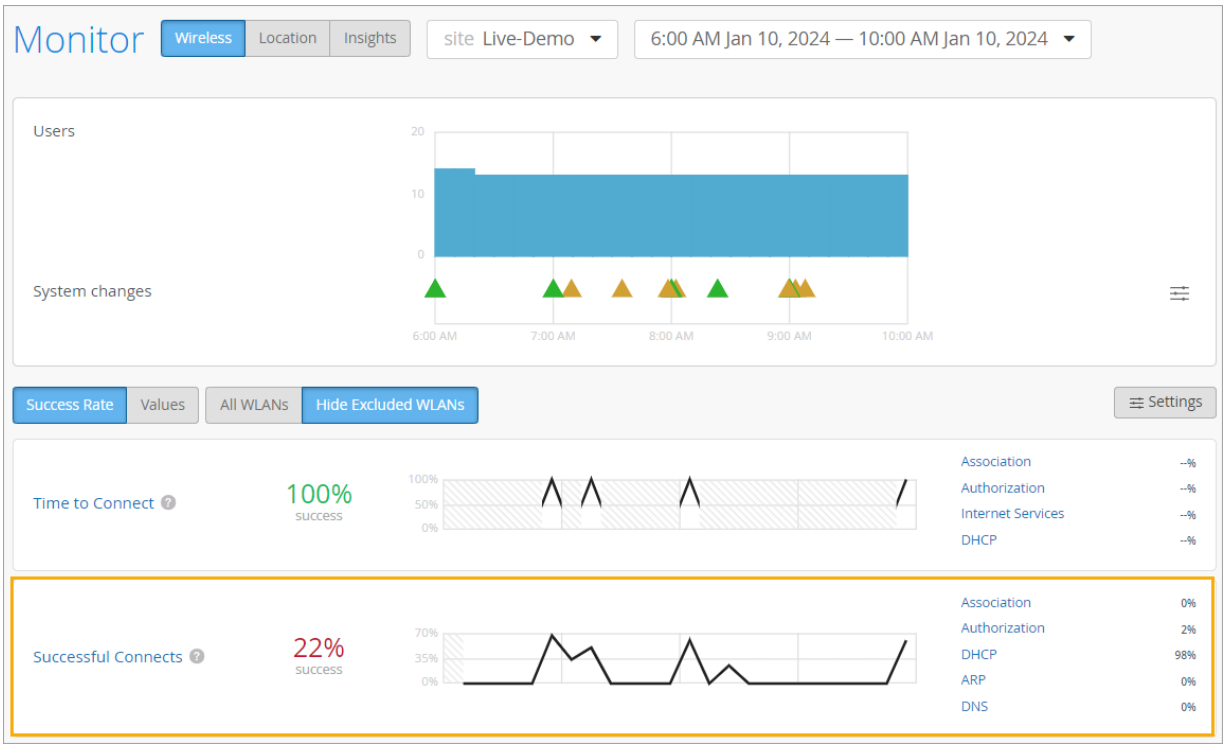


Troubleshooting Common Issues

IN THIS SECTION

Connectivity Issues

This section addresses common problems where devices or users cannot connect to the wired or wireless network. Troubleshooting steps typically involve verifying physical layer integrity, checking VLAN assignments, confirming IP address acquisition (DHCP), and inspecting firewall rules that might block access. For wireless, checks include SSID broadcast, signal strength, and basic authentication failures.

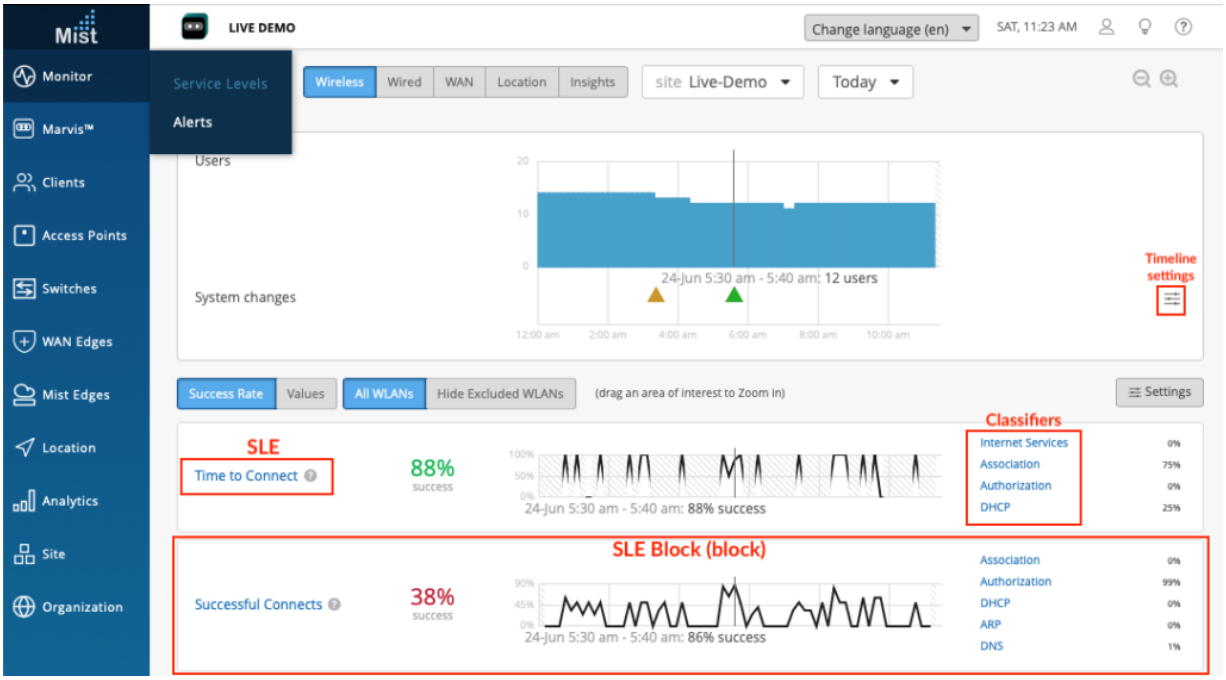


Performance Degradation

Examples include scenarios where clients can connect to the network, but performance is suboptimal which leads to slow application response times, buffering video, or dropped calls. Troubleshooting involves:

- Analyzing bandwidth utilization
- Identifying bottlenecks like congested links or overloaded APs
- Checking for excessive latency
- Checking for packet loss
- Verifying QoS policies are correctly prioritizing critical traffic

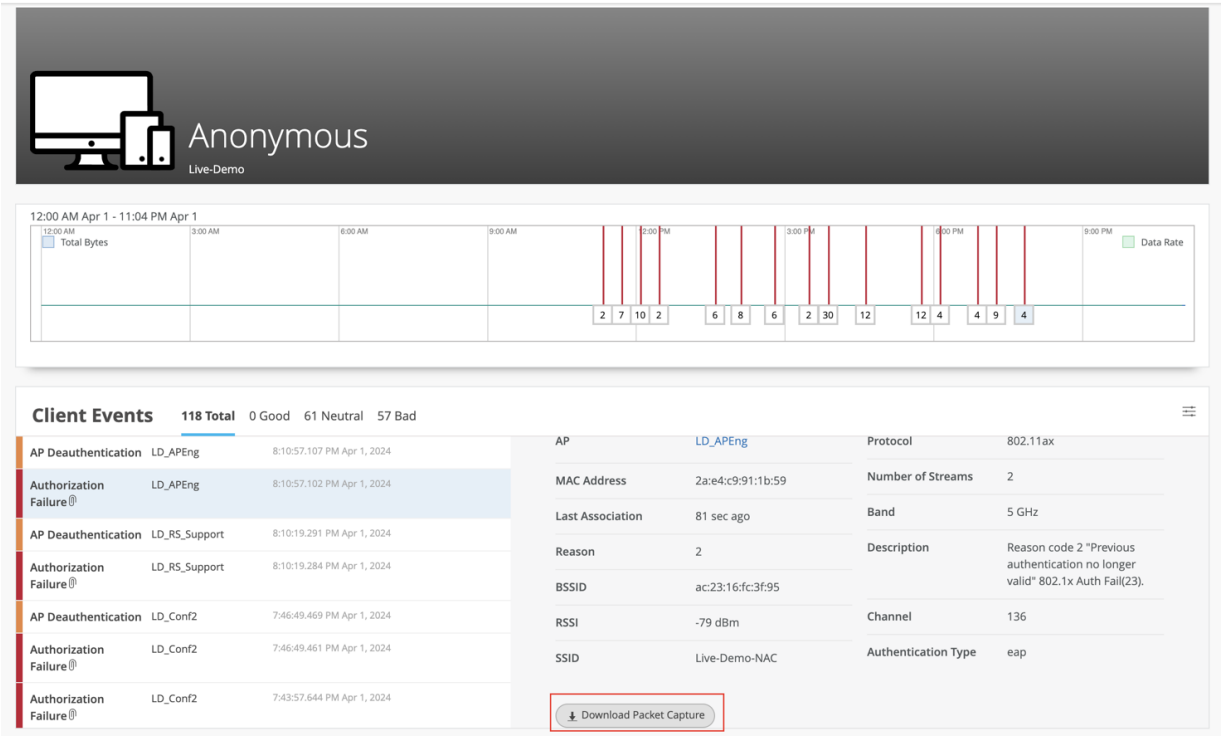
Mist AI's insights into client experience and application performance are crucial in analyzing performance issues.



Authentication Failures

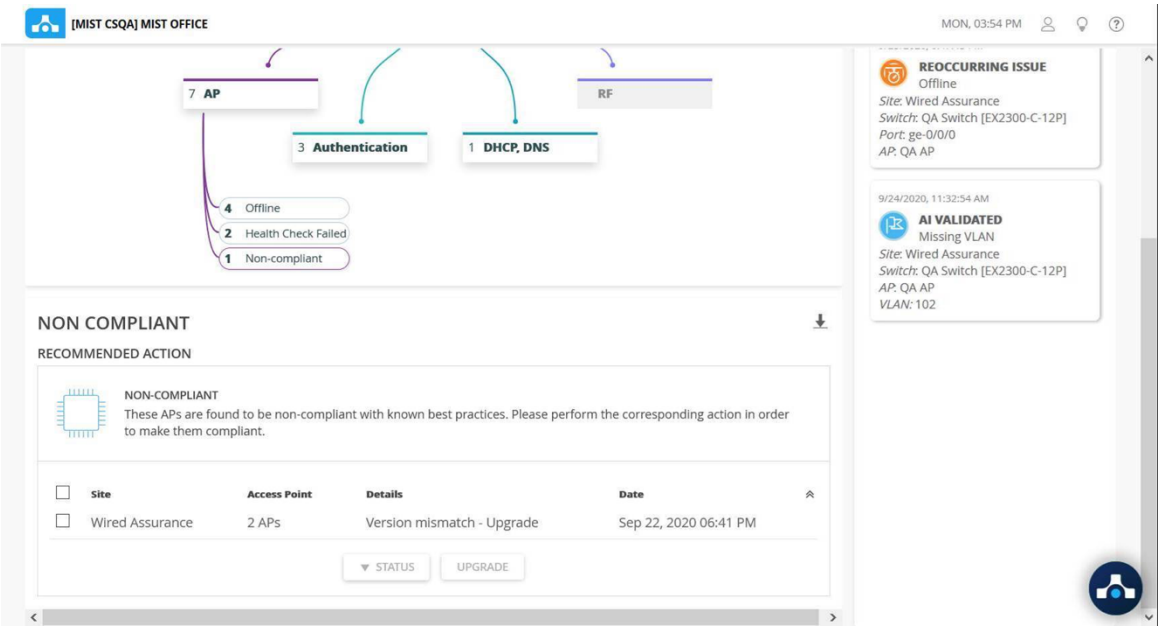
This section covers issues where users or devices cannot authenticate to the network. Common causes include incorrect credentials, misconfigured RADIUS servers, issues with 802.1X supplicants, or problems with identity management system integration (for example, Active Directory). Troubleshooting

involves reviewing authentication logs, checking RADIUS server reachability and configuration, and verifying user and device credentials against the authentication source.



AP or Switch Offline Issues

This addresses situations where APs or EX Series switches appear offline or are not reporting to the Mist Cloud. Common causes include power issues (PoE problems), network connectivity disruptions to the Internet or Mist Cloud, DNS resolution failures, or firewall blocks preventing communication with Mist services. Troubleshooting involves verifying physical power, checking upstream network connectivity, confirming DNS resolution, and reviewing firewall policies.



Conclusion

IN THIS SECTION

Summary of Benefits Achieved

This guide empowers users to plan, deploy, secure, and operate Juniper AI-driven networks with confidence, leveraging automation, best practices, and advanced analytics for superior outcomes. We covered the benefits of:

- Planning—Juniper Mist ensures that your managed network integrates smoothly with the existing infrastructure, meets performance requirements, reduces operations risks, supports scalability, aligns with compliance and security requirements, and more.
- Wireless Deployment—Mist provides automation, centralized management, AI-driven insights, consistency, scalability, and robust security to your wireless network deployment.

- Wired Deployment—Using Mist for wired network deployment brings automation, centralized management, AI-driven assurance, consistency, scalability, advanced analytics, and robust security.
- Operation—Managing your network with Juniper Mist empowers your IT teams to operate the network more efficiently, reduce operational costs, and deliver superior user experiences. Juniper Mist's powerful templating capabilities ensure consistent application of network configurations, policies, and security throughout the sites within your organization.
- Security—A Mist-managed network delivers robust, centralized, and adaptive security by combining Zero Trust principles, granular access control, strong encryption, integrated firewalling, automated certificate management, and continuous monitoring—all managed through a unified cloud platform.
- Automation—Powerful service-level expectations (SLEs) leverage device and client telemetry to deliver insights into your network. These insights allow you to maintain the performance of your network and to pinpoint the root cause of any issues. Marvis allows you to ask questions about your network and clients using natural language and provides direct, easy-to-understand answers

Resources

- Juniper documentation: https://www.juniper.net/documentation/us/en/mist
- Juniper support contacts: https://support.juniper.net/support/
- Training resources: https://learningportal.juniper.net/juniper/default.aspx