Engineering
Simplicity

Juniper Mist Management Guide

Published
2025-01-09

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

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

Juniper Mist 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 Get Started

Mist Configuration Hierarchy | 2

Admin Menu Overview | 3

Initial Configuration Tasks | 4

Create Your Account and Organization | 6

Account Settings and Preferences | 7

Account Settings | 7

Find the My Account Page | 8

Change Your Contact Information | 8

Change Your Password | 8

Enable Two-Factor Authentication for Your Account | 8

Select the MAC Address Format | 9

Set the Time Format | 9

Create a User Token | 10

Receive Notifications of Events and Alerts | 11

Adjust Privacy Settings | 12

Remove Your Account | 12

Select Your Preferred Language (Beta) | 13

2 Security and Access

Security Options | 15

Juniper Mist Clouds | 15

Juniper Mist Firewall Ports and IP Addresses for Firewall Configuration | 17

Add Accounts for Portal Users | 32

Portal User Roles | 33

Revoke a User's Access | 34

User Privileges | 35

Enable or Disable Juniper Mist Support Access | 35

Single Sign-On for the Juniper Mist Portal | 36

Requirements | 37

Multiple Identity Providers | 37

Local User Accounts | 37

Add Identity Providers and Users | 38

Create Custom Roles for Single Sign-On Access | 41

Obtain Juniper Mist Metadata for SAML 2.0 Integration | 43

Find Your Organization ID | 43

Determine Your API Endpoint | 43

Find Your SSO ID | 44

Issue an API Call to Get the Metadata | 44

Troubleshoot Issues with Identity Provider Setup | 44

Viewing Errors from the API | 45

Error: Invalid Certificate | 45

First-Time Login Issues | 46

Error: Email Already Taken | 46

Missing User Names | 47

Monitor SSO Logins | 47

Frequently Asked Questions for SSO | 48

Manage Certificates | 55

Monitor Administrator Activities (Audit Logs) | 56

Overview | 56

Find the Audit Logs Page | 56

Select the Time Period | 56

Filter by Users | 58

Filter by Sites | 59

Filter by Users' Tasks | 60

View Details | 60

Reset the Page to the Defaults | 60

Security Alerts and Advisories | 61

Additional Information About Security | 61

3 Your Organization

Organization Settings (Page Reference) | 64

Find Your Organization ID | 68

Rename an Organization | 69

Delete an Organization | 69

Set a Password Policy for Your Organization | 70

Configure Session Policies | 71

Integrate Your Juniper Support Account with Juniper Mist | 71

Access Apstra Cloud Services | 72

Add Routing Assurance to the Mist Portal | 74

4 Subscriptions and Orders

Juniper Mist Subscriptions | 78

Subscription Types for Juniper Mist | 79

Wireless Assurance | 80

Wired Assurance | 83

WAN Assurance | 98

Access Assurance | 108

Marvis | 110

Location Services | 114

Premium Analytics | 115

Juniper Mist Subscriptions Scope | 116

Activate a Subscription | 120

Renew a Subscription | 120

Subscription Status | 122

Monitor Your Orders | 123

Juniper Mist Subscriptions FAQ | 124

5 Device Management

View and Update Your Device Inventory | 131

View Juniper Support Insights (JSI) for Your Installed Base | **133**

Overview of the Installed Base Page | **134**

Top-of-Page Information | **134**

Find a Device by Using Filters | **135**

Adjust the Columns in the Table Settings | **135**

Field Descriptions on the Installed Base Page | **136**

Device Details | **137**

Device Details for Installed Base | **138**

Auto-Provisioning | 147

Automatically Assign Devices to Sites | **148**

Automatically Assign Device Names | **151**

Automatically Assign Device Profiles to Access Points | **153**

Manipulate Source Strings for Auto-Provisioning | **155**

Divide a String into Segments | **156**

Ignore Starting or Ending Characters | **157**

Select the First Characters | **157**

Add a Prefix or Suffix | **158**

Using Multiple Transformation Options Together | **159**

Claim a Switch | 160

Adopt a Switch from Your Juniper Installed Base | 162

Claim a WAN Edge | 162

Adopt a WAN Edge from Your Juniper Installed Base | 163

Rename Devices | 163

Device Management with the Juniper Mist AI Mobile App | 164

6 Sites

Configure a Site | 170

Site Configuration Settings (Page Reference) | 171

Set the Site Location | 179

Site Groups | 180

Assign, Unassign, and Manage Site Groups | 181

Set the Engagement Dwell Limits and Schedule for a Site | 182

Set Up Occupancy Analytics for a Site | 183

Configure Site Variables | 185

7 Help and Support

Create a Support Ticket | 189

Feature Requests | 194

Submit a Feature Request | 195

View the Feature Requests | 196

Respond to Other Users' Feature Requests | 197

View Your Support Tickets | 197

Find Information and Instructions for Juniper Mist | 198

1

CHAPTER

Get Started

Mist Configuration Hierarchy | 2

Admin Menu Overview | 3

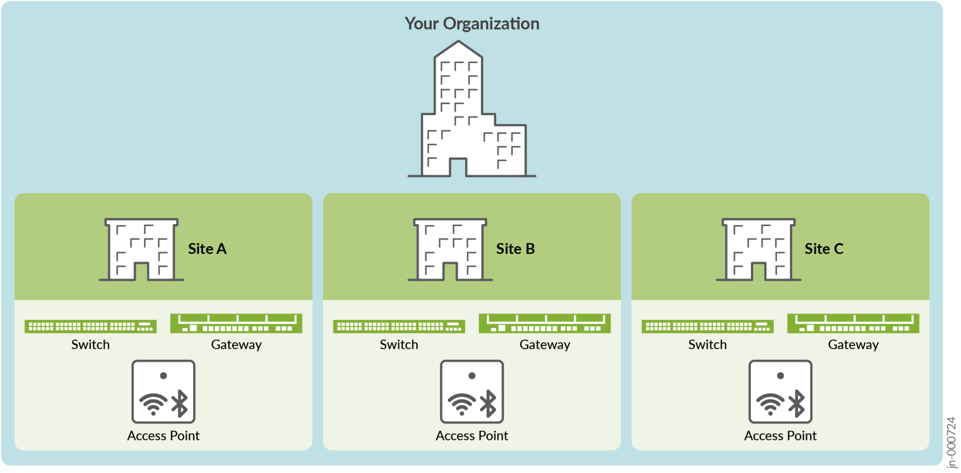
Initial Configuration Tasks | 4

Create Your Account and Organization | 6

Account Settings and Preferences | 7

Mist Configuration Hierarchy

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 avaiable. 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.

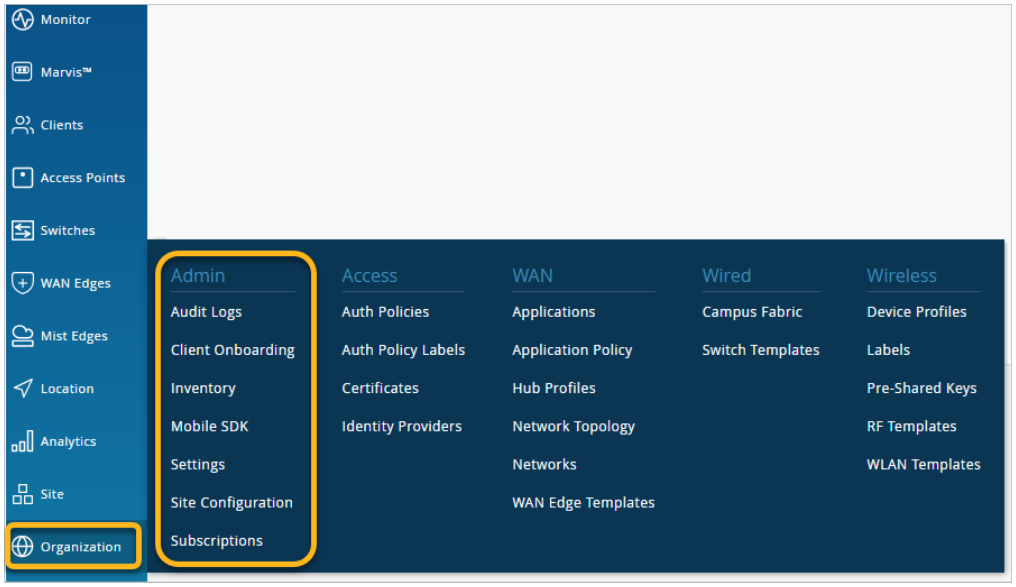
- Wired Assurance—You can use switch templates to set up the same configurations across multiple sites. The template provides the common settings that you want to apply to all the switches. You can then make site-specific or device-specific modifications to cover the devices that need uncommon settings.

- 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

This guide covers the tasks that you can complete by using the Admin menu.

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



The Admin menu includes these 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 33.

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 17

Table 1: Process Overview *(Continued)*

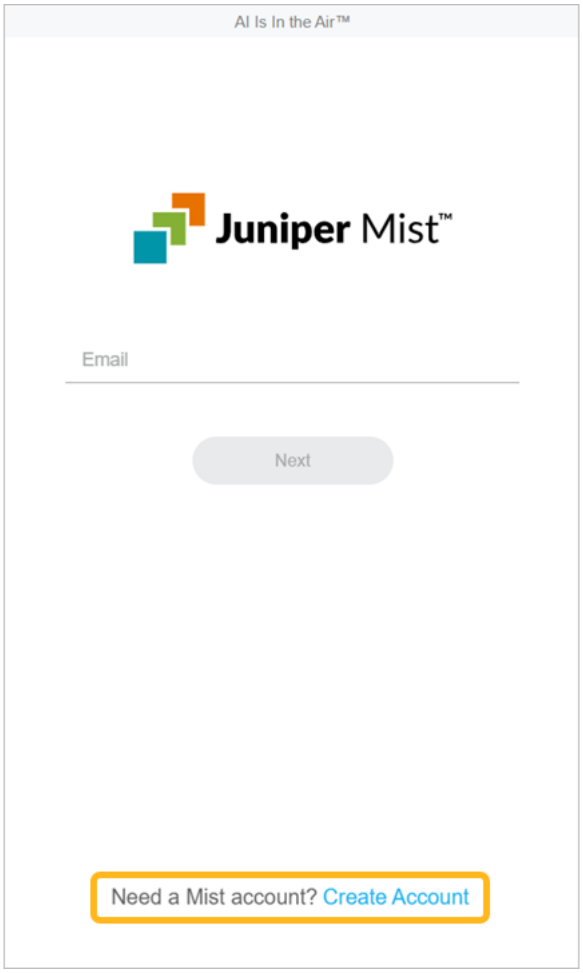
Step	Task	More Information
4	Set up your sites.	"Configure a Site" on page 170
5	Set up local user accounts or enable Single Sign-On.	• "Add Accounts for Portal Users" on page 32 • "Single Sign-On for the Juniper Mist Portal" on page 36
6	Activate your subscriptions.	"Activate a Subscription" on page 120
7	Claim and adopt devices.	• "View and Update Your Device Inventory" on page 131 • "Integrate Your Juniper Support Account with Juniper Mist" on page 71 • "View Juniper Support Insights (JSI) for Your Installed Base" on page 133
8	Configure other settings to meet your business needs.	• "Organization Settings (Page Reference)" on page 64 • "Site Configuration Settings (Page Reference)" on page 171 • "Security Options" on page 15 • "Additional Information About Security" on page 61

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

Create Your Account and 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 33.

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 15.

4. Follow the on-screen prompts to 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 69.

Account Settings and Preferences

IN THIS SECTION

- Account Settings | 7
- Select Your Preferred Language (Beta) | 13

Account Settings

SUMMARY

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

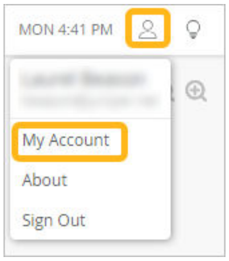
IN THIS SECTION

- Find the My Account Page | 8
- Change Your Contact Information | 8
- Change Your Password | 8

- Enable Two-Factor Authentication for Your Account | 8
- Select the MAC Address Format | 9
- Set the Time Format | 9
- Create a User Token | 10
- Receive Notifications of Events and Alerts | 11
- Adjust Privacy Settings | 12
- Remove Your Account | 12

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

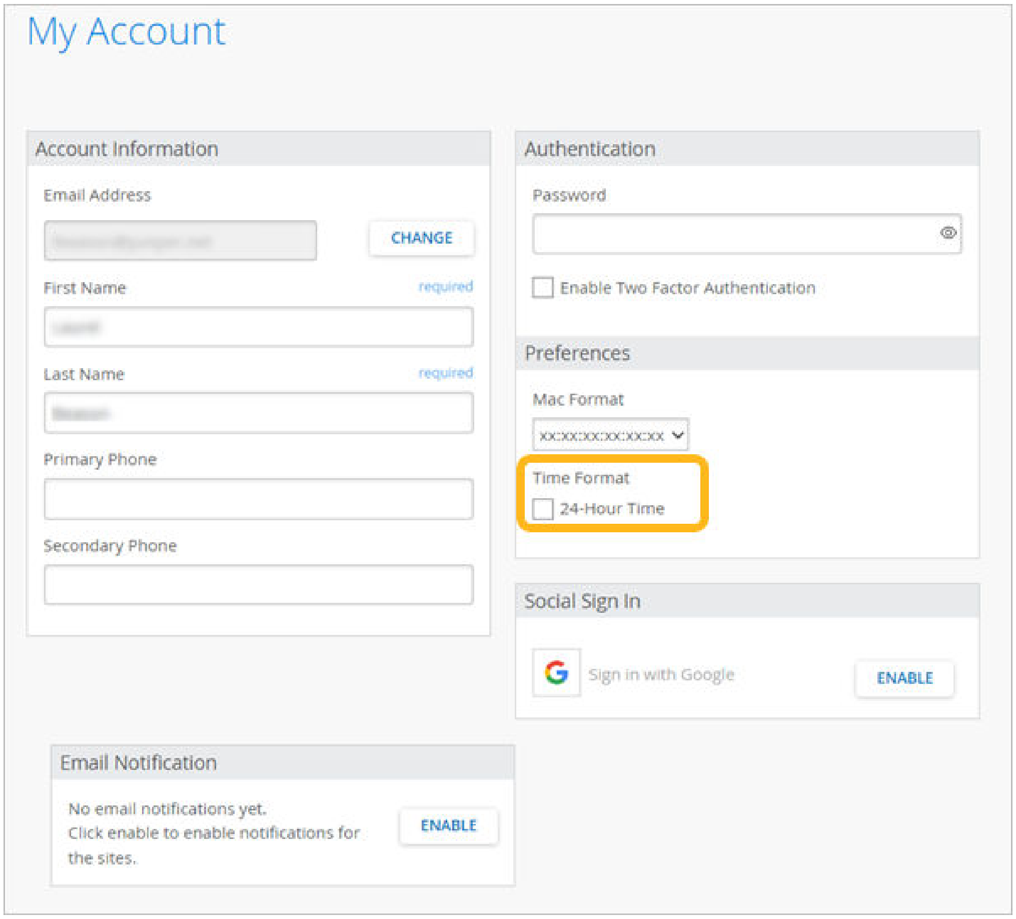
Choose how to display MAC addresses in the Juniper Mist portal.

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**.



My Account

Account Information

Email Address: [redacted]

First Name (required): [redacted]

Last Name (required): [redacted]

Primary Phone

Secondary Phone

Authentication

Password

□ Enable Two Factor Authentication

Preferences

Mac Format: xx:xx:xx:xx:xx:xx

Time Format

□ 24-Hour Time

Social Sign In

Sign in with Google

Email Notification

No email notifications yet. Click enable to enable notifications for the sites.

- 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

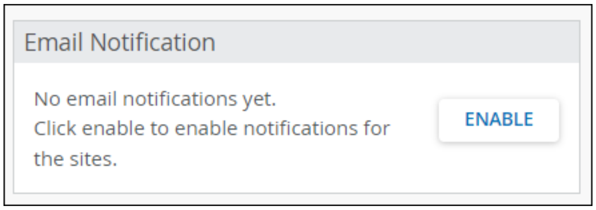
You can set up your Juniper Mist™ account so that you receive notifications of events and alerts. You can enable notifications for the entire organization or specific sites.

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:

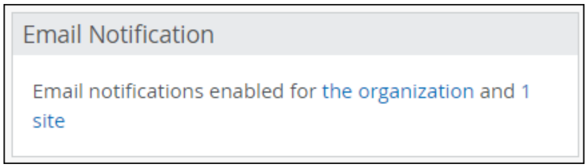
   - If no notifications are enabled, click **Enable** .



Email Notification

No email notifications yet.
Click enable to enable notifications for the sites.

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

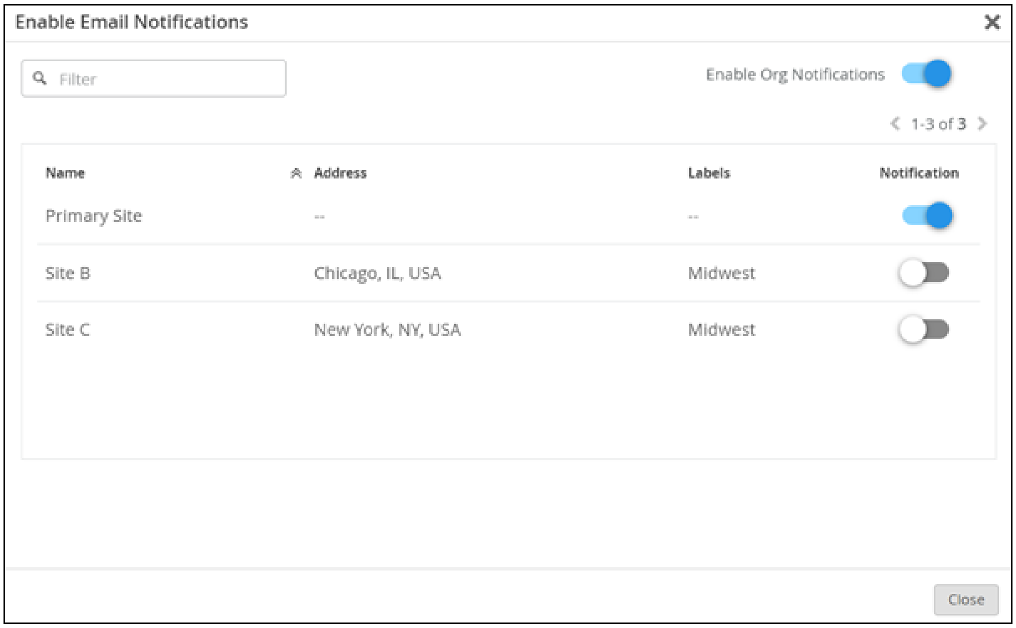


Email Notification

Email notifications enabled for the organization and 1 site

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.



Enable Email Notifications

Enable Org Notifications ●

Name	Address	Labels	Notification
Primary Site	--	--	●
Site B	Chicago, IL, USA	Midwest	○
Site C	New York, NY, USA	Midwest	○

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.

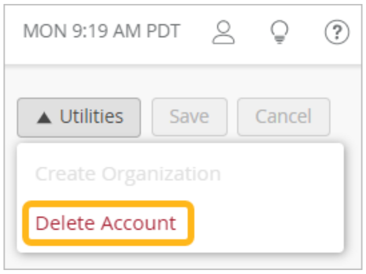
> **NOTE**: Users also are prompted about privacy options when creating an account. If users created their account before the privacy options were implemented, they'll see a message when they log in.

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**.

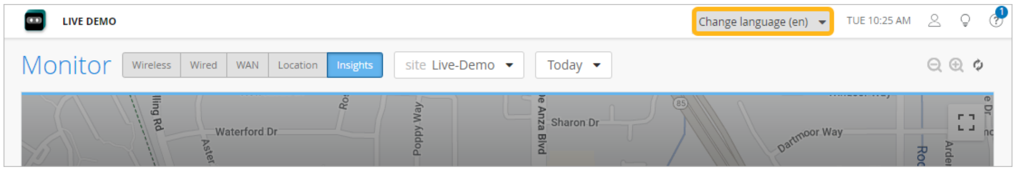


3. Read the confirmation message, and then click **Delete** to remove your account.

Select Your Preferred Language (Beta)

You can select the language that you prefer to see in the Juniper Mist™ portal. This affects only your view of the portal, not the settings for other portal users.

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

Security Options | 15

Juniper Mist Clouds | 15

Juniper Mist Firewall Ports and IP Addresses for Firewall Configuration | 17

Add Accounts for Portal Users | 32

Enable or Disable Juniper Mist Support Access | 35

Single Sign-On for the Juniper Mist Portal | 36

Manage Certificates | 55

Monitor Administrator Activities (Audit Logs) | 56

Security Alerts and Advisories | 61

Additional Information About Security | 61

Security Options

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.

Juniper Mist Clouds

IN THIS SECTION

- Regional Clouds | **15**
- Regions and Hosting Countries | **16**

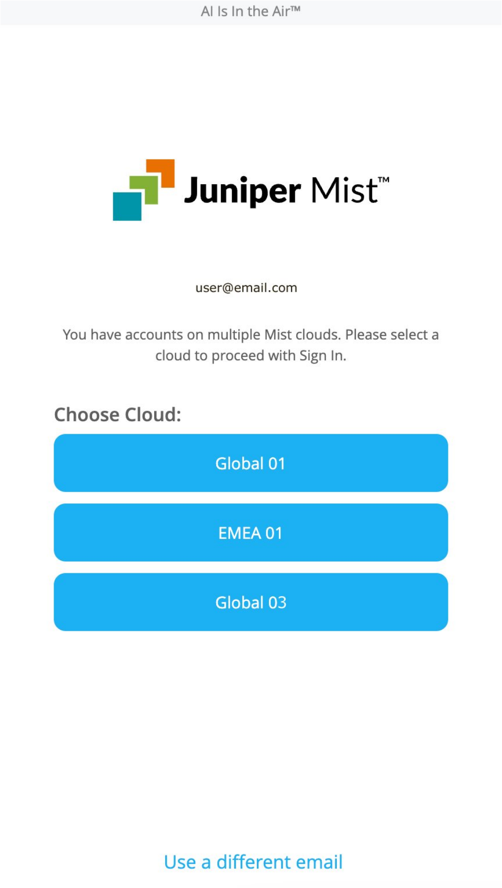
Regional Clouds

The Juniper Mist™ environment uses regional clouds and accounts for optimal performance. When creating an organization, you should use the region nearest to you. For North American users, Global 03 is the current default environment, and all new organizations are created there.

Note that 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 that you have organizations in. Users with multiple accounts can reuse the same email ID across the different clouds whether it’s a local email, SSO, or mix between the environments.

If you already have organizations in Global 01 and do not want to use Global 03 for new organizations, you can contact support at support@mist.com for assistance.

Figure 1: Multiple Accounts



AI Is In the Air™

user@email.com

You have accounts on multiple Mist clouds. Please select a cloud to proceed with Sign In.

Choose Cloud:

Regions and Hosting Countries

Table 3: Cloud Instances

Region	Cloud Instance	Hosting Country
GLOBAL	Global 01	Americas
	Global 02	Americas
	Global 03	Americas
	USGov 01	Americas

Table 3: Cloud Instances *(Continued)*

Region	Cloud Instance	Hosting Country
	Global 04	Canada
EMEA	EMEA 01	Germany
	EMEA 02	England
	EMEA 03	United Arab Emirates
APAC	APAC 01	Australia

RELATED DOCUMENTATION

Juniper Mist Firewall Ports and IP Addresses for Firewall Configuration | 17

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

IN THIS SECTION

- How To Use This Information | 18
- Global 01 | 19
- Global 02 | 20

- Global 03 | 22
- Global 04 | 23
- EMEA 01 | 25
- EMEA 02 | 27
- EMEA 03 | 28
- APAC 01 | 30
- Additional Information | 31

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 15.
- 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 Information" on page 31 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.

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
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)

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

Cloud Service or Device Type	IP Addresses and Ports
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.mist.com (TCP 443) oc-term.mistsys.net (TCP 2200) 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)

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

Cloud Service or Device	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) 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)
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.gc1.mist.com (TCP 443) oc-term.gc1.mist.com (TCP 2200) 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)
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)

Table 6: Global 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.ac2.mist.com (TCP 443) oc-term.ac2.mist.com (TCP 2200) srx-log-terminator.ac2.mist.com (TCP 6514)
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)

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

Cloud Service or Device	IP Addresses and Ports
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
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)
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.gc2.mist.com (TCP 443) oc-term.gc2.mist.com (TCP 2200) srx-log-terminator.gc2.mist.com (TCP 6514)

Table 7: Global 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.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)

EMEA 01

Table 8: 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)
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

Table 8: EMEA 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.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)
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.eu.mist.com (TCP 443) oc-term.eu.mist.com (TCP 2200) srx-log-terminator.eu.mist.com (TCP 6514)
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 9: 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
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)
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.gc3.mist.com (TCP 443) oc-term.gc3.mist.com (TCP 2200) srx-log-terminator.gc3.mist.com (TCP 6514)

Table 9: EMEA 02 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.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 10: 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

Table 10: EMEA 03 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.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)
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.ac6.mist.com (TCP 443) oc-term.ac6.mist.com (TCP 2200) 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)

APAC 01

Table 11: 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
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)

Table 11: APAC 01 IP Addresses and Ports to Allow *(Continued)*

Cloud Service or Device	IP Addresses and Ports
SRX Series Firewalls	redirect.juniper.net (TCP 443) ztp.ac5.mist.com (TCP 443) oc-term.ac5.mist.com (TCP 2200) 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)

Additional Information

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).

- 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.
- We also recommend opening UDP port 443 and TCP port 80.
- 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.

Additional Information for Wired and WAN Assurance

For Wired and WAN Assurance, allow **radsec.nac.mist.com** (TCP 2083).

For Access Assurance for customers in the European Union (EU), allow **radsec-eu.nac.mist.com**(TCP 2083).

NOTE: IP addresses for the terminators will change. Use FQDN-based firewall rules.

Add Accounts for Portal Users

IN THIS SECTION

- Portal User Roles | 33
- Revoke a User's Access | 34
- User Privileges | 35

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

Table 12: Roles

Role	Description
Super User	Full access to all sites; can create new sites and manage other administrators
Network Admin	Full access to selected sites
Observer	Limited access; can monitor selected sites

Table 12: Roles *(Continued)*

Role	Description
Installer	Limited access; can install access points (APs) and switches • Can do the initial installation such as claim APs, assign/unassign an AP, and place an AP on the floorplan. • Cannot unclaim or remove an AP from the organization • Can use the API and the Juniper Mist™ AI app. Cannot access the portal. • Access is allowed for a specified grace period. You can use the Organization Settings page to set the grace period.
Helpdesk	Limited access; can monitor selected sites
Switch Port Operator	Limited access; can view and manage switch port configurations that are allowed by a Super User
Super Observer	Limited access; can monitor all sites and can view organization pages

Revoke a User's Access

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 granted privilege applies.

For example, if a user is granted 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 explicitly granted 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.

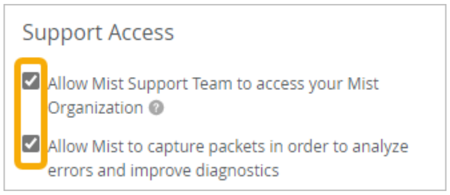
Enable or Disable Juniper Mist Support Access

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.

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



Support Access

☑ Allow Mist Support Team to access your Mist Organization

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

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

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

- Requirements | 37
- Multiple Identity Providers | 37
- Local User Accounts | 37
- Add Identity Providers and Users | 38
- Create Custom Roles for Single Sign-On Access | 41
- Obtain Juniper Mist Metadata for SAML 2.0 Integration | 43
- Troubleshoot Issues with Identity Provider Setup | 44
- Monitor SSO Logins | 47
- Frequently Asked Questions for SSO | 48

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 38.
  - 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 41.

    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.

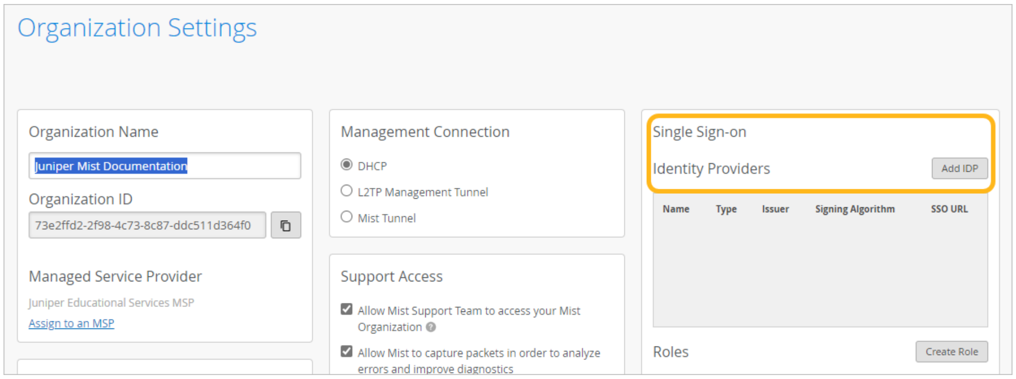
Add Identity Providers and Users

To set up single sign-on (SSO) for the Juniper Mist™ portal, add the identity providers (IdPs) that you want to use to authenticate portal users. When finished, follow the instructions to create custom roles, delete unneeded local accounts, and provide 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**.



Organization Settings

Organization Name: Juniper Mist Documentation

Organization ID: 73e2ffd2-2f98-4c73-8c87-ddc511d364f0

Managed Service Provider: Juniper Educational Services MSP

Management Connection

● DHCP
○ L2TP Management Tunnel
○ Mist Tunnel

Support Access

☑ Allow Mist Support Team to access your Mist Organization
☑ Allow Mist to capture packets in order to analyze errors and improve diagnostics

Single Sign-on

Identity Providers

Name	Type	Issuer	Signing Algorithm	SSO URL

Roles

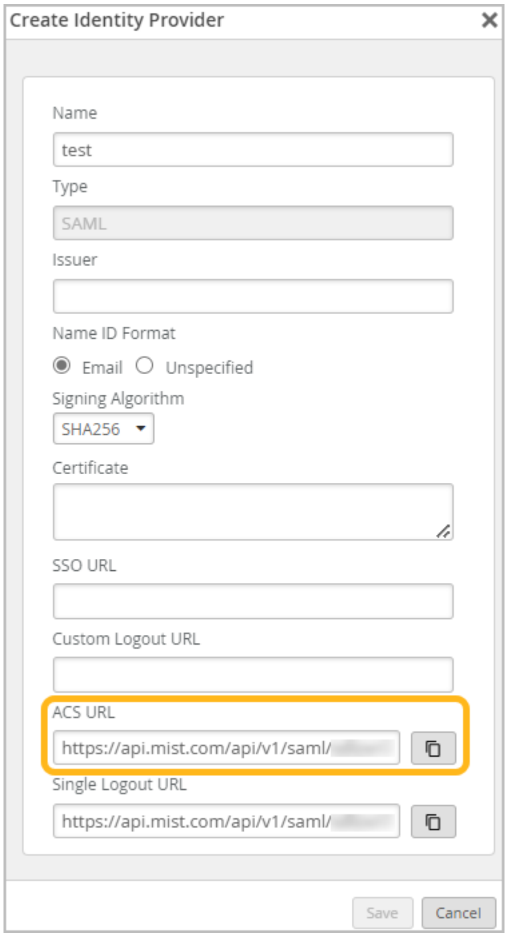
3. In the Create Identity Provider window:

   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.



Create Identity Provider

Name: test

Type: SAML

Issuer:

Name ID Format: ● Email ○ Unspecified

Signing Algorithm: SHA256

Certificate:

SSO URL:

Custom Logout URL:

ACS URL: https://api.mist.com/api/v1/saml/[redacted]

Single Logout URL: https://api.mist.com/api/v1/saml/[redacted]

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 intregation 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 43.

- 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.

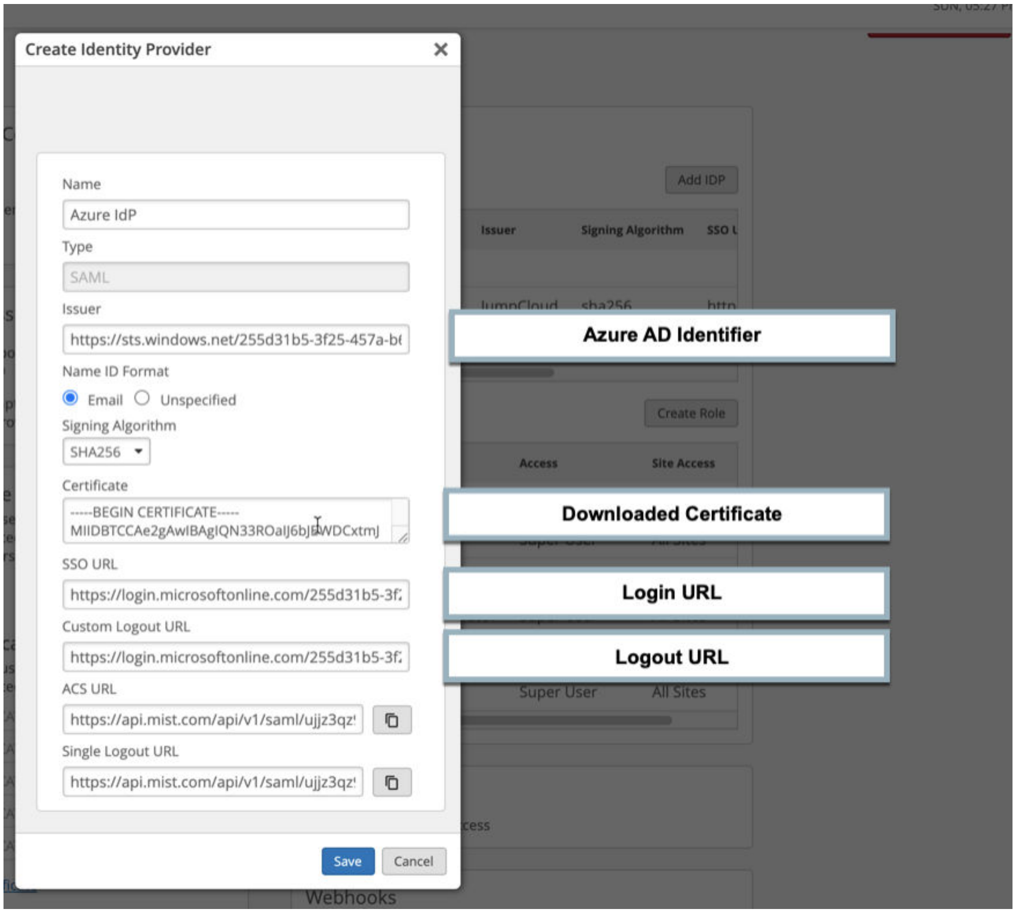
   - **Issuer**

   - **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.



Create Identity Provider ✕

Name: Azure IdP

Type: SAML

Issuer: https://sts.windows.net/255d31b5-3f25-457a-b

Name ID Format: ● Email ○ Unspecified

Signing Algorithm: SHA256

Certificate: -----BEGIN CERTIFICATE----- MIIDBTCCAe2gAwIBAgIQN33ROalJ6bJ8WDCxtmJ

SSO URL: https://login.microsoftonline.com/255d31b5-3f2

Custom Logout URL: https://login.microsoftonline.com/255d31b5-3f2

ACS URL: https://api.mist.com/api/v1/saml/ujjz3qz

Single Logout URL: https://api.mist.com/api/v1/saml/ujjz3qz

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 41.

- **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 34.

  - As an admin, anyone can change the email address that they use for their Mist account. See "Account Settings" on page 7.

- **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).

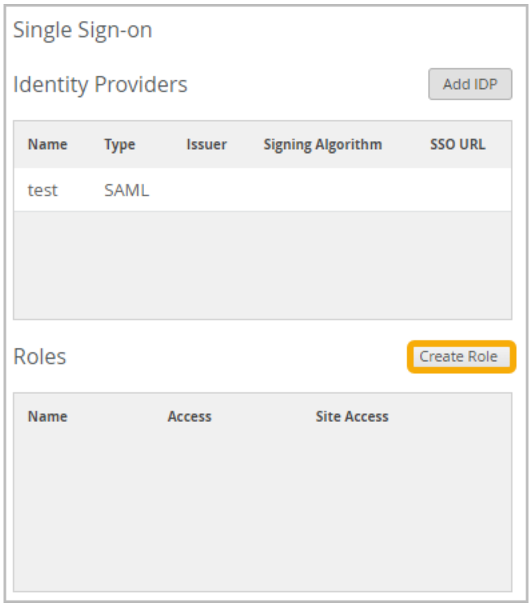
If errors occur, see "Troubleshoot Issues with Identity Provider Setup" on page 44.

Create Custom Roles for Single Sign-On Access

When you configureg 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**.



Name	Type	Issuer	Signing Algorithm	SSO URL
test	SAML			

Name	Access	Site Access

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

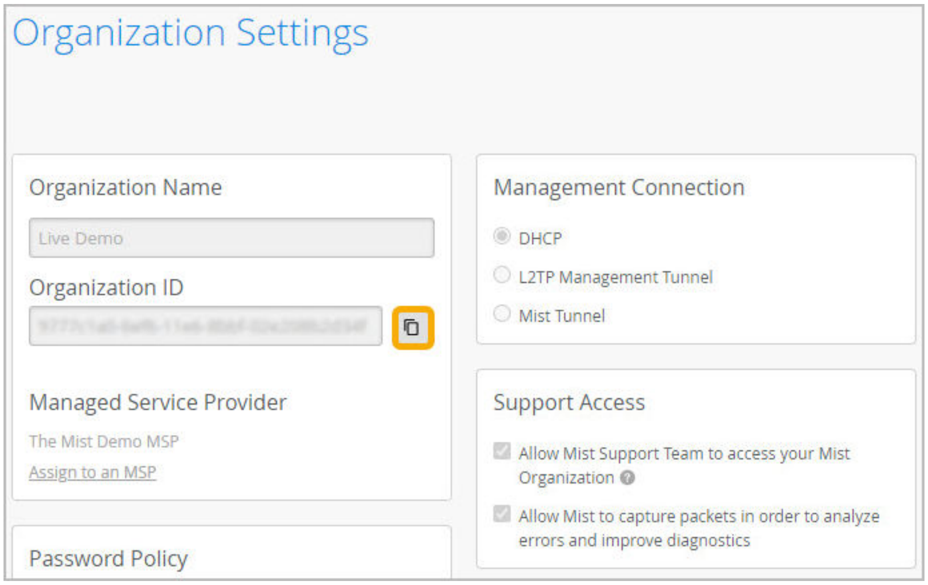
When you set up a SAML 2.0 integration for Juniper Mist™, your Identity Provider (IdP) might require metadata. You can get the metadata from Juniper Mist by issuing an API call. But first you need to find your organization ID, API endpoint, and SSO ID.

IN THIS SECTION

- Find Your Organization ID | 43
- Determine Your API Endpoint | 43
- Find Your SSO ID | 44
- Issue an API Call to Get the Metadata | 44

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.



Organization Settings

Organization Name

Live Demo

Organization ID

[redacted]

Managed Service Provider

The Mist Demo MSP

Assign to an MSP

Password Policy

Management Connection

● DHCP

○ L2TP Management Tunnel

○ Mist Tunnel

Support Access

☑ Allow Mist Support Team to access your Mist Organization

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

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

- Viewing Errors from the API | **45**
- Error: Invalid Certificate | **45**
- First-Time Login Issues | **46**

- Error: Email Already Taken | 46
- Missing User Names | 47

NOTE: If you are just getting started with identity provider setup, see "Add Identity Providers and Users" on page 38.

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 | 45
- Cause | 45
- Solution | 45

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 | 46
- Cause | 46
- Solution | 46

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 | 46
- Solution | 47

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 | 47
- Cause | 47
- Solution | 47

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

IN THIS SECTION

- Q: What are the basics of Mist's SSO implementation I should know? | 48
- Q: What IdPs does Mist Support for SSO Access? | 49
- Q: Does Mist support SP and IdP initiated SSO? | 49
- Q: What attributes do I need to send in my assertion? | 49
- Q: What NameID formats do you support | 49
- Q: What is Role used for? | 49
- Q: Can I return multiple roles for a user? | 50
- Q: How can I troubleshoot SSO failures? | 51
- Q: Do I need to manually provision my SSO users within Mist? | 52
- Q: What is the first-time login process for my SSO users? | 52
- Q: How do I know which SSO users have accessed my Org? | 52
- Q: Does Mist have a metadata file? | 53
- Q: I need multiple SSOs in my Org. Does Mist Support that? | 54
- Q: I have multiple organizations, can I use SSO with multiple Orgs? | 54
- Q: What happens when I delete an SSO within Mist? | 54
- Q: How do API tokens work with SSO users? | 54
- Q: Do I need a local user within Mist? | 54

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 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 38.

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.

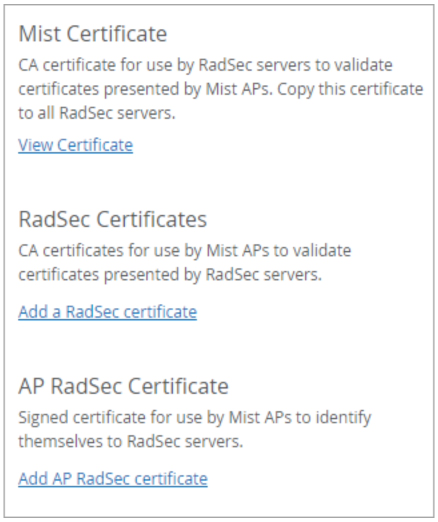
Q: Do I need a local user within Mist?

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 38.

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.

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



Mist Certificate

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

View Certificate

RadSec Certificates

CA certificates for use by Mist APs to validate certificates presented by RadSec servers.

Add a RadSec certificate

AP RadSec Certificate

Signed certificate for use by Mist APs to identify themselves to RadSec servers.

Add AP RadSec certificate

3. Obtain or add certificates:

   - 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 | 56
- Find the Audit Logs Page | 56
- Select the Time Period | 56
- Filter by Users | 58
- Filter by Sites | 59
- Filter by Users' Tasks | 60
- View Details | 60
- Reset the Page to the Defaults | 60

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.

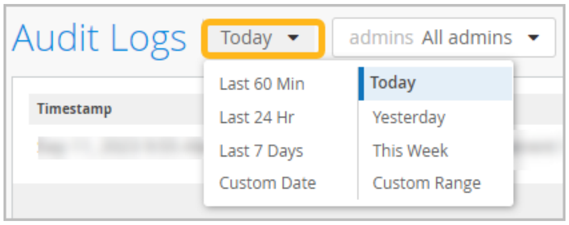
When you first open this page, it shows all logins for all users and all sites on the current date. You can use the drop-down lists at the top of the page to select the time period, filter by users, filter by sites, or search for certain types of activities.

Find the Audit Logs Page

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

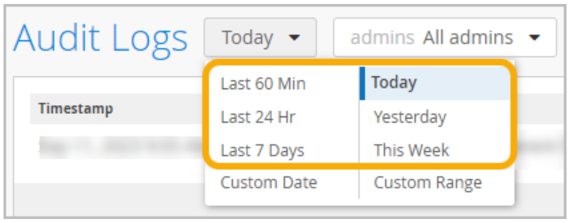
Select the Time Period

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



Select preset times and days, select a date, or enter a range of dates.

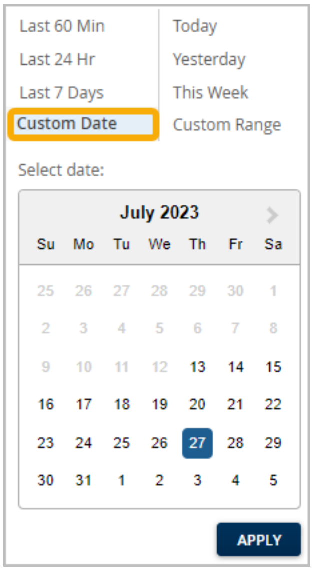
- Preset Times and Days

  - 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.

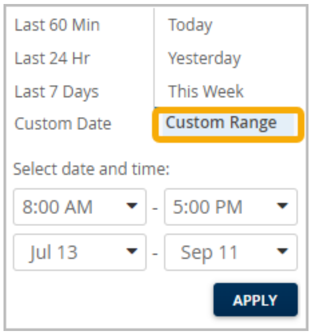
- Custom Date—Select a date within the past 60 days. The Audit Logs page will show all logins from midnight to 11:59 PM on the selected date.

  Custom Date Example



- Custom Range—Specify a range of dates within the past 60 days. On the left, enter the start time and date. On the right, enter the end time and date.

  Custom Range Example



Select date and time:

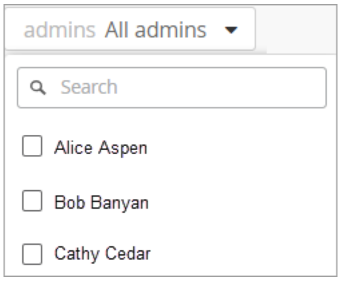
8:00 AM - 5:00 PM

Jul 13 - Sep 11

Filter by Users

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

   Example


admins All admins

Search

□ Alice Aspen

□ Bob Banyan

□ Cathy Cedar

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

IN THIS SECTION

- Configuring Other Security Settings | 61
- Additional Security Information | 62

Configuring Other Security Settings

See the following guides for additional security-related information:

- Juniper Mist Wireless Assurance Configuration Guide—This 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.

- Juniper Mist Wired Assurance Configuration Guide—This 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 WAN Assurance Configuration Guide

  —This 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 AI-Native Operations Guide—This 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—This guide covers various options for automation and integration, including security procedures such as configuring an API token, and monitoring security alerts with webhooks.

Additional Security Information

Use these links to access additional information about Juniper Mist security, data privacy, services, and licensing.

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

- 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

3

CHAPTER

Your Organization

Organization Settings (Page Reference) | 64

Find Your Organization ID | 68

Rename an Organization | 69

Delete an Organization | 69

Set a Password Policy for Your Organization | 70

Configure Session Policies | 71

Integrate Your Juniper Support Account with Juniper Mist | 71

Access Apstra Cloud Services | 72

Add Routing Assurance to the Mist Portal | 74

Organization Settings (Page Reference)

IN THIS SECTION

- Finding the Organization Settings Page | 64
- Major Sections of the Organization Settings Page | 64

Finding the Organization Settings Page

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

Major Sections of the Organization Settings Page

Table 13: Organization Settings

Section	Description	More Information
Name, ID, and Managed Service Provider	Basic information about the organization.	
Password Policy	You can specify password length, special characters, and 2-factor authentication.	"Set a Password Policy for Your Organization" on page 70
Session Policy	Set the maximum session length and the maximum idle time for your portal users.	"Configure Session Policies" on page 71
Switch Management	You can enable or disable switch proxy.	

Table 13: Organization Settings *(Continued)*

Section	Description	More Information
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 147
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.	

Table 13: Organization Settings *(Continued)*

Section	Description	More Information
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 13: Organization Settings *(Continued)*

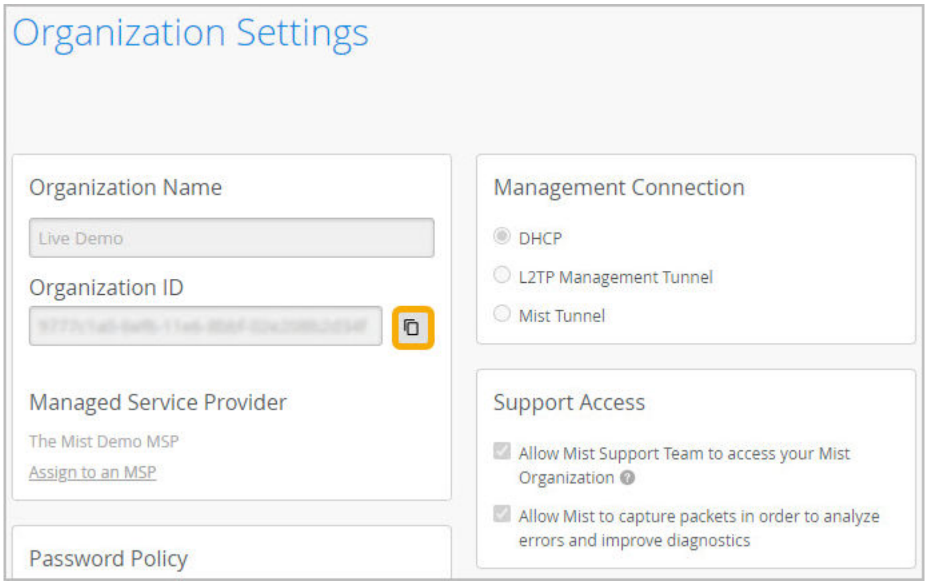
Section	Description	More Information
Management Connection	This setting determines how the APs handle management traffic. • DHCP (default option)—No special requirements for management traffic • L2TP Management Tunnel—Select this option when using static tunnels for secure data transfer between APs and 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 35
Certificates	Manage certificates for use with RadSec.	"Manage Certificates" on page 55
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 71
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 13: 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 36
Installer	Define the parameters for the Installer role.	"Portal User Roles" on page 33
Session Smart Conductor	Point to your Session Smart Conductor. You can enter up to two IP addresses, using a comma as a separator.	
Webhooks	Enable and configure webhooks to automatically send notifications of alerts and events as they occur.	Juniper Mist Automation Guide

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.



Organization Settings

Organization Name

Live Demo

Organization ID

[redacted]

Managed Service Provider

The Mist Demo MSP

Assign to an MSP

Password Policy

Management Connection

● DHCP

○ L2TP Management Tunnel

○ Mist Tunnel

Support Access

☑ Allow Mist Support Team to access your Mist Organization

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

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

Rename an Organization

1. From the left menu, select **Organization** > **Admin** > **Settings**.
2. Enter the new **Organization Name**.
3. Click **Save**.

Delete an Organization

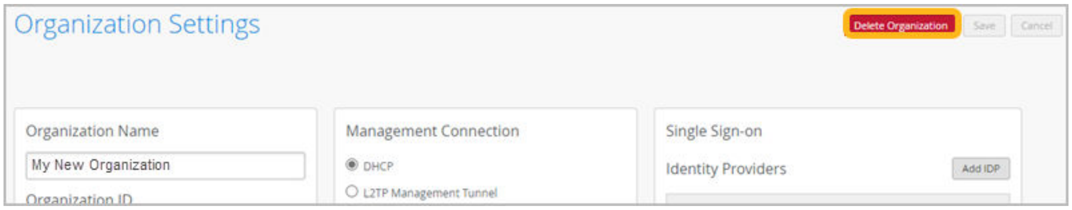
If you no longer need a certain organization in your Juniper Mist™ network, you can delete it. All sites, floorplans, and administrator accounts will be removed. This action is permanent, and the data is not recoverable.

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. Use the buttons at the top of the page to select a device type.

   c. Select all devices on the page, click **More**, and then click **Release**.

   d. Select the next device type, and continue until you have released all devices on all pages of the inventory.
3. From the left menu, select **Organization** > **Admin** > **Settings**.
4. Click **Delete Organization**.



Organization Settings

Organization Name: My New Organization

Organization ID

Management Connection: ● DHCP ○ L2TP Management Tunnel

Single Sign-on

Identity Providers

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

Set a Password Policy for Your Organization

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

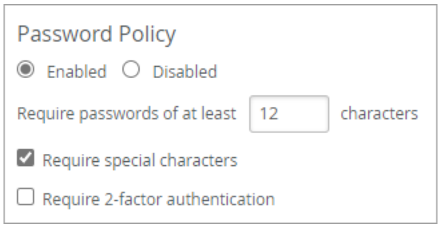
NOTE: Be sure to set the password policy to meet your organization's policy standard.

1. From the left menu, select **Organization** > **Admin** > **Settings**.
2. In the Password Policy section, select **Enabled**.
3. Enter the number of characters that you want to require.
4. (Optional) Enable additional settings:

   - **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.

   In this example, the password policy requires 12 characters, including special characters.

   Password Policy

   ● Enabled ○ Disabled

   Require passwords of at least 12 characters

   ☑ Require special characters

   □ Require 2-factor authentication

5. 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 7.

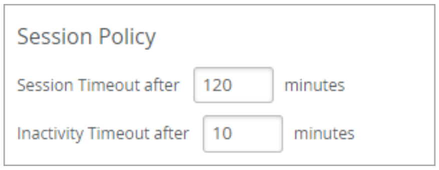
Configure Session Policies

To configure session policies, select **Organization** > **Settings** from the left menu of the Juniper Mist™ portal. Then enter your policy settings according to the following guidelines:

- **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.

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



Session Policy

Session Timeout after 120 minutes

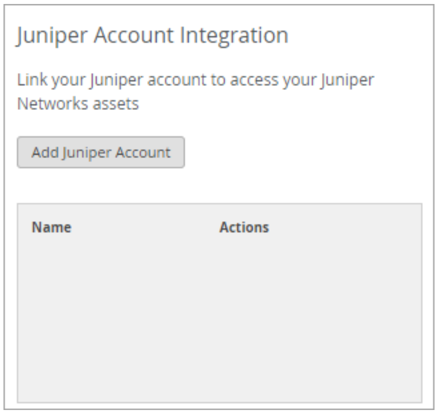
Inactivity Timeout after 10 minutes

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. From the left menu, select **Organization** > **Admin** > **Settings**.
2. Under Juniper Account Integration, click **Add Juniper Account**.



Juniper Account Integration

Link your Juniper account to access your Juniper Networks assets

Name	Actions

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

Juniper Mist validates the Juniper account and links it to your Juniper Mist organization. To view the insights, go to **Organization** > **Admin** > **Inventory**, and then click **Installed Base** at the top of the page.

Access Apstra Cloud Services

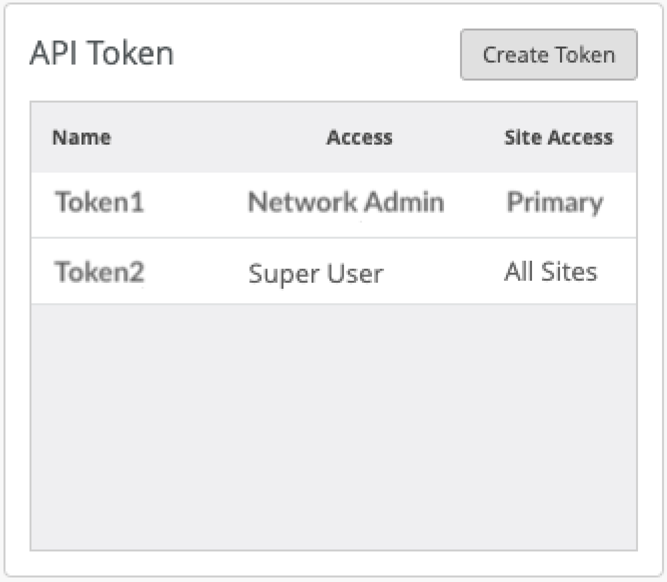
If you manage your enterprise network using Juniper Mist and your data center using Apstra, you can monitor data center events from Mist by linking the organization in Mist with the organization in Juniper Apstra Cloud Services. Once the organization are linked, you can see the total number of data center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

To link your Juniper Mist organization to your Juniper Apstra Cloud Services organization, you need the following information:

- Login credentials with superuser permissions for your Juniper Mist portal
- Login credentials with superuser permissions for your Juniper Apstra Cloud Services portal
- An API token generated in Juniper Apstra Cloud Services

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

1. Log in to Juniper Apstra Cloud Services.
2. In the API Token section of the Organization > Settings page, click **Create Token**.



API Token

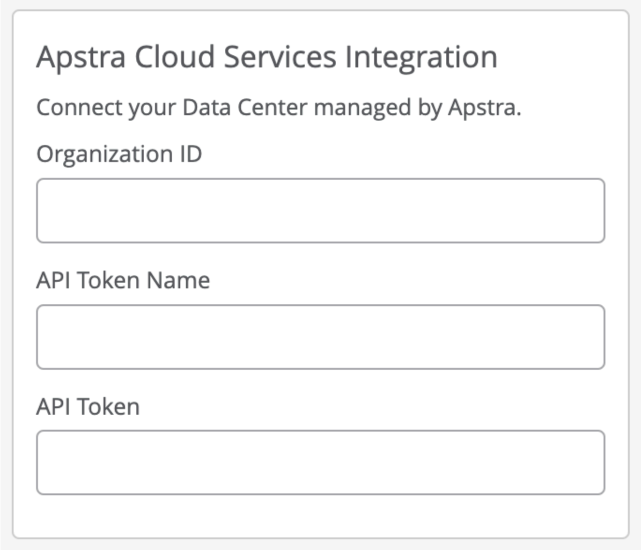
Create Token

Name	Access	Site Access
Token1	Network Admin	Primary
Token2	Super User	All Sites

3. Log in to your Juniper Mist portal.
4. Navigate to the **Organization** > **Settings** page.
5. Locate the Apstra Cloud Services Integration section.

   Enter the following information:

   - Organization ID—Copy the organization ID from Juniper Apstra Cloud Services and paste it here.
   - API Token Name—Enter API token name that you defined in Juniper Apstra Cloud Services.
   - API Token—Copy the API token generated in step 2 in Juniper Apstra Cloud Services and paste it here.



Apstra Cloud Services Integration

Connect your Data Center managed by Apstra.

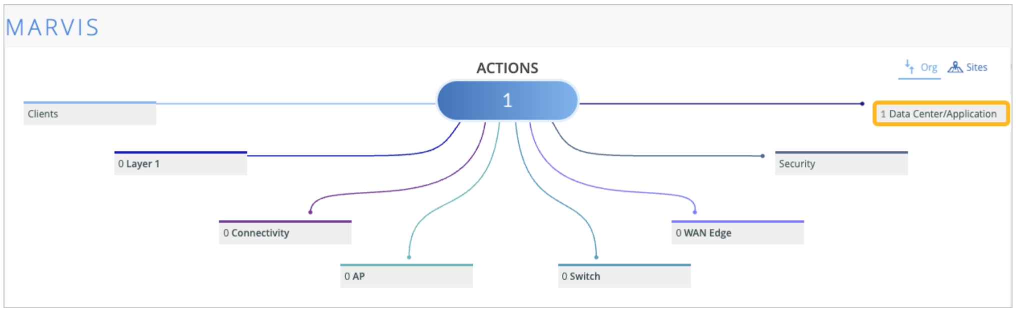
Organization ID

API Token Name

API Token

6. Click **Save**.

The organizations in Juniper Mist and Juniper Apstra Cloud Services 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

https://www.juniper.net/documentation/us/en/software/mist/mist-aiops/topics/concept/datacenter-actions.html

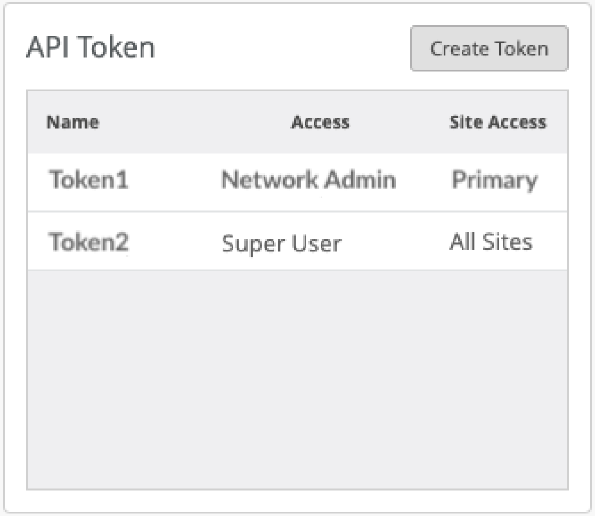
https://www.juniper.net/documentation/us/en/software/juniper-apstra-cloud-services/user-guide/topics/concept/datacenter-assurance-overview.html

Add Routing Assurance to the Mist Portal

Juniper Mist Routing Assurance is a separate AIOps-based routing platform that you can link to from the Juniper Mist portal. Juniper Mist 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 Mist 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 Mist Routing Assurance to establish the link. As such, from the Juniper Mist 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.

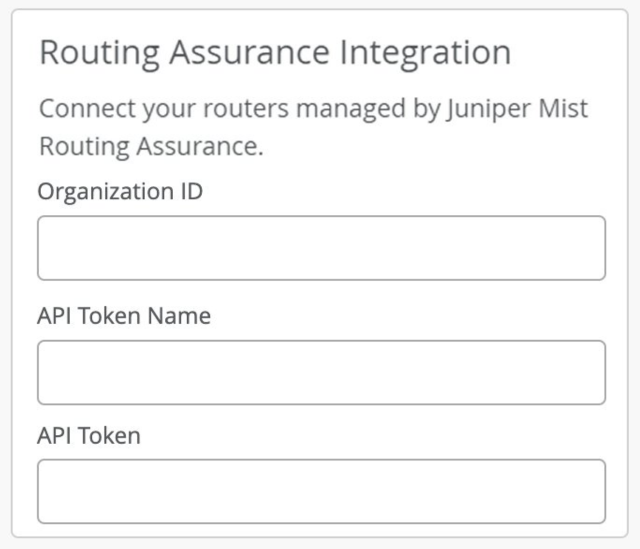

API Token

Name	Access	Site Access
Token1	Network Admin	Primary
Token2	Super User	All Sites

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 Mist Routing Assurance section and enter the following:

   - Organization ID—Use the organization ID from the Juniper Mist Routing Assurance portal.
   - API Token Name—Use the name from Juniper Mist Routing Assurance.
   - API Token—Use the API token you got from the Juniper Mist Routing Assurance portal.

   
   Routing Assurance Integration

   Connect your routers managed by Juniper Mist Routing Assurance.

   Organization ID

   API Token Name

   API Token

4. Click **Save**.

Once linked, Juniper Mist 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 Mist Routing Assurance portal.

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

4

CHAPTER

Subscriptions and Orders

Juniper Mist Subscriptions | 78

Subscription Types for Juniper Mist | 79

Juniper Mist Subscriptions Scope | 116

Activate a Subscription | 120

Renew a Subscription | 120

Subscription Status | 122

Monitor Your Orders | 123

Juniper Mist Subscriptions FAQ | 124

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 | 78
- Subscription Usage | 79
- Managing Subscriptions in the Juniper Mist Portal | 79

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
- Marvis Virtual Network Assistant

Subscription Usage

A Juniper Mist subscription is not associated with a device serial number. Consider this example:

- You buy 12 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. You're keeping the other devices in your inventory as spares.
- If a device fails, you can return it through the RMA process, take a device from your inventory, and install it. You are still using only 10 subscriptions.
- When the RMA device comes back, you can keep it in your inventory so that you have two spares again.

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

- Wireless Assurance | **80**
- Wired Assurance | **83**
- WAN Assurance | **98**
- Access Assurance | **108**
- Marvis | **110**
- Location Services | **114**
- Premium Analytics | **115**

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

- Associated Subscriptions for Wireless Assurance | 80
- Subscriptions for Mist Edges | 83

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 15 on page 80 lists the details of the Wireless Subscription SKUs.

Table 15: 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 16: Associated Standalone Subscriptions for Wireless Assurance

<table>
<tr><th>Subscription SKU</th><th>Description</th><th>SKU Character Definition</th></tr>
<tr><td>SUB-AST-1Y|3Y|5Y</td><td>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.</td><td>SUB—Subscription
AST—Asset Visibility
PMA—Premium Analytics
ENG—User Engagement
VNA—Marvis
1Y|3Y|5Y—Subscription term in years</td></tr>
<tr><td>SUB-PMA-1Y|3Y|5Y</td><td>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.</td><td></td></tr>
<tr><td>SUB-ENG-1Y|3Y|5Y</td><td>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.</td><td></td></tr>
<tr><td>SUB-VNA-1Y|3Y|5Y</td><td>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 .</td><td></td></tr>
</table>

Table 17: 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
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 18: 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

- Wired Assurance Subscriptions | 84
- Associated Subscriptions and Subscription Bundles for Wired Assurance | 88
- Flex Term Subscriptions for Switches | 95

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:

- Standalone Wired Assurance subscription with optional associated subscriptions (Marvis and Premium Analytics) based on your requirement.
- 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 95.

Figure 2 on page 85 summarizes the Mist cloud subscription options for switches.

Figure 2: Mist Cloud Subscription Options for EX Series and QFX Series Switches

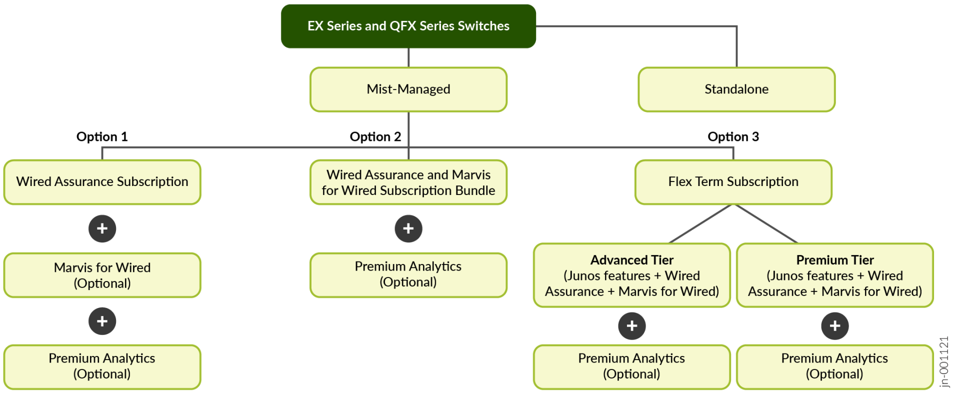

EX Series and QFX Series Switches
Mist-Managed
Standalone
Option 1
Option 2
Option 3
Wired Assurance Subscription
Wired Assurance and Marvis for Wired Subscription Bundle
Flex Term Subscription
+
Marvis for Wired (Optional)
Premium Analytics (Optional)
Advanced Tier (Junos features + Wired Assurance + Marvis for Wired)
Premium Tier (Junos features + Wired Assurance + Marvis for Wired)
Premium Analytics (Optional)
Premium Analytics (Optional)
Premium Analytics (Optional)
jn-001121

Table 19: Standalone Wired Assurance Subscription SKUs for Switches

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 98.
Class 2, 24-port switches		

Table 19: Standalone Wired Assurance Subscription SKUs for Switches *(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 98.
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 98.

Table 19: Standalone Wired Assurance Subscription SKUs for Switches *(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 19: Standalone Wired Assurance Subscription SKUs for Switches *(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 20: 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 20: 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 20: 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 20: 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 21: 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 22: Subscription Bundles for Switches

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 98.
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 98.
Class 3, 32-port or 48-port switches		

Table 22: Subscription Bundles for Switches *(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 98.
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 22: Subscription Bundles for Switches *(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

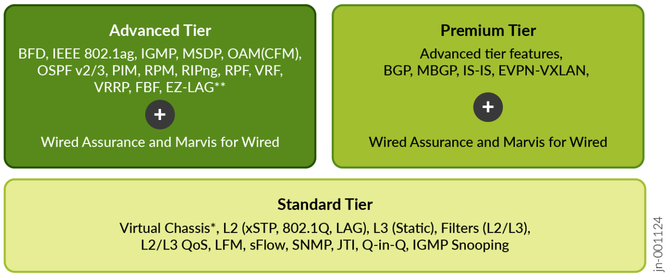
Flex Term Subscriptions for Switches

Flex term subscriptions are special type of subscription bundles which not only include associated subscriptions, but also enable additional Junos capabilities on the switch. 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.

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:


Advanced Tier
BFD, IEEE 802.1ag, IGMP, MSDP, OAM(CFM), OSPF v2/3, PIM, RPM, RIPng, RPF, VRF, VRRP, FBF, EZ-LAG**
+
Wired Assurance and Marvis for Wired
Premium Tier
Advanced tier features, BGP, MBGP, IS-IS, EVPN-VXLAN,
+
Wired Assurance and Marvis for Wired
Standard Tier
Virtual Chassis*, L2 (xSTP, 802.1Q, LAG), L3 (Static), Filters (L2/L3), L2/L3 QoS, LFM, sFlow, SNMP, JTI, Q-in-Q, IGMP Snooping
jn-001124

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 23: Flex Term Subscriptions for Switches

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 98.

Table 23: Flex Term Subscriptions for Switches *(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

- Subscriptions for Session Smart Routers | **99**
- Subscriptions for SRX Firewalls | **103**

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 3 on page 99 summarizes the Mist cloud subscription options for Session Smart Routers.

Figure 3: Mist Cloud Subscription Options for Session Smart Routers

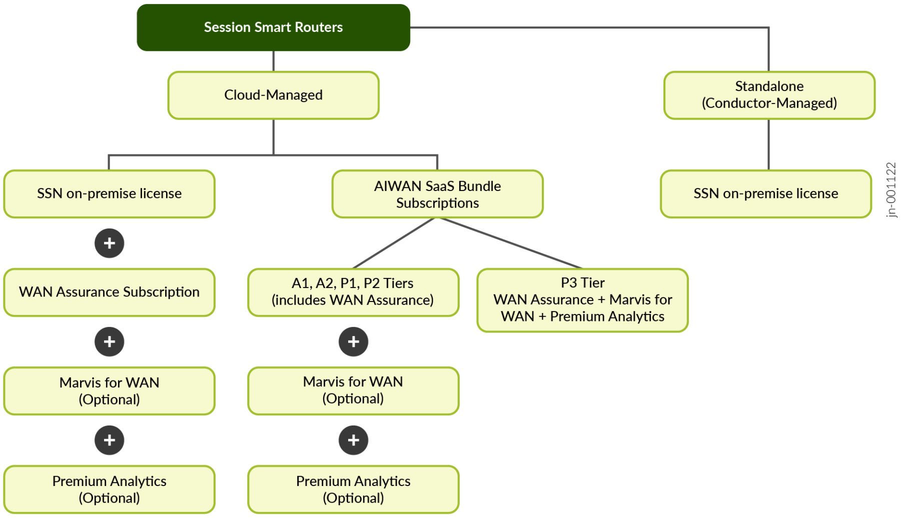

Session Smart Routers
Cloud-Managed
Standalone (Conductor-Managed)
SSN on-premise license
AIWAN SaaS Bundle Subscriptions
SSN on-premise license
+
WAN Assurance Subscription
A1, A2, P1, P2 Tiers (includes WAN Assurance)
P3 Tier WAN Assurance + Marvis for WAN + Premium Analytics
+
Marvis for WAN (Optional)
Marvis for WAN (Optional)
+
Premium Analytics (Optional)
Premium Analytics (Optional)
jn-001122

Table 24: 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 102) 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 25: 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 25: 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 102). **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 26: 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 102) 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 27 on page 102.

Table 27: Bandwidth Throughput Licensing for SSN Flex Tiers

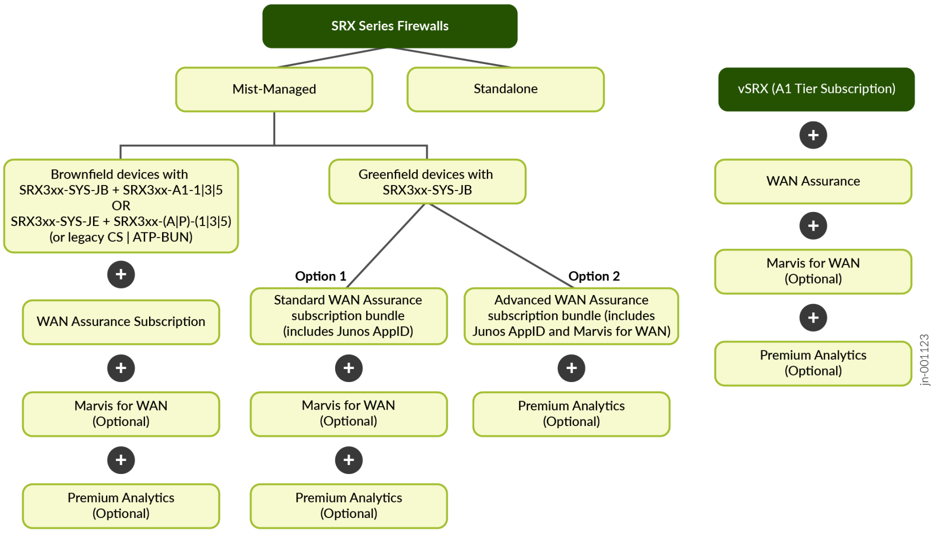
Bandwidth Throughput	L3NID (S)	SER (A1, A2)	Session Smart Router (P1, P2)
10 Mbps		✓	✓
25 Mbps		✓	✓
50 Mbps	✓	✓	✓
100 Mbps	✓	✓	✓
250 Mbps	✓	✓	✓
500 Mbps	✓	✓	✓
1 Gbps	✓	✓	✓
2.5 Gbps	✓	✓	✓
5 Gbps	✓	✓	✓
10 Gbps	✓	✓	✓
20 Gbps		✓	✓
40 Gbps		✓	✓
100 Gbps		✓	✓

Subscriptions for SRX Firewalls

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

Figure 4 on page 103 summarizes the Mist cloud subscription options for SRX Series Firewalls.

Figure 4: Mist Cloud Subscription Options for SRX Series Firewalls


SRX Series Firewalls
Mist-Managed
Standalone
vSRX (A1 Tier Subscription)
Brownfield devices with SRX3xx-SYS-JB + SRX3xx-A1-1|3|5 OR SRX3xx-SYS-JE + SRX3xx-(A|P)-(1|3|5) (or legacy CS | ATP-BUN)
Greenfield devices with SRX3xx-SYS-JB
WAN Assurance
Option 1
Option 2
WAN Assurance Subscription
Standard WAN Assurance subscription bundle (includes Junos AppID)
Advanced WAN Assurance subscription bundle (includes Junos AppID and Marvis for WAN)
Marvis for WAN (Optional)
Premium Analytics (Optional)
Marvis for WAN (Optional)
Marvis for WAN (Optional)
Premium Analytics (Optional)
Premium Analytics (Optional)
Premium Analytics (Optional)
jn-001123

Subscriptions are available for 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 28 on page 104 lists the subscription SKU for brownfield SRX Series Firewalls.

Table 28: WAN Assurance Subscription SKUs for SRX Series Firewalls (Brownfield)

Type	Subscription SKU	SKU Character Description
Brownfield	S-WAN-C1|C2|C3-1|3|5	S—Software WAN—WAN Assurance 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

For greenfield SRX Series Firewalls, you can purchase subscription bundles that include either the WAN Assurance subscription or a combination of WAN Assurance and Marvis for WAN subscriptions.

NOTE: Subscription bundles are available for only greenfield devices.

Table 29: WAN Assurance Subscription Bundles for SRX Series Firewalls (Greenfield)

Type	Subscription SKU	SKU Character Description
Greenfield	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 30: Associated Subscriptions for SRX Series Firewalls

Subscription SKU	Description	SKU Character Description
S-WAN-VNA-C1|C2|C3 – 1|3|5	Marvis for WAN subscription	S—Software WAN—WAN Assurance VNA—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
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 31 on page 107.

Table 31: 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 32: 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 33: 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.	
S-CLIENT-SS-M	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.

Marvis

IN THIS SECTION

- Marvis Subscription Types | 110
- Marvis Actions for Your Subscriptions | 110
- Marvis Subscription SKUs | 112

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 34: 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
Other Actions	Persistently Failing Clients
	Access Port Flap

Table 35: Marvis for WAN Actions

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

Table 36: 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 37 on page 113 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 37: 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 80	Marvis subscription for wireless	See "Wireless Assurance" on page 80
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.	
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 102) 1|3|5 —Subscription term in years

Table 37: Marvis Subscription SKUs *(Continued)*

Subscription Type	Subscription SKU	Description	SKU Character Description
	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
	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

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 38: 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 39: 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 Mist Subscriptions Scope

IN THIS SECTION

- Examples | 119

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.

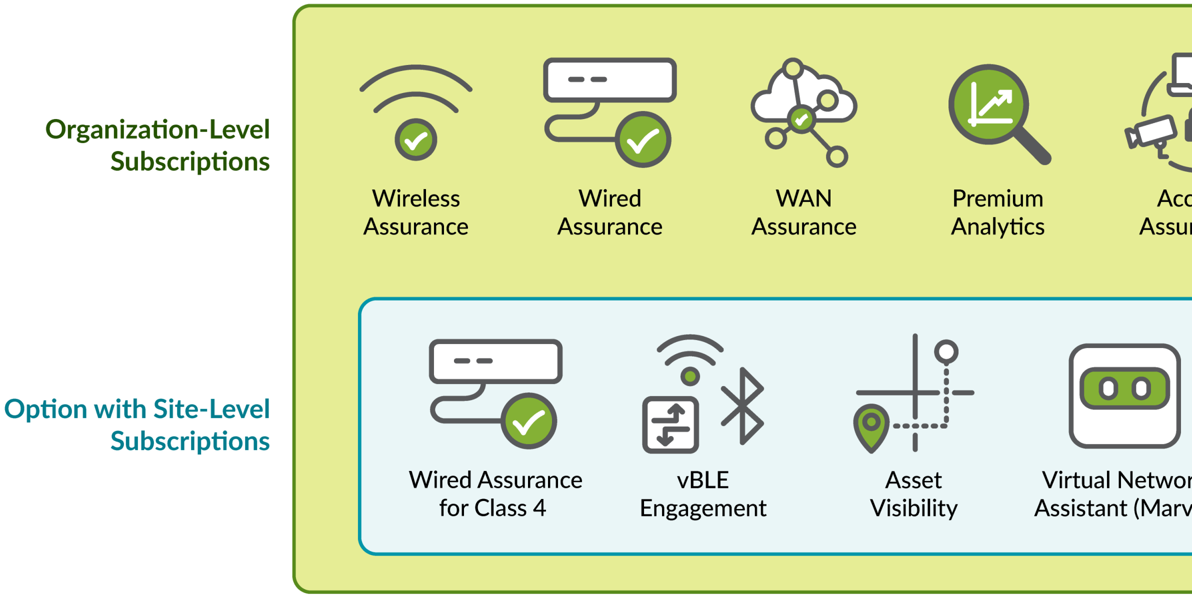
The following table and illustration summarizes the Juniper Mist subscriptions scope.

Features	Organization Level	Site Level
Access Assurance	✓	-

(Continued)

Features	Organization Level	Site Level
Asset Visibility	✓	✓
Marvis Virtual Network Assistant	✓	✓
Premium Analytics	✓	-
vBLE Engagement	✓	✓
WAN Assurance	✓	-
Wi-Fi Management and Assurance	✓	-
Wired Assurance	✓	✓ *
* Applicable to the Wired Assurance for Class 4 subscription only.		

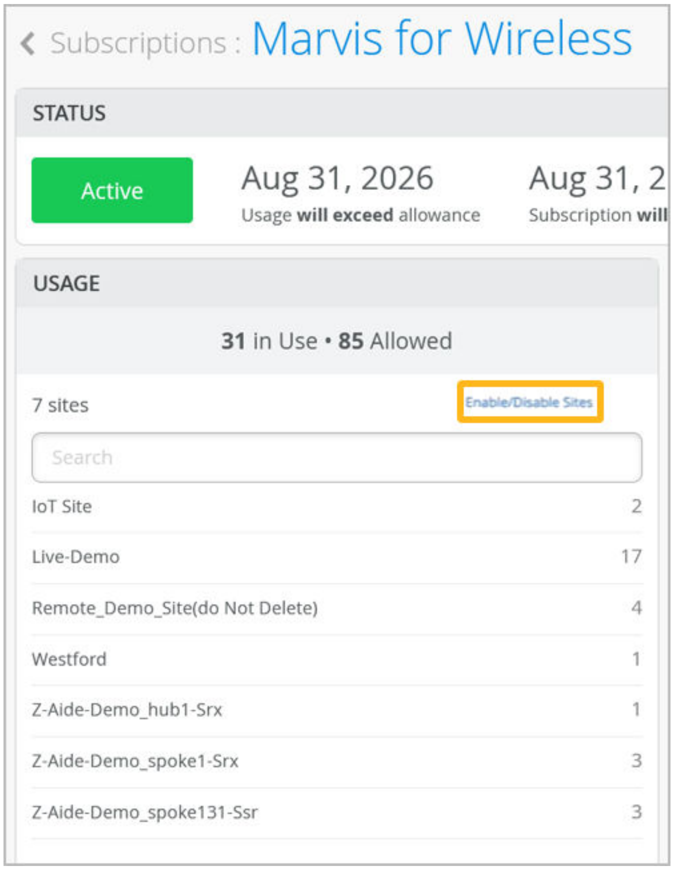
Figure 5: Juniper Mist Subscriptions Scope


Organization-Level Subscriptions
Wireless Assurance
Wired Assurance
WAN Assurance
Premium Analytics
Acc Assu
Option with Site-Level Subscriptions
Wired Assurance for Class 4
vBLE Engagement
Asset Visibility
Virtual Networ Assistant (Marv

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.



Subscriptions : Marvis for Wireless

STATUS

Active

Aug 31, 2026
Usage **will exceed** allowance

Aug 31, 2
Subscription **will**

USAGE

31 in Use • **85** Allowed

7 sites

IoT Site	2
Live-Demo	17
Remote_Demo_Site(do Not Delete)	4
Westford	1
Z-Aide-Demo_hub1-Srx	1
Z-Aide-Demo_spoke1-Srx	3
Z-Aide-Demo_spoke131-Ssr	3

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

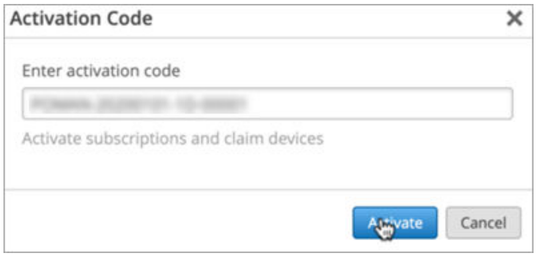
Before You Begin

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**.

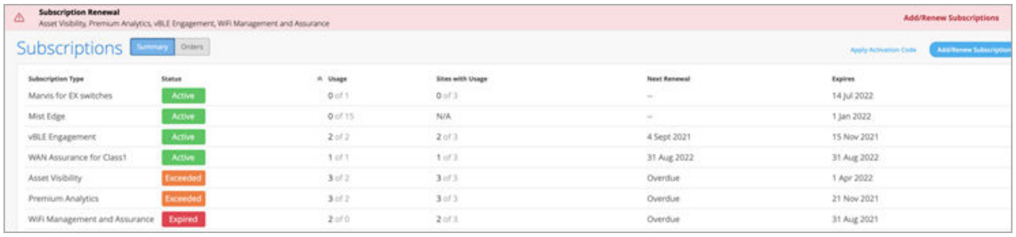


> **NOTE**: If you purchased multiple devices and subscriptions, you'll have one activation code for all of them. In this case, all subscriptions will be activated and the devices will be claimed into your organization.

Renew a Subscription

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



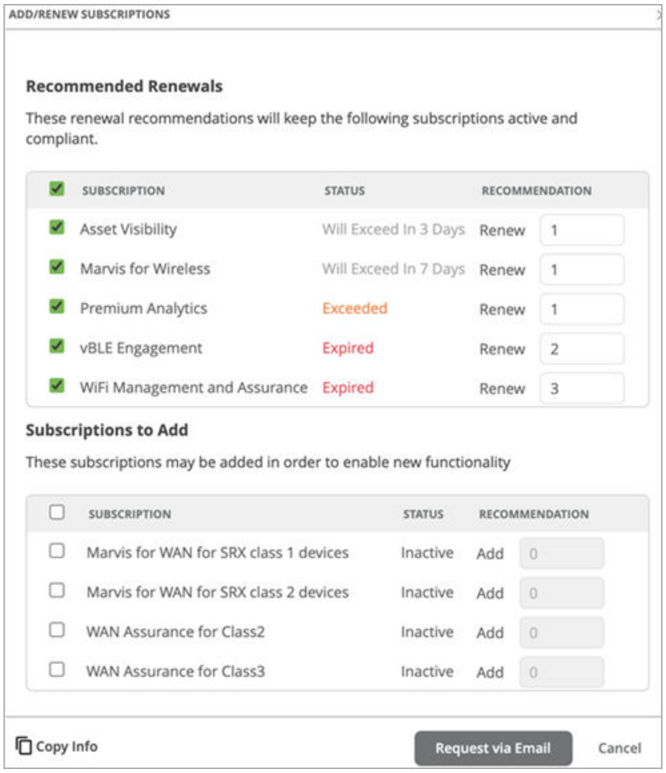
Subscription Renewal
Asset Visibility, Premium Analytics, vBLE Engagement, WiFi Management and Assurance

Subscription Type	Status	Usage	Sites with Usage	Next Renewal	Expires
Marvis for EX switches	Active	0 of 1	0 of 3	--	14 Jul 2022
Mist Edge	Active	0 of 15	N/A	--	1 Jan 2022
vBLE Engagement	Active	2 of 2	2 of 3	4 Sept 2021	15 Nov 2021
WAN Assurance for Class1	Active	1 of 1	1 of 3	31 Aug 2022	31 Aug 2022
Asset Visibility	Exceeded	3 of 2	3 of 3	Overdue	1 Apr 2022
Premium Analytics	Exceeded	3 of 2	3 of 3	Overdue	21 Nov 2021
WiFi Management and Assurance	Expired	2 of 0	2 of 3	Overdue	31 Aug 2021

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 date appears in the **Next 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.



ADD/RENEW SUBSCRIPTIONS

Recommended Renewals

These renewal recommendations will keep the following subscriptions active and compliant.

☑	SUBSCRIPTION	STATUS	RECOMMENDATION	
☑	Asset Visibility	Will Exceed In 3 Days	Renew	1
☑	Marvis for Wireless	Will Exceed In 7 Days	Renew	1
☑	Premium Analytics	Exceeded	Renew	1
☑	vBLE Engagement	Expired	Renew	2
☑	WiFi Management and Assurance	Expired	Renew	3

Subscriptions to Add

These subscriptions may be added in order to enable new functionality

☐	SUBSCRIPTION	STATUS	RECOMMENDATION	
☐	Marvis for WAN for SRX class 1 devices	Inactive	Add	0
☐	Marvis for WAN for SRX class 2 devices	Inactive	Add	0
☐	WAN Assurance for Class2	Inactive	Add	0
☐	WAN Assurance for Class3	Inactive	Add	0

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

IN THIS SECTION

- Subscription Status | 122

Subscription Status

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

NOTE:

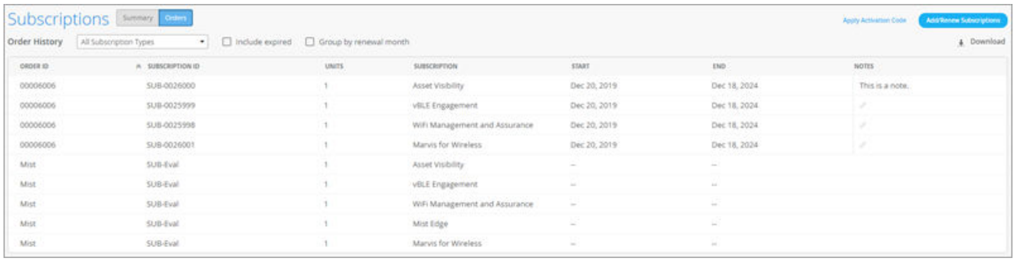
    - A subscription starts when Juniper ships emails the activation code to you.
    - Alerts appear if subscriptions have not been renewed within a 30-day grace period.
    - After a subscription expires, your network will continue to operate. However, no support is provided for expired subscriptions.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

Use the Order History page to check your orders and the upcoming end dates for your Juniper Mist™ subscriptions.

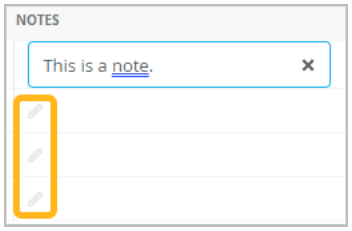
To find the Order History page, select **Organization** > **Admin** > **Subscriptions** from the left menu. Then click the **Orders** button at the top of the page.



ORDER ID	SUBSCRIPTION ID	UNITS	SUBSCRIPTION	START	END	NOTES
00006006	SUB-0026000	1	Asset Visibility	Dec 20, 2019	Dec 18, 2024	This is a note.
00006006	SUB-0025999	1	vBLE Engagement	Dec 20, 2019	Dec 18, 2024	✎
00006006	SUB-0025998	1	WiFi Management and Assurance	Dec 20, 2019	Dec 18, 2024	✎
00006006	SUB-0026001	1	Marvis for Wireless	Dec 20, 2019	Dec 18, 2024	✎
Mist	SUB-Eval	1	Asset Visibility	–	–	
Mist	SUB-Eval	1	vBLE Engagement	–	–	
Mist	SUB-Eval	1	WiFi Management and Assurance	–	–	
Mist	SUB-Eval	1	Mist Edge	–	–	
Mist	SUB-Eval	1	Marvis for Wireless	–	–	

You can customize this page in various ways.

- Use the 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.
- 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.
- To 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.


NOTES

This is a note.

- To 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.
- To delete a note, click the note, click **X**, and then click a blank area of the page to save the change.
- To save the order history as a CSV file, click **Download** on the right side of the page.

Juniper Mist Subscriptions FAQ

IN THIS SECTION

- How can I obtain a trial subscription? | **125**
- Where can I view the subscriptions for a device? | **125**
- What happens when a subscription expires? | **125**
- How do I renew a subscription? | **126**
- What is the difference between Entitled and Usage? | **126**
- What does the **One or more subscriptions have expired or exceeded their entitled usage** warning message indicate? | **126**
- Why does the Subscriptions page display that the subscriptions are decommissioned even though I renewed the subscriptions? | **126**
- Will the Juniper Mist Cloud disconnect the access point (AP) automatically when the subscription expires? | **127**
- Can subscriptions be moved from one organization to another? | **127**
- What are the requirements for moving subscriptions between organizations? | **127**
- Where can I view the API documentation for subscriptions? | **127**
- Can subscriptions be co-termed? | **127**
- How can I move subscriptions from the global environment to the EU environment? | **128**
- Which API call should I use to obtain a summary of the subscriptions? | **128**

- Which API call should I use to obtain the subscription usage information by sites? | 128
- When does my 90-day free trial start? | 128
- When does the term for a subscription start? Is the term tied to the date when the subscription is activated using the activation code? | 129
- Will I receive a notification before my subscriptions expire? | 129

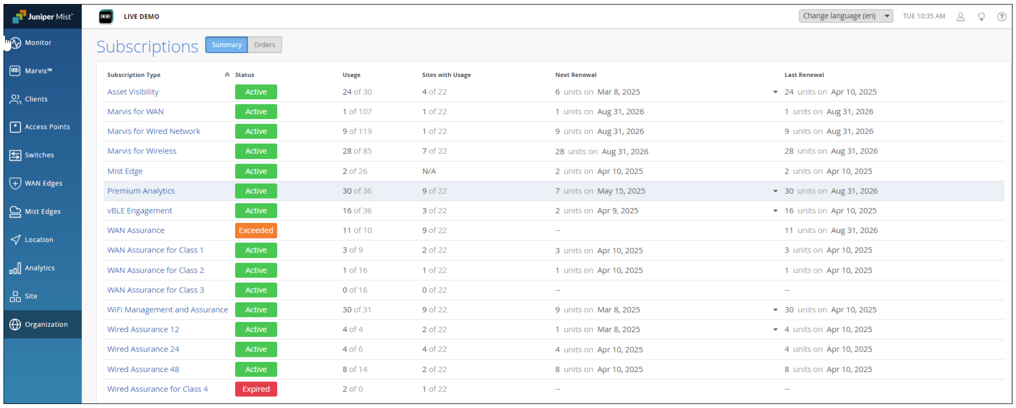
How can I obtain a trial subscription?

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 the subscriptions for a device?

Subscriptions are applicable to organizations and are not tied to any specific device. If the feature is enabled at the site level, then all APs assigned to that site consume the corresponding subscription.

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



Subscription Type	Status	Usage	Sites with Usage	Next Renewal	Last Renewal
Asset Visibility	Active	24 of 30	4 of 22	6 units on Mar 8, 2025	24 units on Apr 10, 2025
Marvis for WAN	Active	1 of 107	1 of 22	1 units on Aug 31, 2026	1 units on Aug 31, 2026
Marvis for Wired Network	Active	9 of 119	1 of 22	9 units on Aug 31, 2026	9 units on Aug 31, 2026
Marvis for Wireless	Active	28 of 85	7 of 22	28 units on Aug 31, 2026	28 units on Aug 31, 2026
Mist Edge	Active	2 of 26	N/A	2 units on Apr 10, 2025	2 units on Apr 10, 2025
Premium Analytics	Active	30 of 36	9 of 22	7 units on May 15, 2025	30 units on Aug 31, 2026
vBLE Engagement	Active	16 of 36	3 of 22	2 units on Apr 9, 2025	16 units on Apr 10, 2025
WAN Assurance	Exceeded	11 of 10	9 of 22	--	11 units on Aug 31, 2026
WAN Assurance for Class 1	Active	3 of 9	2 of 22	3 units on Apr 10, 2025	3 units on Apr 10, 2025
WAN Assurance for Class 2	Active	1 of 16	1 of 22	1 units on Apr 10, 2025	1 units on Apr 10, 2025
WAN Assurance for Class 3	Active	0 of 16	0 of 22	--	--
WiFi Management and Assurance	Active	30 of 31	9 of 22	9 units on Mar 8, 2025	30 units on Apr 10, 2025
Wired Assurance 12	Active	4 of 4	2 of 22	1 units on Mar 8, 2025	4 units on Apr 10, 2025
Wired Assurance 24	Active	4 of 6	4 of 22	4 units on Apr 10, 2025	4 units on Apr 10, 2025
Wired Assurance 48	Active	8 of 14	2 of 22	8 units on Apr 10, 2025	8 units on Apr 10, 2025
Wired Assurance for Class 4	Expired	2 of 0	1 of 22	--	--

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

View and Update Your Device Inventory | 131

Auto-Provisioning | 147

Claim a Switch | 160

Adopt a Switch from Your Juniper Installed Base | 162

Claim a WAN Edge | 162

Adopt a WAN Edge from Your Juniper Installed Base | 163

Rename Devices | 163

Device Management with the Juniper Mist AI Mobile App | 164

View and Update Your Device Inventory

IN THIS SECTION

- View Juniper Support Insights (JSI) for Your Installed Base | 133
- Device Details for Installed Base | 138

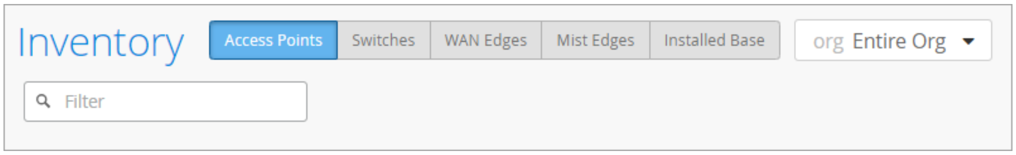
You can view information for all the devices in your Juniper Mist™ inventory. Additionally, you can make changes to individual devices or to multiple devices at once.

Find the Inventory Page

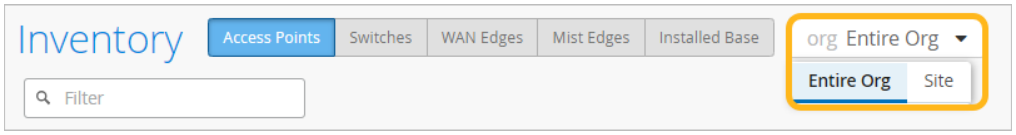
From the left menu, select **Organization** > **Admin** > **Inventory**.

View and Find Information

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



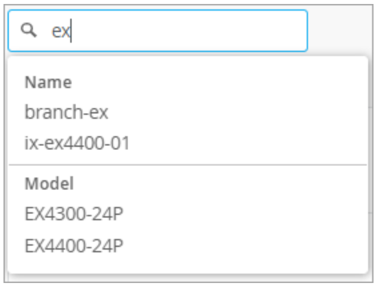
- To select the device type, click a device button:
  - Access Points
  - Switches
  - WAN Edges
  - Cellular Edges
  - Mist Edges
- To view devices that are linked through the Juniper Account Integration option on the Organization Settings page, click the **Installed Base** button. For more information, see "View Juniper Support Insights (JSI) for Your Installed Base" on page 133.
- 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 160
- "Claim a WAN Edge" on page 162

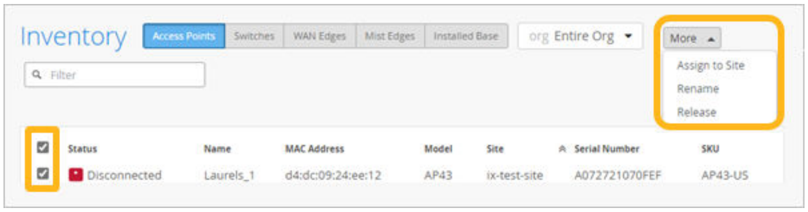
Adopt devices from your Juniper Installed Base:

- "Adopt a Switch from Your Juniper Installed Base" on page 162
- "Adopt a WAN Edge from Your Juniper Installed Base" on page 163

Make Other Changes

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



☑	Status	Name	MAC Address	Model	Site	Serial Number	SKU
☑	Disconnected	Laurels_1	d4:dc:09:24:ee:12	AP43	ix-test-site	A072721070FEF	AP43-US

- **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.

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 view insights for all your Juniper devices.

IN THIS SECTION

- Overview of the Installed Base Page | **134**
- Top-of-Page Information | **134**
- Find a Device by Using Filters | **135**
- Adjust the Columns in the Table Settings | **135**
- Field Descriptions on the Installed Base Page | **136**
- Device Details | **137**

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.

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 71.

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

Overview of 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.

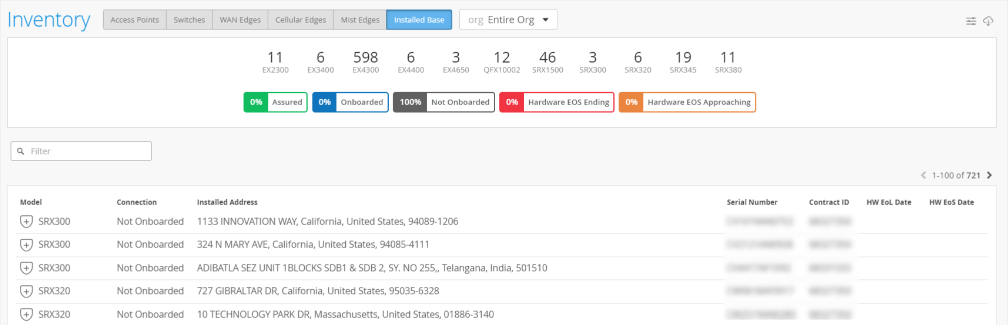
The Installed Base page displays Juniper support information for the Juniper Networks devices linked to your organization. You can access information about:

- Devices associated with the Juniper account that is integrated with the organization.
- Devices directly onboarded to the organization. The devices may or may not be associated with the Juniper account that is integrated with the organization.

For each device in the table, you can view more details by clicking the device. For more information, see "Device Details for Installed Base" on page 138.

Top-of-Page Information

At the top of the Installed Base page, you see high-level information. These info boxes also are buttons that you can click to filter the data.



11	6	598	6	3	12	46	3	6	19	11
EX2300	EX3400	EX4300	EX4400	EX4650	QFX10002	SRX1500	SRX300	SRX320	SRX345	SRX380

Model	Connection	Installed Address	Serial Number	Contract ID	HW EoL Date	HW EoS Date
SRX300	Not Onboarded	1133 INNOVATION WAY, California, United States, 94089-1206	[redacted]	[redacted]		
SRX300	Not Onboarded	324 N MARY AVE, California, United States, 94085-4111	[redacted]	[redacted]		
SRX300	Not Onboarded	ADIBATLA SEZ UNIT 1BLOCKS SDB1 & SDB 2, SY. NO 255,, Telangana, India, 501510	[redacted]	[redacted]		
SRX320	Not Onboarded	727 GIBRALTAR DR, California, United States, 95035-6328	[redacted]	[redacted]		
SRX320	Not Onboarded	10 TECHNOLOGY PARK DR, Massachusetts, United States, 01886-3140	[redacted]	[redacted]		

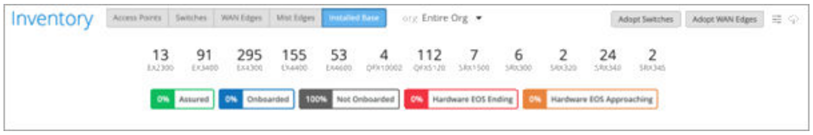
- Device Models—For each model, you see the number of devices of that model.
- Connection Status—For each status, you see the percentage of devices with that status.
  - Assured—Connected to Juniper Mist Routing Assurance or Juniper Apstra Cloud Services
  - Onboarded—Connected to Juniper Support Insights service
  - Not Onboarded—Not connected to any service level

- Hardware Status—For each EOS (End of Sale) category, you see the percentage of devices in that category.
  - Hardware EOS Ending—EOS occurs within 3 months from now.
  - Hardware EOS Approaching—EOS occurs 3 to 6 months from now.

Find a Device by Using Filters

To find a device by using filters:

- Use the filter buttons—The top-of-page information boxes also are buttons that you can click to filter the table. For example, click a model to show only that model in the table. To clear a filter, click the button again.



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

Adjust the Columns in the Table Settings

You can show, hide, and reorganize the columns so that the table shows exactly the information that you want to see.

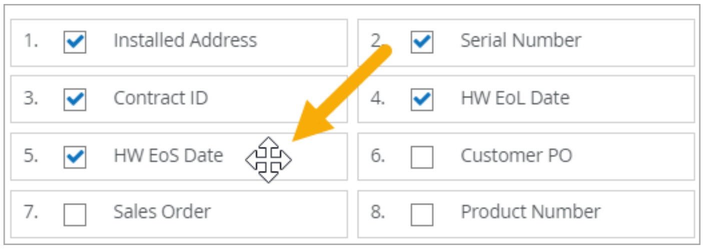
To adjust the data in the table:

Click the Table Settings button at the top right corner of the Installed Base page.

In the pop-up window, select the columns that you want to see, and drag them into the desired order.

- Select the check boxes for the columns that you want to show in the Inventory Base table.
- Clear check boxes to remove columns from the Inventory Base table.
- Drag boxes up or down to change the order of the columns in the Inventory Base table.

  In this example, the mouse is hovering over the HW EoS Date option. This column is now numbered 5, meaning that it is the fifth column in the Installed Base table. As you drag your mouse up or down, the other column options reposition themselves. When you release the mouse, the new column numbers appear.



1.	☑	Installed Address	2.	☑	Serial Number
3.	☑	Contract ID	4.	☑	HW EoL Date
5.	☑	HW EoS Date	6.	□	Customer PO
7.	□	Sales Order	8.	□	Product Number

- When finished selecting and moving columns, click **X** to close the pop-up window.

Field Descriptions on the Installed Base Page

Table 41: Fields in the Installed Base Table

Field	Description *(Columns and column order are determined by Table Settings.)*
Model	The device model
Connection	Connection Status • Assured—Connected to Juniper Mist Routing Assurance or Juniper Apstra Cloud Services • Onboarded—Connected to Juniper Support Insights service • Not Onboarded—Not connected to any service level
Installed Address	Location associated with the installed device.
Serial Number	Unique ID mapped to the device.
Contract ID	Service contract number assigned to the device.
HW EoL Date	End of Life date for the device.
HW EoS Date	End of Service date for the device.
Customer PO	Customer purchase order number for the device.
Sales Order	Sales order number for the device.

Table 41: Fields in the Installed Base Table *(Continued)*

Field	Description *(Columns and column order are determined by Table Settings.)*
Product Number	Stock Keeping Unit (SKU) number assigned to the device.
Contract Type	Type of active support coverage provided for the device. Example: Maintenance.
Contract SKU	SKU assigned to the active support coverage associated with the device.
Contract Start	Service contract start date for the device.
Contract End	Service contract end date for the device.
Ship Date	Date on which the device was shipped to your company's site.
Reseller	Reseller of the device.
Distributor	Distributor of the device.
Warranty Type	Warranty type associated with the device. Example: Standard Hardware Warranty.
Warranty Start Date	Start date of warranty for the device.
Warranty End Date	End date of warranty for the device.

Device Details

Every table row is a link to details about the device, including security incidence tickets and proactive bug notifications.

Click a table row to go to the device details page for that device. For more information, see"Device Details for Installed Base" on page 138 .

Device Details for Installed Base

SUMMARY

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

IN THIS SECTION

- Overview Information | 138
- SIRT (Security Incidence Response Team Tickets) Information | 141
- PBN (Proactive Bug Notification) | 143

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

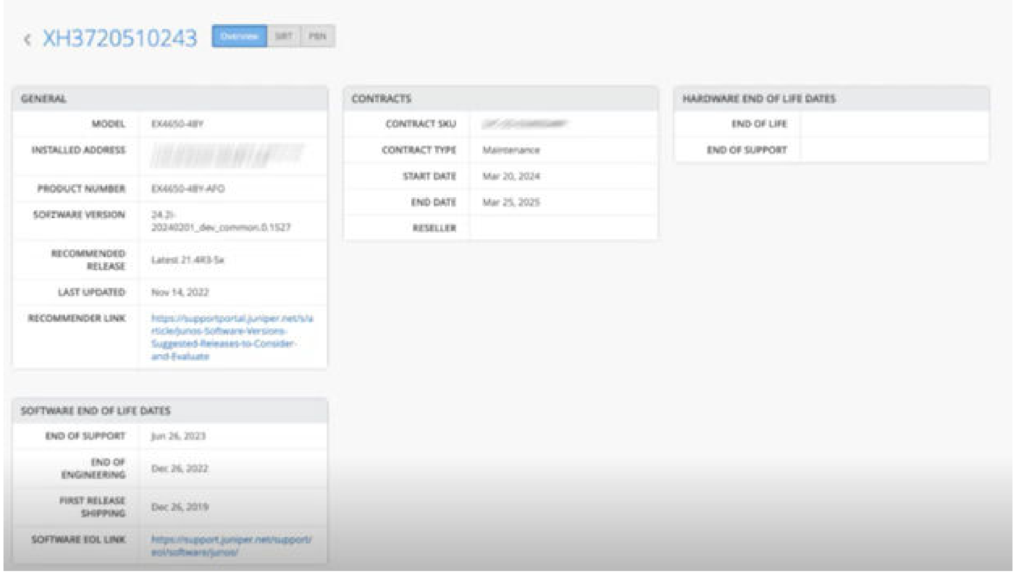
NOTE: For more information about the Installed Base page, see "View Juniper Support Insights (JSI) for Your Installed Base" on page 133 .

Use the buttons at the top of the page to select the type of information to view:

- Overview
- SIRT (Security Incidence Response Team Tickets)
- PBN (Proactive Bug Notification)

Overview Information

For general device information and contract information, click the **Overview** tab.



GENERAL

MODEL	EX4650-48Y
INSTALLED ADDRESS	[redacted]
PRODUCT NUMBER	EX4650-48Y-AFO
SOFTWARE VERSION	24.2I-20240201_dev_common.0.1527
RECOMMENDED RELEASE	Latest 21.4R3-S4
LAST UPDATED	Nov 14, 2022
RECOMMENDER LINK	https://supportportal.juniper.net/s/article/Junos-Software-Versions-Suggested-Releases-to-Consider-and-Evaluate

CONTRACTS

CONTRACT SKU	[redacted]
CONTRACT TYPE	Maintenance
START DATE	Mar 20, 2024
END DATE	Mar 25, 2025
RESELLER	

HARDWARE END OF LIFE DATES

END OF LIFE	
END OF SUPPORT	

SOFTWARE END OF LIFE DATES

END OF SUPPORT	Jun 26, 2023
END OF ENGINEERING	Dec 26, 2022
FIRST RELEASE SHIPPING	Dec 26, 2019
SOFTWARE EOL LINK	https://support.juniper.net/support/eol/software/junos/

Table 42: Fields in the Overview Information

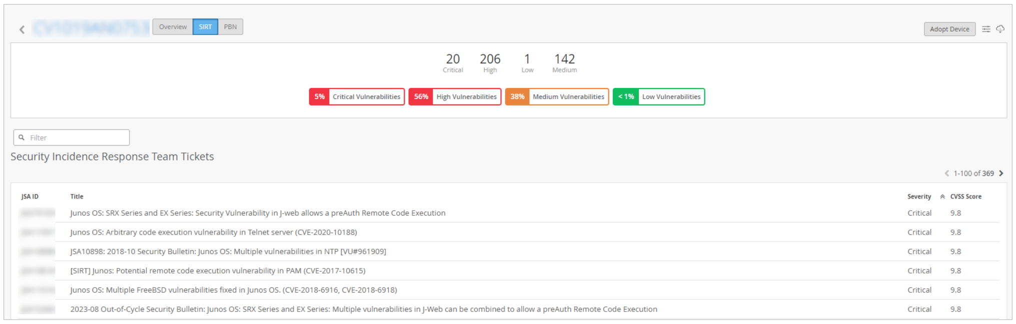
Field	Description
General	
Model	Device model
Installed Address	Address of the site where the device is installed.
Product Number	Stock Keeping Unit (SKU) number assigned to the device.
Software Version	The Junos OS version installed on the device.
Recommended Release	Recommended Junos OS software version for the device.
Last Updated	Date on which the recommended Junos OS software was last updated.
Recommended Link	Link to a Juniper Support Portal Knowledge Base article with a list of recommended Junos OS versions for each Juniper platform.
Contracts	
Contract SKU	SKU assigned to the device's service contract.
Contract Type	Type of active support coverage provided for the device. Example: Maintenance.

Table 42: Fields in the Overview Information *(Continued)*

Field	Description
Start Date	Date on which the service contract starts for the device.
End Date	Date on which the service contract ends for the device.
Reseller	Name of the reseller through which your company acquired the device.
Hardware End of Life Dates (Displayed if at least one of the following hardware EOL information is available for the device.)	
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.
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.
End of Engineering	Date on which the Junos OS software version installed on the device reaches end of engineering-level 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.

SIRT (Security Incidence Response Team Tickets) Information

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



20	206	1	142
Critical	High	Low	Medium

Security Incidence Response Team Tickets

1-100 of 369

JSA ID	Title	Severity	CVSS Score
[redacted]	Junos OS: SRX Series and EX Series: Security Vulnerability in J-web allows a preAuth Remote Code Execution	Critical	9.8
[redacted]	Junos OS: Arbitrary code execution vulnerability in Telnet server (CVE-2020-10188)	Critical	9.8
[redacted]	JSA10898: 2018-10 Security Bulletin: Junos OS: Multiple vulnerabilities in NTP [VU#961909]	Critical	9.8
[redacted]	[SIRT] Junos: Potential remote code execution vulnerability in PAM (CVE-2017-10615)	Critical	9.8
[redacted]	Junos OS: Multiple FreeBSD vulnerabilities fixed in Junos OS. (CVE-2018-6916, CVE-2018-6918)	Critical	9.8
[redacted]	2023-08 Out-of-Cycle Security Bulletin: Junos OS: SRX Series and EX Series: Multiple vulnerabilities in J-Web can be combined to allow a preAuth Remote Code Execution	Critical	9.8

> **NOTE**: If the Juniper Networks device is in Assured or Onboarded state, the SIRT tab displays a list of security vulnerabilities specific to the type of Juniper Networks device and the Junos OS version installed. If a Juniper device is in Not Onboarded state, the SIRT tab displays a list of security vulnerabilities specific to the type of Juniper Networks device only.

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 tickets with that status. To clear a filter, click the button again.

- Keywords Filter box (above the table)—To find a ticket by entering keywords, start typing in the Filter box. When the matching items appear in the drop-down list, click the ticket 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.

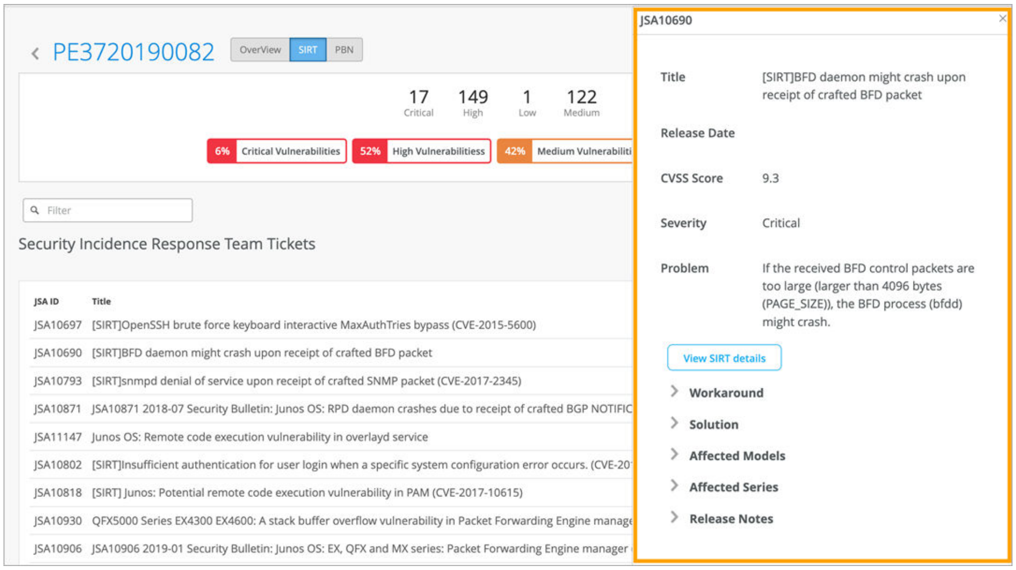
  In the pop-up window, select the columns that you want to see, and drag them into the desired order. Clear check boxes to remove columns from the Inventory Base table. When finished selecting and moving columns, click **X** to close the pop-up window.

- 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 ticket. Click on any of the SIRT tickets to view the Quick View panel for the SIRT ticket.

  Example



Security Incidence Response Team Tickets

JSA ID	Title
JSA10697	[SIRT]OpenSSH brute force keyboard interactive MaxAuthTries bypass (CVE-2015-5600)
JSA10690	[SIRT]BFD daemon might crash upon receipt of crafted BFD packet
JSA10793	[SIRT]snmpd denial of service upon receipt of crafted SNMP packet (CVE-2017-2345)
JSA10871	JSA10871 2018-07 Security Bulletin: Junos OS: RPD daemon crashes due to receipt of crafted BGP NOTIFIC
JSA11147	Junos OS: Remote code execution vulnerability in overlayd service
JSA10802	[SIRT]Insufficient authentication for user login when a specific system configuration error occurs. (CVE-20
JSA10818	[SIRT] Junos: Potential remote code execution vulnerability in PAM (CVE-2017-10615)
JSA10930	QFX5000 Series EX4300 EX4600: A stack buffer overflow vulnerability in Packet Forwarding Engine manage
JSA10906	JSA10906 2019-01 Security Bulletin: Junos OS: EX, QFX and MX series: Packet Forwarding Engine manager

JSA10690

Title: [SIRT]BFD daemon might crash upon receipt of crafted BFD packet

Release Date

CVSS Score: 9.3

Severity: Critical

Problem: If the received BFD control packets are too large (larger than 4096 bytes (PAGE_SIZE)), the BFD process (bfdd) might crash.

Table 43: Fields in the SIRT Information

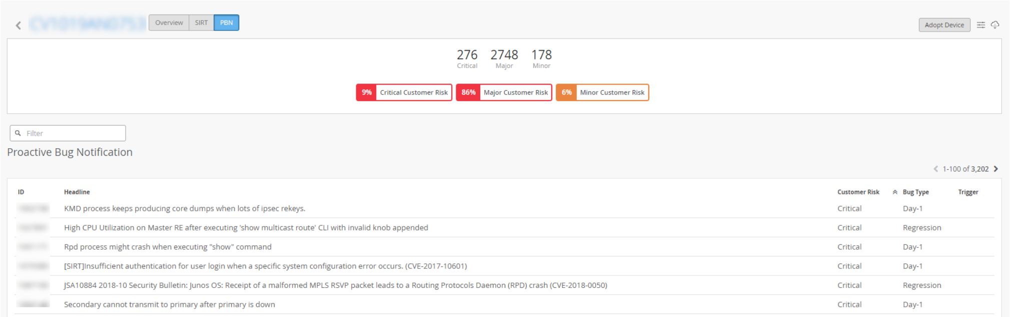
Field	Description *(Columns and column order are determined by Table Settings.)*
JSA ID	Unique value that identifies the security advisory on Juniper Networks Support Portal.
Title	Synopsis of the security advisory.

Table 43: Fields in the SIRT Information *(Continued)*

Field	Description *(Columns and column order are determined by Table Settings.)*
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.
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.

PBN (Proactive Bug Notification)

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



276 Critical 2748 Major 178 Minor

9% Critical Customer Risk | 86% Major Customer Risk | 6% Minor Customer Risk

Filter

Proactive Bug Notification

1-100 of 3,202

ID	Headline	Customer Risk	Bug Type	Trigger
[redacted]	KMD process keeps producing core dumps when lots of ipsec rekeys.	Critical	Day-1	
[redacted]	High CPU Utilization on Master RE after executing 'show multicast route' CLI with invalid knob appended	Critical	Regression	
[redacted]	Rpd process might crash when executing "show" command	Critical	Day-1	
[redacted]	[SIRT]Insufficient authentication for user login when a specific system configuration error occurs. (CVE-2017-10601)	Critical	Day-1	
[redacted]	JSA10884 2018-10 Security Bulletin: Junos OS: Receipt of a malformed MPLS RSVP packet leads to a Routing Protocols Daemon (RPD) crash (CVE-2018-0050)	Critical	Regression	
[redacted]	Secondary cannot transmit to primary after primary is down	Critical	Day-1	

NOTE: If the Juniper Networks device is in Assured or Onboarded state, the PBN tab displays a list of known issues relevant to the type of Juniper Networks device and the Junos OS version installed. If a Juniper device is in Not Onboarded state, the PBN tab displays a list of known issues specific to the type of Juniper Networks device only.

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 tickets with that status. To clear a filter, click the button again.

- Keywords Filter box (above the table)—To find a ticket by entering keywords, start typing in the Filter box. When the matching items appear in the drop-down list, click the ticket 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.

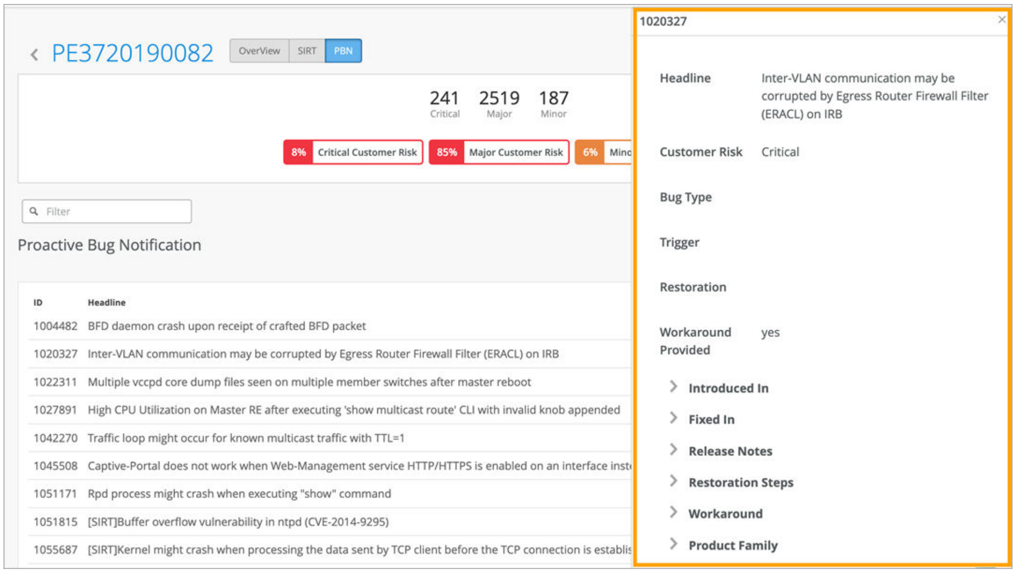
- Table Settings button (top-right corner of page)—Click this button to show, hide, and reorganize the columns so that the table shows exactly the information that you want to see.

  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 ticket.

  Example

- 

Proactive Bug Notification

ID	Headline
1004482	BFD daemon crash upon receipt of crafted BFD packet
1020327	Inter-VLAN communication may be corrupted by Egress Router Firewall Filter (ERACL) on IRB
1022311	Multiple vccpd core dump files seen on multiple member switches after master reboot
1027891	High CPU Utilization on Master RE after executing 'show multicast route' CLI with invalid knob appended
1042270	Traffic loop might occur for known multicast traffic with TTL=1
1045508	Captive-Portal does not work when Web-Management service HTTP/HTTPS is enabled on an interface inst
1051171	Rpd process might crash when executing "show" command
1051815	[SIRT]Buffer overflow vulnerability in ntpd (CVE-2014-9295)
1055687	[SIRT]Kernel might crash when processing the data sent by TCP client before the TCP connection is establis

1020327

Headline	Inter-VLAN communication may be corrupted by Egress Router Firewall Filter (ERACL) on IRB
Customer Risk	Critical
Bug Type	
Trigger	
Restoration	
Workaround Provided	yes

Table 44: 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.
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.

Table 44: Fields on the PBN Tab of the *Device* Details Page *(Continued)*

Field	Description *(Columns and column order are determined by Table Settings.)*
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.
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

- Automatically Assign Devices to Sites | **148**
- Automatically Assign Device Names | **151**
- Automatically Assign Device Profiles to Access Points | **153**
- Manipulate Source Strings for Auto-Provisioning | **155**

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.

Consider these examples.

- **Dynamically assigning devices to sites:** 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 can 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. This feature also is available for Cellular Edge devices, using the device name or the model. See "Automatically Assign Devices to Sites" on page 148.

- **Dynamically naming devices:** 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.

  This feature can assign names to APs based on the LLDP port or the MAC address. See "Automatically Assign Device Names" on page 151.

- **Dynamically assigning device profiles:** 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.

  This feature can 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 153.

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.

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.

NOTE: Auto-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.

Device Attributes for APs

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

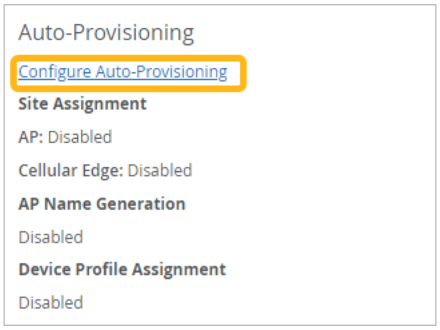
- The device name. For this option, you need to configure each device name to include the site name.
- The Link Layer Discovery Protocol (LLDP) system name of the switch that the device is connected to. For this option, you need to configure the LLDP system name to include the site name.
- The Domain Name System (DNS) suffix. For this option, you need to configure each DNS suffix to include the site name.
- The subnet that you connect the device to. For this option, you'll create a list of subnets and their corresponding sites when you configure the auto-provisioning rule.
- 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**.



Auto-Provisioning

Configure Auto-Provisioning

Site Assignment

AP: Disabled

Cellular Edge: Disabled

AP Name Generation

Disabled

Device Profile Assignment

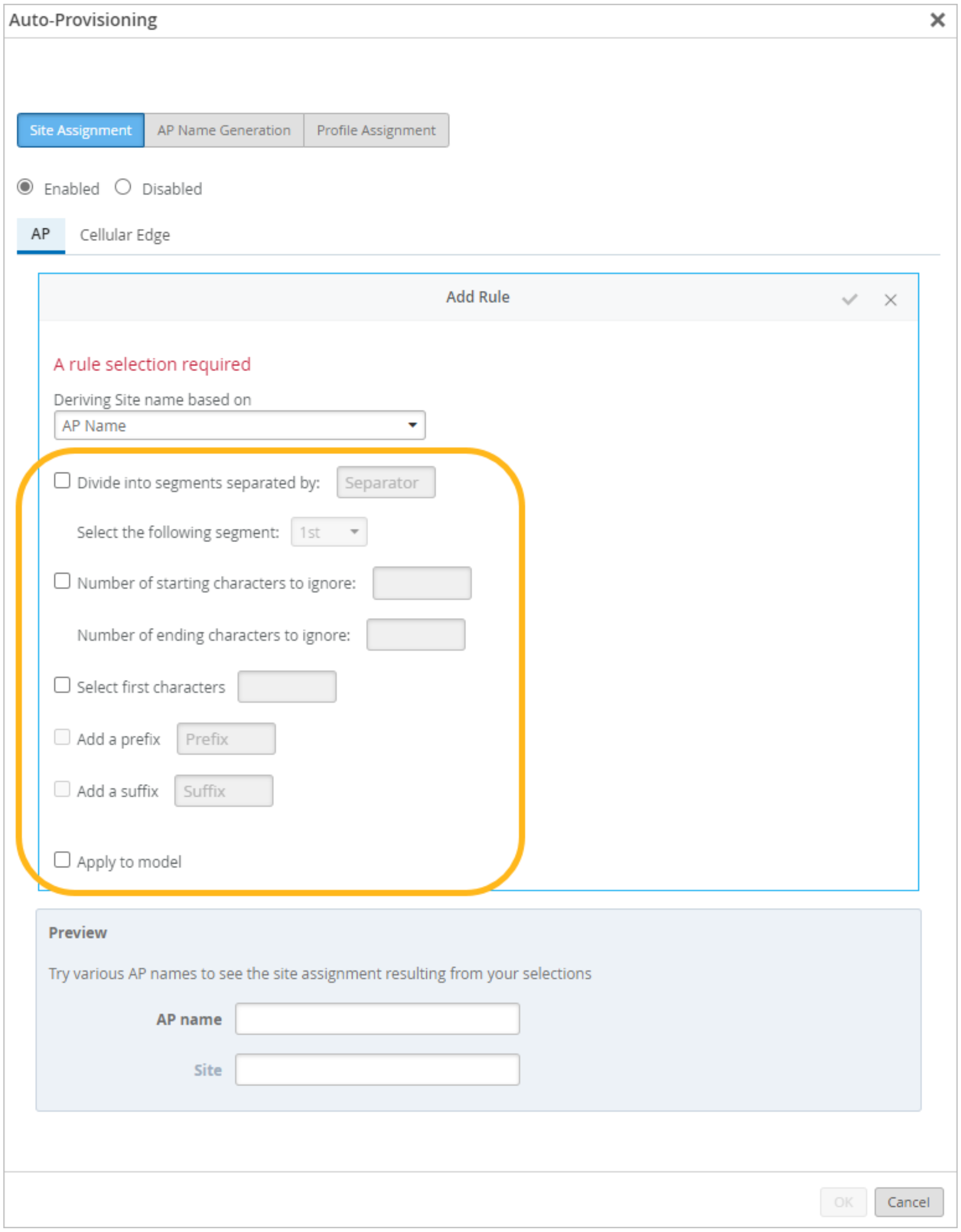
Disabled

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:

   - **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.



Auto-Provisioning ✕

● Enabled ○ Disabled

Add Rule ✓ ✕

A rule selection required

Deriving Site name based on: AP Name

□ Divide into segments separated by: Separator

Select the following segment: 1st

□ Number of starting characters to ignore:

Number of ending characters to ignore:

□ Select first characters

□ Add a prefix: Prefix

□ Add a suffix: Suffix

□ Apply to model

Preview

Try various AP names to see the site assignment resulting from your selections

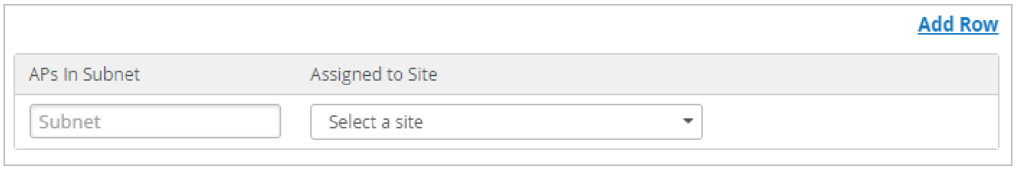
AP name:

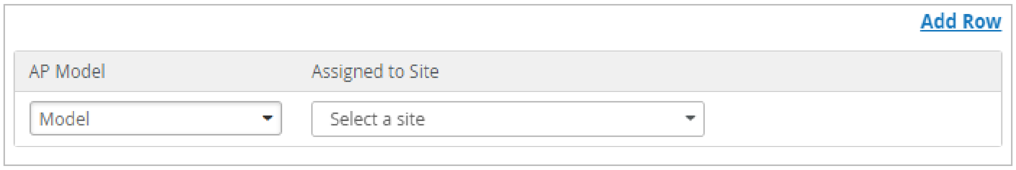
Site:

NOTE: The **Apply to model** option is available when AP Name is selected as the source.

For information and examples, see "Manipulate Source Strings for Auto-Provisioning" on page 155.

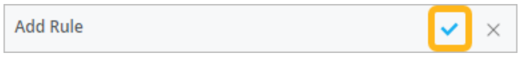
- **Subnet** or **Model**—Complete the table at the bottom of the Auto-Provisioning window to match each subnet or model to a site.





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 155.

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

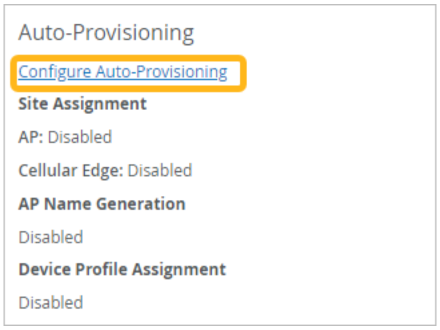
Speed up onboarding and configuration by using auto-provisioning to dynamically assign names to devices based on the device attributes.

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**.



Auto-Provisioning

Configure Auto-Provisioning

Site Assignment

AP: Disabled

Cellular Edge: Disabled

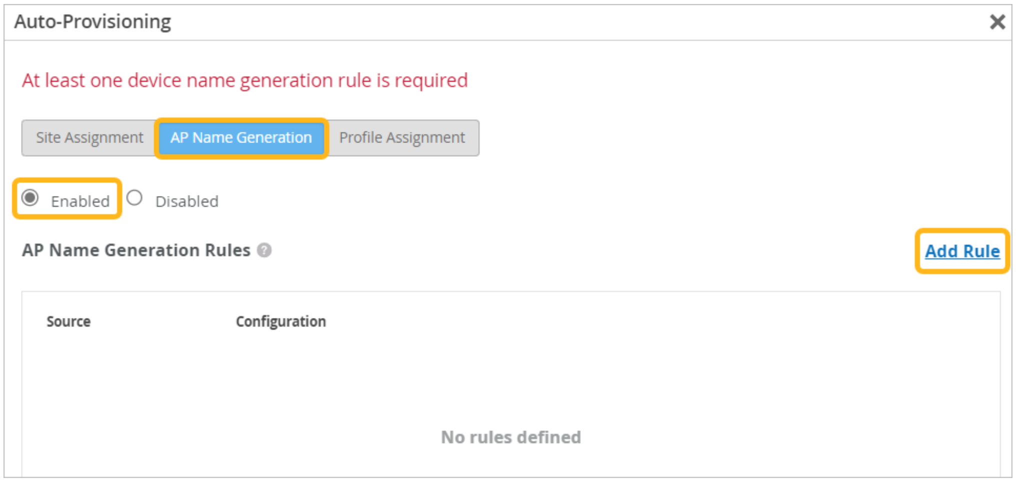
AP Name Generation

Disabled

Device Profile Assignment

Disabled

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



Auto-Provisioning

At least one device name generation rule is required

Site Assignment | AP Name Generation | Profile Assignment

● Enabled ○ Disabled

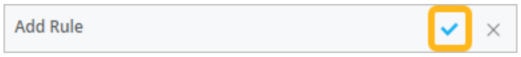
AP Name Generation Rules

Add Rule

Source	Configuration

No rules defined

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 155.
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.

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.

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.

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.

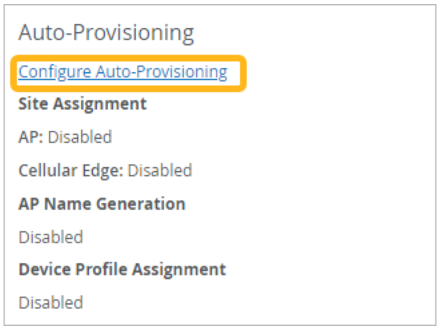
Juniper Mist can automatically assign a device profile based on:

- The Link Layer Discovery Protocol (LLDP) system name of the switch that the AP is connected to. To use this option, configure the LLDP system name to include the device profile name.
- The subnet that the AP is connected to. To use this option, create a list of subnets and their corresponding device profiles when you configure the auto-provisioning rule.
- 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.

- The AP's Domain Name System (DNS) suffix. To use this option, configure each DNS suffix 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**.



Auto-Provisioning

Configure Auto-Provisioning

Site Assignment

AP: Disabled

Cellular Edge: Disabled

AP Name Generation

Disabled

Device Profile Assignment

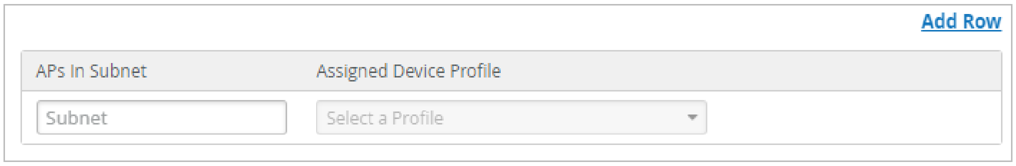
Disabled

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 information and examples, see "Manipulate Source Strings for Auto-Provisioning" on page 155.

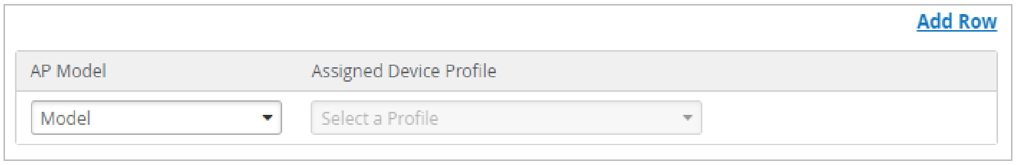
   - Subnet—Complete the subnet/profile table at the bottom of the Auto-Provisioning window. On the left, enter the first subnet, using the format *x.x.x.x/x*. On the right, select the site that you want to assign that subnet to. For each additional subnet, select **Add Row**, and then enter the subnet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



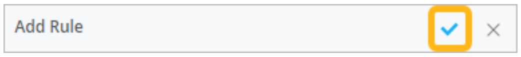
Add Row

APs In Subnet	Assigned Device Profile
Subnet	Select a 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

- Divide a String into Segments | **156**
- Ignore Starting or Ending Characters | **157**
- Select the First Characters | **157**
- Add a Prefix or Suffix | **158**
- Using Multiple Transformation Options Together | **159**

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.

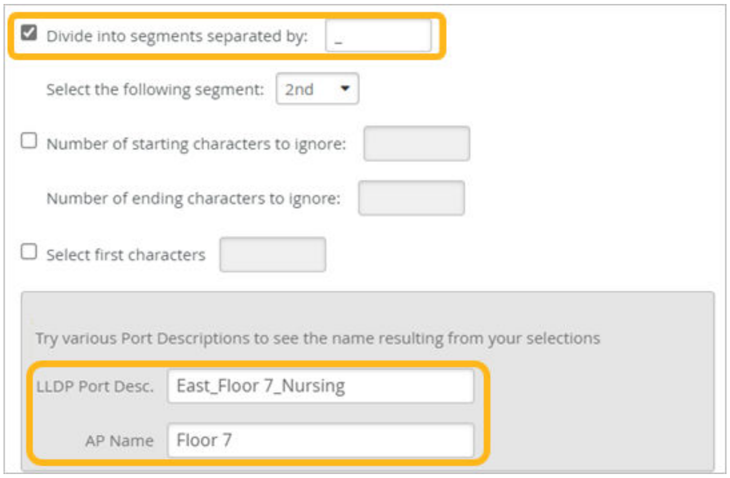
Divide a String into Segments

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.



☑ Divide into segments separated by: _

Select the following segment: 2nd

☐ Number of starting characters to ignore:

Number of ending characters to ignore:

☐ Select first characters

Try various Port Descriptions to see the name resulting from your selections

LLDP Port Desc. East_Floor 7_Nursing

AP Name Floor 7

9. Click **OK**.

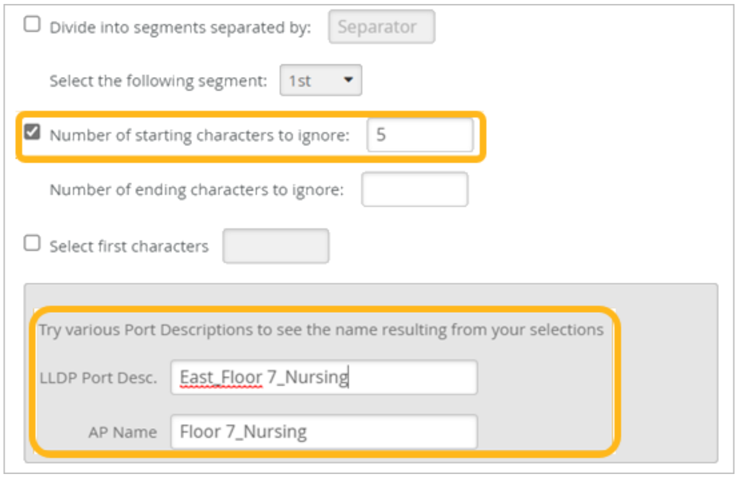
Ignore Starting or Ending Characters

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.



□ Divide into segments separated by: Separator

Select the following segment: 1st

☑ Number of starting characters to ignore: 5

Number of ending characters to ignore:

□ Select first characters

Try various Port Descriptions to see the name resulting from your selections

LLDP Port Desc. East_Floor 7_Nursing

AP Name Floor 7_Nursing

8. Click **OK**.

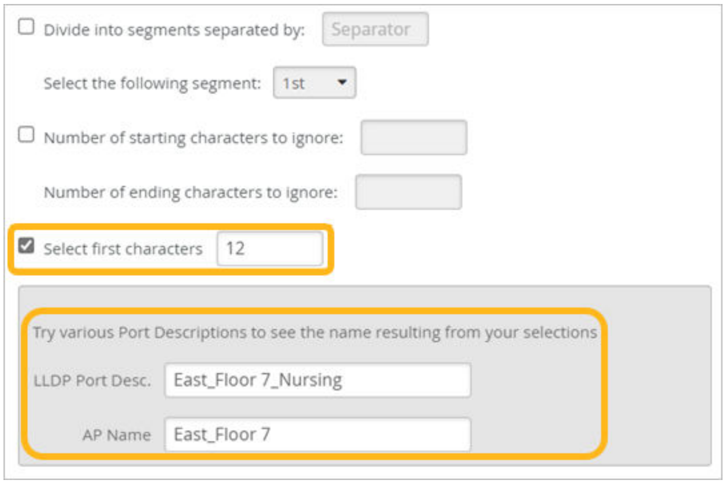
Select the First Characters

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.



□ Divide into segments separated by: Separator

Select the following segment: 1st

□ Number of starting characters to ignore:

Number of ending characters to ignore:

☑ Select first characters 12

Try various Port Descriptions to see the name resulting from your selections

LLDP Port Desc. East_Floor 7_Nursing

AP Name East_Floor 7

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.

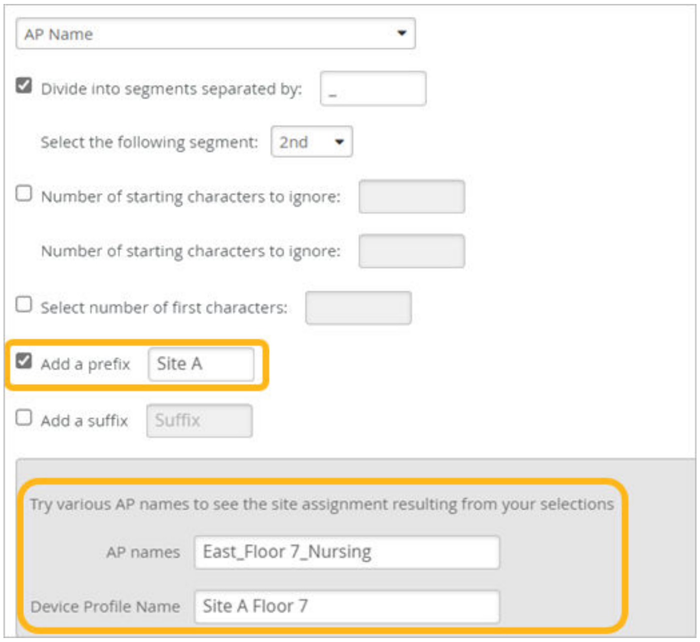
1. On the Organization Settings page, select **Configure Auto-Provisioning**.
2. Select the type of auto-provisioning: **Site Assignment** or **Profile Assignment**.

> **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.



AP Name

☑ Divide into segments separated by: _

Select the following segment: 2nd

☐ Number of starting characters to ignore:

Number of starting characters to ignore:

☐ Select number of first characters:

☑ Add a prefix Site A

☐ Add a suffix Suffix

Try various AP names to see the site assignment resulting from your selections

AP names East_Floor 7_Nursing

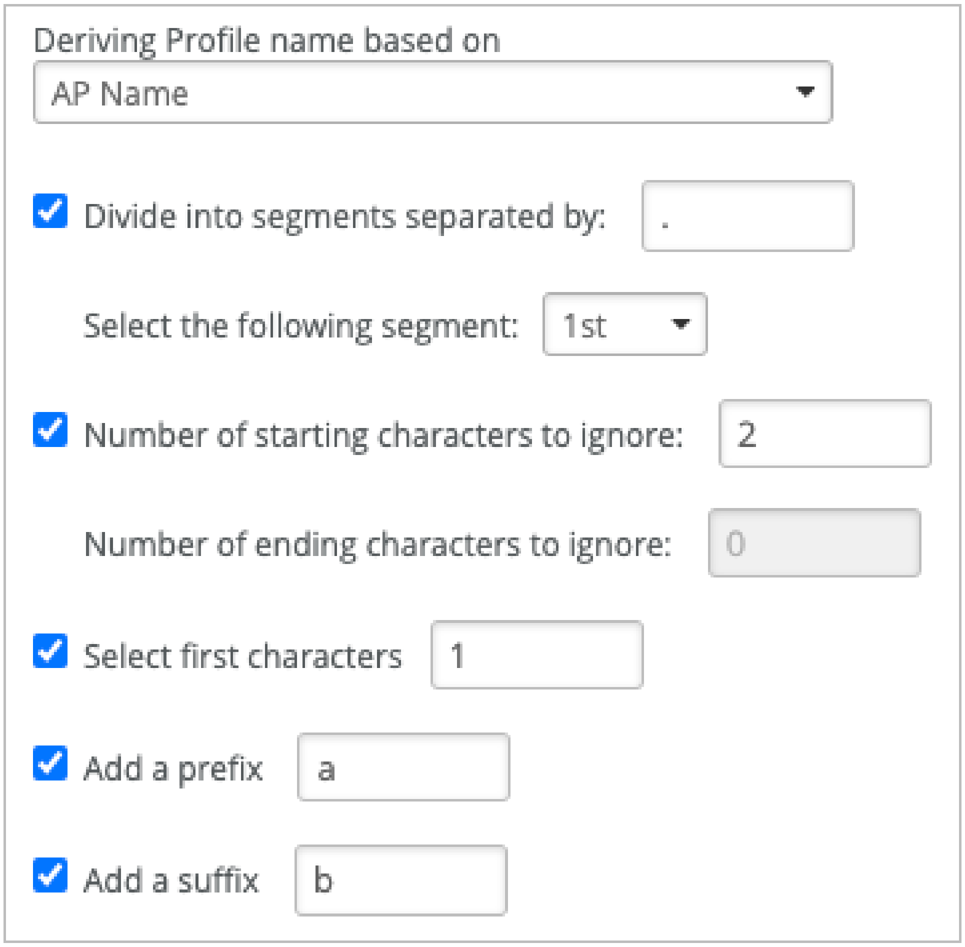
Device Profile Name Site A Floor 7

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.



Deriving Profile name based on

AP Name

☑ Divide into segments separated by: .

Select the following segment: 1st

☑ Number of starting characters to ignore: 2

Number of ending characters to ignore: 0

☑ Select first characters 1

☑ Add a prefix a

☑ Add a suffix b

Let's say that the source string is **1234.5678**.

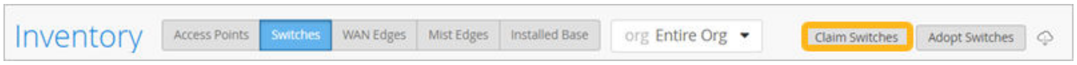
- With the first option, the source string is segmented a the dot (.), and the first segment is selected. The result is **1234**. Only these characters are processed by the next option.
- Next, the first two characters are ignored, resulting in **34**. Only these characters are processed by the next 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

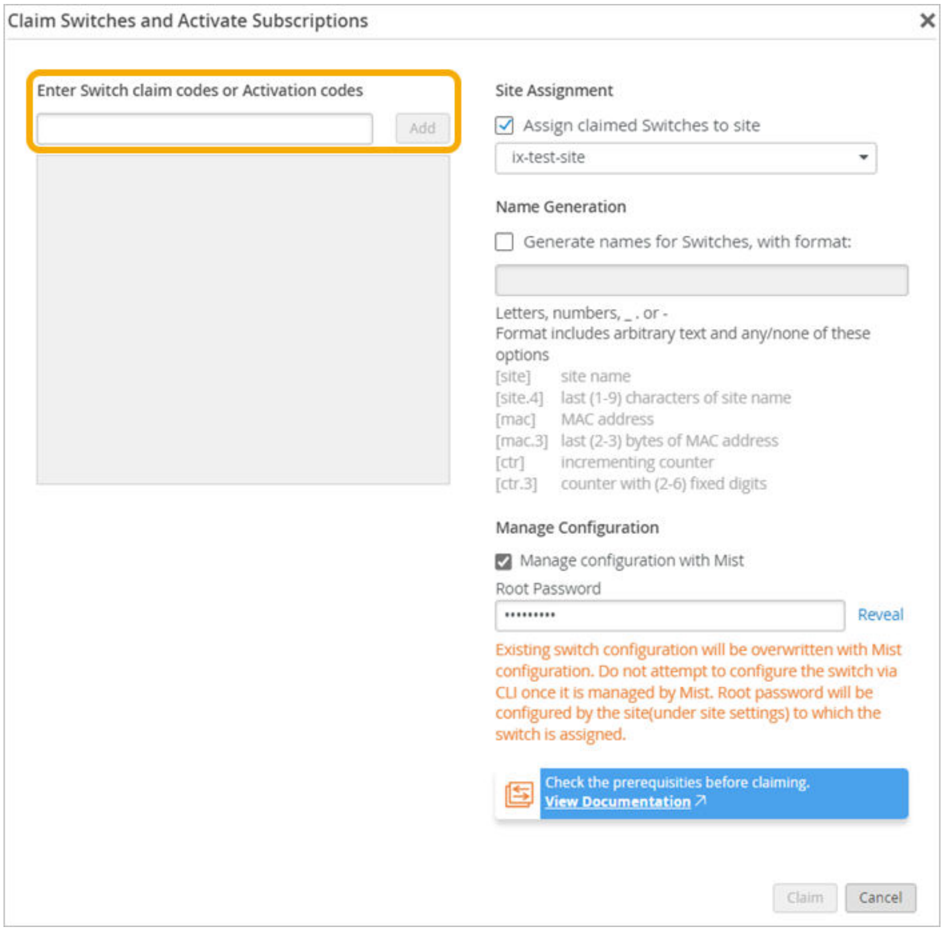
To connect a switch to the Juniper Mist™ cloud, you need to claim it into your Juniper Mist organization.

NOTE: Follow this procedure to claim new switches. If you want to add a switch from your Juniper Installed Base, see "Adopt a Switch from Your Juniper Installed Base" on page 162.

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.



Claim Switches and Activate Subscriptions

Enter Switch claim codes or Activation codes

Site Assignment

☑ Assign claimed Switches to site

ix-test-site

Name Generation

☐ Generate names for Switches, with format:

Letters, numbers, _ . or -
Format includes arbitrary text and any/none of these options

[site]	site name
[site.4]	last (1-9) characters of site name
[mac]	MAC address
[mac.3]	last (2-3) bytes of MAC address
[ctr]	incrementing counter
[ctr.3]	counter with (2-6) fixed digits

Manage Configuration

☑ Manage configuration with Mist

Root Password

•••••••••

Existing switch configuration will be overwritten with Mist configuration. Do not attempt to configure the switch via CLI once it is managed by Mist. Root password will be configured by the site(under site settings) to which the switch is assigned.

Check the prerequisities before claiming.
View Documentation

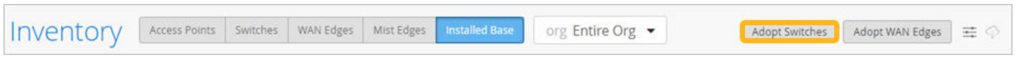
4. Select other options as needed, and then click **Claim**.

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

If you integrated your Juniper account with your Juniper Mist™ account, you need to adopt the switches into your Juniper Mist organization.

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.

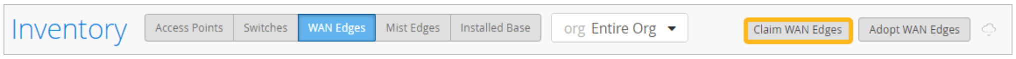
NOTE: For detailed instructions, go to the Juniper Mist Supported Hardware page, and find the Quick Start Guide for your device.

Claim a WAN Edge

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 163.

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.

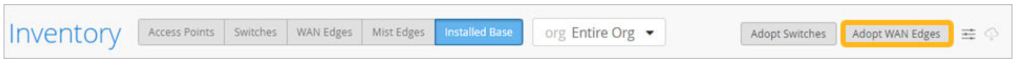
5. Make note of the on-screen information about the impact that this action will have on the existing gateway configuration.
6. Select other options as needed, and then click **Claim**.

> **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

If you integrated your Juniper account with your Juniper Mist™ organization, you need to adopt the WAN Edges into your Juniper Mist organization.

1. From the left menu, select **Organization** > **Admin** > **Inventory**.
2. Click **Installed Base** at the top center of the page, and then click **Adopt WAN Edges** at the top right.



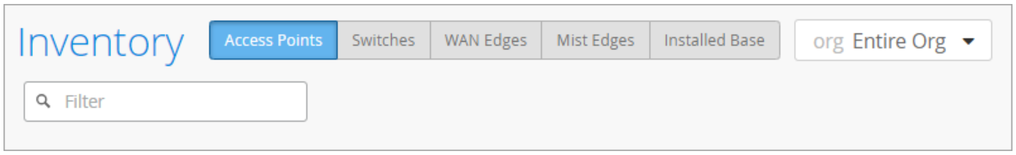
> **NOTE**: You also can adopt WAN Edges on the WAN Edges page.

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.

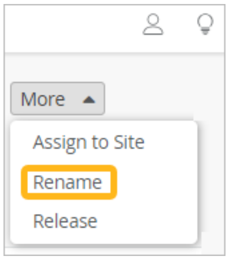
> **NOTE**: For detailed instructions, go to the Juniper Mist Supported Hardware page, and find the Quick Start Guide for your device.

Rename Devices

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**.

Device Management with the Juniper Mist AI Mobile App

IN THIS SECTION

- Download the App | 165
- Supported User Roles | 165
- Log In | 165
- Device Inventory | 166
- Claim Devices | 167
- Sites | 167

AP Details | 167

Identify APs | 168

The Mist AI™ app can help to streamline your installation process.

Download the App

You can download the Mist AI app 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 10 or later.

Supported User Roles

These user roles can use the Mist AI app:

- Superusers
- Installers
- Observers
- Network admins who have access to all sites in the organization

NOTE: The app does not allow access by network admins who only have access to specific sites within the organization.

Log In

To log in to the app, you need to know:

- The email address and password for your Juniper Mist login. An administrator must add you as a user in the Juniper Mist portal. Your user account must have either the Admin or the Installer role.
- The name of your Juniper Mist organization.
- The environment for your Juniper Mist organization. You can easily identify your environment by looking at the URL for your Juniper Mist portal.

Table 45: URLs and Environments

Juniper Mist Portal URL	Environment to Select in Mist AI App
manage.mist.com	Production-AWS
manage.gc1.mist.com	Production-GCP
manage.ac2.mist.com	AWS-East
manage.gc2.mist.com	Production-GCP-Canada
manage.eu.mist.com	EU
manage.ac5.mist.com	Production-APAC

Device Inventory

On the homepage, tap **Device Inventory** to view information about all devices that have been claimed by this organization.

On the Device Inventory page, you can:

- Use the tabs at the top to select a device type.
- Scroll or search to find a device.
- Unassign a device—Tap the device, and then tap **Unassign**.
- Add a new device—Tap **+** in the top right corner. Then scan the QR code or enter the claim code.
- Tap an AP to go to the AP Details page.

Claim Devices

You can claim devices in several ways:

- On the homepage, tap **Claim Devices to Org**.
- On other pages, tap **+** in the top right corner.

Then scan the QR code or enter the claim code.

Sites

On the homepage, under Sites, tap a site to go to the Site page, where you can see the assigned APs and floorplans.

On the Site page, you can:

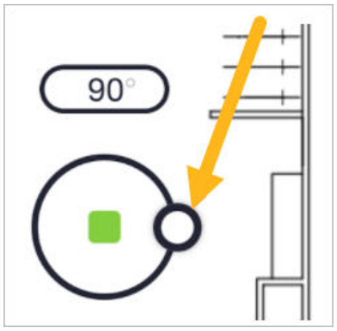
- Tap **+** in the top right corner to claim an AP. Then scan the QR code or enter the claim code.
- Tap an AP to go to the AP Details page.

AP Details

From the Device Inventory page or Site page, select an AP to go to the AP Details page. On this page, 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 flashing.
- Tap **Name** to change the AP name. Then enter the new name.
- Tap **Status** to see if the AP is connected or disconnected.
- To view additional information about an AP, tap **Mac Address**, **Uptime**, or **Version.**
- Verify an AP's location (available in the IOS version of the Mist AI app only). To begin, turn on **Verify AP** at the bottom of the page. Tap an AP, and note if the AP placement is GOOD or BAD.
- Tap **Replace device**.
- Place an AP on the floorplan. If the Map field contains the **Place on a map** link, this means that the AP has not yet been added to a floorplan. Click 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.



Identify APs

This option is only available in the IOS version of the Mist AI app. Use this option to scan for nearby APs.

On the homepage, tap **Identify APs**, and then tap **Scan** to start scanning.

NOTE: Before scanning, enable Bluetooth on your device. Also ensure that the following tasks have been completed in the Juniper Mist portal:

- Enable vBLE Engagement on the Organization Settings page.
- Place all APs on a floorplan.

6

CHAPTER

Sites

Configure a Site | 170

Site Configuration Settings (Page Reference) | 171

Set the Site Location | 179

Site Groups | 180

Assign, Unassign, and Manage Site Groups | 181

Set the Engagement Dwell Limits and Schedule for a Site | 182

Set Up Occupancy Analytics for a Site | 183

Configure Site Variables | 185

Configure a Site

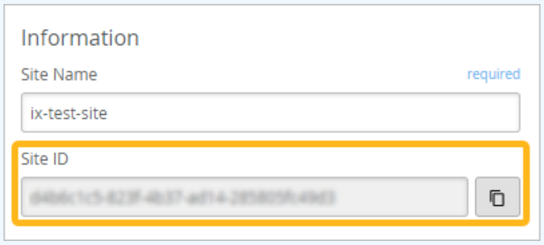
Use sites to configure and manage different physical locations or logical sub-divisions of your organization. For example, each site can have different RF templates and access point settings, different firmware upgrade schedules, and different settings for features such as location services, occupancy 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 179. For information about other settings, see"Site Configuration Settings (Page Reference)" on page 171 .

    > **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.

    Information

    Site Name required

    ix-test-site

    Site ID

    [redacted]

    - 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)

IN THIS SECTION

- Finding the Site Configuration Page | 171
- Major Sections of the Site Configuration Page | 171

Finding the Site Configuration Page

From the left menu, select **Organization** > **Admin** > **Site Configuration**.

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 46: 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 179
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*

Table 46: Site Configuration Settings *(Continued)*

Section	Description	More Information
Site Groups	For more efficient configuration and management, add similar sites to site groups.	"Site Groups" on page 180
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
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.	

Table 46: Site Configuration Settings *(Continued)*

Section	Description	More Information
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.	
Switch Management	Enter the root password and enable or disable switch proxy.	
WAN Edge Management	Enter the root password.	
Session Smart Conductor	Enter up to two comma-separated IP addresses.	

Table 46: 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 182
Occupancy Analytics	Set the parameters for the occupancy data on the Occupancy Analytics page.	"Set Up Occupancy Analytics for a Site" on page 183
Webhooks	Add and manage webhooks, which push notifications of Juniper Mist alarms and events to a server that you specify.	Juniper Mist Automation and Integration Guide

Table 46: 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 46: 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 46: 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 46: 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 185

Table 46: Site Configuration Settings *(Continued)*

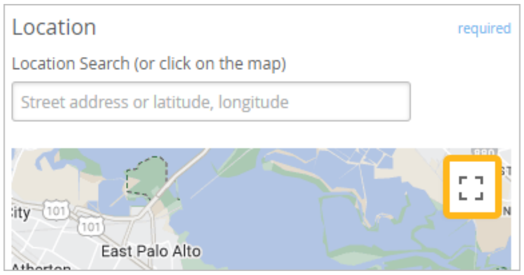
Section	Description	More Information
Zones	A proximity zone is an RSSI-based feature that applies to individual or grouped APs. RSSI data from the clients triggers the zone entry and exit events. To add a zone, click the button. In the Generate Proximity Zones window, select the check boxes for the APs 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

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.


Location

required

Location Search (or click on the map)

Street address or latitude, longitude

- 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

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.

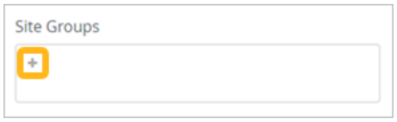
- You can add a site to multiple groups. For example, you can assign a site to your Large Stores group and your Southwest Region group.
- You can apply a WLAN template to a site group that contains a site with unique settings. To bypass the template settings for that site, mark that site as an exception.

For information about managing site groups, see "Assign, Unassign, and Manage Site Groups" on page 181.

Assign, Unassign, and Manage Site Groups

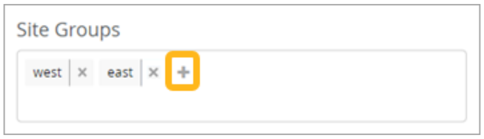
Site groups can help you to manage your sites more efficiently. Use the Site Configuration page to assign and make changes to site groups.

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.

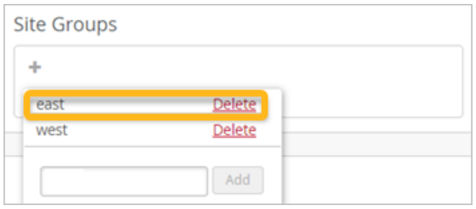
   - To create a site group and assign this site to it, click **+** (the plus sign). Then enter the new group name in the text box and click **Add**. Juniper Mist creates the site group and assigns this site to the new group.
   - To unassign this site from a listed site group, click **X** (the close icon) 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

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

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:

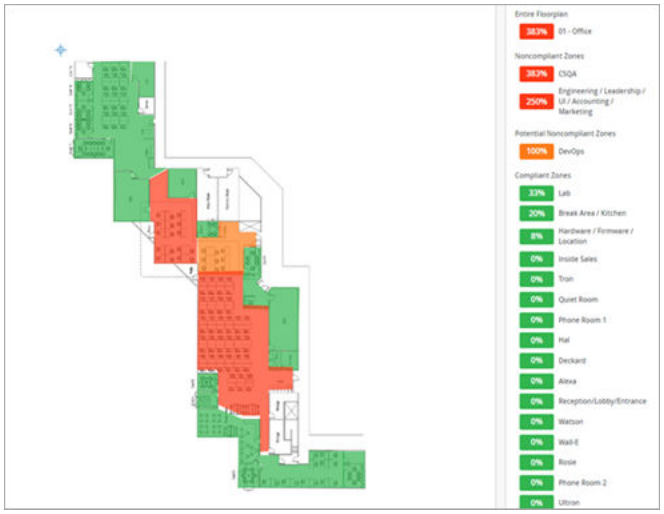
1. From the left menu, select **Organization** > **Admin** > **Site Configuration**.
2. Select the site that you want to set up.
3. Under Occupancy Analytics, enter the settings.

   - 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).

   - 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.



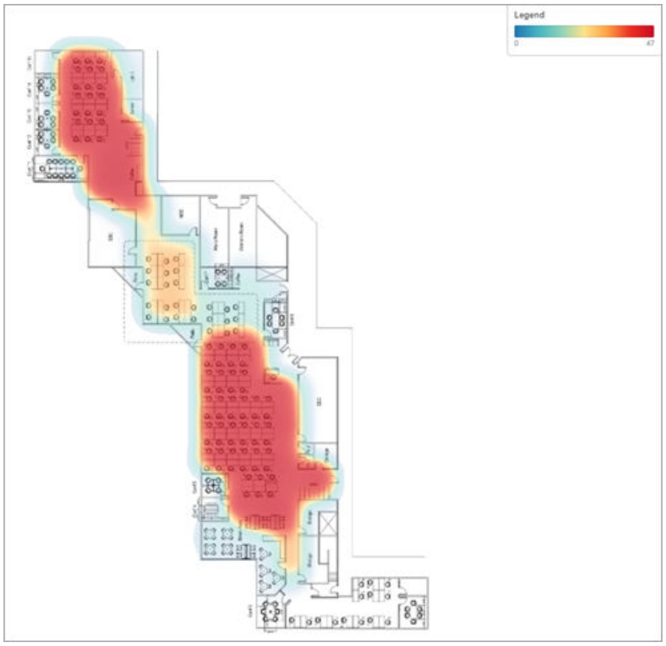
Entire Floorplan
383% 01 - Office

Noncompliant Zones
383% CSQA
250% Engineering / Leadership / UI / Accounting / Marketing

Potential Noncompliant Zones
100% DevOps

Compliant Zones
33% Lab
20% Break Area / Kitchen
8% Hardware / Firmware / Location
0% Inside Sales
0% Tron
0% Quiet Room
0% Phone Room 1
0% Hal
0% Deckard
0% Alexa
0% Reception/Lobby/Entrance
0% Watson
0% Wall-E
0% Rosie
0% Phone Room 2
0% Ultron

- 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.



- 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.
- 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

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.

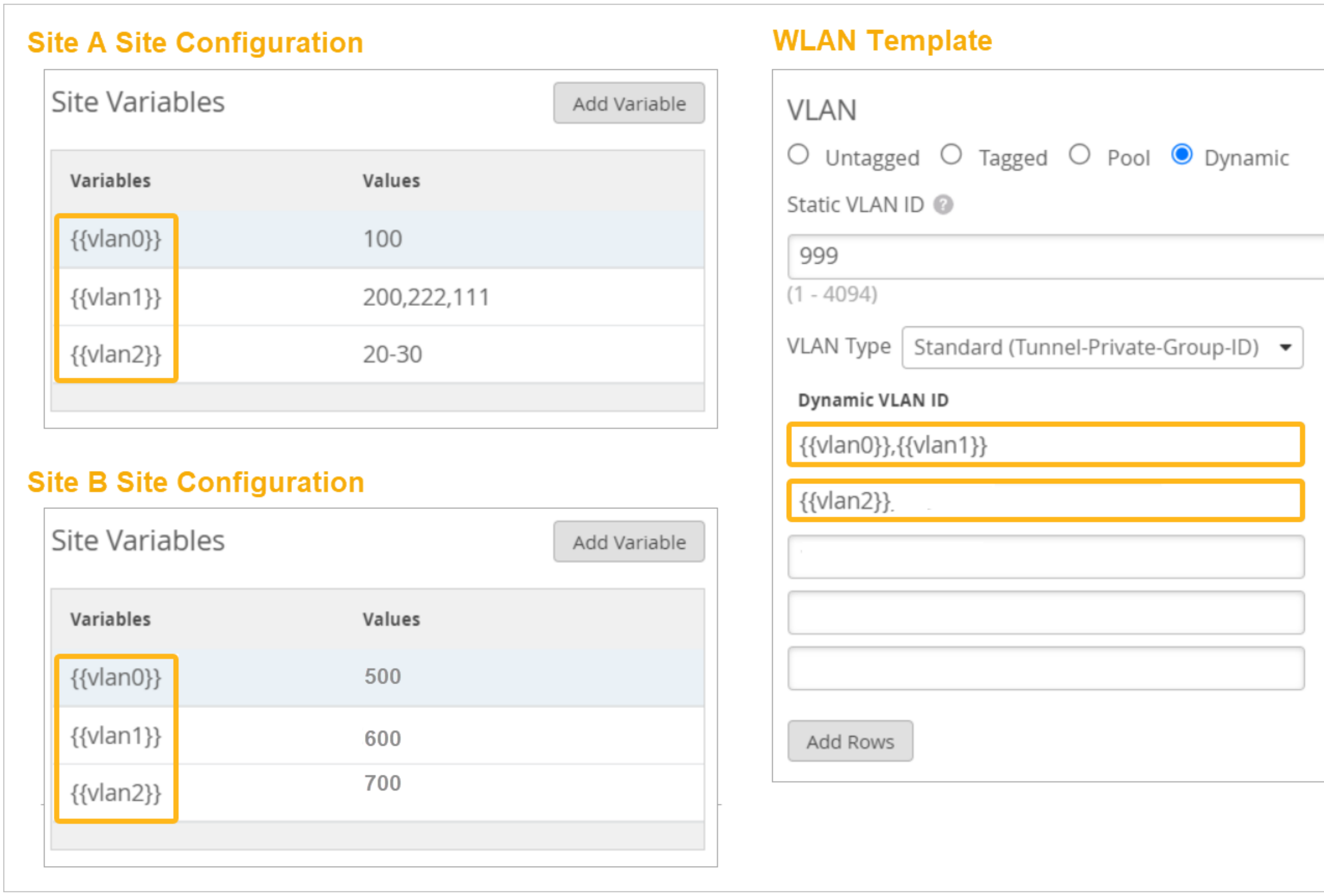
Naming Syntax

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.



Site A Site Configuration

Site Variables

Variables	Values
{{vlan0}}	100
{{vlan1}}	200,222,111
{{vlan2}}	20-30

Site B Site Configuration

Site Variables

Variables	Values
{{vlan0}}	500
{{vlan1}}	600
{{vlan2}}	700

WLAN Template

VLAN

○ Untagged ○ Tagged ○ Pool ● Dynamic

Static VLAN ID: 999

(1 - 4094)

VLAN Type: Standard (Tunnel-Private-Group-ID)

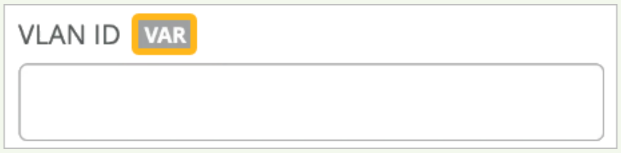
Dynamic VLAN ID

{{vlan0}},{{vlan1}}

{{vlan2}}

- 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.

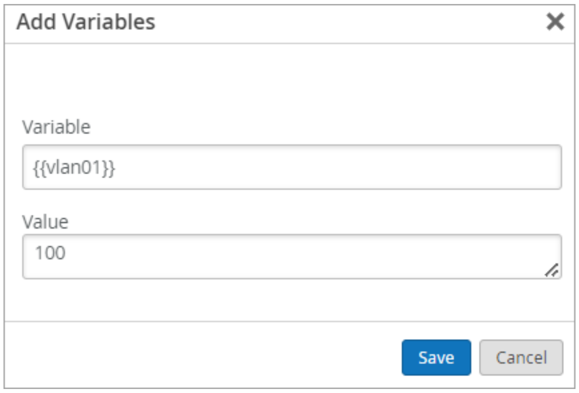
TIP: When working on configuration screens, look for the VAR indicators. Fields with this indicator allow site variables.



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**.

      Variable

      {{vlan01}}

      Value

      100

    - 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.

7

CHAPTER

Help and Support

Create a Support Ticket | 189

Feature Requests | 194

View Your Support Tickets | 197

Find Information and Instructions for Juniper Mist | 198

Create a Support Ticket

If issues occur and you need help, create a support ticket. You can get help with general questions, subscriptions, configuration options, merchandise returns, device outages, and network-wide issues.

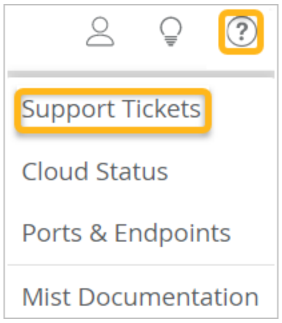
TIP: As you create your ticket, be aware of features that can help you to resolve the issue on your own:

- 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.

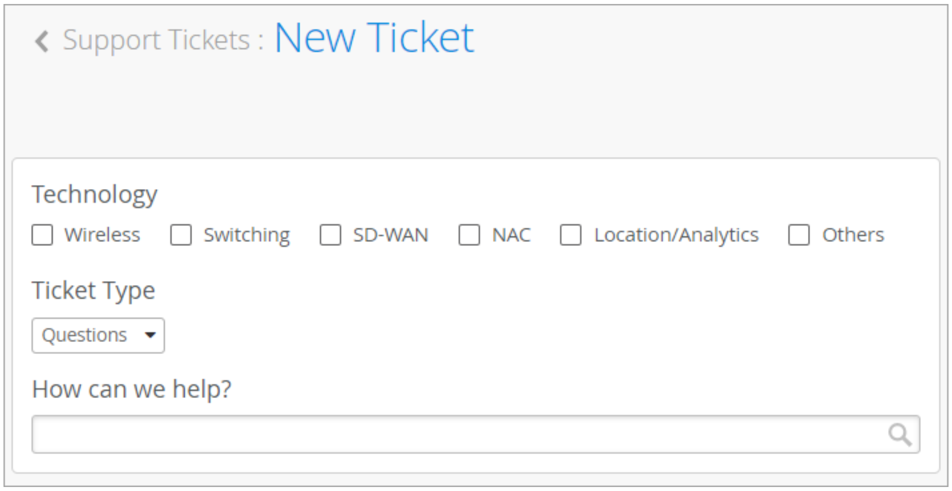
- For certain ticket types, Marvis subscribers will see Marvis buttons on the support form. Click to start troubleshooting with Marvis. You can resolve many types of issues this way.

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**.



< Support Tickets : New Ticket

Technology

□ Wireless □ Switching □ SD-WAN □ NAC □ Location/Analytics □ Others

Ticket Type

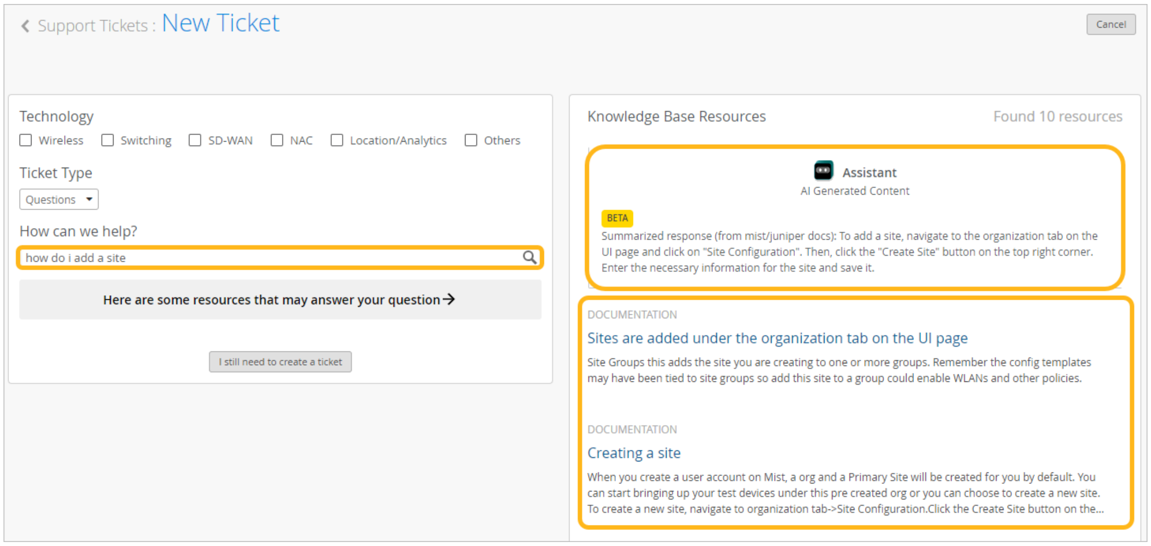
Questions ▾

How can we help?

NOTE: The available options depend on which ticket type is selected.

4. Select a **Ticket Type**.

- **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**.



< Support Tickets : New Ticket

Technology

□ Wireless □ Switching □ SD-WAN □ NAC □ Location/Analytics □ Others

Ticket Type

Questions ▾

How can we help?

how do i add a site

Here are some resources that may answer your question →

Knowledge Base Resources

Found 10 resources

Assistant

AI Generated Content

BETA

Summarized response (from mist/juniper docs): To add a site, navigate to the organization tab on the UI page and click on "Site Configuration". Then, click the "Create Site" button on the top right corner. Enter the necessary information for the site and save it.

DOCUMENTATION

Sites are added under the organization tab on the UI page

Site Groups this adds the site you are creating to one or more groups. Remember the config templates may have been tied to site groups so add this site to a group could enable WLANs and other policies.

DOCUMENTATION

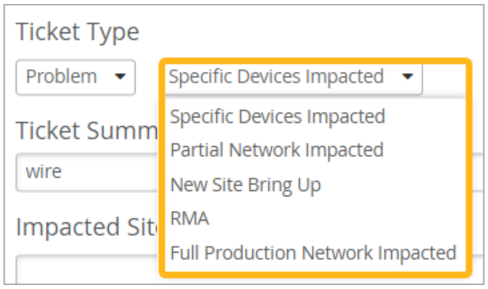
Creating a site

When you create a user account on Mist, a org and a Primary Site will be created for you by default. You can start bringing up your test devices under this pre created org or you can choose to create a new site. To create a new site, navigate to organization tab->Site Configuration.Click the Create Site button on the...

- **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.

- **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.

  Ticket Type: Problem

  Specific Devices Impacted

  Ticket Summ: wire

  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 to request a Return Merchandise Authorization.
  - **Full Production Network Impacted**—The problem affects most or all of your network.

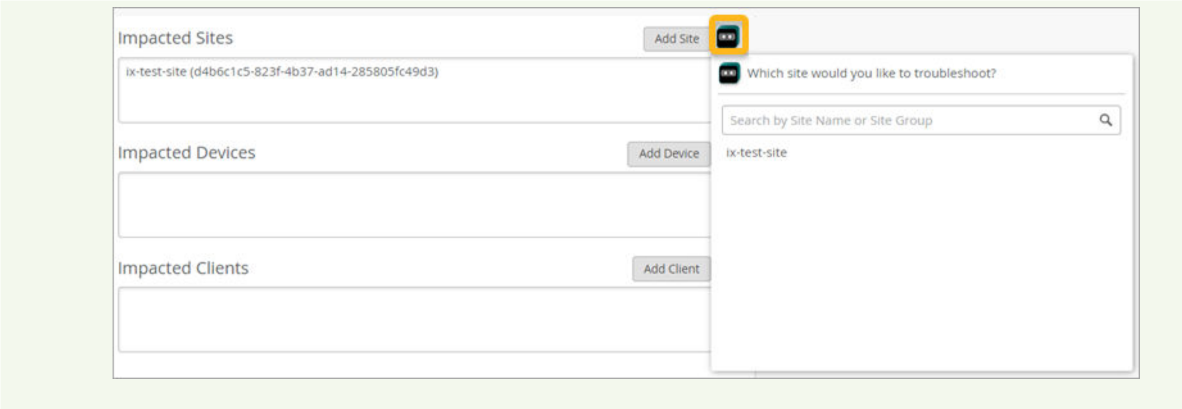
- **Onboarding Help for New Deployment**—Select this ticket type only if you're doing a new deployment. You'll get assistance with initial setup, configuration, and basic troubleshooting. Available only when the **Technology Type** is wireless, switching, or SD-WAN.

  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



Impacted Sites: ix-test-site (d4b6c1c5-823f-4b37-ad14-285805fc49d3)

Which site would you like to troubleshoot?

Search by Site Name or Site Group

ix-test-site

To complete the other fields, follow these tips.

Table 47: 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 47: 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 47: 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.)

6. Click **Submit Ticket**.

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

Feature Requests

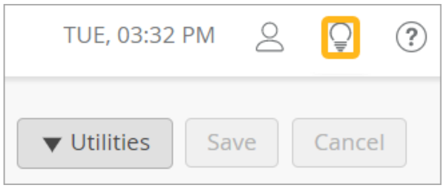
SUMMARY

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

- Submit a Feature Request | 195
- View the Feature Requests | 196
- Respond to Other Users' Feature Requests | 197

To go to the Product Features pages, click the lightbulb icon (near the top right corner of the Juniper Mist portal).



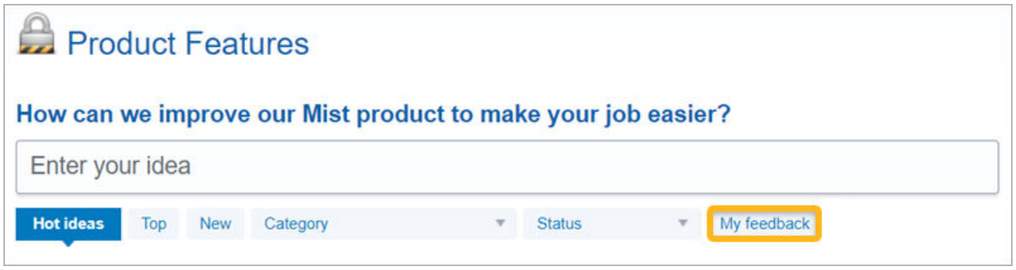
On this page, you can:

- "Submit a Feature Request" on page 195
- "View the Feature Requests" on page 196

"Respond to Other Users' Feature Requests" on page 197

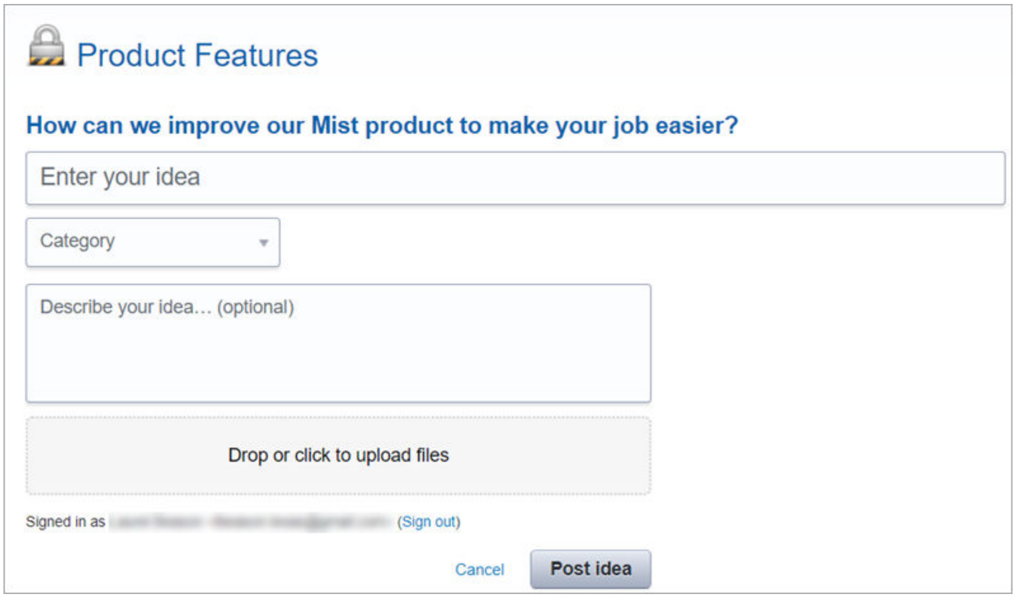
Submit a Feature Request

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.



Product Features

How can we improve our Mist product to make your job easier?

Enter your idea

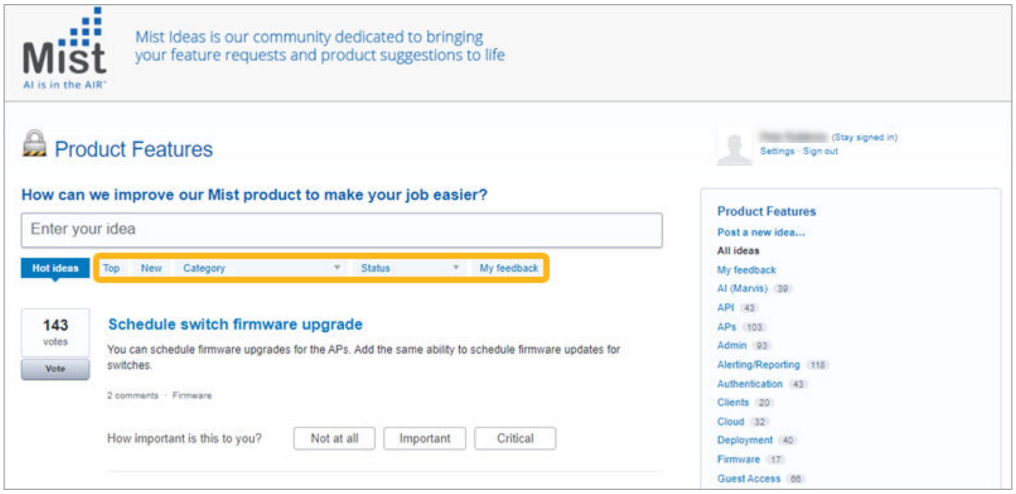
Describe your idea… (optional)

Signed in as [redacted] (Sign out)

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.



Mist Ideas is our community dedicated to bringing your feature requests and product suggestions to life

Product Features

How can we improve our Mist product to make your job easier?

Enter your idea

[redacted] (Stay signed in)

143 votes

Schedule switch firmware upgrade

You can schedule firmware upgrades for the APs. Add the same ability to schedule firmware updates for switches.

2 comments · Firmware

How important is this to you?

- 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.

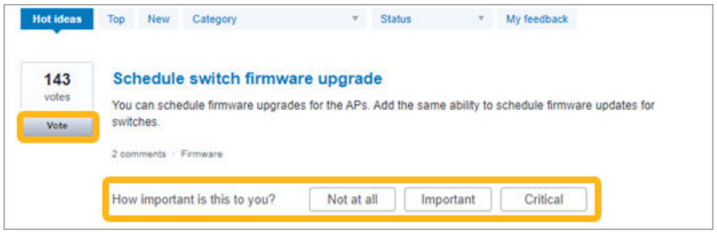
- Category—Filter the list based on the category that the user assigned when creating the request.

> **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.



Schedule switch firmware upgrade

You can schedule firmware upgrades for the APs. Add the same ability to schedule firmware updates for switches.

2 comments · Firmware

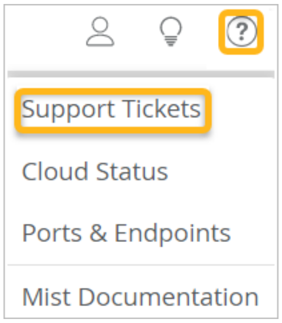
How important is this to you?

- 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**.

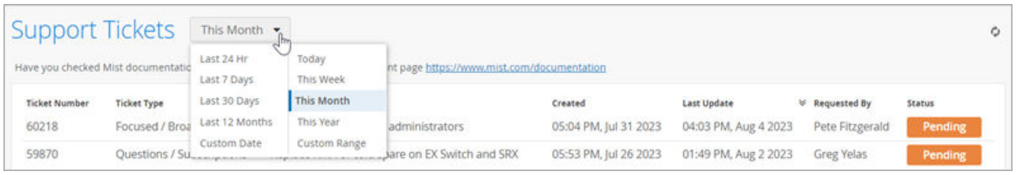
View Your Support Tickets

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.



Have you checked Mist documentatic nt page https://www.mist.com/documentation

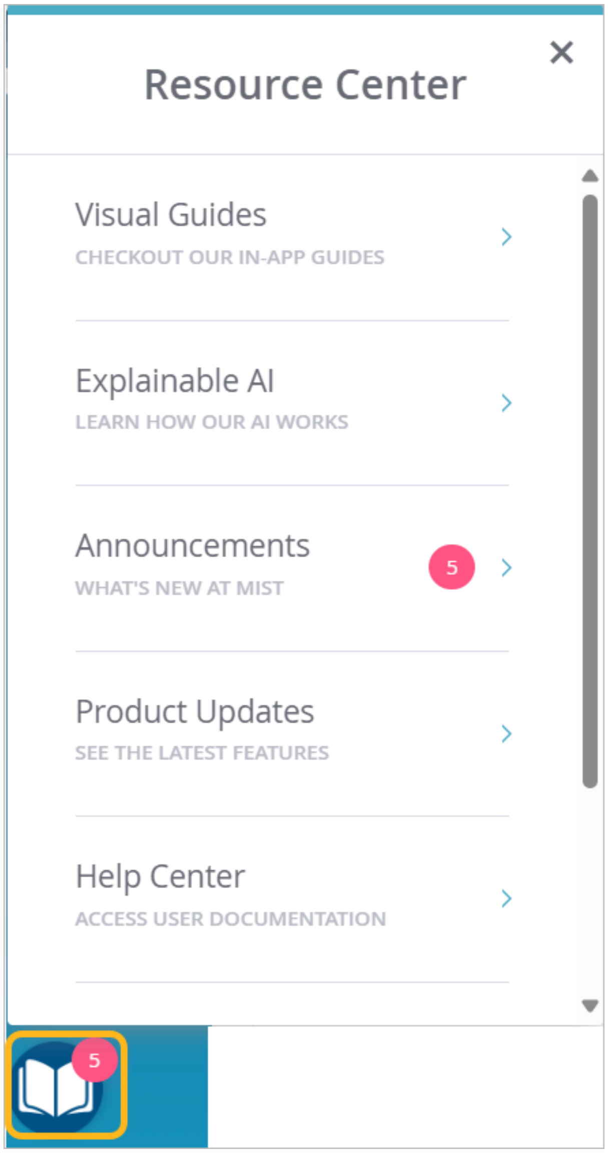
Ticket Number	Ticket Type		Created	Last Update	Requested By	Status
60218	Focused / Broa	administrators	05:04 PM, Jul 31 2023	04:03 PM, Aug 4 2023	Pete Fitzgerald	Pending
59870	Questions / Su	are on EX Switch and SRX	05:53 PM, Jul 26 2023	01:49 PM, Aug 2 2023	Greg Yelas	Pending

3. Click the ticket that you want to view.

Find Information and Instructions for Juniper Mist

In the Juniper Mist™ portal, use these features to find information and instructions:

- Resource Center—Click the book icon (at the bottom of the left menu) to open the Resource Center.



Resource Center

Visual Guides
CHECKOUT OUR IN-APP GUIDES

Explainable AI
LEARN HOW OUR AI WORKS

Announcements 5
WHAT'S NEW AT MIST

Product Updates
SEE THE LATEST FEATURES

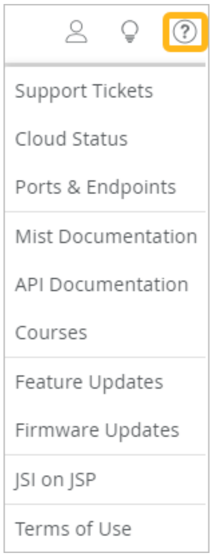
Help Center
ACCESS USER DOCUMENTATION

5

The Resource Center includes:

  - Visual Guides—Interactive tutorials that lead you step by step through common tasks
  - Explainable UI—Essential concepts presented in whiteboard videos
  - Announcements—Information about new features, security advisories, and more
  - Product Updates—Juniper Mist release notes
  - Help Center—Juniper Mist help topics

- Question menu—Click the question icon (at the top-right corner of the page) and then select a menu option.



- Mist Documentation—Juniper Mist help topics
- API Documentation—Developer documentation
- Courses—Juniper Mist training
- Feature Updates—Release notes for Juniper Mist
- Firmware Updates—Release notes for Juniper device firmware
- Terms of Use—End User License Agreement