Juniper Networks | Engineering Simplicity

Juniper Mist Management Guide

Published
2026-01-27

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

Juniper Mist Management Guide

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

1
CHAPTER

Get Started

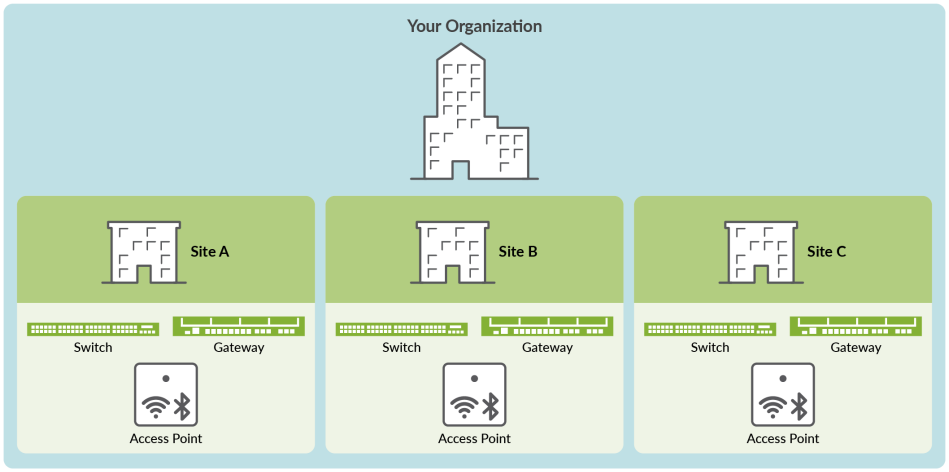
IN THIS CHAPTER

Mist Configuration Hierarchy

SUMMARY

Compare organizations, sites, and devices to understand how configuration templates and device-specific configurations are applied in Juniper Mist™.

Juniper Mist™ has a three-tier configuration hierarchy.



- Organization—At the organization level, you manage administrator accounts, your Juniper Mist subscriptions, and organization-wide settings such as single sign-on (SSO) and CA certificates. You also can set up configuration templates and device profiles, to streamline the configuration process across all sites.
- Site—An organization can include one or more sites. A site can represent a physical location or a logical sub-division or your enterprise or campus. At this level, you can set site-wide preferences for features such as analytics, automatic upgrades, and access point (AP) security. Site-level settings supersede the settings in the organization-level configuration templates.
- Devices—Devices are assigned to organizations and sites. The devices inherit certain properties from the organization-level settings, templates, device profiles, and site configuration. You can modify device settings for any devices that need settings that differ from those in the configuration templates.

NOTE: In the case of Managed Service Providers (MSPs), a fourth tier is available. MSPs can manage multiple organizations from the Juniper Mist MSP portal. Certain organization settings can come from MSP-level templates.

Putting this information into action, be aware that configuring organization- and site-level templates enables rapid deployment. Yet you have flexibility to make modifications for individual devices.

For example:

- Wireless Assurance—You can create WLAN templates and RF templates to quickly configure thousands of access points (APs) at once. Create different templates for different use cases in your organization. For example, at an office complex, use one WLAN template for IoT devices and another for guest networks. At a college campus, create one RF template to cover hallway APs and another for APs in dorm rooms.
- Wired Assurance—You can use switch templates to set up the same configurations across multiple sites. The template provides the common settings that you want to apply to all the switches. You can then make site-specific or device-specific modifications to cover the devices that need uncommon settings.
- WAN Assurance—You can use WAN Edge templates to simplify the process of SD-WAN deployment with potentially hundreds of spoke sites and headends.

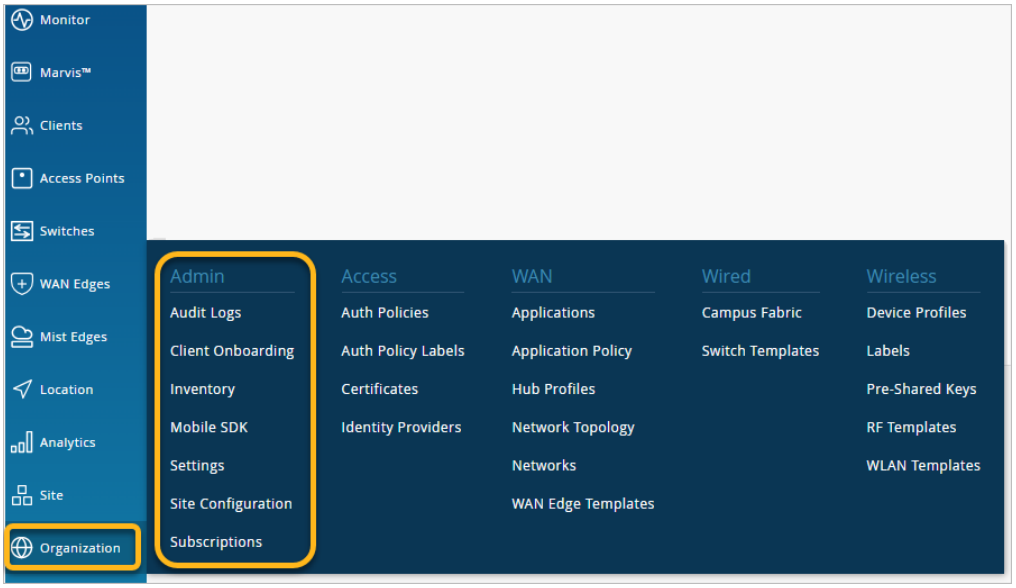
Admin Menu Overview

SUMMARY

Get familiar with the options on the Admin menu in the Juniper Mist™ portal.

You'll use this guide for help with tasks on the Admin menu in the portal. To begin, how do you find this menu?

To find the Admin menu, select **Organization** from the left menu of the Juniper Mist™ portal.



What tasks can you perform with the menu options?

- Administrators—Add and manage portal users.
- Audit Logs—View a complete record of logins.
- Inventory—View information about all devices that in your organization.
- Mobile SDK—Create and manage MobileSDK secret keys. Use the secret key to access your organization in the Juniper Mist SDK. For more information, see the Juniper Mist SDK Manuals for Android Devices and iOS Devices.
- Settings—Set up your organization.
- Site Configuration—Set up your sites.
- Subscriptions—Manage your subscriptions and orders.

NOTE: Most tasks on the Admin menu require a user account with the Super User or Network Admin role. For more information, see "Portal User Roles" on page 43.

Initial Configuration Tasks

SUMMARY

Complete these essential tasks to get started with Juniper Mist.

Table 1: Process Overview

Step	Task	More Information
1	Understand the relationships between organizations, sites, and devices in Juniper Mist.	"Mist Configuration Hierarchy" on page 2
2	Create your account and organization.	"Create Your Account and Organization" on page 6
3	Configure your firewall to allow essential traffic.	"Juniper Mist Firewall Ports and IP Addresses for Firewall Configuration" on page 19
4	Set up your sites.	"Configure a Site" on page 201
5	Set up local user accounts or enable Single Sign-On.	• "Add Accounts for Portal Users" on page 42 • "Single Sign-On for the Juniper Mist Portal" on page 54
6	Activate your subscriptions.	"Activate a Subscription" on page 148
7	Claim and adopt devices.	• "View and Update Your Device Inventory" on page 161 • "Integrate Your Juniper Support Account with Juniper Mist" on page 94 • "View Juniper Support Insights (JSI) for Your Installed Base" on page 164

Table 1: Process Overview *(Continued)*

Step	Task	More Information
8	Configure other settings to meet your business needs.	• "Organization Settings (Page Reference)" on page 85 • "Site Configuration Settings (Page Reference)" on page 202 • "Security Options" on page 16 • "Additional Information About Security" on page 81

NOTE: Also see other Juniper Mist guides for information about setting up wireless, wired, or WAN assurance.

Create Your Account and Organization

SUMMARY

Follow these steps to create your Juniper Mist™ organization.

Create your Juniper Mist™ organization by creating the first administrator account and entering a name for your organization. By default, you will have the Super User role, with full access to all the features and sites. For more information, see "Portal User Roles" on page 43.

1. Go to: https://manage.mist.com
2. At the bottom of the window, click **Create Account**.

3. Select your region.

   By selecting your region, you are selecting the location of your Juniper Mist cloud instance. For more information, see "Juniper Mist Clouds" on page 17.

4. Enter the required information.
5. Read the information about privacy, and accept or decline.

   - Select the check box if you want to allow Mist to analyze information about your interactions with the product.
   - Clear the check box to prevent Mist from conducting this analysis.

   Click the **Privacy Notice** link for more information.

6. Click **Create Account**.
   You will receive a link in your email to finalize the account setup.
7. Go to your email inbox, open the email from Mist.com, and then click the validation link.
8. Follow the on-screen prompts to log in.
9. Click **Create Organization**.
10. Enter a name for your organization.

    The organization name will appear in various places, such as the Juniper Mist login screen, the Juniper Mist portal, and any emails that Juniper Mist sends to new portal users.

> **NOTE**: You can always change the name if needed. See "Rename an Organization" on page 91.

Account Settings and Preferences

IN THIS SECTION

Account Settings

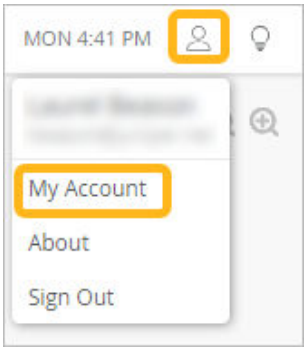
SUMMARY

Use the My Account page to update your password and preferences, create a new organization, or delete your account.

IN THIS SECTION

Find the My Account Page

At the top-right corner of the Juniper Mist™ portal, click the **Mist Account** button, and then click **My Account**.



Use the My Account page to manage your account information, password, sign-in options, and preferences. You also can generate API user tokens, and remove your account.

Change Your Contact Information

1. On the My Account page, under **Account Information**, enter your email address, name, and other information.
2. Click **Save** at the top-right corner of the page.

Change Your Password

1. On the My Account page, under **Authentication**, enter your new password.
2. Click **Save** at the top-right corner of the page.

Enable Two-Factor Authentication for Your Account

Use this procedure if you want to add two-factor authentication to your own account.

NOTE: Your administrator might require two-factor authentication for all users by setting a Password Policy on the Organization Settings page.

Juniper Mist allows you to use any authenticator app. Juniper Mist does not support two-factor authentication through SMS or email.

To set up two-factor authentication for your own account:

1. On the My Account page, under **Authentication**, select **Enable Two Factor Authentication**.
2. Click **Save** at the top-right corner of the page.

From now on, the login process will require a code from your authenticator application.

Select the MAC Address Format

Choose how to display MAC addresses in the Juniper Mist portal.

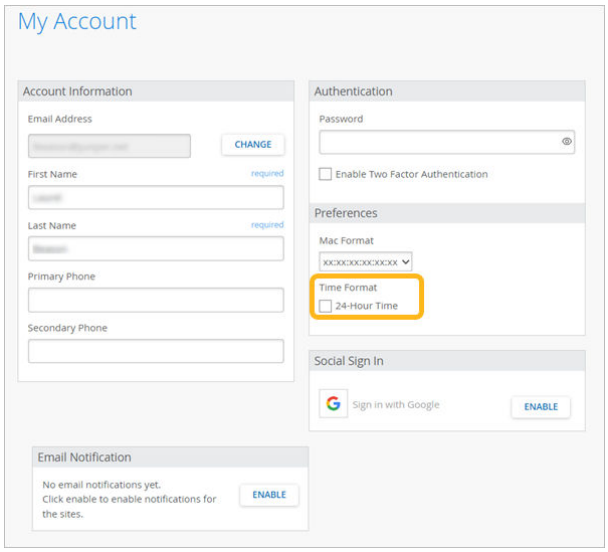
1. On the My Account page, under **Preferences**, click **Mac Format**.

2. Select the format that you prefer.
3. Click **Save** at the top-right corner of the page.

Set the Time Format

You can set a 12-hour or 24-hour time format.

1. On the My Account page, under **Preferences**, select or deselect **24-Hour Time**.



   - When the checkbox is selected, hours proceed from 00:00 (midnight) to 23:59 (11:59 p.m.).
   - When the checkbox is not selected, hours proceed from 00:00 (midnight) to 11:59 a.m., then from 12:00 p.m. (noon) to 11:59 p.m.
2. Click **Save** at the top-right corner of the page.

Create a User Token

API tokens send user identification information to the API server. API user tokens are bound to specific users. You can create a user token on the My Account page.

> **NOTE**: For more information about API tokens and automation for Juniper Mist, see the Juniper Mist Automation Guide.

1. On the My Account page, under **API Token**, click **Create Token**.
2. Enter a name for the token.
3. Click **Generate**.
4. Click the copy button next to the **Key** field.
5. Store the key somewhere for safekeeping.

The key will not be displayed anywhere in the UI after you close this window. If you misplace the key, you'll need to create a new one.

6. Click **Done**.

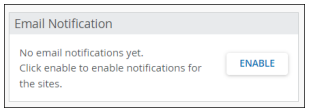
Receive Notifications of Events and Alerts

You can set up your Juniper Mist™ account so that you receive notifications of events and alerts. You can enable notifications for the entire organization or specific sites.

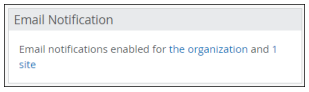
NOTE: The types of alerts are determined by the selections on the Alerts Configuration page. To find this page, select **Monitor** > **Alerts** from the left menu of the Juniper Mist portal, and then select the **Alert Configuration** button.

To manage notifications:

1. On the My Account page, go to the **Email Notification** section, and then select the appropriate option:
   - If no notifications are enabled, click **Enable** .

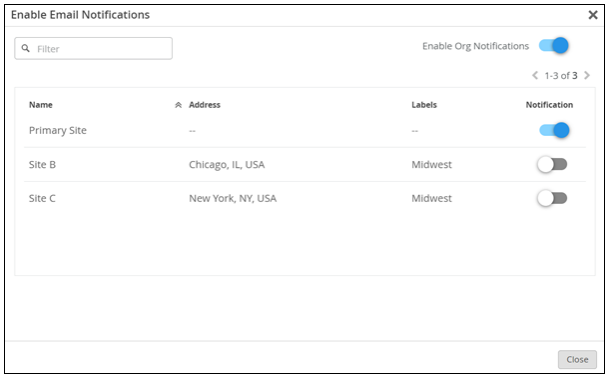


   - If you previously configured notifications, click the link text.



2. In the pop-up window, toggle the notifications on or off for the organization and for each site.

   In this example, the administrator turned on the notifications for the organization and the primary site. The administrator turned off the notifications for the other two sites.



3. Click **Close** to save your changes.

Adjust Privacy Settings

By default, Juniper Mist analyzes certain information about your interactions and recreates user sessions, which may contain personal information. This analysis enables advanced troubleshooting, provides contextual access to user guides, and is used for product enhancements. You can shut off this option if you prefer not to enable this feature.

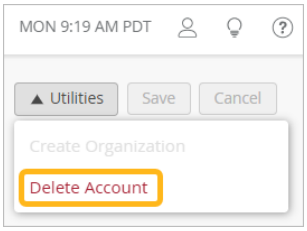
NOTE: Users also are prompted about privacy options when creating an account. If users created their account before the privacy options were implemented, they'll see a message when they log in.

1. On the My Account page, go to **Privacy Settings**.

   The screen displays the current settings. For example, you might have already accepted or declined this option in response to an on-screen prompt when creating your account or logging in.
2. Click the **Privacy Notice** link if you need more information.
3. Select the checkbox to allow Juniper Mist to analyze information, or clear the checkbox to disable this feature.
4. Click **Save** at the top-right corner of the page.

Remove Your Account

1. On the My Account page, click **Utilities**.
2. Click **Delete Account**.



3. Read the confirmation message, and then click **Delete** to remove your account.

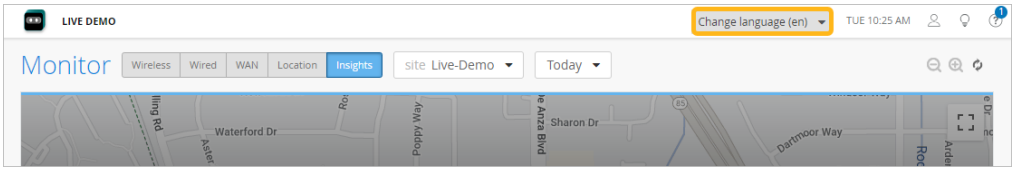
Select Your Preferred Language (Beta)

SUMMARY

Follow these steps to select the language that you want to see in the portal.

Your language selection affects only your view of the portal, not the settings for other users in your organization.

To select your preferred language, use the Change Language list near the top-right corner of the Juniper Mist portal.



The selected language is used for all text in the portal and the support site.

NOTE: Certain languages are available only to Beta participants.

2

CHAPTER

Security and Access

SUMMARY

Use the information in this section of the guide to configure your firewall, add administrator accounts, enable Single Sign-On (SSO), and manage certificates.

IN THIS CHAPTER

What Do You Want to Do?

Table 2: Top Tasks

If you want to...	Use these resources:
Set Up Your Firewall *To ensure connectivity and proper operations, configure your firewall to open the required ports and allow traffic to/from the Juniper Mist IP addresses for your region.*	"Juniper Mist Firewall Ports and IP Addresses for Firewall Configuration" on page 19
Manage Administrator Accounts *Add and remove portal access for your personnel who manage, monitor, and install Juniper Mist.*	"Add Accounts for Portal Users" on page 42
Enable Single Sign-On *Allow users to access the Juniper Mist portal by using single sign-on (SSO). You can use any identity provider (IdP) that supports Security Assertion Markup Language (SAML) 2.0.*	"Single Sign-On for the Juniper Mist Portal" on page 54
Manage Certificates *If you configure a RadSec authentication server for a wireless LAN (WLAN), copy the Juniper Mist certificate to your RadSec servers, and add the RadSec certificates to your Juniper Mist organization.*	"Manage Certificates" on page 74
Configure Juniper Mist Access Assurance *Juniper Mist Access Assurance secures your wireless and wired network by providing identity-based network access to devices and users.*	• Juniper Mist Access Assurance Product Information • Juniper Mist Access Assurance Guide

Security Options

SUMMARY

Start getting familiar with Juniper Mist™ security features.

IN THIS SECTION

Use the information in this chapter to configure your firewall, select security options for your organization, control access to the Juniper Mist portal, and monitor logins. Also explore additional resources about the security features of the Juniper Mist cloud, data privacy at Juniper, and setting up security in your wireless, wired, or WAN configuration.

End Support for Cipher Suites Using Cipher Block Chaining (CBC)

Juniper Mist has ended support of cipher suites using the Cipher Block Chaining (CBC). These cipher suites are known to be susceptible to attacks such as padding oracle attack, which can lead to data leaks and other security issues. This change affects the systems and software that rely on the following cipher suites to interact with Juniper Mist API and Mist Dashboard:

- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384

The following ciphers are supported for TLS 1.2+ protocols (Server Preferred Order):

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384

More Information

A cipher suite is a cryptographic algorithm set to secure network communications. CBC is a mode of operation for block ciphers commonly used in Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. Therefore, modern security standards recommend using more secure cipher suites, such as Galois/Counter Mode (GCM).

Juniper Mist Clouds

SUMMARY

Understand how regional clouds are used in Juniper Mist™ and look up the cloud ID for your region.

IN THIS SECTION

Regional Clouds

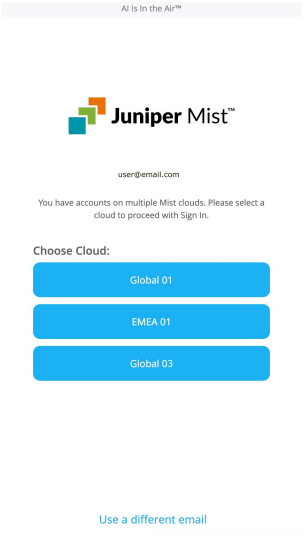
The Juniper Mist™ environment uses regional clouds and accounts for optimal performance. When creating an organization, you should use the region nearest to you.

Organizations created in one cloud are not available on another. Likewise, accounts created in one cloud do not apply to organizations on another cloud. You must create an account for each cloud where you have organizations.

Users with multiple accounts can reuse the same email ID across the different clouds whether it's a local email, SSO, or a mix between the environments.

If you have accounts on multiple clouds, you'll have the option to choose a cloud after you log in.

Global Login Across Cloud Instances



Regions and Hosting Countries

Table 3: Cloud Instances

Region	Cloud Instance	Hosting Country
GLOBAL	Global 01	Americas
	Global 02	Americas
	Global 03	Americas
	Global 04	Canada
	Global 05 (default instance for region)	Americas
	USGov 01	Americas
EMEA	EMEA 01 (default instance for region)	Germany
	EMEA 02	England

Table 3: Cloud Instances *(Continued)*

Region	Cloud Instance	Hosting Country
	EMEA 03	United Arab Emirates
	EMEA 04	Kingdom of Saudi Arabia
APAC	APAC 01 (default instance for region)	Australia
	APAC 02	India
	APAC 03	Japan

RELATED DOCUMENTATION

Juniper Mist Firewall Ports and IP Addresses for Firewall Configuration | **19**

https://www.juniper.net/documentation/us/en/software/mist/mist-management/topics/topic-map/mist-subscription-types.html

https://www.juniper.net/documentation/us/en/software/mist/mist-management/topics/ref/admin-roles.html

https://www.juniper.net/documentation/us/en/software/mist/mist-management/topics/task/install-devices-mobile-app.html

Juniper Mist Firewall Ports and IP Addresses for Firewall Configuration

SUMMARY

To ensure connectivity and proper operations of Juniper Mist™, configure your firewall to open the

IN THIS SECTION

required firewall ports and allow traffic to/from the Juniper Mist IP addresses for your region.

How To Use This Information

- Within this document, refer to the appropriate table for your regional cloud instance (such as Global 01, Global 02, and so on). For help identifying your cloud instance, see "Juniper Mist Clouds" on page 17.
- Cloud Services—The tables identify the IP addresses and ports to allow for various cloud services, as listed.
  - Admin Portal
  - API

    Guest Wi-Fi Portal
  - Webhooks Source IP Addresses
- Device Types—The tables identify the IP addresses and ports to allow for various Juniper devices. You can ignore any device types that you don't have in your organization.

- Juniper Mist Access Points and Juniper Mist Edge
- EX Series Switches
- SRX Series Firewalls
- SSR Series Routers

> **NOTE**: For terminators in the tables, use FQDN-based firewall rules. Their IP addresses will change.

- Additional Information—Also allow the ports and IP addresses in the "Additional Hosts to Allow" on page 41 section.
- You need to provide unrestricted access to debian and mistsys repo in the environments where you create the Mist Edge VM for initial bring up. Also, ensure that the Firewall has Port-80 and Port-443 open.
- You must allow outbound DNS access to 8.8.8.8 and 1.1.1.1. These addresses are hard-coded into SSR Series routers. The router must make DNS requests to one of these addresses.

Global 01

Table 4: Global 01 IP Addresses and Ports to Allow

Cloud Service or Device Type	IP Addresses and Ports
Admin Portal	manage.mist.com/signin.html (TCP 443) api-ws.mist.com (TCP 443) api.mist.com (TCP 443)
API	api.mist.com (TCP 443)
Guest Wi-Fi Portal	portal.mist.com (TCP 443)
Webhooks Source IP Addresses (static IP addresses)	54.193.71.17 54.215.237.20

Table 4: Global 01 IP Addresses and Ports to Allow *(Continued)*

Cloud Service or Device Type	IP Addresses and Ports
Juniper Mist Support	support-portal.mist.com
Juniper Mist Access Points and Juniper Mist Edge	ep-terminator.mistsys.net (TCP 443) portal.mist.com (TCP 443) redirect.mist.com (TCP 443)
EX Series Switches	redirect.juniper.net (TCP 443) jma-terminator.mistsys.net (TCP 443) ztp.mist.com (TCP 443) oc-term.mistsys.net (TCP 2200) **NOTE**: If you are using the Juniper CloudX architecture for your EX and QFX switches, also disable SSL decryption on the firewall.
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.mist.com (TCP 443) oc-term.mistsys.net (TCP 2200) signatures.juniper.net/cgi-bin/index.cgi srx-log-terminator.mist.com (TCP 6514)
SSR Series Routers	ep-terminator.mistsys.net (TCP 443) portal.mist.com (TCP 443) redirect.mist.com (TCP 443) software.128technology.com (TCP 443) rp.cloud.threatseeker.com (TCP 443)

Global 02

Table 5: Global 02 IP Addresses and Ports to Allow

Cloud Service or Device	IP Addresses and Ports
Admin Portal	manage.gc1.mist.com (TCP 443) api-ws.gc1.mist.com (TCP 443) api.gc1.mist.com(TCP 443)
API	api.gc1.mist.com (TCP 443)
Guest Wi-Fi Portal	portal.gc1.mist.com (TCP 443)
Webhooks Source IP Addresses (static IP addresses)	34.94.226.48/28 (34.94.226.48-34.94.226.63)
Juniper Mist Support	support-portal.mist.com
Juniper Mist Access Points and Juniper Mist Edge	ep-terminator.mistsys.net (TCP 443) ep-terminator.gc1.mist.com (TCP 443) portal.gc1.mist.com (TCP 443) redirect.mist.com (TCP 443)
EX Series Switches	redirect.juniper.net (TCP 443) jma-terminator.gc1.mist.com (TCP 443) ztp.gc1.mist.com (TCP 443) oc-term.gc1.mist.com (TCP 2200) cdn.juniper.net (TCP 443) **NOTE**: If you are using the Juniper CloudX architecture for your EX and QFX switches, also disable SSL decryption on the firewall.

Table 5: Global 02 IP Addresses and Ports to Allow *(Continued)*

Cloud Service or Device	IP Addresses and Ports
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.gc1.mist.com (TCP 443) oc-term.gc1.mist.com (TCP 2200) signatures.juniper.net/cgi-bin/index.cgi srx-log-terminator.gc1.mist.com (TCP 6514)
SSR Series Routers	ep-terminator.mistsys.net (TCP 443) ep-terminator.gc1.mist.com (TCP 443) portal.gc1.mist.com (TCP 443) redirect.mist.com (TCP 443) software.128technology.com (TCP 443) rp.cloud.threatseeker.com (TCP 443)

Global 03

Table 6: Global 03 IP Addresses and Ports to Allow

Cloud Service or Device	IP Addresses and Ports
Admin Portal	manage.ac2.mist.com (TCP 443) api-ws.ac2.mist.com (TCP 443) api.ac2.mist.com(TCP 443)
API	api.ac2.mist.com (TCP 443)
Guest Wi-Fi Portal	portal.ac2.mist.com (TCP 443)

Table 6: Global 03 IP Addresses and Ports to Allow *(Continued)*

Cloud Service or Device	IP Addresses and Ports
Webhooks Source IP Addresses (static IP addresses)	34.231.34.177 54.235.187.11 18.233.33.230
Juniper Mist Support	support-portal.mist.com
Juniper Mist Access Points and Juniper Mist Edge	ep-terminator.mistsys.net (TCP 443) ep-terminator.ac2.mist.com (TCP 443) portal.ac2.mist.com (TCP 443) redirect.mist.com (TCP 443)
EX Series Switches	redirect.juniper.net (TCP 443) jma-terminator.ac2.mist.com (TCP 443) ztp.ac2.mist.com (TCP 443) oc-term.ac2.mist.com (TCP 2200) cdn.juniper.net (TCP 443) **NOTE**: If you are using the Juniper CloudX architecture for your EX and QFX switches, also disable SSL decryption on the firewall.
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.ac2.mist.com (TCP 443) oc-term.ac2.mist.com (TCP 2200) signatures.juniper.net/cgi-bin/index.cgi srx-log-terminator.ac2.mist.com (TCP 6514)

Table 6: Global 03 IP Addresses and Ports to Allow *(Continued)*

Cloud Service or Device	IP Addresses and Ports
SSR Series Routers	ep-terminator.mistsys.net (TCP 443) ep-terminator.ac2.mist.com (TCP 443) portal.ac2.mist.com (TCP 443) redirect.mist.com (TCP 443) software.128technology.com (TCP 443) rp.cloud.threatseeker.com (TCP 443)

Global 04

Table 7: Global 04 IP Addresses and Ports to Allow

Cloud Service or Device	IP Addresses and Ports
Admin Portal	manage.gc2.mist.com (TCP 443) api-ws.gc2.mist.com (TCP 443) api.gc2.mist.com (TCP 443)
API	api.gc2.mist.com (TCP 443)
Guest Wi-Fi Portal	portal.gc2.mist.com (TCP 443)
Webhooks Source IP Addresses (static IP addresses)	34.152.4.85 35.203.21.42 34.152.7.156
Juniper Mist Support	support-portal.mist.com

Table 7: Global 04 IP Addresses and Ports to Allow *(Continued)*

Cloud Service or Device	IP Addresses and Ports
Juniper Mist Access Points and Juniper Mist Edge	ep-terminator.mistsys.net (TCP 443) ep-terminator.gc2.mist.com (TCP 443) portal.gc2.mist.com (TCP443) redirect.mist.com (TCP 443)
EX Series Switches	redirect.juniper.net (TCP 443) jma-terminator.gc2.mist.com (TCP 443) ztp.gc2.mist.com (TCP 443) oc-term.gc2.mist.com (TCP 2200) cdn.juniper.net (TCP 443) **NOTE**: If you are using the Juniper CloudX architecture for your EX and QFX switches, also disable SSL decryption on the firewall.
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.gc2.mist.com (TCP 443) oc-term.gc2.mist.com (TCP 2200) signatures.juniper.net/cgi-bin/index.cgi srx-log-terminator.gc2.mist.com (TCP 6514)
SSR Series Routers	ep-terminator.mistsys.net (TCP 443) ep-terminator.gc2.mist.com (TCP 443) portal.gc2.mist.com (TCP443) redirect.mist.com (TCP 443) software.128technology.com (TCP 443) rp.cloud.threatseeker.com (TCP 443)

Global 05

Table 8: Global 05 IP Addresses and Ports to Allow

Cloud Service or Device	IP Addresses and Ports
Admin Portal	manage.gc4.mist.com (TCP 443) api-ws.gc4.mist.com (TCP 443) api.gc4.mist.com (TCP 443)
API	api.gc4.mist.com (TCP 443)
Guest Wi-Fi Portal	portal.gc4.mist.com (TCP 443)
Webhooks Source IP Addresses (static IP addresses)	35.192.224.0/29 (35.192.224.0 - 35.192.224.7)
Juniper Mist Support	support-portal.mist.com
Juniper Mist Access Points and Juniper Mist Edge	ep-terminator.mistsys.net (TCP 443) ep-terminator.gc4.mist.com (TCP 443) portal.gc4.mist.com (TCP443) redirect.mist.com (TCP 443)
EX Series Switches	redirect.juniper.net (TCP 443) jma-terminator.gc4.mist.com (TCP 443) ztp.gc4.mist.com (TCP 443) oc-term.gc4.mist.com (TCP 2200) cdn.juniper.net (TCP 443) **NOTE**: If you are using the Juniper CloudX architecture for your EX and QFX switches, also disable SSL decryption on the firewall.

Table 8: Global 05 IP Addresses and Ports to Allow *(Continued)*

Cloud Service or Device	IP Addresses and Ports
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.gc4.mist.com (TCP 443) oc-term.gc4.mist.com (TCP 2200) signatures.juniper.net/cgi-bin/index.cgi srx-log-terminator.gc4.mist.com (TCP 6514)
SSR Series Routers	ep-terminator.mistsys.net (TCP 443) ep-terminator.gc4.mist.com (TCP 443) portal.gc4.mist.com (TCP443) redirect.mist.com (TCP 443) software.128technology.com (TCP 443) rp.cloud.threatseeker.com (TCP 443)

EMEA 01

Table 9: EMEA 01 IP Addresses and Ports to Allow

Cloud Service or Device	IP Addresses and Ports
Admin Portal	manage.eu.mist.com (TCP 443) api-ws.eu.mist.com (TCP 443)
API	api.eu.mist.com (TCP 443)
Guest Wi-Fi Portal	portal.eu.mist.com (TCP 443)

Table 9: EMEA 01 IP Addresses and Ports to Allow *(Continued)*

Cloud Service or Device	IP Addresses and Ports
Webhooks Source IP Addresses (static IP addresses)	3.122.172.223 3.121.19.146 3.120.167.1
Juniper Mist Support	support-portal.mist.com
Juniper Mist Access Points and Juniper Mist Edge	ep-terminator.mistsys.net (TCP 443) ep-terminator.eu.mist.com (TCP 443) portal.eu.mist.com (TCP 443) redirect.mist.com (TCP 443)
EX Series Switches	redirect.juniper.net (TCP 443) jma-terminator.eu.mist.com (TCP 443) ztp.eu.mist.com (TCP 443) oc-term.eu.mist.com (TCP 2200) cdn.juniper.net (TCP 443) **NOTE**: If you are using the Juniper CloudX architecture for your EX and QFX switches, also disable SSL decryption on the firewall.
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.eu.mist.com (TCP 443) oc-term.eu.mist.com (TCP 2200) signatures.juniper.net/cgi-bin/index.cgi srx-log-terminator.eu.mist.com (TCP 6514)

Table 9: EMEA 01 IP Addresses and Ports to Allow *(Continued)*

Cloud Service or Device	IP Addresses and Ports
SSR Series Routers	ep-terminator.mistsys.net (TCP 443) ep-terminator.eu.mist.com (TCP 443) portal.eu.mist.com (TCP 443) redirect.mist.com (TCP 443) software.128technology.com (TCP 443) rp.cloud.threatseeker.com (TCP 443)

EMEA 02

Table 10: EMEA 02 IP Addresses and Ports to Allow

Cloud Service or Device	IP Addresses and Ports
Admin Portal	manage.gc3.mist.com (TCP 443) api-ws.gc3.mist.com (TCP 443)
API	api.gc3.mist.com (TCP 443)
Guest Wi-Fi Portal	portal.gc3.mist.com (TCP 443)
Webhooks Source IP Addresses (static IP addresses)	35.234.156.66
Juniper Mist Support	support-portal.mist.com

Table 10: EMEA 02 IP Addresses and Ports to Allow *(Continued)*

Cloud Service or Device	IP Addresses and Ports
Juniper Mist Access Points and Juniper Mist Edge	ep-terminator.mistsys.net (TCP 443) ep-terminator.gc3.mist.com (TCP 443) portal.gc3.mist.com (TCP 443) redirect.mist.com (TCP 443)
EX Series Switches	redirect.juniper.net (TCP 443) jma-terminator.gc3.mist.com (TCP 443) ztp.gc3.mist.com (TCP 443) oc-term.gc3.mist.com (TCP 2200) cdn.juniper.net (TCP 443) **NOTE**: If you are using the Juniper CloudX architecture for your EX and QFX switches, also disable SSL decryption on the firewall.
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.gc3.mist.com (TCP 443) oc-term.gc3.mist.com (TCP 2200) signatures.juniper.net/cgi-bin/index.cgi srx-log-terminator.gc3.mist.com (TCP 6514)
SSR Series Routers	ep-terminator.mistsys.net (TCP 443) ep-terminator.gc3.mist.com (TCP 443) portal.gc3.mist.com (TCP 443) redirect.mist.com (TCP 443) software.128technology.com (TCP 443) rp.cloud.threatseeker.com (TCP 443)

EMEA 03

Table 11: EMEA 03 IP Addresses and Ports to Allow

Cloud Service or Device	IP Addresses and Ports
Admin Portal	manage.ac6.mist.com (TCP 443) api-ws.ac6.mist.com (TCP 443)
API	api.ac6.mist.com (TCP 443)
Guest Wi-Fi Portal	portal.ac6.mist.com (TCP 443)
Webhooks Source IP Addresses (static IP addresses)	51.112.15.151 51.112.76.109 51.112.86.222
Juniper Mist Support	support-portal.mist.com
Juniper Mist Access Points and Juniper Mist Edge	ep-terminator.mistsys.net (TCP 443) ep-terminator.ac6.mist.com (TCP 443) portal.ac6.mist.com (TCP 443) redirect.mist.com (TCP 443)
EX Series Switches	redirect.juniper.net (TCP 443) jma-terminator.ac6.mist.com (TCP 443) ztp.ac6.mist.com (TCP 443) oc-term.ac6.mist.com (TCP 2200) cdn.juniper.net (TCP 443) **NOTE**: If you are using the Juniper CloudX architecture for your EX and QFX switches, also disable SSL decryption on the firewall.

Table 11: EMEA 03 IP Addresses and Ports to Allow *(Continued)*

Cloud Service or Device	IP Addresses and Ports
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.ac6.mist.com (TCP 443) oc-term.ac6.mist.com (TCP 2200) signatures.juniper.net/cgi-bin/index.cgi srx-log-terminator.ac6.mist.com (TCP 6514)
SSR Series Routers	ep-terminator.mistsys.net (TCP 443) ep-terminator.ac6.mist.com (TCP 443) portal.ac6.mist.com (TCP 443) redirect.mist.com (TCP 443) software.128technology.com (TCP 443) rp.cloud.threatseeker.com (TCP 443)

EMEA 04

Table 12: EMEA 04 IP Addresses and Ports to Allow

Cloud Service or Device	IP Addresses and Ports
Admin Portal	manage.gc6.mist.com (TCP 443) api-ws.gc6.mist.com (TCP 443)
API	api.gc6.mist.com (TCP 443)
Guest Wi-Fi Portal	portal.gc6.mist.com (TCP 443)

Table 12: EMEA 04 IP Addresses and Ports to Allow *(Continued)*

Cloud Service or Device	IP Addresses and Ports
Webhooks Source IP Addresses (static IP addresses)	34.166.152.112/29 (34.166.152.112 - 34.166.152.119)
Juniper Mist Support	support-portal.mist.com
Juniper Mist Access Points and Juniper Mist Edge	ep-terminator.mistsys.net (TCP 443) ep-terminator.gc6.mist.com (TCP 443) portal.gc6.mist.com (TCP 443) redirect.mist.com (TCP 443)
EX Series Switches	redirect.juniper.net (TCP 443) jma-terminator.gc6.mist.com (TCP 443) ztp.gc6.mist.com (TCP 443) oc-term.gc6.mist.com (TCP 2200) cdn.juniper.net (TCP 443) **NOTE**: If you are using the Juniper CloudX architecture for your EX and QFX switches, also disable SSL decryption on the firewall.
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.gc6.mist.com (TCP 443) oc-term.gc6.mist.com (TCP 2200) signatures.juniper.net/cgi-bin/index.cgi srx-log-terminator.gc6.mist.com (TCP 6514)

Table 12: EMEA 04 IP Addresses and Ports to Allow *(Continued)*

Cloud Service or Device	IP Addresses and Ports
SSR Series Routers	ep-terminator.mistsys.net (TCP 443) ep-terminator.gc6.mist.com (TCP 443) portal.gc6.mist.com (TCP 443) redirect.mist.com (TCP 443) software.128technology.com (TCP 443) rp.cloud.threatseeker.com (TCP 443)

APAC 01

Table 13: APAC 01 IP Addresses and Ports to Allow

Cloud Service or Device	IP Addresses and Ports
Admin Portal	manage.ac5.mist.com (TCP 443) api-ws.ac5.mist.com (TCP 443) api.ac5.mist.com (TCP 443)
API	api.ac5.mist.com (TCP 443)
Guest Wi-Fi Portal	portal.ac5.mist.com(TCP 443)
Webhooks Source IP Addresses (static IP addresses)	54.206.226.168 13.238.77.6 54.79.134.226
Juniper Mist Support	support-portal.mist.com

Table 13: APAC 01 IP Addresses and Ports to Allow *(Continued)*

Cloud Service or Device	IP Addresses and Ports
Juniper Mist Access Points and Juniper Mist Edge	ep-terminator.mistsys.net (TCP 443) ep-terminator.ac5.mist.com (TCP 443) portal.ac5.mist.com (TCP 443) redirect.mist.com (TCP 443)
EX Series Switches	redirect.juniper.net (TCP 443) jma-terminator.ac5.mist.com (TCP 443) ztp.ac5.mist.com (TCP 443) oc-term.ac5.mist.com (TCP 2200) cdn.juniper.net (TCP 443) **NOTE**: If you are using the Juniper CloudX architecture for your EX and QFX switches, also disable SSL decryption on the firewall.
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.ac5.mist.com (TCP 443) oc-term.ac5.mist.com (TCP 2200) signatures.juniper.net/cgi-bin/index.cgi srx-log-terminator.ac5.mist.com (TCP 6514)
SSR Series Routers	ep-terminator.mistsys.net (TCP 443) ep-terminator.ac5.mist.com (TCP 443) portal.ac5.mist.com (TCP 443) redirect.mist.com (TCP 443) software.128technology.com (TCP 443) rp.cloud.threatseeker.com (TCP 443)

APAC 02

Table 14: APAC 02 IP Addresses and Ports to Allow

Cloud Service or Device	IP Addresses and Ports
Admin Portal	manage.gc5.mist.com (TCP 443) api-ws.gc5.mist.com (TCP 443) api.gc5.mist.com (TCP 443)
API	api.gc5.mist.com (TCP 443)
Guest Wi-Fi Portal	portal.gc5.mist.com (TCP 443)
Webhooks Source IP Addresses (static IP addresses)	34.47.180.168/29 (34.47.180.168 - 34.47.180.175)
Juniper Mist Support	support-portal.mist.com
Juniper Mist Access Points and Juniper Mist Edge	ep-terminator.mistsys.net (TCP 443) ep-terminator.gc5.mist.com (TCP 443) portal.gc5.mist.com (TCP 443) redirect.mist.com (TCP 443)
EX Series Switches	redirect.juniper.net (TCP 443) jma-terminator.gc5.mist.com (TCP 443) ztp.gc5.mist.com (TCP 443) oc-term.gc5.mist.com (TCP 2200) cdn.juniper.net (TCP 443) **NOTE**: If you are using the Juniper CloudX architecture for your EX and QFX switches, also disable SSL decryption on the firewall.

Table 14: APAC 02 IP Addresses and Ports to Allow *(Continued)*

Cloud Service or Device	IP Addresses and Ports
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.gc5.mist.com (TCP 443) oc-term.gc5.mist.com (TCP 2200) signatures.juniper.net/cgi-bin/index.cgi srx-log-terminator.gc5.mist.com (TCP 6514)
SSR Series Routers	ep-terminator.mistsys.net (TCP 443) ep-terminator.gc5.mist.com (TCP 443) portal.gc5.mist.com (TCP 443) redirect.mist.com (TCP 443) software.128technology.com (TCP 443) rp.cloud.threatseeker.com (TCP 443)

APAC 03

Table 15: APAC 03 IP Addresses and Ports to Allow

Cloud Service or Device	IP Addresses and Ports
Admin Portal	manage.gc7.mist.com (TCP 443) api-ws.gc7.mist.com (TCP 443) api.gc7.mist.com (TCP 443)
API	api.gc7.mist.com (TCP 443)
Guest Wi-Fi Portal	portal.gc7.mist.com(TCP 443)

Table 15: APAC 03 IP Addresses and Ports to Allow *(Continued)*

Cloud Service or Device	IP Addresses and Ports
Webhooks Source IP Addresses (static IP addresses)	34.104.128.8/29 (34.104.128.8 - 34.104.128.15)
Juniper Mist Support	support-portal.mist.com
Juniper Mist Access Points and Juniper Mist Edge	ep-terminator.mistsys.net (TCP 443) ep-terminator.gc7.mist.com (TCP 443) portal.gc7.mist.com (TCP 443) redirect.mist.com (TCP 443) **NOTE**: For Mist Edges to function effectively on the APAC 03 cloud instance, a new version of the tunnel termination service is required. This version will be released at a later date. If you want to use Mist Edge with the tunnel service in this region, contact your account team for guidance.
EX Series Switches	redirect.juniper.net (TCP 443) jma-terminator.gc7.mist.com (TCP 443) ztp.gc7.mist.com (TCP 443) oc-term.gc7.mist.com (TCP 2200) cdn.juniper.net (TCP 443) **NOTE**: If you are using the Juniper CloudX architecture for your EX and QFX switches, also disable SSL decryption on the firewall.
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.gc7.mist.com (TCP 443) oc-term.gc7.mist.com (TCP 2200) signatures.juniper.net/cgi-bin/index.cgi srx-log-terminator.gc7.mist.com (TCP 6514)

Table 15: APAC 03 IP Addresses and Ports to Allow *(Continued)*

Cloud Service or Device	IP Addresses and Ports
SSR Series Routers	ep-terminator.mistsys.net (TCP 443) ep-terminator.gc7.mist.com (TCP 443) portal.gc7.mist.com (TCP 443) redirect.mist.com (TCP 443) software.128technology.com (TCP 443) rp.cloud.threatseeker.com (TCP 443)

Additional Hosts to Allow

- **portal.mist.com** for WiFi captive portal
- **manage.mist.com/signin.html** for Admin UI access
- **api.mist.com** for Admin API access
- **api-ws.mist.com** for Admin websocket API access
- **support-portal.mist.com** for Admin Support Portal access

Additional Information for Access Points

- APs require TCP port 443 to connect to the Juniper Mist cloud. Optionally, you can tunnel this traffic by using Layer 2 Tunneling Protocol (L2TP).
- We also recommend opening UDP port 443 and TCP port 80. Port 443 is the primary communication channel for AP's talking to cloud (onboarding, telemetry, configuration). Port 80 is recommended as a backup.
- The Domain Name System (DNS) requires UDP port 53 to look up the cloud hostnames. However, the DNS does not need a public DNS server.
- The Dynamic Host Control Protocol (DHCP) initially requires UDP ports 67 and 68. After initial device onboarding, you can configure static IP on the device if you prefer.

- The Network Time Protocol (NTP) may require UDP port 123 in some environments. The AP will by default attempt to receive the time from pool.ntp.org. The AP can also receive time through DHCP option 42.
- The IP addresses change periodically and may resolve to something like this: ep-terminator-production-839577302.us-west-1.elb.amazonaws.com.
- Proxy settings are supported and the proxy setting is used if available, but if not the AP will still try to connect.

Ports for Access Assurance (NAC), Wired Assurance, and WAN Assurance

We recommend that you use FQDN-based firewall rules because the IP addresses for the terminators are subject to change.

For Wired and WAN Assurance, allow outbound connections to:

- **radsec.nac.mist.com** (TCP 2083)

For Access Assurance in the European Union (EU), allow outbound connections to:

- **radsec-eu.nac.mist.com**(TCP 2083)

Add Accounts for Portal Users

SUMMARY

Set up admin accounts with appropriate permissions for the various personnel who need access to your organization.

IN THIS SECTION

To add an account:

1. From the left menu, select **Organization** > **Admin** > **Administrators**.

> **NOTE**: You'll use the **Organization** > **Admin** > **Administrators** page to set up all user accounts, including non-administrators such as installers.

2. Click **Invite Administrator**.
3. Enter the user's email address and contact information.
4. Under **Administrator Roles**, read the descriptions, and then select the appropriate role.
5. Under **Site Access**, select the sites or site groups that this user can access.

   Keep the default setting of **All Sites**, or limit access to certain site groups or sites.

   To assign site groups or sites:

   a. Click the appropriate button: **Site Groups** or **Specific Sites**.

   b. Click **+** (the plus button).

   c. Select the locations that you want this user to access.
6. Click **Invite** near the top-right corner of the screen.

Juniper Mist sends an email to the specified email address. The recipient uses the emailed link to accept the invitation. Then Juniper Mist sends a confirmation email with a link to create a login.

Portal User Roles

SUMMARY

Get familiar with the various roles that you can apply to admin accounts, whether your personnel need full read-write access or limited permissions, such as Installer or Help Desk roles.

Table 16: Roles

Role	Description
Super User	Read/write access to entire organization. No restrictions. • Full access to all sites • Create new sites • Manage other administrators • Manage all device types and configuration settings

Table 16: Roles *(Continued)*

Role	Description

Org Admin	Write access to all components within the Juniper Mist portal and API, ***except administrative functions, such as:***
	• Creating or managing other admin users
	• Modifying login and authentication settings
	NOTE: The above permissions require the Super User role.
	For all sites in the entire organization, the Org Admin can view and modify:
	• Organization-level configurations:
	  • Audit logs
	  • Inventory
	  • Mobile SDK
	  • Organization settings
	  • Site configuration
	  • Subscriptions
	• Access Assurance features (with subscription):
	  • Auth policies and labels
	  • Certificates
	  • Client onboarding
	  • Endpoints
	  • Identity providers
	• WAN Assurance features (with subscription):
	  • Applications and appliacation policies

Table 16: Roles *(Continued)*

Role	Description

	• Hub profiles
	• Networks and network topology
	• WAN Edge templates
	• Wired Assurance features (with subscription):
	  • Campus fabric
	  • Switch Templates
	• Wireless Assurance features (with subscription):
	  • Device prolfes
	  • Templates for RF and WLAN
	  • Pre-shared keys
	  • Labels

Table 16: Roles *(Continued)*

Role	Description
Network Admin	Permissions depend on the sites that this person is granted access to. **All Sites**—Has the following permissions for all sites in the organization: • Modify all site-level features • Read access to your organization's audit logs and inventory • Manage all device types and configuration settings at the device level • View and update existing support tickets • Cannot claim or assign devices • Cannot configure organization-level features **Selected Sites or Site Groups**—Has limited read/write access for the specified sites: • Manage all device types and configuration settings in the sites that the account can access • No access to audit logs and inventory • No access to support tickets • Cannot configure organization-level features • Cannot claim devices **Additional Optional Permissions** You also can grant read-only access to organization level templates by selecting "Allow read access to select org level configurations" **NOTE**: Note: If a user had a Network Admin account before the August 2025 release, certain changes were made to the user's account automatically:

Table 16: Roles *(Continued)*

Role	Description
	• If the user previously had All Sites access, the user's role was elevated to Org Admin. • If the user previously had access only to selected sites/groups, the **Allow read access to select org level configurations** check box was automatically selected for the user. Thus, the user has read-only access to organization level templates.
Observer	• Read-only access to allowed sites • Read-only access to Inventory if granted access to All Sites; no access to other organization-level features
Installer	Limited access for the specified grace period • Do the initial installation for APs and switches: claim devices, assign/unassign devices, and place an AP on the floorplan • Use the API and the Juniper Mist AI app. Cannot access the portal • Cannot unclaim or remove a device from an organization

Table 16: Roles *(Continued)*

Role	Description

Helpdesk	• Read-only access to allowed sites
	• Basic device management such as upgrading, rebooting, running tests, etc. (not modifying configurations)
	• Basic RF management such as running the RF Environment, making RF recordings, etc.
	• Manual PCAP
	• Read-only access to other site-level pages:
	  • Monitor
	  • Clients
	  • Access Points
	  • Location
	  • Analytics
	  • Switches
	  • Mist Edge Devices
	  • WAN Edge Devices
	• Read access to Inventory if granted access to All Sites; no read/write access to other organization-level pages

Switch Port Operator	Can view and manage switch port configurations that are allowed by a Super User
Super Observer	Can monitor all sites and can view organization pages

Table 16: Roles *(Continued)*

Role	Description
Reporting	Read-only access to analytics tools: • Engagement Analytics • Occupancy Analytics • Network Analytics • Premium Analytics (requires subscription)
Location	Read/write access to location-related features: • Live View (add/change floorplans, zones, APs, virtual beacons, and so on) • Engagement Analytics • Occupancy Analytics
Marketing	Read-only access to location-related features: • Live View (view floorplans) • Engagement Analytics • Occupancy Analytics
Mist Edge Admin	Similar to the Super Admin role, but with access only to the Mist Edges and Mist Tunnels for the sites that the admin can access.

Revoke a User's Access

SUMMARY

Follow these steps to remove a user's access to your organization.

When users leave your company or no longer have responsibilities for Juniper, you can revoke their access to the Juniper Mist™ portal.

To revoke a user's access:

1. From the left menu, select **Organization** > **Admin** > **Administrators**.
2. Click the name of the administrator whose account you want to remove.
3. Click **Revoke Access** and then confirm the action.

User Privileges

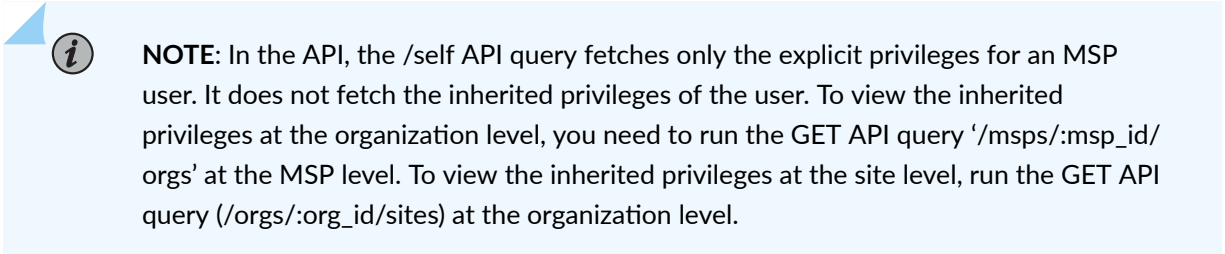
SUMMARY

Understand how conflicting privileges are resolved.

The Juniper Mist portal won't allow you to configure multiple privileges for a user; however, you can get into this situation when setting up user accounts through the API.

When different user roles are assigned at different levels (Managed Service Provider, organization, or site), the highest privilege applies.

For example, if a user has the Super User role at the organization level and the Helpdesk role at the site level, the Super User role takes effect at the site level.



NOTE: In the API, the /self API query fetches only the explicit privileges for an MSP user. It does not fetch the inherited privileges of the user. To view the inherited privileges at the organization level, you need to run the GET API query '/msps/:msp_id/orgs' at the MSP level. To view the inherited privileges at the site level, run the GET API query (/orgs/:org_id/sites) at the organization level.

Enable or Disable Juniper Mist Support Access

SUMMARY

Follow these steps to temporarily allow Juniper Mist support personnel to access your organization for troubleshooting.

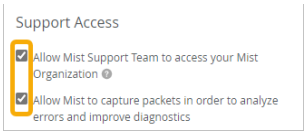
In your organization settings, you can enable or disable access for the Juniper Mist™ support team. As a best practice, disable this feature except during specific time frames when you are working with support to resolve an issue. In that situation, temporarily enable access, and disable it after the issue is resolved.

When this feature is enabled, the support personnel can:

- See all the device information in the portal.
- Capture packets. Juniper personnel do not capture payload data, only network data, for analyzing errors and improving diagnostics.

To enable or disable support access:

1. From the left menu, select **Organization** > **Admin** > **Settings**.
2. In the Support Access section, select or clear the check boxes.



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

Set a Password Policy for Your Organization

SUMMARY

If you're not using an identity provider for user logins, follow these steps to set requirements for portal passwords.

You can configure a password policy for access to your Juniper Mist™ portal.

NOTE:

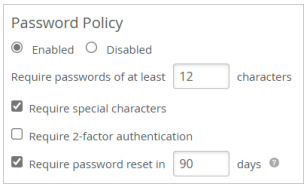
- Be sure to set the password policy to meet your organization's policy standard.
- These policies do not apply if you're using SSO for authentication because passwords are enforced via the identity provider.

1. From the left menu, select **Organization** > **Admin** > **Settings**.
2. In the Password Policy section, select **Enabled**.
3. Enter the password requirements:

   Table 17: Options for Passwords

Feature	Description
Require passwords of at least	Enter the number of characters that you want to require.
Require special characters	Users must include special characters in their passwords.
Two factor authentication	After users log in for the first time, Juniper Mist prompts them to set up two-factor authentication. From then on, they'll need to enter login credentials and a code from their authenticator app. Juniper Mist allows any choice of an authenticator app.
Require password reset	Set the number of days that passwords remain valid. Juniper Mist will prompt users to reset their passwords by displaying a reminder. It will appear in a banner, starting 14 days before password expiration.

   In this example, the password policy requires 12 characters, including special characters, and the password expires after 90 days.



4. Click **Save**.

After users register and validate their accounts, Mist prompts them to create a password that meets all the requirements. If you enabled two-factor authentication, Juniper Mist redirects them to the Account Settings page, where they must set up two-factor authentication for their account.

NOTE: As an administrator, you might want to share the two-factor setup instructions with your users for quick reference. For more information, see "Account Settings" on page 8.

Single Sign-On for the Juniper Mist Portal

SUMMARY

Understand important concepts to implement single sign-on (SSO) for the Juniper Mist™ portal.

IN THIS SECTION

You can set up your organization to allow users to access the Juniper Mist portal by using single sign-on (SSO). You can use any identity provider (IdP) that supports Security Assertion Markup Language (SAML) 2.0.

NOTE: Your IdP can be any provider that supports SAML 2.0 integrations. Examples include Azure, ADFS, Google, Okta, and more.

Requirements

- You can use any IdP that supports SAML 2.0.
- Your SAML configuration must include these attributes, with the capitalization and spacing as shown.
  - FirstName (recommended)
  - LastName (recommended)
  - NameID (required)—NameID is the unique identifier for the user account. You select the ID format (e-mail address or unspecified) when you add the IdP on the Organization Settings page. For more information, see "Add Identity Providers and Users" on page 56.
  - Role (required if you configure default_role via API)—Role is used to derive the permissions that the user should be granted. The role that you assign to the IdP account must be configured as a custom role in Juniper Mist. For more information, see "Create Custom Roles for Single Sign-On Access" on page 59.

    NOTE: If a user account is associated with multiple roles, be sure that all of them are configured as custom roles in Juniper Mist. If a role is missing, access will be denied.

Multiple Identity Providers

If you use multiple IdPs for your user accounts, you can add all the IdPs in the organization settings.

Keep in mind that an SSO user account must be associated with only one SSO. This is typically most relevant when you use different IdPs for test and production purposes. In this situation, ensure that the user's two IdP accounts are set up with different usernames (or email addresses, if that is the format that you use for NameID).

Local User Accounts

Set up at least one local user account with the Super User administrator role. This way, if there is an SSO issue, such as an expired certificate, at least one administrator will have access to the Juniper Mist portal.

Other users do not need local user accounts. With SSO, you set up the user accounts in your IdP portal, and the IdP performs authentication when the user logs in to the Juniper Mist portal. The users' assigned roles determine the features that they can access in the portal.

Add Identity Providers and Users

SUMMARY

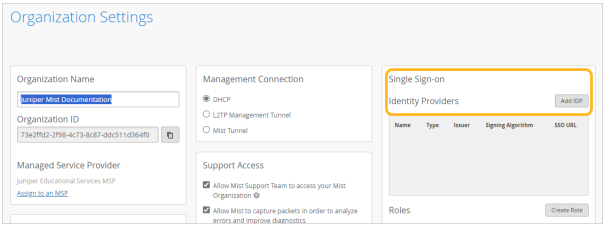
Follow these steps to add identity providers (IdPs) to use to authenticate your portal users.

Add your IdPs to your organization and then add your custom roles, delete unneeded local accounts, and provide your users with first-time login instructions.

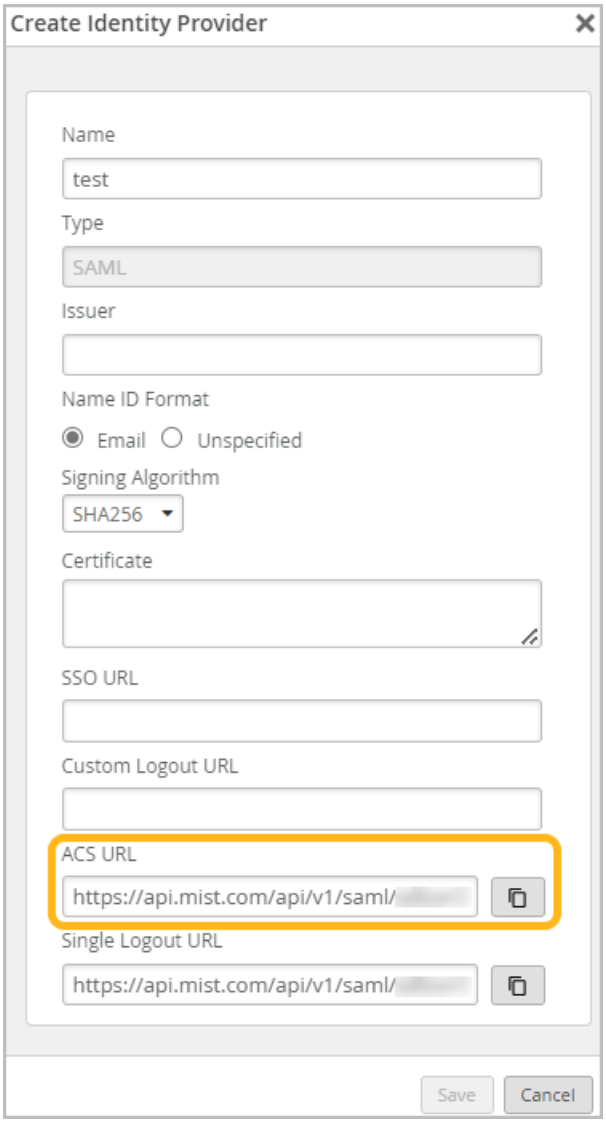
NOTE: You need the Super User admin role to configure SSO.

To add identity providers:

1. On the left menu of the Juniper Mist portal, select **Organization** > **Admin** > **Settings**.
2. In the **Identity Providers** section, click **Add IDP**.



3. In the Create Identity Provider window:
   a. Enter a name, and then click **Add**.
   b. For the **Name ID Format**, select the format that you want to use.
      Most people use the e-mail address for the name ID. If you use a different identifier for your IdP user accounts, select **Unspecified**.
   c. Copy the **ACS URL** (Assertion Consumer Service URL), which you'll need to complete the SAML 2.0 integration in your IdP's portal.



d. Keep the Create Identity Provider window open so that you can return to it later in this procedure.

4. Go to your IdP portal and complete these tasks:

- Set up the user accounts and roles for the users who will use this integration to authenticate to Juniper Mist portal.
- Create a SAML 2.0 SSO integration for Juniper Mist.

> **NOTE**: If your IdP requires metadata from Juniper Mist, see "Obtain Juniper Mist Metadata for SAML 2.0 Integration" on page 61.

- Get the following information from the SAML 2.0 SSO integration:

- Signing Algorithm
- Issuer
- SSO URL

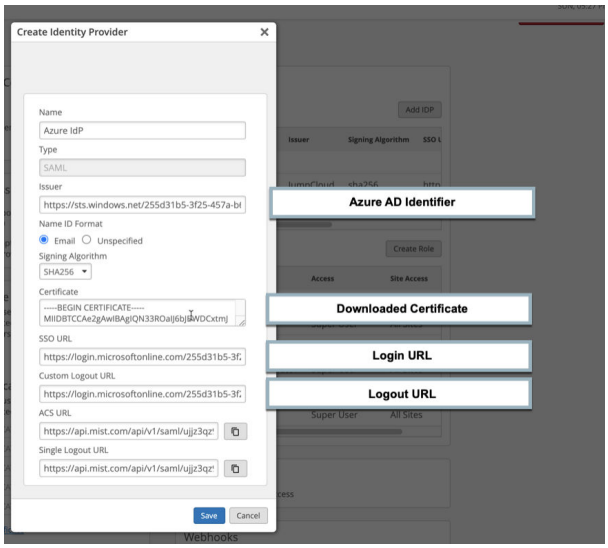
- Download the certificate.

5. Return to the Create Identity Provider in Juniper Mist, and use the information from the SAML 2.0 SSO integration to complete these fields:

   - **Signing Algorithm**—Select the same signing algorithm that you selected in your IdP SAML 2.0 integration.
   - **Issuer**
   - **SSO URL**
   - **Certificate**—Open the certificate that you downloaded. Copy the entire text and paste it into this field. Include the *BEGIN CERTIFICATE* and *END CERTIFICATE* lines.

   Example:

   This example shows how you would complete the Juniper Mist fields on the left by entering the values from the Microsoft Azure fields on the right.



6. Click **Save** to save the settings and close the window.
7. To ensure user access, complete all of the following requirements:

   - **Create custom roles.** Create custom roles corresponding to the IdP roles for your users who will access Juniper Mist through SSO. The user role determines which portal features the user can access. For help with custom roles, see "Create Custom Roles for Single Sign-On Access" on page 59.

- **Delete local accounts.**Delete any previously created admin accounts for your Mist organization, except one Super User account.

  Here's why:

  Since you want to use your IdP instead of Mist to authenticate users, their previously created Mist accounts serve no purpose. When someone uses SSO to login, that email address is "linked" to the SSO IdP, and their previously created local account cannot be used unless the SSO configuration is deleted.

  We recommend having one local account with the Super User role as an emergency backup. This way, in case SSO issues occur, one person is able to use their local account to access your Mist organization.

  Since a person cannot use one email address for both SSO and a local account, the local account should be set up with a different email address than the one they'll use with SSO. For example, use a personal email address for the local account and use the work email address for the SSO account.

  - As a Super User, you can remove account. See "Revoke a User's Access" on page 50.
  - As an admin, anyone can change the email address that they use for their Mist account. See "Account Settings" on page 8.

- **Provide first-time login instructions.** Ensure that your users understand the first-time login process. When they first log in to Juniper Mist, they must connect to Juniper Mist by using the SSO URL or their IdP dashboard. This step is necessary for the first login only, to establish the account as an SSO account. After that, they can use the SSO URL or go to directly to the Juniper Mist portal (manage.mist.com).

If errors occur, see "Troubleshoot Issues with Identity Provider Setup" on page 62.

Create Custom Roles for Single Sign-On Access

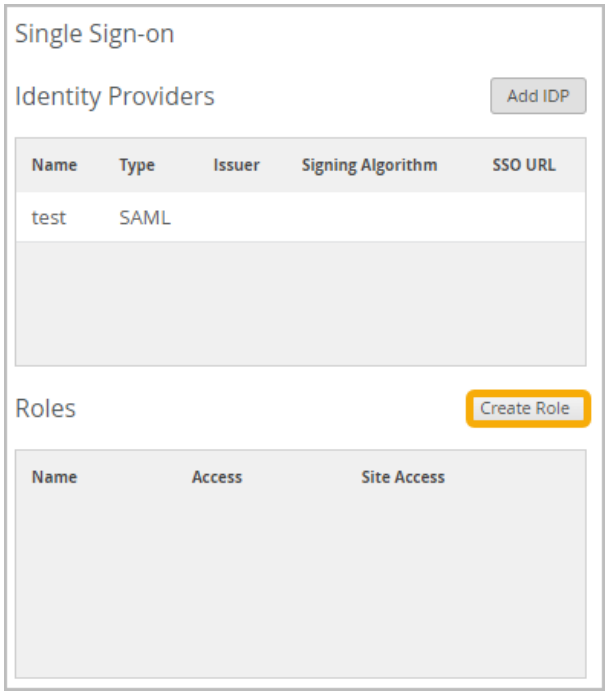
SUMMARY

Follow these steps to add all custom roles that you need for user authentication.

When you configure administrator single sign-on (SSO) for your organization, you must create custom roles in Juniper Mist™ that correspond to the roles for the user accounts in your identity provider (IdP) portal. These roles determine the permissions that users have in the Juniper Mist portal.

To create custom roles for SSO access:

1. From the left menu, select **Organization** > **Admin** > **Settings**.
2. In the Roles section of the Organization Settings page, click **Create Role**.



3. In the Create Role window, enter a name, which needs to match a role in your IdP portal.

   For example, if *super-admin* is a role in your IdP portal, enter **super-admin**.
4. Read the on-screen descriptions of the administrator roles, and then select the level of access that you want this role to have.
5. Under **Site Access**, keep the default setting of **All Sites**, or restrict access to specific sites or site groups.

   To select the sites or site groups that this role can access:

   a. Click either **Site Groups** or **Specific Sites**.

   b. Click **+** (the plus button).

   c. Select the locations that you want this role to access.
6. Click **Create**.

Obtain Juniper Mist Metadata for SAML 2.0 Integration

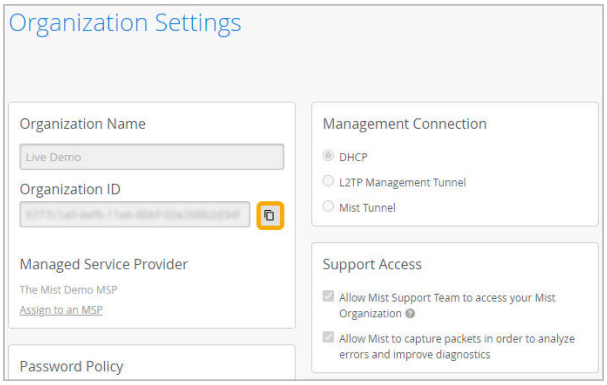
SUMMARY

When you set up a SAML 2.0 integration for Juniper Mist™, your Identity Provider (IdP) might require metadata. You can get the metadata from Juniper Mist by issuing an API call. But first you need to find your organization ID, API endpoint, and SSO ID.

IN THIS SECTION

Find Your Organization ID

From the left menu, select **Organization** > **Admin** > **Settings**. The Organization ID appears near the top of the page. You can use the copy button to quickly copy this long string.



NOTE: Juniper Mist generates this ID, which you cannot change.

Determine Your API Endpoint

You can determine the correct API endpoint for your organization by looking in the address bar of the Juniper Mist portal.

1. Log in to the Juniper Mist portal.
2. In the address bar, notice the first part of the URL, starting with the word *manage* and ending with *com*.

   Example: https://**manage.ac2.mist.com**/admin/?org_id=xxxxxxx-xxxx-xxx

   Your API endpoint is similar but starts with *api* instead of *manage*.

In the above example, the resulting API endpoint is **api.ac2.mist.com**.

TIP: The portal URL also contains your organization ID. In the URL, the organization ID section starts with these characters: *org_id=*

Find Your SSO ID

You can find your SSO ID by issuing an API call. You'll use the information you've obtained so far: your API endpoint URL and organization ID.

To find your SSO ID:

1. Issue this API call: *api_endpoint*/api/v1/orgs/:*org_id*/ssos
2. Look in the ID field to find your SSO ID.

Issue an API Call to Get the Metadata

Now that you've completed the above procedures, you have the information that you need to get the metadata. You'll use all of the information that you've obtained: your API endpoint, organization ID, and SSO ID.

To issue an API call to find your SSO ID:

Issue this API call: /api/v1/orgs/:*org_id*/ssos/:*sso_id*/metadata

Troubleshoot Issues with Identity Provider Setup

SUMMARY

This information will help you to resolve common issues when setting up a new identity provider (IdP).

IN THIS SECTION

NOTE: If you are just getting started with identity provider setup, see "Add Identity Providers and Users" on page 56.

Viewing Errors from the API

As an administrator, you can view failures via API endpoint **/api/v1/orgs/:org_id/ssos/:sso_id/failures**.

Error: Invalid Certificate

IN THIS SECTION

Problem

This error message appears during IdP setup on the Organization Settings page of the Juniper Mist™ portal.

Cause

This error indicates that the Certificate field in the IdP window is missing required information, such as the header and footer.

Solution

Download the certificate, copy the full text of the certificate (including the headers and footer), and paste the full text into the **Certificate** field on the IdP window.

First-Time Login Issues

IN THIS SECTION

Problem

This issue occurs when users are logging in to the Juniper Mist portal for the first time.

Cause

The first time that someone logs in, they need to use the SSO URL or another IdP-initiated login method. This step is necessary to establish a user's Juniper Mist account as an SSO account. After that, users can use the SSO URL or go directly to the Juniper Mist portal (manage.mist.com).

Solution

Advise users to use the SSO URL or another IdP-initiated login method the first time that they log in to the Juniper Mist portal.

Error: Email Already Taken

IN THIS SECTION

Problem

This error appears during login. It indicates that the user already has a Juniper Mist account. Typically, this error occurs when someone is trying to use the same email address for a local Juniper Mist account and an SSO account.

Solution

Consider deleting the user's local account on the Juniper Mist portal. A Juniper Mist organization requires only one local account. For all other users, a local account is not necessary. They can delete their local accounts, and this will resolve the "email already taken" issue.

Another option is to set up the two accounts (local and SSO) with different email addresses.

Missing User Names

IN THIS SECTION

Problem

In this scenario, the user name is not showing up in the Juniper Mist portal.

Cause

This issue occurs when the SAML configuration is missing the FirstName, LastName, Role, and Name ID attributes.

Solution

In the IdP portal, update the SAML configuration to include the missing attributes.

Monitor SSO Logins

The Audit Logs page lists all logins.

From the left menu, select **Organization** > **Admin** > **Audit Logs**.

The log identifies the users by name, ID, and role.

Frequently Asked Questions for SSO

SUMMARY

Get answers to common questions about Mist's SSO implementation, requirements, provisioning, and more.

IN THIS SECTION

Q: What are the basics of Mist's SSO implementation I should know?

A: Mist supports SAML2.0 based SSO in several parts of our product, with identical implementations. While this document is written for Admin SSO, we also support SSO for guest access, as well as PPSK self provisioning where the implementations are the same, except for the mandatory attributes. So this document can be applied to all of Mist's SSOs.

A user account in Mist can be one of three types of accounts, based on how it authenticates to Mist; as a local account to Mist, and SSO account, or and OAUTH2 account. An account can only be one of those types. So an SSO account would always authenticate to Mist via the IdP (unless the user changes their account type).

Make sure to sign the IdP assertion and response and return the correct attributes in the assertion with correct capitalization of the attribute names.

Q: What IdPs does Mist Support for SSO Access?

A: Mist supports any IdP that supports SAML2.0.

Q: Does Mist support SP and IdP initiated SSO?

A: Yes, Mist supports both SP and IdP initiated SSO. With the caveat that the very first login for a SSO user to Mist must be IdP initiated. Please also note for SP initiated login the entity ID entered in the IdP must be the same as ACS URL.

Q: What attributes do I need to send in my assertion?

A: These are the attributes Mist expects in the SAML assertion:

Note the capitalization is important.

- NameID
- Role

- FirstName
- LastName

NameID is required. Role is required except when you configure`default_role`via API. FirstName and LastName are recommended, or else you will see ? ? as the user's first and last names.

Q: What NameID formats do you support?

A: NameID is used as the unique identifier for the user. We support email and unspecified. Most people use email, but you can really send anything as long as you configure unspecified in the Mist SSO configuration. If you use unspecified, you can send us most anything, as long as it is unique and consistent. You will see we generate a unique ID for the user within Mist with unspecified.

Q: What is a role used for?

A: Role is used to derive the permission the user should be granted. The role returned in the assertion would match to a Role in the Mist SSO Role config on the Org settings page. Please note the user permission is dynamically generated per SSO login.

Q: Can I return multiple roles for a user?

A: Yes, if multiple roles are returned and matched, we will take the superset of the permissions. Please note, by default all roles must be matched, otherwise the user will be denied access. To allow partial matching of roles, there is an API option ignore_unmatched_roles. Alternatively, there is also an API option default_role, when no roles are matched.

We accept multiple roles in a variety of formats in the assertion. Multiple roles can be sent as comma separated, multiple AttributeValue pairs, or with CN parsing. Here are a few examples:

Comma-separated "Role" attributes

```
<Attribute Name="Role">

    <AttributeValue>"Employee,Mist,Developer"</AttributeValue>

</Attribute>
```

parsed list of roles

```
['Employee', 'Mist', 'Developer']
```

Multiple “Role” attribute values pairs

```
<Attribute Name="Role">

    <AttributeValue>"Employee"</AttributeValue>

    <AttributeValue>"Mist"</AttributeValue>

    <AttributeValue>"Developer"</AttributeValue>

</Attribute>
```

parsed list of roles

```
['Employee', 'Mist', 'Developer']
```

Combination of comma separated and multiple AV pairs

```
<Attribute Name="Role">

    <AttributeValue>"Employee,Mist"</AttributeValue>

    <AttributeValue>"Developer"</AttributeValue>

</Attribute>
```

parsed list of roles

```
['Employee,Mist', 'Developer']
```

Example of CN extraction – “role_attr_extraction”: “CN”,

```
<saml2:Attribute ="Role">

    <saml2:AttributeValue>CN=Employee,OU=groups,OU=ou1,OU=ou2</saml2:AttributeValue>

    <saml2:AttributeValue>CN=Mist,OU=groups,OU=ou1,OU=ou2</saml2:AttributeValue>

    <saml2:AttributeValue>CN=Developer,OU=ou1,OU=ou2</saml2:AttributeValue>
```

```
</saml2:Attribute>
```

parsed list of roles

```
['Employee', 'Mist', 'Developer']
```

Q: How can I troubleshoot SSO failures?

A: You can view failures by issuing this API call: *{api_endpoint}*/api/v1/orgs/:*{org_id}*/ssos/:*{sso_id}*/failures

You'll see the failure reason as well as the assertion that was received.

To issue the API call, you'll need to replace the italicized, bracketed terms with the actual values.

- *{api_endpoint}*

  If you're unsure of your organization's API endpoint URL, you can derive it from your Juniper Mist portal URL. The portal URL starts with *manage*. The corresponding API endpoint URL replaces *manage* with *api*. Notice the bolded characters in the following examples.

  Portal URL

  manage.ac2.mist.com/admin/?org_id=xxxxxxx-xxxx-xxx

  Corresponding API Endpoint URL

  api.ac2.mist.com/admin/?org_id=xxxxxxx-xxxx-xxx

- *{org_id}*

  You also can find your organization ID in the Juniper Mist portal URL. The ID appears after the characters *org_id=*. Notice the bolded characters in the following example.

  Organization ID in Portal URL

  manage.ac2.mist.com/admin/?org_id=**12345678-1a2b-3456cdef-xyz123**

- *{sso_id}*
  To find your SSO ID, issue this API call: *{api_endpoint}*/api/v1/orgs/:*{org_id}*/ssos

  Look in the ID field to find your SSO ID.

Q: Do I need to manually provision my SSO users within Mist?

A: No you don't. Access for SSO users is granted on demand by your IdP. That is to say SSO users are authenticated by the IdP, not but Mist. The access level to the Mist Dashboard is controlled by the role attribute returned in the assertion matching to a role defined in Mist.

Q: What is the first-time login process for my SSO users?

Give your SSO users your Mist organization's SSO URL for first-time login. This step is necessary for the first login only, to establish the account as an SSO account. After that, they can use the SSO URL or go to directly to the Juniper Mist portal (manage.mist.com). For more information about user setup with SSO, see "Add Identity Providers and Users" on page 56.

Q: How do I know which SSO users have accessed my Org?

A: You would check the Audit Logs under the Organization tab. You would see a log similar to: Austin Powers austin@groovy.com Login with Role "Groove-Master"

Q: Does Mist have a metadata file?

A: Yes, it can be found /api/v1/orgs/:org_id/ssos/:sso_id/metadata or /metadata.xml.

For example:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/
2000/09/xmldsig#" entityID="https://saml-x6qlonl8.mist.com"
validUntil="2032-03-29T00:44:08.503310+00:00">

<md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://api.mist.com/api/v1/saml/x6qlonl8/logout"/>

<md:NameIDFormat>

urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

</md:NameIDFormat>

<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://api.mist.com/api/v1/saml/x6qlonl8/login" index="0" isDefault="true"/>
```

```
<md:AttributeConsumingService index="0">

<md:ServiceName xml:lang="en-US">Mist</md:ServiceName>

<md:RequestedAttribute Name="Role" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic" isRequired="true"/>

<md:RequestedAttribute Name="FirstName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic" isRequired="false"/>

<md:RequestedAttribute Name="LastName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic" isRequired="false"/>

</md:AttributeConsumingService>

</md:SPSSODescriptor>

</md:EntityDescriptor>
```

Q: I need multiple SSOs in my Org. Does Mist Support that?

A: Yes, absolutely. Multiple SSOs within an Org are supported. Keep in mind, while an organization can have multiple SSOs, and a user can have permissions to multiple organizations, an SSO user in Mist can only “belong” to one SSO. This is typically most relevant when you have a “dev” and “production” SSO and use the same email for both.

Q: I have multiple organizations, can I use SSO with multiple Orgs?

A: Yes, this is also possible. It can be handled in two ways. First you have a “home” Org where you have the SSO. Then you can manually invite users to your second Org. When they login they would see both Orgs listed. The second way is to use our MSP feature (which is a controlled access feature). Where you place the SSO at the MSP Level and based on the role returned, users would have access to the MSP, or just specific orgs in the MSP.

Q: What happens when I delete an SSO within Mist?

A: When you delete an SSO, it will automatically delete all the user accounts within Mist associated with that SSO. This is particularly useful when migrating from one SSO to another, such as “dev” to “production.”

Q: How do API tokens work with SSO users?

A: SSO users are able to use Org API Tokens. Super Users can create Org API with necessary permissions. SSO users do not support “user based” API tokens. Alternatively, local service accounts can be used as well based on customer preference.

Q: Do I need a local user within Mist?

A: When you start using SSO, you can delete any previously created local user accounts in Mist, except one. It is recommend to keep a local user with the Super User role to ensure that you do not get locked out of the org in the event of an issue with the SSO. Since a person cannot use one email address for both SSO and a local account, the local account should be set up with a different email address than the one they'll use with SSO. For example, use a personal email address for the local account and use the work email address for the SSO account. For more information about steps to set up SSO users, see "Add Identity Providers and Users" on page 56.

Q: Why do I see a certificate mismatch error when setting up SSO?

A certificate mismatch error usually occurs when the Identity Provider (IdP) certificate configured in Mist does not match the certificate used by your IdP for signing SAML assertions, causing authentication failures. This error typically occurs due to missing certificate information, expired certificates, incorrect certificates, or multiple certificates in the IdP. To resolve this issue:

- Download the correct certificate from your IdP and ensure it includes the full text with headers and footers.
- Confirm that the certificate is valid. If the certificate has expired, generate a new certificate in your IdP portal and update the details in the Mist portal.
- Confirm whether the IdP has issued a new certificate and update the latest certificate information in the Mist portal.

Additionally, it is important to maintain at least one local administrator account in Mist. This ensures alternative access if SSO fails due to certificate-related issues.

Q: Why doesn't a local account convert to an SSO account when authenticating through the IdP?

When you set up Single Sign-On (SSO) and a user logs in through the Identity Provider (IdP), Mist automatically converts the user’s account from a local account to an SSO account. However, this conversion does not happen if

- The e-mail address in the IdP assertion does not exactly match the e-mail address of the user's account in Mist.
- The IdP does not send the correct attribute (such as Name ID or e-mail address) to Mist for user identification.
- The same e-mail address is tied to an SSO account in another organization.
- The local user has a role that does not map correctly to the SSO role.

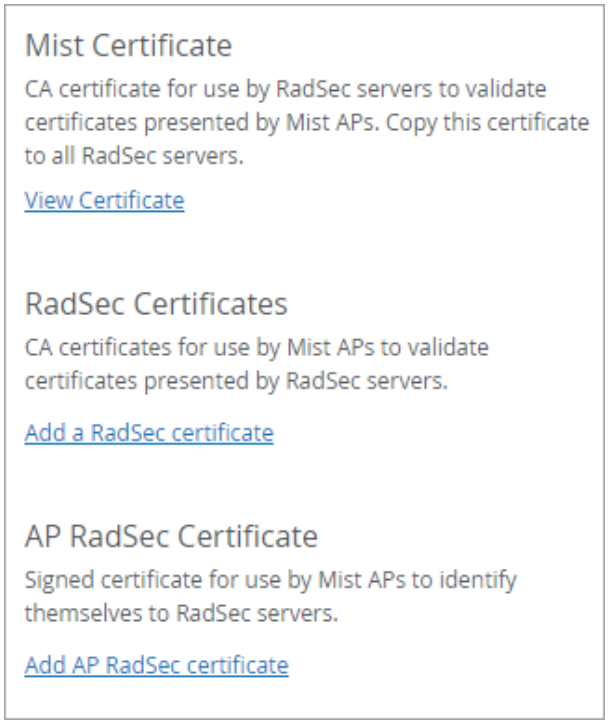
Manage Certificates

SUMMARY

Follow these steps to manage certificates for RadSec authentication.

If you configure a RadSec authentication server for a wireless LAN (WLAN), copy the Juniper Mist™ certificate to your RadSec servers, and add the RadSec certificates to your Juniper Mist organization.

1. From the left menu, select **Organization** > **Admin** > **Settings**.
2. Review the on-screen information for the certificates that you need to install.



3. Obtain or add certificates:

Table 18: Certificate Options

Feature	Description
Mist Certificate	Your RadSec servers need this certificate to validate the certificates from your access points (APs). Click **View Certificate**, and then click **Copy**. Copy this certificate to your RadSec servers.
RadSec Certificates	Juniper Mist needs these certificates so that your APs can validate the certificates from your RadSec servers. Click **Add a RadSec Certificate**. Paste the certificate that you obtained from your RadSec server, and then click **Add**.
AP RadSec Certificate	Juniper Mist needs a signed certificate so that your APs can identify themselves to your RadSec servers. Click **Add AP RadSec Certificate**. Enter the **Private Key** and the **Signed Certificate** that you obtained from your RadSec server. Then click **Save**.

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

Monitor Administrator Activities (Audit Logs)

SUMMARY

Use the Audit Logs page to monitor logins and to see what actions were taken by each user.

IN THIS SECTION

Overview

On the Audit Logs page, you can see who logged in to the Juniper Mist™ portal, when they logged in, and what they did.

When you first open this page, it shows all logins for all users and all sites on the current date. You can use the drop-down lists at the top of the page to select the time period, filter by users, filter by sites, or search for certain types of activities.

Find the Audit Logs Page

From the left menu, select **Organization** > **Admin** > **Audit Logs**.

Select the Time Period

To select the time period: Use the first drop-down menu.

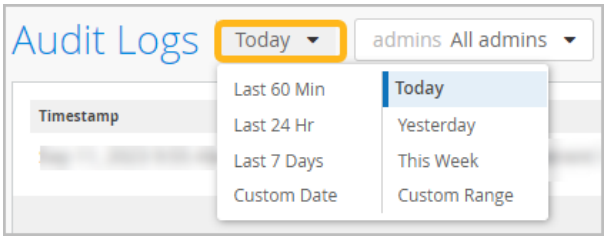
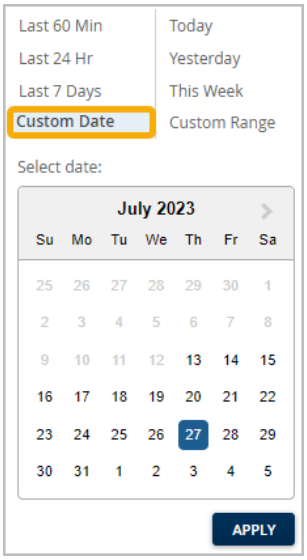
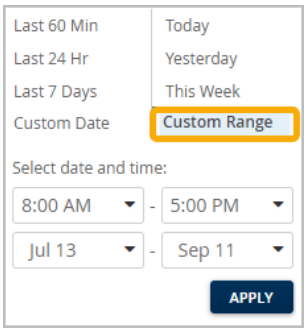


Table 19: Time Period Options

Time Period	Description
Last 60 Min	From 60 minutes ago to the current time.
Last 24 Hr	From 24 hours ago to the current time.
Last 7 Days	From the midnight 7 days ago to the current date and time.
Today	From midnight to the current time today.
Yesterday	From midnight to 11:59 PM on the previous day.
This Week	From midnight Sunday to the current date and time.

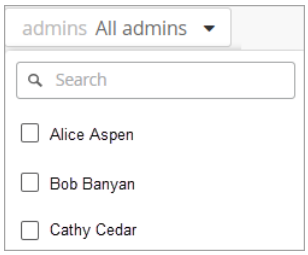
Table 19: Time Period Options *(Continued)*

Time Period	Description
Custom Date	Select a date within the past 180 days. The Audit Logs page will show all logs from midnight to 11:59 PM on the selected date. Custom Date Example 
Custom Range	Specify a range of dates within the past 180 days. On the left, enter the start time and date. On the right, enter the end time and date. Custom Range Example 

Filter by Users

1. At the top of the page, click the **Admins** drop-down menu.

   Example



2. Select the check box for the user whose logins you want to see.

   The page reloads, showing the logins for the selected user.

TIP:

- To select additional users, repeat the previous steps until the page shows all the users that you want to see.
- To quickly find a user, start typing in the **Search** box. As you type, the drop-down list shows only the names that match your search string. Select the check box for the user that you want to include.
- To deselect a user, click the **Admins** drop-down menu, and clear the check box from the user's name.

Filter by Sites

1. At the top of the page, click the **site** drop-down menu.
2. Select the check box for the site that you want to include.

   The page reloads, showing the logins at the selected site.

TIP:

- To select additional sites, repeat the previous steps until the page shows all the sites that you want to see.

- To quickly find a site, start typing in the **Search** box. As you type, the drop-down list shows only the sites that match your search string. Select the check box for the site that you want to include.
- To deselect a site, click the **site** drop-down menu, and clear the check box from the site name.

Filter by Users' Tasks

Use the **Search by Message** box to find records for particular tasks, such as accessing the organization or updating the site settings.

To filter by users' tasks:

1. Skim through the records to get familiar with the task descriptions in the **Message** column.

   Messages typically consist of a few words. These words might include:

   - An action word such as *accessed*, *update*, *add*, or *delete*.
   - The name of an organization, site, user, or other entity (such as webhook or API token) that was affected by the action.
   - The name of a feature that the user updated, such as *subscription*, *zone*, or *site settings*.
2. Start typing in the **Search by Message** box.

   As you type, the page reloads to show only the messages that contain the specified characters.

View Details

For certain types of actions, additional details are available.

If the **View details** link appears, click it to see more information about the action.

To close the View details window, click **X** in the top right corner.

Reset the Page to the Defaults

To reset the page, click the **Refresh** button in the web browser's toolbar.

Security Alerts and Advisories

SUMMARY

Security advisories are available for Juniper Mist™ and other Juniper products.

- For Juniper Mist, see Mist.com Security Alerts.

  You can subscribe via RSS feed using this link: https://www.mist.com/documentation/category/security-alerts/feed/.

- For other Juniper products, see Security Advisories in the Juniper Support Portal.

  You can subscribe to notifications via email or RSS.

  - How to subscribe to email notifications
  - How to subscribe to RSS

Additional Information About Security

SUMMARY

Follow these links to find more information about security and your Juniper products.

IN THIS SECTION

Configuring Other Security Settings

See the following guides for additional security-related information:

- Juniper Mist Access Assurance Guide—Includes information about authentication methods, identity provider integration, digital certificates, BYOD PSK, and more.

- Juniper Mist AI-Native Operations Guide—Includes information about monitoring security alerts (among other alerts that you can monitor and manage with Juniper Mist).
- Juniper Mist Automation and Integration Guide—Covers various options for automation and integration, including security procedures such as configuring an API token, and monitoring security alerts with webhooks.
- Juniper Mist WAN Assurance Configuration Guide

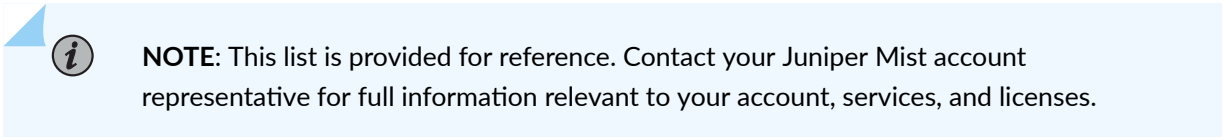
  —Contains extensive information about configuring WAN security, including options such as Secure Edge services, application policies, IDP-based threat detection, and application visibility. After your network is up and running, you can monitor the status of services such as intrusion detection and prevention, URL filtering, and application visibility.
- Juniper Mist Wired Assurance Configuration Guide—Covers additional security settings for your wired network. For example, when you add switch configuration templates, configure a campus fabric topology, and set up port profiles, you can configure a number of security settings.
- Juniper Mist Wireless Assurance Configuration Guide—Covers additional security settings for your wireless network. For example, when you add WLANs and WLAN templates or set up a guest portal, you can configure a number of security settings to protect your wireless network and ensure compliance with standards such as Payment Card Industry Data Security Standard (PCI DSS). In addition, after your network is up and running, Juniper Mist assists you in identifying potential security threats such as rogue APs, honeypots, and neighbor APs.

Additional Security Information

Juniper Mist supports SOC 2 Type II attestation of compliance (AOC). This attestation underscores our ongoing commitment to protecting customers' data. In order to obtain Juniper Mist - SOC 2 Type II report, contact your Juniper Account Representative.

For more security information, use these links below.

- Juniper Cloud Service Description - Mist AI
- Juniper Networks Purchase and License Agreement
- Juniper Network's Privacy Notice
- Juniper Mist Supplemental Information
- Juniper Mist Wired Assurance for Federal Government



NOTE: This list is provided for reference. Contact your Juniper Mist account representative for full information relevant to your account, services, and licenses.

3

CHAPTER

Your Organization

IN THIS CHAPTER

Organization Settings (Page Reference)

SUMMARY

Get familiar with the various features that you can configure on the Organization Settings page.

IN THIS SECTION

Finding the Organization Settings Page

From the left menu, select **Organization** > **Admin** > **Settings**.

Major Sections of the Organization Settings Page

Table 20: Organization Settings

Section	Description	More Information
Name ID	Basic information about the organization.	
Managed Service Provider	Displays the Managed Service Provider (MSP) if this organization is managed under an MSP account.	If you have an MSP account, you can click **Assign to an MSP** to add this organization to your MSP dashboard. Also see: Juniper Mist Managed Service Provider (MSP) Guide
Password Policy	You can specify password length, special characters, and 2-factor authentication.	"Set a Password Policy for Your Organization" on page 52

Table 20: Organization Settings *(Continued)*

Section	Description	More Information
Session Policy	Set the maximum session length and the maximum idle time for your portal users.	"Configure Session Policies" on page 93
Switch Management	You can enable or disable switch proxy.	
Firmware Upgrade—Switch Upgrades (BETA)	Set upgrades for your switches: • Upgrade Status—Check the status of a bulk upgrade process that you've scheduled. • Add Upgrade—To update multiple switches at once, schedule an upgrade. • Enable Auto Upgrade—Select the check box to enable automatic upgrades. Then click **Auto Upgrade Settings** to select the options and firmware version.	For more information about upgrade options, see "Upgrade Junos OS on Switches," in the Wired Assurance guide.
Auto-Provisioning	With auto-provisioning, you can ship APs to sites, and they'll be provisioned as your installers connect them to the network. Configure auto-provisioning to automatically assign device names, sites, and device profiles based on device attributes (for example, model, subnet, and more).	"Auto-Provisioning" on page 180

Table 20: Organization Settings *(Continued)*

Section	Description	More Information
API Token	Create access tokens for API development. The organization token behaves similarly to a user-based API token, but instead is tied to the selected organization. Set the access level and identify the sites or groups that the token can be used for.	Juniper Mist Automation Guide
Third Party Token	Generate Cellular Edge tokens for Cradlepoint integrations.	
Marvis Minis	Marvis Minis is a network digital twin, which uses your network infrastructure to assess the network connectivity and service reachability of your network. By proactively simulating user connections through an access point (AP), Marvis Minis can help detect and resolve issues before they impact users. Marvis Minis is available with a Marvis for Wireless subscription. Marvis Minis is always on and can be initiated on-demand. Options include: **Disable Marvis Minis**—Select this check box if you don't want to use Marvis Minis. **Add Custom URLs**—List URLs to be included in Marvis Minis connectivity tests. **Excluded VLANs**—List VLAND IDs that you want Marvis Minis to ignore.	Juniper Mist AI-Driven Operations Guide

Table 20: Organization Settings *(Continued)*

Section	Description	More Information
Management Connection	This setting determines how the APs handle management traffic. • DHCP (default option)—No special requirements for management traffic • L2TP Management Tunnel—Select this option when using static tunnels for secure data transfer between APs and Mist Edge. If you use this option, be sure to open UDP port 1701 on any firewalls in the traffic path. • Mist Tunnel—Select this option for Mist Edge implementations.	
Support Access	Allow or deny the Juniper support team access to certain troubleshooting data.	"Enable or Disable Juniper Mist Support Access" on page 52
Certificates	Manage certificates for use with RadSec.	"Manage Certificates" on page 74
CloudShark Integration	Integrate your CloudShark account with Juniper Mist.	
Juniper Account Integration	Add your Juniper accounts so that you can monitor your Juniper devices on the Inventory page of the Juniper Mist portal.	"Integrate Your Juniper Support Account with Juniper Mist" on page 94
Application Insights Integration (Beta)	Enables Juniper Mist to gather information from the specified applications. Click **Link Account** to go to the application's authorization page, and then log in to complete the integration.	

Table 20: Organization Settings *(Continued)*

Section	Description	More Information
Single Sign-On	Set up Identity Providers so that your team can log in to the Juniper Mist portal by using single sign-on.	"Single Sign-On for the Juniper Mist Portal" on page 54
Installer	Define the parameters for the Installer role.	"Portal User Roles" on page 43
Session Smart Conductor	Point to your Session Smart Conductor. You can enter up to two IP addresses, using a comma as a separator.	

Table 20: Organization Settings *(Continued)*

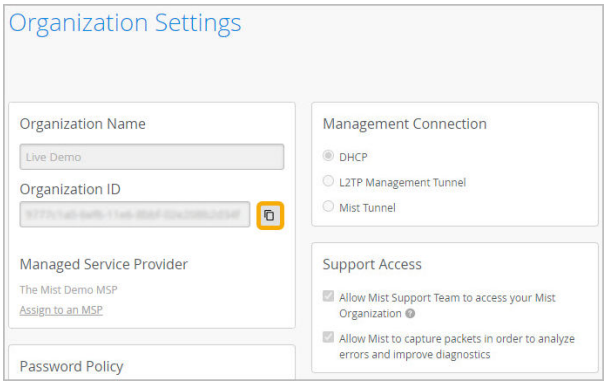
Section	Description	More Information
WAN Speed Test Scheduler	This feature is enabled by default to allow Marvis to run self-driving speed tests on your WAN interfaces automatically during low activity times. The test results are incorporated into the WAN SLE's Bandwidth Headroom classifier. To decide whether to keep the default setting or disable this feature, be aware of these factors: • This feature requires a WAN Assurance subscription. It also requires a Marvis for WAN subscription for each device that you want to run Marvis self-driving speed tests on. • This feature is recommended for WAN interfaces that are configured as Ethernet interfaces. • It's *not recommended* for devices with built-in LTE. The reason is that this feature uses bandwidth and can be costly if you pay for bandwidth usage through a service provider. You can disable this feature in the WAN interface configuration.	Juniper Mist WAN Assurance Guide
Webhooks	Enable and configure webhooks to automatically send notifications of alerts and events as they occur. After adding webhooks, you can click **View** to check the delivery status for the webhook events.	Juniper Mist Automation Guide

Find Your Organization ID

SUMMARY

Look up your organization ID, which Juniper Mist™ automatically assigns when you create a new organization.

From the left menu, select **Organization** > **Admin** > **Settings**. The Organization ID appears near the top of the page. You can use the copy button to quickly copy this long string.



NOTE: Juniper Mist generates this ID, which you cannot change.

Rename an Organization

SUMMARY

Follow these steps to change the name of your organization.

1. From the left menu, select **Organization** > **Admin** > **Settings**.

2. Enter the new **Organization Name**.
3. Click **Save**.

Delete an Organization

SUMMARY

Follow these steps if you no longer need your Juniper Mist™ organization.

First you need to remove all devices from the inventory. Then you'll delete the organization.

All sites, floorplans, and administrator accounts will be removed.

> ⚠ **CAUTION**: This action is permanent, and the data is not recoverable.

1. Log in to the organization that you want to delete.
2. Release all devices from the inventory:
   a. From the left menu, select **Organization** > **Admin** > **Inventory**.
   b. Click a device type at the top of the page.
   c. Select all devices on the page, click **More**, and then click **Release**.
   d. Repeat the above steps for each device type that has inventory, until the inventory is empty.
3. Delete the organization:
   a. From the left menu, select **Organization** > **Admin** > **Settings**.
   b. Click **Delete Organization**.

   c. When prompted to confirm the deletion, enter the organization name, and then click **Delete Organization**.

Configure Session Policies

SUMMARY

Set the maximum session length and the inactivity timer.

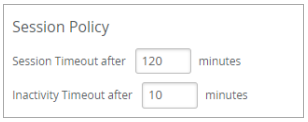
To configure session policies, select **Organization** > **Settings** from the left menu of the Juniper Mist™ portal. Then enter the timeout values.

Table 21: Timeout Options

Feature	Description
Session Timeout	Enter the maximum number of minutes that a user can remain logged in to the Juniper Mist portal. When this period elapses, the user must log in to continue working in the portal.
Inactivity Timeout	Enter the maximum number of minutes that a user can be inactive in the Juniper Mist portal. When this period elapses, the user must log in to resume working in the portal.

NOTE: The activity timer considers activity across all browser tabs where you're viewing your organization's Juniper Mist portal. The timeout won't be triggered if you're inactive on one tab but active on others.

In this example, users must log in again if their session exceeds 120 minutes or if they are inactive for more than 10 minutes.



Integrate Your Juniper Support Account with Juniper Mist

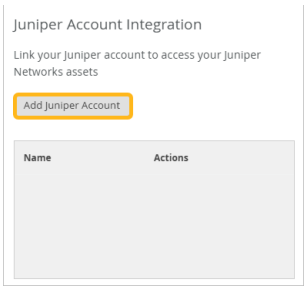
SUMMARY

For full access to Juniper device data and to features such as bug reports and security alerts, integrate your Juniper support account with Juniper Mist™.

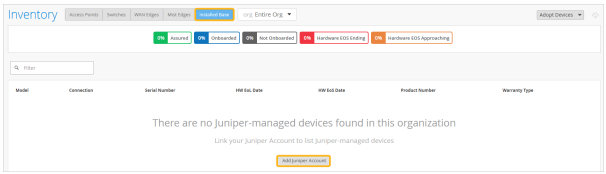
When you integrate your Juniper Account with your Juniper Mist™ organization, the Inventory page presents actionable intelligence about your Juniper devices. This information is powered by Juniper Support Insights (JSI). With these insights, you can transform your support experience from reactive to focused and proactive.

To integrate your Juniper support account with Juniper Mist:

1. Start from the Organization Settings page or the Installed Base page:
   - Organization Settings—From the left menu, select **Organization** > **Admin** > **Settings**. Under **Juniper Account Integration**, click **Add Juniper Account**.



   - Installed Base—From the left menu, select **Organization** > **Admin** > **Inventory**. At the top of the Inventory page, click the **Installed Base** button. Click **Add Juniper Account**.



2. In the pop-up window, enter the login credentials for your Juniper account, and then click **Add**.

On successful integration, the primary account name associated with your credentials is listed in the Linked Accounts section. The Linked Account section also lists other primary accounts that are currently linked to the organization.

If you no longer wish to view Juniper-maintained asset information for devices associated with an account in your organization, you can unlink the account.

To view the insights, go to **Organization** > **Admin** > **Inventory**, and then click **Installed Base** at the top of the page.

Access Juniper®Data Center Assurance

SUMMARY

To access your data center information from your Apstra account, link your Juniper Mist organization to your Juniper Data Center Assurance.

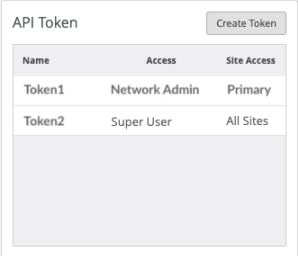
If you manage your enterprise network using Juniper Mist and your data center using Apstra, you can monitor data center events from Mist by linking the organization in Mist with the organization in Juniper Data Center Assurance. Once the organizations are linked, you can see the total number of data center events in the **Data Center/Application** leg of the Marvis Actions page in the **Data Center Actions** option in the Mist portal. You can even access Juniper Data Center Assurance by clicking **Data Center/ Application** > **Data Center Actions** to view more detailed information about data center events.

Before you begin, you need the following information:

- Login credentials with superuser permissions for your Juniper Mist portal
- Login credentials with superuser permissions for your Juniper Data Center Assurance portal
- An API token generated in Juniper Data Center Assurance

To link the Mist and Apstra organizations and allow Apstra access from Mist:

1. Log in to Juniper Data Center Assurance.
2. In the API Token section of the Organization > Settings page, click **Create Token**.

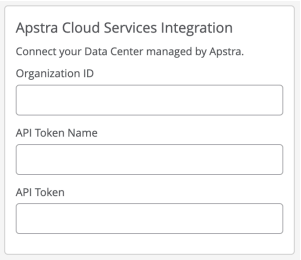


3. Log in to your Juniper Mist portal.
4. Navigate to the **Organization** > **Settings** page.
5. Locate the Data Center Assurance Integration section.

   Enter the following information:

   Table 22: Fields for Token Creation

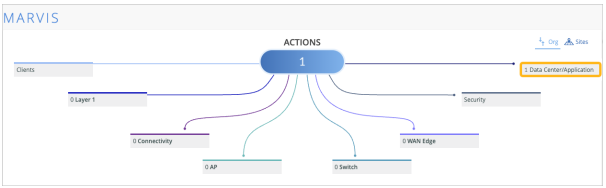
Field	Description
Organization ID	Copy the organization ID from Juniper Data Center Assurance and paste it here.
API Token Name	Enter API token name that you defined in Juniper Data Center Assurance.
API Token	Copy the API token generated in step 2 in Juniper Data Center Assurance and paste it here.



NOTE: The name of the integration section will be Apstra Cloud Services Integration until we update the Mist GUI with the name Data Center Assurance Integration.

6. Click **Save**.

   The organizations in Juniper Mist and Juniper Data Center Assurance are linked now. In a few minutes, you'll notice that the **Data Center/Application** leg in Marvis > Marvis Actions is active and displays the total number of data center events from your Apstra organization.



RELATED DOCUMENTATION

- Data Center/Application Actions
- Juniper Data Center Assurance Overview

Add Routing Assurance to the Mist Portal

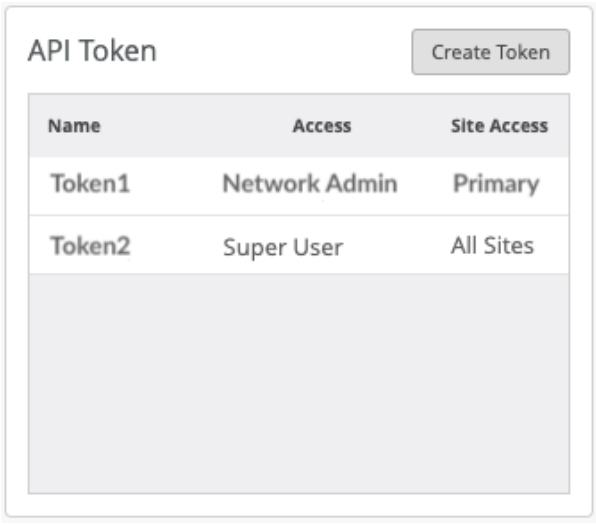
SUMMARY

Follow these steps to link your Routing Assurance account to Juniper Mist™ and to enable the WAN Edges menu in the Juniper Mist portal.

Juniper Routing Assurance is a separate AIOps-based routing platform that you can link to from the Juniper Mist portal. Juniper Routing Assurance analyzes router performance, detects network anomalies, and provides visibility into forwarding and routing health. You can also identify peering issues with upstream devices, including those of cloud providers and partners.

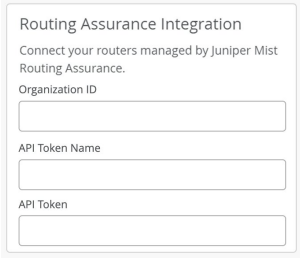
To link services, you need a SuperUser account in Juniper Routing Assurance. In addition, if your Juniper Mist account is read-only, access to Routing Access will likewise be read-only, and the same is true for read-write access. There is a limit of one Routing assurance instance per Mist organization.

Juniper Mist uses an API token from Juniper Routing Assurance to establish the link. As such, from the Juniper Routing Assurance portal, you'll need to provide the **Organization ID** and create a **API Token**. Log in to the Routing Assurance portal and select **Organization > Settings** to create a Super User token and copy the Org ID.



To link Routing Assurance to your Mist account:

1. Log in to your Juniper Mist portal.
2. Navigate to the **Organization** > **Settings** page.
3. Scroll down to the Juniper Routing Assurance section and enter the following:
   - Organization ID—Use the organization ID from the Juniper Routing Assurance portal.
   - API Token Name—Use the name from Juniper Routing Assurance.
   - API Token—Use the API token you got from the Juniper Routing Assurance portal.



4. Click **Save**.

Once linked, Juniper Routing Assurance will be available in the Juniper Mist portal in the **WAN Edges** menu. Select **Core Routers** to open Routing Assurance in a new tab, and then sign in to the Juniper Routing Assurance portal.

If Routing Assurance doesn't open when selected in the Mist menu, check for a pop-up blocker.

View Support Insights for Your Organization

SUMMARY

Use the Support Insights page to get a consolidated view of all Juniper assets that you've linked to your organization, including both cloud-connected and non-cloud connected devices.

IN THIS SECTION

Before You Begin

Complete these tasks before using the Support Insights page:0

- **Link your Juniper Account**—The Support Insights page shows data for Juniper assets with a Juniper support account that you've linked to your Juniper Mist organization. If you haven't yet linked your account, see "Integrate Your Juniper Support Account with Juniper Mist" on page 94.
- **Onboard your devices**—The Support Insights page shows data for devices that you've onboarded into this organization. If you haven't yet onboarded all devices, do so, and then they'll be included in the insights.

Navigate to the Support Insights Page

From the left menu, select **Organization** > **Admin** > **Support Insights**.

Or, if you're viewing the Installed Base page, click the **Support Insights** button near the top-right corner of the page.

Overview of the Support Insights Page

When you integrate your Juniper Account with your Juniper Mist™ organization, the Support Insights page presents actionable intelligence about your Juniper devices. This information is powered by Juniper Support Insights (JSI). With these insights, you can transform your support experience from reactive to focused and proactive.

The Support Insights page includes the Assets dashboard. This dashboard gives you a consolidated view of all the Juniper assets that you've linked to your organization, including both cloud-connected and non-cloud connected devices. With the dashboard, you can monitor all your Juniper assets in one place, track their connection status and warranty coverage, and prioritize support action to minimize operational impact.

Data includes:

- Model
- Serial Number
- Device Host Name
- Warranty Type

NOTE: Integrating your account also gives you access to device-specific support insights on the Installed Base page. See "View Juniper Support Insights (JSI) for Your Installed Base" on page 164.

Tips

- Use the search box to filter the data based on the characters that you enter.
- Click a device model to view only data for that model.
- To export the data, click the **Download CSV** button.

NOTE: Any non-English characters might appear as special characters when you open the file. To prevent this issue, follow these steps:

1. Open a new Excel file and then select **File** > **Import** > **CSV File** > **Import**.
2. Select the file to be opened and then click **Get Data**.

   The window appears.
3. In the Text Import Wizard, select **Unicode (UTF-8)** as the **File Origin**.
4. Click **Finish**.

4

CHAPTER

Subscriptions and Orders

SUMMARY

Use the information in this chapter to know the subscription options and understand how to manage your subscriptions.

IN THIS CHAPTER

What Do You Want to Do?

Table 23: Top Tasks

If you want to...	Use these resources:
Explore the subscription options for Juniper Mist *Know the subscription options available for Juniper Mist. View the list of subscriptions, tiers, and SKUs for wired, wireless, and WAN networks.*	"Subscription Types for Juniper Mist" on page 104 • "Wireless Assurance" on page 105 • "Wired Assurance" on page 109 • "WAN Assurance" on page 124 • "Access Assurance" on page 134 • "Marvis" on page 136 • "Marvis Client" on page 141 • "Location Services" on page 142 • "Premium Analytics" on page 142 • "Routing Assurance" on page 143
Know the scope of a subscription *Is a subscription applied at the organization level or site level? Learn how to apply a subscription to specific sites.*	"Juniper Mist Subscriptions Scope" on page 145
Get answers to common questions *Learn about trials, expiration, renewal, terms like "Entitled" and "Usage," API calls, and more.*	"Juniper Mist Subscriptions FAQ" on page 154
Manage subscriptions *Activate a subscription, renew a subscription, and view the status of your subscriptions.*	• "Activate a Subscription" on page 148 • "Renew a Subscription" on page 149 • "Subscription Status" on page 152

Juniper Mist Subscriptions

SUMMARY

Use the information in this chapter to explore subscription options, contact sales for subscriptions, and use the Juniper Mist™ portal to activate or renew subscriptions. You also can monitor your orders and check the status of your subscriptions.

IN THIS SECTION

Available Subscriptions

Juniper Mist™ is a subscription-based service. Juniper offers a variety of subscriptions to meet your business needs.

To learn more about these services, go to these pages:

- Juniper Mist Wi-Fi Assurance

  NOTE: Juniper Mist Wi-Fi Assurance is a mandatory subscription if you are using Juniper access points.

- Juniper Mist Access Assurance
- Juniper Mist Asset Visibility
- Juniper Mist Premium Analytics
- Juniper Mist User Engagement
- Juniper Mist WAN Assurance
- Juniper Mist Wired Assurance
- Juniper Routing Assurance
- Marvis Virtual Network Assistant
- Marvis Client

- Juniper Mist Edge

Subscription Usage

Juniper Mist subscriptions are associated with the device count, not devices. That is, the subscriptions are hardware-agnostic and are not bound to specific device serial numbers. Consider this example:

- You buy 10 devices and 10 subscriptions.
- You install 5 devices at Site A and 5 devices at Site B, using the 10 subscriptions. You now have used your subscriptions.
- If a device fails, you can replace it with another device (such as an RMA replacement or a spare) without needing a new subscription, provided the number of active devices in use does not exceed 10. When an RMA device comes back, you can keep it in your inventory as a spare.
- You can also move devices between sites. For example, you can move two devices from Site B to Site A or to another site.

Managing Subscriptions in the Juniper Mist Portal

After you purchase a subscription, you can activate and manage it in the Juniper Mist portal. On the left menu of the Juniper Mist portal, select **Organization** > **Admin** > **Subscriptions**.

Subscription Types for Juniper Mist

SUMMARY

Explore the various subscription types available for Mist.

IN THIS SECTION

Juniper Mist supports subscription-based cloud services. Mist provides subscriptions that cover the wireless, wired, and WAN domains. You can opt for subscription bundles for 1-year, 3-year, or 5-year terms or standalone subscriptions based on your requirements.

Wireless Assurance

IN THIS SECTION

Wireless Assurance provides key features that you would require in your day-to-day operations such as RRM, SLEs, dynamic packet capture, guest Wi-Fi access, and WLAN policy creation. For more information about the features, see Overview of Juniper Mist Wireless Assurance.

Table 24 on page 105 lists the details of the Wireless Subscription SKUs.

Table 24: Wireless Assurance Subscriptions

Subscription SKU	Description	SKU Character Definition
SUB-MAN-1Y|3Y|5Y	Wireless Assurance subscription for a specified term.	SUB—Subscription MAN—Wireless Assurance 1Y|3Y|5Y—Subscription term in years

Associated Subscriptions for Wireless Assurance

Associated subscriptions are optional subscriptions that you can use with the Wireless Assurance subscription to enable additional capabilities on the Mist wireless network. You can opt for associated subscriptions as either standalone subscriptions or subscription bundles, provided you have a Wireless Assurance (SUB-MAN) subscription.

You can also opt for a combination of an Access Point (AP) and a subscription bundle in one subscription (a combo bundle).

The following tables list the associated subscriptions that you can order in addition to the mandatory Wireless Assurance (SUB-MAN) subscription.

Table 25: Associated Standalone Subscriptions for Wireless Assurance

Subscription SKU	Description	SKU Character Definition
SUB-AST-1Y|3Y|5Y	Asset Visibility subscription that allows you to quickly locate key resources in your organization using virtual Bluetooth beacons. See Asset Visibility **NOTE**: SUB-MAN, SUB-ENG, and SUB-AST are site-level subscriptions. The number of subscriptions must match the number of APs in a site.	SUB—Subscription AST—Asset Visibility PMA—Premium Analytics ENG—User Engagement VNA—Marvis 1Y|3Y|5Y—Subscription term in years
SUB-PMA-1Y|3Y|5Y	Premium Analytics subscription that provides insights across your wired, wireless, and WAN networks. Premium Analytics allows you to run reports at a more granular level and can store and manage historic data up to 13 months. See Premium Analytics.	

Table 25: Associated Standalone Subscriptions for Wireless Assurance *(Continued)*

Subscription SKU	Description	SKU Character Definition
SUB-ENG-1Y|3Y|5Y	User Engagement subscription that uses Virtual BLE (vBLE) array technology to improve the accuracy of real-time indoor location services, from wayfinding to location-based proximity notifications. See User Engagement. **NOTE**: SUB-ENG is supported only on APs with vBLE support.	
SUB-VNA-1Y|3Y|5Y	Marvis Virtual Network Assistant subscription that provides a comprehensive view of your network from an organizational level to a client level with detailed insights. Marvis simplifies troubleshooting, and provides an enhanced user experience. See Marvis Virtual Network Assistant .	

Table 26: Associated Subscription Bundles for Wireless Assurance

Subscription SKU	Description	SKU Character Definition
Subscription Bundles		
SUB-1S|2S|3S-1Y|3Y|5Y	Subscription for a specific number of subscriptions for one AP for a specific duration.	SUB—Subscription 1S|2S|3S—Subscription for a specific number of services You can specify the subscriptions that you want (SUB-MAN, SUB-ENG, SUB-AST, SUB-VNA, or SUB-PMA). 1Y|3Y|5Y—Subscription term in years

Table 26: Associated Subscription Bundles for Wireless Assurance *(Continued)*

Subscription SKU	Description	SKU Character Definition
SUB-AI-1Y|3Y|5Y	Subscription for all services for one AP for a specific duration.	SUB—Subscription AI—Subscriptions for all services (SUB-MAN, SUB-ENG, SUB-AST, SUB-VNA, SUB-PMA) 1Y|3Y|5Y—Subscription term in years
Combo Bundles (AP and a subscription bundle)		
MIST-AP*xx*-1S|2S|3S-1Y|3Y|5Y	AP hardware and subscription for a specific number of services for a specific duration.	MIST—Mist APxx—AP model number. See Juniper Mist Access Points for the list of supported APs. AI—Subscription for all services (SUB-MAN, SUB-ENG, SUB-AST, SUB-VNA, and SUB-PMA). **NOTE**: For BT11, only SUB-ENG and SUB-AST services are available. 1S|2S|3S—Subscription for a specific number of services. 1Y|3Y|5Y—Subscription term in years.
MIST-AP*xx*-AI-1Y|3Y|5Y	AP hardware and subscription for all services for a specific duration.	
MIST-BT11-1S|2S-1Y|3Y|5Y	BT11 hardware and subscription for specific services for a specific duration.	
MIST-BT11-AI-1Y|3Y|5Y	BT11 hardware and subscription for all services for a specific duration.	

Subscriptions for Mist Edges

The Mist Edge solution helps organizations to maintain a centralized datapath architecture for campus or branch deployments. You'll need a Mist Edge device and Mist Edge subscriptions to deploy the solution.

NOTE: Ensure that the number of Mist Edge subscriptions matches the number of APs tunneling to the Mist Edges in your organization.

For more information about Mist Edges, see Juniper Mist Edge Overview.

Table 27: Subscriptions for Mist Edges

Subscription SKU	Description	SKU Character Description
S-ME-S-1|3|5	Subscription for Mist Edge (data tunneling service) for one AP for a specific duration.	S—Software ME—Mist Edge S—Standard 1|3|5—Subscription term in years

Wired Assurance

IN THIS SECTION

You can operate and manage the Juniper Networks® EX Series and QFX Series switches either in standalone mode or through the Juniper Mist cloud. This section covers information about the cloud-based subscriptions for managing your switches through Juniper Mist. For information about licenses needed for standalone mode, see Software Licenses for EX Series Switches and Software Licenses for QFX Series Switches.

Wired Assurance Subscriptions

Subscriptions for switches are based on the following:

- Tiers
  - Standard—Supports basic Layer 2/3 features and is included with the switch hardware.
  - Advanced—Supports advanced Layer 2/3 features such as IGMP, OSPF, and VRF.

  - Premium—Supports advanced Layer 3 protocols such as BGP and ISIS.

- Class (based on number of access ports)
- Term (1,3, or 5-year subscription)

For more information, see Software License Model Overview.

You can use one of the following options to manage your switches though the Juniper Mist cloud:

- Wired Assurance subscription with optional associated subscriptions (Marvis and Premium Analytics) based on your requirement.

  NOTE:
  Marvis is an optional, associate subscription that you can use with the base Wired Assurance subscription. A Marvis subscription cannot operate without an active Wired Assurance subscription.

- Subscription bundles
- Flex licenses, which include subscription bundles and Junos feature sets. You can order the Premium Analytics subscription separately. For more information about flex licenses, see "Flex Term Subscriptions for Switches" on page 121.

NOTE: For information about standalone (Flex Perpetual) licenses, see:

- Flex Three-Tier License Model SKUs Definition for EX Series Switches
- Flex Three-Tier License SKUs Definition for QFX Series Switches

Figure 1 on page 111 summarizes the Mist cloud subscription options for switches.

Figure 1: Mist Cloud Subscription Options for EX Series and QFX Series Switches

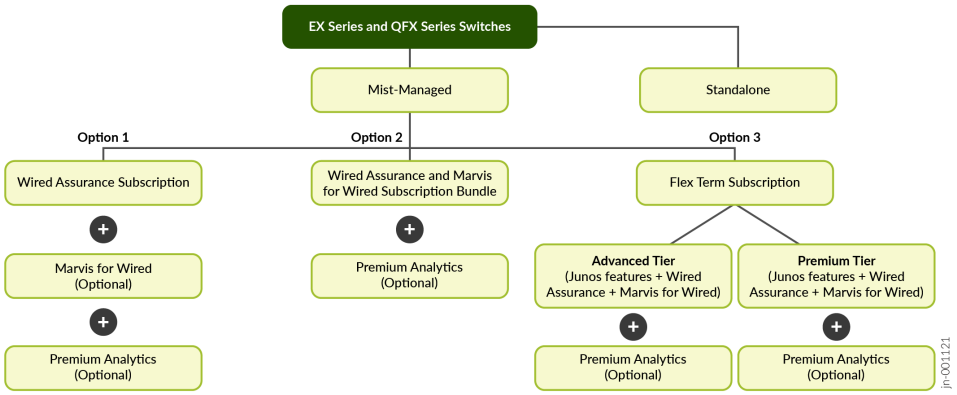


Table 28: Wired Assurance Subscription SKUs for Mist-Managed Switches (Option 1)

Device	Subscription SKU	SKU Character Description
Class 1, 12-port switches		
EX2300-C-12T/P EX4100-F-12T/P	SUB-EX12-1S -1Y|3Y|5Y-[COR|N|S] SUB-EX12-1S-1|3|5-[AC|P|CAC|CP|SAC|SP|NAC|NP]	SUB—Subscription EX12—12-port EX Series switches 1S—Wired Assurance subscription 1Y|3Y|5Y—Subscription term in years [COR|N|S]/[AC|P|CAC|CP|SAC|SP|NAC|NP]—Customer support type. See "Customer Support Services for EX-Series and QFX-Series Switches" on page 124.
Class 2, 24-port switches		

Table 28: Wired Assurance Subscription SKUs for Mist-Managed Switches (Option 1) *(Continued)*

Device	Subscription SKU	SKU Character Description
EX2300-24T/P/MP EX4100-F-24T/P EX3400-24T/P EX4100-24T/P/MP EX4300-24T/P EX4400-24T/24X/P/MP	SUB-EX24-1S-1Y|3Y|5Y-[COR|N|S] SUB-EX24-1S-1|3|5-[AC|P|CAC|CP|SAC|SP|NAC|NP]	SUB—Subscription EX24—24-port EX Series switches 1S—Wired Assurance subscription 1Y|3Y|5Y—Subscription term in years [COR|N|S]/[AC|P|CAC|CP|SAC|SP|NAC|NP]—Customer support type. See "Customer Support Services for EX-Series and QFX-Series Switches" on page 124.
Class 3, 32-port or 48-port switches		
EX2300-48T/P/MP EX3400-48T/P EX4100-F-48T/P EX4100-48T/P/MP EX4300-32F EX4300-48T/P/MP EX4400-48T/P/MP/F	SUB-EX48-1S-1Y|3Y|5Y-[COR|N|S] SUB-EX48-1S-1|3|5-[AC|P|CAC|CP|SAC|SP|NAC|NP]	SUB—Subscription EX48—32-port or 48-port EX Series switches 1S—Wired Assurance subscription 1Y|3Y|5Y—Subscription term in years [COR|N|S]/[AC|P|CAC|CP|SAC|SP|NAC|NP]—Customer support type. See "Customer Support Services for EX-Series and QFX-Series Switches" on page 124.

Table 28: Wired Assurance Subscription SKUs for Mist-Managed Switches (Option 1) *(Continued)*

Device	Subscription SKU	SKU Character Description
EX4600 EX4650	SUB-EX48-1S-1Y|3Y|5Y-46C|N|S SUB-EX46-1S-1|3|5-[CAC|CP|SAC|SP|NAC|NP]	
QFX5120-48Y/YM/T/S QFX5110-48S	SUB-EX48-1S-1Y|3Y|5Y SUB-EX48-1S-1|3|5-[AC|P|CAC|CP|SAC|SP|NAC|NP]	
Class 4 switches		
EX9204 QFX5110-36Q QFX5120-32C QFX5130-32CD QFX5700 QFX10002-36Q	S-SW-S-C4-1|3|5	S—Software SW—Switch S—Wired Assurance subscription C4— Class 4 switch 1|3|5—Subscription term in years
Class 5 switches		
EX9208 QFX10002-60C QFX10002-72Q	S-SW-S-C5-1|3|5	S—Software SW—Switch S—Wired Assurance subscription C5— Class 5 switch 1|3|5—Subscription term in years

Table 28: Wired Assurance Subscription SKUs for Mist-Managed Switches (Option 1) *(Continued)*

Device	Subscription SKU	SKU Character Description
Class 6 switches		
EX9214	S-SW-S-C6-1|3|5	S—Software SW—Switch S—Wired Assurance subscription C6— Class 6 switch 1|3|5—Subscription term in years
Class 7 switches		
QFX10008	S-SW-S-C7-1|3|5	S—Software SW— Switch S—Wired Assurance subscription C7— Class 7 switch 1|3|5—Subscription term in years
Class 8 switches		
QFX10016	S-SW-S-C8-1|3|5	S—Software SW—Switch S—Wired Assurance subscription C8— Class 8 switch 1|3|5—Subscription term in years

Associated Subscriptions and Subscription Bundles for Wired Assurance

Associated subscriptions are optional subscriptions that you can use with Wired Assurance to enable additional capabilities on the Mist wired network. These associated subscriptions cannot operate without a Wired Assurance subscription.

Along with your Wired Assurance subscription, you can order the optional Marvis for Wired and Premium Analytics subscriptions. You can also opt to order subscription bundles. The following tables list the associated subscriptions that you can order in addition to the Wired Assurance subscription.

Table 29: Marvis for Wired Subscriptions

Device	**Subscription SKU**	SKU Character Description
Class 1, 12-port switches		
EX2300-C-12T/P EX4100-F-12T/P	SUB-EX-VNA-1Y|3Y|5Y	SUB—Subscription EX—EX switch VNA—Marvis subscription 1Y|3Y|5Y—Subscription term in years
Class 2, 24-port switches		
EX2300-24T/P/MP EX4100-F-24T/P EX3400-24T/P EX4100-24T/P/MP EX4300-24T/P EX4400-24T/24X/P/MP	SUB-EX-VNA-1Y|3Y|5Y	SUB—Subscription EX—EX switch VNA—Marvis subscription 1Y|3Y|5Y—Subscription term in years
Class 3, 32-port or 48-port switches		

Table 29: Marvis for Wired Subscriptions *(Continued)*

Device	**Subscription SKU**	SKU Character Description
EX2300-48T/P/MP EX3400-48T/P EX4100-F-48T/P EX4100-48T/P/MP EX4300-32F EX4300-48T/P/MP EX4400-48T/P/MP/F	SUB-EX-VNA-1Y|3Y|5Y	SUB—Subscription EX—EX switch VNA—Marvis subscription 1Y|3Y|5Y—Subscription term in years
EX4600 EX4650	SUB-EX-VNA-1Y|3Y|5Y	
QFX5120-48Y/YM/T/S QFX5110-48S	SUB-EX-VNA-1Y|3Y|5Y	
Class 4 switches		

Table 29: Marvis for Wired Subscriptions *(Continued)*

Device	**Subscription SKU**	SKU Character Description
EX9204 QFX5110-36Q QFX5120-32C QFX5130-32CD QFX5700 QFX10002-36Q	S-SW-WA-VNA-C4-1|3|5	S—Software SW—Switch WA—Wired Assurance VNA—Marvis subscription C4— Class 4 switch 1|3|5—Subscription term in years
Class 5 switches		
EX9208 QFX10002-60C QFX10002-72Q	S-SW-WA-VNA-C5-1|3|5	S—Software SW—Switch WA—Wired Assurance VNA—Marvis subscription C5— Class 5 switch 1|3|5—Subscription term in years
Class 6 switches		
EX9214	S-SW-WA-VNA-C6-1|3|5	S—Software SW—Switch WA—Wired Assurance VNA—Marvis subscription C6— Class 6 switch 1|3|5—Subscription term in years

Table 29: Marvis for Wired Subscriptions *(Continued)*

Device	**Subscription SKU**	SKU Character Description
Class 7 switches		
QFX10008	S-SW-WA-VNA-C7-1|3|5	S—Software SW—Switch WA—Wired Assurance VNA—Marvis subscription C7— Class 7 switch 1|3|5—Subscription term in years
Class 8 switches		
QFX10016	S-SW-WA-VNA-C8-1|3|5	S—Software SW—Switch WA—Wired Assurance VNA—Marvis subscription C8— Class 8 switch 1|3|5—Subscription term in years

Table 30: Premium Analytics Subscriptions for Switches

Subscription SKU	Description	SKU Character Definition
SUB-PMA-1Y|3Y|5Y-[AC|P]	Premium Analytics subscription for a specified term with or without customer support.	SUB—Subscription PMA—Premium Analytics 1Y|3Y|5Y—Subscription term in years AC—Advanced Care P—Premium Care

Table 31: Subscription Bundles for Mist-Managed Switches (Option 2)

Device	Subscription SKU	SKU Character Description
Class 1, 12-port switches		
EX2300-C-12T/P EX4100-F-12T/P	SUB-EX12-2S -1Y|3Y|5Y-[COR|N|S] SUB-EX12-2S-1|3|5-[AC|P|CAC|CP|SAC|SP|NAC|NP]	SUB—Subscription EX12—12-port EX Series switches 2S—Wired Assurance and Marvis subscription 1Y|3Y|5Y—Subscription term in years [COR|N|S]/[AC|P|CAC|CP|SAC|SP|NAC|NP]—Customer support type. See "Customer Support Services for EX-Series and QFX-Series Switches" on page 124.
Class 2, 24-port switches		
EX2300-24T/P/MP EX4100-F-24T/P EX3400-24T/P EX4100-24T/P/MP EX4300-24T/P EX4400-24T/24X/P/MP	SUB-EX24-2S-1Y|3Y|5Y-[COR|N|S] SUB-EX24-2S-1|3|5-[AC|P|CAC|CP|SAC|SP|NAC|NP]	SUB—Subscription EX24—24-port EX Series switches 2S—Wired Assurance and Marvis subscription 1Y|3Y|5Y—Subscription term in years [COR|N|S]/[AC|P|CAC|CP|SAC|SP|NAC|NP]—Customer support type. See "Customer Support Services for EX-Series and QFX-Series Switches" on page 124.
Class 3, 32-port or 48-port switches		

Table 31: Subscription Bundles for Mist-Managed Switches (Option 2) *(Continued)*

Device	Subscription SKU	SKU Character Description
EX2300-48T/P/MP EX3400-48T/P EX4100-F-48T/P EX4100-48T/P/MP EX4300-32F EX4300-48T/P/MP EX4400-48T/P/MP/F	SUB-EX48-2S-1Y|3Y|5Y-[COR|N|S] SUB-EX48-2S-1|3|5-[AC|P|CAC|CP|SAC|SP|NAC|NP]	SUB—Subscription EX48—32-port or 48-port EX Series switches 2S—Wired Assurance and Marvis subscription 1Y|3Y|5Y—Subscription term in years [COR|N|S]/[AC|P|CAC|CP|SAC|SP|NAC|NP]—Customer support type. See "Customer Support Services for EX-Series and QFX-Series Switches" on page 124.
EX4600 EX4650	SUB-EX48-2S-1Y|3Y|5Y-46C|N|S SUB-EX46-2S-1|3|5-[CAC|CP|SAC|SP|NAC|NP]	
QFX5120-48Y/YM/T/S QFX5110-48S	SUB-EX48-2S-1Y|3Y|5Y SUB-EX48-2S-1|3|5-[AC|P|CAC|CP|SAC|SP|NAC|NP]	
Class 4 switches		

Table 31: Subscription Bundles for Mist-Managed Switches (Option 2) *(Continued)*

Device	Subscription SKU	SKU Character Description
EX9204 QFX5110-36Q QFX5120-32C QFX5130-32CD QFX5700 QFX10002-36Q	S-SW-A-C4-1|3|5	S—Software SW—Switch A—Wired Assurance and Marvis subscription C4— Class 4 switch 1|3|5—Subscription term in years

Flex Term Subscriptions for Switches

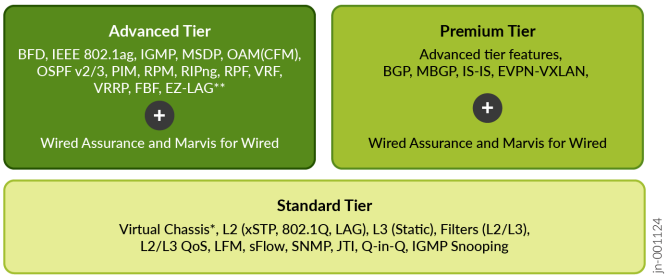
Flex term subscriptions for Wired Assurance are special types of subscription bundles which include Wired Assurance, Marvis and Junos Flex Advanced or Premium subscriptions. Flex term subscriptions for switches include Wired Assurance and Marvis subscriptions by default. If you need Premium Analytics, then you'll need to order it separately.

When you add flex term subscriptions in the Juniper Mist portal, the Junos Flex Advanced or Premium capabilities on the EX Series switches are automatically activated.

The flex term subscriptions are classified under the following tiers:

- Standard— Supports basic Layer 2 (L2) or Layer 3 (L3) features. This subscription is included as part of the EX-Series hardware.
- Advanced— Supports advanced L2 or L3 features such as IGMP, OSPF, VRF, and EZ-LAG.
- Premium—Supports advanced L3 protocols such as BGP and IS-IS.

The following figure summarizes the features available for each tier:



NOTE: For the Standard tier, the Virtual Chassis license is included along with the EX2300-C-12, EX3400, and EX4300 hardware. For the 24-port and 48-port EX2300 switches, you'll need to purchase the Virtual Chassis license separately.

**EZ-LAG (single EVPN peer) in the Advanced tier is supported only on EX4400 (among access switches).

Table 32: Flex Term Subscriptions for Mist-Managed Switches (Option 3)

Device	Subscription SKU	SKU Character Description
Class 1, 12-port switches: EX2300-C-12T/P EX4100-F-12T/P	For EX2300 switches: S-EX-A-Cn-1|3|5-[COR|SD|ND|AC|P|CAC|SAC|NAC|CP|SP|NP] For all the other switches: S-EX-A|P-Cn-1|3|5-[COR|SD|ND|AC|P|CAC|SAC|NAC|CP|SP|NP]	S—Software EX—EX switch A|P—Advanced or Premium flex tier Cn—Class of switch (C1, C2, or C3) 1|3|5—Subscription term in years [COR|SD|ND|AC|P|CAC|SAC|NAC|CP|SP|NP]—Customer support type. See "Customer Support Services for EX-Series and QFX-Series Switches" on page 124.

Table 32: Flex Term Subscriptions for Mist-Managed Switches (Option 3) ***(Continued)***

Device	Subscription SKU	SKU Character Description
Class 2, 24-port switches: EX2300-24T/P/MP EX4100-F-24T/P EX3400-24T/P EX4100-24T/P/MP EX4300-24T/P EX4400-24T/24X/P/MP/F		
Class 3, 32 or 48-port switches: EX2300-48T/P/MP EX3400-48T/P EX4100-F-48T/P EX4100-48T/P/MP EX4300-32F EX4300-48T/P/MP EX4400-48T/P/MP/F		

Customer Support Services for EX-Series and QFX-Series Switches

You can opt for subscriptions with or without support services.

- C/COR—CORE HW support
- S/SD—Same Day HW support
- N/ND—Next Day HW support
- AC—Advanced Care (30 min SLA)
- P—Premium Care (15 min SLA)
- CAC—CORE hardware support + Advanced Care (30 min SLA)
- SAC—Same day hardware support + Advanced Care (30 min SLA)
- NAC—Next day hardware support + Advanced Care (30 min SLA)
- CP—CORE hardware support + Premium Care (15 min SLA)
- SP—Same day hardware support + Premium Care (15 min SLA)
- NP—Next day hardware support + Premium Care (15 min SLA)

WAN Assurance

IN THIS SECTION

WAN Assurance enables simplified network deployment and operations and improved visibility into end-user experiences. Mist AI uses the data from Session Smart Routers and SRX Series Firewalls to provide insights for optimum user, device, and application experiences in branch and remote locations. For more information about WAN Assurance, see Introduction to Juniper Mist WAN Assurance.

Subscriptions for Session Smart Routers

You can deploy and manage the Juniper® Session Smart™ Routers either in standalone mode or through the Juniper Mist cloud. Juniper provides the following subscription options:

- Standalone SSN on-premises license (conductor-managed)

  The SSN on-premises license is classified under the following tiers:

  - Standard—Layer 3 Network Interface Device (L3NID) license that provides features such as monitoring and remote access, network management, application identification, analytics, and static routing.
  - Advanced—Session Edge Router (SER) license that provides the Standard tier features along with high availability, dynamic routing, network address translation, network firewall, SIP ALG, GRE and IPsec.
  - Premium—Session Smart Router license that provides Advanced tier features and advanced security features.

- SSN on-premises flex license—SSN on-premises license that you can pair with Mist subscriptions (WAN Assurance, Marvis, and Premium Analytics).
- Subscription bundles—SaaS bundles that include SSN and WAN Assurance subscriptions.

Figure 2 on page 125 summarizes the Mist cloud subscription options for Session Smart Routers.

Figure 2: Mist Cloud Subscription Options for Session Smart Routers

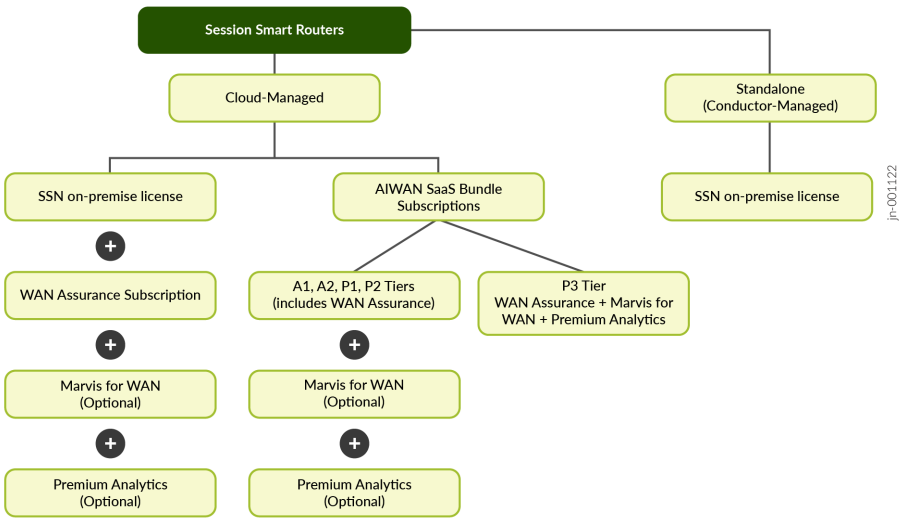


Table 33: SSN Licenses for Session Smart Routers

Subscription SKU	Subscription	SKU Character Description
S-SSN-S|A1|A2|P1|P2-xxxxM-1|3|5	On-premises license for the Session Smart Routers.	S—Software SSN—Session Smart Networking product S|A1|A2|P1|P2—Flex tier • S—Standard: Layer 3 Network Interface Device (L3NID) • A1, A2—Advanced: Session Edge Router (SER) • P1, P2—Premium: Session Smart Router xxxxM—Bandwidth tier ("Bandwidth Tier for SSN Flex Licenses" on page 128) H—High Availability node 1|3|5—Subscription term in years
S-SSN-S|A1|A2|P1|P2-xxxxM-H-1|3|5	On-premises license for the secondary node in HA deployments.	

Associated Subscriptions and Subscription Bundles for SSR

Associated subscriptions are optional subscriptions that you can use to enable additional capabilities on the Mist WAN network.

Table 34: Associated Mist Subscriptions for Session Smart Routers

Subscription SKU	Subscription	SKU Character Description
S-WAN-A1|A2|P1|P2-xxxxM-1|3|5	WAN assurance subscription for Session Smart Routers.	S—Software WAN—WAN Assurance A1|A2|P1|P2—Flex tier • A1, A2—Advanced: Session Edge Router (SER) You can use the A1 for Standard tier (L3NID).
S-WAN-A1|A2|P1|P2-xxxxM-H-1|3|5	WAN assurance subscription for Session Smart Routers (secondary node).	

Table 34: Associated Mist Subscriptions for Session Smart Routers *(Continued)*

Subscription SKU	Subscription	SKU Character Description
S-WAN-VNA-xxxxM-1|3|5	Marvis for WAN subscription **NOTE**: For a HA deployment, you'll need two Marvis subscriptions.	• P1, P2—Premium: Session Smart Router xxxxM—Bandwidth tier ("Bandwidth Tier for SSN Flex Licenses" on page 128). **NOTE**: The bandwidth tier must match the tier specified in the SSN on-premises license. H—High Availability node 1|3|5—Subscription term in years
SUB-PMA-1|3|5	Premium Analytics subscription **NOTE**: For a HA deployment, you'll need two Premium Analytics subscriptions.	

You can opt for AIWAN SaaS bundles that include the Advanced or Premium SSN license and the WAN Assurance subscription. You'll need to order the Marvis for WAN (S-WAN-VNA-xxM-1|3|5) and Premium Analytics (SUB-PMA-1|3|5) subscriptions separately.

NOTE: AIWAN SaaS bundles are not available for L3NID.

Table 35: SaaS Bundle Subscriptions for Session Smart Routers

Subscription SKU	Subscription	SKU Character Description
S-AIWAN-A1|A2|P1|P2|P3-xxM-1|3|5	AIWAN SaaS bundle	S—Software AIWAN—AIWAN A1|A2|P1|P2|P3—Flex tier **NOTE**: AIWAN subscriptions are not available for L3NID. P3 includes Marvis and Premium Analytics subscriptions. xxM—Bandwidth tier ("Bandwidth Tier for SSN Flex Licenses" on page 128) H—High Availability node 1|3|5—Subscription term in years
S-AIWAN-A1|A2|P1|P2|P3-xxMH-1|3|5	AIWAN SaaS bundle for the secondary node in HA deployments.	

Bandwidth Tier for SSN Flex Licenses

Each SSN license entitles you to a maximum bandwidth throughput as listed in Table 36 on page 128.

Table 36: Bandwidth Throughput Licensing for SSN Flex Tiers

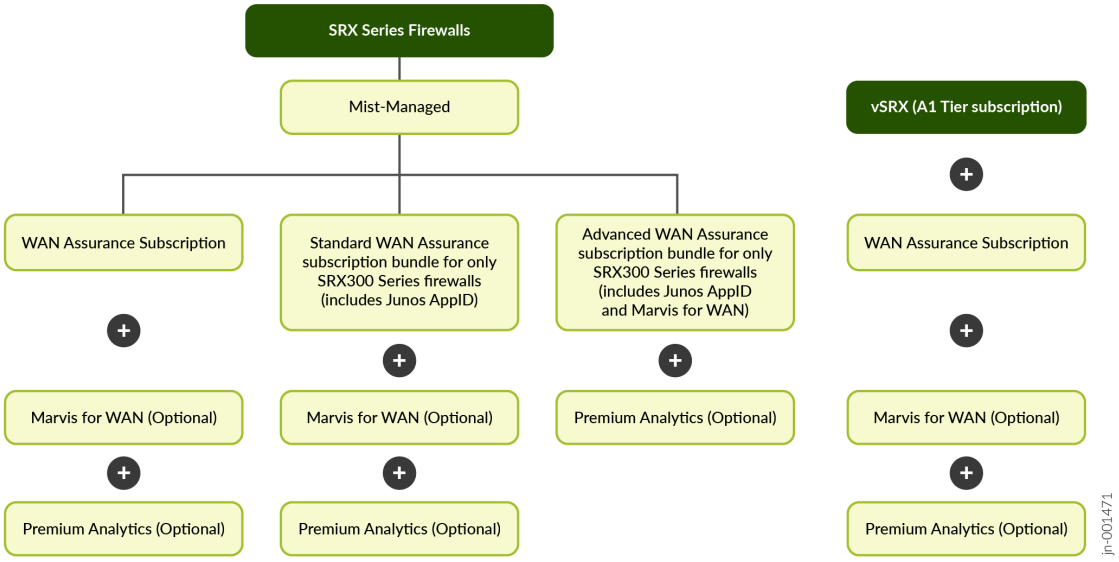
Bandwidth Throughput	L3NID (S)	SER (A1, A2)	Session Smart Router (P1, P2)
10 Mbps		✓	✓
25 Mbps		✓	✓
50 Mbps	✓	✓	✓
100 Mbps	✓	✓	✓
250 Mbps	✓	✓	✓
500 Mbps	✓	✓	✓
1 Gbps	✓	✓	✓
2.5 Gbps	✓	✓	✓
5 Gbps	✓	✓	✓
10 Gbps	✓	✓	✓
20 Gbps		✓	✓
40 Gbps		✓	✓
100 Gbps		✓	✓

Subscriptions for SRX Firewalls

You can operate and manage the Juniper Networks® SRX Series Firewalls through the Juniper Mist cloud. This section covers information about the cloud-based subscriptions for managing your SRX Series Firewalls through Juniper Mist.

Figure 3 on page 129 summarizes the Mist cloud subscription options for SRX Series Firewalls.

Figure 3: Mist Cloud Subscription Options for SRX Series Firewalls



Subscriptions are applicable to both brownfield and greenfield devices. Greenfield SRX Series Firewalls are new cloud-ready firewalls, while brownfield SRX Series Firewalls are the firewalls that are being brought into the Juniper Mist cloud architecture from a previous deployment. Table 37 on page 130 lists the WAN Assurance subscription SKU for SRX Series Firewalls.

Table 37: WAN Assurance Subscription SKUs for SRX Series Firewalls

Subscription SKU	SKU Character Description
S-WAN-C1|C2|C3|C4|C5|C6-1|3|5	S—Software WAN—WAN Assurance C1|C2|C3|C4|C5|C6—Class of device • Class 1 (C1)—SRX300, SRX320 • Class 2 (C2)—SRX340, SRX345 • Class 3 (C3)—SRX380 • Class 4 (C4)—SRX1500, SRX1600 • Class 5 (C5)—SRX2300, SRX4100, SRX4200, SRX4300 • Class 6 (C6)—SRX4600, SRX4700 1|3|5—Subscription term in years

For SRX300 Series Firewalls, you can opt to purchase subscription bundles that include WAN Assurance, Marvis for WAN, and Junos Application Identification (AppID) subscriptions.

When you add these subscription bundles in the Juniper Mist portal, the Junos AppID licenses are automatically activated on the SRX300 Series Firewalls.

Table 38: WAN Assurance Subscription Bundles for SRX300 Series Firewalls

Subscription SKU	SKU Character Description
S-SRX-S|A-C1|C2|C3-1|3|5-COR|SD|ND|CP	S—Software SRX—SRX Series Firewall S|A—Standard or Advanced subscription bundle • S—Standard bundle (includes WAN Assurance only) • A—Advanced bundle (includes WAN Assurance and Marvis) C1|C2|C3—Class of device • Class 1 (C1)—SRX300, SRX320 • Class 2 (C2)—SRX340, SRX345 • Class 3 (C3)—SRX380 1|3|5—Subscription term in years COR|SD|ND|CP—Customer support type • COR—CORE hardware support • SD—Same day hardware support • ND—Next day hardware support • CP—CORE hardware support and Premium care

Associated Subscriptions for SRX Series Firewalls

Associated subscriptions are optional subscriptions that you can use with the WAN Assurance subscription to enable additional capabilities on the Mist WAN network. You can opt for associated subscriptions provided you have a WAN Assurance subscription.

Table 39: Associated Subscriptions for SRX Series Firewalls

Subscription SKU	Description	SKU Character Description
S-WAN-VNA-C1|C2|C3|C4|C5|C6 – 1|3|5	Marvis for WAN subscription	S—Software WAN—WAN Assurance VNA—Marvis C1|C2|C3|C4|C5|C6—Class of device • Class 1 (C1)—SRX300, SRX320 • Class 2 (C2)—SRX340, SRX345 • Class 3 (C3)—SRX380 • Class 4 (C4)—SRX1500, SRX1600 • Class 5 (C5)—SRX2300, SRX4100, SRX4200, SRX4300 • Class 6 (C6)—SRX4600, SRX4700 1|3|5—Subscription term in years
SUB-PMA-1Y|3Y|5Y-[AC|P]	Premium Analytics subscription for a specified term with or without customer support.	SUB—Subscription PMA—Premium Analytics 1Y|3Y|5Y—Subscription term in years AC—Advanced Care P—Premium Care

WAN Assurance Subscriptions for vSRX

For vSRX, the subscriptions are based on the device class as listed in Table 40 on page 133.

Table 40: WAN Assurance Subscription SKUs for vSRX

Subscription SKU	Description	SKU Character Description
S-WAN-C2|C3|C4|C5-1|3|5	WAN Assurance subscription	S—Software WAN—WAN Assurance VNA—Marvis C2|C3|C4|C5—Device class • C2—vSRX 2 CPU Cores • C3—vSRX 5 CPU Cores • C4—vSRX 9 CPU Cores • C5—vSRX 17 CPU Cores 1|3|5—Subscription term in years

You can opt for the following associated subscriptions provided you have a WAN Assurance subscription for vSRX.

Table 41: Associated Subscriptions for vSRX

Subscription SKU	Description	SKU Character Description
S-WAN-VNA-C2|C3|C4|C5-1|3|5	Marvis for WAN subscription	S—Software WAN—WAN Assurance VNA—Marvis C2|C3|C4|C5—Device class • C2—vSRX 2 CPU Cores • C3—vSRX 5 CPU Cores • C4—vSRX 9 CPU Cores • C5—vSRX 17 CPU Cores 1|3|5—Subscription term in years
SUB-PMA-1Y|3Y|5Y-[AC|P]	Premium Analytics subscription for a specified term with or without customer support.	SUB—Subscription PMA—Premium Analytics 1Y|3Y|5Y—Subscription term in years AC—Advanced Care P—Premium Care

Access Assurance

Juniper Mist Access Assurance is a cloud-based network access control (NAC) service that secures your network by providing identity-based network access to devices and users. The Access Assurance subscription includes the subscription for IoT Assurance, which provides access control functionality using multiple and private pre-shared keys (MPSK and PPSK). For more information about Access Assurance, see Juniper Mist Access Assurance.

If your network has third-party wired or wireless network infrastructure, you'll need the ME-X1-M or ME-VM-OC-PROXY Mist Edge along with the Access Assurance subscription. Mist Edge enables the third-party vendor devices to communicate over the standard RADIUS to the Mist Edge Auth Proxy.

Table 42: Access Assurance Subscription SKUs

Subscription SKU	Description	SKU Character Description
S-CLIENT-S-1|3|5|7	Standard access and IoT assurance subscription for one active client. Standard access includes EAP-TTLS, EAP-TLS, PEAP-TLS, TEAP, PSK/MPSK, and IoT Assurance, MAB, MPSK.	S—Software S—Standard Access and IoT assurance subscription for one active client A—Advanced access and IoT assurance subscription for one active client 1|3|5|7—Subscription term in years
S-CLIENT-A-1|3|5|7	Advanced access and IoT assurance subscription for one active client. Advanced access includes the standard access options plus UEM/EMM/MDM and firewall Integrations. Client-onboarding with PKI infrastructure.	
S-CLIENT-SS-M (Monthly subscription)	Site Survivability subscription that allows local authentication for Internet connectivity failure scenarios when compared with an on-premises solution.	S—Software SS—Site Survivability M—Monthly subscription term that should match the Access Assurance subscription term. As an example, consider that you purchase an Access Assurance subscription for 2 years: • If you purchase the Site Survivability subscription at the same time, then the value of M will be 24. • If you purchase the Site Survivability subscription later, say after 6 months, then the value of M will be 18 (that is, 24 - 6), not 24. **NOTE**: To enable Site Survivability, you'll need the ME-X1-M or ME-VM-OC-PROXY Mist Edge.

Table 42: Access Assurance Subscription SKUs *(Continued)*

Subscription SKU	Description	SKU Character Description
S-CLIENT-SS-1|3|5|7 (Yearly subscription)	Site Survivability subscription that allows local authentication for Internet connectivity failure scenarios when compared with an on-premises solution.	S—Software SS—Site Survivability 1|3|5|7—Subscription term in years **NOTE**: To enable Site Survivability, you'll need the ME-X1-M or ME-VM-OC-PROXY Mist Edge.

Marvis

IN THIS SECTION

Marvis, a virtual network assistant, provides a comprehensive view of your network with real-time network visibility and detailed insights. For more information about Marvis and its features, see Get Started with Marvis.

Marvis Subscription Types

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

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

Marvis Actions for Your Subscriptions

Different Marvis subscriptions enable different Marvis actions. Your Marvis subscriptions determine the actions that you'll see on the Actions dashboard. Be aware of the requirements for the *types* of subscription and purchase the subscriptions that you need for your network. For example, you need a Marvis for Wired subscription to see Wired actions.

Available actions vary for different subscriptions, as appropriate for the types of devices that are associated with these subscriptions. The following tables show the available actions for each subscription type.

Table 43: Marvis for Wired Actions

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

Table 44: Marvis for WAN Actions

Category	Marvis for WAN Actions
WAN Edge	MTU Mismatch
	Bad WAN Uplink
	VPN Path Down
	Non-Compliant

Table 45: Marvis for Wireless Actions

Category	Marvis for Wireless Actions
Layer 1	Bad Cable
Connectivity	Authentication Failure
	DHCP Failure
	ARP Failure
	DNS Failure
AP	Offline
	Health Check Failed
	Non-compliant
	Coverage Hole
	Insufficient Capacity
	AP Loop Detected
Switch	Missing VLAN
Other Actions	Persistently Failing Clients

Marvis Subscription SKUs

Marvis subscriptions are available as standalone SKUs or as part of the Wired, Wireless, or WAN assurance subscription bundle. Table 46 on page 139 lists the standalone SKUs that you can order separately. Note that you'll need an Assurance (Wired, Wireless, or WAN) subscription and a Marvis subscription per device.

Table 46: Marvis Subscription SKUs

Subscription Type	Subscription SKU	Description	SKU Character Description
Marvis for Wireless	SUB-VNA Ordered as part of the Wireless Assurance subscription. See "Wireless Assurance" on page 105	Marvis subscription for wireless	See "Wireless Assurance" on page 105
Marvis for Wired	SUB-EX-VNA- 1Y|3Y|5Y	Marvis subscription for Class 1/2/3 switches.	SUB—Subscription EX—EX switch VNA—Marvis subscription C4/C5/C6/C7/C8—Class of switch 1Y|3Y|5Y or 1|3|5 —Subscription term in years
	S-SW-WA-VNA- C4-1|3|5	Marvis subscription for Class 4 switches.	
	S-SW-WA-VNA- C5-1|3|5	Marvis subscription for Class 5 switches.	
	S-SW-WA-VNA- C6-1|3|5	Marvis subscription for Class 6 switches.	
	S-SW-WA-VNA- C7-1|3|5	Marvis subscription for Class 7 switches.	
	S-SW-WA-VNA- C8-1|3|5	Marvis subscription for Class 8 switches.	

Table 46: Marvis Subscription SKUs *(Continued)*

Subscription Type	Subscription SKU	Description	SKU Character Description
Marvis for WAN	S-WAN-VNA-xxM-1|3|5	Marvis subscription for Session Smart Routers	S—Software WAN—WAN Assurance VNA—Marvis subscription xxM—Bandwidth tier ("Bandwidth Tier for SSN Flex Licenses" on page 128) 1|3|5 —Subscription term in years
	S-WAN-VNA-C1| C2|C3-1| 3|5	Marvis subscription for SRX Firewalls	S—Software WAN—WAN Assurance VNA—Marvis subscription C1|C2|C3—Class of device • Class 1 (C1)—SRX300, SRX320 • Class 2 (C2)—SRX340, SRX345 • Class 3 (C3)—SRX380 1|3|5 —Subscription term in years

Table 46: Marvis Subscription SKUs *(Continued)*

Subscription Type	Subscription SKU	Description	SKU Character Description
	S-WAN-VNA-C2| C3|C4| C5-1| 3|5	Marvis subscription for vSRX	S—Software WAN—WAN Assurance VNA—Marvis subscription C2|C3|C4|C5—Device class • C2—vSRX 2 CPU Cores • C3—vSRX 5 CPU Cores • C4—vSRX 9 CPU Cores • C5—vSRX 17 CPU Cores 1|3|5 —Subscription term in years

Marvis Client

Marvis client is a software agent that is installed on end-user devices to view the network from the end user's perspective. Available for Android, Windows, and macOS devices, Marvis client provides detailed data and telemetry about how the connected device experiences the wireless connection. For more information about the Marvis client, see Marvis Client Overview.

Table 47: Marvis Client Subscription SKUs

Subscription SKU	Description	SKU Character Definition
S-VNACLIENT-S-1| 3|5|7	Marvis Client subscription (per client)	S—Software VNACLIENT—Marvis Client S—Standard 1|3|5|7 —Subscription term in years

Location Services

Juniper Mist leverages the virtual BLE (vBLE) array technology and cloud-based machine learning to provide location services such as wayfinding, proximity messaging with vBLE, and asset visibility. Mist APs ship with the vBLE array, which can be activated by purchasing the user engagement and/or asset visibility subscriptions (in addition to the Wireless Assurance base subscription). For more information about location services, see Juniper Mist Location Services Overview.

Table 48: Location Services Subscription SKUs

Subscription SKU	Description	SKU Character Definition
SUB-AST-1Y|3Y|5Y-[AC|P]	Subscription for asset visibility, which allows you to quickly locate key resources in your organization using virtual Bluetooth beacons. See Asset Visibility	SUB—Subscription AST—Asset Visibility ENG-User Engagement 1Y|3Y|5Y—Subscription term in years AC—Advance Care P—Premium Care
SUB-ENG-1Y|3Y|5Y-[AC|P]	Subscription for user engagement. Mist uses Virtual BLE (vBLE) array technology to improve the accuracy of real-time indoor location services, from wayfinding to location-based proximity notifications. See User Engagement **NOTE**: SUB-ENG is supported only on APs with vBLE support.	

Premium Analytics

The Juniper Mist™ Premium Analytics is an advanced, cloud-based analytics service that provides insights into your network and business operations. Premium analytics allows you to run reports over data sets at a more granular level, mix and match different datasets, and observe data going back up to 13 months. Premium Analytics subscription requires a Wireless Assurance, WAN Assurance, or Wired Assurance base subscription. For more information about Premium Analytics, see Introduction to Juniper Mist Analytics.

Table 49: Premium Analytics Subscription SKUs

Subscription SKU	Description	SKU Character Definition
SUB-PMA-1Y|3Y|5Y-[AC|P]	Premium Analytics subscription for a specified term with or without customer support.	SUB—Subscription PMA—Premium Analytics 1Y|3Y|5Y—Subscription term in years AC—Advanced Care P—Premium Care

Juniper Routing Assurance

Juniper Routing Assurance is a routing observability platform that provides visibility into the performance of the routers in the network. Key features include router insights, Marvis Actions, and service level expectations.

We offer two types of subscriptions for Routing Assurance—standard and add-on. The standard subscription provides features such as router insights, Marvis Actions, and service level expectations (SLEs). The add-on subscription provides the Marvis Virtual Network Assistant (VNA).

Table 50: Juniper Routing Assurance—Standard Subscriptions

Subscription SKU	Description	Supported Device Models	SKU Character Definition
S-RA-S-C2-1|3|5|7	Routing Assurance for Class 2 devices for a specific duration.	ACX7020 ACX7024 ACX7024X ACX7100 MX204	S—Subscription RA—Routing Assurance S—Standard C2/C3/C4—Class of device 1|3|5|7—Subscription term in years

Table 50: Juniper Routing Assurance—Standard Subscriptions *(Continued)*

Subscription SKU	Description	Supported Device Models	SKU Character Definition
S-RA-S-C3-1|3|5|7	Routing Assurance for Class 3 devices for a specific duration.	MX240 MX304 MX480	
S-RA-S-C4-1|3|5|7	Routing Assurance for Class 4 devices for a specific duration.	MX960	

Table 51: Juniper Routing Assurance—Add-On Subscriptions

Subscription SKU	Description	Supported Device Models	SKU Character Definition
S-RA-A-C2-1|3|5|7	Marvis Virtual Network Assistant add-on for Class 2 devices for a specific duration.	ACX7020 ACX7024 ACX7024X ACX7100 MX204	S—Subscription RA—Routing Assurance A—Advanced C2/C3/C4—Class of device 1|3|5|7—Subscription term in years
S-RA-A-C3-1|3|5|7	Marvis Virtual Network Assistant add-on for Class 3 devices for a specific duration.	MX240 MX304 MX480	
S-RA-A-C4-1|3|5|7	Marvis Virtual Network Assistant add-on for Class 4 devices for a specific duration.	MX960	

Juniper Mist Subscriptions Scope

SUMMARY

Learn which subscriptions operate at the organization or site level, and understand which metrics are used to calculate subscription utilization. Finally, apply a subscription to a site.

IN THIS SECTION

Juniper Mist provides subscriptions at both the organization level and the site level.

When applied organization-wide, a subscription is not tied to any specific hardware or site. Instead, each license added to the organization increases the number of a device that can use the feature across the entire organization.

Alternatively, you can apply subscriptions at the site level for specific features. If a feature subscription is enabled for a particular site, it will only impact that site. All access points (APs) assigned to it will consume the corresponding subscription.

The following table and illustration summarizes the Juniper Mist subscriptions scope.

Features	Organization Level	Site Level	Subscription Usage Based On
Access Assurance	✓	-	Number of active clients using NAC
Asset Visibility	-	✓	Number of APs or beacon points
Marvis Virtual Network Assistant (Wireless)	✓	-	Number of APs or beacon points
Marvis Virtual Network Assistant (Wired)	✓	-	Number of switches
Marvis Virtual Network Assistant (WAN)	✓	-	Number of WAN Edges
Marvis Client	✓		Number of clients

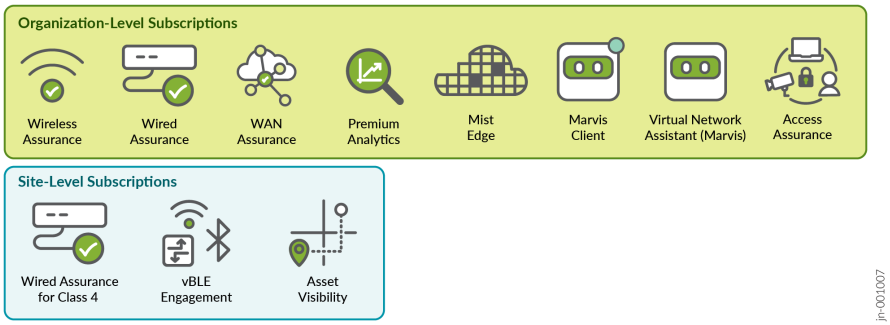
(Continued)

Features	Organization Level	Site Level	Subscription Usage Based On
Mist Edge	✓	-	Number of APs forming tunnels
Premium Analytics	✓*	-	• Number of APs or beacon points (Wireless) • Number of switches (Wired) • Number of WAN Edges (WAN)
vBLE Engagement	-	✓	Number of APs or beacon points
WAN Assurance	✓	-	Number of WAN Edges
Wi-Fi Management and Assurance	✓	-	Number of APs or beacon points
Wired Assurance	✓	✓ **	Number of switches

* Enforced for a specific technology—Wireless, Wired, or WAN

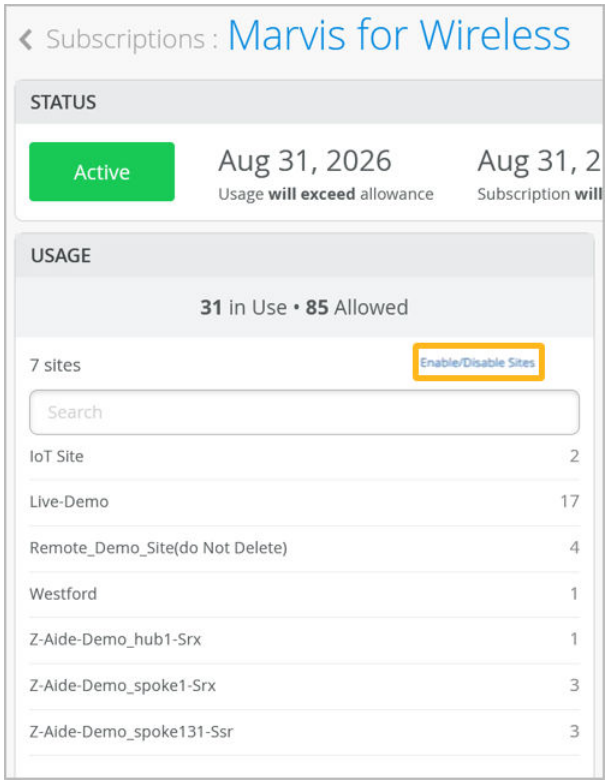
** Applicable to the Wired Assurance for Class 4 subscription only.

Figure 4: Juniper Mist Subscriptions Scope



To apply subscriptions for a specific site:

1. From the left menu, select **Organization** > **Admin** > **Subscriptions**.
2. Click the subscription type to open the subscription window.



You'll notice that the **Enable/Disable Sites** option on the right side is active. This indicates that the subscription can be applied to the selected sites. Otherwise, the option will appear grayed out.

3. Click **Enable/Disable Sites** to select specific sites within the organization to apply the subscription.

Examples

Organization-Level Subscriptions

Consider an organization with 10 sites and 100 devices. These 100 devices require 802.1X. Then you'll need 100 subscriptions and you'll need to apply them at the organization level. Here, licenses are calculated at the organization level. You can move devices across sites. As long as the total subscription count stays within the subscriptions purchased (100), devices can use the feature.

Site-Level Subscriptions

Consider an organization with 10 sites and 100 devices. Suppose 20 devices in five sites of the organization need Marvis and the remaining devices in the other five sites do not require Marvis. Then, you can enable only five sites and apply 20 subscriptions. These 20 subscriptions are utilized among the devices within these five sites.

Activate a Subscription

SUMMARY

Follow these steps to enter your activation code and apply it to your organization.

Before You Begin

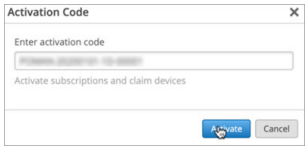
Decide which Juniper Mist™ subscription you need, and then contact MistRenewal@juniper.net to purchase them. We'll email your activation codes to you.

NOTE: For more information about Juniper Cloud Services, see https://www.juniper.net/us/en/products/cloud-services.html.

To activate a subscription:

1. From the left menu, select **Organization** > **Admin** > **Subscriptions**.
2. Click **Apply Activation Code** (near the top-right corner of the screen).
3. Enter the code.

4. Click **Activate**.



NOTE: If you purchased multiple devices and subscriptions, you'll have one activation code for all of them. In this case, all subscriptions will be activated and the devices will be claimed into your organization.

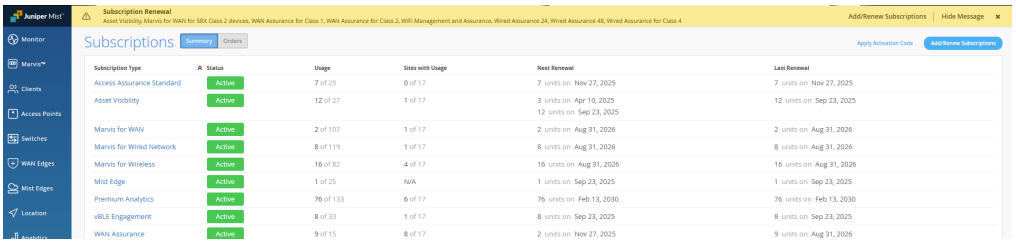
Renew a Subscription

SUMMARY

Follow these steps to review the status of your subscriptions and to request renewals for those that have expired or are expiring soon.

Juniper provides 90 days' notice of subscription expiration so that you can plan renewals accordingly. Reminders also appear in a banner message at the top of the Juniper Mist™ portal.

Banner Example

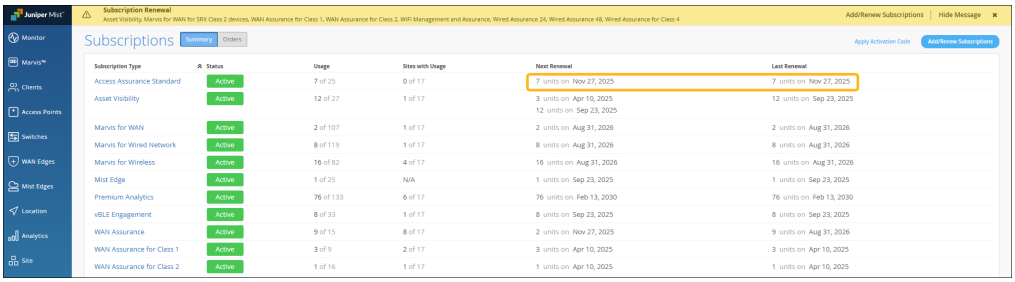


To renew your subscription:

1. From the left menu, select **Organization** > **Admin** > **Subscriptions**.
2. (Optional) Review the information about your subscriptions and orders.
   - The status appears as Active, Inactive, Expired, or Exceeded.

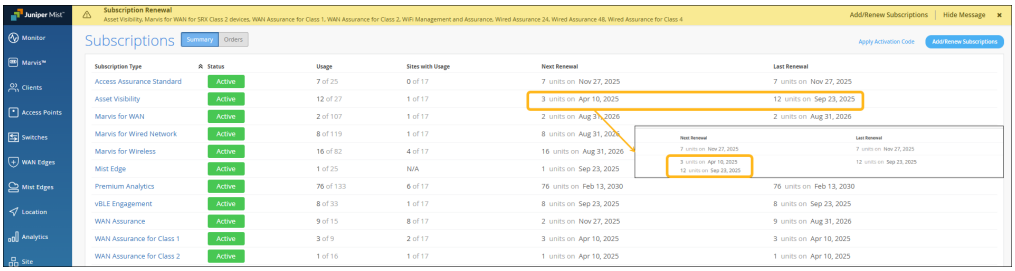
- The expiration dates for the subscriptions appear in the **Next Renewal** and **Last Renewal** columns. You can have two scenarios here:

  - Same dates listed in both the columns



    This scenario is applicable if you have a single subscription or multiple subscriptions that will expire on the same date (renewal date).

  - Different dates listed in the columns



    This scenario is applicable if you have multiple subscriptions that will expire on different dates.

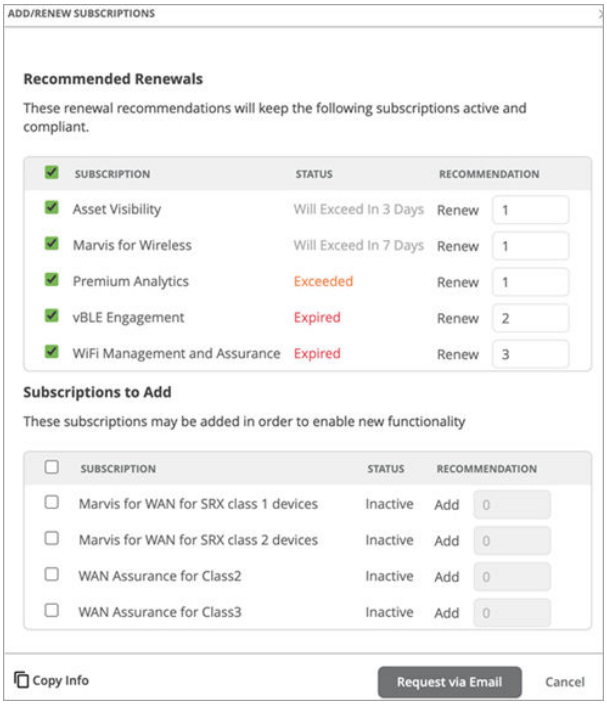
    In the above example, you can see that the **Next Renewal** column lists 3 units due for renewal on Apr 10 and the **Last Renewal** column lists 12 units due for renewal on Sep 23. If you click the entry in the **Next Renewal** column, you'll notice the breakup of the total subscription units due for renewal. The last set of subscriptions due for renewal is listed in the **Last Renewal** column.

- To review the usage details for a subscription, click the subscription.

- To review your subscription orders, click **Orders** (at the top of the screen).

3. Click **Add/Renew Subscriptions**.

   The pop-up window displays renewal recommendations.



The Recommended Renewals list includes:

- Expired subscriptions
- Exceeded subscriptions
- Active subscriptions that are due to expire within 90 days
- The recommended number of licenses for each subscription

4. In the Recommended Renewals section:
   - Select the subscriptions that you want to renew, and clear the check boxes for the other subscriptions.
   - If needed, edit the number of licenses for each subscription.
5. In the Subscriptions to Add section, select the check box for each subscription that you want to add.

   This section appears if your organization lacks any of the available subscriptions.
6. Click **Request via Email**.

Juniper Mist sends an email to support to request the selected subscriptions.

When your order is processed, Juniper will email your activation code to you. You can then activate your subscription.

Subscription Status

SUMMARY

Learn about the various statuses that you'll see on the Subscriptions page in the Juniper Mist™ portal.

IN THIS SECTION

Subscription Status

- Active—The subscription was activated and is still valid.
- Expired—The subscription term has expired.

  NOTE:

  - A subscription starts when Juniper ships or emails the activation code to you.
  - Alerts appear if subscriptions have not been renewed within a 30-day grace period.
  - After a subscription expires, your network will continue to operate. However, no support is provided for expired subscriptions.
  - After 90 days, Juniper can give read-only access or terminate access.

- Exceeded—Usage exceeds the license limit. "Usage" is the number of access points (APs) on which this subscription's features are enabled.
- Inactive—This status can occur in either of these situations:
  - The subscription was purchased but has not been activated.
  - The subscription expired and there is no usage.

Monitor Your Orders

SUMMARY

Follow these steps to monitor your orders and check the upcoming end dates for your Juniper Mist™ subscriptions.

To monitor your orders:

1. Select **Organization** > **Admin** > **Subscriptions** from the left menu.
2. Click the **Orders** button at the top of the page.
3. Use the following features, as needed:
   - Filter the table—Use the filter options above the table to filter the orders by subscription type, group the orders by renewal month, or include the expired subscriptions in the order history.
   - Sort the table—Click any column heading to sort the order history by that column. Click a heading again to sort the order history in the reverse order.
   - Add a note—Click the pencil icon in the **Notes** column, enter your note, and then click a blank area of the page to save the note.
   - Edit a note—Click the note in the **Notes** column, make your changes, and then click a blank area of the page to save the changes.
   - Delete a note—Click the note, click **X**, and then click a blank area of the page to confirm the change.
   - Save the order history as a CSV file—Click **Download** on the right side of the page.

Juniper Mist Subscriptions FAQ

SUMMARY

Learn about subscription renewal and expiration, and get answers to common questions about obtaining, viewing, and moving subscriptions.

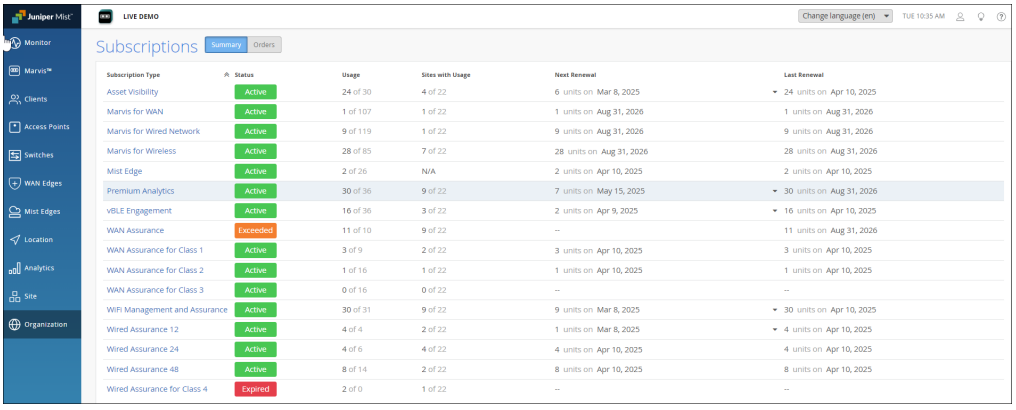
IN THIS SECTION

How can I obtain a trial subscription?

You can obtain a trial subscription when you create a new organization. To obtain a trial subscription for an existing organization, contact the sales or support team.

Where can I view my subscriptions?

You can view the details of your subscriptions in the **Organization** > **Admin** > **Subscriptions** page in the Juniper Mist portal.



How can I view or move subscriptions for devices?

Subscriptions are applicable to organizations, not specific devices. If an organization has a subscription, the corresponding devices consume the subscription. You can view all your subscriptions on the Subscriptions page, and you don't need to assign them to devices.

What happens when a subscription expires?

If a subscription expires or if you have insufficient subscriptions, devices remain operational. You'll receive sufficient warning notifications ahead of the subscription expiry. If the subscriptions expire and you do not renew them, then the access to the Juniper Mist portal will be disabled. You cannot monitor or make any further configuration changes to your network until you renew the subscriptions.

How do I renew a subscription?

You'll receive an activation code when you renew a subscription. You can claim that code in the Juniper Mist portal, and the subscriptions will be added to your organization. See Renew a Subscription.

What is the difference between Entitled and Usage?

For an organization, *Entitled* indicates the number of active subscriptions for a subscription type. *Usage* indicates the number of APs located at sites that have this feature enabled. If the Usage value exceeds the Entitled value, the Mist dashboard displays a warning message.

What does the One or more subscriptions have expired or exceeded their entitled usage warning message indicate?

This warning message indicates that you do not have sufficient subscriptions—for example, SUB-MAN (Wireless) and SUB-VNA (Marvis)—for the services that you are currently using. We recommend that you contact your sales representative to purchase the required quantity of subscriptions.

Why does the Subscriptions page display that the subscriptions are decommissioned even though I renewed the subscriptions?

You should receive a new activation code by e-mail when you request for a subscription renewal. You can add this code to your organization to renew the subscriptions. See Activate a Subscription.

If you do not receive the activation code, open a support ticket and provide your order number.

Will the Juniper Mist Cloud disconnect the access point (AP) automatically when the subscription expires?

No. Your network will continue to operate after the subscription expires. However, if you do not intend to renew the subscription, Juniper Networks reserves the right to disable access to the Juniper Mist portal or to terminate the organization dashboard. No support will be available for inactive subscriptions.

Can subscriptions be moved from one organization to another?

Yes, provided that the administrator moving the subscriptions is a Super User in both the organizations.

What are the requirements for moving subscriptions between organizations?

Contact the Juniper Mist support team for this information.

Where can I view the API documentation for subscriptions?

You can view the API documentation at https://www.juniper.net/documentation/us/en/software/mist/api/http/api/orgs/licenses/overview.

Can subscriptions be co-termed?

Yes. Contact the Juniper Mist support team for more details.

How can I move subscriptions from the global environment to the EU environment?

You'll need to delete the subscription from the global environment and then reclaim it in the EU environment by using the following API:

```
PUT /api/v1/orgs/:org_id/licenses
{
   "op": "delete",
   "subscription_id": "SUB-XXXXXXX"
}
```

Which API call should I use to obtain a summary of the subscriptions?

`GET /api/v1/orgs/:org_id/licenses`

For more information, see Get Org Licenses Summary.

Which API call should I use to obtain the subscription usage information by sites?

`GET /api/v1/orgs/:org_id/licenses/usages`

For more information, see Get Org Licenses by Site.

When does my 90-day free trial start?

Your 90-day free trial starts when you create an organization.

When does the term for a subscription start? Is the term tied to the date when the subscription is activated using the activation code?

The start date for a subscription is the date when we ship the order or send you the activation code by e-mail.

Will I receive a notification before my subscriptions expire?

Yes, we will notify you multiple times so that you can plan the renewals accordingly. We will send you the first notification 90 days before the expiry date of your subscription.

5

CHAPTER

Device Management

SUMMARY

Use the information in this chapter to onboard devices and manage your organization's device inventory.

IN THIS CHAPTER

What Do You Want to Do?

Table 52: Top Tasks

If you want to...	Use these resources:
Manage all devices in your inventory *View your entire inventory. Claim, adopt, rename, and release devices.*	"View and Update Your Device Inventory" on page 161 If you want to use the Mist AI mobile app to manage devices, see "Mist AI Mobile App Overview" on page 224.
Streamline onboarding with auto-provisioning *Set up auto-provisioning to automatically assign device names, assign devices to sites, and assign device profiles to access points.*	"Auto-Provisioning" on page 180
Learn about supported devices *Get datasheets, quick start guides, and deployment guides for access points, switches, firewalls, and more.*	Juniper Mist Supported Hardware (web page)

View and Update Your Device Inventory

SUMMARY

Follow these steps to view and manage your Juniper Mist™ device inventory.

IN THIS SECTION

Find the Inventory Page

From the left menu, select **Organization** > **Admin** > **Inventory**.

View and Find Information

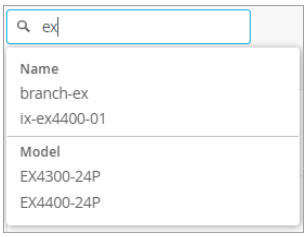
Use the various buttons at the top of the Inventory page to view and find information.

- To select the device type, click a device button:
  - Access Points
  - Switches
  - WAN Edges
  - Cellular Edges
  - Mist Edges
- To view devices that are linked through the Juniper Account Integration option on the Organization Settings page, click the **Installed Base** button. For more information, see "View Juniper Support Insights (JSI) for Your Installed Base" on page 164.
- To select an organization or a site, use the **org** drop-down list.

- To view the complete inventory as a CSV file, click the cloud button (near the top-right corner of the screen).

- To find a specific device, use the **Filter** box below the device buttons. Enter characters from any of the device information fields that you see on the screen. When the matching devices appear in the drop-down list, select the device that you want to view.

  Example: Start typing the letters *ex*. The drop-down list shows devices with *ex* in the device name (such as *branch-ex* and *ix-ex4400-01*) and the model name (such as *EX4300-24P* and *EX4400-24P*).



Claim or Adopt Devices

To manage devices as part of your Juniper Mist organization, you need to claim or adopt them.

Claim new devices:

- *Claim a Juniper Access Point*
- "Claim a Switch" on page 194
- "Claim a WAN Edge" on page 197

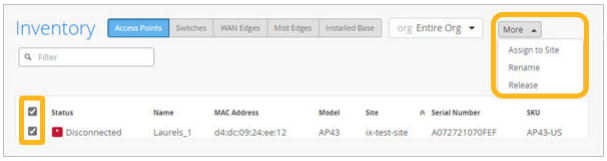
Adopt devices from your Juniper Installed Base:

- "Adopt a Switch from Your Juniper Installed Base" on page 196
- "Adopt a WAN Edge from Your Juniper Installed Base" on page 197

Make Other Changes

You also can assign devices to a site, change the device names, or release devices from this organization's inventory.

Select the devices that you want to assign, rename, or release. Then click the **More** button and select the action that you want to take.



- **Assign to Site**—Select a site to assign this device to.
- **Rename**—Enter a new device name.
- **Release**—Remove (delete) the device from this organization's inventory and delete the device configuration.

Follow the on-screen prompts to complete the action.

View Juniper Support Insights (JSI) for Your Installed Base

SUMMARY

Use the Installed Base tab of the Inventory page to gain actionable support insights for the Juniper devices associated with your organization.

IN THIS SECTION

When you integrate your Juniper Account with your Juniper Mist™ organization, the Installed Base page presents actionable intelligence for all Juniper devices associated with your organization, whether they are cloud-connected or linked through the account linkage workflow.

Use the Installed Base tab page to:

- Gain a centralized view of the Juniper assets linked to your organization
- Track hardware and software lifecycle milestones
- Review contract status of your assets
- View advisories on security vulnerabilities and known issues on a per device basis through the JSI Device Details page. For more information, see "Device Details for Installed Base" on page 172.

These insights are powered by Juniper Support Insights (JSI). With these insights, you can transform your support experience from reactive to focused and proactive. Leverage JSI to identify potential issues early, optimize device performance, and streamline support operations.

NOTE: To view your Juniper Networks devices on the Installed Base page, you must first link your Juniper Networks account to your organization. See "Integrate Your Juniper Support Account with Juniper Mist" on page 94.

It may take up to four hours for details of devices onboarded through device-specific tabs to appear in the Installed Base.

Read the sections below to learn more about the information and options on the Installed Base Page.

Features

Enhance your Mist experience with Juniper's accumulated knowledge of your deployed assets—Juniper augments the information about your deployed assets by correlating your Mist experience with the information that Juniper maintains in its business systems about those same assets. You can track whether your onboarded assets have the latest software installed, their exposure to security vulnerabilities, known problems, and so on. This correlation is achieved by integrating your Juniper maintained asset information with your organization through the Account Integration workflow by using the email address that you registered through the Juniper Support Portal.

After you enter your registered email address and password in the Account Integration tile on the Organization Settings page, the Account Integration workflow retrieves the Installed Base information of your deployed assets from Juniper's business systems. It then correlates this information with all your deployed assets and assigns them Juniper Support Insights (JSI) data artifacts, such as location, contract, warranty, hardware and software end of life dates, and so on. You can access these insights on the **Organization** > **Inventory** > **Installed Base** page.

Account Integration 2.0 enhances your support experience by considering not only the primary assets associated with your registered email address but also the complete set of secondary assets. This enhancement ensures that the Installed Base information for all the deployed assets associated with your registered email address and maintained in Juniper's business systems, covered by an active Juniper support contract, and compatible with Mist Wired and WAN Assurance, is accessible from the Installed Base view.

JSI data artifacts for all onboarded assets—The assets that you onboard may not always completely correlate to the set of assets known by Juniper to be associated with the Admin User that executed the Account Integration workflow. The consequence of which may be that some onboarded assets are left without JSI data artifacts being assigned to them. With this release, following the successful execution of the Account Integration workflow, all onboarded Mist Wired and WAN Assurance assets will be enabled with JSI artifacts.

Asset model number alignment—The assets that you onboard may not always completely correlate with how that asset is identified in different business systems. The consequence of which may be that it is left to you to normalize the asset identification or that some assets are left out of the rendering. With this release, the asset identification conventions used within these environments are now normalized to standard model number. This framework will be maintained and extended as new cloud-compatible assets are released.

Navigate to the Installed Base Page

To find the Installed Base page, select **Organization** > **Admin** > **Inventory** from the left menu. Then click the **Installed Base** button at the top of the page.

Overview of the Installed Base Page

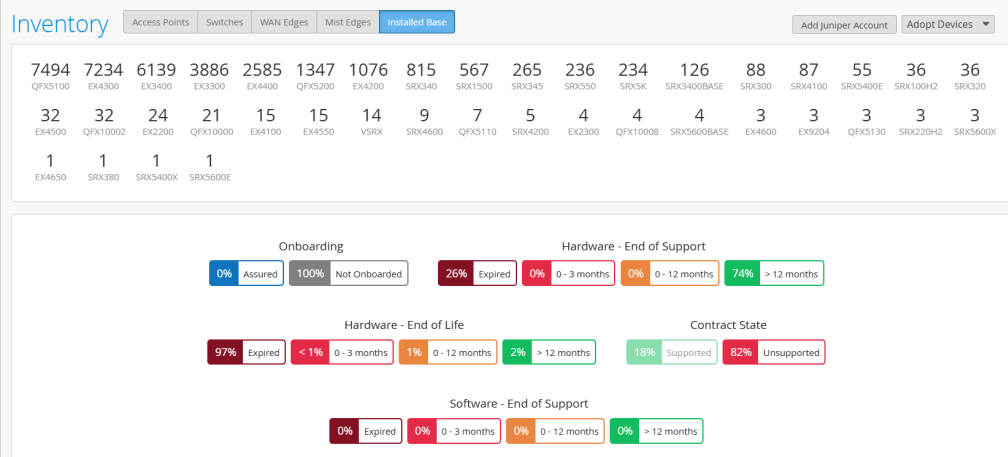
The Installed Base tab displays all Junos OS-based devices associated with your organization, including:

- Cloud-connected devices onboarded through the Mist platform.
- Devices linked through the account integration workflow, which includes your primary Juniper Service Direct account and any associated secondary service accounts, provided that the assets are compatible with Wired Assurance and WAN Assurance.

The Installed Base page is divided into two main sections: Stats Panel and Device Table.

Stats Panel

The Stats panel provides a high-level visual summary of your device inventory and support metrics.



Use this panel to:

- Quickly assess your organization's device distribution, hardware and software lifecycle milestones, and contract coverage.
- Perform interactive filtering by clicking on any category to refine the device list in the Device table.

Each category in the panel offers actionable insights to help you monitor device health, plan upgrades, and maintain support coverage.

Table 53: Categories

Feature	Description
Device Models	Displays the number of devices in the organization per model. Use it to identify distribution of device models in your organization. Click a model to filter the Device table to show only devices of that model.

Table 53: Categories *(Continued)*

Feature	Description
Onboarding	Displays the connection status of the devices. Use it to track which devices are connected and which are not. For each status, you see the percentage of devices with that status. • Assured—Onboarded to an Assured service level (Juniper Mist Cloud). • Not Onboarded—Not onboarded to Juniper Mist Cloud. Click a connection state to filter the Device table by that state.
Hardware - End of Support	Displays the hardware End of Support (EOS) milestones. Use it to identify devices nearing or past their hardware support end date and plan replacements or renewals. For each category, you see the percentage of devices in that category. The categories are: • Expired • 0 - 3 months • 0 - 12 months • > 12 months
Hardware - End of Life	Displays the End of Life (EOL) milestones. Use it to identify devices approaching EOL to schedule migration to newer hardware and avoid operational impact. For each category, you see the percentage of devices in that category. The categories are: • Expired • 0 - 3 months • 0 - 12 months • > 12 months

Table 53: Categories *(Continued)*

Feature	Description
Contract State	Displays the contract coverage to ensure JTAC support eligibility. Use it to monitor support coverage and prioritize contract renewals. Click a contract state to filter the Device table by contract state. **NOTE**: • By default, the Supported filter is selected. You can click it to clear the selection. • Unsupported devices can still be onboarded and managed within your organization. For each category, you see the percentage of devices that are currently Supported and Unsupported. • **Supported**—Devices recognized as being covered by an active support contract. These devices are eligible for JTAC support. • **Unsupported**—Devices recognized as not being covered by an active support contract. JTAC support may not be available for these devices until the contract is renewed. If you find any data discrepancy, contact Customer Care for resolution. Once resolved, the data will be updated during the next data refresh cycle.

Table 53: Categories *(Continued)*

Feature	Description
Software - End of Support	Displays the software End of Support(EOS) milestones. Use it to identify devices running outdated software and plan upgrades to recommended releases. For each category, you see the percentage of devices in that category. The categories are: • Expired • 0 - 3 months • 0 - 12 months • > 12 months

Device Table

Provides detailed support insights at the device level, allowing you to perform deeper support analysis and troubleshooting.

Use the table to:

- View comprehensive support insights for each device in your organization.
- Apply filters from the Stats Panel or perform keyword-based searches to refine the device records.
- Drill down into specific devices to get more support insights, including advisories and bug reports.

When you first open the Installed Base page, the table shows only devices with active support contracts. This is because the Supported filter is applied by default.

If you want to see all devices, including those with expired contracts, click the **Supported** category in the Stats Panel to clear the filter.

TIP: Use the Stats Panel to quickly identify areas of concern, then explore the Device Table for actionable insights.

Table 54: Fields in the Installed Base Table

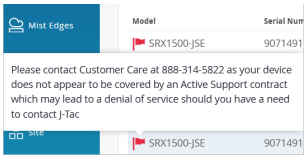
Field	Description
Model	The device model For Unsupported devices, a red flag icon is displayed next to the device model. On hover, a pop-up appears indicating that the device is not recognized as being covered by an active support contract and may not be eligible for JTAC support.  If you find any data discrepancy, contact Customer Care for resolution. Once resolved, the data will be updated during the next data refresh cycle.
Serial Number	Unique ID mapped to the device.
Status	Service level to which the device is onboarded. Blue checkmark indicates that the device is onboarded to Juniper Mist Cloud. **NOTE**: This field appears blank for devices not onboarded to Juniper Mist Cloud.
Device Host Name	Hostname of the device. **NOTE**: This field appears blank for devices not onboarded to the organization.
End of Support	Hardware End of Support date for the device.
End of Life	Hardware End of Life date for the device.
Software Release	Junos OS software version installed on the device. **NOTE**: This field appears blank for devices not onboarded to the organization.
Suggested Release	Recommended Junos OS software version for the device. **NOTE**: This field appears blank for devices not onboarded to the organization.
EOS	End of Service date for the device. **NOTE**: This field appears blank for devices not onboarded to the organization.

Table 54: Fields in the Installed Base Table *(Continued)*

Field	Description
FRS	Date on which the Junos OS software version was first released. **NOTE**: This field appears blank for devices not onboarded to the organization.

Find a Device by Using Filters

The Installed Base page offers multiple ways to narrow down your search.

- Use the filter buttons—The Stats Panel supports interactive filters.

  Click a category to show only matching devices in the table. To clear a filter, click the button again.

  For example, Click **MX480** to view only MX480 devices in the table.

- Apply batch filters—Combine multiple filters to narrow down your search. Batch filters let you apply more than one criterion at the same time.

  For example, select SRX4200 from Device Model and Unsupported from Contract State to show only unsupported SRX4200 devices in the table.

  Currently, batch filter supports device model, onboarding, and contract state criteria.

  > **NOTE**: Active filters are highlighted in the Stats Panel. To clear a filter, click the highlighted item again.

- Enter keywords in the Filter box—Start typing in the **Filter** box. For example, start typing the model name. As you type each character, matching entries appear in the drop-down list. Click the device that you want to show in the table. To clear the filter, click **Clear All**.

Tasks You Can Perform

- Add Juniper Account—Click **Add Juniper Account** button and enter your Juniper Support credentials (created through the Juniper Support Portal), to integrate your Juniper resources to your organization. You can associate multiple Juniper accounts with your organization and view all the linked accounts listed on this window.

  Alternatively, you can integrate your Juniper resources with your organization from the Organization Settings page (**Organization > Admin > Settings**).

- Adopt Devices—You can adopt switches and WAN Edges from Installed Base.

- Export details of all the devices in the CSV format—To export the data, click 
.

> **NOTE**: Any non-English characters might appear as special characters when you open the file. To prevent this issue, follow these steps:
>
> 1. Open a new Excel file and then select **File > Import > CSV File > Import**.
> 2. Select the file to be opened and then click **Get Data**.
> 3. In the Text Import Wizard, select **Unicode (UTF-8)** as the **File Origin**.
> 4. Click **Finish**.

Device Details for Installed Base

SUMMARY

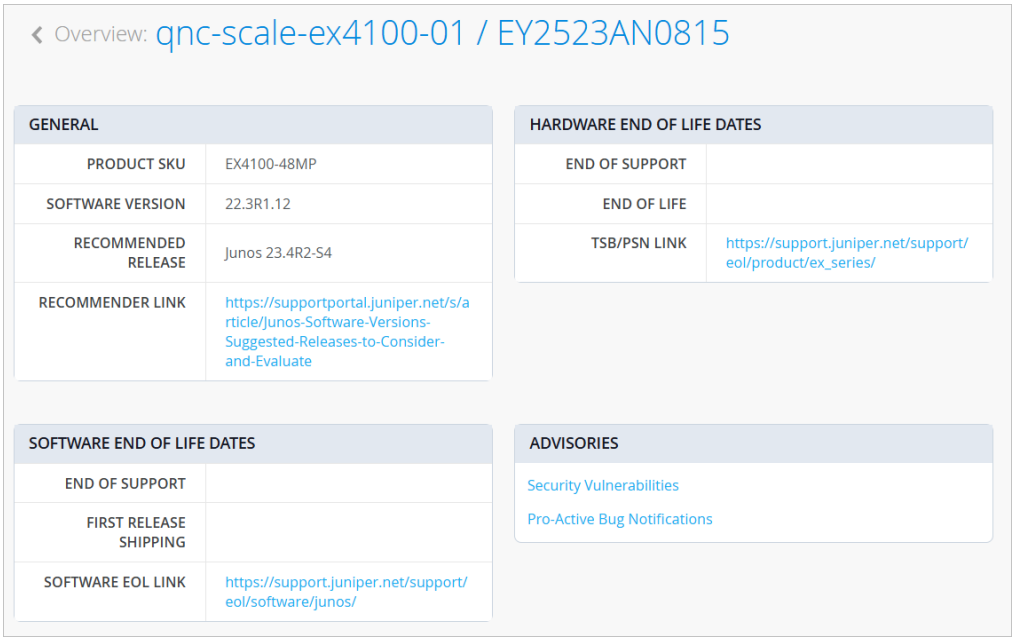
You can use the Device Details page to access additional support insights about the Juniper devices in your Installed Base.

IN THIS SECTION

To go to the Device Details page, click a device on the Installed Base page.

> **NOTE**: For more information about the Installed Base page, see "View Juniper Support Insights (JSI) for Your Installed Base" on page 164.

This page provides information about the product and includes links to information about hardware end of life, software end of life, security vulnerabilities, and bugs.



General Information

Use the General section to get general device information.

Table 55: Fields on the Overview Page

Field	Description
General	
Product SKU	Stock Keeping Unit (SKU) number assigned to the device.
Software Version	The Junos OS version installed on the device. **NOTE**: This field is blank for devices that aren't connected to the cloud.
Recommended Release	Recommended Junos OS software version for the device.
Recommended Link	Link to a Juniper Support Portal Knowledge Base(KB) article with a list of recommended Junos OS versions for each Juniper platform.
Hardware End of Life Dates	

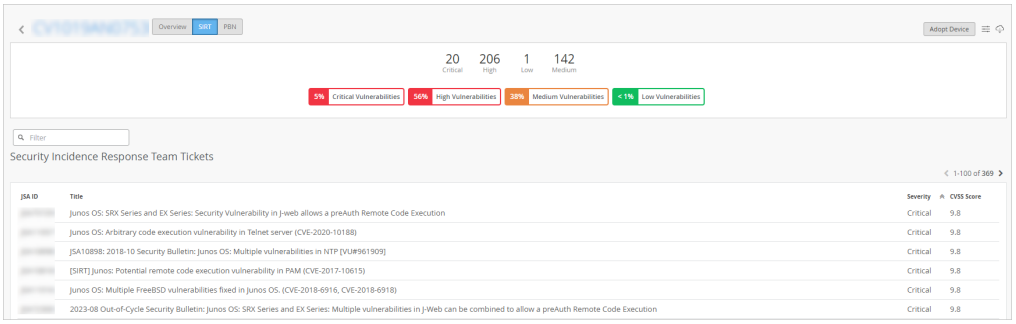
Table 55: Fields on the Overview Page *(Continued)*

Field	Description
End of Life	Date on which the device reaches end of life. Severity icons for hardware End of Life: • Red (critical)—Less than 3 months • Orange—3-6 months • Yellow—6-12 months • No icon—More than 12 months
End of Support	Date on which the Junos OS software version installed on the device reaches end of support.
TSN/PSN Link	Link to the Technical Support Bulletin (TSB) or Product Support Notification (PSN) that communicates end of life notifications for the specific device series.
Software End of Life Dates (Software EOL information is available only for connected devices.)	
End of Support	Date on which the Junos OS software version installed on the device reaches end of support.
First Release Shipping	Date on which the Junos OS software version was first released.
Software EOL Link	Link to the Junos OS Dates & Milestones page in the Juniper support website. This page contains dates of important milestones for all Junos OS versions.

Security Incidence Response Team (SIRT) Advisories

You can view Security Incident Response Team (SIRT) advisories (security vulnerabilities) for cloud-connected devices in your organization.

To view Security Incidence Response Team, click the **SIRT** tab.



If the device is cloud-connected (Assured), the Security Incident Response Team page displays a list of security vulnerabilities specific to the type of device and the Junos OS version installed. This information is not available for devices that are not connected to the cloud.

Features and Actions

- Filter buttons (top of page)—The top-of-page information boxes also are buttons that you can click to filter the table. For example, click a status, such as Critical, to show only advisories with that status. To clear a filter, click the button again.
- Keywords Filter box (above the table)—To find an advisory by entering keywords, start typing in the Filter box. When the matching items appear in the drop-down list, click the advisory that you want to see. To clear the filter, click **Clear All**.
- Adopt Device button (top-right corner of page)—Click this button to adopt the device into your organization.
- Table Settings button (top-right corner of page)—Click this button to show, hide, and reorganize the columns so that the table shows exactly the information that you want to see.

  In the pop-up window, select the columns that you want to see, and drag them into the desired order. Clear check boxes to remove columns from the Inventory Base table. When finished selecting and moving columns, click **X** to close the pop-up window.
- Download button (top-right corner of page)—Click this button to download the entire SIRT table.

  
- Table row link—In the table, click any row to open the Quick View Panel about the SIRT. In the panel, you can view more information or click the View SIRT Details button to go to the security bulletin in the Juniper Support Portal.
- Open a Quick View panel to view more information about the SIRT advisory. Click on any of the SIRT record to view the Quick View panel for the SIRT advisory.

Example

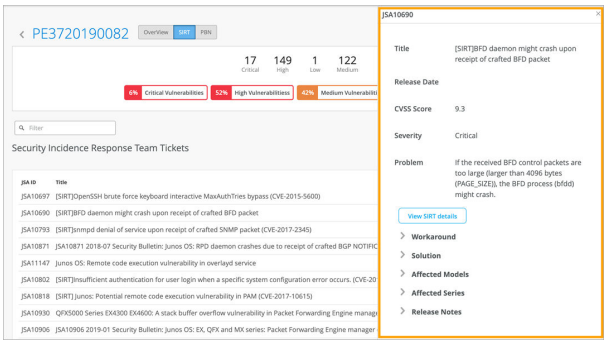


Table 56: Fields in the SIRT Information

Field	Description
JSA ID	Unique value that identifies the security advisory on Juniper Networks Support Portal.
Title	Synopsis of the security advisory.
Severity	Severity rating of the security advisory. The values are: • Critical • High • Medium • Low
CVSS Score	Common Vulnerability Scoring System (CVSS) severity assessment score of the advisory in the range of 0-10. This field is available on the **SIRT Quick View Pane** only.
Affected Models	Device models affected by the security advisory.
OS Versions Affected	Junos or Junos Evo versions affected by the security advisory.
Release Date	Date on which the security advisory was first published.
JSA Updated Date	Date on which the security advisory was last updated.
Problem	Description of the security advisory.

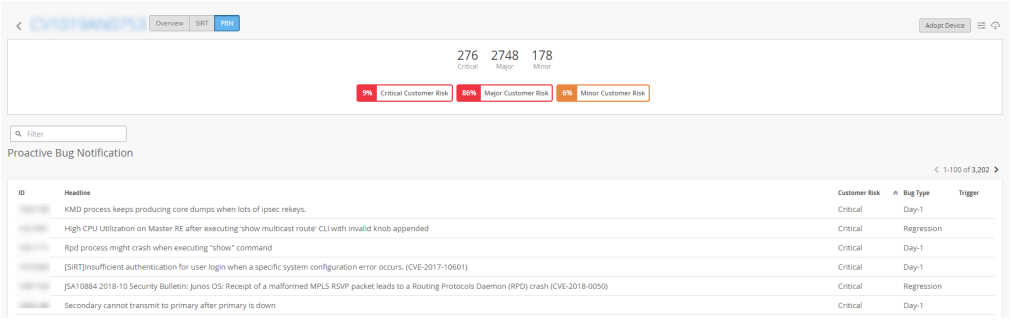
Table 56: Fields in the SIRT Information *(Continued)*

Field	Description
Solution	Solution for the security vulnerability described in the advisory.
Workaround	Detailed explanation on how to temporarily resolve the problem.
Affected Series	Identifies one or more product series affected by the security advisory.
Release Notes	Short description of the security advisory.

Proactive Bug Notification (PBN)

You can view Proactive Bug Notifications (PBNs) for cloud-connected devices in your organization.

To view proactive bug notifications, click the **PBN** tab.



If the device is cloud-connected (Assured), the page displays a list of known software issues relevant to the type of device and the Junos OS version installed. This information is not available for devices that are not connected to the cloud.

Features and Actions

- Filter buttons (top of page)—The top-of-page information boxes also are buttons that you can click to filter the table. For example, click a status, such as Critical, to show only notifications with that status. To clear a filter, click the button again.
- Keywords Filter box (above the table)—To find a notification by entering keywords, start typing in the Filter box. When the matching items appear in the drop-down list, click the record that you want to see. To clear the filter, click **Clear All**.
- Adopt Device button (top-right corner of page)—Click this button to adopt the device into your organization.

- Table Settings button (top-right corner of page)—Click this button to show, hide, and reorganize the columns so that the table shows exactly the information that you want to see.

  In the pop-up window, select the columns that you want to see, and drag them into the desired order. Clear check boxes to remove columns from the Inventory Base table. When finished selecting and moving columns, click **X** to close the pop-up window.

- Download button (top-right corner of page)—Click this button to download the entire PBN table.

- Table row link—In the table, click any row to open the Quick View Panel about the PBN notification.

  Example

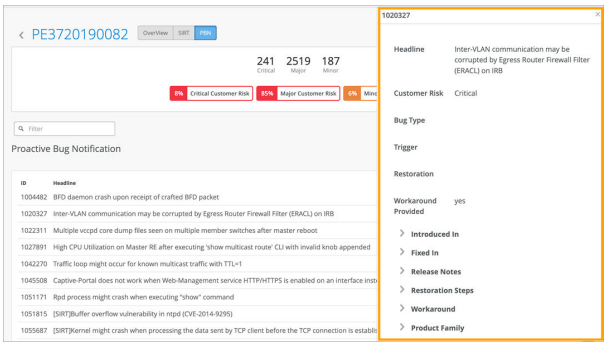
  

Table 57: Fields on the PBN Tab of the *Device* Details Page

Field	Description *(Columns and column order are determined by Table Settings.)*
ID	Unique value that identifies the Problem Report.
Headline	Synopsis of the problem.

Table 57: Fields on the PBN Tab of the *Device* Details Page *(Continued)*

Field	Description *(Columns and column order are determined by Table Settings.)*
Customer Risk	Classification of the potential impact to the customer if the bug was encountered in the network. The values include: • Critical—Conditions that could severely affect service, capacity or traffic, billing, and maintenance capabilities. • Major—Conditions that could seriously affect system operation, maintenance, administration, and so on. • Minor—Conditions that would not significantly impair the functioning of the network or significantly affect services.
Bug Type	Indicates the phase or activity during which the problem was discovered. Example: Day-1.
Trigger	Describes the events that happened before or at the time the problem occurred, or the event that caused the problem.
Introduced In	Junos or Junos Evo release where the problem was first found and reported.
Fixed In	Junos or Junos Evo release in which the problem was resolved.
Release Notes	Short description of the problem.
Restoration	Indicates how the service can be restored when the problem occurs. Values include: • Self-recovery—Service, traffic, or operation disruptions are automatically restored without any user intervention. • Not-possible—It is not possible to restore the service or traffic. • Manual—User intervention is required to restore the service, traffic, or operation disruption.
Restoration Steps	Steps to restore the service when the problem occurs.

Table 57: Fields on the PBN Tab of the *Device* Details Page *(Continued)*

Field	Description *(Columns and column order are determined by Table Settings.)*
Workaround	Detailed explanation of how to temporarily resolve the problem until a permanent resolution is available.
Workaround Provided	Indicates whether a workaround for the problem is provided or not. Values include: • Yes—Workaround is available and is described in the **Workaround** field. • Not-possible—There are no workarounds to the problem.
Product Family	Identifies one or more products affected by the problem.

Auto-Provisioning

SUMMARY

Speed up onboarding & configuration by using auto-provisioning to dynamically name devices, assign them to sites, and apply device configuration profiles.

IN THIS SECTION

Auto-provisioning simplifies the deployment process by enabling administrators to configure rules to automatically name an AP, assign an AP to a site, and assign a device profile to an AP. Using auto-provisioning, administrators need to only claim devices to an organization, and installers can install the devices at the site.

Without auto-provisioning, it can be tedious and time-consuming to complete these tasks. With auto-provisioning, Juniper Mist uses device attributes to automatically configure your devices as you onboard them. You can create simple auto-provisioning rules to:

- **Dynamically assign devices to sites:** Assign APs to sites based on the device name, model, DNS suffix, the LLDP system name, or the subnet that you connect the AP to. You can also assign Cellular Edge devices to sites based on the device name or the model. See "Automatically Assign Devices to Sites" on page 181.

  Example: A university has different subnets for each dorm. They set up auto-provisioning to assign devices on 10.1.0.0/16 to the Dorm 1 site, devices on 10.2.0.0/16 to the Dorm 2 site, and so on.

- **Dynamically name devices:** Assign names to APs based on the LLDP port or the MAC address. See "Automatically Assign Device Names" on page 185.

  Example: A large enterprise wants their device names to reflect the name of the switch that the device is connected to. They set up auto-provisioning to generate device names from the LLDP port description.

- **Dynamically assign device profiles:** Assign device profiles to APs based on the device name, model, DNS suffix, LLDP system name, or subnet. See "Automatically Assign Device Profiles to Access Points" on page 186.

  Example: A retail chain has different AP models that need different device settings. They set up auto-provisioning to assign Profile A to AP12 access points and Profile B to AP45 access points.

Juniper Mist generates audit logs for each instance of site assignment, device profile assignment, and AP name generation.

Automatically Assign Devices to Sites

SUMMARY

Speed up onboarding and configuration by using auto-provisioning to dynamically assign devices to sites based on the device attributes.

Automatic site assignments apply to devices that are claimed by your organization but not yet assigned to a site. This process will not reassign a device that is already assigned to a site. You'll need to preconfigure the sites before configuring the auto-provisioning rules for site assignment.

For example, a university has different subnets for each dorm. They set up auto-provisioning to assign devices on 10.1.0.0/16 to the Dorm 1 site, devices on 10.2.0.0/16 to the Dorm 2 site, and so on.

This feature is available for APs and Cellular Edge Devices.

Device Attributes for APs

For APs, Juniper Mist™ can automatically assign a site based on these device attributes:

- The device name. For this option, you need to configure each device name to include the site name.

  After an administrator creates an auto-provisioning rule, an installer must configure the device name using the following PUT operation:

  PUT: /installer/orgs/:org_id/devices/:device_mac

  See https://www.juniper.net/documentation/us/en/software/mist/api/http/api/installer/overview.

  If you have already provided a name for your AP through the Juniper Mist portal, you'll need to rename the AP using the API for the auto-provisioning to work.

- The Link Layer Discovery Protocol (LLDP) system name of the switch that the device is connected to. For this option, you need to preconfigure the LLDP system name to include the site name.

- The Domain Name System (DNS) suffix. For this option, you need to preconfigure the DNS suffix on the WAN Edge or router to include the site name.

- The subnet within which the IP address of the AP falls. You can view the IP address of the AP under the Status section on the AP Details page. For this option, you'll create a list of subnets and their corresponding sites when you configure the auto-provisioning rule.

  You might need to add multiple rules to match individual subnets to corresponding sites. This attribute is suitable for deployment across a small number of sites, each with a unique subnet.

  To assign all APs to a single site, add a rule for the 0.0.0.0/0 subnet.

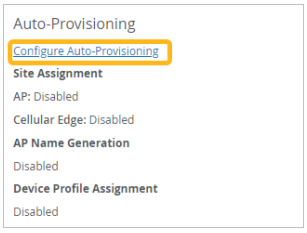
- The device model. For this option, you'll create a list of models and their corresponding sites when you configure the auto-provisioning rule.

Device Attributes for Cellular Edge Devices

For Cellular Edge devices, Juniper Mist can assign a site based on the device name or model.

To configure auto-provisioning for site assignments:

1. From the left menu, select **Organization** > **Admin** > **Settings**.
2. Click **Configure Auto-Provisioning**.



3. Click **Site Assignment**.
4. Click **Enabled**.
5. Click the **AP** tab or the **Cellular Edge** tab.
6. Click **Add Rule**.
7. Under **Deriving Site name based on**, select the device attribute that you want to use to identify the site.

   For example, select AP Name if you've included the site name in the AP device name. Or select model if you want to set up a correspondence between models and sites (you'll be able to do this in Auto-Provisioning window).
8. Based on the selected source, set the remaining options.

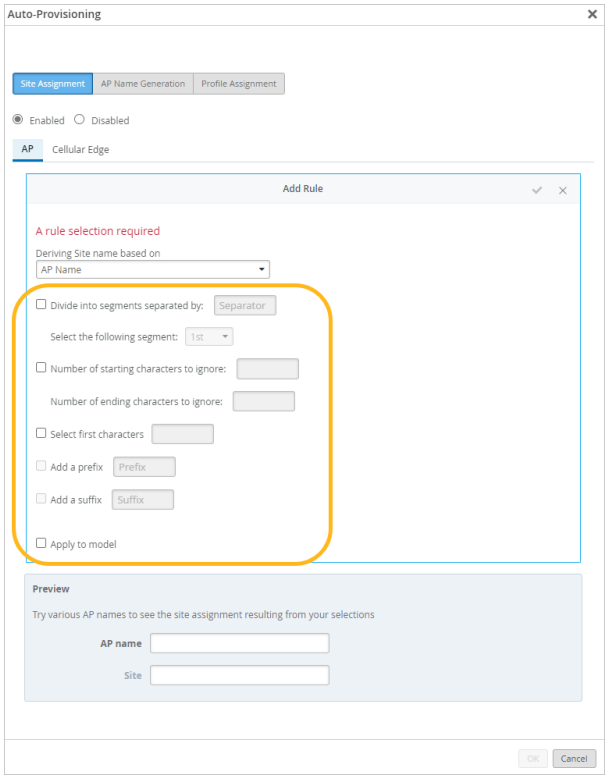
   If you're on the **AP** tab, you can derive the site name from these attributes based on the rule you configure.

   - **AP Name**, **LLDP System Name**, or **DNS Suffix**—Use the various options to transform the attribute into a valid site name, and then test your rule by using the **Preview** box. For auto-provisioning to work, the extracted information must exactly match the site name configured in the Juniper Mist portal.

     NOTE: If you want to use the AP Name attribute, you must use the installer API to preconfigure the AP name to include site identification information. See https://www.juniper.net/documentation/us/en/software/mist/api/http/api/installer/overview.

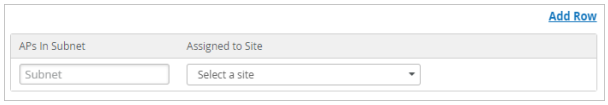
     If you have already provided a name for your AP through the Juniper Mist portal, you'll need to rename the AP using the API for the auto-provisioning to work

     In addition, you can also select the **Apply to Model** check box if you want to assign specific AP models to the site.



For information and examples, see "Manipulate Source Strings for Auto-Provisioning" on page 189.

- **Subnet** or **Model**—Complete the table at the bottom of the Auto-Provisioning window to match each subnet or model to a site.



If you're on the **Cellular Edge** tab, you can derive the site name from the **Cellular Edge Name** or **Cellular Edge Model**. Use the various options to transform the attribute into a valid site name, and then test your rule by using the **Preview** box. For information and examples, see "Manipulate Source Strings for Auto-Provisioning" on page 189.

9. Click the check mark at the top of the Add Rule area.

10. As needed, add more rules on the AP tab or the Cellular Edge tab.

If you add multiple rules, they're evaluated in a top-down manner. When Juniper Mist encounters a rule that identifies a site, it assigns the device and ignores any remaining rules. If it can't identify a site, you'll have to assign one manually.

For example, let's say the top rule on the AP tab is for AP Name and the next rule is for LLDP System Name. If Juniper Mist finds a matching site based on the AP name, it ignores the remaining rules.

11. Click **OK** to save your settings.

Automatically Assign Device Names

SUMMARY

Speed up onboarding and configuration by using auto-provisioning to dynamically assign names to devices based on the device attributes.

You can set up auto-provisioning to automatically assign names for APs based on the AP MAC address or the LLDP port to which the AP is connected.

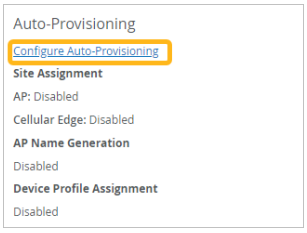
To use this feature, the AP must be claimed and assigned to a site.

For example, a large enterprise wants their device names to reflect the name of the switch that each device is connected to. They set up auto-provisioning to generate device names from the LLDP port description.

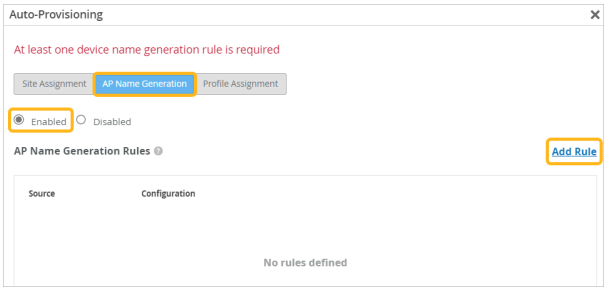
NOTE: This feature applies only to APs, not other types of devices. It does not rename an AP that already has a name.

To configure auto-provisioning for device names:

1. From the left menu, select **Organization** > **Admin** > **Settings**.
2. In the **Auto-Provisioning** section, click **Configure Auto-Provisioning**.



3. Click **AP Name Generation**.
4. Click **Enabled**.
5. Click **Add Rule**.



6. Under **Deriving AP Name from**, select **LLDP Port Description** or **MAC**.
7. Use the various options to transform the attribute into the desired characters, and then test your rule by using the **Preview** box. For information and examples, see "Manipulate Source Strings for Auto-Provisioning" on page 189.
8. Click the check mark at the top of the Add Rule area.

9. Add more rules if needed.

   If you add multiple rules, they're evaluated in a top-down manner. When Juniper Mist encounters an applicable rule, it assigns a name and ignores any remaining rules. If it can't find an applicable rule, you'll have to assign a device name manually.

   For example, let's say the top rule is for LLDP Port Description and the next rule is for MAC. If the port has a description, the rule is applied. If the port does not, then the MAC rule is applied.
10. Click **OK** to save your settings.

Automatically Assign Device Profiles to Access Points

SUMMARY

Speed up onboarding and configuration by using auto-provisioning to dynamically assign device profiles based on the device attributes.

You can set up auto-provisioning to automatically assign device profiles to access points (APs) that are claimed for your organization and have been assigned to a site.

For example, a retail chain has different AP models that need different device settings. They set up auto-provisioning to assign Profile A to AP12 access points and Profile B to AP45 access points.

NOTE:

- This feature applies only to APs, not other types of devices.
- This process will not assign a device profile if an AP already has one.

Juniper Mist can automatically assign a device profile based on:

- The Link Layer Discovery Protocol (LLDP) system name of the switch that the AP is connected to. To use this option, preconfigure the LLDP system name to include the device profile name.
- The subnet within which the IP address of the AP falls. You can view the IP address of the AP under the Status section on the AP Details page. To use this option, create a list of subnets and their corresponding device profiles when you configure the auto-provisioning rule.
  To assign all APs to a single profile, add a rule for the 0.0.0.0/0 subnet.
- The AP model. To use this option, create a list of AP models and their corresponding device profiles when you configure the auto-provisioning rule.
- The AP's device name. To use this option, configure each device name to include the device profile name.
  After an administrator creates an auto-provisioning rule, an installer must configure the device name using the following PUT operation:

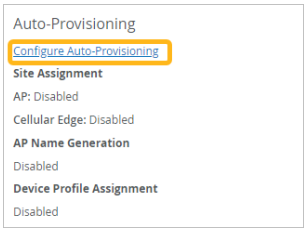
  PUT: /installer/orgs/:org_id/devices/:device_mac

  See https://www.juniper.net/documentation/us/en/software/mist/api/http/api/installer/overview.

  If you have already provided a name for your AP through the Juniper Mist portal, you'll need to rename the AP using the API for the auto-provisioning to work.
- The AP's Domain Name System (DNS) suffix. To use this option, you need to preconfigure the DNS suffix on the WAN Edge or router to include the device profile name.

To configure auto-provisioning for device profile:

1. From the left menu, select **Organization** > **Admin** > **Settings**.
2. In the **Auto-Provisioning** section, click **Configure Auto-Provisioning**.



3. Click **Profile Assignment**.
4. Click **Enabled**.
5. Click **Add Rule**.
6. Under **Deriving Profile name based on**, select the device attribute that you want to use to identify the profile.

   For example, select AP Name if you've included the profile name in the AP device name. Or select AP Model if you want to set up a correspondence between models and sites (you'll be able to do this in Auto-Provisioning window).
7. Based on the selected source, set the remaining options:

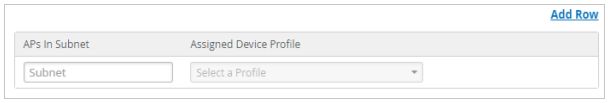
   - AP Name, LLDP System Name, or DNS Suffix—Use the various options to transform the attribute into a valid profile name, and then test your rule by using the **Preview** box. For auto-provisioning to work, the extracted information must exactly match the device profile name configured in the Juniper Mist portal. For information and examples, see "Manipulate Source Strings for Auto-Provisioning" on page 189.

     NOTE: If you want to use the AP Name attribute, you must use the installer API to preconfigure the AP name to include site identification information. See https://www.juniper.net/documentation/us/en/software/mist/api/http/api/installer/overview.

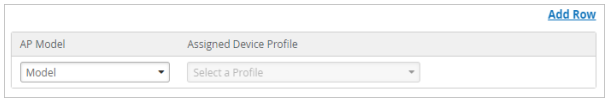
     If you have already provided a name for your AP through the Juniper Mist portal, you'll need to rename the AP using the API for the auto-provisioning to work

     In addition, you can also select the **Apply to Model** check box if you want to assign the profile to only specific AP models.

   - Subnet—Complete the subnet/profile table at the bottom of the Auto-Provisioning window. On the left, enter the first subnet, using the format *x.x.x.x/x*. On the right, select the site that you want to assign that subnet to. For each additional subnet, select **Add Row**, and then enter the subnet and the profile.



- AP Model—Complete the model/profile table at the bottom of the Auto-Provisioning window. On the left, select the model. On the right, select the site that you want to assign that model to. For each additional model, select **Add Row**, and then select the model and the profile.



8. Click the check mark at the top of the Add Rule area.

9. Add more rules if needed.

   If you add multiple rules, they're evaluated in a top-down manner. When Juniper Mist encounters a rule that identifies a device profile, it assigns the profile and ignores any remaining rules. If it can't identify a device profile, you'll have to assign one manually.

   For example, let's say the top rule on the AP tab is for AP Name and the next rule is for LLDP System Name. If Juniper Mist finds a matching device profile based on the AP name, it ignores the remaining rules.

10. Click **OK** to save your settings.

Manipulate Source Strings for Auto-Provisioning

SUMMARY

For certain auto-provisioning options, you can add or remove characters from the source string to identify the site, device name, or device profile that you want to assign to a device.

IN THIS SECTION

When adding auto-provisioning rules, you can transform a device attribute into a device name, site name, or profile name by extracting characters, ignoring characters, selecting characters, or adding characters.

You also can use multiple transformation options together.

Use these examples to experiment with the various options and understand how to transform your source strings into the desired result.

NOTE: Different options are available for different device attributes.

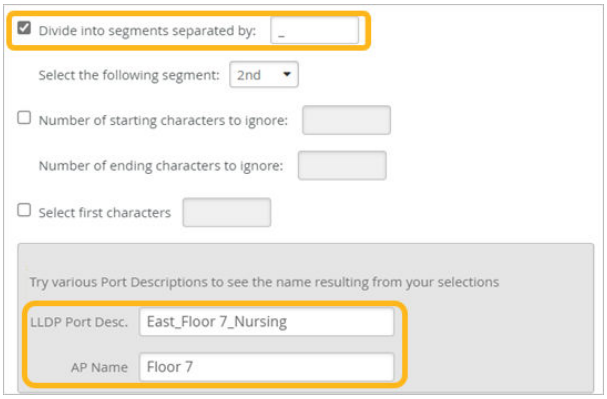
Divide a String into Segments

With this option, Juniper Mist selects one segment of a character-delimited source string. The source string must include one of the permitted delimiter characters:

- - (dash)
- _ (underscore)
- . (period)
- / (forward slash)

1. On the Organization Settings page, click **Configure Auto-Provisioning**.
2. Select the type of auto-provisioning: **Site Assignment**, **AP Name Generation**, or **Profile Assignment**.
3. Click **Enabled**.
4. (For Site Assignment or Profile Assignment only) Select the **Source**.
5. Select the check box for **Divide into segments separated by**.
6. For **Separator**, enter a valid delimiter character: **- _ . /**
7. Select the segment that you want to use for auto-provisioning (1st, 2nd, and so on).
8. Verify your selections by entering sample strings in the gray box at the bottom of the Auto-Provisioning window.

   In this example, the administrator wants Juniper Mist to use only the characters in the second segment of the AP name. To verify that this will enable Juniper Mist to generate the desired name, the administrator enters a sample AP name. Juniper Mist responds with the resulting name.



9. Click **OK**.

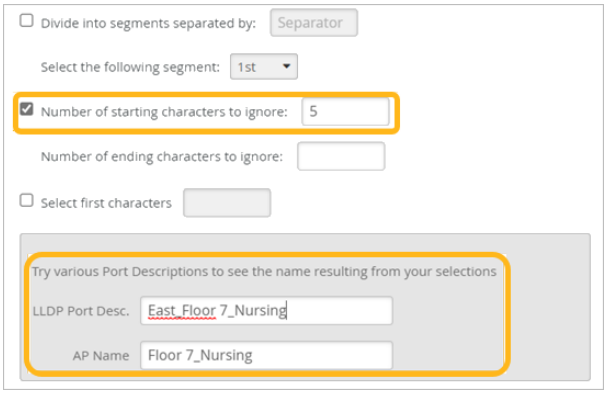
Ignore Starting or Ending Characters

With this option, Juniper Mist ignores the first characters, the final characters, or both ends of the source string.

1. On the Organization Settings page, select **Configure Auto-Provisioning**.
2. Select the type of auto-provisioning: **Site Assignment**, **AP Name Generation**, or **Profile Assignment**.
3. Click **Enabled**.
4. (For Site Assignment or Profile Assignment only) Select the **Source**.
5. Select the check box for **Number of starting characters to ignore**.
6. Enter the number of characters to ignore.

   You must enter a number in at least one of the **characters to ignore** text boxes.
7. Verify your selections by entering sample strings in the gray box at the bottom of the Auto-Provisioning window.

   In this example, the administrator wants Juniper Mist to ignore the first five characters of the AP name. To verify that this will enable Juniper Mist to generate the desired name, the administrator enters a sample AP name. Juniper Mist responds with the resulting name.



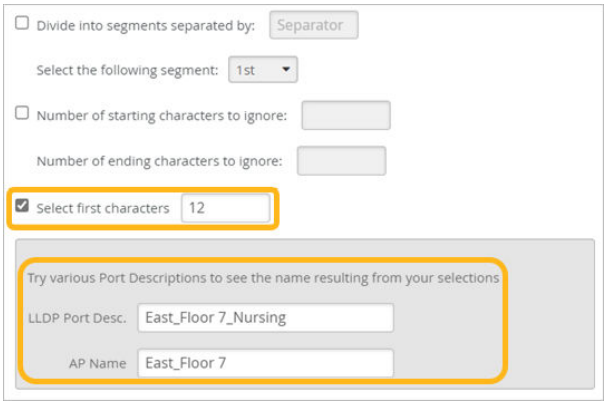
8. Click **OK**.

Select the First Characters

With this option, Juniper Mist uses only the specified number of characters from the start of the source string.

1. On the Organization Settings page, select **Configure Auto-Provisioning**.
2. Select the type of auto-provisioning: **Site Assignment**, **AP Name Generation**, or **Profile Assignment**.
3. Click **Enabled**.
4. (For Site Assignment or Profile Assignment only) Select the **Source**.
5. Select the check box for **Select first characters**.
6. Enter the number of characters to use.
7. Verify your selections by entering sample strings in the gray box at the bottom of the Auto-Provisioning window.

   In this example, the administrator wants Juniper Mist to select the first 12 characters of the AP name. To verify that this will enable Juniper Mist to generate the desired name, the administrator enters a sample AP name. Juniper Mist responds with the resulting name.



8. Click **OK**.

Add a Prefix or Suffix

With these options, Juniper Mist adds characters to the start of the source string (prefix), the end of the source string (suffix), or both.

1. On the Organization Settings page, select **Configure Auto-Provisioning**.
2. Select the type of auto-provisioning: **Site Assignment** or **Profile Assignment**.

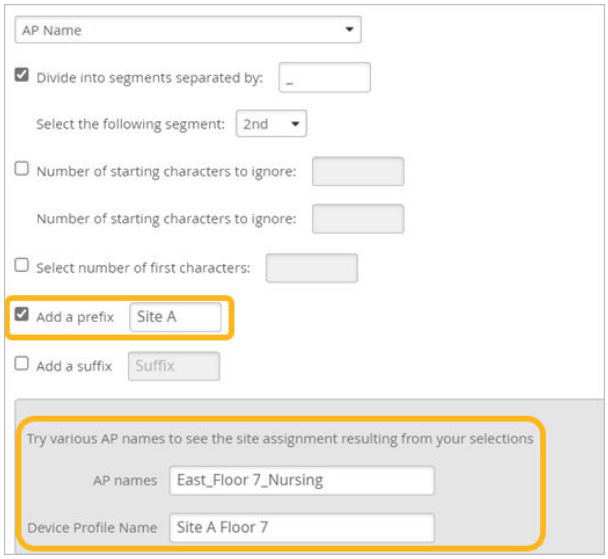
> **NOTE**: You cannot add a prefix or suffix when setting up auto-provisioning to generate an AP name.

3. Click **Enabled**.
4. Select the check box for **Add a prefix**, **Add a suffix**, or both.
5. Enter the characters to add.

6. Verify your selections by entering sample strings in the gray box at the bottom of the Auto-Provisioning window.

   In this example, the administrator wants Juniper Mist to use only the characters in the second segment of the AP name.

   In this example, the administrator wants Juniper Mist to add a prefix consisting of these characters: *Site A*. To verify that these selections will enable Juniper Mist to find the corresponding device profile, the administrator enters a sample AP name. Juniper Mist responds with the resulting device profile name.

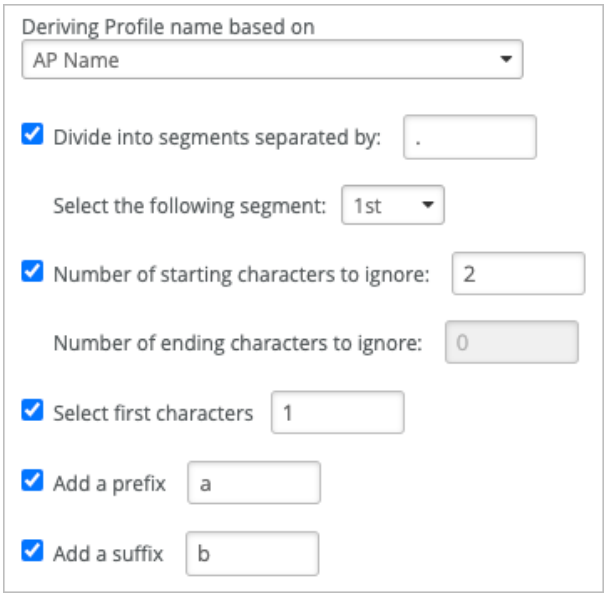


7. Click **OK**.

Using Multiple Transformation Options Together

When you use multiple options together, the string is transformed by the first selected option. Then the resulting characters are transformed by the next option, and so on until all options are applied.

Let's look at this example, where five options are selected.



Let's say that the source string is **1234.5678**.

- With the first option, the source string is segmented a the dot (.), and the first segment is selected. The result is **1234**. Only these characters are processed by the next option.
- Next, the first two characters are ignored, resulting in **34**. Only these characters are processed by the next option.
- Next, only the first character, **3**, is selected. Only this character is processed by the next option.
- Now the letter **a** is added as a prefix, resulting in **a3**.
- Finally, the letter **b** is added as a suffix, resulting in **a3b**.

Claim a Switch

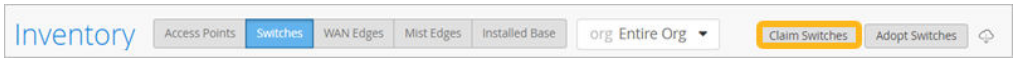
SUMMARY

Follow these steps to claim a new switch into your Juniper Mist™ organization.

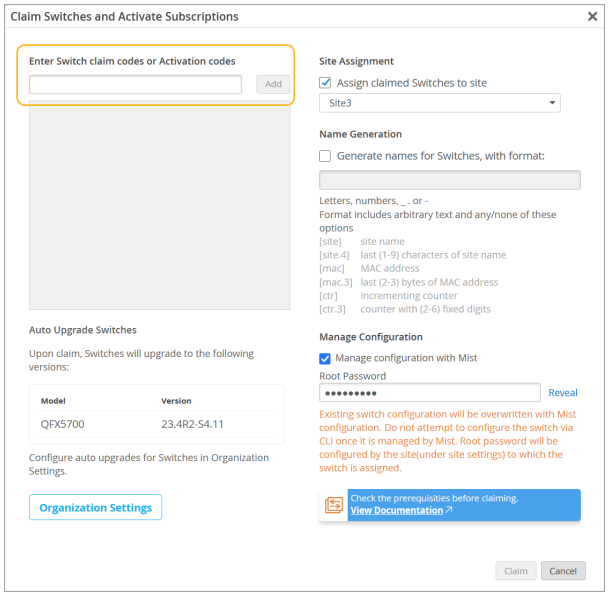
To connect a new switch to the Juniper Mist™ cloud, you need to claim it into your organization. Or, if you want to add a switch from your Juniper Installed Base, see "Adopt a Switch from Your Juniper

Installed Base" on page 196. Note that virtual devices such as vJunos-switch, and legacy devices that predate the Mist claim code on the physical hardware, cannot be claimed and instead must be adopted from the Inventory page or your Juniper Installed Base.

1. From the left menu, select **Organization** > **Admin** > **Inventory**.
2. Click **Switches** at the top left of the page, and then click **Claim Switches** at the top right.



3. Enter the activation code or claim code.



If the organization has automatic upgrade settings configured for the switch being claimed, the switch will be upgraded to the specified Junos version when onboarded. The Auto Upgrade Switches section displays the switch models (along with the target Junos version) for which automatic upgrade configuration is available. If you want to configure or modify these settings, refer to Configure Automatic Upgrade Settings for Switches.

4. Select other options as needed, and then click **Claim**.

NOTE: For detailed instructions, go to the Juniper Mist Supported Hardware page, and find the Quick Start Guide for your device.

Adopt a Switch from Your Juniper Installed Base

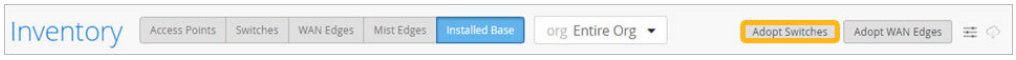
SUMMARY

Follow these steps to adopt a previously onboarded switch into your Juniper Mist™ organization.

If you integrated your Juniper account with your Juniper Mist™ account, you need to adopt the switches into your Juniper Mist organization.

For virtual devices such as a vJunos-switch or legacy devices that predate the use of Mist claim codes on the hardware, you need to adopt, rather than claim them. Note that if a VM has been claimed in one environment, such as Global02, it may not be available from the inventory or installed base of another environment or organization because the MAC address may still be attached to the original environment. To prevent this, be sure to release the device from the original environment, or recreate the virtual device, which will generate a new virtual MAC for it.

1. From the left menu, select **Organization** > **Admin** > **Inventory**.
2. Click **Installed Base** at the top center of the page, and then click **Adopt Switches** at the top right.



> **NOTE**: You also can adopt switches on the Switches page.

3. In the Switch Adoption window, follow the on-screen instructions to check the prerequisites and copy the code. Then apply the copied CLI commands to your switch.
4. Click X in the top right corner of the Switch Adoption window.

> **NOTE**: For detailed instructions, go to the Juniper Mist Supported Hardware page, and find the Quick Start Guide for your device.

Claim a WAN Edge

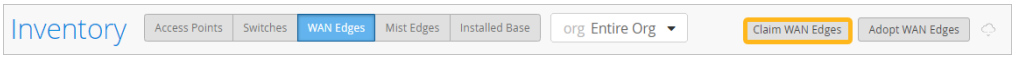
SUMMARY

Follow these steps to claim a new WAN Edge into your Juniper Mist™ organization.

To connect a WAN Edge to the Juniper Mist™ cloud, you need to claim it into your Juniper Mist organization.

NOTE: Follow this procedure to claim new WAN Edges. If you want to add a WAN Edge from your Juniper Installed Base, see "Adopt a WAN Edge from Your Juniper Installed Base" on page 197.

1. From the left menu, select **Organization** > **Admin** > **Inventory**.
2. Click **WAN Edges** at the top left of the page, and then click **Claim WAN Edges** at the top right.



3. Enter the activation code or claim code.
4. Enter the root password.
5. Make note of the on-screen information about the impact that this action will have on the existing gateway configuration.
6. Select other options as needed, and then click **Claim**.

NOTE: For detailed instructions, go to the Juniper Mist Supported Hardware page, and find the Quick Start Guide for your device.

Adopt a WAN Edge from Your Juniper Installed Base

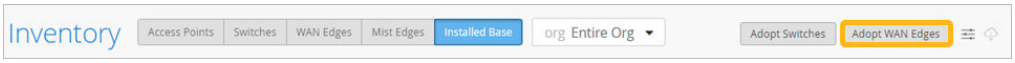
SUMMARY

Follow these steps to adopt a previously onboarded WAN Edge into your Juniper Mist™ organization.

If you integrated your Juniper account with your Juniper Mist™ organization, you need to adopt the WAN Edges into your Juniper Mist organization.

For virtual devices, such as virtual devices such as vSRX and vSSRs, and legacy devices that predate the use of Mist claim codes on the hardware, you need to adopt, rather than claim the device. Note that if a VM has been claimed in one environment, such as Global02, it may not be available from the inventory or installed base of another environment or organization because the MAC address may still be attached to the original environment. To prevent this, be sure to release the device from the original environment, or recreate the virtual device, which will generate a new virtual MAC for it.

1. From the left menu, select **Organization** > **Admin** > **Inventory**.
2. Click **Installed Base** or **WAN Edges** at the top center of the page, and then click **Adopt WAN Edges** at the top right.



3. In the WAN Edge Adoption window, follow the on-screen instructions to check the prerequisites and copy the code. Then apply the copied CLI commands to your Juniper WAN Edge.
4. Click X in the top right corner of the WAN Edge Adoption window.

NOTE: For detailed instructions, go to the Juniper Mist Supported Hardware page, and find the Quick Start Guide for your device.

Rename Devices

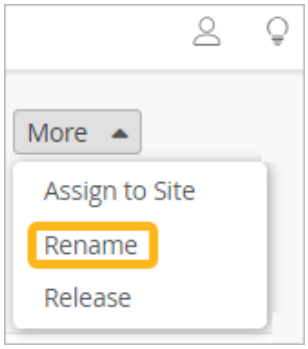
SUMMARY

Follow these steps to give new names to devices in your Juniper Mist™ organization.

1. From the left menu, select **Organization** > **Admin** > **Inventory**.

2. At the top of the Inventory page, click the button for the type of device that you're looking for.

3. Select the check box for the device or devices that you want to rename.
4. Click the **More** button, and then click **Rename**.



5. Use one of these options to change the device name:
   - Enter a new name in the text box.
   - Leave the text box blank to remove the names and leave the devices unnamed.
   - Read the on-screen information about the variables for name generation, and then enter a name that includes the variables that you want. For example, enter *[site]-[ctr]* to generate names such as *Main Site 1*, *Main Site-2*, and so on.
6. Click **Rename APs**.

6
CHAPTER

Sites

IN THIS CHAPTER

Configure a Site

SUMMARY

Follow these steps to add, modify, or remove sites in your Juniper Mist™ organization.

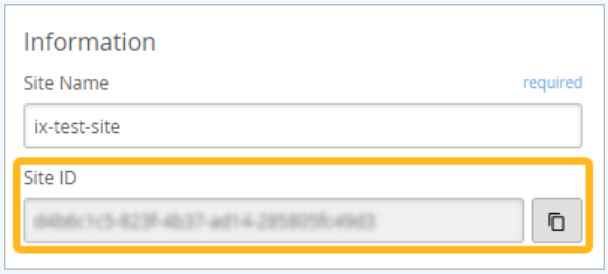
Use sites to configure and manage different physical locations or logical sub-divisions of your organization. For example, each site can have different RF templates and access point settings, different firmware upgrade schedules, and different settings for features such as location services, occupancy analytics, and engagement analytics.

When you create your organization on the Juniper Mist™ portal, Juniper Mist creates a site called Primary Site. You need to give the site a descriptive name and enter the location information. Then add sites to represent each physical location in your organization.

NOTE: The automatically generated site, Primary Site, has no special role among the sites. You can update or remove it.

1. From the left menu of the Juniper Mist portal, select **Organization** > **Site Configuration**.
2. Add or update sites as needed.
   - To configure the site settings, click the site.
   - At a minimum, enter the name, time zone, and location. For more information about location settings, see "Set the Site Location" on page 212. For information about other settings, see"Site Configuration Settings (Page Reference)" on page 202 .

     NOTE: You cannot change the site ID, which Juniper Mist automatically assigns when creating the site. This ID uniquely identifies the site in Juniper Mist cloud.

- To clone a site and copy its settings to a new site, click the site and then click **Clone Site**.
- To create a site without cloning, click **Create Site**.
- To delete a site, click the site, and then click **Delete Site**.

Site Configuration Settings (Page Reference)

SUMMARY

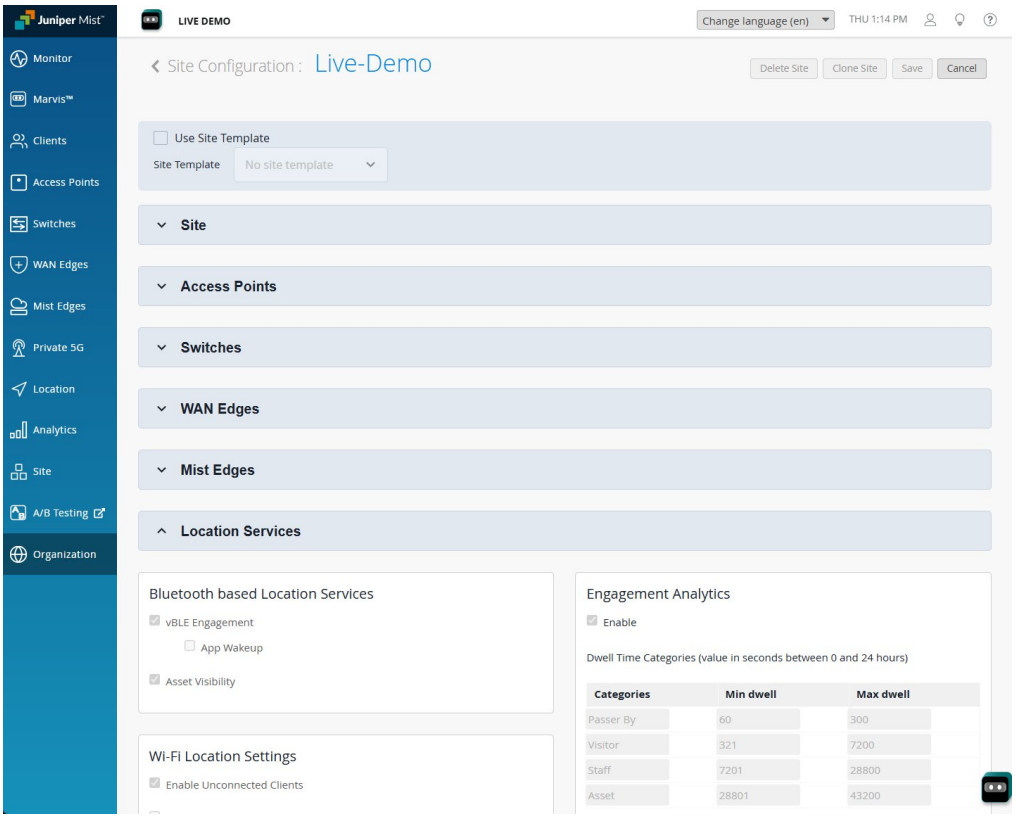
Learn about the various settings and options on the Site Configuration page.

IN THIS SECTION

Finding the Site Configuration Page

From the left menu, select **Organization** > **Admin** | **Site Configuration**. If you have multiple sites in your organization, a list of those sites appears. Select one to open the configuration settings page, as shown in Figure 1. The various site-level configuration options are organized by category, so you can display the configuration details for the groupset you want to configure and hide the details for the rest.

Figure 5: The Site Configuration Page



Major Sections of the Site Configuration Page

NOTE: If you make changes in the settings, click **Save** in the top right corner of the Site Configuration page.

Table 58: Site Configuration Settings

Section	Description	More Information
Information	Enter your site name, country, and time zone. Juniper Mist generates the Site ID, which cannot be changed.	
Location	Enter your location.	"Set the Site Location" on page 212

Table 58: Site Configuration Settings *(Continued)*

Section	Description	More Information
Notes	Enter notes, as needed.	
RF Template	If you want assign an RF template to this site, select the template.	*Radio Settings (RF Templates)* in the *Juniper Mist Wireless Guide*
Site Groups	For more efficient configuration and management, add similar sites to site groups.	"Site Groups" on page 213
AP Firmware Upgrade	Enable automatic updates and set the upgrade schedule.	*Enable Auto Updates* in the *Juniper Mist Wireless Guide*
Bluetooth based Location Services	Enable features for location-based services.	Juniper Mist Location Services Guide
WiFi Location Settings	If you enable this option, you also can opt to include or exclude unconnected wireless clients in occupancy analytics.	Juniper Mist Analytics Guide

Table 58: Site Configuration Settings *(Continued)*

Section	Description	More Information
Access Point Settings	Select the features that you want to enable for the access points (APs) at this site. • Local Status Page—Client devices can use the Local Status Page to get information about the AP that they're connected to. If you enable this option, enter the hostname, which is the address where users can view this page. • Automatically Revert Configuration—When you enable this feature, the APs at this site can automatically revert to their last known good configuration if they get disconnected from the cloud. This feature is applicable to all APs that are running 0.7.x firmware or newer.	
Wireless Mesh	A mesh network is a group of connectivity devices, such as APs, that act as a single network. Use this option to enable a wireless mesh network at the site level. After you enable the mesh network, you can then configure mesh settings for each AP on the Access Points page of the portal.	Using APs in a Mesh in the *Juniper Mist Wireless Guide*
DFS Scanning	If you enable wireless mesh, this option also appears. Dynamic Frequency Selection (DFS) prevents channel conflicts with systems such as weather radar, commonly located in airports. If a conflict is detected, the AP switches to a new channel.	

Table 58: Site Configuration Settings *(Continued)*

Section	Description	More Information
Switch Management	Enter a root password for your switches, and enable or disable switch proxy. If you don't define a root password in your site configuration, then the moment you activate a device to be managed by Mist Cloud, it will receive a randomly assigned root password.	
WAN Edge Management	Enter a root password for your WAN edge devices. If you don't define a root password in your site configuration, then the moment you activate a device to be managed by Mist Cloud, it will receive a randomly assigned root password.	
Session Smart Conductor	Enter up to two comma-separated IP addresses.	

Table 58: Site Configuration Settings *(Continued)*

Section	Description	More Information
Site Proxy	You can use a proxy server as a middleman between your local network and the Internet. Using a proxy server can provide extra security as well as a more controlled network environment. To integrate a proxy server with the Juniper Mist cloud, enter the proxy URL. Use this format: *http://user:password@proxy.internal:8080*. Once this feature is enabled, the configuration is pushed out to the access points. All transactions will then go through the proxy server. The proxy server will change the client's IP address to its own and send the traffic to the remote system. It will handle the reply from the remote system in the same way.	
Engagement Analytics	If you enable this features, Engagement Analytics is available on the Analytics menu. Set the dwell time categories and the days and times to monitor.	"Set the Engagement Dwell Limits and Schedule for a Site" on page 215
Occupancy Analytics	Set the parameters for the occupancy data on the Occupancy Analytics page.	"Set Up Occupancy Analytics for a Site" on page 216
Webhooks	Add and manage webhooks, which push notifications of Juniper Mist alarms and events to a server that you specify. After adding webhooks, you can click **View** to check the delivery status for the webhook events.	Juniper Mist Automation and Integration Guide

Table 58: Site Configuration Settings *(Continued)*

Section	Description	More Information
Security Configuration	Enable Juniper Mist to detect APs that might pose a security risk to your network. If you enable these options, these threats will be detected and displayed on the Security page.	Rogues, Honeypots, and Neighbor APs in the *Juniper Mist Wireless Guide*
AP Config Persistence	When you enable this feature, APs at this site store their last known configuration for fast retrieval.	*Enable Configuration Persistence* in the *Juniper Mist Wireless Guide*
AP Uplink Monitoring	Enable this feature if you want APs to monitor their uplink Ethernet ports for link status and automatically disable their WLANs upon loss of link. You might opt to disable this feature during special circumstances, such as an AP survey, when you expect APs to have power but no Ethernet link. **NOTE**: Uplink monitoring is automatically disabled for mesh relay APs.	

Table 58: Site Configuration Settings *(Continued)*

Section	Description	More Information
Juniper ATP	Integration with Juniper Advanced Threat Protection (ATP) Cloud adds another layer of security. If you enable this feature, also select the **Send IP-MAC Mapping to Juniper ATP** check box. This option allows better tracking of client hosts because Juniper Mist supplies the MAC addresses to Juniper ATP Cloud. **NOTE**: To complete the integration, you also need to enroll your SRX Series Firewalls in the Juniper ATP Cloud realm and enable the Juniper Mist integration in the Juniper ATP Cloud portal.	Juniper Advanced Threat Prevention Cloud (ATP Cloud) User Guide
Mist Tunnels	For site-level Juniper Mist Edge clusters, configure tunnels for this site.	
Radius Proxy	For site-level Juniper Mist Edge clusters, enable Radius Proxy and add the RADIUS servers. **NOTE**: First enable the site-level Juniper Mist Edge tunnels.	

Table 58: Site Configuration Settings *(Continued)*

Section	Description	More Information
Access Assurance Site Survivability	Site survivability keeps the Juniper Mist Access Assurance services up even when the cloud connectivity is down, by maintaining a cache of clients that were successfully authenticated in the past. In this setup, Access Assurance services run on a specified Mist Edge device inside the customer site. This Mist Edge acts as a backup when the WAN links are down. Requirements: • Juniper Mist Access Assurance subscription • At least one Mist Edge is assigned to the site. • Endpoints (laptops, mobiles and IoT devices) are authenticated and authorized into your corporate network. • WAN connectivity to the cloud is highly available. Settings: • **Caching Period**—Enter the number of days (1 to 30) to cache each NAC client. • **Default MAB VLAN**—Enter the VLAN ID or VLAN Name of the VLAN for unknown MAB clients. • **Default 802.1X VLAN**—Enter the VLAN ID or name of the VLAN for unknown 802.1X	

Table 58: Site Configuration Settings *(Continued)*

Section	Description	More Information
	clients that pass EAP-TLS authentication. • **Mist Edge IPs**—Enter the IP addresses of the Mist Edges to use for Site Survivability.	
Upstream Resource Monitoring	For site-level Juniper Mist Edge clusters, you can enable this feature to monitor the health of the upstream resources that you specify. If the health check fails, the Juniper Mist Edge prompts the APs to failover to the next member and shuts down the tunnel terminator service until the upstream resources are healthy and reachable again.	
CoA/DM Server	If you enabled Radius Proxy, you can also add CoA/DM servers.	Change of Authorization (CoA) in the *Juniper Mist Wireless Guide*
WAN Edge Advanced Security	As part of the SD-WAN configuration procedures, set the time and day for auto-upgrades. Also select **My SRX devices have an App Track license**. **NOTE**: Valid licenses must be loaded onto the SRX devices.	
Site Variables	Add variables to use in your configuration templates, such as WLAN and WAN Edge templates.	"Configure Site Variables" on page 220

Table 58: Site Configuration Settings *(Continued)*

Section	Description	More Information
Zones	A proximity zone is an RSSI-based feature that applies to individual or grouped APs. RSSI data from the clients triggers the zone entry and exit events. To add a zone, click the button. In the Generate Proximity Zones window, select the check boxes for the APs to include in the zone. Enter a name for the zone, and set the **Distance**, which is the RSSI level that triggers zone events. Repeat these steps for each zone that you want to create. **NOTE**: You also can add proximity zones to a floorplan on the Location Live View page.	*Add Proximity Zones to a Floorplan* in the *Juniper Mist Location Services Guide*

Set the Site Location

SUMMARY

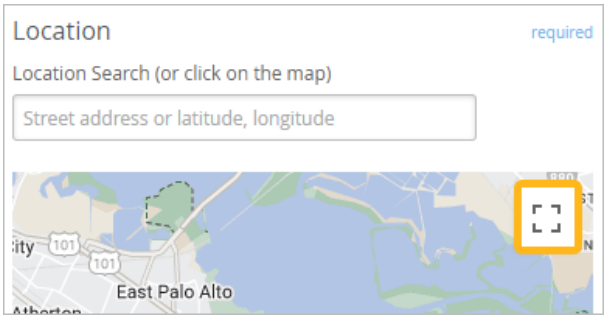
Follow these steps to correctly identify the exact location of your site.

1. From the left menu, select **Organization** > **Admin** > **Site Configuration**.
2. Click the site.
3. Under Location, set the location by using one of these options:
   - Enter the street address in the text box.
   - Enter the latitude and longitude coordinates in the text box.

- Use the map to select your location.

  Tips for using the map:

  - To enter or exit full-screen view, click the **Toggle fullscreen view** button in the top-right corner of the map.



  - To explore, drag the map up, down, left, or right.
  - To zoom in and out, use the plus and minus buttons.
  - To select a location, click it.

> **NOTE**: If you cannot connect to Google Maps, you can enter the street address, latitude, or longitude in text boxes.

4. Click **Save**.

Site Groups

SUMMARY

Understand the benefits of creating site groups and using them in your WLAN templates.

If your Juniper Mist™ organization includes multiple sites, you can create site groups to ensure consistent settings. For example, you could create a site group for each region (such as East, West, North, and South) or each purpose (Warehouse, Retail, and so on). Then assign a specific wireless LAN (WLAN) template to each site group.

You also can use site groups to manage administrator access. When you add an administrator account, you can allow access to all sites, specific sites, or site groups.

You can adapt site groups according to your needs.

- You can add a site to multiple groups. For example, you can assign a site to your Large Stores group and your Southwest Region group.
- You can apply a WLAN template to a site group that contains a site with unique settings. To bypass the template settings for that site, mark that site as an exception.

For information about managing site groups, see "Assign, Unassign, and Manage Site Groups" on page 214.

Assign, Unassign, and Manage Site Groups

SUMMARY

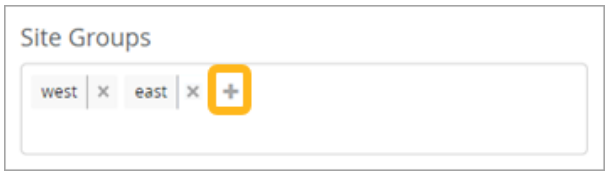
Follow these steps to create and manage the site groups for your organization.

Site groups can help you to manage your sites more efficiently. Use the Site Configuration page to assign and make changes to site groups.

1. From the left menu, select **Organization** > **Admin** > **Site Configuration**.
2. Select a site.
3. In the **Site Groups** section, assign, unassign, add, and remove site groups.
   - To assign this site to an existing site group, click **+** (the plus sign). Then click the site group.

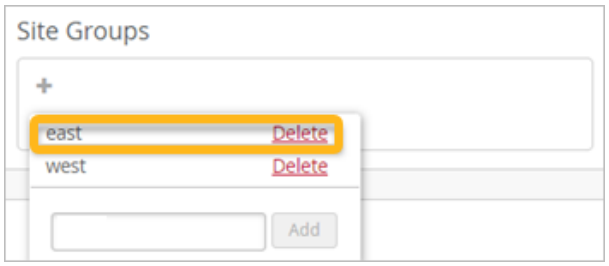
   - To create a site group and assign this site to it, click **+** (the plus sign). Then enter the new group name in the text box and click **Add**. Juniper Mist creates the site group and assigns this site to the new group.
   - To unassign this site from a listed site group, click **X** (the close icon) for the site group.

Example



- To delete a site group from your organization, click **+** (the plus sign), locate the site group in the pop-up window, and then click **Delete**. Juniper Mist deletes the site group and removes the site group assignment from all the member sites.

  Example



4. Click **Save**.

Set the Engagement Dwell Limits and Schedule for a Site

SUMMARY

Follow these steps to set the minimum and maximum dwell times and the data collection schedule for engagement analytics at your site.

When you enable engagement analytics for a Juniper Mist™ site, the Engagement Analytics page displays details about client activity for the organization, site, floorplan, and zone. You set up this feature in the site configuration.

1. From the left menu, select **Organization** > **Admin** > **Site Configuration**.
2. Select the site that you want to set up.

3. Under **Engagement Analytics**, enable this feature, define the categories, and set the monitoring periods.

   NOTE: If you disable this feature for all sites, Engagement Analytics is no longer available on the Analytics menu.

   - Define each category by entering the **Min dwell** and **Max dwell** times in seconds. The highest value that you can enter is 86,400 seconds (24 hours).

     These categories are used to segment the bar graphs on the Engagement Analytics page. Define each category based on the time frames that are relevant at the selected site. For example, at a small boutique, you might define a Customer as someone who stays between 3 minutes (180 seconds) and 30 minutes (1800 seconds). At a large furniture store, you might define a Customer as someone who stays between 15 minutes (900 seconds) and 3 hours (10800 seconds).

   - To set the periods when Juniper Mist collects data, set the **Start** and **End** times for each day. For example, you might want to collect data only during your posted business hours. For continuous monitoring, select 12:00 AM as the Start and End times every day.

     NOTE: This setting affects all zone-based location data, including occupancy analytics and zone-event webhooks. Data is only collected during the specified days and times.

4. Click **Save**.

Other Setup Tasks for Engagement Analytics

For full access to all features on the Engagement Analytics page, also complete these tasks:

- Set up your floorplans.
- Add zones to your floorplans.

For help with floorplan setup, see the Juniper Mist Location Services Guide.

Set Up Occupancy Analytics for a Site

SUMMARY

Follow these steps to enable features such as dwell duration, visualizations, and the types of occupants to track at your site.

Occupancy analytics are useful if you need to enforce capacity limits and prevent overcrowding at a Juniper Mist™ site. The Occupancy Analytics page provides real-time data about current conditions.

In the site configuration, set the minimum dwell duration, specify the types of occupants to track, and enable email alerts. You also can add a public occupancy dashboard, which allows anyone, such as contractors, security guards, and others to view real-time occupancy data without having to log into the Juniper Mist portal.

To set up occupancy analytics for a site:

1. From the left menu, select **Organization** > **Admin** > **Site Configuration**.
2. Select the site that you want to set up.
3. Under Occupancy Analytics, enter the settings.

Table 59: Options for Occupancy Analytics

Feature	Description
Minimum Dwell Duration	This is the amount of time that someone must be present to be counted as an occupant. For example, if a lobby or waiting area has a lot of passerby traffic, you might want to count people who have been there at least 60 seconds. Enter the time in seconds. The highest value that you can enter is 86,400 seconds (24 hours).

Table 59: Options for Occupancy Analytics *(Continued)*

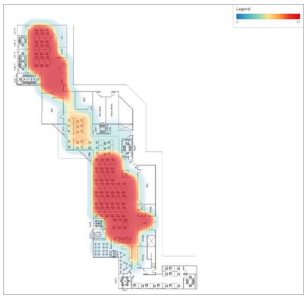
Feature	Description
Public Occupancy Dashboard	Enable or disable this feature and set the visualization mode. When enabled, anyone with the URL can access a public webpage that shows the occupancy data on the floorplan. The Visualization Mode determines how Juniper Mist presents the data on the public dashboard. • If you select Zone Occupancy, the zones are color-coded so that you can quickly identify the ratio of occupancy to capacity. For example, zones with low occupancy (below 50 percent of capacity) are green. Zones with excess occupancy (over 100 percent of capacity) are red.  • If you select Client Density, a heat map depicts the current occupancy across the floorplan. For example, the areas with highest number of occupants are red, and the areas with the fewest occupants are blue. 

Table 59: Options for Occupancy Analytics *(Continued)*

Feature	Description
Notifications	When you enable this feature, Mist notifies you when a zone is over capacity. • Compliance Duration—Mist will notify you immediately or will wait the specified amount of time. For example, if you select **5 min**, Mist will send a notification only if a zone's population exceeds its capacity limit for 5 full minutes. • Email Addresses—Click **+** to add an email address. Click **X** to remove an email address.
Occupant Types	Select the Occupant Types that you want to collect occupancy data for. • Connected WiFi Clients—Track clients that are currently connected to your Wi-Fi network. • Mobile Apps—Track clients that are using your Juniper Mist SDK-enabled applications. • Assets/Badges—Track Bluetooth Low Energy (BLE) tags that you have attached to employee badges and high-value equipment.

4. Click **Save**.

Other Setup Tasks for Occupancy Analytics

For full access to all features on the Occupancy Analytics page, also complete these tasks:

- Set up your floorplans, and add location zones. For help, see the Juniper Mist Location Services Guide.
- Set the capacity for each zone. To do this, select **Analytics** > **Occupancy Analytics** from the left menu, and then select a floorplan. For each zone, click the pencil icon, and then enter the maximum number of occupants.

Configure Site Variables

SUMMARY

Follow these steps to create site variables to use in your templates.

You can streamline and standardize the Juniper Mist™ configuration process by using site variables in your templates, such as WLAN and WAN Edge templates.

With variables, you can easily use a single template to configure multiple sites, even though they have different attributes such as subnet addresses and VLAN IDs.

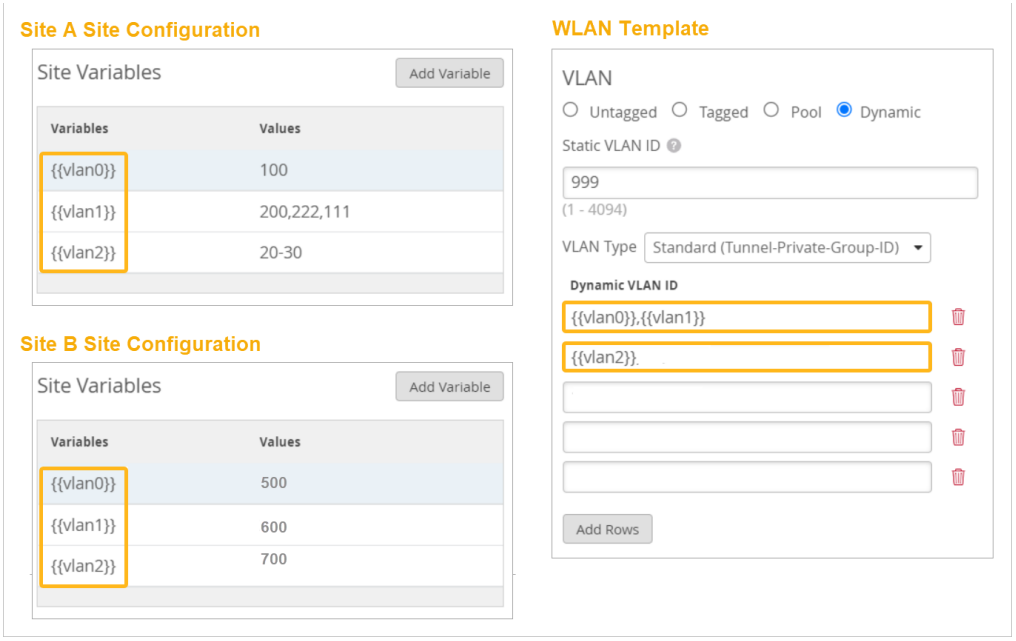
Naming Syntax

Variable names must be properly formatted.

- Contain the name within double curly brackets, such as *{{variableName}}*.
- The name can include letters, numbers, and underscores. Do not include any other special characters.

Example

This example shows how you can use one WLAN template for two sites that have different VLAN IDs.



- For Site A and Site B, you add variables with the same variable names, but different values.
- In the WLAN template, you enter the variable names.
- Juniper Mist uses this WLAN template to configure devices with the correct VLAN IDs for their respective sites.

TIP: When working on configuration screens, look for the VAR indicators. Fields with this indicator allow site variables.

To configure site variables:

1. From the left menu, select **Organization** > **Admin** > **Site Configuration**.
2. Click the site.
3. On the Site Configuration page, scroll down to the **Site Variables** section.
4. Add, import, or modify site variables:
   - To manually add a site variable, click **Add Variable**. Enter the name (following the naming syntax), enter the value, and then click **Save**.

   - To import a list of variables, first set up a CSV file that contains a header row and body rows similar to the example below. To avoid errors, be sure to follow the naming syntax. On the Site Configuration page, click **Import Variables**, select the file, and then click **Save**.

     CSV Example

     Variable,Value

     {{vlan01}},10

{{vlan02}},20

> **NOTE**: If your file contains a variable that already exists in the Site Variables list, Juniper Mist ignores that row of the CSV file.

- To edit a variable, click it, make your changes, and then click **Save**.
- To delete a variable, click it, and then click **Delete**.

5. To save the site configuration, click **Save** at the top right corner of the page.

   Be sure to save your changes before you leave the Site Configuration page. Although your changes appear in the **Site Variables** section, they are not saved until you click the **Save** button at the top of the page.

CHAPTER 7

Mist AI Mobile App

IN THIS CHAPTER

Mist AI Mobile App Overview

SUMMARY

Get started using the Mist AI mobile app to onboard devices.

IN THIS SECTION

The Mist AI mobile app enables you to onboard and manage devices and sites in your network directly from your mobile device. You can view device inventories, claim new devices, assign devices to sites, unassign devices from a site, and manage floor plans.

With this app, you can verify access point (AP) placements, update AP names, set the orientation and height for an AP, and replace APs. The app provides iOS users with additional advantages— for example— users can identify nearby APs through Bluetooth and verify AP placement using visual indicators.

Any modifications made through the app are synchronized with the Mist portal, ensuring seamless integration and real-time updates across the network infrastructure.

Requirements to Use the Mist AI Mobile App

To start using the app, you need to create an account on the Juniper Mist portal. See Create Your Account and Organization.

To log in to the app, you'll need to know:

- The e-mail address and password for your Mist user account. An administrator must add you as a user in the Juniper Mist portal.
- The name of your Juniper Mist organization.
- The environment for your Juniper Mist organization. See Juniper Mist Clouds.

Supported User Roles

These user roles can use the Mist AI app:

- Superusers
- Org Admin
- Network Admins with read access to the organization settings

> **NOTE**: Network Admins without read access to the organization settings cannot access the app.

- Observers with access to all sites
- Installers

Download and Install the App

The Mist AI app is available for download from Google Play Store and Apple App Store. The Mist AI app is compatible with the following devices:

- Android phone and tablet with OS version 6.0 or later.
- iPhone, iPod, and iPad with OS version 14 or later.

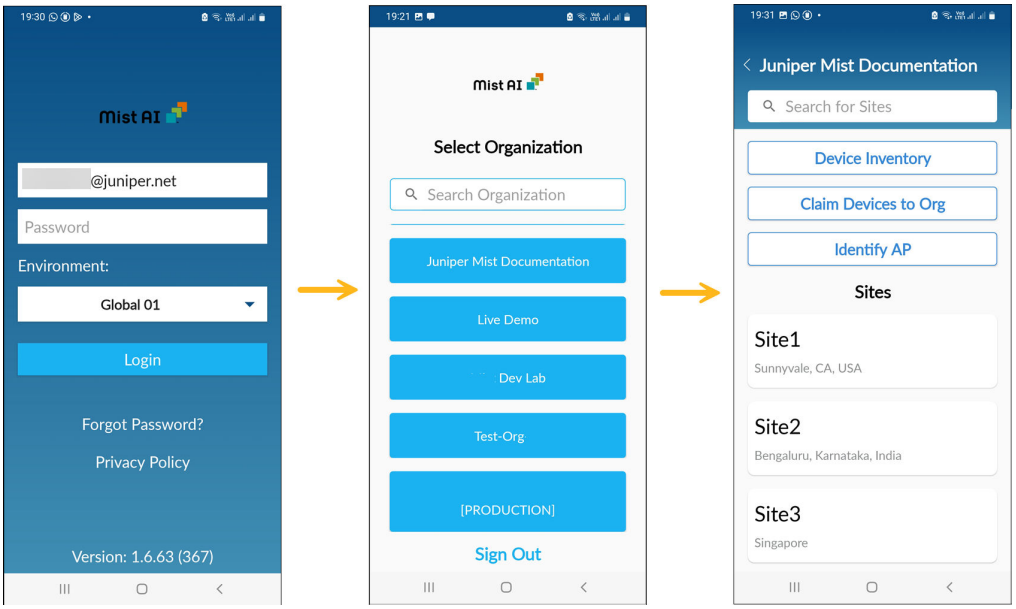
To download the app, navigate to the App Store or Play Store on your device and search for **Mist AI**. After you download and install the app, tap the Mist AI icon to start using the app.

Log In to the Mist AI Mobile App

Log in to the app using your registered e-mail address. You'll need to select the environment (for example, Global 01, Global 03).
If you have enabled two-factor authentication, use the Authenticator app to verify the device. The next time you log in, you can use Touch ID, Face ID, or passcode to log into the app directly.

> **NOTE**: You can use biometric authentication if your device supports it. You'll need to enable biometric authentication in your device settings.

You can then select your organization. When you select an organization, you can see the sites in that organization. Sites need to be created through the Juniper Mist portal. The app fetches the list of sites from the portal.



Claim and Assign Devices to a Site Using the Mist AI Mobile App

SUMMARY

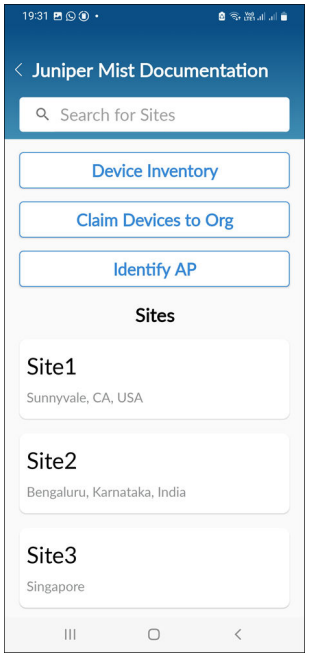
Onboard a switch, AP, WAN Edge, or Mist Edge using the Mist AI mobile app.

IN THIS SECTION

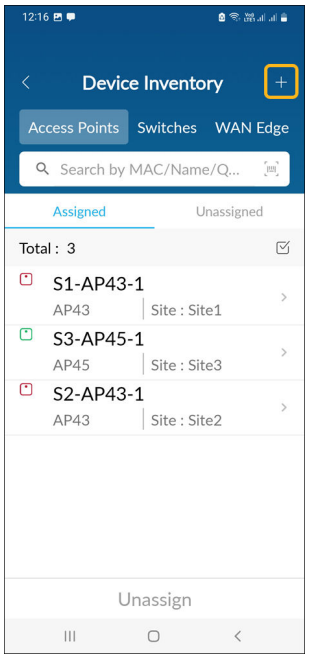
You can use the Mist AI mobile app to quickly onboard and assign a switch, an access point (AP), a WAN Edge device, or a Mist Edge device to a site.

To onboard a device using the Mist AI mobile app:

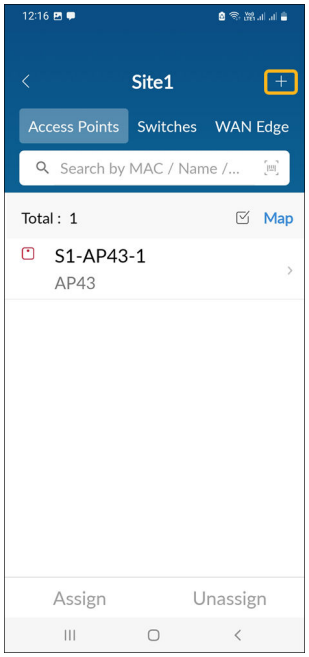
1. Open the Mist AI app and log in using your account credentials.
2. Select your organization.
3. Claim the device. You can claim a device in several ways:
   - On the home page, tap **Claim Devices to Org**. The device is only claimed with this step, and you'll need to manually assign the device to a site.



- On the Device Inventory page, select the appropriate device tab (Switches, Access Points, WAN Edges, or Mist Edges), and tap **+** in the top-right corner. The device is only claimed with this step, and you'll need to manually assign the device to a site.



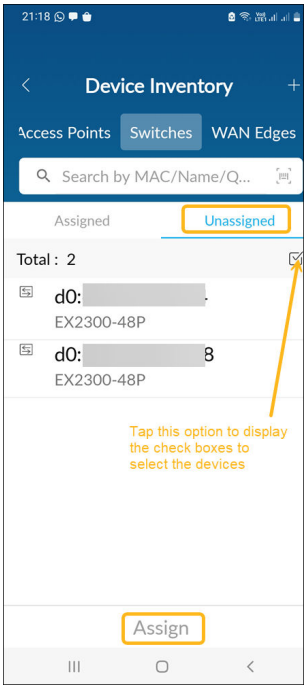
- On the Site page, select the appropriate device tab (Switches, Access Points, WAN Edges, or Mist Edges), and tap **+** in the top-right corner. In this case, the device is claimed and assigned to the site.



4. Locate the QR code on the device.
5. Focus the camera on the QR code. Alternatively, you can enter the claim code manually.
   The app automatically claims the device and you see the new device listed under the respective tab.

Assign a Device to a Site

Assigning a device to a site is a simple and quick process using the app. The Device Inventory page provides the list of assigned and unassigned devices in an organization. You can select the unassigned devices, tap **Assign**, and select the site to which the devices need to be assigned.



To unassign a device from a site, select the device from the Assigned tab and tap **Unassign**.

You can also assign a device to a site or unassign a device from a site using the Sites page.

View Site and Device Information in the Mist AI Mobile App

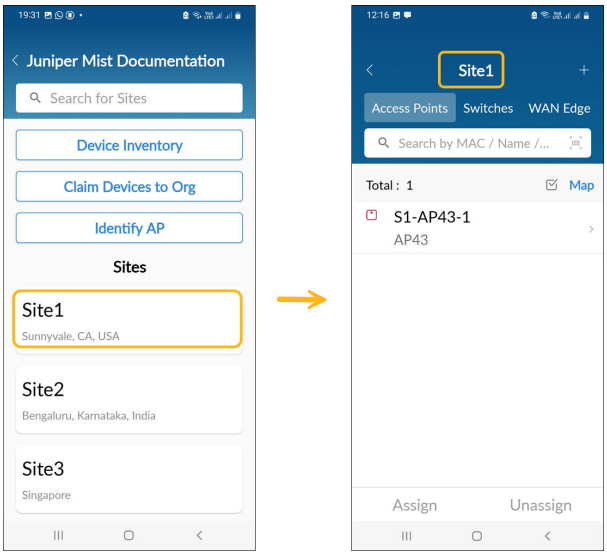
SUMMARY

Know how you can quickly access site and device details for an organization using the Mist AI mobile app.

IN THIS SECTION

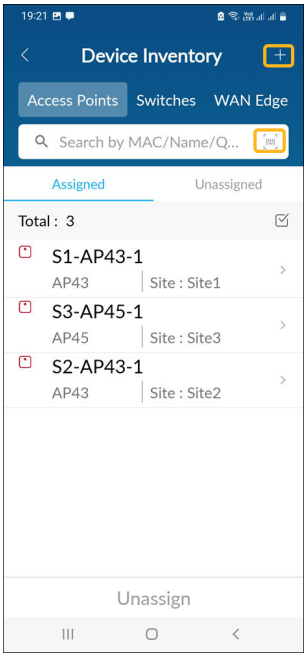
View Site Details

On the home page you see the list of sites in the selected organization. You can select a site and view the details of the devices located within the site.



View Device Inventory

On the home page, tap **Device Inventory** to view information about all the devices (APs, switches, WAN Edges, and Mist Edges) that have been claimed into the organization.



On the Device Inventory page, you can:

- Use the tabs at the top to select a device type.
- View assigned and unassigned devices.
- Search for a device by entering the MAC address or device name in the text box. Alternatively, you can search for a device using the QR code. Tap the camera icon to scan a QR code.
- Tap a device to go to the device details page.

Based on your user role, you can:

- Unassign a device—Tap the device under the Assigned tab, and then tap **Unassign**.
- Assign a device—Tap the device under the Unassigned tab, then tap **Assign**, and select the site to which the device needs to be assigned.
- Add a new device—Tap **+** in the top-right corner. Then scan the QR code or enter the claim code.

View Device Details

From the Device Inventory page or Site page, select a device to go to the device details page. On this page, you can:

- View the status to see if the device is connected or disconnected.
- Site to which the device is assigned.

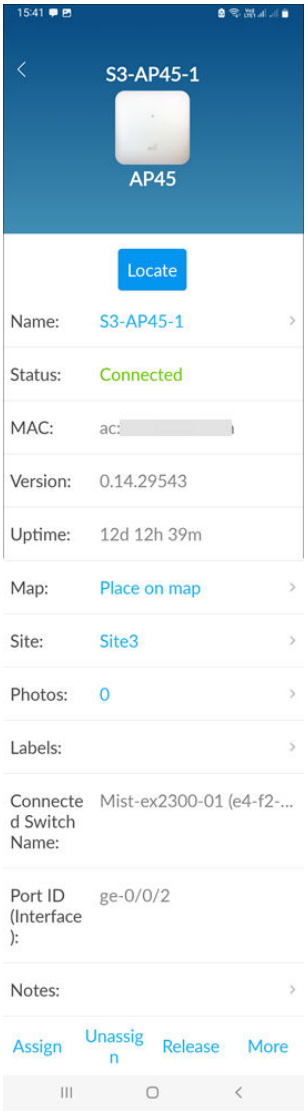
Based on your user role, you can:

- Assign a device to a site or unassign a device from a site.
- Release a device.
- Replace a device.

Some of the data on the device details page might vary depending on the device type.

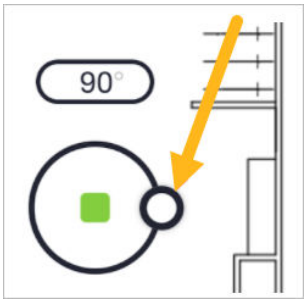
Here are a few examples of the device details page:

- **AP**

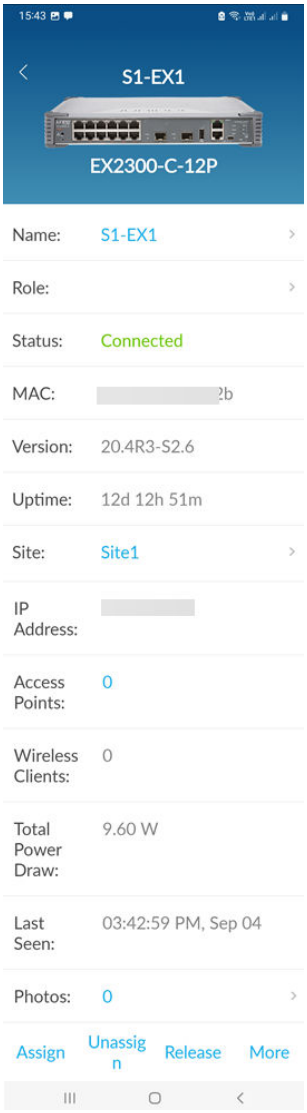


Additionally, for APs you can:

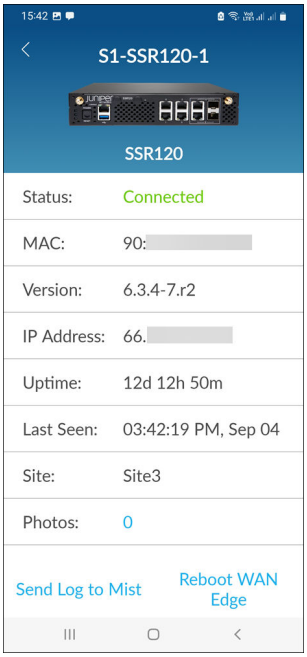
- Tap **Locate** to verify the AP placement. After you select this option, the LEDs on the physical AP start flashing green and purple. Tap **Unlocate** to stop this behavior.
- Place an AP on the floor plan. The Map field contains the **Place on a map** link if the AP has not yet been added to a floor plan. Tap the link and then drag the AP to its correct position. Finally, set the orientation by dragging the knob so that its position corresponds to the position of the LED on the AP. Also enter the height of the AP.



- **Switch**


15:43
S1-EX1
EX2300-C-12P
Name: S1-EX1
Role:
Status: Connected
MAC:
Version: 20.4R3-S2.6
Uptime: 12d 12h 51m
Site: Site1
IP Address:
Access Points: 0
Wireless Clients: 0
Total Power Draw: 9.60 W
Last Seen: 03:42:59 PM, Sep 04
Photos: 0
Assign
Unassign
Release
More

- WAN Edge



For WAN Edges, you can:

- Use the **Send Log to Mist** option to send logs to Juniper Mist Support for troubleshooting.
- Reboot the device.

Additional Options in the Mist AI Mobile App

SUMMARY

Know about the other options that the Mist AI mobile app provides.

IN THIS SECTION

Rename a Device

When you first claim a device, Juniper Mist assigns the MAC address of the device as its name by default. To give the device a more recognizable name, you can rename the device.

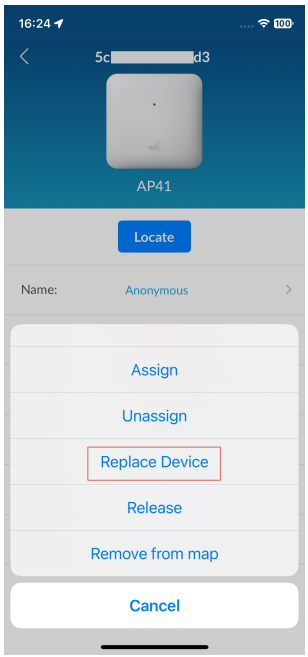
To rename a device:

1. Navigate to the Device Inventory or Site page on the Mist AI mobile app.
2. Select the device tab and tap the device to go to the details page.
3. Tap the device name.
4. Enter the new name you wish to assign to the device and tap **OK** to save the changes.

Replace a Device Using the Mist AI Mobile App

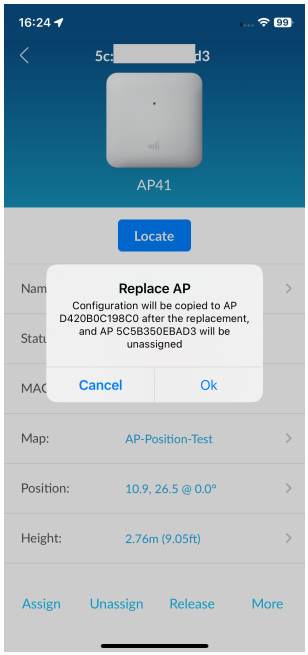
You can replace APs and switches from the mobile app.

1. Navigate to the Device Inventory or Site page on the Mist AI mobile app.
2. Select the device tab and tap the device to go to the details page.
3. Tap **More > Replace Device**.



4. Enter the claim code or scan the QR code of the new device.

   If you have not already claimed the device, the application automatically claims the device and assigns the device to the site. The app then prompts you to confirm the replace operation.



5. Tap **OK**.

Release a Device from Inventory

Releasing a device from your Mist organization's inventory is a useful feature if you no longer need the device to be part of your network or if you need to reallocate it to a different organization. Before you release a device, you must consider whether you need to retain any configuration settings associated with the device. These settings will not be accessible once you release the device.

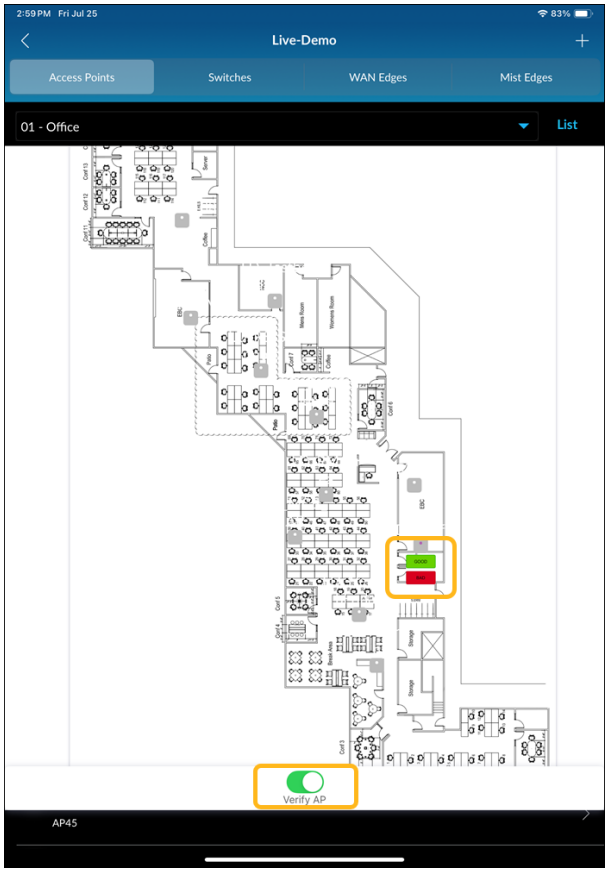
To release a device:

1. Navigate to the Device Inventory or Site page on the Mist AI mobile app.
2. Select the device tab and select the device that you want to release.
3. Tap **More > Release**.

Verify AP Placement

On iOS devices only, you can verify whether the location of an AP is good or bad.

1. On the home page, select a site, and go to the Access Point page.
2. Tap the Map option on the upper-right corner of the Access Points page.
   The floor plan is displayed.
3. Enable the **Verify AP** option located at the end of the page.



4. Select an AP.

   Mist evaluates the placement of the selected AP and assigns a label indicating whether the placement is good or bad.

Identify APs

Before scanning:

- Enable Bluetooth on your device.
- In the Juniper Mist portal, enable vBLE Engagement on the **Organization**>**Site Configuration** page.
- In the Juniper Mist portal, place all APs on a floor plan.

1. On the home page, tap **Identify AP**.
2. Tap **Scan** to start scanning.

Manage a Virtual Chassis Using the Mist AI Mobile App (iOS Devices Only)

SUMMARY

Know how you can create or modify a Virtual Chassis using the Mist AI mobile app.

IN THIS SECTION

A Virtual Chassis allows multiple switches to operate as a single logical device, simplifying management and improving scalability. The switches in a Virtual Chassis are interconnected through Virtual Chassis ports (VCPs), which handle data and control traffic. A Virtual Chassis can consist of two to ten switches, offering increased resilience if a switch fails. For more information about Virtual Chassis, see Virtual Chassis Overview (Juniper Mist).

With the Mist AI Mobile app, you can now create and manage a Virtual Chassis directly from your mobile device. The mobile app supports:

- Virtual Chassis creation and modification for devices without a VCP (EX2300, EX4650, and QFX5120).
- Virtual Chassis modification for devices with a VCP.

NOTE: Superusers and Org Admins can create and manage a Virtual Chassis. Installers can also use the feature, but with some limitations. Installers cannot upgrade the firmware or access the configurations in the Mist portal.

Create a Virtual Chassis Using the Mist AI Mobile App

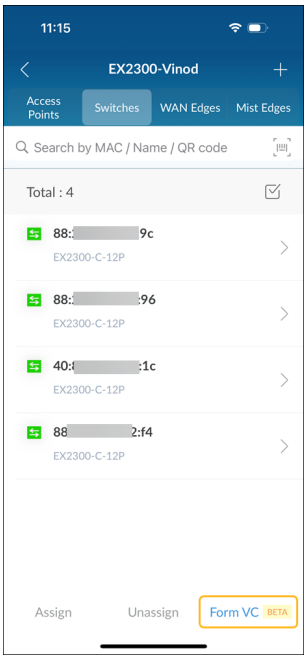
You can create a Virtual Chassis using the EX2300, EX4650, or QFX5120 switches, which do not have a dedicated VCP. The firmware upgrade on the switches that you include in the Virtual Chassis occurs as part of the Virtual Chassis creation process.

NOTE: Before you begin this task, ensure that you have enabled configuration management on the switches that'll be part of the Virtual Chassis. You must enable the option through the Juniper Mist portal, as it cannot be enabled from the app.

The **Modify VC** button is disabled on the app when the **Configuration Management** option is disabled for the switch.

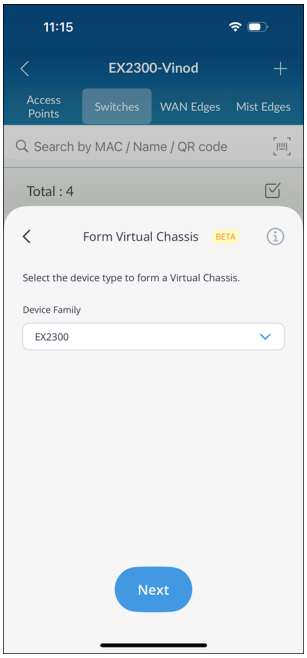
To create a Virtual Chassis:

1. On the mobile app home page, tap the site on which the Virtual Chassis needs to be created and select the **Switches** tab.
2. Tap the **Form VC** option at the lower-right corner of the Switches page.

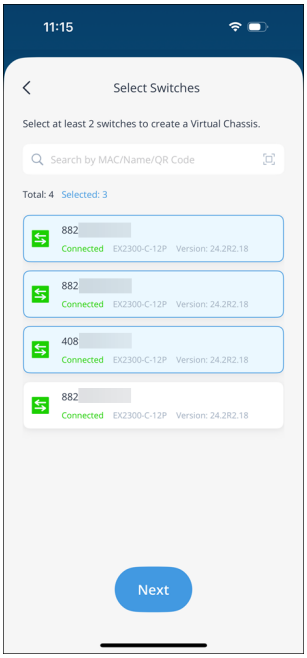


You'll see the list of switch family SKUs that support Virtual Chassis creation (EX2300, EX4650, and QFX5120).

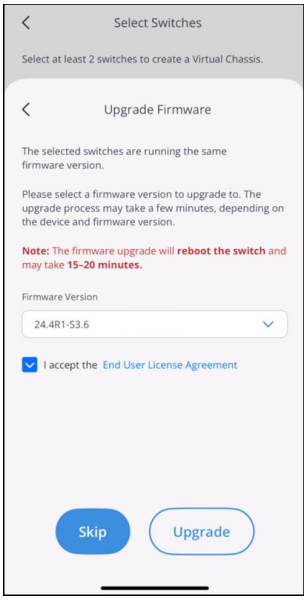
3. Select a device family and tap **Next**.



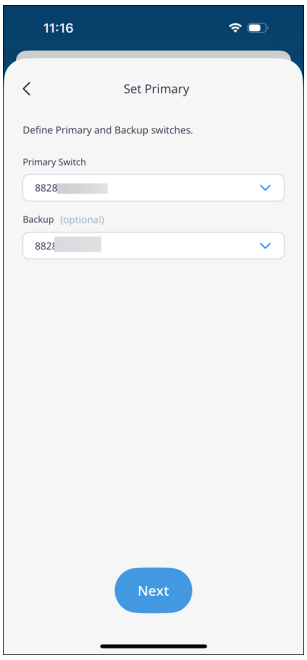
4. Select the devices that you want to add to the Virtual Chassis and tap **Next**. You'll see only the list of switch models for the selected device family. You'll need to select at least two switches.



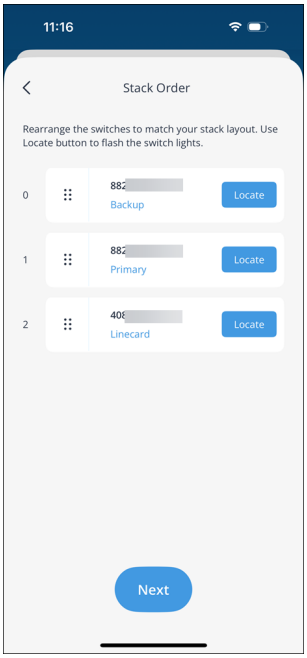
5. Upgrade the firmware on the switches so that all the switches in the Virtual Chassis run the same Junos OS version. If all the switches are already on the same Junos OS version, you can skip this step.



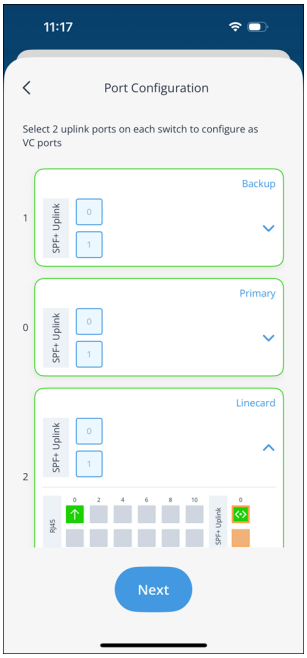
6. Select the primary and backup switches for the Virtual Chassis and tap **Next**.



7. Rearrange the switches to match the physical stack layout and tap **Next**. You can also identify the switches that use the locate functionality.

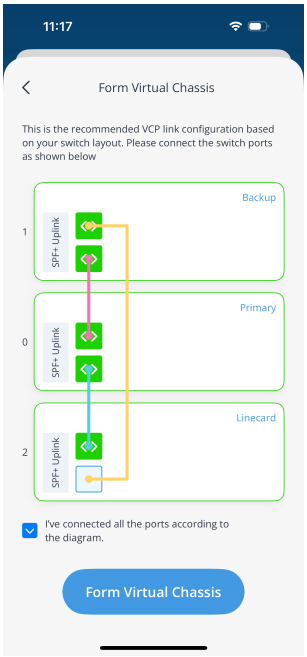


8. Select the ports to be configured as uplink ports and tap **Next**.



The Mist app displays the recommended VCP link configuration.

9. Connect the uplink ports by following the recommendation and select the **I've connected all the ports according to the diagram** check box. You can also upload a picture of the VCP link configuration.



NOTE: We recommend using a ring topology, which ensures that each switch is connected to both the preceding switch and the following switch, creating a continuous loop. The switches at the edges are also interconnected. If one of the connections fails, the circular design and the presence of redundant links keep the Virtual Chassis operational, enhancing reliability and network resilience.

10. Tap **Form Virtual Chassis**.

Modify a Virtual Chassis Using the Mist AI Mobile App

IN THIS SECTION

The Mist AI mobile app provides a flexible and convenient way to modify a Virtual Chassis. You can add a new device to the Virtual Chassis stack or delete a member from the Virtual Chassis stack. You can also change the device roles or the order of devices in the stack. You can perform these operations using the **Modify VC** option under the **More** option on the Switch details page.

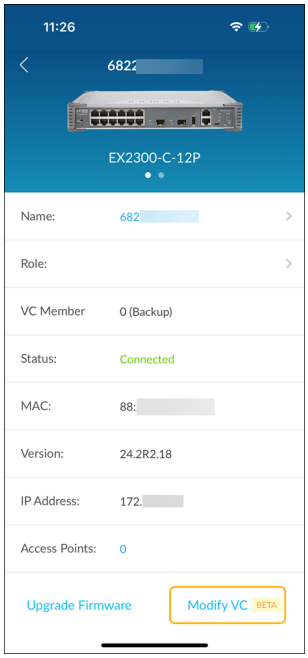
Add a Switch to a Virtual Chassis Using the Mist AI Mobile App

Before adding a new switch to an existing Virtual Chassis, ensure the following prerequisites are met:

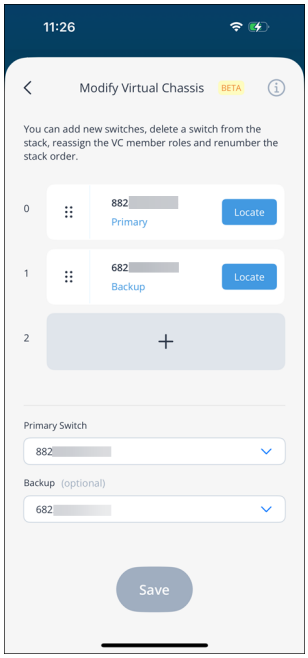
- Model compatibility—The new switch must belong to the same model family as the existing members of the Virtual Chassis.
- Network connectivity—The new switch must be connected to the network (applicable to EX2300, EX4650, and QFX5120).
- Site assignment—The new switch must be assigned to the same site as the other members of the Virtual Chassis.
- Virtual Chassis exclusivity—The new switch must not already be part of any other Virtual Chassis.

To add a switch to an existing Virtual Chassis:

1. Select the Virtual Chassis that you want to modify and tap **Modify VC**.



2. On the Modify Virtual Chassis page, tap + to add a switch to the Virtual Chassis.



3. Select a switch from the list displayed and tap **Next**. The app displays the switches that belong to the same switch family as the other switches in the Virtual Chassis.
4. Upgrade the switch firmware to the same Junos OS version as the other switches in the Virtual Chassis. If the switches are already on the same Junos OS version, you can skip this step.
5. Select the ports to be configured as uplink ports and tap **Next**.

   The Mist app displays the recommended VCP link configuration.
6. Connect the uplink ports by following the recommendation and select the **I've connected all the ports according to the diagram** check box.
7. Tap **Update Virtual Chassis**.

Remove a Switch from a Virtual Chassis Using the Mist AI Mobile App

To remove a switch from the Virtual Chassis stack, you'll need to first disconnect the switch from the Virtual Chassis. Power off the switch or remove the VCP cable from it. The mobile app prompts you to confirm whether you want to remove the switch from the Virtual Chassis.

NOTE: If you are replacing the primary member, perform a graceful switchover from the primary role to the backup role. To perform this step, log in to the Remote Shell and run the following CLI command. The Remote Shell provides direct access to the CLI through the Mist portal.

```
request chassis routing-engine master switch
```

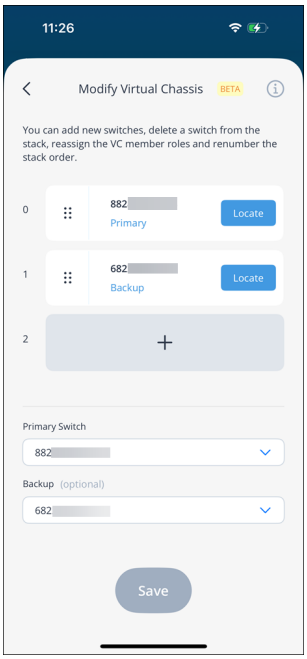
When the backup switch becomes the new primary switch, power off the original primary member (the member to be replaced). Then remove the VCP cables from this member.

Renumber the Virtual Chassis Members Using the Mist AI Mobile App

If you prefer to have the order of switches reflect their physical stacking arrangement on the app, you can reorder the switches after they are powered on and connected to the Virtual Chassis. The process of modifying the order of member switches is quite simple in the app. To rearrange the switches in the stack, tap and hold the stack of 3 dots located on the left side of each switch. Drag the switch to your desired position and release to drop it in place.

Reassign Virtual Chassis Member Roles Using the Mist AI Mobile App

You can change the role of a switch from the Modify Virtual Chassis page in the app. You can change the role from primary to backup, backup to line card, or line card to primary.



8
CHAPTER

Help and Support

IN THIS CHAPTER

Create a Support Ticket

SUMMARY

Explore how to use self-help options, get assistance with new deployments, return merchandise, and request support with various types of issues.

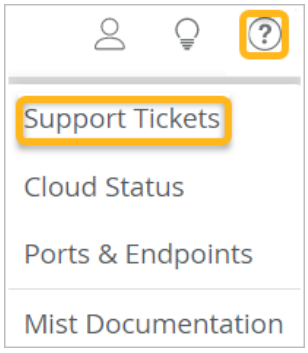
If issues occur and you need help, create a support ticket. You can get help with general questions, subscriptions, configuration options, new deployments, merchandise returns, device outages, and network-wide issues.

TIP: As you create your ticket, be aware of features that can help you to resolve the issue on your own:

- For general questions, start entering a little information about your issue, and suggested resources appear. Marvis subscribers will see an AI-generated response that summarizes information from Juniper Mist documentation. For many types of problems and configuration questions, you can find the answers that you need without further assistance.
- For certain ticket types, Marvis subscribers will see Marvis buttons on the support form. Click to start troubleshooting with Marvis. You can resolve many types of issues this way.

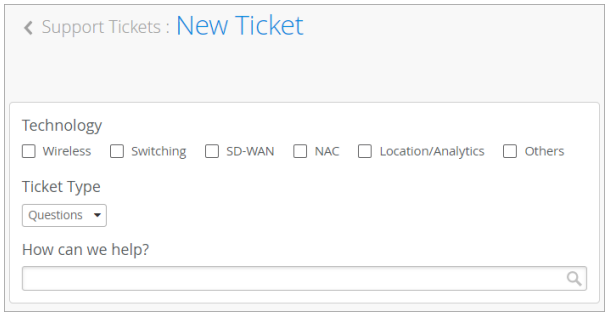
To create a support ticket:

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



2. Click **Create a Ticket**.

3. (Optional) Select the **Technology**.



NOTE: The available options depend on which ticket type is selected.

4. Select a **Ticket Type**.

Table 60: Ticket Types

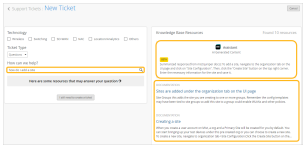
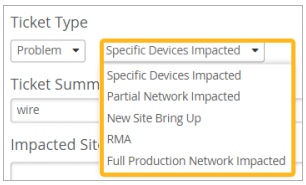
Type	Description
Questions	Select this ticket type if you have general questions. Then start typing in the **How can we help?** box. As you type, suggested resources appear on the right side of the screen. Marvis subscribers will see an AI-generated response that summarizes information from Juniper Mist documentation. Often the on-screen information provides the help that you need. Or, to get help from the support team, click **I still need to create a ticket**. 
Subscriptions	Select this ticket type if you have a question or problem concerning a subscription or order.
Configuration Help	Select this ticket type if you need help configuring your organization, site, network, or devices.

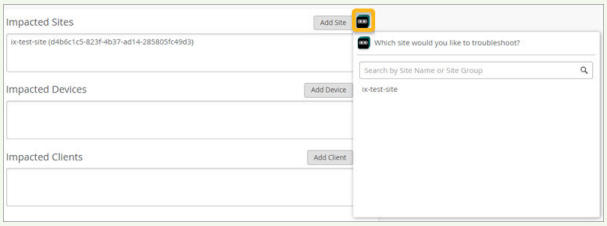
Table 60: Ticket Types *(Continued)*

Type	Description
Problem	Select this ticket type if you need help with an outage, setting up a new site, or returning merchandise. Also select the impact in the second drop-down list.  Impact options include: • **Specific Devices Impacted**—The problem is limited to specific devices on the network. • **Partial Network Impacted**—The problem affects part but not all your network. • **New Site Bring Up**—The problem involves a new site that is not in production yet. • **RMA**—You want a Return Merchandise Authorization to return a Juniper device. • **Full Production Network Impacted**—The problem affects most or all of your network.
Onboarding Help for New Deployment	Select this ticket type only if you're doing a new deployment. You'll get assistance with initial setup, configuration, and basic troubleshooting. Available only when the **Technology Type** is wireless, switching, or SD-WAN. These services do not include network design. Enter the **Summary** and **Description**, and complete the **Checklist**. As you complete the checklist, you can use suggested hyperlinks for self-help. If you still need assistance after using the self-help suggestions, finalize your ticket by selecting your preferred time slot for the onboarding help session. Submit this ticket at least 48 hours in advance of the selected time.

5. In the remaining fields, provide the support team with full details about the issue.

TIP: For the Problem and Configuration Help ticket types, customers with a Marvis subscription will see Marvis buttons by the Impacted Sites, Impacted Devices, and Impacted Clients fields. Click a button to get assistance. Marvis can answer configuration questions and provide more details of issues with sites, devices, or clients. If you are able to resolve the issue with help from Marvis, you can cancel this support ticket by clicking **Cancel** at the top right corner of the New Ticket page.

Example



The following table provides more information.

Table 61: Field Descriptions

Field	Ticket Types	Tips
Ticket Summary	All ticket types	Enter a short description of the issue.
Description	All ticket types	Enter a detailed description of the issue.
CC	All ticket types	Enter the email addresses of any other people who you'd like to receive updates about this ticket. **NOTE**: When you're updating a ticket, this field is titled Additional Emails.
Schedule	Onboarding Help	Select the date and time of day for the onboarding help session. Be sure to submit your ticket at least 48 hours in advance.

Table 61: Field Descriptions *(Continued)*

Field	Ticket Types	Tips
Impacted Sites	Question Configuration Help Problem	• Add a site—Click **Add Site**, and then click the impacted site. If you have a long list of sites, you can search by entering the site name or the site group name. • Delete a site from the Impacted Sites list—Click the site, and then press the Delete key on your keyboard.
Impacted Devices *	Question Configuration Help Problem	• Add a device—Click **Add Device**, click a device type, and then click the impacted device. If you have a long list of devices, you can search by entering the device name or MAC address. • Delete a device from the Impacted Devices list—Click the device, and then press the Delete key on your keyboard.
Impacted Clients	Question Configuration Help Problem	• Add a client—Click **Add Client**, click a client type, and then click the impacted client. If you have a long list of clients, you can search by entering the client name or MAC address. • Delete a client from the Impacted Clients list—Click the client, and then press the Delete key on your keyboard.
Order Number	Subscriptions	Enter the order number for the subscription.

Table 61: Field Descriptions *(Continued)*

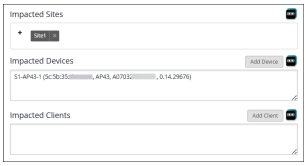
Field	Ticket Types	Tips
Time of Issue	Question Configuration Help Problem	Click in the box, and then use the calendar and time list to enter the time when the issue occurred.
Contact Number	Problem	Enter a phone number for the person that the support team can contact about this problem.
Juniper Account Team Name and Contact	Problem (Full Production Network issues only)	Enter the name and contact information for your Juniper Account representative. (Applicable only if you selected Full Production Network Impacted in the impact drop-down list.)

* When you list a device in the **Impacted Devices** field:

- The device automatically sends its system logs to Mist, enabling the support team to analyze the issue more effectively and respond faster.

  The device must be in a connected state for logs to be sent. If more than 10 devices are listed, log collection will be limited to the first 10 devices.

- The device model, serial number, and firmware version are included in addition to the device MAC address. If the firmware version is unavailable or if the device is disconnected, the version is displayed as "--".



6. Click **Submit Ticket**.

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

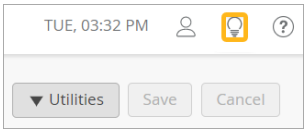
Feature Requests

SUMMARY

You can submit feature requests through the Juniper Mist™ portal. You also can view other users' requests and vote or comment on them.

IN THIS SECTION

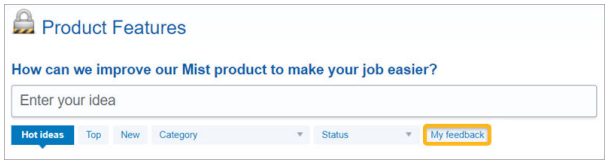
To go to the Product Features pages, click the lightbulb icon (near the top right corner of the Juniper Mist portal).



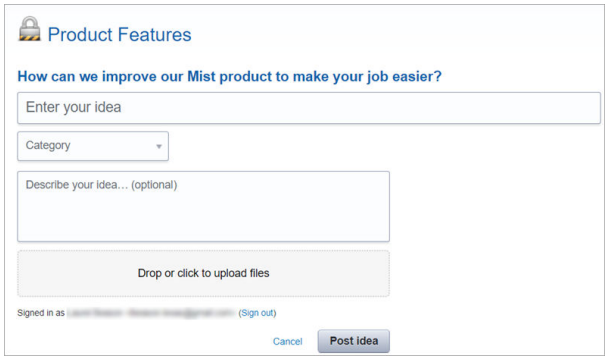
On this page, you can:

Submit a Feature Request

1. Type a short description of your idea in the **Enter your idea** text box.



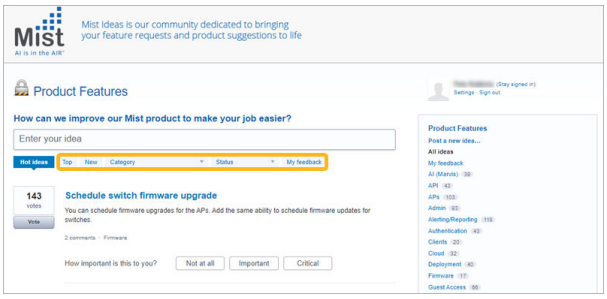
   As you type, Juniper Mist searches for similar ideas.
2. If similar requests appear, vote on them or click **Post a new idea** to go to the request form.
3. When the feedback form appears, enter details about your idea, and upload any files that you want to share.



4. Click **Post idea**.

View the Feature Requests

To view the feature requests that you are most interested in, use the buttons, drop-down lists, and category menu.



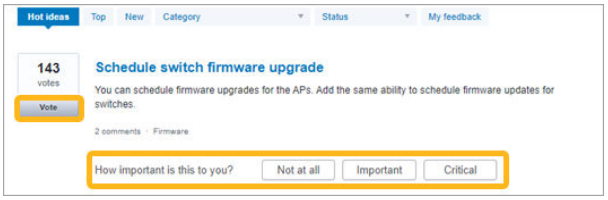
- Top—Sort the requests from the highest number of votes to the lowest number of votes.
- New

  —Sort the requests from the most recent submission to the least recent submission.
- Category—Filter the list based on the category that the user assigned when creating the request.

  TIP: Another way to filter by category is to use the category menu on the right side of the page.
- Status—Filter the list based on the current status.
- My feedback—View only the feature requests that you've supported or commented on.

Respond to Other Users' Feature Requests

You can respond to the feature requests that other users submitted.



- To vote in favor of a request, click **Vote** on the left side of the page.
- To rate the importance of a request, click the appropriate button: **Not at all**, **Important**, **Critical**.
- To add a comment, click the title of the request, then type in the **Add a comment** text box, and then click **Post comment**.

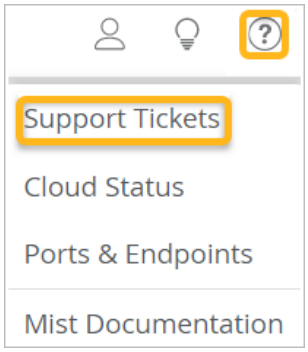
View Your Support Tickets

SUMMARY

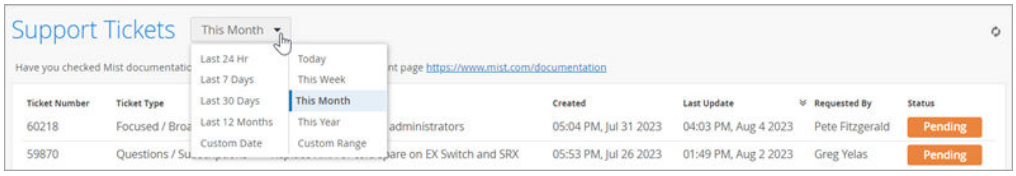
Follow these steps to go to your support dashboard and view the status of your tickets.

You can view your support tickets from the Juniper Mist™ portal.

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



2. (Optional) Select the time period.



3. Click the ticket that you want to view.

Find Information and Instructions for Juniper Mist

SUMMARY

Get familiar with the various help features of the Juniper Mist portal.

In the Juniper Mist™ portal, use these features to find information and instructions:

- Resource Center—Click the book icon (at the lower-left corner of the portal) to open the Resource Center.

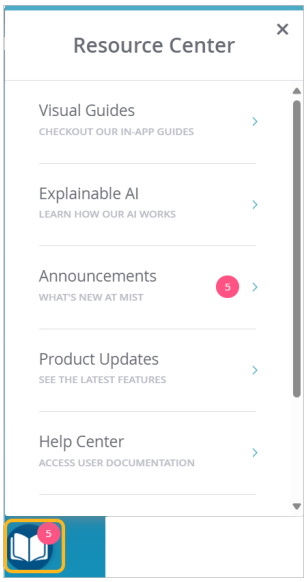


Table 62: Features of the Resource Center

Feature	Description
Visual Guides	Click-through demos that introduce various features
Explainable AI	Essential concepts presented in whiteboard videos
Announcements	Information about new features, security advisories, and more
Help Center	Juniper Mist help topics
Product Updates	Juniper Mist release notes

- Support Tickets and Documentation menu—Click the question icon (at the top-right corner of the portal) and then select a menu option.

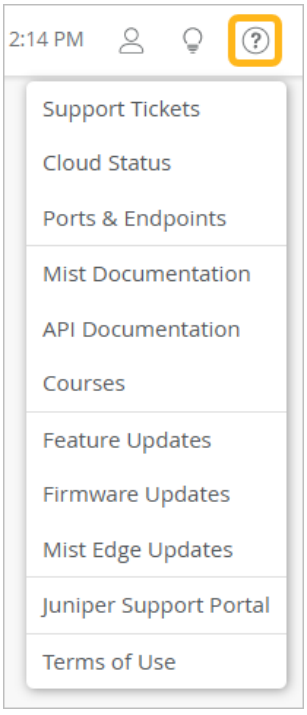


Table 63: Options on the Support Tickets and Documentation Menu

Feature	Description
Support Tickets	Create and view support tickets for your Juniper Mist organization.
Cloud Status	Check the current status of the Mist cloud for your region.
Ports & Endpoints	Get help about which ports and IP addresses to allow for your cloud instance.
Mist Documentation	Browse Juniper Mist help topics.
API Documentation	View developer documentation.
Courses	View the available training courses at Mist.com.
Feature Updates	Release notes for Juniper Mist
Firmware Updates	Learn about Juniper Mist product updates.
Mist Edge Updates	Learn about Mist Edge product updates.
Juniper Support Portal	Go to the support portal, where you can log in to view information, support cases, and more for your Juniper devices.
Terms of Use	End User License Agreement