

Juniper Mist AI Wired workshop

PUBLICATION INFO: THE AMERICAN JOURNAL OF ENGINEERING AND TECHNOLOGY (ISSN: 2689-0984)

ISBN: -978-1-957653-71-6

CROSSREF DOI: - <https://doi.org/10.37547/tajet/book-26-03>

PUBLISHED DATE: -29 JULY 2026

LAB GUIDE

Version: 1.0

IGOR CHINCHAK

COMPUTER DATA INC | Southfield, MI, US

<u>Lab 1: Testing Lab Connectivity</u>	3
<u>Task 1-1: Remote Lab access</u>	5
<u>Task 1-2: Testing connectivity</u>	6
<u>Task 1-3: HPE Juniper Networking Mist AI access</u>	9
<u>Task 1-4: HPE Aruba Networking Central access</u>	18
<u>Lab 2: Day 0: Onboard Juniper EX switch to Mist AI</u>	24
<u>Task 2-1: Create Site and Switch Template in Mist AI</u>	25
<u>Task 2-2: Adopt Juniper EX Switch in Mist AI and assign to Site</u>	34
<u>Task 2-3: Validate and monitor Juniper EX Switch connectivity to Mist AI</u>	43
<u>Task 2-4: General switch configuration</u>	56
<u>Lab 3: Day 1: Configure VLANs, ports and LAGs</u>	64
<u>Task 3-1: Port profiles and networks configuration</u>	65
<u>Task 3-2: LAG configuration</u>	88
<u>Task 3-3: Dynamic port configuration</u>	94
<u>Task 3-4: Network Access Control</u>	107
<u>Lab 4: Day 2: Wired network Monitoring and Troubleshooting</u>	128
<u>Task 4-1: Wired Visibility</u>	129
<u>Task 4-2: Monitor with Service Levels</u>	141
<u>Task 4-3: Marvis Actions</u>	156
<u>Task 4-4: Packet Capture for Wired client traffic</u>	166
<u>Lab 5: Configuration Scalability</u>	173
<u>Task 5-1: Use Site variables</u>	174
<u>Task 5-2: Use CLI Configuration in Mist AI</u>	185
<u>Task 5-3: Use Select Switches Configuration</u>	197
<u>Task 5-4: Use bulk upload of switch configuration</u>	219

Lab 1: Testing Lab connectivity

Objectives

After completing this lab, you will become familiar with the lab environment and prepare for the workshop activities.

Overview

The Remote Lab provides with all required equipment to complete the workshop activities. You should know the purpose and access procedures for this equipment. Juniper Mist web UI could be changed over the time and will not match screenshots in this workshop. Ask your instructor for assistance if you struggle finding required settings in Juniper Mist.

MGMT PC: This client is used for remote lab management access, traffic analysis, and to access the switch's CLI via SSH.

PC-1: This wired and wireless client is used for connectivity testing.

PC-4: This wired and wireless client is used for connectivity testing.

Edge-1 switch: This is the AOS-CX edge switch.

Edge-2 switch: This is the Junos OS EX4100 edge switch.

Core-1 switch: This is the primary AOS-CX core switch.

Core-2 switch: This is the secondary AOS-CX core switch.

Core router: This is preconfigured virtual AOS-CX core switch used to connect table devices to Internet.

AP-1: This is the HPE Aruba Networking AP connected to your Edge-1 on port 1/1/2.

AP-2: This is the HPE Juniper Networking AP connected to the Edge-2 port on 0/0/2.

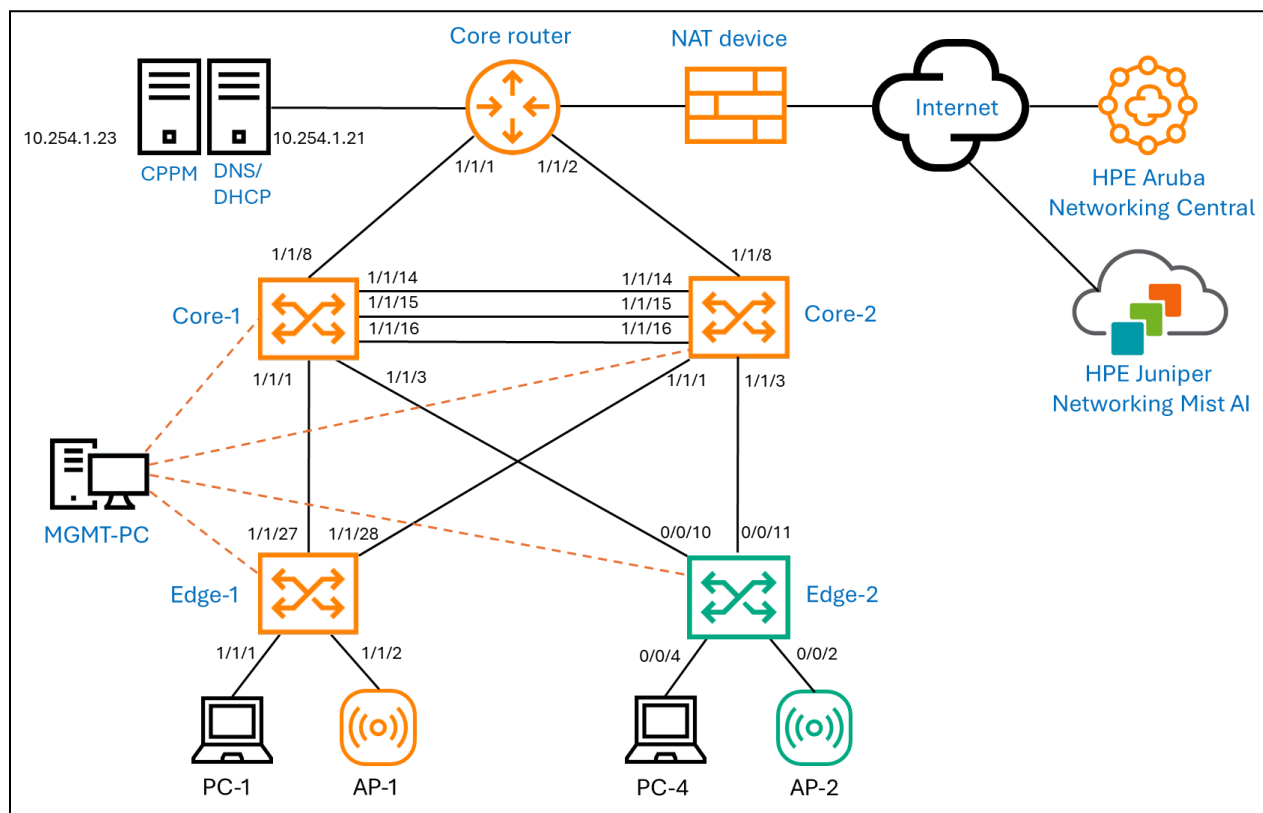
OOBM switch: You have NO access to this switch; it connects the OOBM ports of the lab switches.

DNS/DHCP: This server provides DHCP, DNS, and NTP services for the lab devices. You have NO access to this server.

CPPM: This is ClearPass Policy Manager server, an AAA RADIUS solution for your network environment.

HPE Aruba Networking Central: This is Cloud-Native network management and automation platform access with assigned table credentials.

HPE Juniper Networking Mist AI: This is AI-Native, cloud-based network management and automation platform access with assigned table credentials.



Task 1-1: Remote Lab access

Objectives

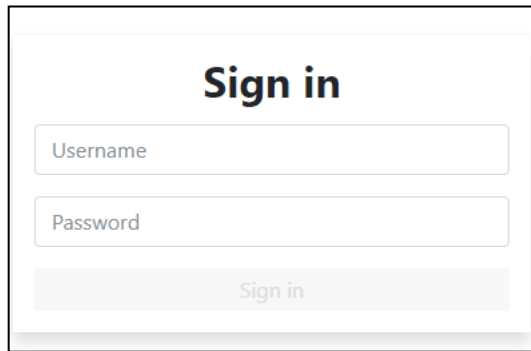
Validate remote lab connectivity and ability to log in.

Ensure that you have remote lab access during this workshop.

Steps

Launch a web browser in *private* or *incognito* mode on your local computer and access the Remote Lab web portal at the URL: <https://arubatraininglab.computerdata.com>.

Enter your *username* and *password* and click the **Sign in** button (alternatively use a link from email if you receive it after the registration for this workshop).

A screenshot of a web form titled "Sign in". The form has a light gray background and a white border. It contains two input fields: "Username" and "Password", both with light gray borders and placeholder text. Below the input fields is a "Sign in" button with a light gray background and dark gray text. The entire form is centered on a white background.

Sign in

Username

Password

Sign in

Task 1-2: Testing connectivity

Objectives

Test connectivity and admin credentials for each of the devices.

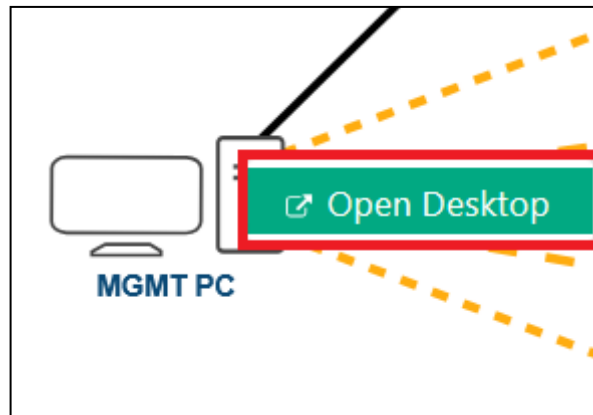
Connect and log into the lab devices and client PCs using Remote Lab network diagram.

Steps

MGMT PC

The MGMT PC is used for remote device management access.

To connect to the **MGMT PC** desktop, right-click the lab diagram icon and select **Open Desktop**.



A new browser tab will open with a remote desktop. Verify that you can view the remote desktop.

Edge-2

This is Juniper EX 4100 switch where Juniper access point and PC-4 testing client are connected. This switch is not provisioned in Mist AI yet and will be provisioned and managed in Mist AI in the following labs.

Locate MTPuTTY or Putty application on **MGMT PC** Desktop and launch it.

Connect to Edge-2 switch with SSH using saved session or type IP address **10.251.1.10**.

Login with **admin/Aruba123!** credentials. Verify the hostname is **sw-edge**.

```
login as: admin
Keyboard-interactive authentication prompts from server:
| Password: Aruba123!
End of keyboard-interactive prompts from server
Last login: Sun Apr 19 18:41:45 2026 from 10.251.1.90
--- JUNOS 22.4R3.25 Kernel 64-bit  JNPR-12.1-20231013.108e0b3_buil
{master:0}
admin@sw-edge>
```

Take note of the Juniper EX switch information. Enter command “show system information”.

```
admin@sw-edge> show system information
Model: ex4100-f-12t
Family: junos-ex
Junos: 22.4R3.25
Hostname: sw-edge
```

Confirm that there is only admin user configured on the switch with “show configuration system login” command. Make sure user mist is configured.

```
admin@sw-edge> show configuration system login
user admin {
    uid 2000;
    class super-user;
    authentication {
        encrypted-password
"$6$iY04D4zw$lEf8yFF.pIlI1fOV8sVa/owtdcvg87oWECsEeilHFDyM6uNa2mIpyBshg6ArI3gl0yvKKrsFCEe
GBiFKvGd0u1"; ## SECRET-DATA
    }
}
```

Core-1 and Core-2

These 6300 AOS-CX switches are preconfigured as VSX peers with VLANs, SVIs and VSX LAGs.

Open SSH connection from **MGMT PC** to **Core-1** using saved sessions or type IP address **10.251.1.2**.

Log in with **admin/Aruba123!** credentials. Verify the prompt is **sw-core1**.

```
login as: admin
admin@10.251.1.2's password: Aruba123!
sw-core1#
```

Validate VSX cluster state on **sw-core1** with “show vsx status” command.

```
sw-core1# show vsx status
VSX Operational State
-----
ISL channel      : In-Sync
ISL mgmt channel : operational
Config Sync Status : In-Sync
NAE              : peer_reachable
HTTPS Server     : peer_reachable

Attribute          Local          Peer
-----
ISL link           lag256         lag256
ISL version        2             2
System MAC         02:00:00:02:00:01  88:3a:30:a5:06:40
Platform          6300          6300
Software Version   FL.10.16.1006   FL.10.16.1006
Device Role        primary        secondary
```

Open SSH connection from **MGMT PC** to **Core-2** using saved sessions or type IP address **10.251.1.3** and log in with **admin/Aruba123!** credentials. Verify the prompt is **sw-core2**.

```
login as: admin
admin@10.251.1.3's password: Aruba123!
```

```
sw-core2#
```

Edge-1

This is physical AOS-CX 6300 switch where AOS-10 Aruba access point and PC-1 testing client are connected.

Open SSH connection from **MGMT PC** to **Edge-1** using saved sessions or type IP address **10.251.1.4** and log in with **admin/Aruba123!** credentials. Verify the prompt is **sw-edge1**.

```
login as: admin
admin@10.251.1.4's password: Aruba123!
```

```
sw-edge1#
```

PC-1 and PC-4

PC1 and PC4 are wired and wireless testing clients.

To access **PC-1** Desktop, right-click the icon in the lab diagram and select **Open Desktop**.

A new browser tab will open with a remote desktop. Verify that you can view the remote desktop.

Repeat the previous two steps on **PC-4**.

NOTE: The primary method to configure, troubleshoot and monitor your table switches will be HPE Aruba Networking Central for AOS-CX 6300 switches and HPE Juniper Networking Mist AI for EX 4100 Junos OS switch. You can use SSH from MGMT PC to connect to your table switches with local CLI and you can use remote console connection to your table switches for troubleshooting in case if they are unreachable. To connect to your table switches with a remote console, right-click the lab diagram icon of one of your table switches and select **Open Console**.

Task 1-3: HPE Juniper Networking Mist AI access

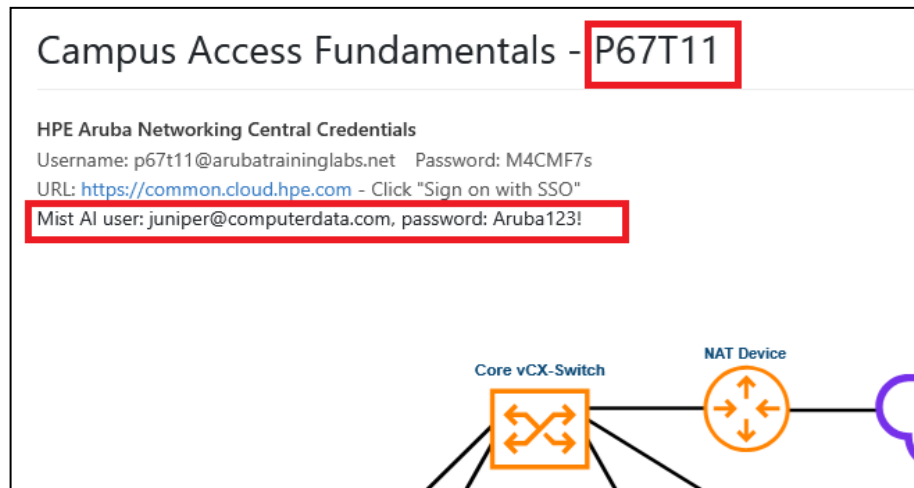
Objectives

Test access to your table Mist AI organization with provided credentials.

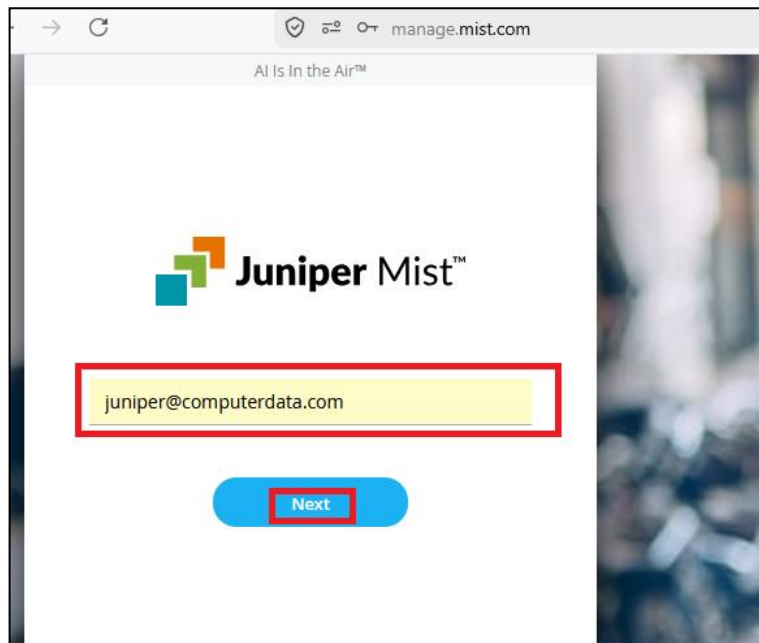
Validate that Mist AI organization is ready for the workshop.

Steps

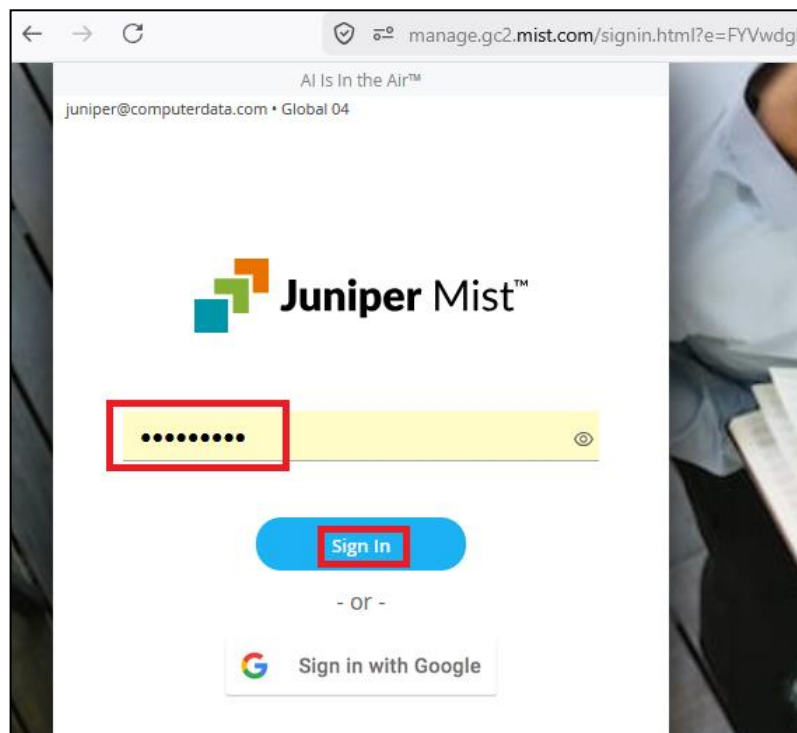
Find your Mist AI credentials on the WebGate page with the network diagram and take notes about your table and POD numbers. In this example table number is 11 and POD number is 67 (P – POD, T – table).



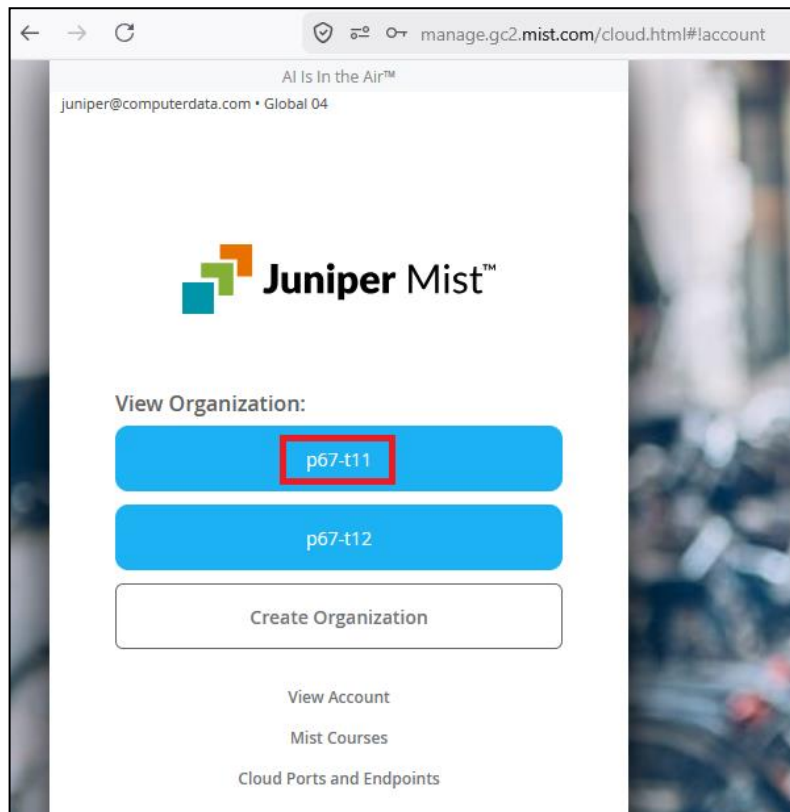
Navigate to <https://manage.mist.com> webpage and type Mist AI username and click **Next**.



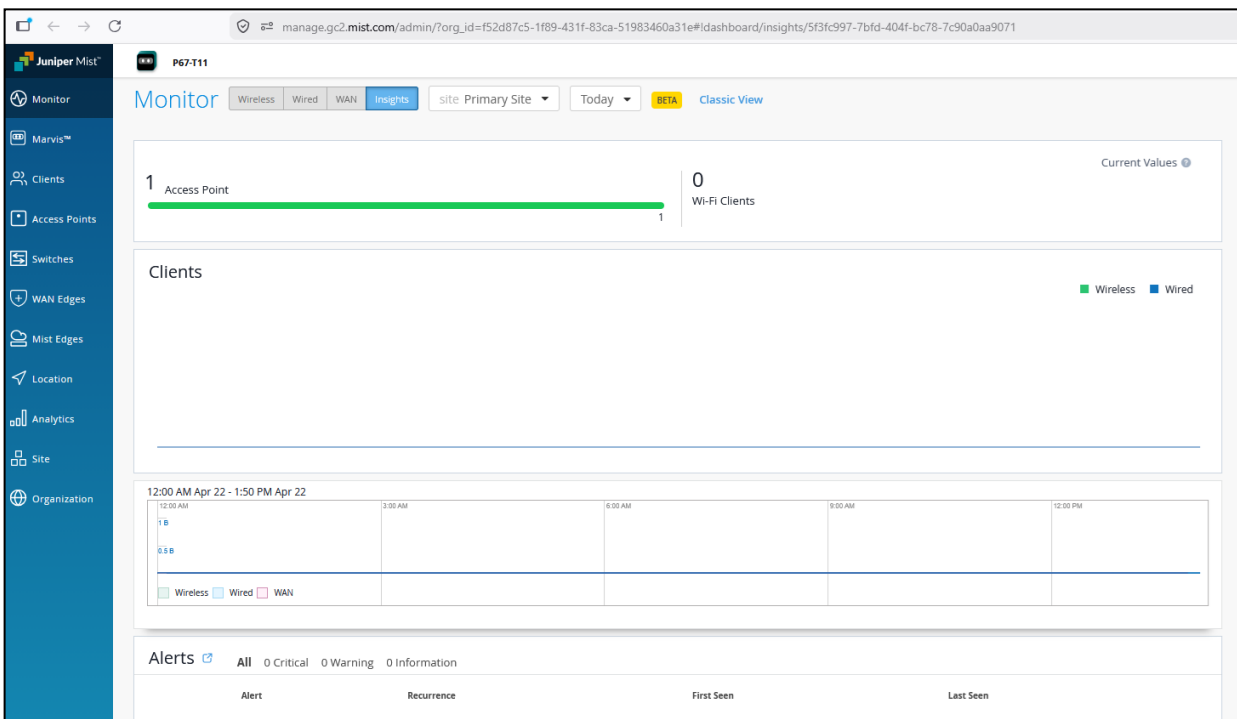
Enter your Mist AI password and click **Sign In**.



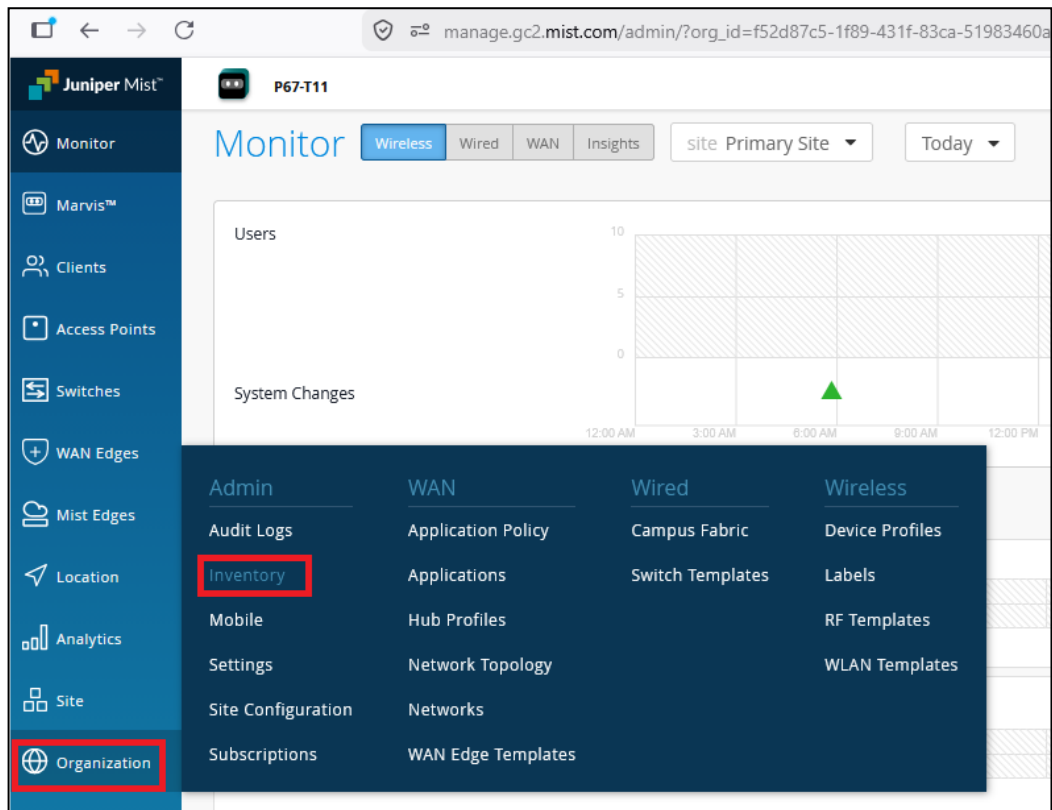
Click on your table number from the list of organizations to access Mist AI instance assigned to your table (In this example, it's table 11).



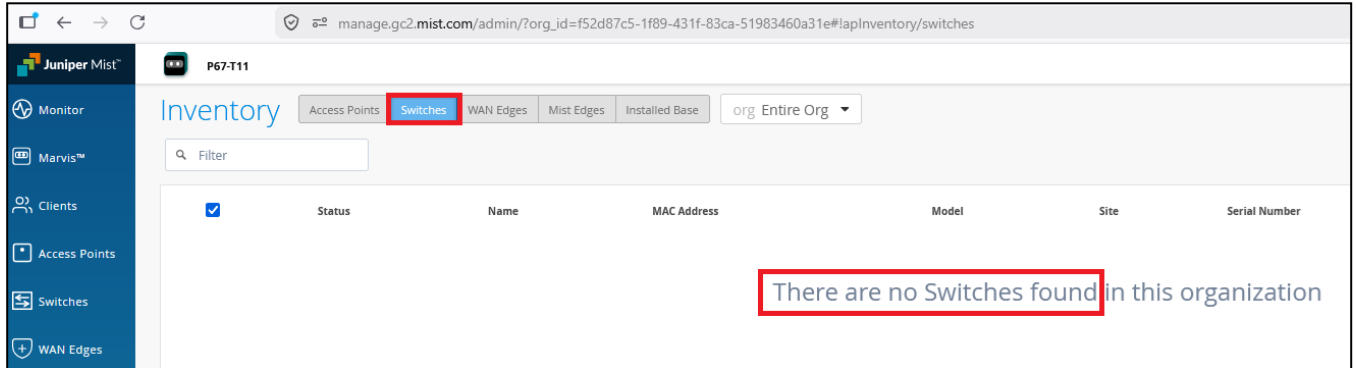
After successful login you will be redirected to Mist AI home page. Close “Getting Started” pop-up windows. At the start of class state you will have only one Access Point Connected.



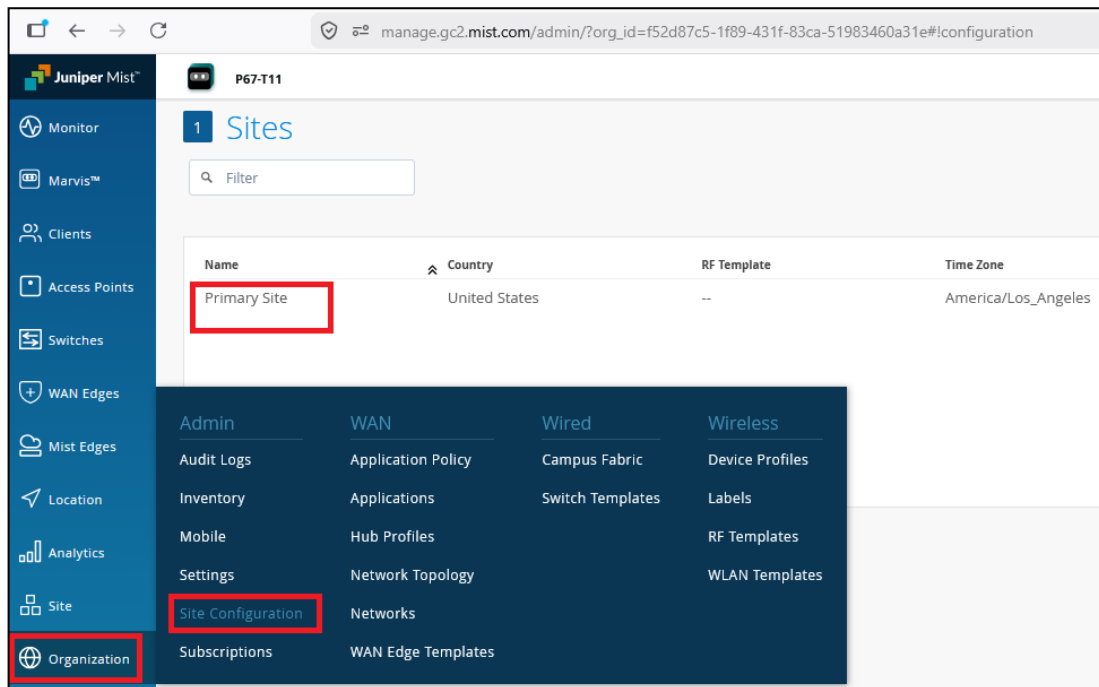
Navigate to **Organization** at the bottom of the left-hand sidebar menu and select **Inventory**.



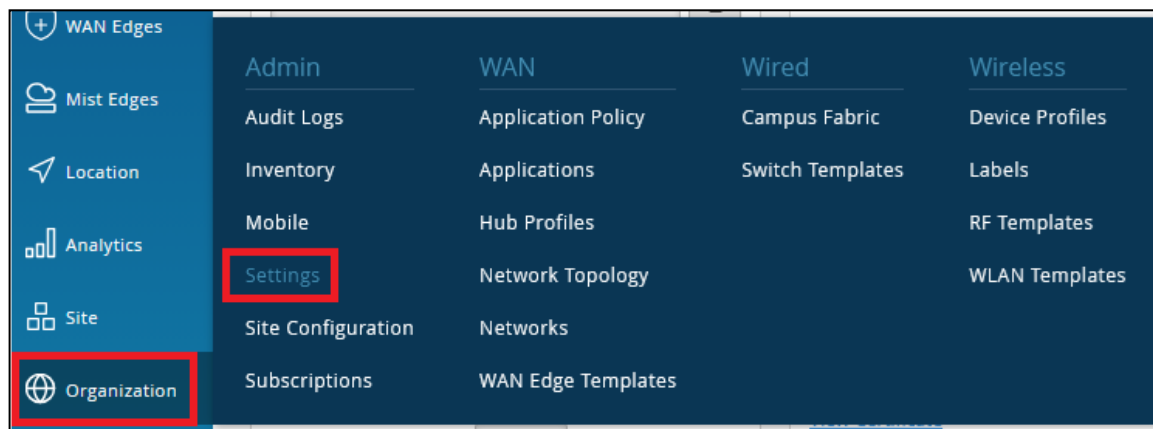
Select Switches tab and confirm that no switches are listed.



Navigate to Organization -> Site Configuration and confirm that you have only Primary Site by default.



Navigate to **Organization > Settings**.



Review Mist AI Organization settings page. On this page you can find and change organization name with sufficient authorization, manage Single sign-on settings, configure password policy, change the session policy, enable/disable remote shell access to your devices, schedule firmware upgrade for devices per site, manage your API Tokens and configure Mist AI integration with other solutions.

Organization Settings

Organization Name
p67-t11

Organization ID
f52d87c5-1f89-431f-83ca-51983460a31e

Managed Service Provider
(none)

Password Policy
☐ Enabled ☒ Disabled

Session Policy
Session Timeout after 1440 minutes
Inactivity Timeout after 0 minutes

Switch Management
Switch Proxy
☐ Enabled ☒ Disabled

Device Management
☐ Disable Remote Shell Access
Role Based Remote Shell Access **BETA**
☐ Enabled ☒ Disabled

Roles
Access
Super User Read/Write

Management Connection
☒ DHCP
☐ L2TP Management Tunnel

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

Mist Certificate
CA certificate for use by RadSec servers to validate certificates presented by Mist APs. Copy this certificate to all RadSec servers.
[View Certificate](#)

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](#)

SSL Proxy Root Certificate
[View Certificate](#)

Single Sign-on
Identity Providers [Add IDP](#)

Name	Type	Issuer	Signing Algorithm	SSO URL
CPM	SAML			

Roles [Create Role](#)

Name	Access	Site Access
------	--------	-------------

Installer
Grace period 7 days
Site and Device access based on time grace period.
☐ Allow all devices after grace period
☐ Allow extra sites after grace period

Webhooks [Add Webhook](#)

Name	Status	No. Topics	Deliveries
------	--------	------------	------------

Navigate to **Organization > Subscriptions** and explore the page. On this page you have access to Add/Renew subscriptions in the top-right corner, apply activation code and review available subscriptions. In this case you should see a list of Trial subscriptions and only one Wi-Fi Management and Assurance subscription in use. Later you will onboard EX switch to Mist AI and it will be auto-assigned with Wired Assurance subscription.

Subscription Type	Status	Usage	Sites with Usage
Asset Visibility	Trial	--	0 of 1
Marvis for WAN	Trial	--	0 of 1
Marvis for Wired Network	Trial	--	0 of 1
Marvis for Wireless	Trial	--	0 of 1
vBLE Engagement	Trial	--	0 of 1
WAN Assurance	Trial	--	0 of 1
WAN Assurance for Class 1	Trial	--	0 of 1
WAN Assurance for Class 2	Trial	--	0 of 1
WAN Assurance for Class 3	Trial	--	0 of 1
WAN Assurance for Class 4	Trial	--	0 of 1
WAN Assurance for Class 5	Trial	--	0 of 1
WAN Assurance for Class 6	Trial	--	0 of 1
Wi-Fi Management and Assurance	Trial	1	1 of 1
Wired Assurance 12	Trial	--	0 of 1
Wired Assurance 24	Trial	--	0 of 1
Wired Assurance 48	Trial	--	0 of 1

Click on “**Support Tickets and Documentation**” button with the “?” icon to access the drop-down menu with several options. Click on “Cloud Status” to check Mist AI status and any recently reported issues, click on “Ports & Endpoints” to access the documentation with a list of Firewall ports required for different Juniper devices to communicate with Mist AI, click on “Mist Documentation” to find more information about Mist AI and “API Documentation” to get the access to MIST AI REST API resources.

Support Tickets – allows you to manage TAC support tickets.

Cloud Status – displays MIST cloud status for different regions along with previous incidents details.

Ports & Endpoints – gives you a quick link to a documentation with TCP ports listed required to access the admin portal, run API calls, used to communicate with managed EX switches, Mist APs, Mist Edges, SSR devices and SRX Gateways.

Mist Documentation – redirects you to Mist documentation.

API Documentation – reveals API overview and explanation about how to use it.

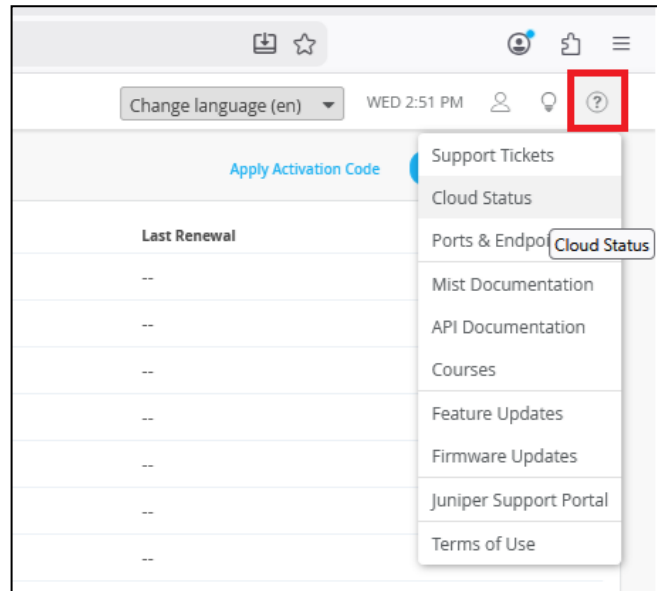
Courses – allows you to start or resume Mest technology and Wi-Fi basic free courses.

Feature Updates – quick link to the Mist documentation with details about latest updates.

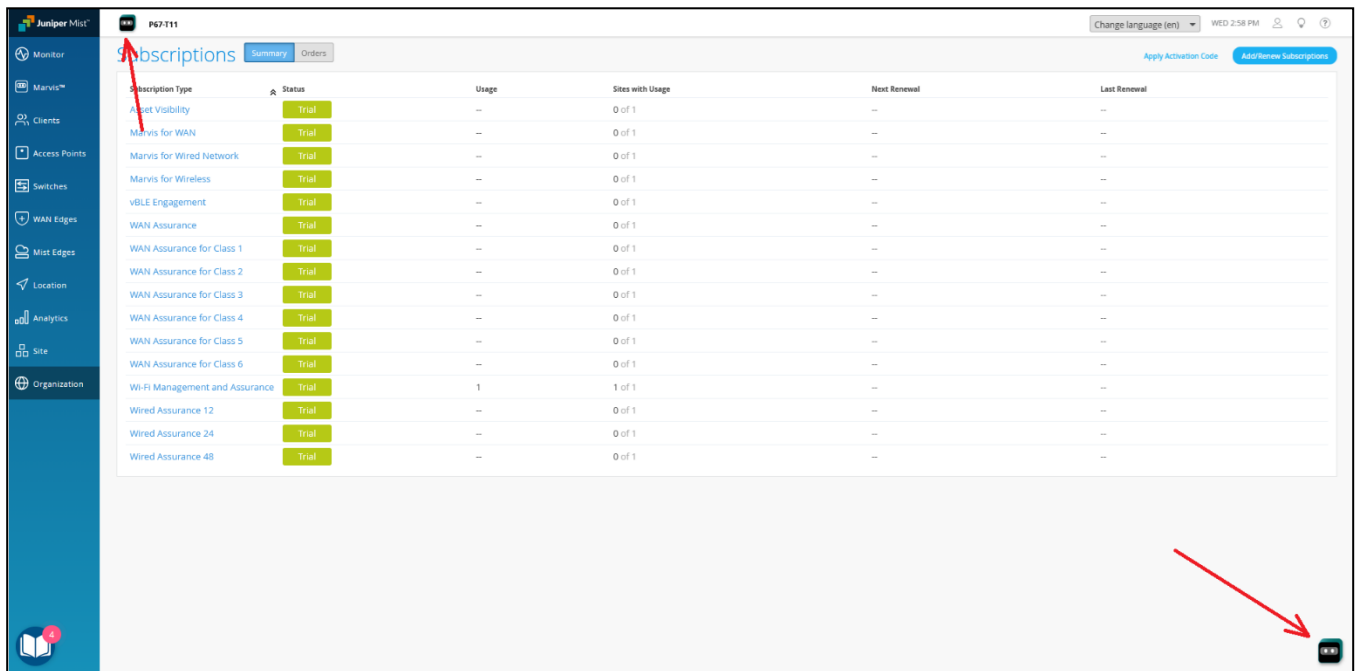
Firmware Updates – details about Access Points firmware versions and bug fixes.

Juniper Support Portal – Juniper Support Insights on Juniper Support Portal.

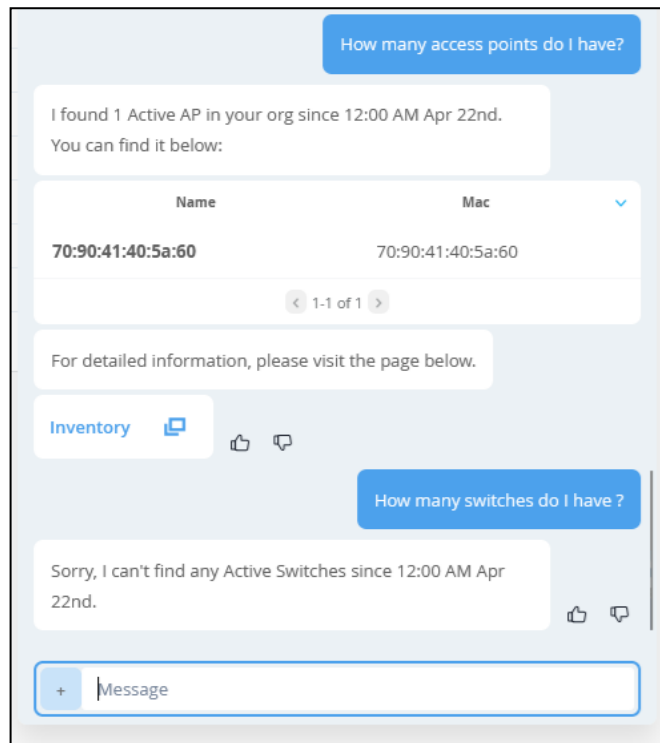
Terms of Use – Juniper General Terms and conditions.



Click on Marvis icon in the top-left or bottom-right corner.



Ask Marvis a question about Juniper devices you have in Mist AI: "How many switches do I have?", "How many access points do I have?" Feel free to ask additional questions to practice with Marvis.



NOTE: You may spend some additional time to explore Mist AI web interface and become more familiar with menu options and how it's organized.

Task 1-4: HPE Aruba Networking Central access

Objectives

Test access to your table HPE Aruba Networking Central customer with provided credentials.

Validate that HPE Aruba Networking Central customer is ready for the workshop.

Steps

Find HPE GreenLake credentials required to launch HPE Aruba Networking Central Service on the WebGate page with network diagram.

Campus Access Fundamentals - P67T11

HPE Aruba Networking Central Credentials

Username: p67t11@arubatraininglabs.net Password: M4CMF7s
URL: <https://common.cloud.hpe.com> - Click "Sign on with SSO"
Mist AI user: juniper@computerdata.com, password: Aruba123!

Core vCX-Switch NAT Device

Navigate to <https://common.cloud.hpe.com>, click on **Sign in with SSO** button.

Sign In [Try new sign in](#)

Username

☐ Remember Me

Next

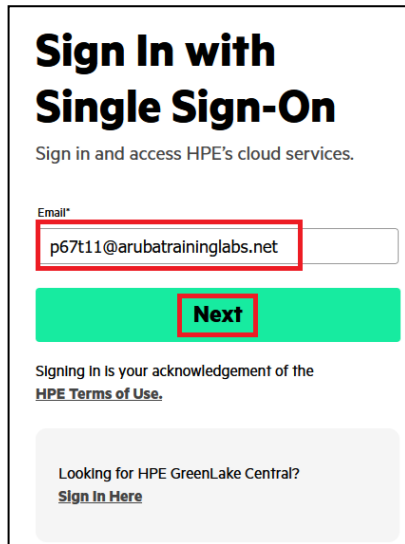
OR

Sign in with SSO

[Need help Signing in?](#)

New to HPE? [Create account](#)

Enter your HPE GreenLake username from step 1 and click **Next**.



Sign In with Single Sign-On

Sign in and access HPE's cloud services.

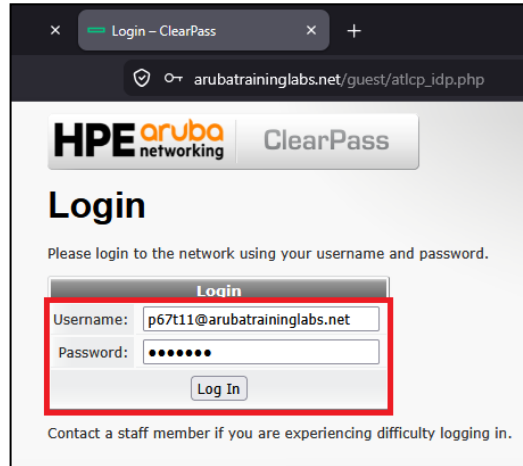
Email*

Next

Signing In is your acknowledgement of the [HPE Terms of Use](#).

Looking for HPE GreenLake Central?
[Sign In Here](#)

Enter your username and password from step 1 and click **Log In**.



Login - ClearPass

arubatraininglabs.net/guest/atlcp_idp.php

HPE aruba networking ClearPass

Login

Please login to the network using your username and password.

Login

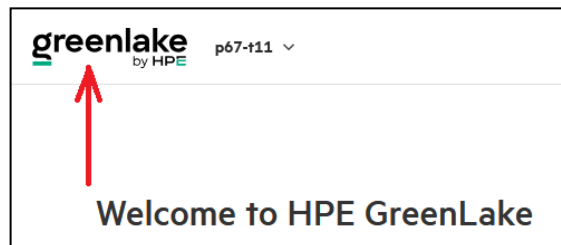
Username:

Password:

Log In

Contact a staff member if you are experiencing difficulty logging in.

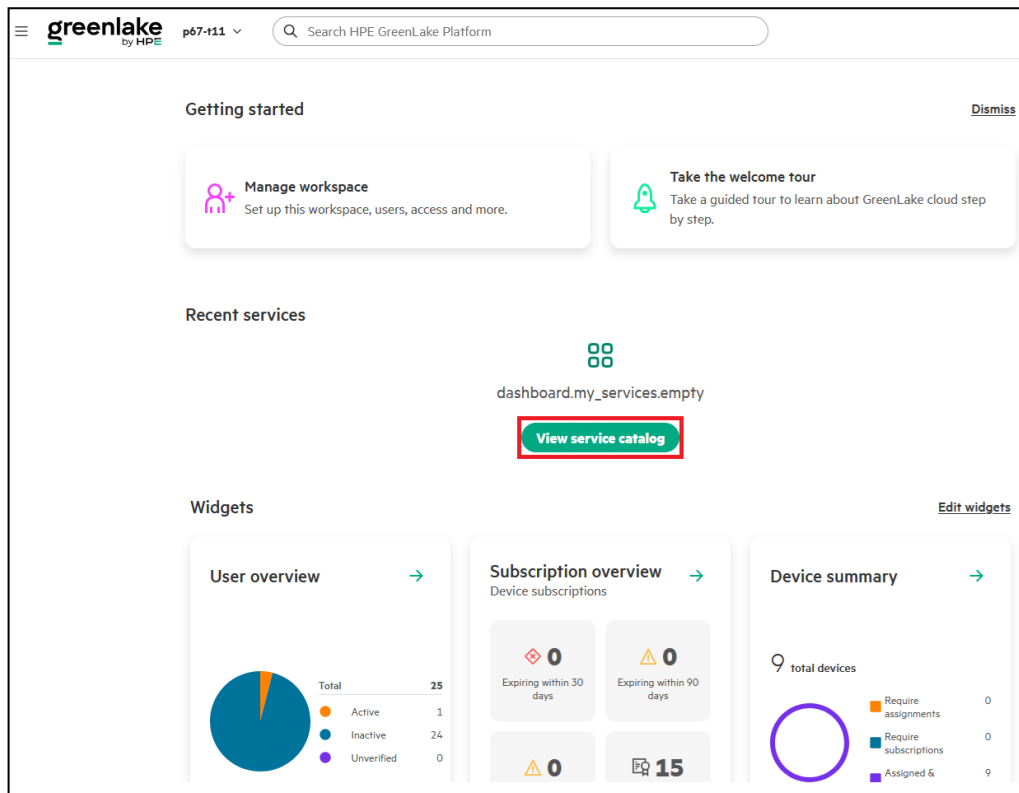
Click on **greenlake by HPE** logo in the top-left corner if it doesn't show your workspace.



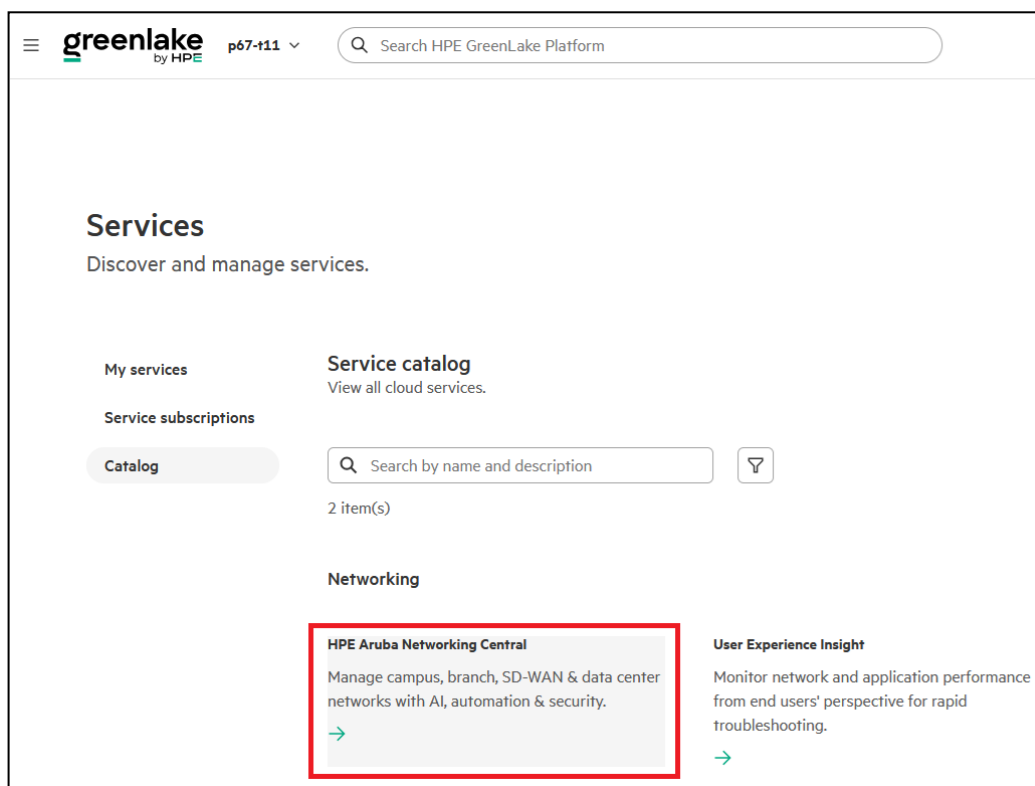
greenlake by HPE p67-t11 ▾

Welcome to HPE GreenLake

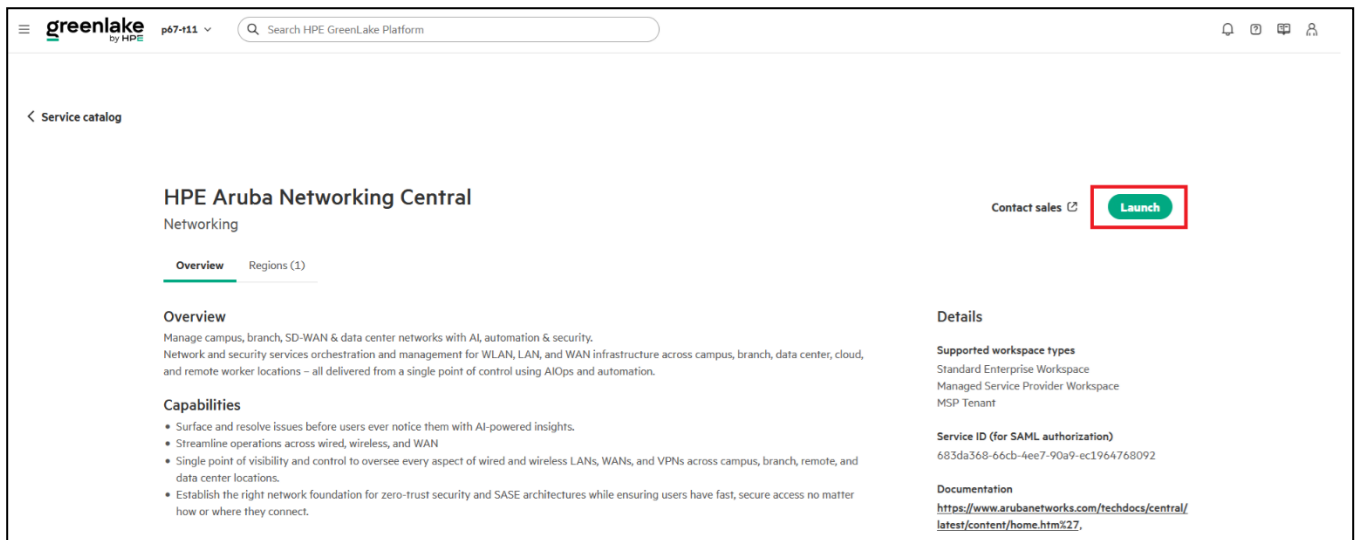
Click on **View service catalog**.



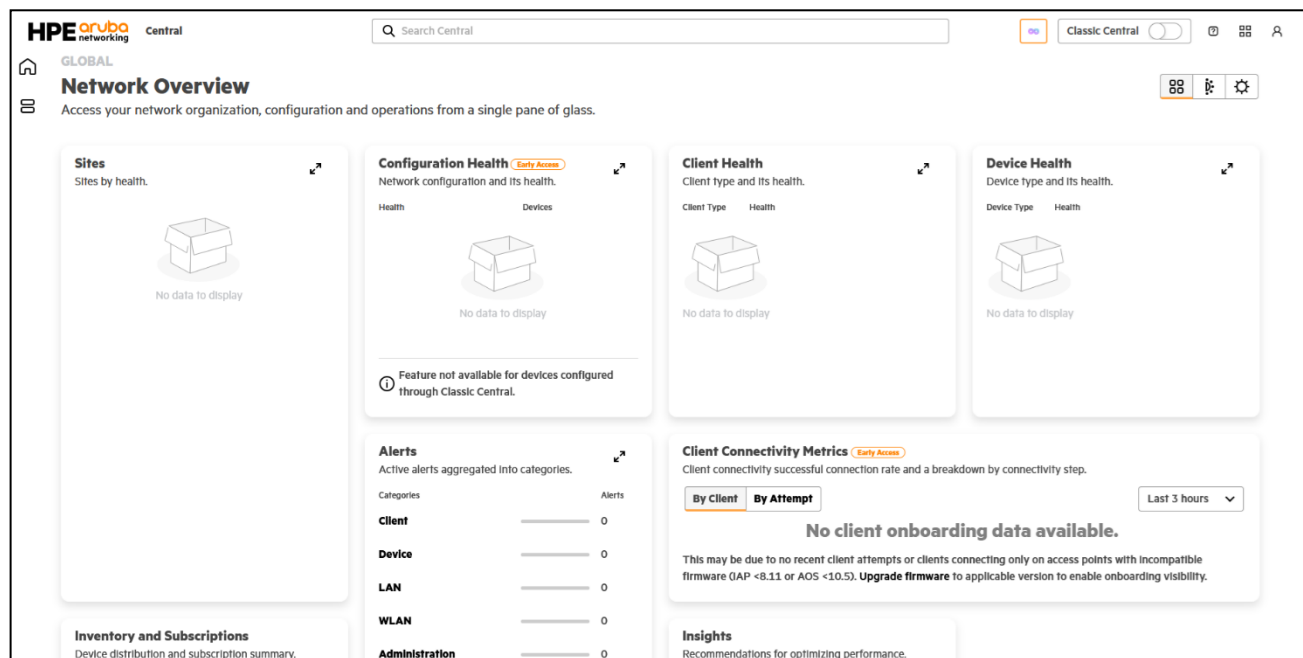
Select **HPE Aruba Networking Central**.



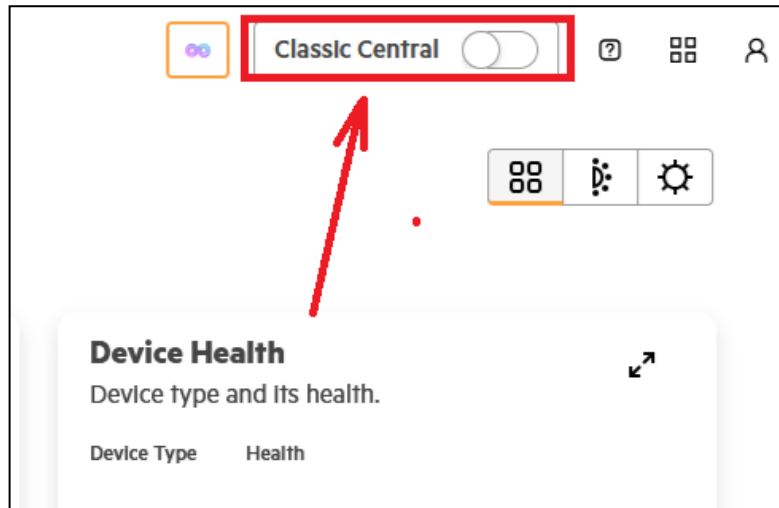
Click **Launch**.



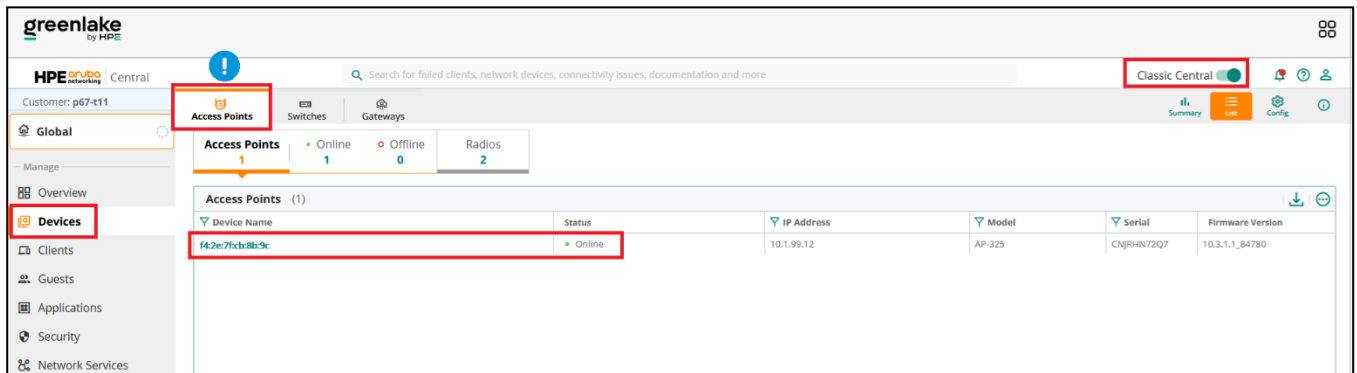
This should successfully launch HPE Aruba Networking Central service.



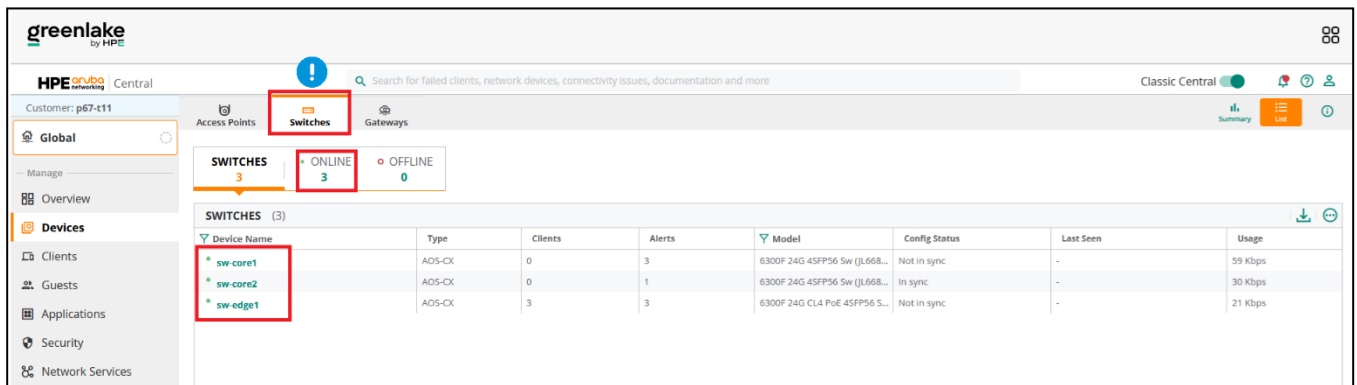
Use toggle in the top-right corner to switch between **Classic Central** and **New Central** modes.



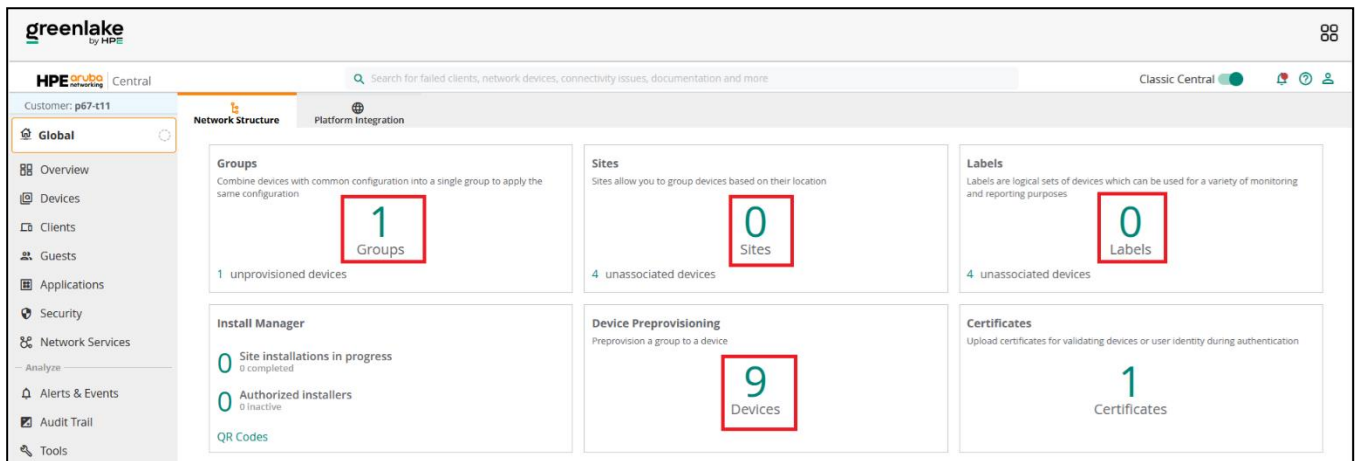
Switch to **Classic Central** mode and navigate to **Devices > Access Points**. Conform that you have 1 Online Access Point.



Switch to **Switches** tab and confirm that you have 3 Online Switches.



Click on **Organization** section in the left-hand sidebar menu and confirm that you have only 1 group (default), not sites, no labels and 9 Device Preprovisioning.



NOTE: You may spend some additional time to explore HPE Aruba Networking Central web interface and become more familiar with menu options and how it's organized. At the start of workshop state all devices are **not** managed in HPE Aruba Networking Central.

You have completed this lab!

Lab 2: Day 0: Onboard Juniper EX switch to Mist AI

Objectives

- Create Site and Switch Template in Mist AI.
- Adopt Juniper EX Switch in Mist AI and assign to Site.
- Validate and monitor Juniper EX Switch connectivity to Mist AI.
- General switch configuration.

Overview

After completing this lab, you will learn how to onboard Juniper EX switch to Juniper Mist AI and troubleshoot connectivity to Mist AI. Juniper Mist web UI could be changed over the time and will not match screenshots in this workshop. Ask your instructor for assistance if you struggle finding required settings in Juniper Mist.

Task 2-1: Create Site and Switch Template in Mist AI

Objectives

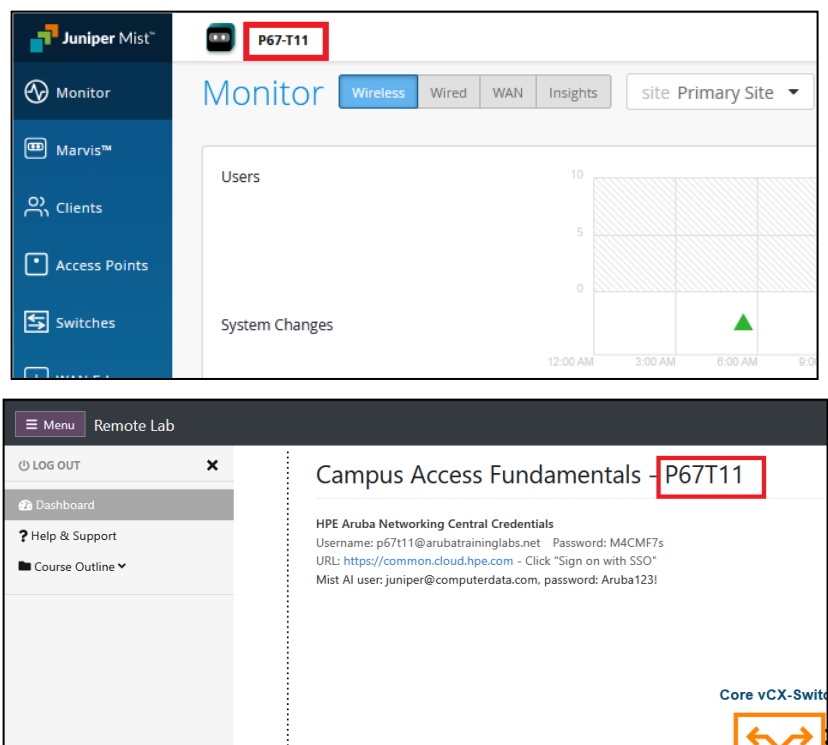
Create and configure Sites in Mist AI

Create, configure and assign Switch Templates in Mist AI

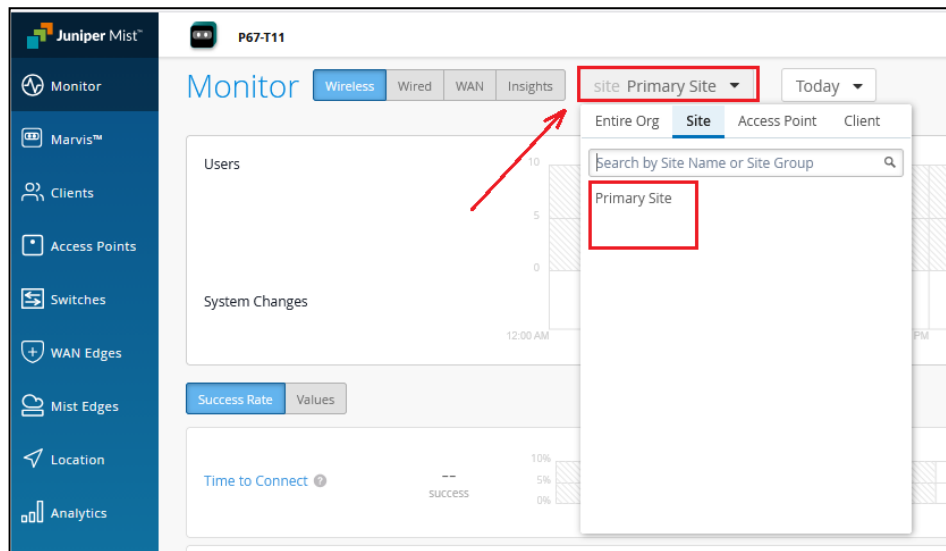
Steps

Navigate to <https://manage.mist.com> web page and login to your table Mist AI organization as explained in Task 1-3.

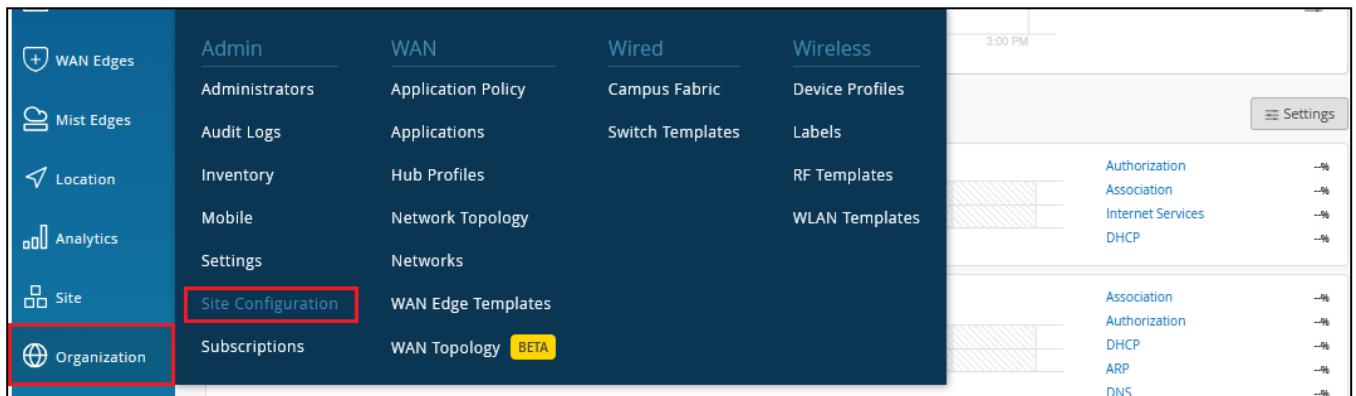
NOTE: Make sure that the right Mist AI organization is selected. In this example POD number is 67 and table number is 11.



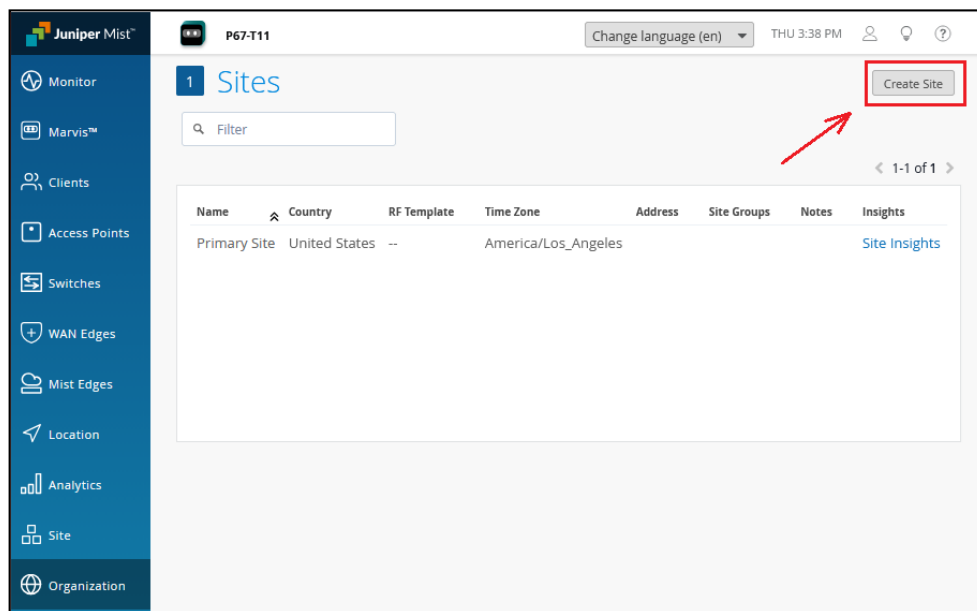
Click on “site Primary Site” next to Insights at the top of the page to confirm that you have only one site configured.



Navigate to Organization > Admin > Site Configuration.



Click on **Create Site**.



Complete the following information:

Information Site Name: **p<pod>t<table>-site** (example for POD 67 and table 11: **p67t11-site**).

Information Country: **United States**

Information Time Zone: **America/Detroit**

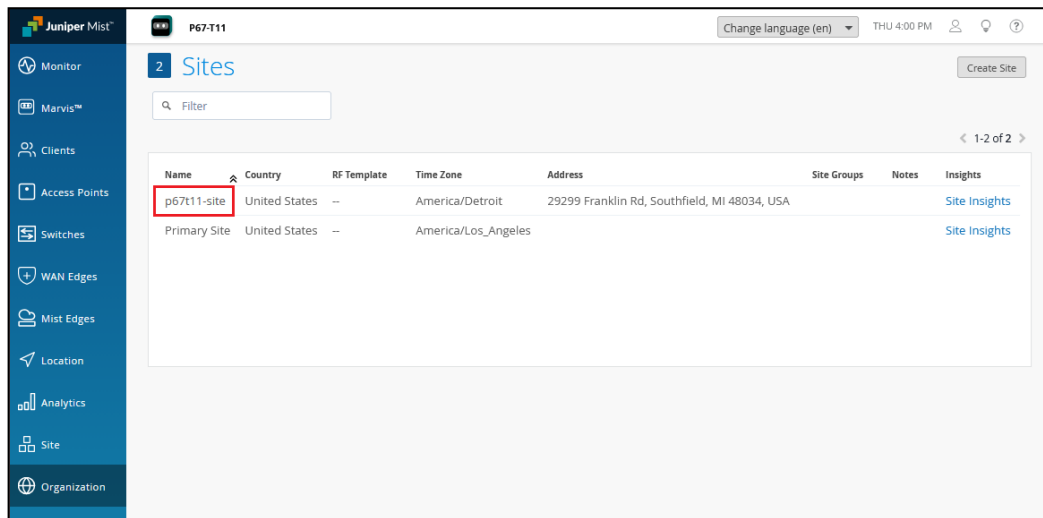
Location: **29299 Franklin Road Southfield, MI, USA**

Click **Save** button in the top-right corner.

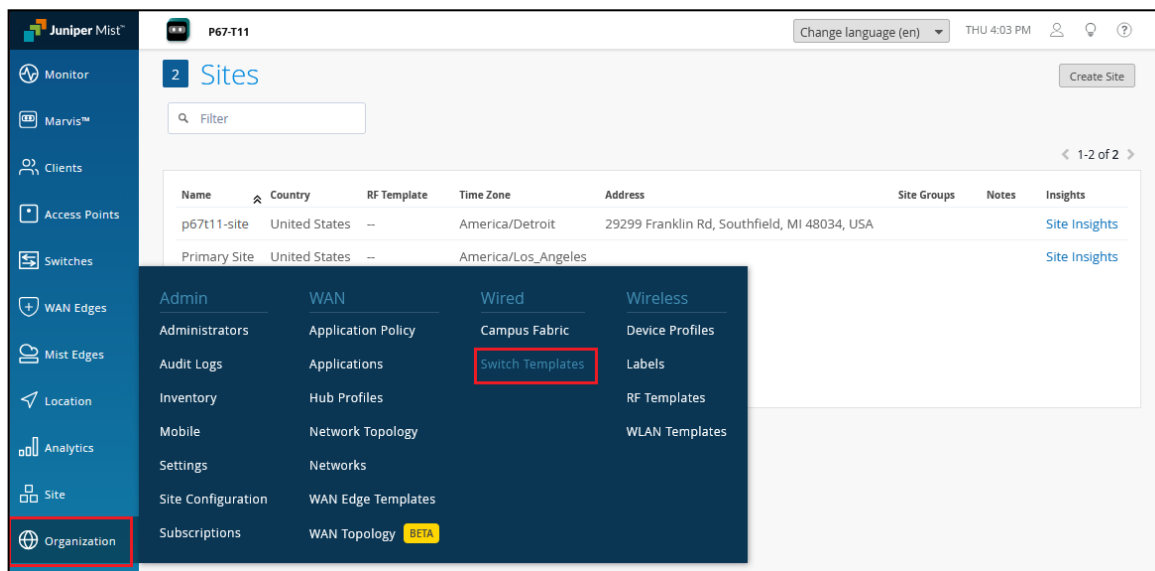
The screenshot shows the Juniper Mist web interface for configuring a new site. The left sidebar contains navigation links: Monitor, Marvis™, Clients, Access Points, Switches, WAN Edges, Mist Edges, Location, Analytics, Site, and Organization. The main content area is titled 'Site Configuration : New Site'. At the top right, there is a 'Save' button highlighted with a red box and a red arrow pointing to it, and a 'Cancel' button. Below the title bar, there is a 'Site' section with the following fields:

- Information**
 - Site Name: p67t11-site (required)
 - Country: United States (required)
 - Time Zone: America/Detroit (GMT -05:00/-04:00)
- Notes**
 - Add Notes
- Site Proxy**
 - Proxy URL: http://username:password@proxy.internal:8080
- Location** (required)
 - Location Search (or click on the map): 29299 Franklin Road Southfield, MI, USA
 - Map: A Google Map showing the location of Southfield, MI, with a blue dot indicating the site location.
 - Street Address: 29299 Franklin Rd, Southfield, MI 48034, USA
 - Latitude: 42.502666, Longitude: -83.308142

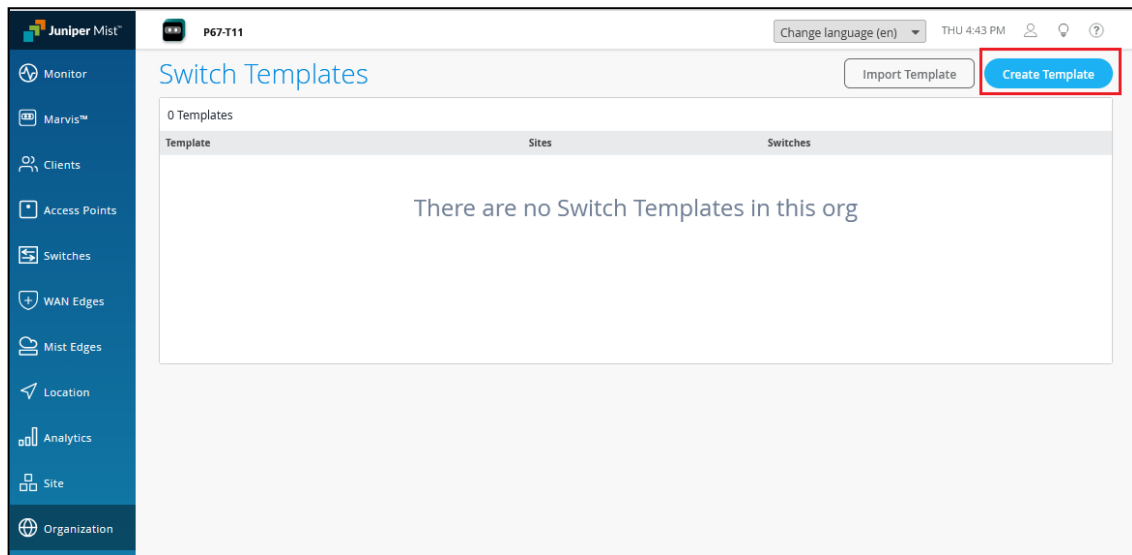
Confirm that your new site is displayed in the list of sites.



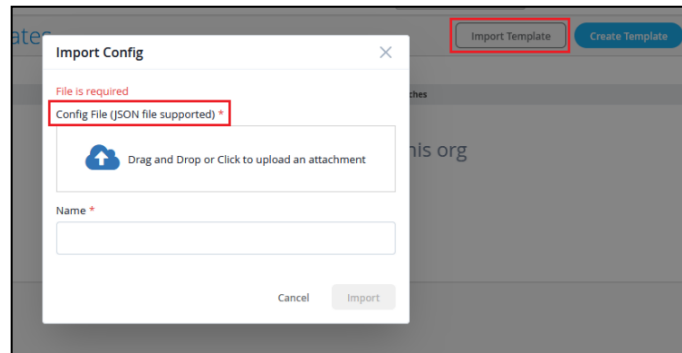
Navigate to Organization > Wired > Switch Templates.



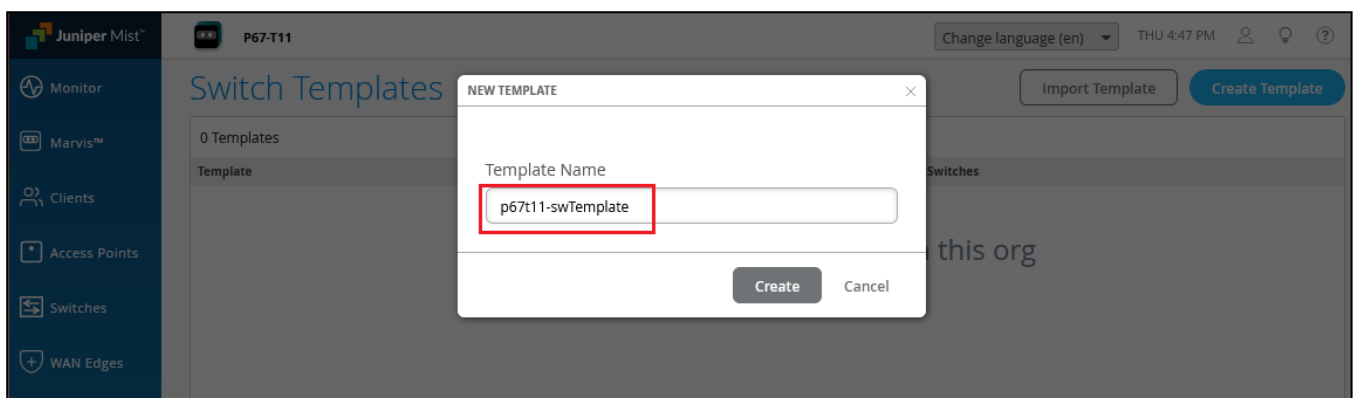
Click **Create Template**.



NOTE: Template could be exported and imported in JSON format.



Name your template as **p<pod>t<table>-swTemplate** (example: *p67t11-swTemplate*) and click **Create**.



Enter **NTP server** IP address 10.254.1.21 and **DNS server** IP address 10.254.1.21 and then click **Save**.

Juniper Mist™ P67-T11

Change language (en) THU 4:52 PM

Switch Templates: **p67t11-swTemplate**

Delete Template Save Cancel

INFO

Name: p67t11-swTemplate

APPLIES TO SITES

0 sites 0 switches Assign to Sites

All Switches Configuration

AUTHENTICATION SERVERS

Authentication Servers: Radius

Authentication Servers: No servers defined

Timeout: 5 (0 - 1000 seconds)

Retries: 3 (0 - 100)

Enhanced Timers: Disabled

Load Balance: Disabled

NTP

NTP Servers: 10.254.1.21

DNS SETTINGS

DNS Servers: 10.254.1.21

DNS Suffix:

CLI CONFIGURATION

Additional CLI Commands

OSPF

OSPF Areas: No areas defined

VRRP

Review changes and confirm by clicking Save.

Juniper Mist™ P67-T11

Change language (en) THU 4:54 PM

Confirm Changes

APPLIES TO SITES

0 sites 0 switches

Show only differences + Added - Removed * Template or System inherited

DNS Settings

Servers

+ 0: 10.254.1.21

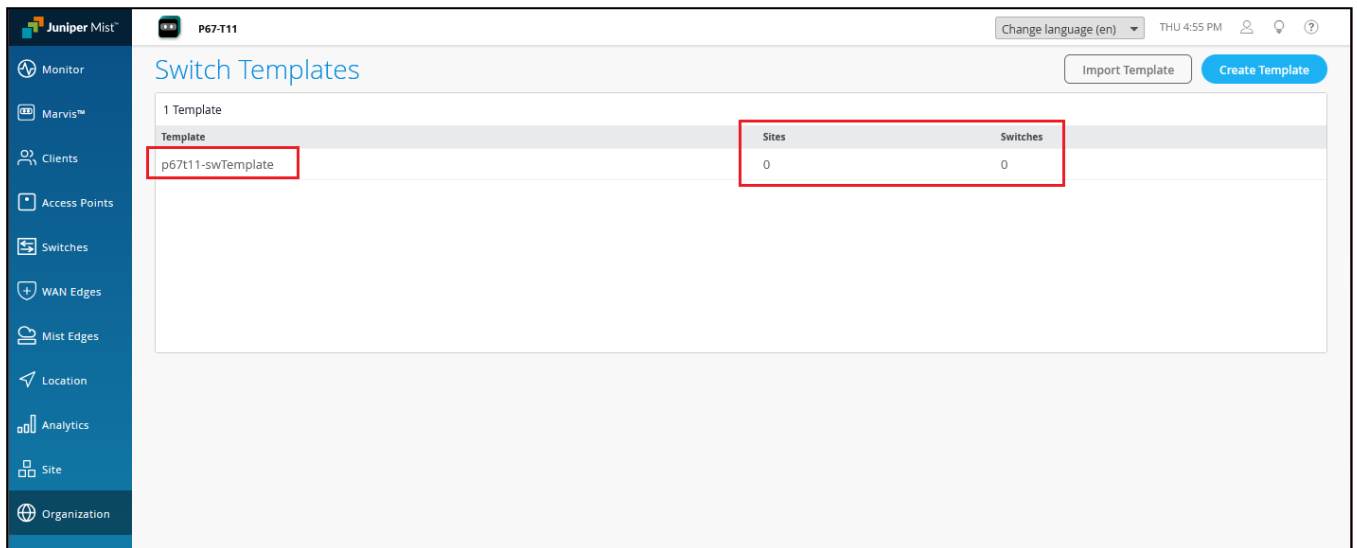
NTP

Servers

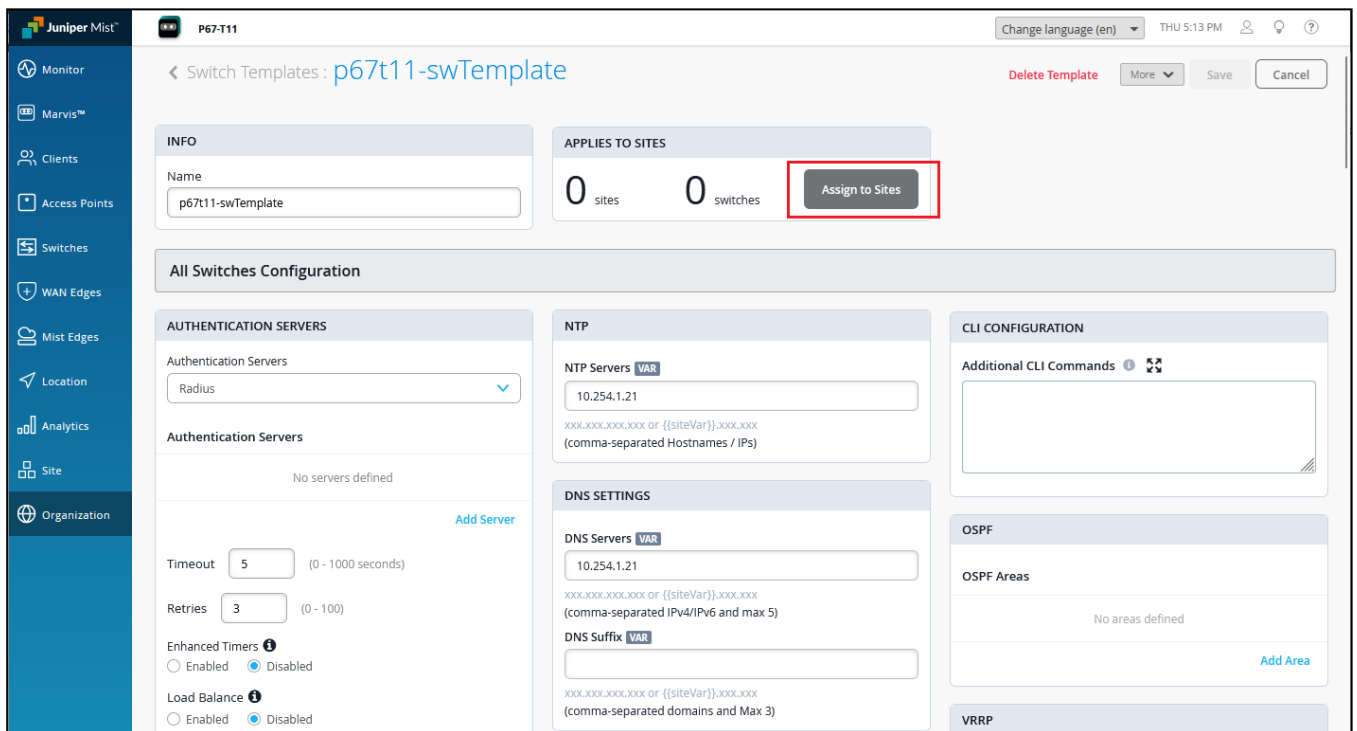
+ 10.254.1.21

Save Cancel

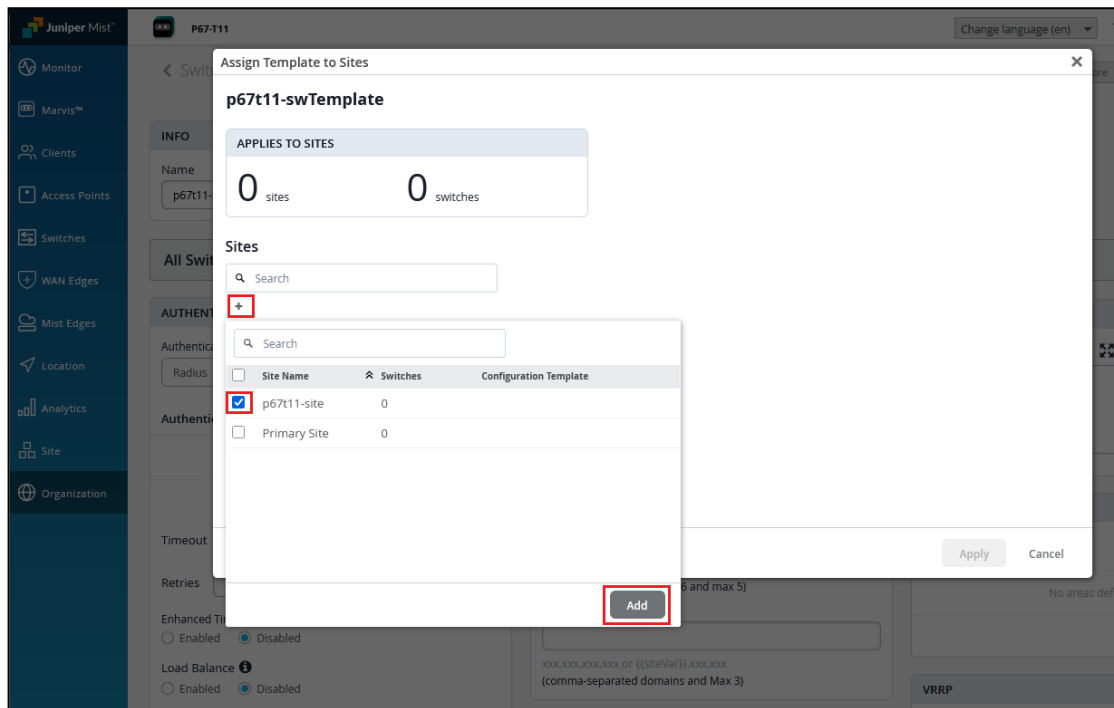
Your new Switch Template will be displayed in the list with no sites and Switches assigned.



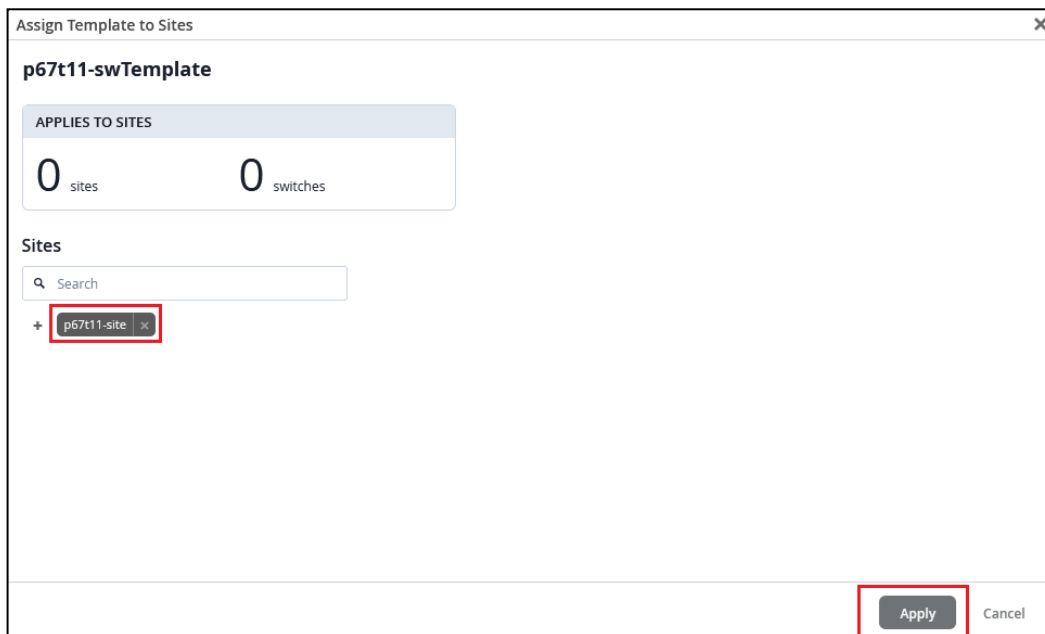
Click on your switch template name to return to your switch template configuration and then click **Assign to Sites**.



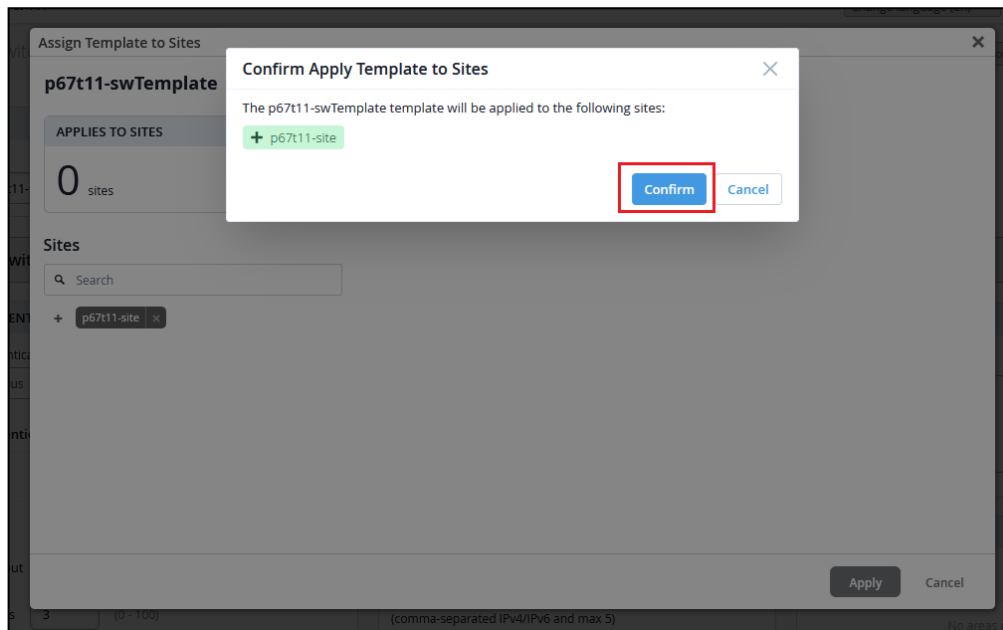
Click on “+” icon below Search, then select your new site and click **Add**.



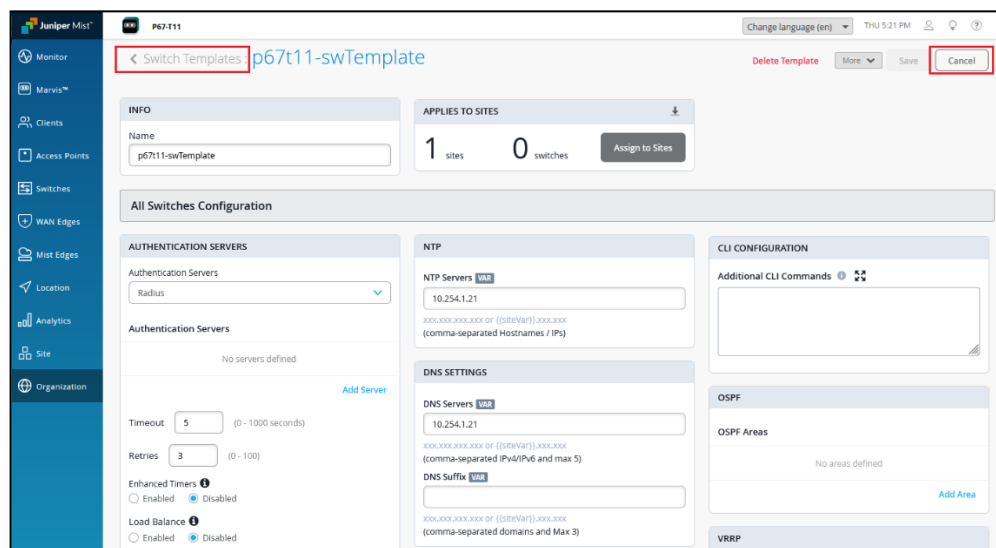
Confirm that recently created site is listed and click Apply.



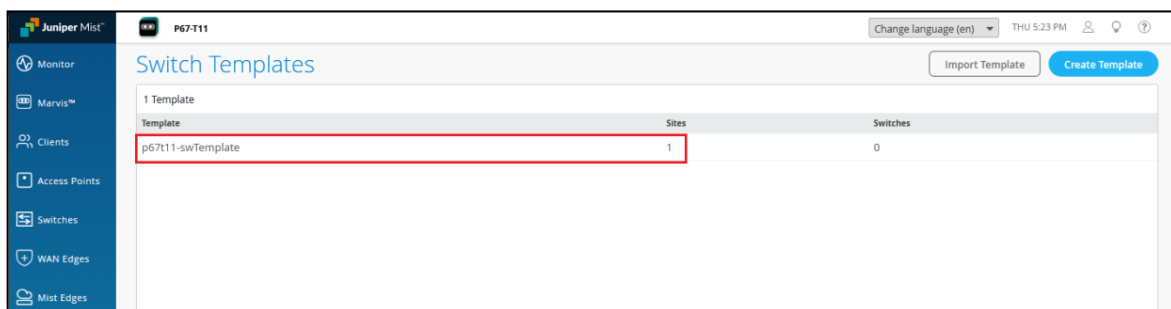
Click **Confirm** to confirm apply Template to Sites.



You should see now 1 site is shown where this switch template is applied. Click Return arrow or Cancel to return to the list with switch templates.



Switch template is listed now with 1 site assigned.



Task 2-2: Adopt Juniper EX Switch in Mist AI and assign to Site

Objectives

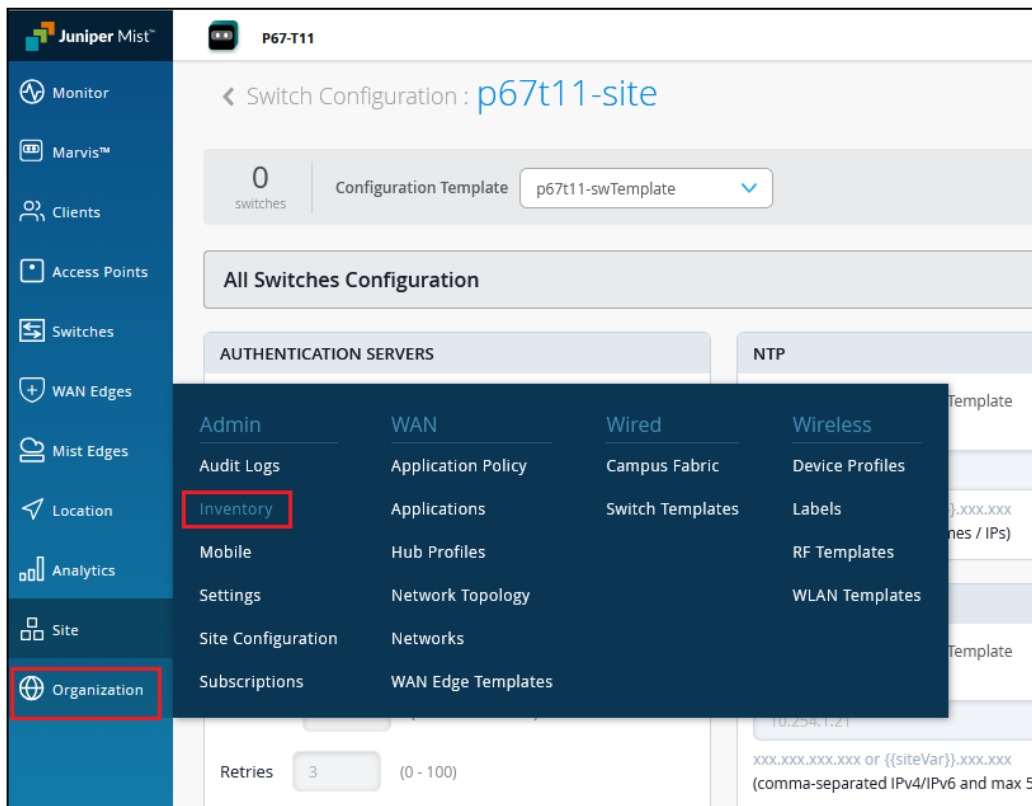
Adopt Juniper EX switch in Mist AI.

Assign EX switch to Mist AI Site.

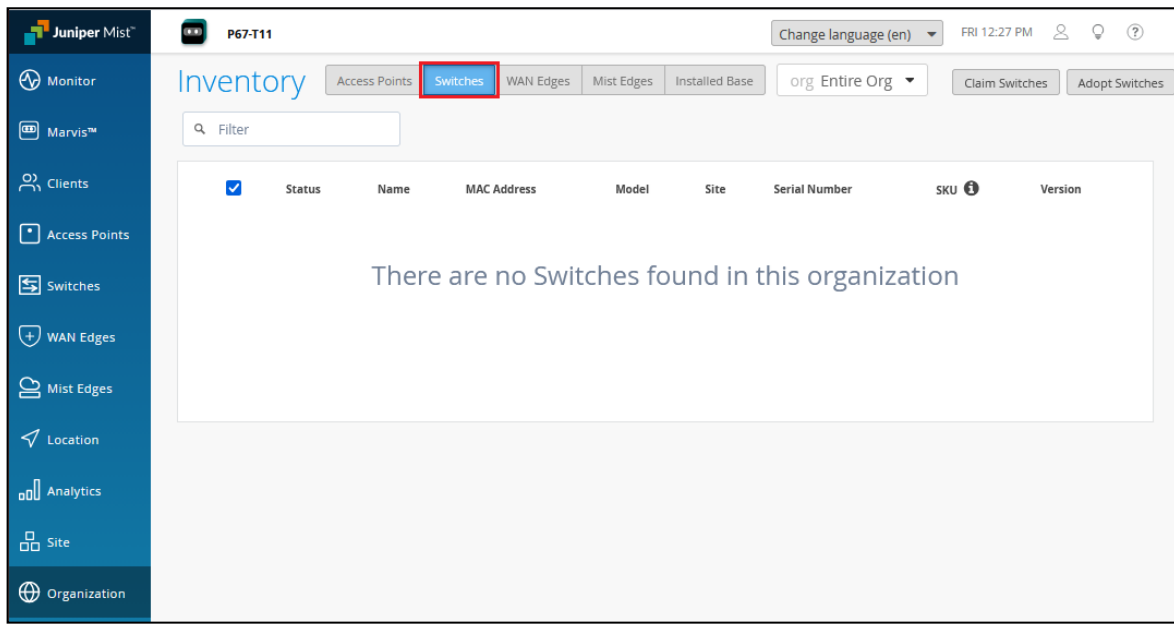
Validate EX switch assignment.

Steps

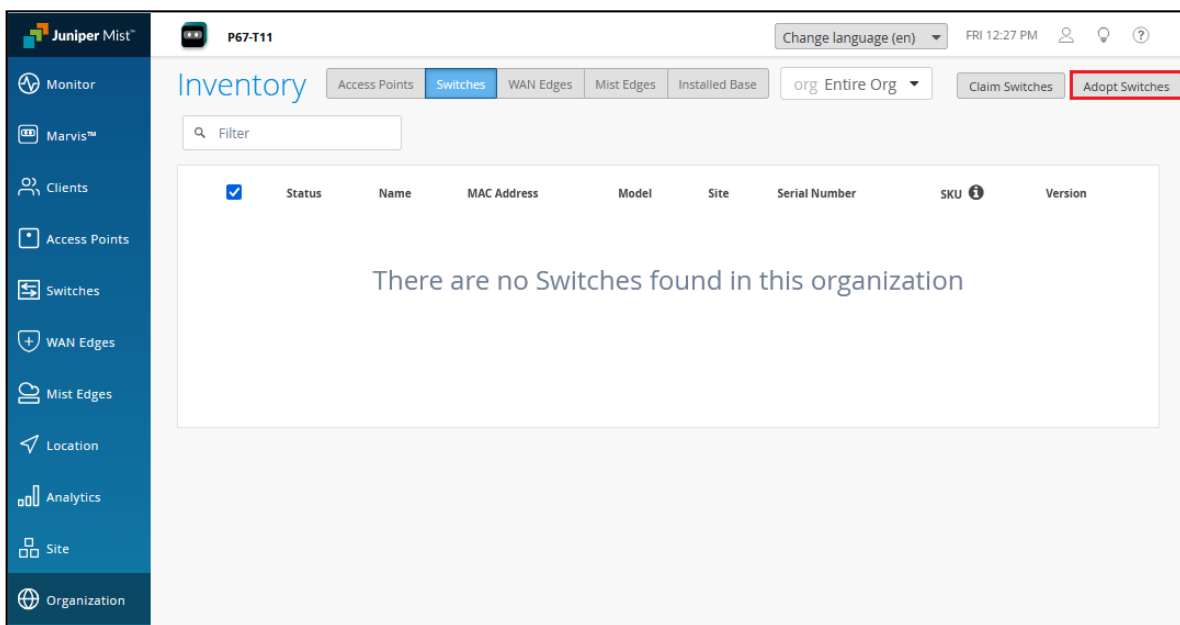
Navigate in Mist AI to Organization > Admin > Inventory.



Select **Switches** tab at the top of the page. You should see this message: “There are no Switches found in this organization” since you didn’t add any switches yet.



Click **Adopt Switches** button.



NOTE: There are two options you can use to connect Juniper switches to Mist AI:

Claim Switches – used in greenfield scenarios, switches can be automatically added to the Juniper Mist cloud using the zero-touch provisioning (ZTP) option, or manually by entering an activation or claim code in the Juniper Mist portal.

Adopt Switches – used in brownfield scenarios, switches being brought into the Juniper Mist cloud from a previous deployment. This option requires to enter CLI commands on a switch which you can copy from the Juniper Mist cloud.

Read instructions and review the list of Junos OS CLI commands that you need to copy and paste into your table switch.

Switch Adoption

Please check whether your Switch(s) meet the requirements before adopting the Switch: [Prerequisites](#)
Apply the following CLI commands to adopt a Juniper switch

Copy to Clipboard

```
set system services ssh protocol-version v2
set system authentication-order password
set system login user mist class super-user
set system login user mist authentication encrypted-password
$6$xZNbMIH9pc7PeTdv$LQ3fXmsm.1k//7gNnX1eybT2HnQ2JF6qAENrpqeUricwevAlHslPn3DnjjavHPQJwD2S3jc35UWX.jtyJ0nvn1
set system login user mist authentication ssh-rsa "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC9uku4eTPRDHQL3yjY5815fhY/
LmxEfNTBI8oMXpJKC7aRwuPMFrkv2PQs7xi97bmk0ZjGnr4Fp2/4dzZVukPlmvoqHNeeMR71bOYJgEaMw1LKXuv/
cEoJCNz4DHuPg1wLhKmMrISEcig21InMWjDNQs+PyG+4RDZUbjW6XqtQJAMHzEQ2nIQJgGijppRFUdXoPXNf/
G+bufspLDuDIVTcQt78vLoUKt6lifdhlxL+f3poNWpzX7bAecil/
aRReOH07pDfj2ee88z+S3PtPj9U1JkAuOUcD1pODCBjy4GE10Kx2aOzuJT1H+YguIRbDDOF2etSwiujSfrmiWYt6HLKMLqezFFCFYmavt9
rM3OG6WOQJzFjLTnQEyzU3Hvm12LuFXHNDyy6IEB1qEkxjegEl8SfWVBX3heLMegSDUoUdKlq23TfeuLuQxMBbygiktv+RzwZo6JUYHT
51Eed+B8XSkDgN8lWDQsPlSytnQgzxSAZ075212YoxLb4ROLp2FI0= mist@f52d87c5-1f89-431f-83ca-51983460a31e"
set system services outbound-ssh client mist device-id f52d87c5-1f89-431f-83ca-51983460a31e
set system services outbound-ssh client mist secret
b9f8a7e50519775a1456b22f94265031d9472ff86051f6597bb96b4e7c622bfb43442b12e0a5f21d1f9e40208bf0f535b69d66d2ba37
603ebc7cf268effcbbfa
set system services outbound-ssh client mist services netconf keep-alive retry 12 timeout 5
set system services outbound-ssh client mist oc-term.gc2.mist.com port 2200 timeout 60 retry 1000
delete system phone-home
```

These commands will enable SSH service, create user “mist” with encrypted password and super-user class, set outbound-ssh client device-id, secret, Netconf and cloud server hostname depending on the used cluster and region.

Click **Copy to Clipboard**.

Switch Adoption

Please check whether your Switch(s) meet the requirements before adopting the Switch: [Prerequisites](#)
Apply the following CLI commands to adopt a Juniper switch

Copy to Clipboard

```
set system services ssh protocol-version v2
set system authentication-order password
set system login user mist class super-user
set system login user mist authentication encrypted-password
$6$xZNbMIH9pc7PeTdv$LQ3fXmsm.1k//7gNnX1eybT2HnQ2JF6qAENrpqeUricwevAlHslPn3DnjjavHPQJwD2S3jc35UWX.jtyJ0nvn1
set system login user mist authentication ssh-rsa "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC9uku4eTPRDHQL3yjY5815fhY/
LmxEfNTBI8oMXpJKC7aRwuPMFrkv2PQs7xi97bmk0ZjGnr4Fp2/4dzZVukPlmvoqHNeeMR71bOYJgEaMw1LKXuv/
```

Open **MGMT PC** Remote Desktop and connect with SSH to 10.251.1.10 (sw-edge2) switch CLI then log in with credentials provided in Task 1-2. Or use existing SSH session.

```
login as: admin
```



```
Keyboard-interactive authentication prompts from server:
| Password: Aruba123!
End of keyboard-interactive prompts from server
Last login: Fri May  8 17:14:40 2026 from 10.251.1.90
--- JUNOS 22.4R3.25 Kernel 64-bit  JNPR-12.1-20231013.108e0b3_buil
{master:0}
admin@sw-edge>
```

On sw-edge2, enter configuration mode with “configure” command.

```
admin@sw-edge> configure
Entering configuration mode

{master:0}[edit]
admin@sw-edge#
```

NOTE: Notice that prompt will be changed from operational “>” to configuration mode “#”.

Operational mode – used for monitoring and troubleshooting commands.

Configuration mode – used for making configuration changes.

Paste CLI commands from the Juniper Mist cloud to **sw-edge2**, hit Enter at the end of the input.

NOTE: Use clipboard to copy and paste text between your computer and virtual lab PC. It could be accessed with Ctrl+Alt+Shift keyboard combination or by clicking on a small black arrow in a middle of the left-side of the windows with remote desktop.

```
<Output omitted>

{master:0}[edit]
admin@sw-edge# ...0f535b69d66d2ba37603ebc7cf268effccbfa

{master:0}[edit]
admin@sw-edge# ...t services netconf keep-alive retry 12 timeout 5

{master:0}[edit]
admin@sw-edge# ...t oc-term.gc2.mist.com port 2200 timeout 60 retry 1000

{master:0}[edit]
admin@sw-edge# delete system phone-home

{master:0}[edit]
admin@sw-edge#
```

Validate the candidate uncommitted configuration with “show | compare” command. Press space to list the output till the bottom.

```
<Output omitted>
+           port 2200;
+           retry 1000;
+           timeout 60;
+       }
+   }
+ }
```

```
[edit system]
-   phone-home {
-       server https://redirect.juniper.net;
-       rfc-compliant;
-   }

{master:0}[edit]
admin@sw-edge#
```

On **sw-edge2**, enter “**commit**” command to apply new configuration.

```
{master:0}[edit]
admin@sw-edge# commit
configuration check succeeds
commit complete

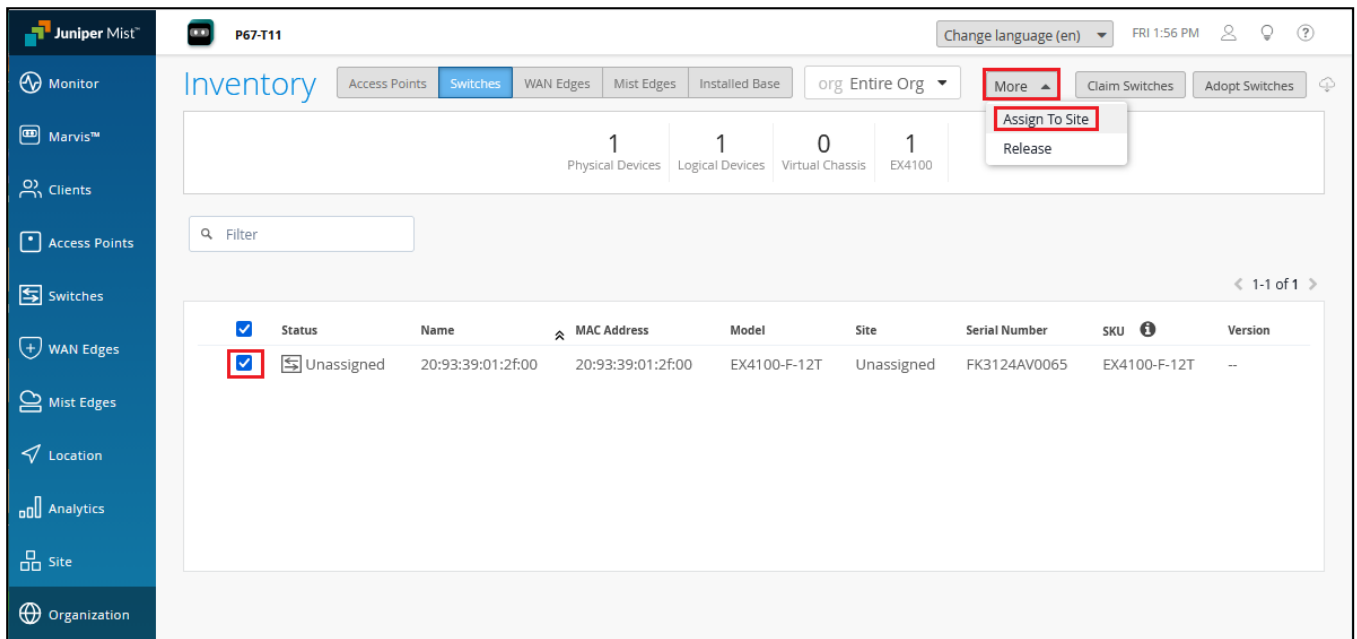
{master:0}[edit]
admin@sw-edge#
```

Leave the SSH session open, return to Mist AI web UI, close the Switch Adoption window and refresh the page. You should see your table switch displayed with Unassigned status.

The screenshot shows the Juniper Mist AI web UI. The left sidebar contains navigation links: Monitor, Marvis™, Clients, Access Points, Switches, WAN Edges, Mist Edges, Location, Analytics, Site, and Organization. The main content area is titled 'Inventory' and has tabs for Access Points, Switches (selected), WAN Edges, Mist Edges, and Installed Base. A summary bar shows 1 Physical Device and 1 Logical Device. Below this is a table with the following data:

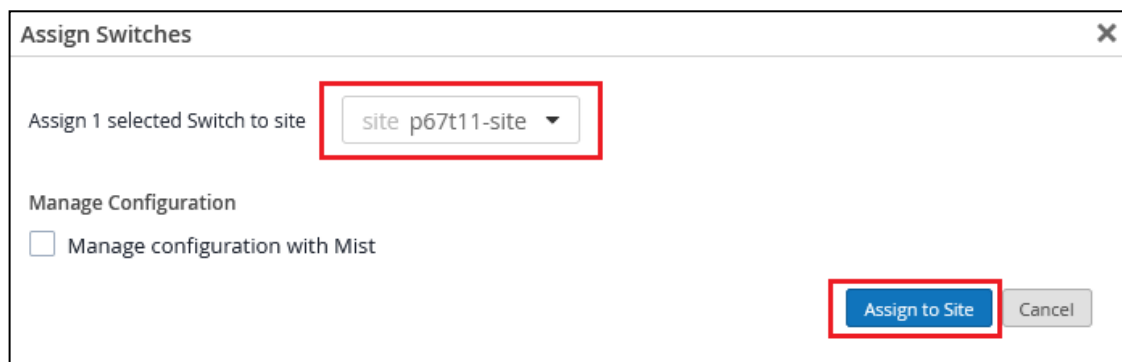
Status	Name	MAC Address	Model	Site	Serial Number	SKU	Version
Unassigned	20:93:39:01:2f:00	20:93:39:01:2f:00	EX4100-F-12T	Unassigned	FK3124AV0065	EX4100-F-12T	--

Select your switch with a checkbox, then click **More** at the top of the screen and click **Assign to Site**.

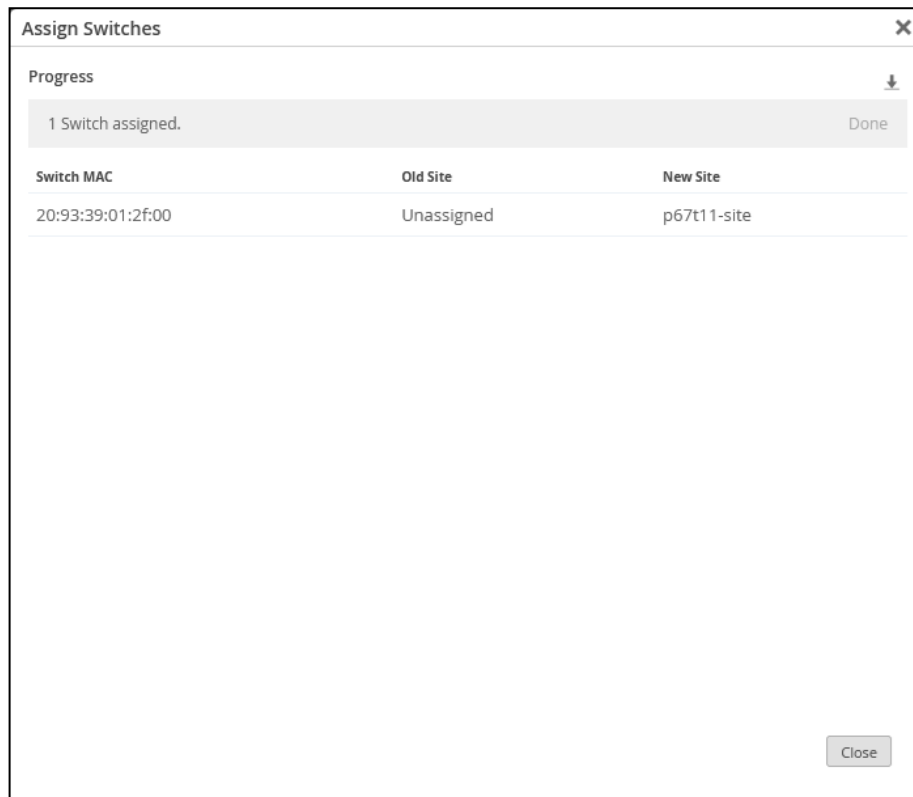


In a popup window recently created site should be selected (**p67t11-site**), leave “Manage configuration with Mist” checkbox **disabled** and click **Assign to Site**.

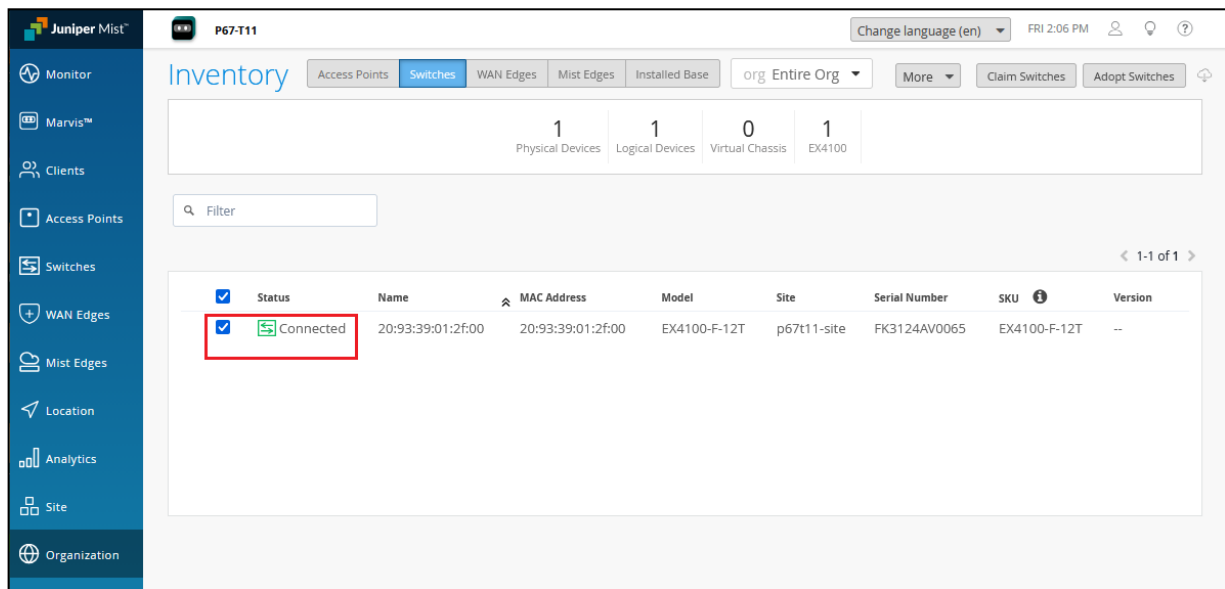
NOTE: Do not enable Manage Configuration yet, you will enable it later when your complete the configuration template settings.



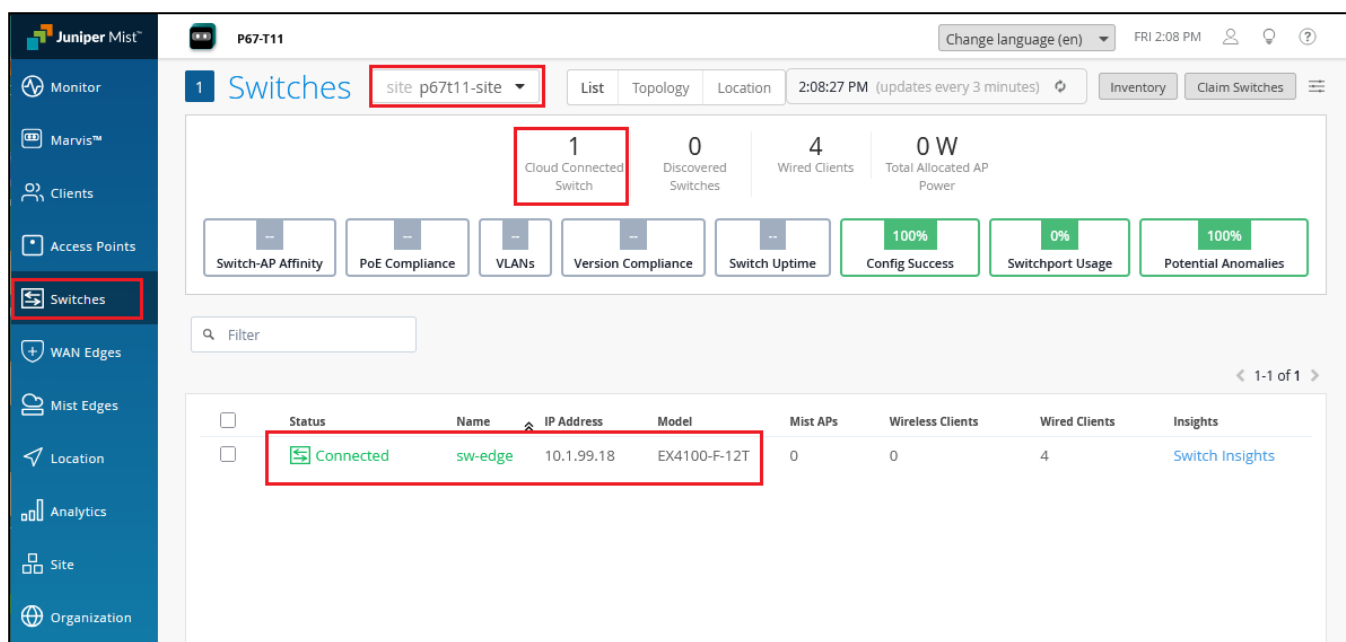
Review site assignment changes and click **Close**.



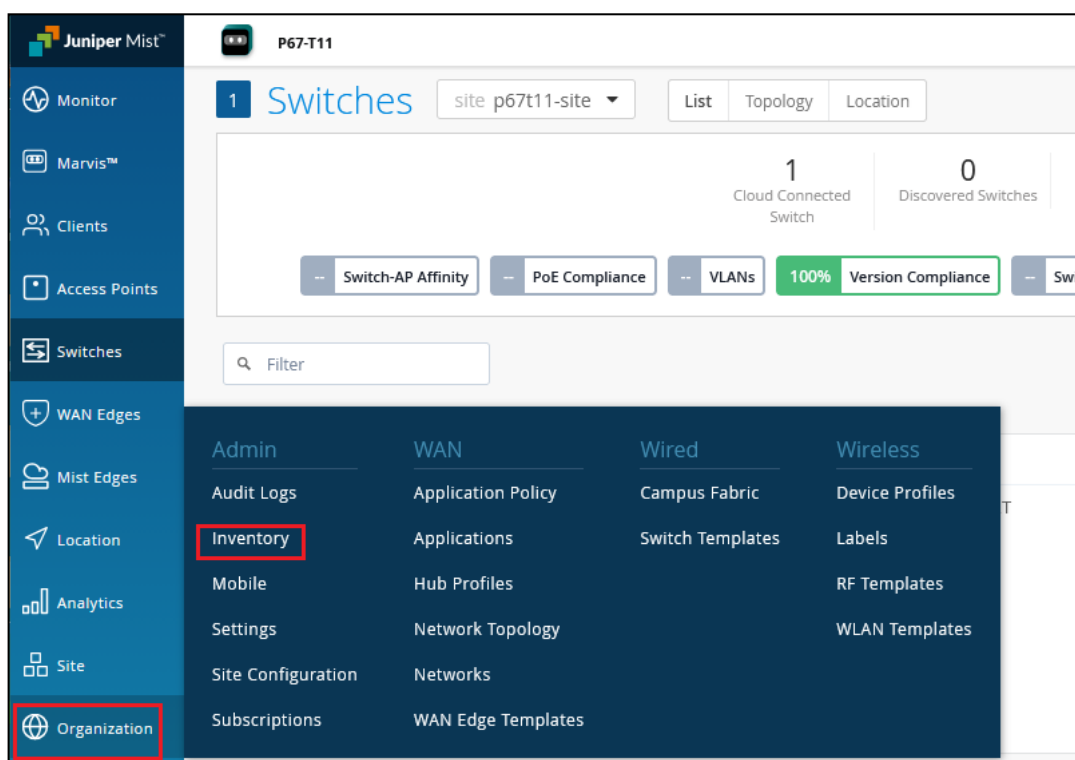
Confirm that your switch is displayed with Connected status in Mist organization inventory.



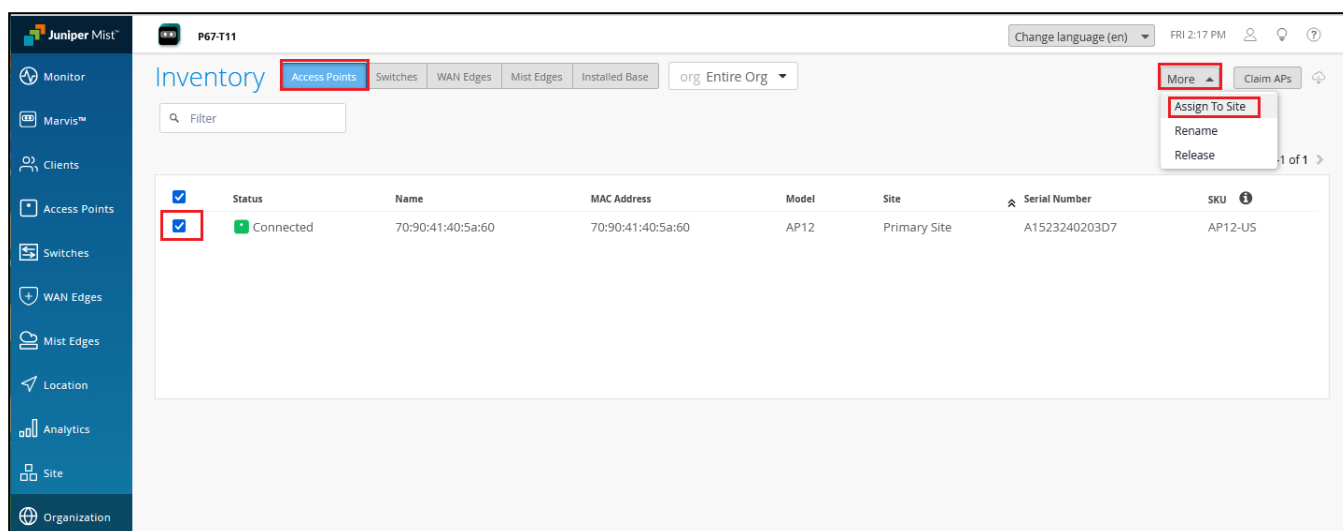
Navigate to Switches section in the left-hand side-bar menu and confirm that your switch is listed with connected status and config success state.



Navigate to Organization > Admin > Inventory.



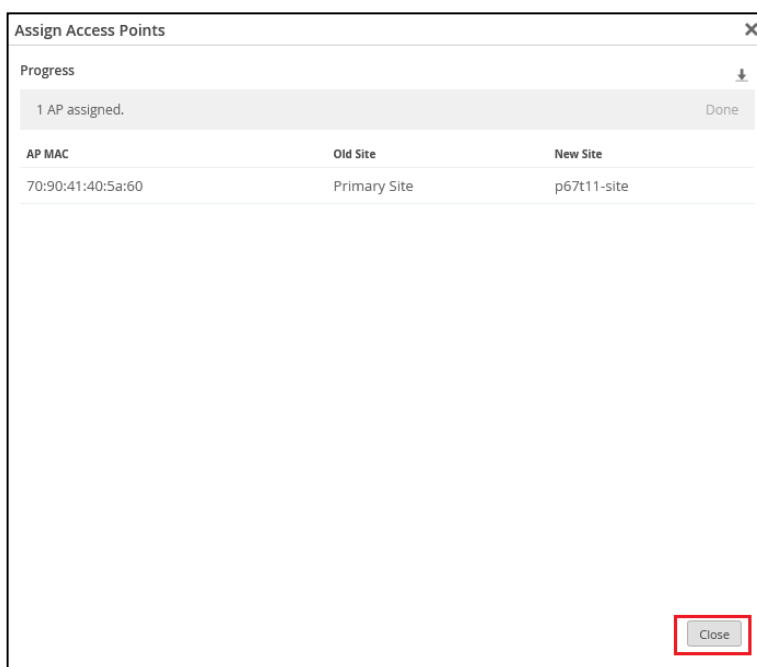
In Access Points tab select your Mist AP, click More and Assign to Site.



Select your site and click **Assign to Site**.



Review and close the site assignment changes window.



Task 2-3: Validate and monitor Juniper EX Switch connectivity to Mist AI

Objectives

Practice with Mist AI monitoring and troubleshooting tools.

Practice with JunosOS CLI troubleshooting and validation commands.

Steps

In Mist AI, navigate to Switches section in left-hand sidebar menu and click on your switch name.

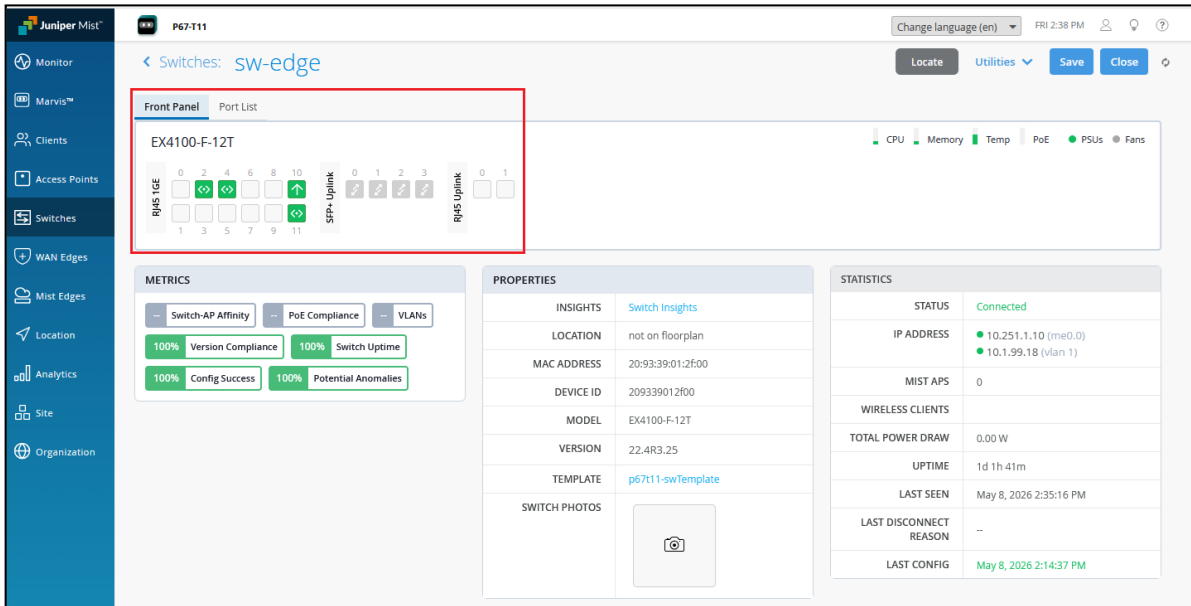
Status	Name	IP Address	Model	Mist APs	Wireless Clients	Wired Clients	Insights
Connected	sw-edge	10.1.99.18	EX4100-F-12T	0	0	4	Switch Insights

Review sw-edge2 statistics. This page shows connection status between the switch and Mist AI, static and dynamic IP addresses, uptime, last config and other details.

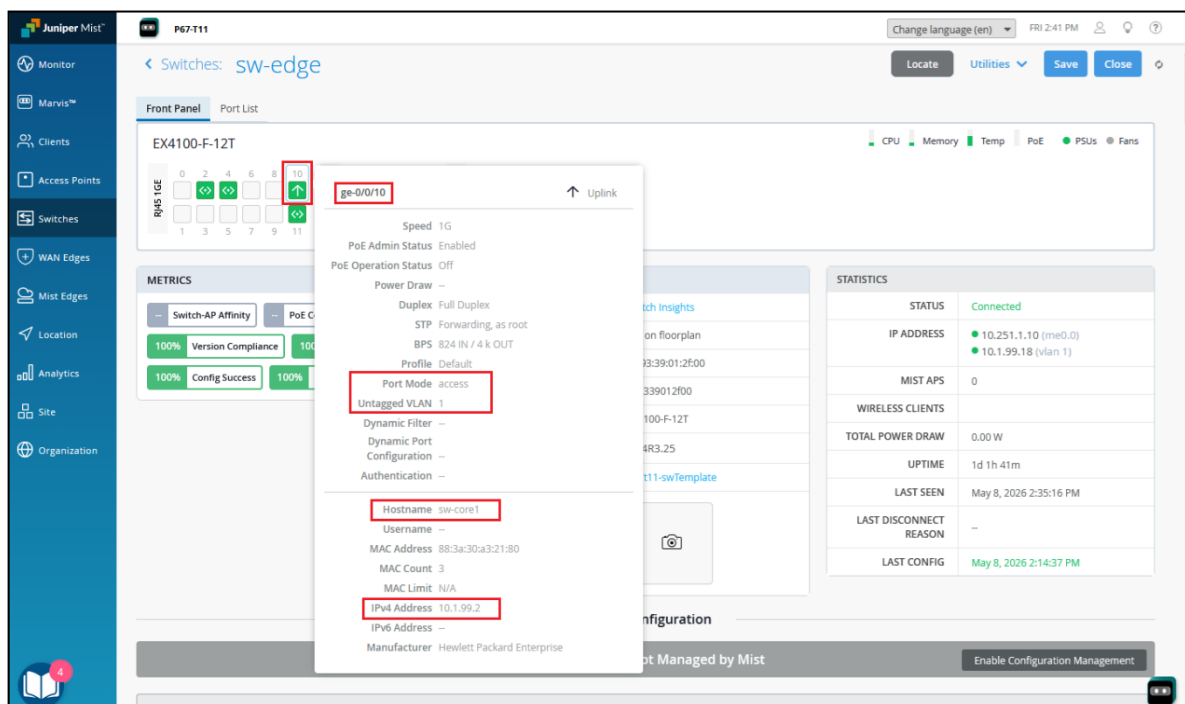
STATUS	Connected
IP ADDRESS	10.251.1.10 (me0.0) 10.1.99.18 (vlan 1)
MIST APS	0
WIRELESS CLIENTS	0
TOTAL POWER DRAW	0.00 W
UPTIME	1d 1h 35m
LAST SEEN	May 8, 2026 2:30:16 PM
LAST DISCONNECT REASON	--
LAST CONFIG	May 8, 2026 2:14:37 PM

NOTE: Mist AP is not connected directly to your table Juniper EX switch, instead it's connected through a fanout PoE switch. That is why Mist AP is not displayed in statistics.

Review the front panel of the switch. Port 10 is connected to sw-core1, port 11 is connected to sw-core-2, port 2 is connected to Mist AP through a fanout switch and port 4 is connected to a testing client PC4 through a fanout switch, ESXi host and virtual distribution switch vDS.



Hover your mouse over port 10. This allows you to see details about your port configuration and devices which are connected through this port. You should see sw-core1 listed with its IP address.



Hover your mouse over port 11 to see details about this port configuration and sw-core2 hostname and IP address, then hover your mouse over ports 2 and 4 to review details.

Click on **port 10** to access port configuration, statistics and troubleshooting. On this page you can assign port profiles, access live traffic counters, bounce port, perform cable test, clear MAC and capture packets.

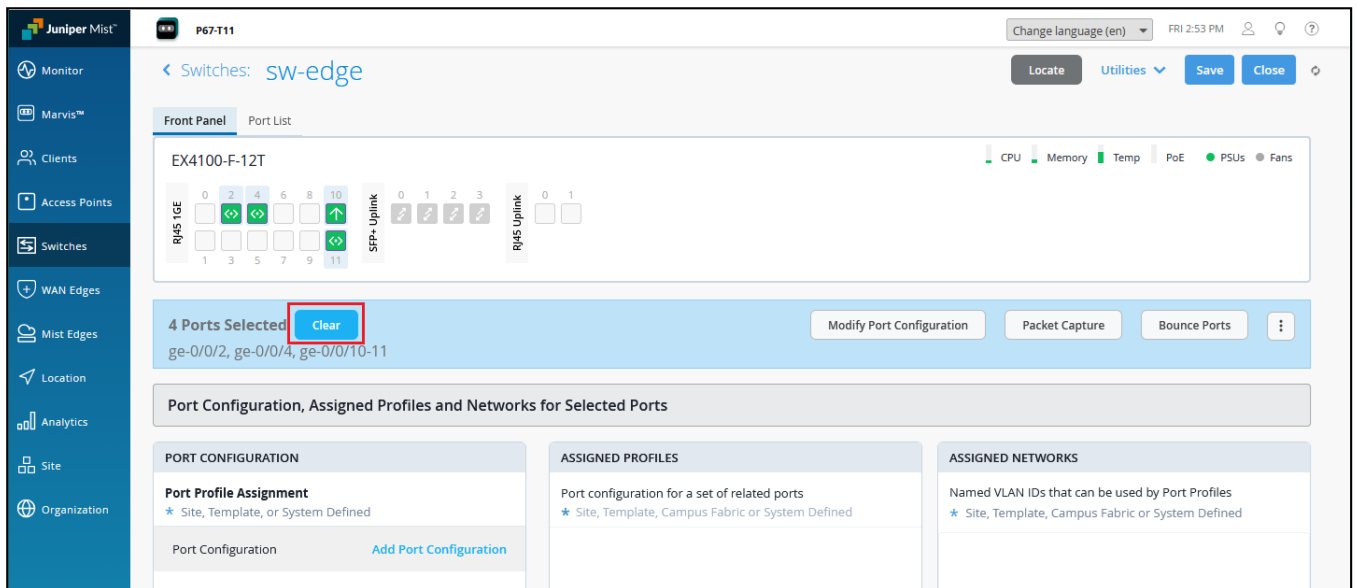
The screenshot shows the Juniper Mist web interface for switch **sw-edge**. The **Port List** tab is active, showing a grid of ports. Port 10 is highlighted with a red box. Below the grid, the **1 Port Selected** section shows the selected port **ge-0/0/10**. The **Port Configuration, Assigned Profiles and Networks for Selected Ports** section is expanded, showing the **PORT CONFIGURATION** tab. The **Port Profile Assignment** section shows a list of port configurations. The **ASSIGNED PROFILES** section shows a list of profiles. The **Port Statistics** section shows a table of statistics for the selected port.

STATISTICS	
SPEED	1G
POWER ALLOCATED	--
POE ADMIN STATUS	Enabled
POE PRIORITY	--
POE OPERATION STATUS	Off
POE OPERATION STATUS DETAIL	--
FULL DUPLEX	Yes
BPS (TX/RX)	18 k / 1 k

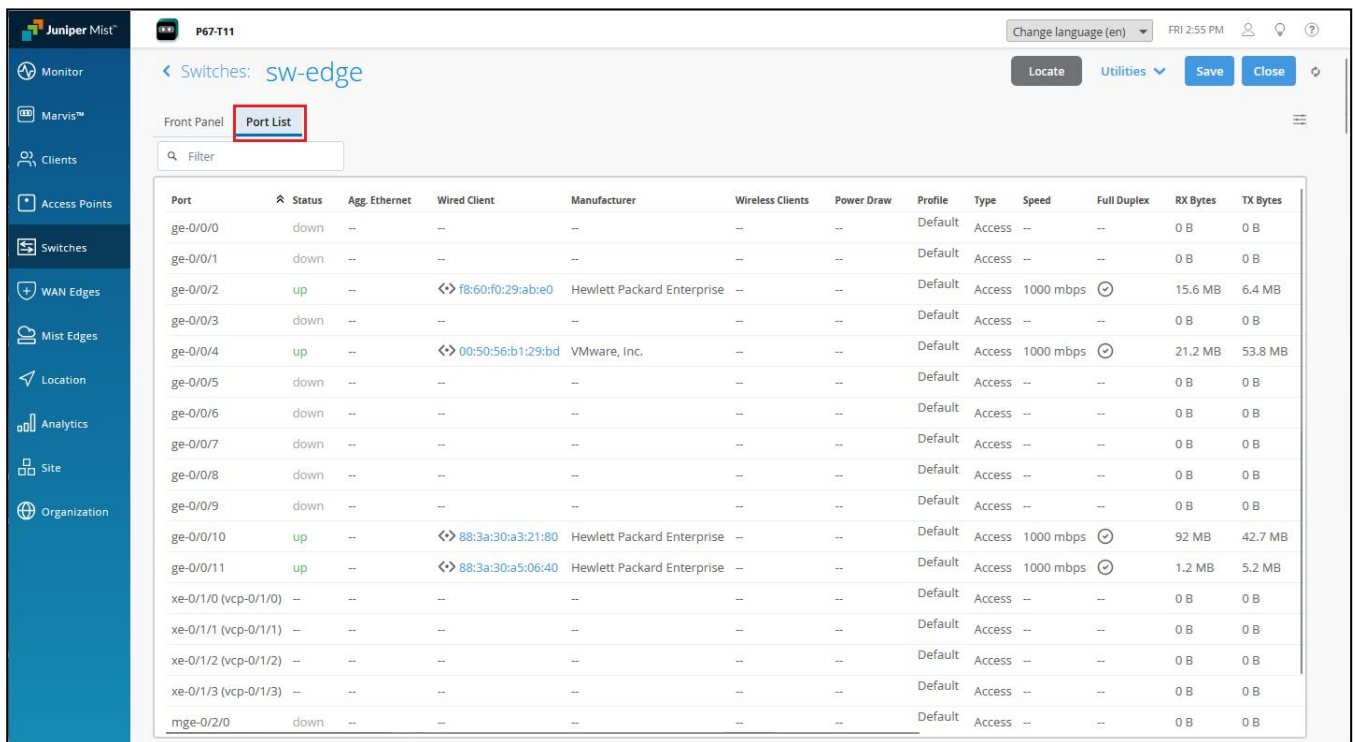
Click on ports 11, 2 and 4. This allows you to select multiple ports and change their settings.

The screenshot shows the Juniper Mist web interface for switch **sw-edge**. The **Port List** tab is active, showing a grid of ports. Ports 11, 2, and 4 are highlighted with red boxes. Below the grid, the **4 Ports Selected** section shows the selected ports **ge-0/0/2, ge-0/0/4, ge-0/0/10-11**. The **Port Configuration, Assigned Profiles and Networks for Selected Ports** section is expanded, showing the **PORT CONFIGURATION** tab. The **Port Profile Assignment** section shows a list of port configurations. The **ASSIGNED PROFILES** section shows a list of profiles. The **ASSIGNED NETWORKS** section shows a list of networks.

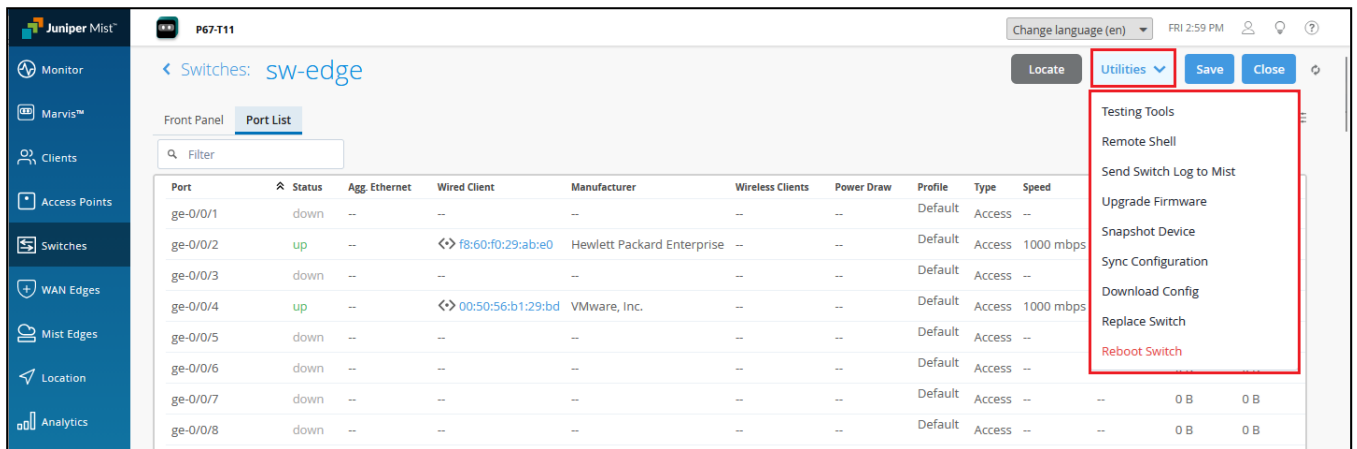
Click **Clear** to unselect all ports or click on each selected port.



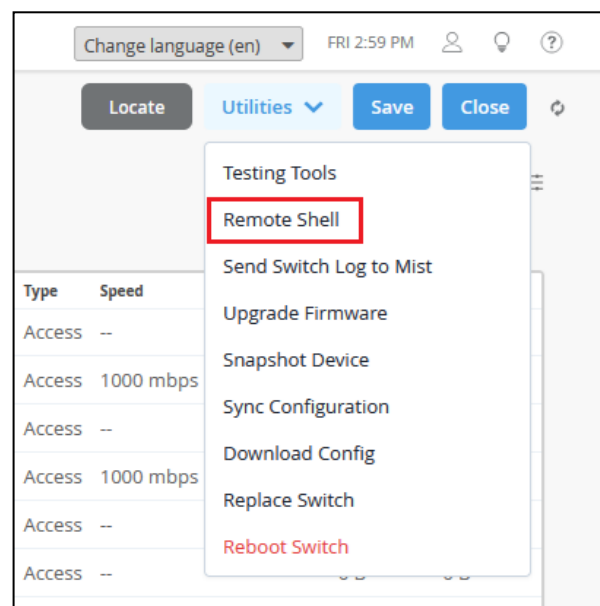
Switch to **port list** view. In this view you can select and unselect one or multiple ports to modify their configuration and review details about wired clients, port profiles and statistics. You can access client monitoring if you click on a client MAC address.



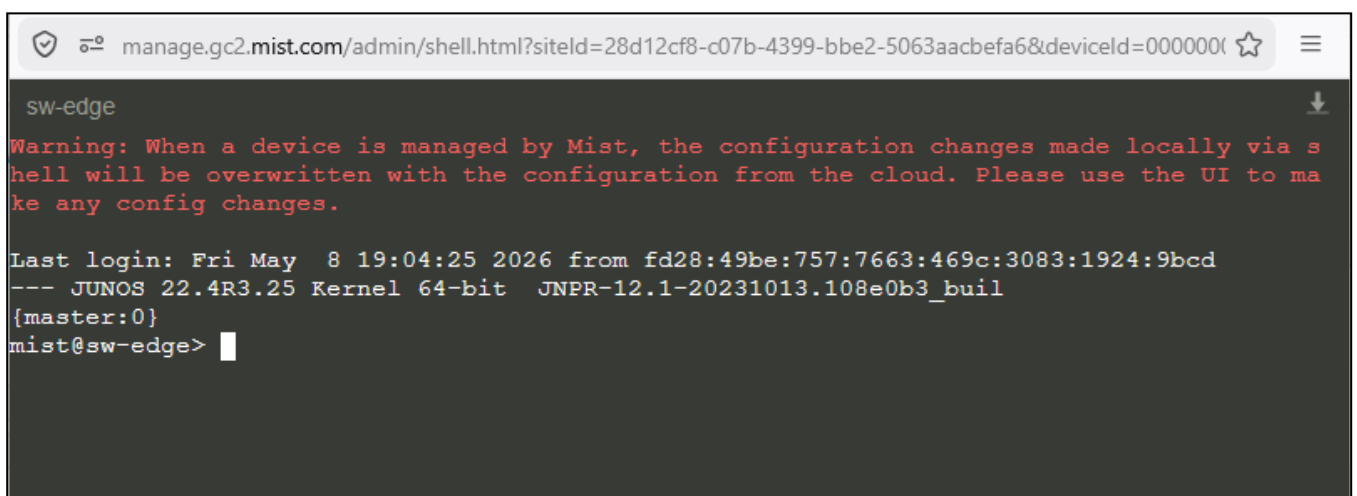
On your switch page, click **Utilities** in the top-right corner. This menu allows you to run different testing tools, open a remote shell, trigger to send switch log to Mist, Upgrade your switch firmware, take your device snapshot, trigger configuration synchronization, download your switch config, initiate switch replacement or reboot your switch.



Click on Remote Shell.



Read carefully the warning message about the switch configuration when it's managed in Mist AI.



Enter command “ping count 5 github.com” and review the output.

```
mist@sw-edge> ping count 5 github.com
PING github.com (140.82.112.4): 56 data bytes
64 bytes from 140.82.112.4: icmp_seq=0 ttl=243 time=31.940 ms
64 bytes from 140.82.112.4: icmp_seq=1 ttl=46 time=29.259 ms
64 bytes from 140.82.112.4: icmp_seq=2 ttl=243 time=33.563 ms
64 bytes from 140.82.112.4: icmp_seq=3 ttl=46 time=30.005 ms
64 bytes from 140.82.112.4: icmp_seq=4 ttl=243 time=34.718 ms

--- github.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 29.259/31.897/34.718/2.063 ms

{master:0}
mist@sw-edge>
```

Get a brief information about your switch interfaces in CLI with “show interface terse” command.

```
mist@sw-edge> show interfaces terse
Interface           Admin Link Proto  Local          Remote
ge-0/0/0            up   down
ge-0/0/0.0          up   down eth-switch
gr-0/0/0            up   up
pfe-0/0/0           up   up
pfe-0/0/0.16383     up   up   inet
                   up   up   inet6

pfh-0/0/0           up   up
pfh-0/0/0.16383     up   up   inet
pfh-0/0/0.16384     up   up   inet
ge-0/0/1            up   down
ge-0/0/1.0          up   down eth-switch
ge-0/0/2            up   up
ge-0/0/2.0          up   up   eth-switch
ge-0/0/3            up   down
ge-0/0/3.0          up   down eth-switch
ge-0/0/4            up   up
ge-0/0/4.0          up   up   eth-switch
ge-0/0/5            up   down
ge-0/0/5.0          up   down eth-switch
ge-0/0/6            up   down
ge-0/0/6.0          up   down eth-switch
ge-0/0/7            up   down
ge-0/0/7.0          up   down eth-switch
ge-0/0/8            up   down
ge-0/0/8.0          up   down eth-switch
ge-0/0/9            up   down
ge-0/0/9.0          up   down eth-switch
ge-0/0/10           up   up
ge-0/0/10.0         up   up   eth-switch
ge-0/0/11           up   up
ge-0/0/11.0         up   up   eth-switch
mge-0/2/0           up   down
mge-0/2/0.0         up   down eth-switch
mge-0/2/1           up   down
mge-0/2/1.0         up   down eth-switch
bme0                up   up
```

```

bme0.0          up    up    inet    128.0.0.1/2
               up    up    inet    128.0.0.4/2
               up    up    inet    128.0.0.16/2
               up    up    inet    128.0.0.63/2
cbp0            up    up
dsc             up    up
esi            up    up
fti0           up    up
fti0.1073741824 up    up    inet6   fd28:49be:757:7663:0:2093:3901:2f00/64
gre            up    up
ipip           up    up
irb            up    up
irb.0          up    up    inet    10.1.99.18/24
               up    up    inet6   fe80::2293:3900:1:2f00/64
jsrv           up    up
jsrv.1         up    up    inet    128.0.0.127/2
lo0            up    up
lo0.16385      up    up    inet
lsi            up    up
me0            up    up
me0.0          up    up    eth-switch
mtun           up    up
pimd           up    up
pime           up    up
pip0           up    up
tap            up    up
vme            up    up
vme.0          up    up    inet    10.251.1.10/24
vtep           up    up

{master:0}
mist@sw-edge>

```

Type command “show system connections | grep 443” to check connectivity with Mist AI.

```

mist@sw-edge> show system connections | grep 443
tcp4          0      0 10.1.99.18.53588      34.152.35.145.443      ESTABLISHED

{master:0}
mist@sw-edge>

```

Validate system LED status with “show chassis led” command.

```

mist@sw-edge> show chassis led
                LED status for: FPC 0
                -----
LEDs status:
  Alarm LED : Off
  System LED: Green
  Master LED: Green
Cloud LED : SOLID WHITE(Cloud Connected)

Interface      LED(SPD/DPX/ADM/POE)
-----
ge-0/0/0       Off
ge-0/0/1       Off
ge-0/0/2       Green

```

```

ge-0/0/3      Off
ge-0/0/4      Green
ge-0/0/5      Off
ge-0/0/6      Off
ge-0/0/7      Off
ge-0/0/8      Off
ge-0/0/9      Off
ge-0/0/10     Green
ge-0/0/11     Green
mge-0/2/0     Off
mge-0/2/1     Off

{master:0}
mist@sw-edge>

```

Check system uptime with “show system uptime” command.

```

mist@sw-edge> show system uptime
fpc0:
-----
Current time: 2026-05-08 19:35:03 UTC
Time Source:  LOCAL CLOCK
System booted: 2026-05-07 16:53:37 UTC (1d 02:41 ago)
Protocols started: 2026-05-07 16:55:34 UTC (1d 02:39 ago)
Last configured: 2026-05-08 17:49:13 UTC (01:45:50 ago) by mist
  7:35PM  up 1 day,  2:41, 2 users, load averages: 1.10, 0.79, 0.66

{master:0}
mist@sw-edge>

```

Display list of logged in admin users.

```

mist@sw-edge> show system users
fpc0:
-----
  7:35PM  up 1 day,  2:42, 2 users, load averages: 1.09, 0.80, 0.66
USER      TTY      FROM                                LOGIN@  IDLE WHAT
mist      pts/1    fd28:49be:757:7663:469c:3083:1924:9bcd 7:14PM  -  -cli
admin     pts/0    10.251.1.90                        5:28PM  16  -cli

{master:0}
mist@sw-edge>

```

On **MGMT PC**, open SSH session to **sw-core1** with IP 10.251.1.2 and check IP address configured on interface VLAN1. You should see 10.1.99.2/24.

```

sw-core1# show running-config interface vlan1
interface vlan 1
  ip address 10.1.99.2/24
  ip helper-address 10.254.1.21
exit

```

On **sw-core1**, shutdown interface VLAN 1 which is used as a default gateway. This will cause Juniper switch disconnection from Mist AI.

```

sw-core1# configure terminal
sw-core1(config)# interface vlan 1
sw-core1(config-if-vlan)# shutdown

```

On sw-edge2, attempt to ping 1.1.1.1 with count 10. Ping should fail.

```
admin@sw-edge> ping count 10 1.1.1.1
PING 1.1.1.1 (1.1.1.1): 56 data bytes

--- 1.1.1.1 ping statistics ---
10 packets transmitted, 0 packets received, 100% packet loss

{master:0}
admin@sw-edge>
```

On sw-edge2, check LED status. You should see Cloud LED with 5 YELLOW Blink (GW IP is not reachable).

```
admin@sw-edge> show chassis led
LED status for: FPC 0
-----
LEDs status:
  Alarm LED : Off
  System LED: Green
  Master LED: Green
  Cloud LED : 5 YELLOW Blink(GW IP is not reachable)

Interface      LED(SPD/DPX/ADM/POE)
-----
ge-0/0/0       Off
ge-0/0/1       Off
ge-0/0/2       Green
ge-0/0/3       Off
ge-0/0/4       Green
ge-0/0/5       Off
ge-0/0/6       Off
ge-0/0/7       Off
ge-0/0/8       Off
ge-0/0/9       Off
ge-0/0/10      Green
ge-0/0/11      Green
mge-0/2/0      Off
mge-0/2/1      Off

{master:0}
admin@sw-edge>
```

On sw-edge2, troubleshoot Mist AI connectivity with CLI command “op mist_debug.py check-connectivity”. This command should give you the same conclusion as Cloud LED status.

```
admin@sw-edge> op mist_debug.py cmd check-connectivity
Starting Cloud Connection Troubleshooting
Management routing-instance is not configured
Checking if Switch IP is configured...
Switch IPs configured: ['10.1.99.18', '10.251.1.10']
-----
Checking if Gateway is configured...
Default gateway is configured: 10.1.99.2
-----
Checking if Gateway is reachable...
Default gateway is not reachable
Failed
```

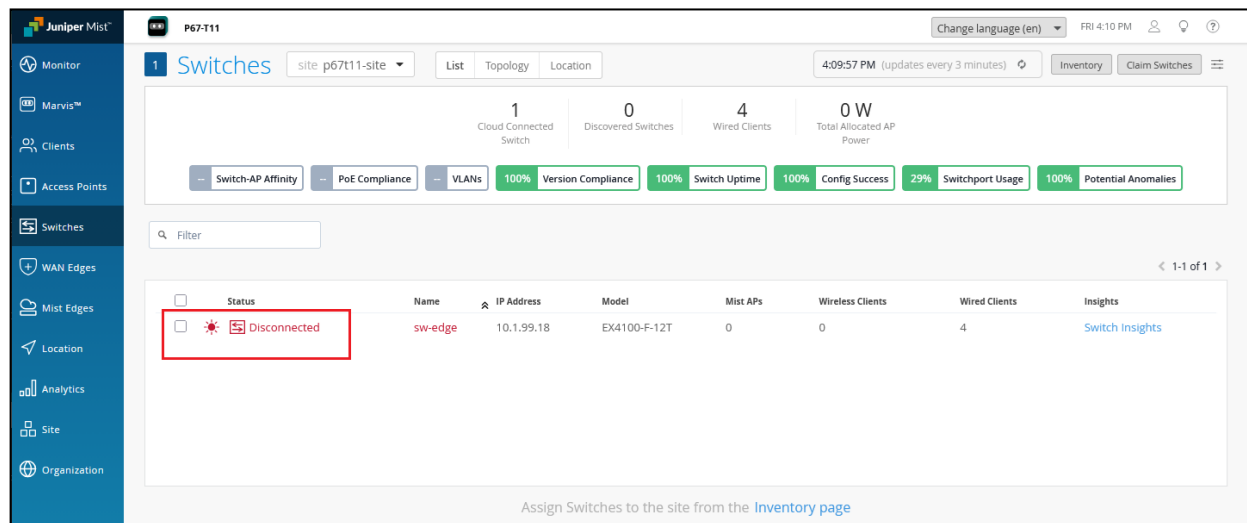
```
Troubleshooting ended with trouble code: GATEWAY_UNREACHABLE
```

```
{master:0}  
admin@sw-edge>
```

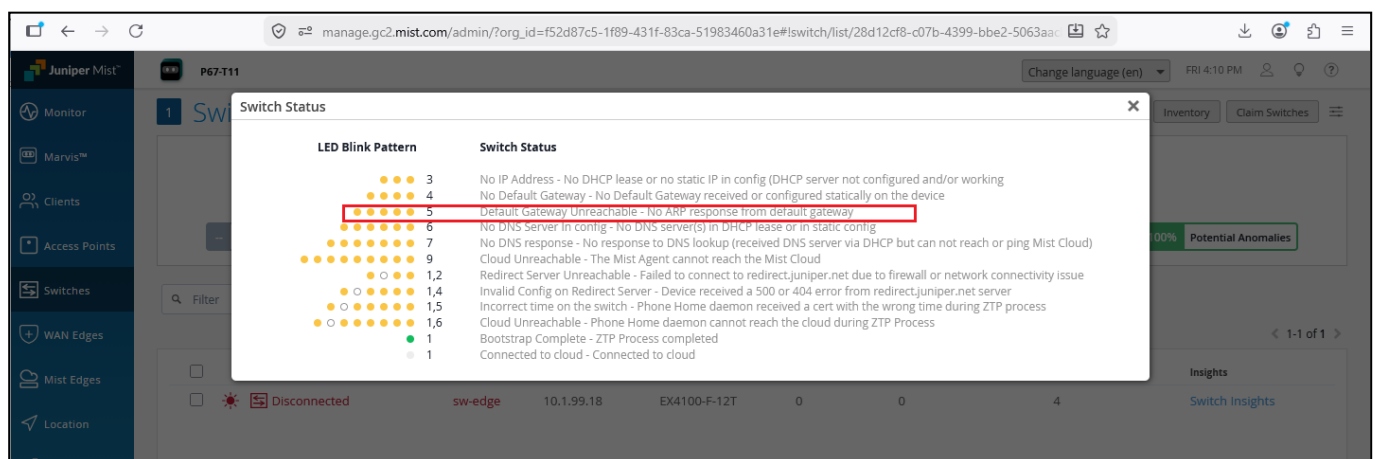
On **sw-edge2**, check TCP session for HTTPS port. It's not established anymore.

```
admin@sw-edge> show system connections | grep 443  
tcp4          0  5034  10.1.99.18.53588  34.152.35.145.443  FIN_WAIT_1  
  
{master:0}  
admin@sw-edge>
```

In Mist AI, refresh the page with switches and confirm that your switch is listed with disconnected status.



Click on your switch in Mist AI to get a description about Cloud LED blink pattern which could help to find the reason of disconnection without CLI access and with only visual contact. Close Switch status windows when you are done reading.

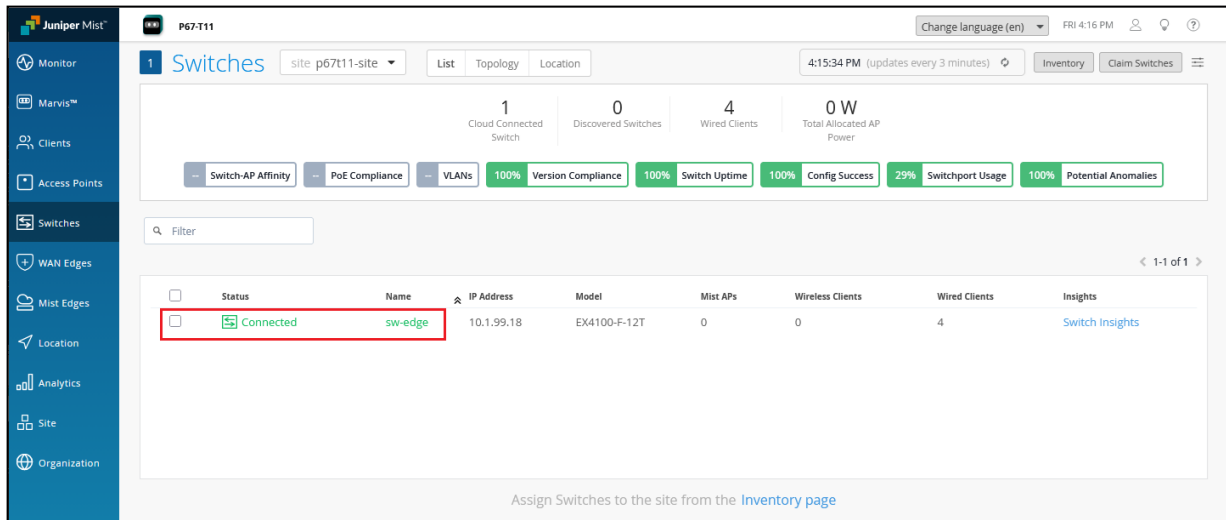


On **MGMT PC**, in SSH session to **sw-core1**, enable interface VLAN 1.

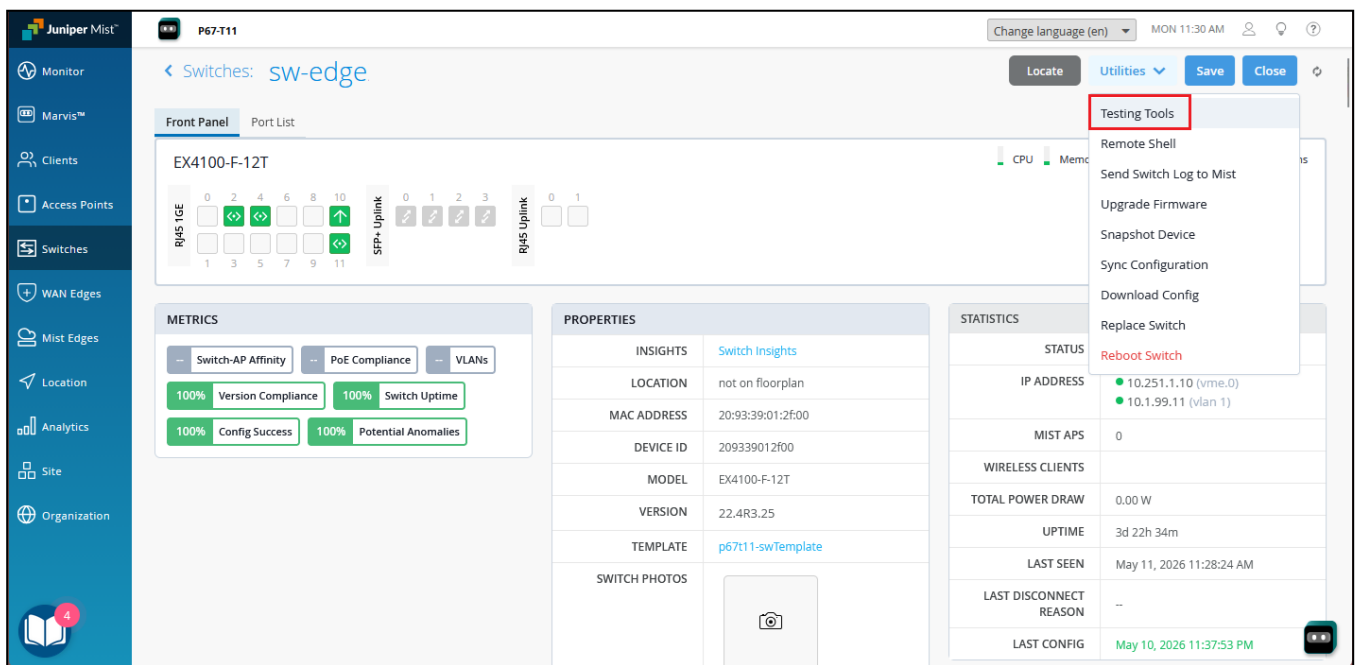
```
sw-core1(config-if-vlan)# no shutdown  
sw-core1(config-if-vlan)# end
```


sw-core1#

Return to Mist AI, refresh the page with switches and confirm that your switch is now listed with connected status. **Click** on your switch name.



Click Utilities, then Testing Tools.



Enter "10.254.1.21" in hostname field and 5 on count. Click **Ping**. Ping should be successful.



Ping 10.254.1.21

```
May 11, 2026 11:33:55 AM
PING 10.254.1.21 (10.254.1.21): 56 data bytes
64 bytes from 10.254.1.21: icmp_seq=0 ttl=126 time=13.389 ms
64 bytes from 10.254.1.21: icmp_seq=1 ttl=126 time=12.461 ms
64 bytes from 10.254.1.21: icmp_seq=2 ttl=126 time=12.795 ms
64 bytes from 10.254.1.21: icmp_seq=3 ttl=126 time=6.151 ms
64 bytes from 10.254.1.21: icmp_seq=4 ttl=126 time=20.096 ms

--- 10.254.1.21 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 6.151/12.978/20.096/4.421 ms
```

Switch to **Traceroute** tab, enter "10.254.1.21" in hostname field and click **Traceroute**. You should see 3 hops.

Traceroute 10.254.1.21

```
May 11, 2026 11:35:09 AM
 1 10.1.99.2 (10.1.99.2) 14.124 ms 9.639 ms 9.738 ms
 2 10.254.101.254 (10.254.101.254) 9.736 ms 9.141 ms 9.739 ms
 3 aruba-ad.training.arubanetworks.com (10.254.1.21) 9.801 ms * 13.784 ms
traceroute to 10.254.1.21 (10.254.1.21), 30 hops max, 52 byte packets
```

Switch to **Cable Test** tab, select port name ge-0/0/4 and click **Cable Test**.

Cable Test ge-0/0/4

```
May 11, 2026 11:36:59 AM

Interface TDR detail:
Test status                  : Test successfully executed ge-0/0/4

Interface TDR detail:
Interface name                : ge-0/0/4
Test status                   : Passed
Link status                   : UP
MDI pair                      : 1-2
  Cable status                 : Normal
  Cable length/Distance To Fault: 0 Meters
MDI pair                      : 3-6
  Cable status                 : Normal
  Cable length/Distance To Fault: 0 Meters
MDI pair                      : 4-5
  Cable status                 : Normal
  Cable length/Distance To Fault: 0 Meters
MDI pair                      : 7-8
  Cable status                 : Normal
  Cable length/Distance To Fault: 0 Meters
Polartiy swap                 : Normal
```

Pair swap	: MDI
Downshift	: No Downshift

Switch to Bounce Port tab, select port name ge-0/0/4 and click Bounce Port.

Bounce Port ge-0/0/4 May 11, 2026 11:38:21 AM Bouncing port... Port bounce complete.
--

Task 2-4: General switch configuration

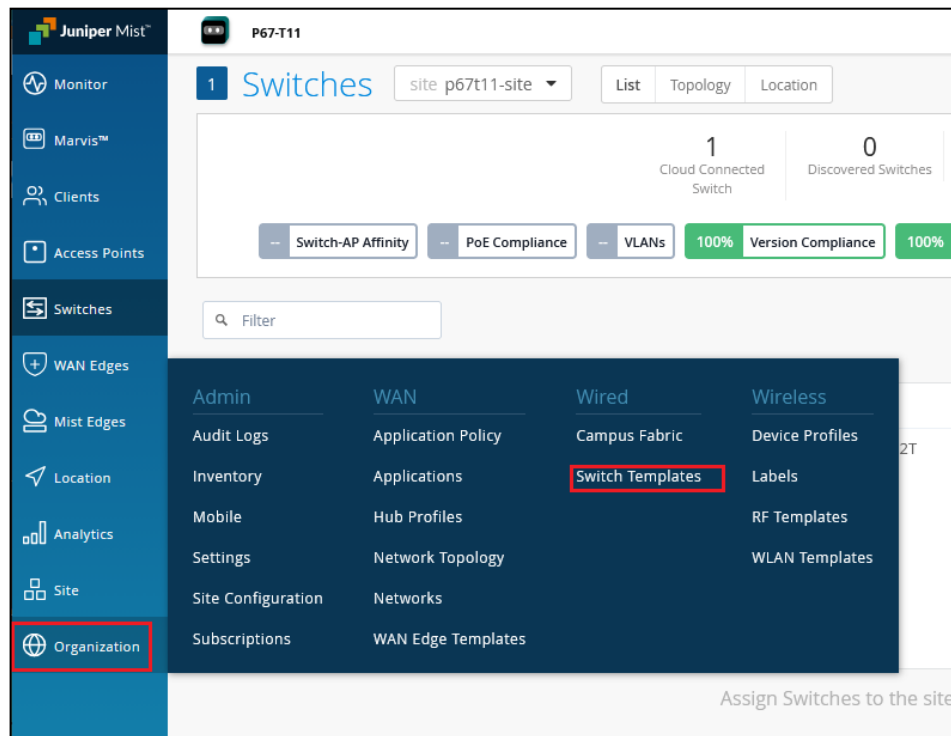
Objectives

Configure Juniper EX switch hostname and MGMT IP address.

Enable configuration management for your switch in Mist AI.

Steps

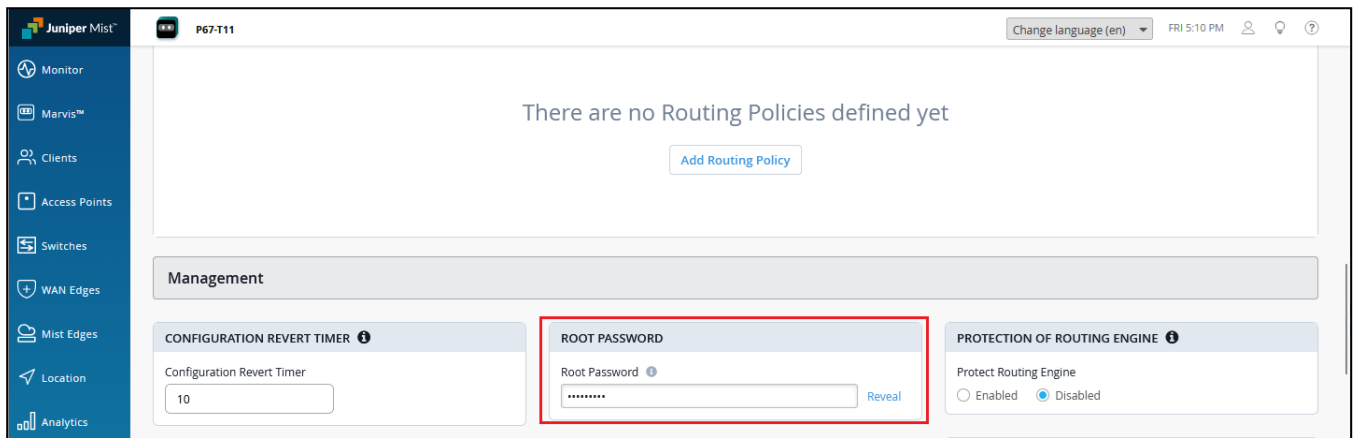
Navigate to Mist AI Organization > Wired > Switch Templates



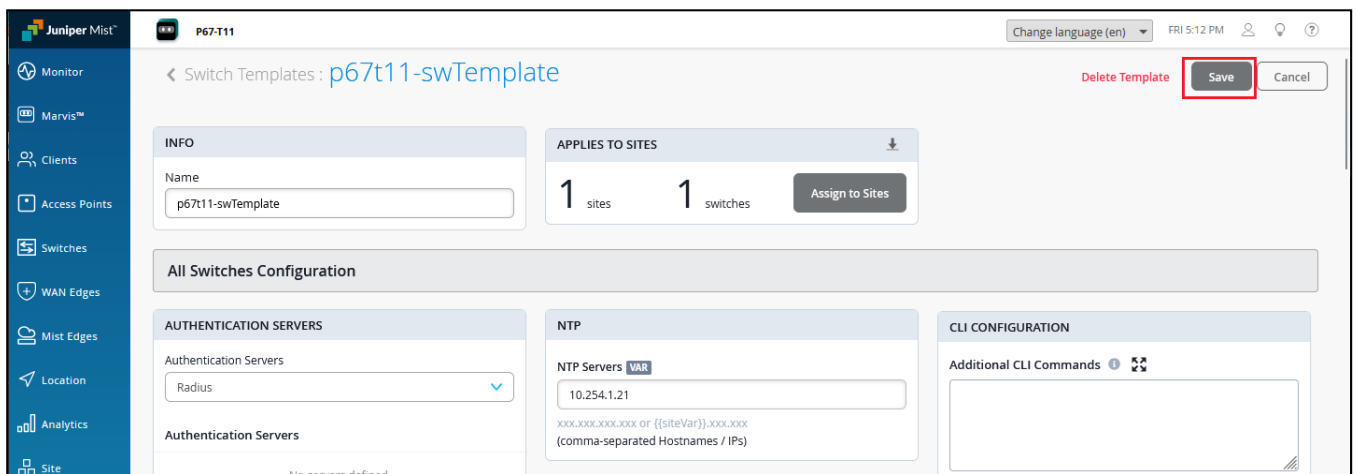
Click template name you configured previously.



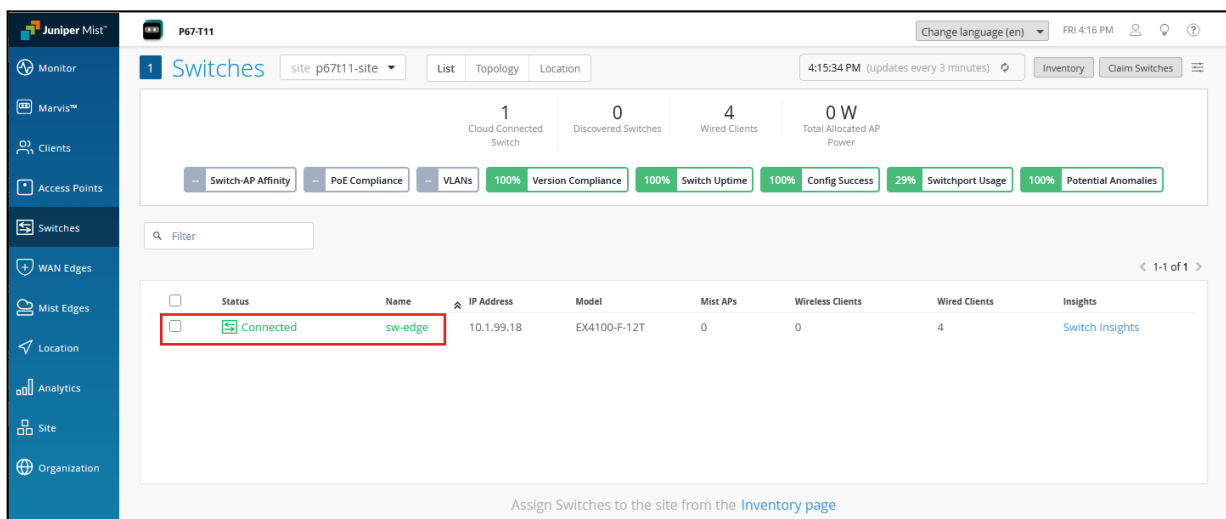
Scroll down till the Management section and enter root password “Aruba123!”.



Click **Save** at the top of the page, then review changes and click **save** again to confirm.



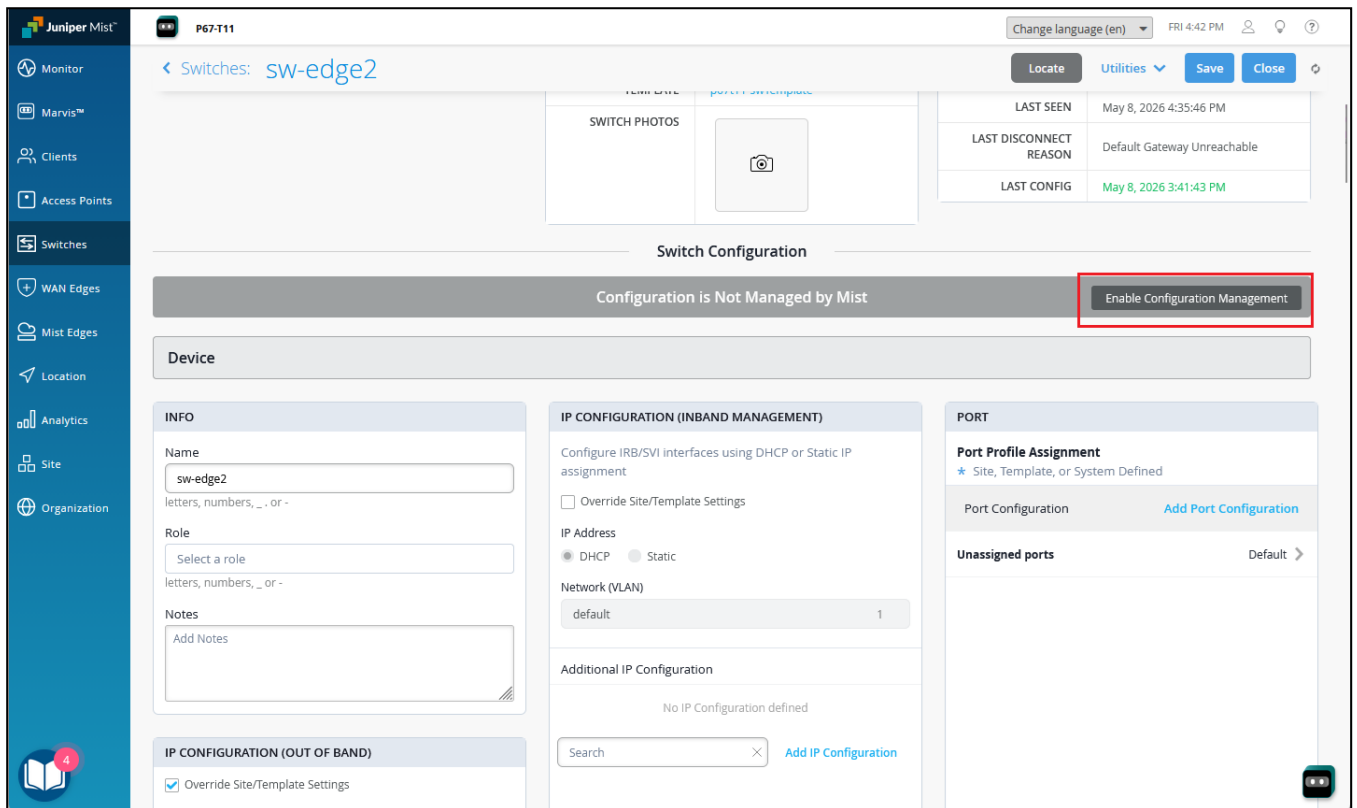
Navigate to Mist AI **switches** and click on your switch.



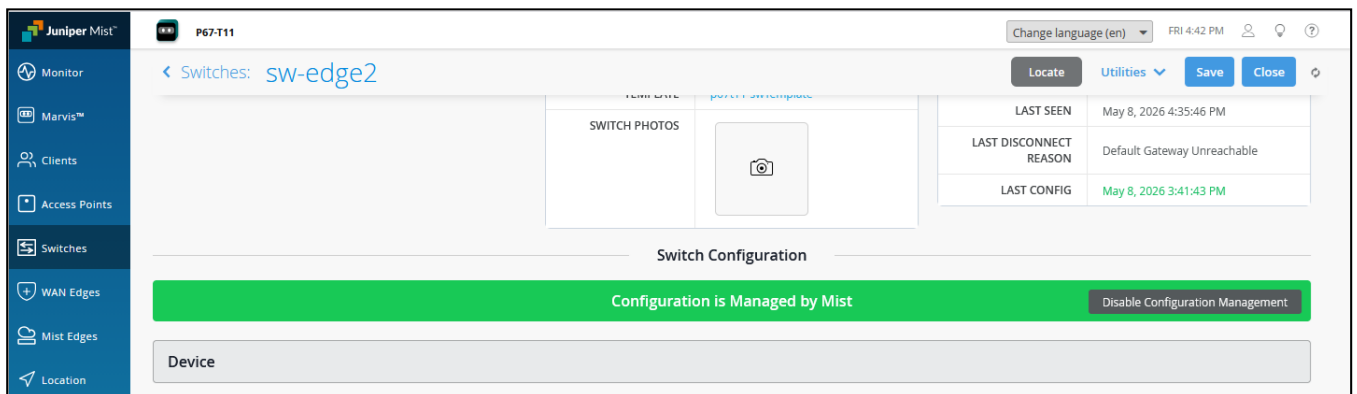
Scroll down to Switch Configuration section, update switch hostname to "sw-edge2", enable override Site/Template settings and set a static Out of Band management IP address to 10.251.1.10/24.
Click **Save**.

Confirm changes by clicking **Save** button.

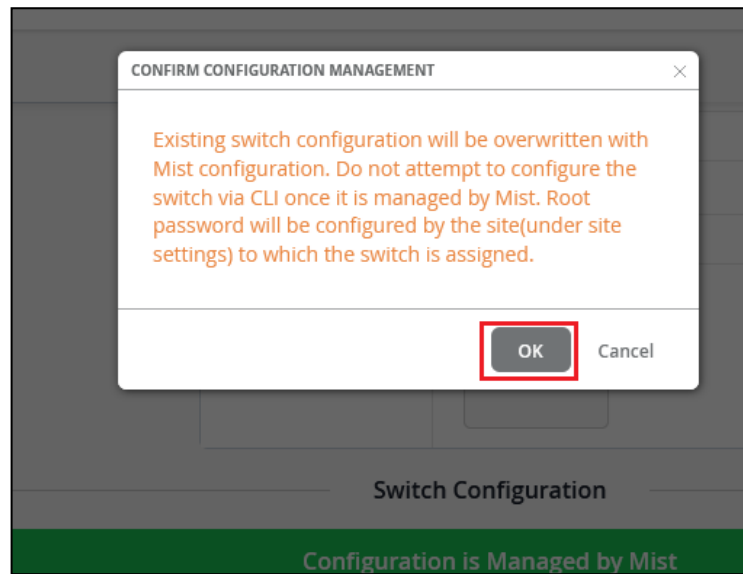
Click **Enable Configuration Management** button.



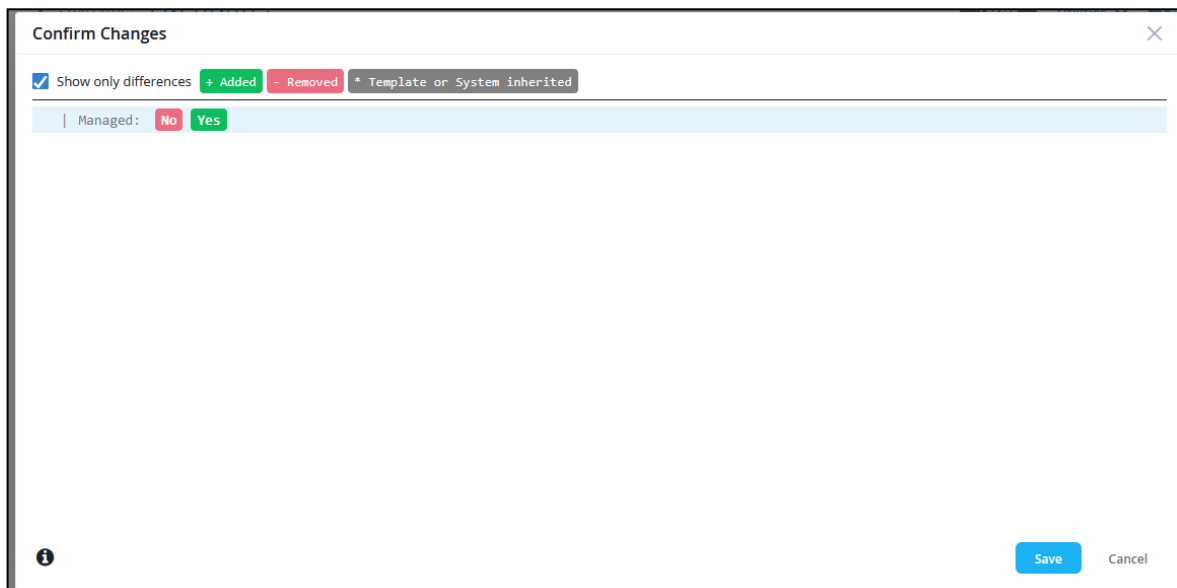
This will change the message to “Configuration is Managed by Mist” and message color from gray to green.



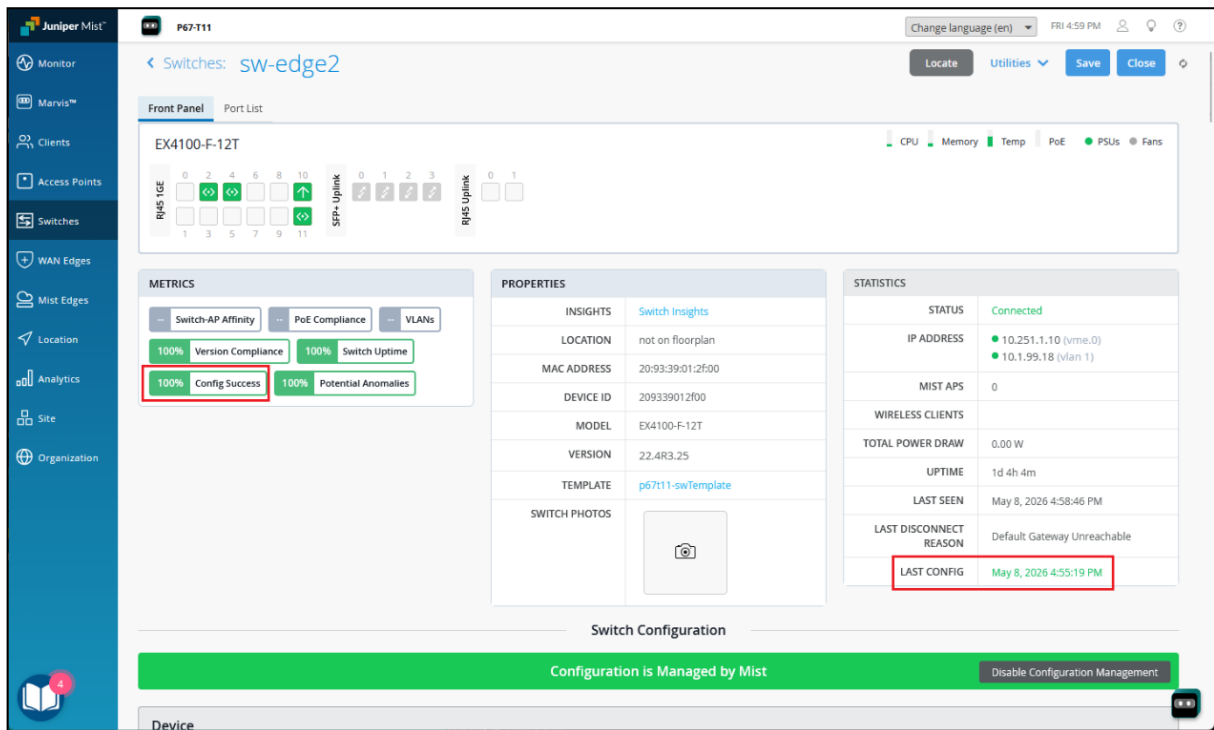
Click **Save** in the top-right corner, then OK to confirm this action.



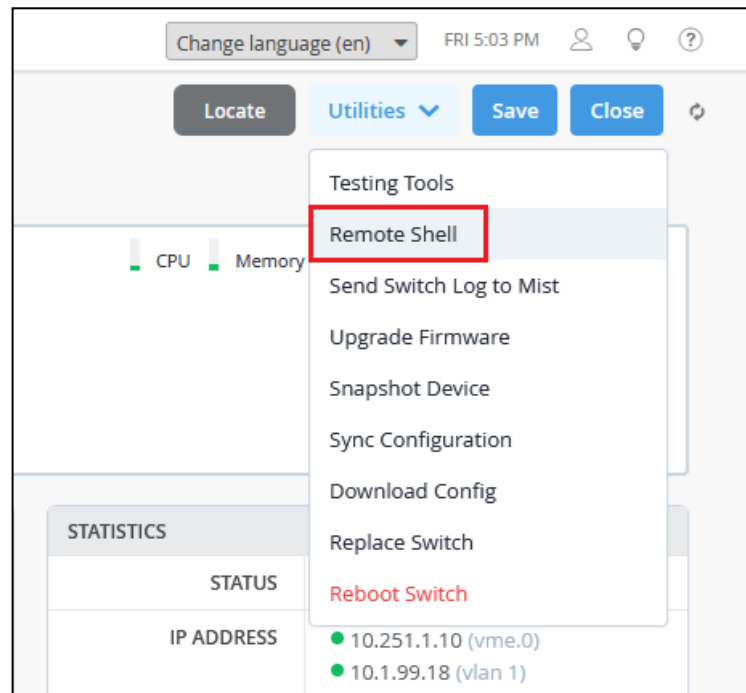
Confirm changes by clicking Save



Wait several minutes, refresh the page and confirm that you can see 100% config Success and last config date which should reflect the timestamp close to the current time in selected time zone.



Click **Utilities** and select **Remote Shell**.



Confirm that the hostname was changed to **sw-edge2** and close remote shell.

Navigate to Mist AI Switches and click Switch Insights.

The screenshot shows the Juniper Mist web interface. On the left is a navigation sidebar with options like Monitor, Marvis, Clients, Access Points, Switches (highlighted with a red box), WAN Edges, Mist Edges, Location, Analytics, Site, and Organization. The main content area is titled 'Switches' and shows a summary for site 'p67t11-site'. It includes metrics for Cloud Connected Switch (1), Discovered Switches (0), Wired Clients (4), and Total Allocated AP Power (0 W). Below these are status bars for various metrics: Switch-AP Affinity, PoE Compliance, VLANs, Version Compliance (100%), Switch Uptime (100%), Config Success (100%), Switchport Usage (29%), and Potential Anomalies (100%). A table lists the switches, with one entry 'sw-edge2' shown. The 'Status' column shows 'Connected', and the 'Insights' column has a red box around the 'Switch Insights' link. At the bottom, there is a link to 'Assign Switches to the site from the Inventory page'.

Find a record stating that switch configuration was changed by User.

The screenshot shows the Juniper Mist 'Monitor' page for switch 'sw-edge2'. The top navigation bar includes 'Wireless', 'Wired', 'WAN', and 'Insights' (selected). Below the header is a graph showing 'Total Bytes' and 'Port Errors' over time. The 'Switch Events' section is expanded, showing a table of events. The first event is 'Config Changed by User' at 4:55:18.004 PM May 8, 2026, which is highlighted with a red box. The 'Admin Info' section on the right shows a log entry: 'Update Device "sw-edge2" by Computer Data (juniper@computerdata.com) at May 8, 2026 4:55:18 PM', also highlighted with a red box.

You have completed this lab!

Lab 3: Day 1: Configure VLANs, ports and LAGs

Objectives

After completing this lab, you will be able to:

- Configure Port profiles and networks configuration
- Complete LAG configuration
- Use Dynamic port configuration
- Implement Network Access Control basics

Overview

After completing this lab, you will become familiar with Juniper MIST AI web interface. Will be able to configure VLANs, port profiles, LAGs, use Dynamic port configuration and implement network access control with ClearPass Policy Manager used as a RADIUS server. Juniper Mist web UI could be changed over the time and will not match screenshots in this workshop. Ask your instructor for assistance if you struggle finding required settings in Juniper Mist.

Task 3-1: Port profiles and networks configuration

Objectives

Use Mist AI Switch Template to configure networks and VLANs

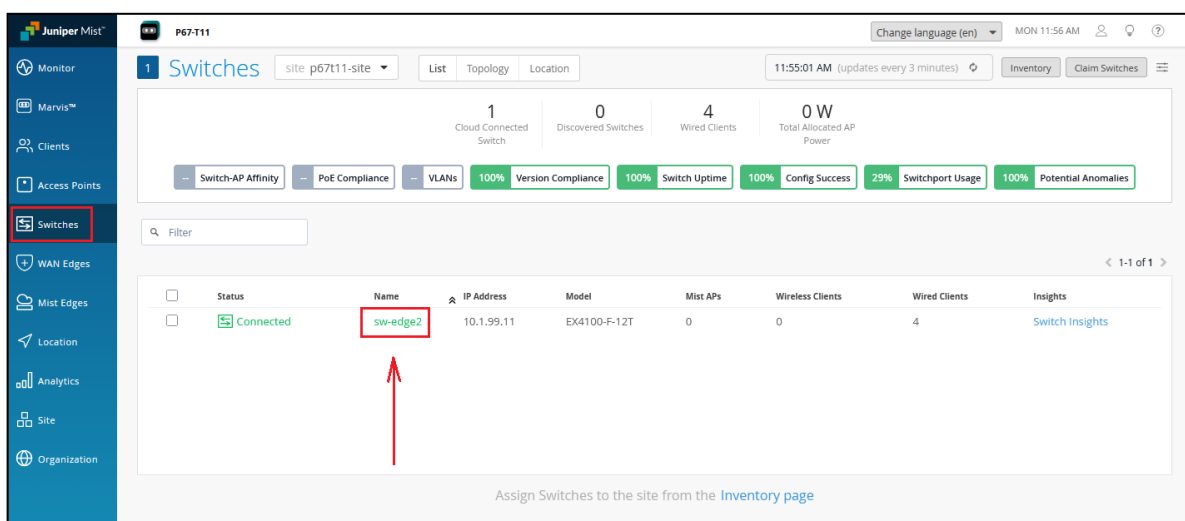
Configure Port Profiles with Switch Templates

Assign Port Profiles to switch ports with Port Configuration

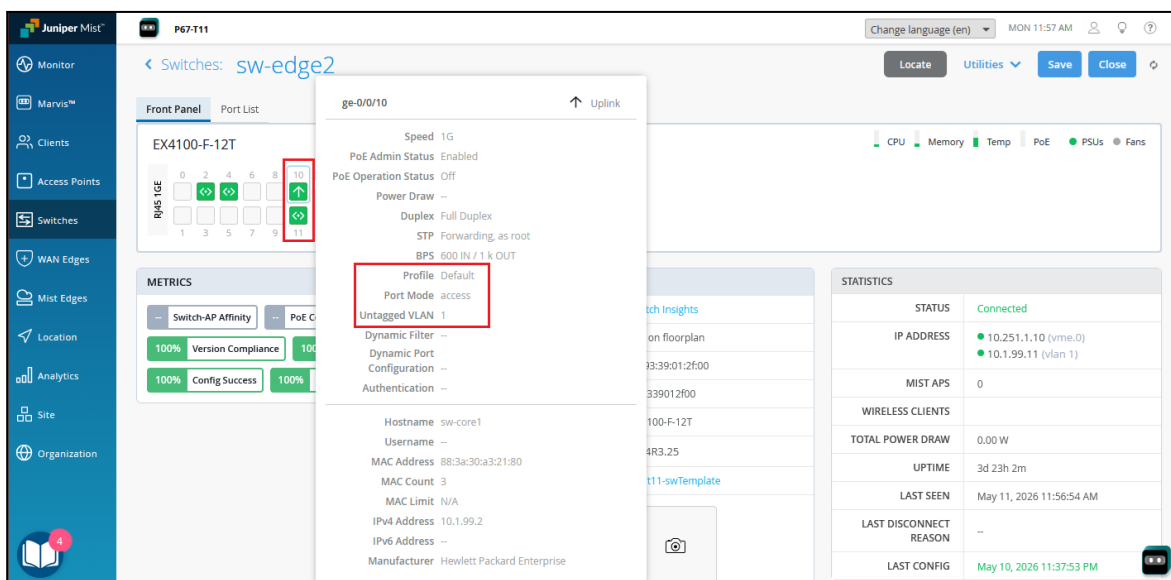
Validate configuration with Front Panel view and CLI commands.

Steps

Navigate to Mist AI Switches page and click on your switch name.

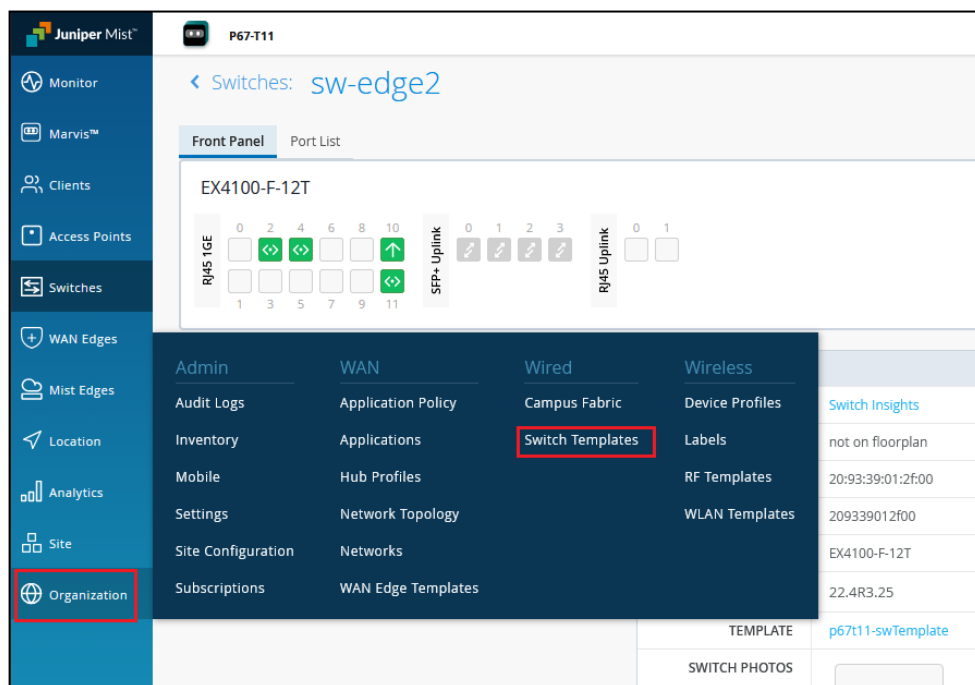


Hover your mouse over switch uplinks – ports 10 and 11. Notice that it shows Default port profile applied and Untagged VLAN 1 which is used in these labs as ZTP VLAN.

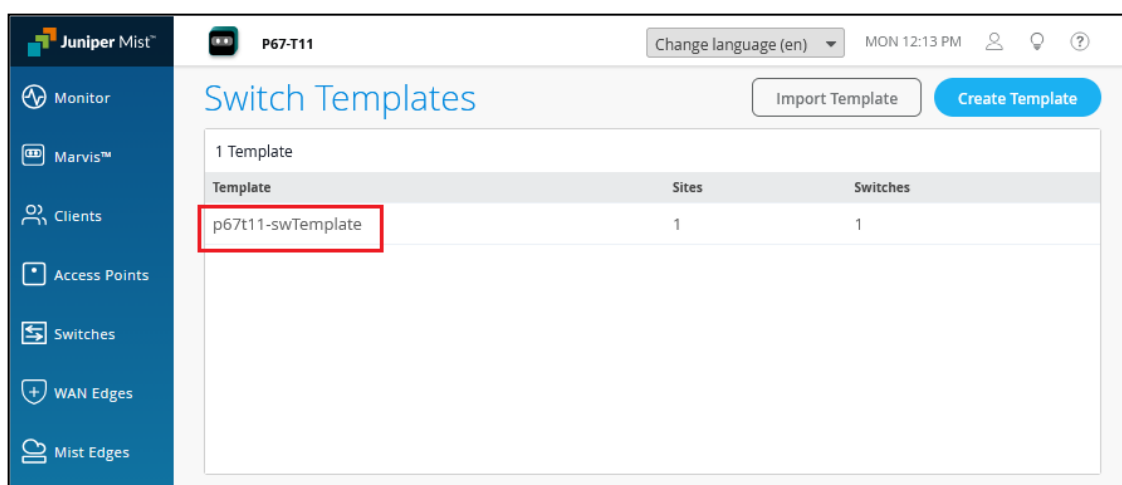


NOTE: Core switches are AOS-CX switches and are preconfigured with VLANs 3, 11-14, VSX and SVIs for these VLANs with virtual IP addresses which are used as default gateway IPs. VSX LAGs on 6300 Core switches are configured with LACP fallback which allows your table Juniper switch to communicate with Mist AI without LAG configured on uplinks. Once LAG is configured on Juniper EX4100 switch it will start sending LACP frames and Core switches will automatically switch VSX LAGs to LACP mode.

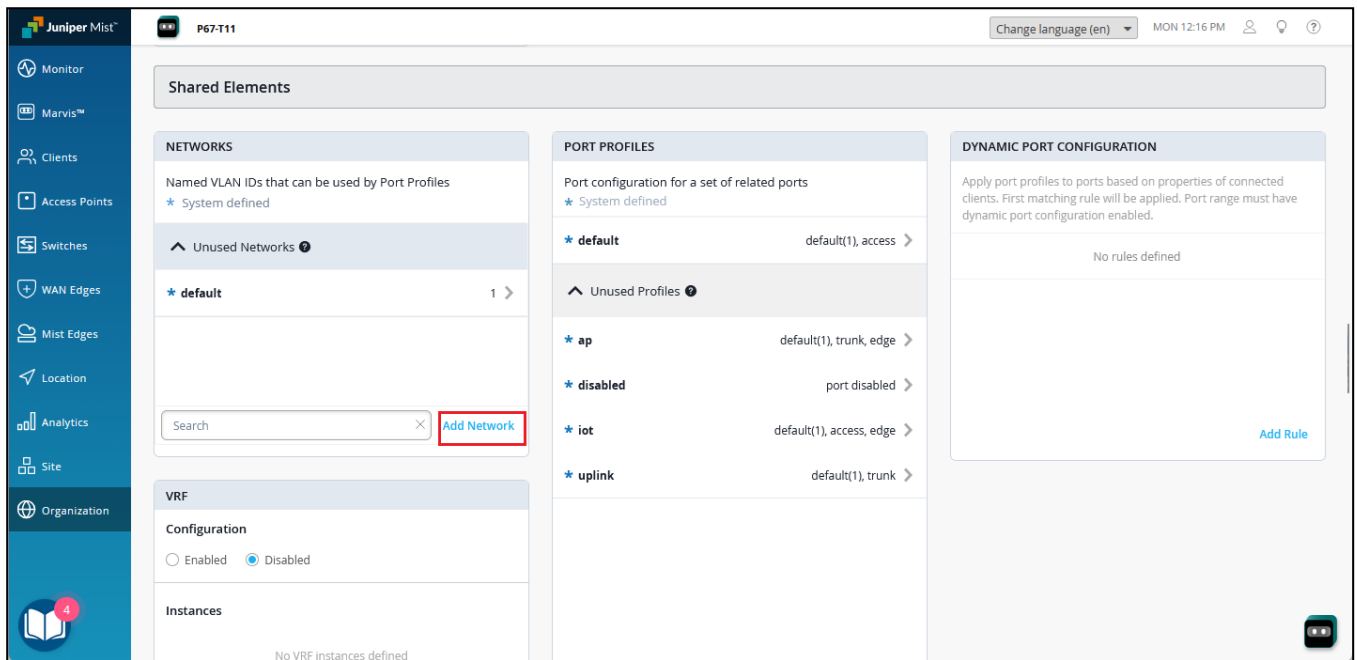
Now it's time to create several networks in Mist AI for your Juniper EX4100 switch. Navigate to Organization > Wired > Switch Templates.



Click on template name you previously created.



Scroll the page down till **Shared Elements** section and click **Add Network**.

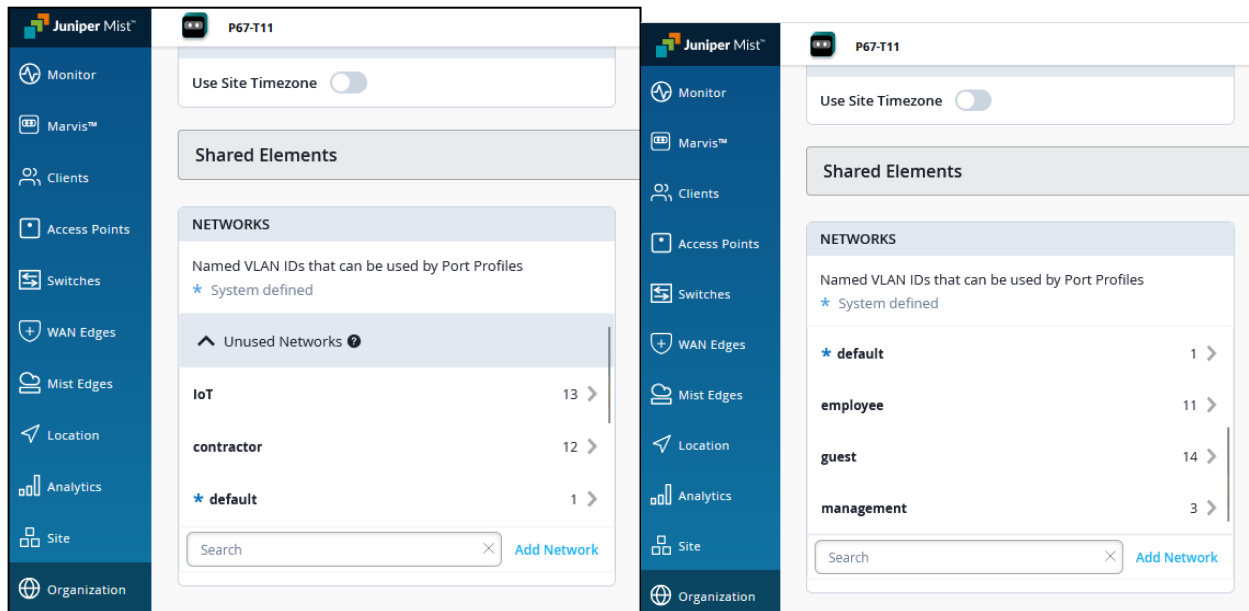


Enter “management” as a name and VLAN ID 3. Click on a check mark to complete new network configuration.

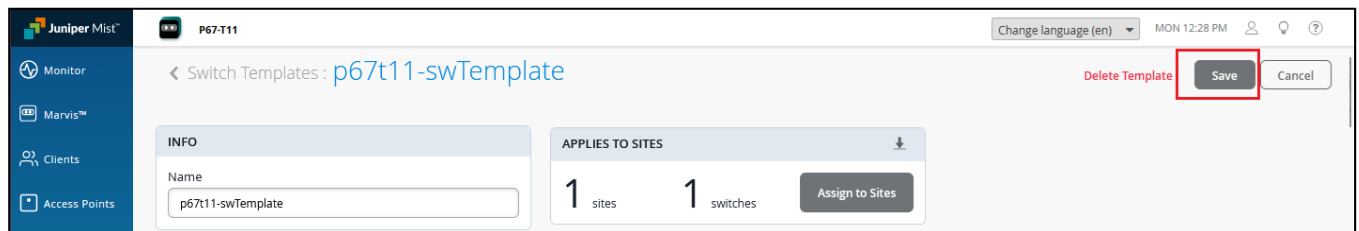
Repeat the previous step to create the following VLANs:

Network Name	VLAN ID
employee	11
contractor	12
IoT	13
guest	14

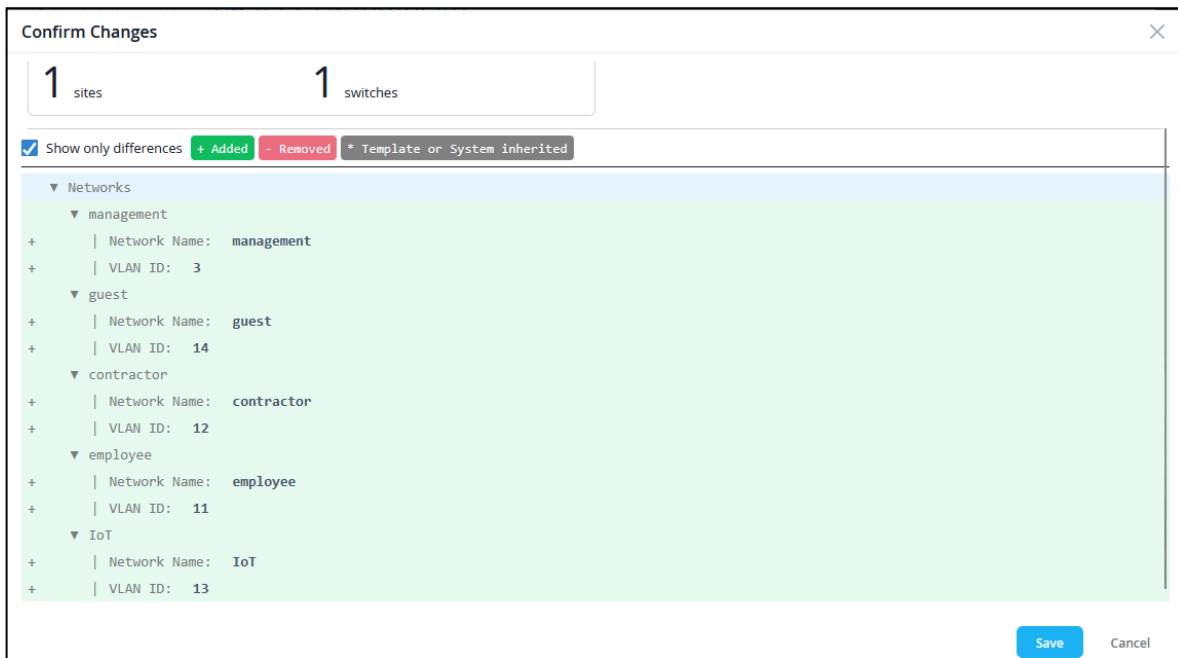
Check your list of unused networks you just created.



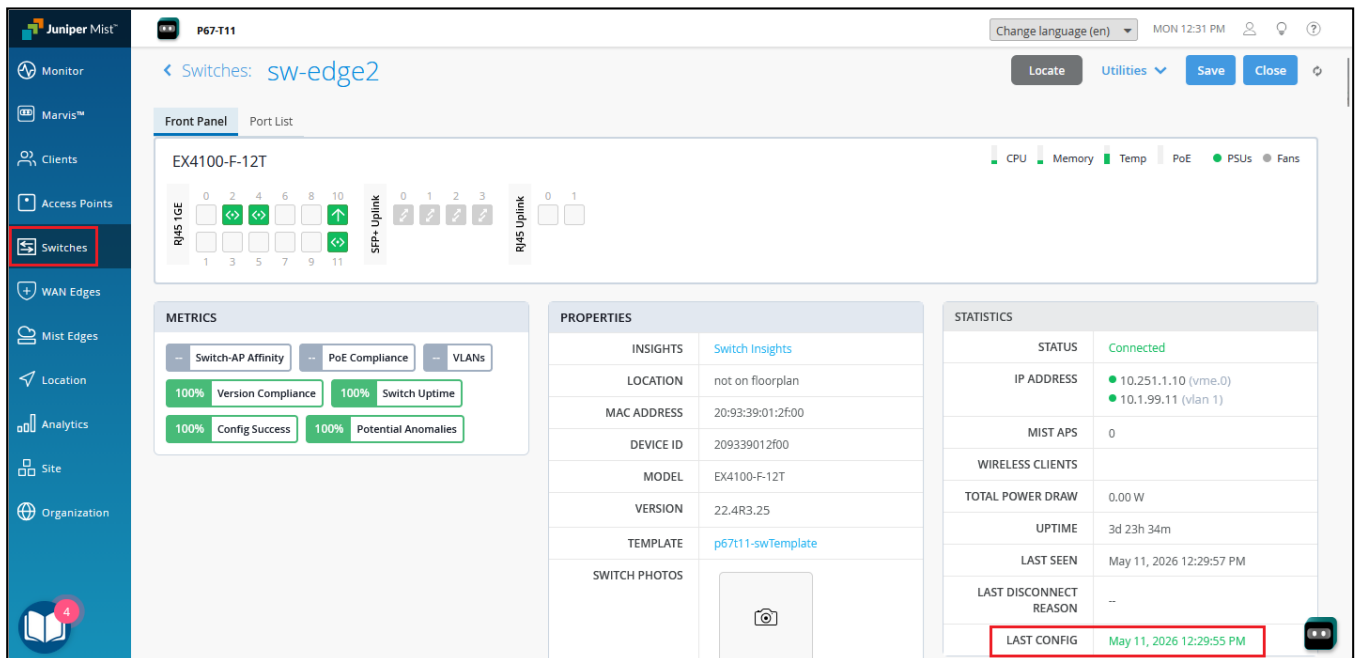
Scroll the Switch Template configuration page to the top and click **Save**.



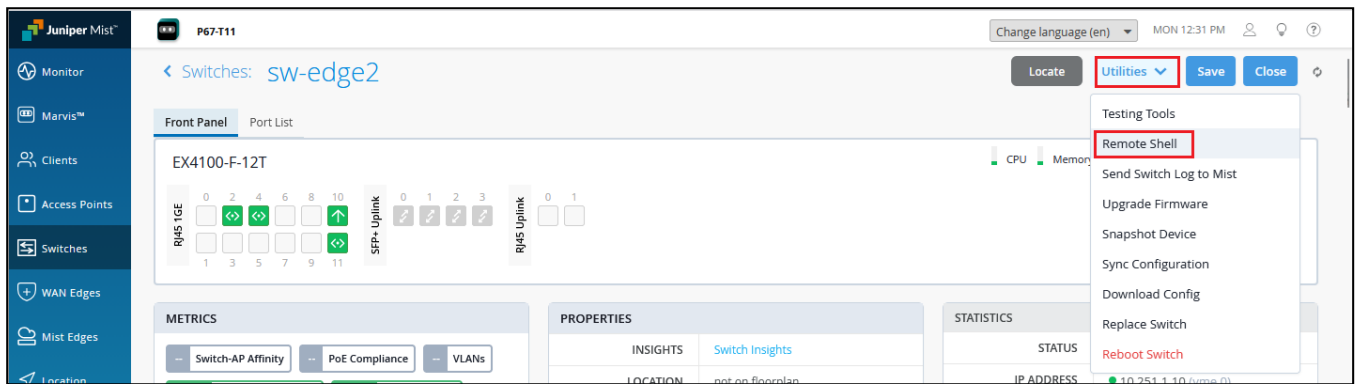
Review and confirm changes by clicking **Save** again.



Navigate to Mist AI Switches and click on your switch name. Check the last config timestamp which should be a recent time (you might need to wait a minute and remember time is displayed in previously configured time zone).



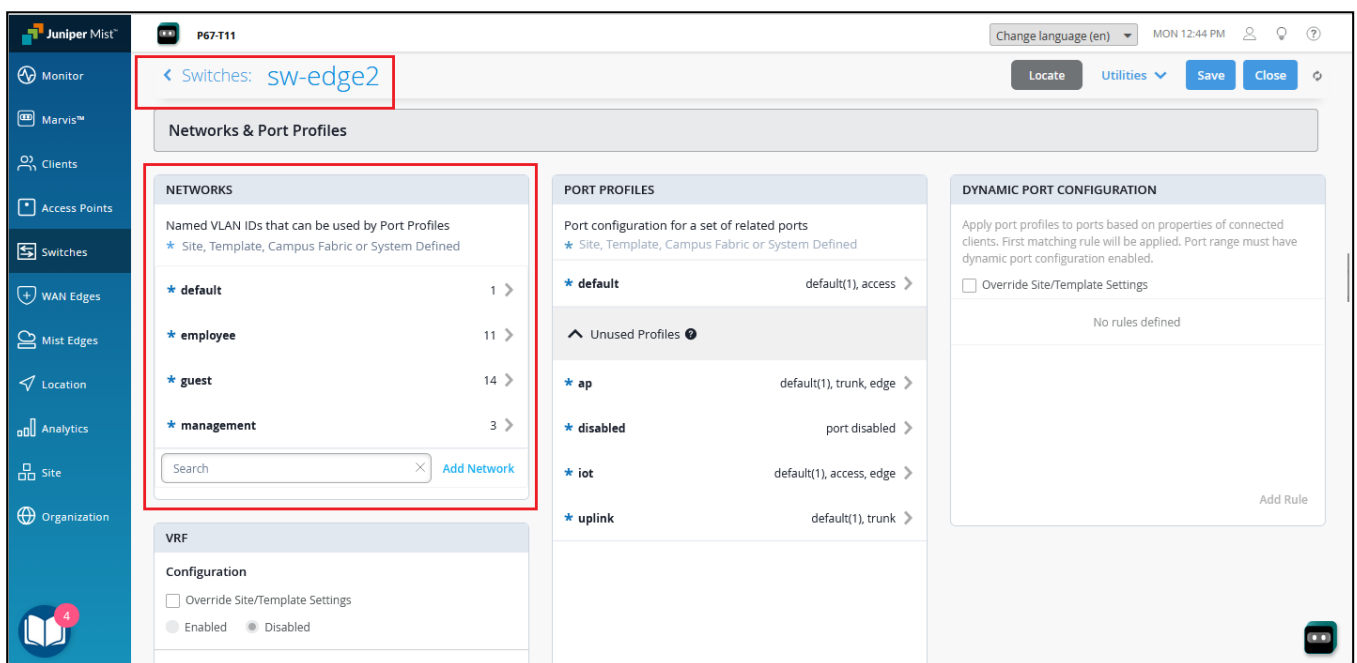
Click **Utilities** > **Remote Shell**.



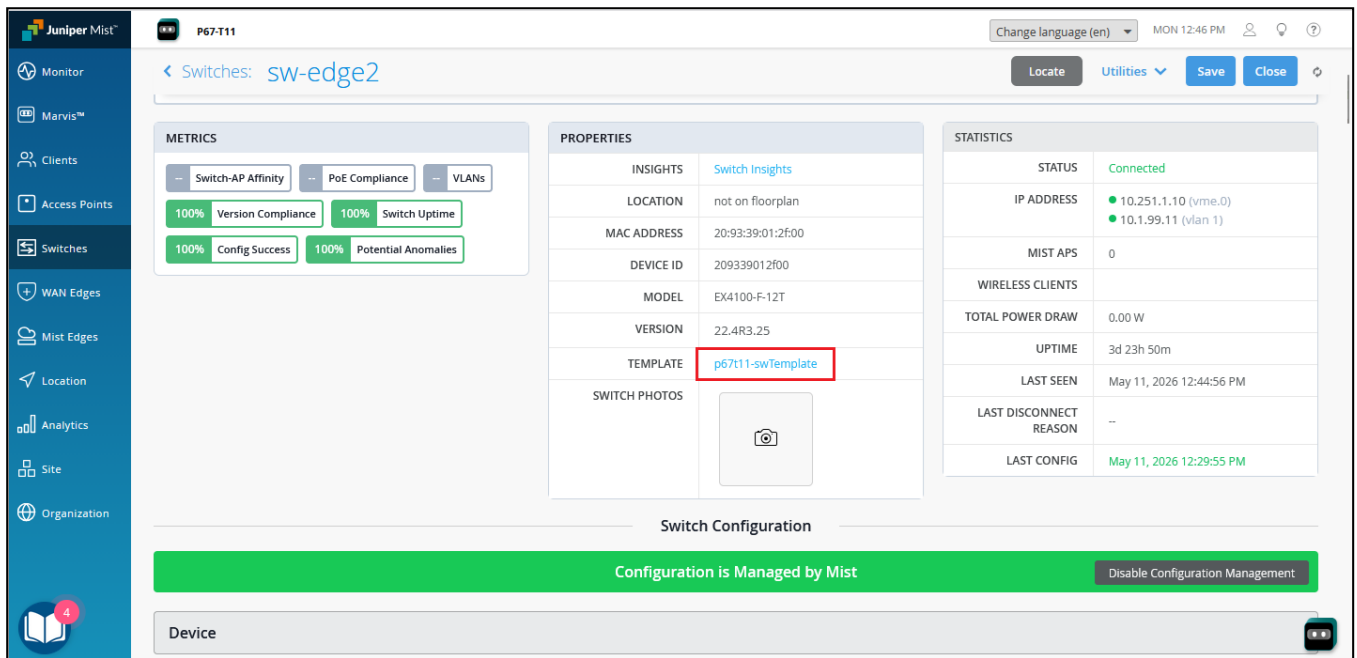
Check VLANs configured on the switch with “show configuration vlans” command. It should show only VLAN 1 at the moment, since new VLANs are not in use in any port profile.

```
mist@sw-edge2> show configuration vlans
default {
    vlan-id 1;
    13-interface irb.0;
}
{master:0}
mist@sw-edge2>
```

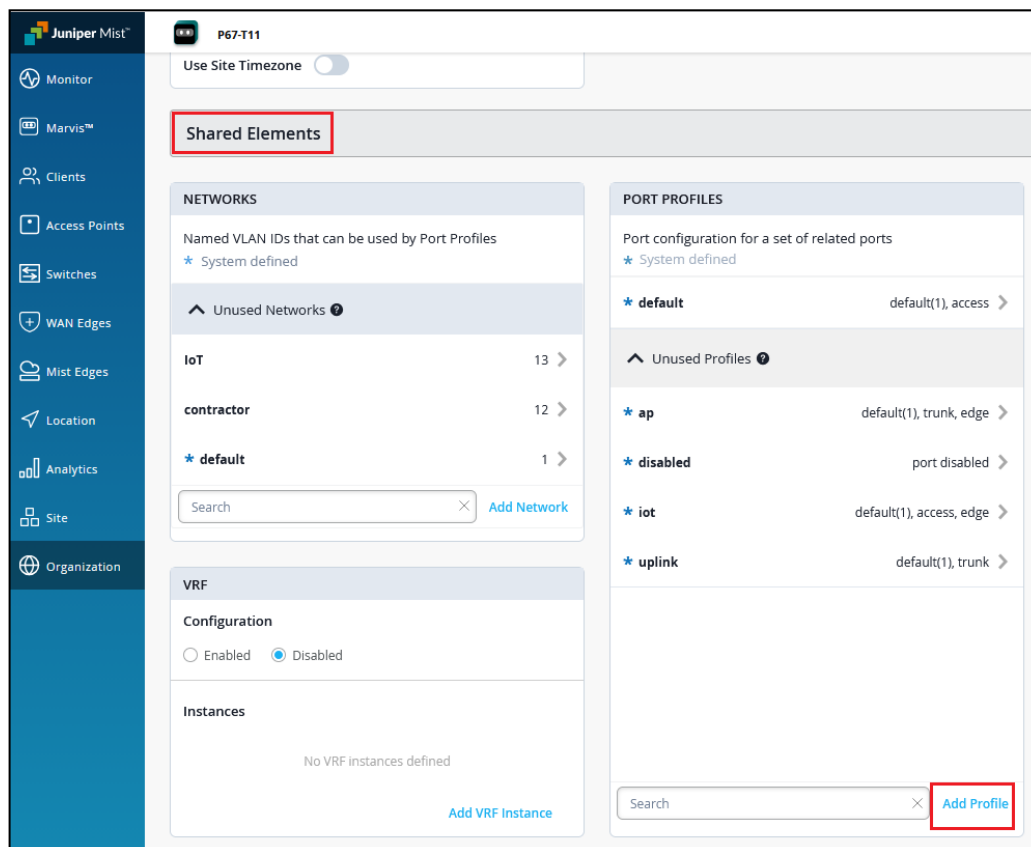
Close Remote Shell and scroll down till the Networks & Port Profiles section where you should see all VLANs IDs inherited from the Switch Template.



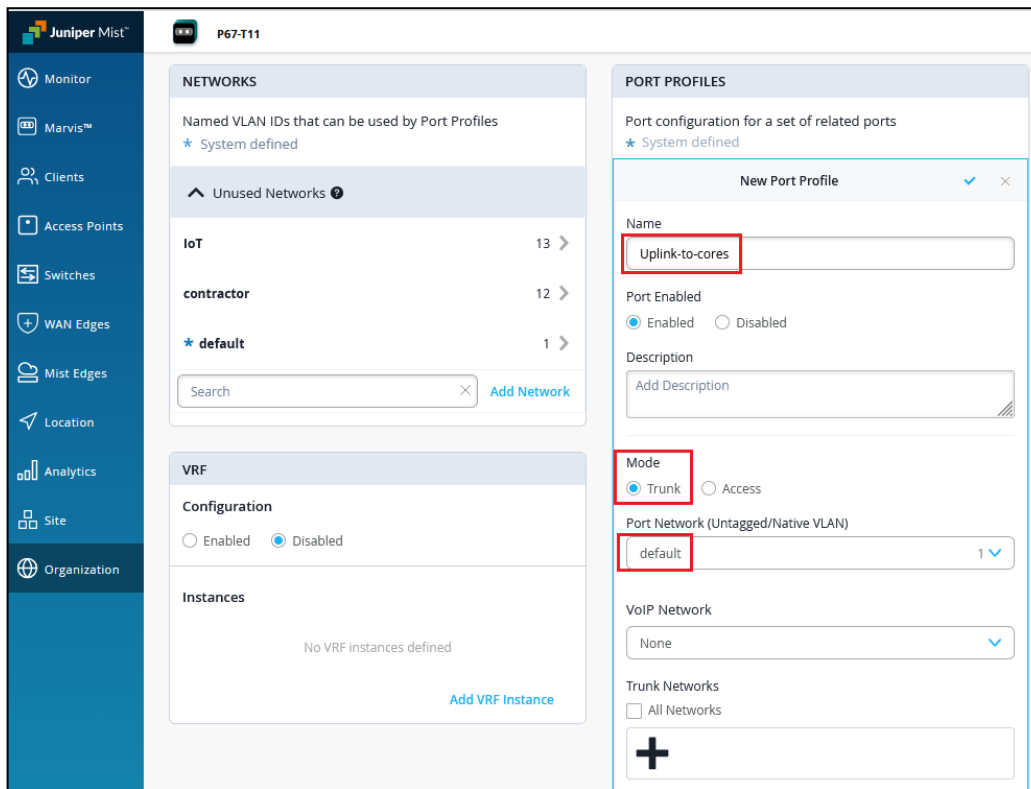
Scroll up and click on your template name in Properties section at the top of the page. This will bring you back to the Switch Template configuration page.



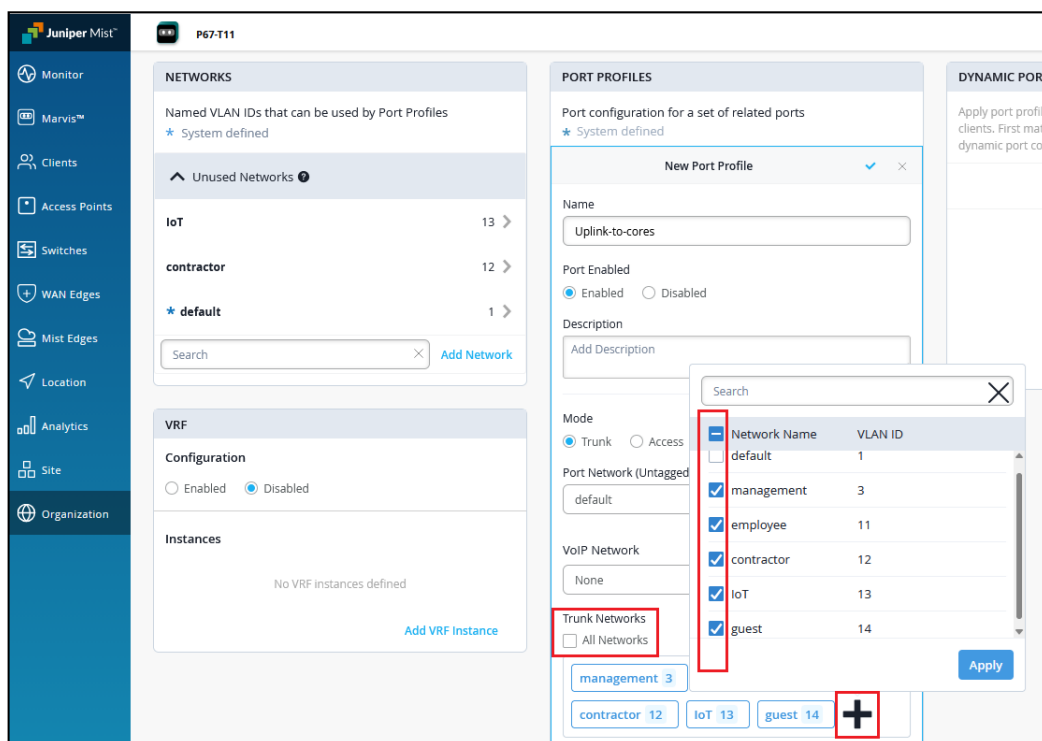
Scroll down to the Shared Elements and click Add Profile button to create a new Port Profile.



Set the name to "Uplink-to-cores" (upper-case "U" and lower-case other letters), change Mode to Trunk and leave default VLAN 1 as a native VLAN.



Click on “+” icon in Trunk Networks and select all VLANs excepting VLAN 1 then click **Apply**.



Scroll down the page to see other available options for this new Port Profile. You will not change any other options, scroll the page up and click on the check mark to apply your changes to the template.

Scroll the page all the way up to the top and click Save.

Review the list of changes and click **Save** to apply these changes.

Confirm Changes

APPLIES TO SITES

1 sites

1 switches

☒ Show only differences
 + Added
 - Removed
 * Template or System inherited

▼ Port Usages

▼ Uplink-to-cores

+

Profile Name:

Uplink-to-cores

+

All Networks:

No

+

Auto-Negotiation:

Enabled

+

Block STP BPDUs:

Disabled

+

Duplex:

Auto

+

Enable MTU:

Disabled

+

Enable QoS:

Disabled

+

High Priority:

Disabled

+

Legacy PD:

Disabled

+

Mac Limit:

0

+

Mode:

trunk

+

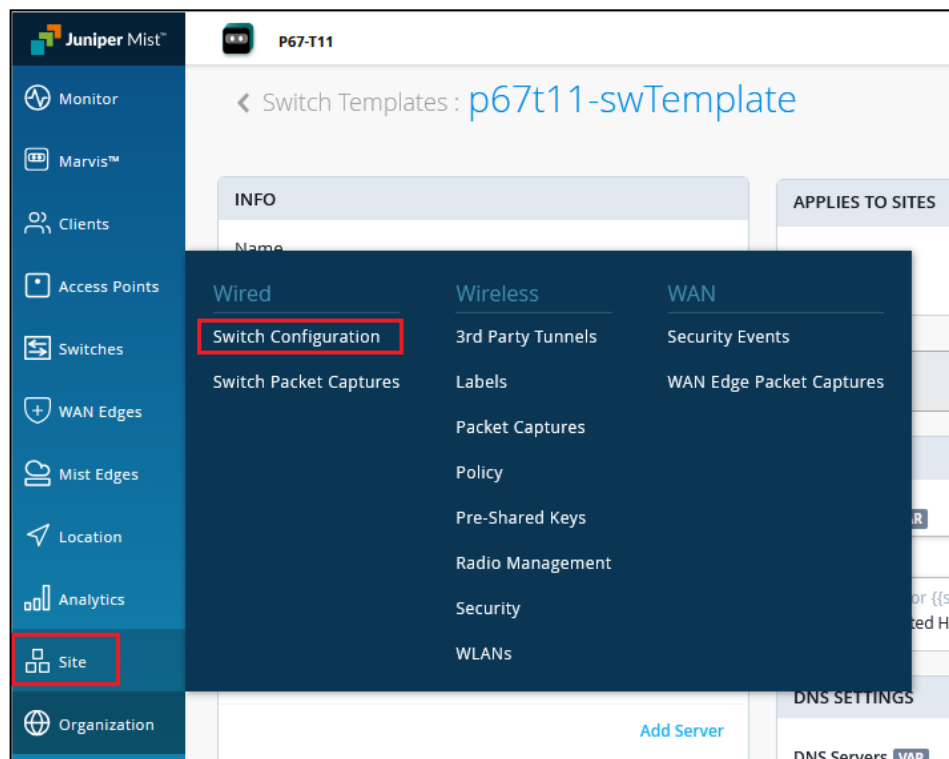
Per VLAN STP:

Disabled

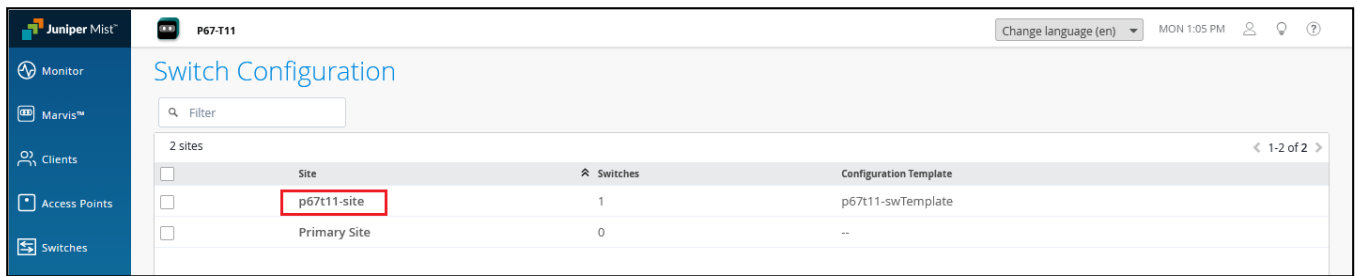
Save

Cancel

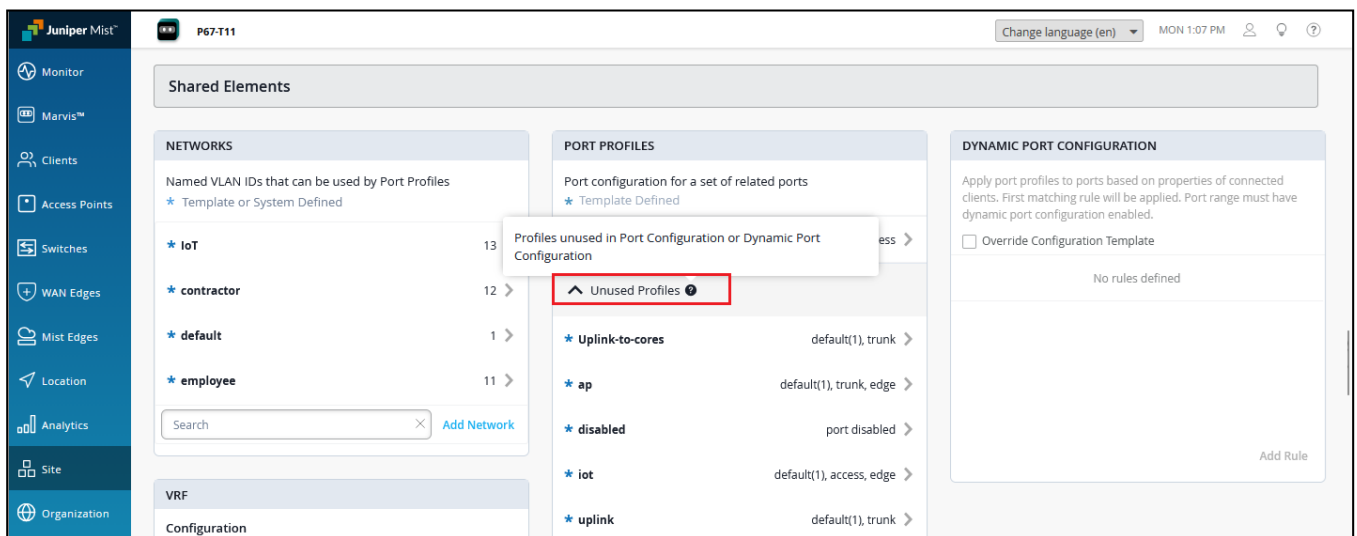
Navigate to Site > Wired > Switch Configuration



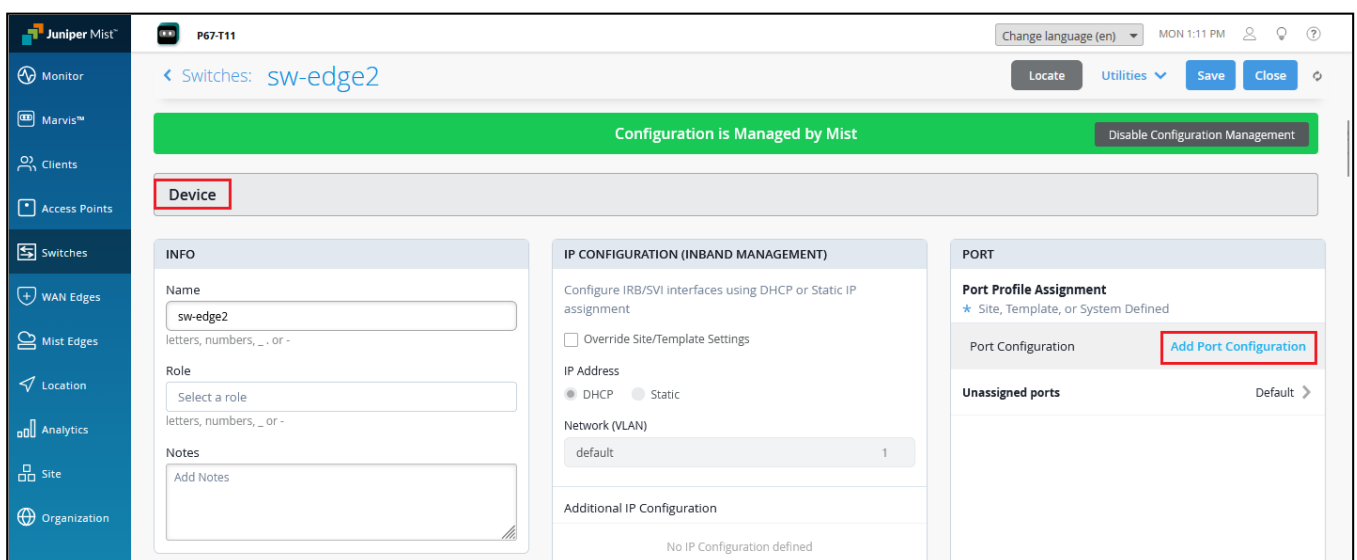
Click on your site name that you recently created.



Scroll down to the Shared Elements section and notice that Networks and Port profiles you configured in the Switch Template were inherited by the site where this template is assigned. Notice another detail about Port profiles – all profiles are listed as Unused Profiles. Hover your mouse over the question mark next to Unused Profiles.

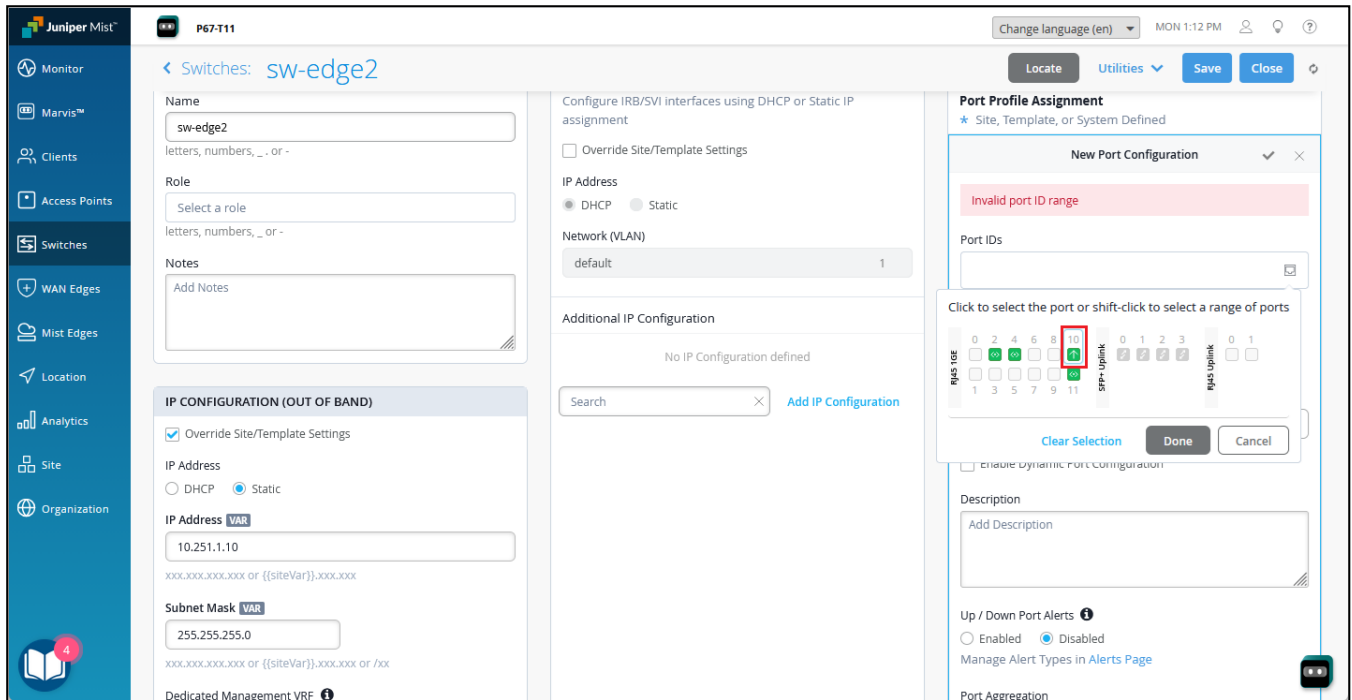


Navigate to Switches and click on your switch name, then scroll the page down till the Device section. Click **Add Port Configuration**.



NOTE: It's possible to apply port configuration at the template or site level to multiple switches at a time with Select Switches Configuration. This will be explained in Lab 5.

In Port IDs select only port 10 and click **Done**.



Click on Configuration Profile and select "Uplink-to-cores".

Locate Utilities Save Close

Port Profile Assignment

★ Site, Template, or System Defined

New Port Configuration ✓ ✕

Port IDs
ge-0/0/10
(ge-0/0/1, ge-0/0/4, ge-0/1/1-23, etc)

Interface
☒ L2 interface ☐ L3 interface ☐ L3 sub-interfaces

Configuration Profile
AP default(1), trunk, edge
Q-in-Q
Uplink-to-cores default(1), trunk
ap default(1), trunk, edge
default default(1), access
disabled port disabled
iot default(1), access, edge
uplink default(1), trunk
Search Add Profile

Port Aggregation
☐ Enabled ☒ Disabled

Check other options available for the Port Configuration and click on the check mark to apply a new configuration.

Port Profile Assignment
★ Site, Template, or System Defined

New Port Configuration

Port IDs

ge-0/0/10

(ge-0/0/1, ge-0/0/4, ge-0/1/1-23, etc)

Interface

☒ L2 interface
☐ L3 interface
☐ L3 sub-interfaces

Configuration Profile

Uplink-to-cores default(1), trunk

☐ Enable Dynamic Port Configuration

Description

Add Description

Up / Down Port Alerts ⓘ

☐ Enabled
☒ Disabled

[Manage Alert Types in Alerts Page](#)

Port Aggregation

☐ Enabled
☒ Disabled

Allow switch port operator to modify port profile

☐ Yes
☒ No

Click Save button at the top of the page.

Juniper Mist™ P67-T11

Change language (en) MON 1:19 PM

< Switches: sw-edge2

Locate Utilities **Save** Close

Configuration is Managed by Mist [Disable Configuration Management](#)

Device

INFO

Name

sw-edge2

letters, numbers, _ or -

Role

Select a role

letters, numbers, _ or -

Notes

IP CONFIGURATION (INBAND MANAGEMENT)

Configure IRB/SVI interfaces using DHCP or Static IP assignment

☐ Override Site/Template Settings

IP Address

☒ DHCP
☐ Static

Network (VLAN)

default 1

PORT

Port Profile Assignment

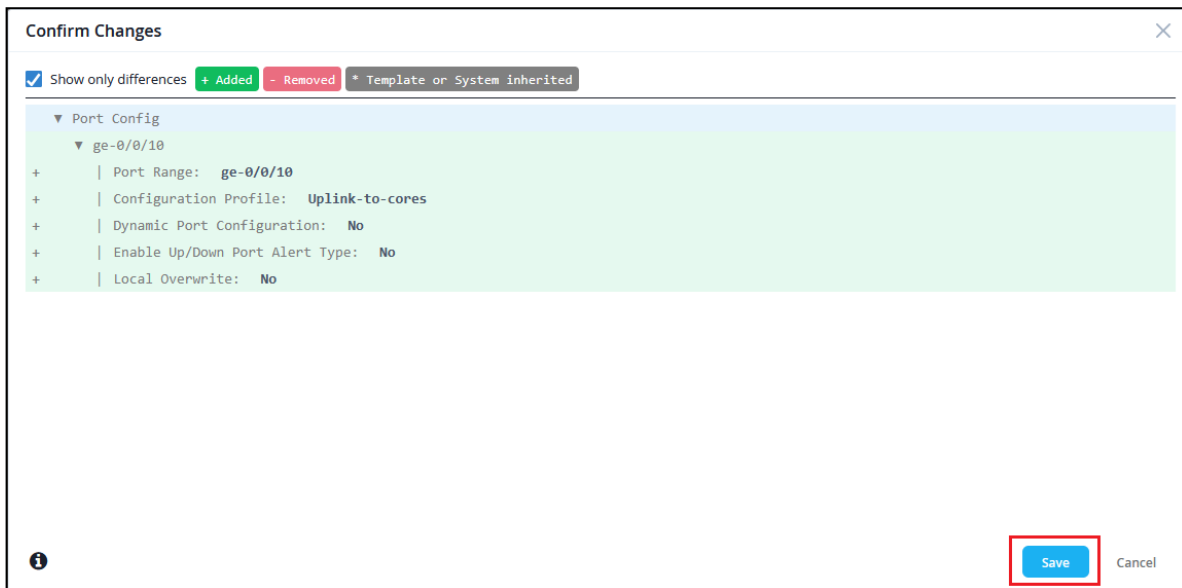
★ Site, Template, or System Defined

Port Configuration [Add Port Configuration](#)

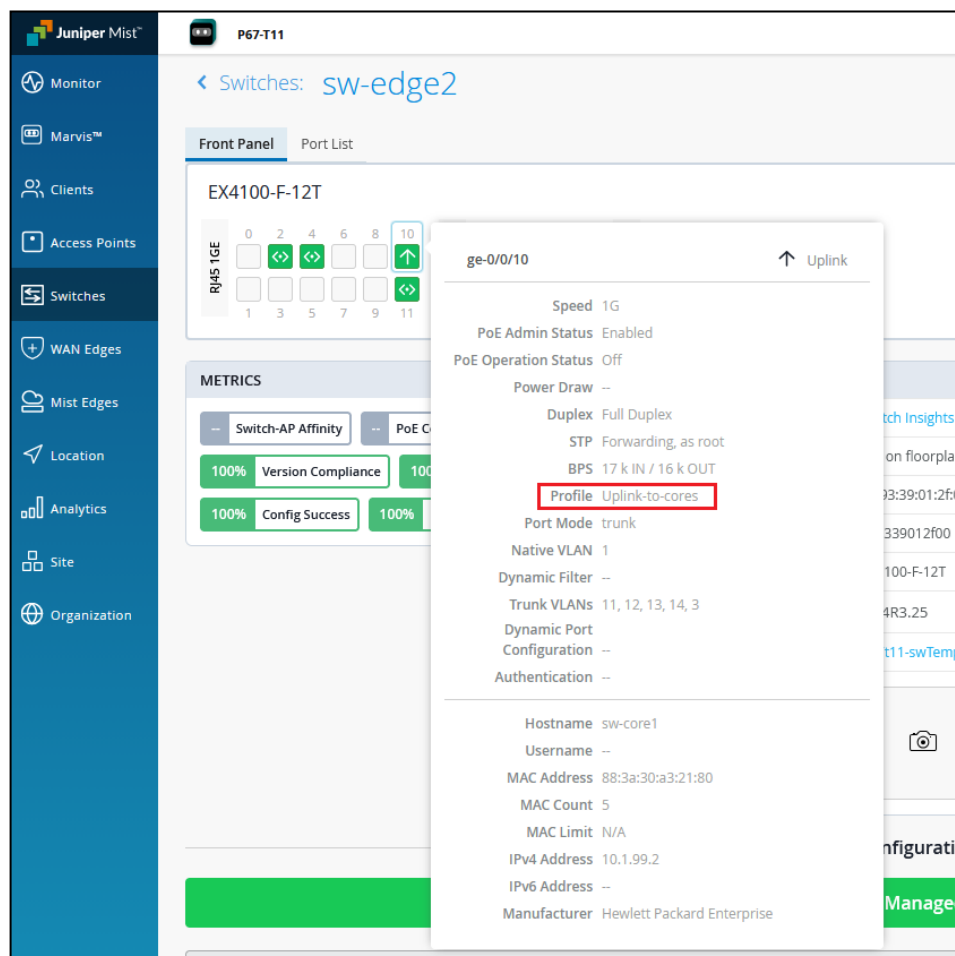
ge-0/0/10	Uplink-to-cores
-----------	-----------------

Unassigned ports Default

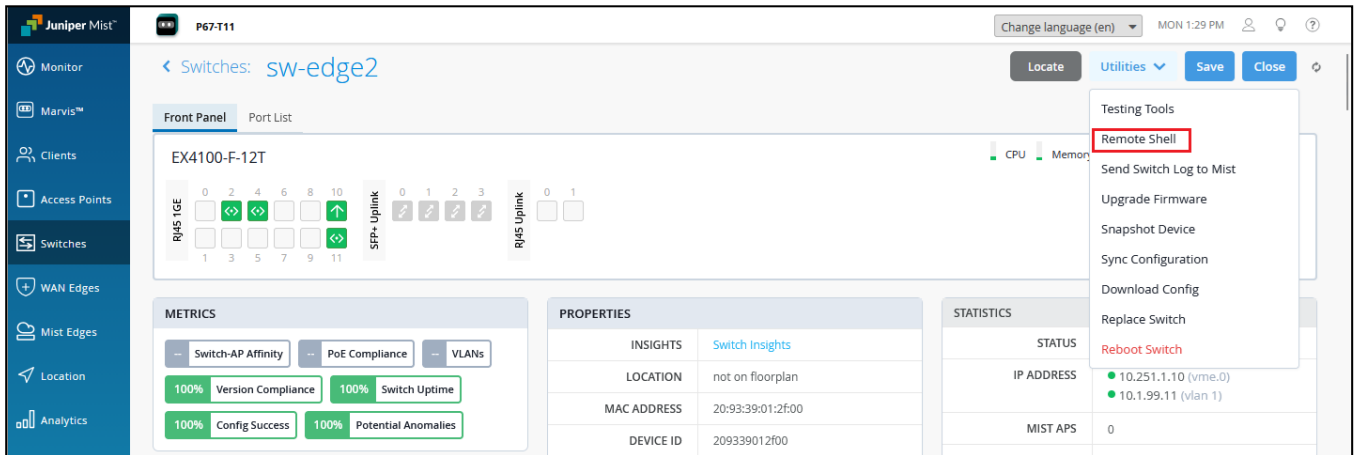
Review Changes and click Save.



Scroll the page up to the top and hover your mouse over Interface 10. You should see Profile “Uplink-to-cores” applied. If you see Configured profile “Uplink-to-cores” and reported profile “Default” displayed, it means that you need to wait a couple of minutes until it synchronizes the new configuration and refresh the page.



Navigate to Utilities > **Remote Shell**.



Check the list of VLANs configured on your switch with “show vlans” command. New VLANs should be displayed now.

```
mist@sw-edge2> show vlans
```

Routing instance	VLAN name	Tag	Interfaces
default-switch	IoT	13	ge-0/0/10.0*
default-switch	contractor	12	ge-0/0/10.0*
default-switch	default	1	ge-0/0/0.0 ge-0/0/1.0 ge-0/0/10.0* ge-0/0/11.0* ge-0/0/2.0* ge-0/0/3.0 ge-0/0/4.0* ge-0/0/5.0 ge-0/0/6.0 ge-0/0/7.0 ge-0/0/8.0 ge-0/0/9.0 mge-0/2/0.0 mge-0/2/1.0
default-switch	employee	11	ge-0/0/10.0*
default-switch	guest	14	ge-0/0/10.0*
default-switch	management	3	ge-0/0/10.0*

```
{master:0}  
mist@sw-edge2>
```

Check new configuration applied to interfaces hierarchy with “show configuration interfaces” command.

```
mist@sw-edge2> show configuration interfaces
```

```

interface-range default {
    member "et-0/1/[0-3]";
    member "ge-0/0/[0-9]";
    member ge-0/0/11;
    member "ge-0/2/[0-1]";
    member "xe-0/2/[0-3]";
    apply-groups default;
}
interface-range Uplink-to-cores {
    member ge-0/0/10;
    apply-groups Uplink-to-cores;
}
<Output omitted>

```

Check more details about “Uplink-to-cores” group with “show configuration groups Uplink-to-cores” command.

```

mist@sw-edge2> show configuration groups Uplink-to-cores
interfaces {
    <*> {
        native-vlan-id 1;
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members [ management employee contractor IoT guest default ];
                }
            }
        }
    }
}

```

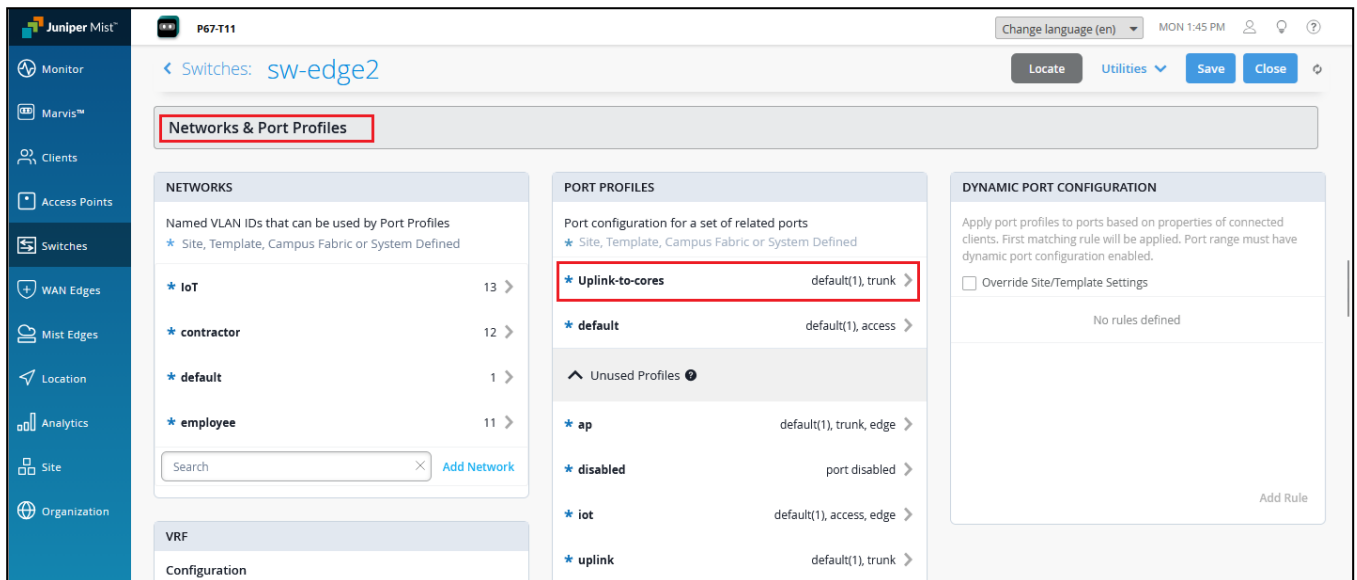
Check the list of configured VLANs with “show configuration vlans” command.

```

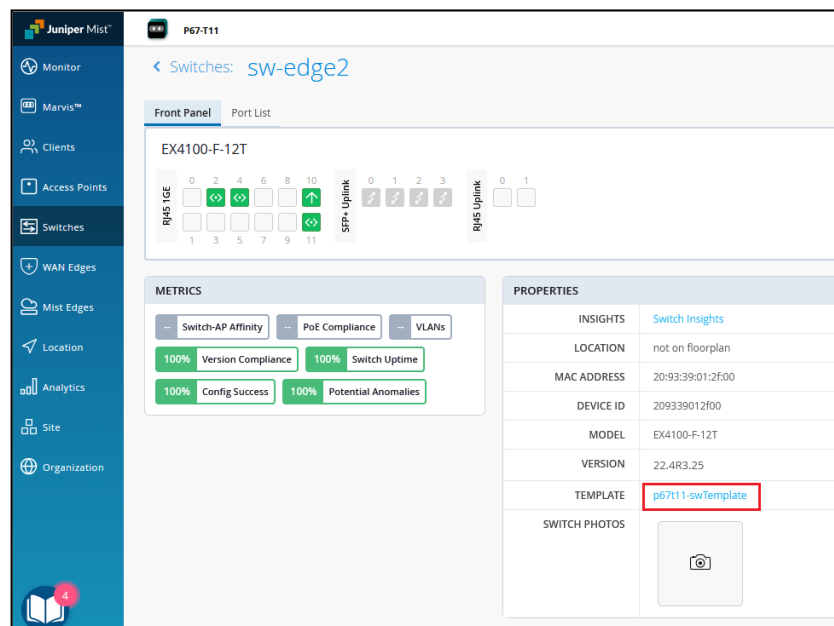
mist@sw-edge2> show configuration vlans
IoT {
    vlan-id 13;
}
contractor {
    vlan-id 12;
}
default {
    vlan-id 1;
    13-interface irb.0;
}
employee {
    vlan-id 11;
}
guest {
    vlan-id 14;
}
management {
    vlan-id 3;
}

```

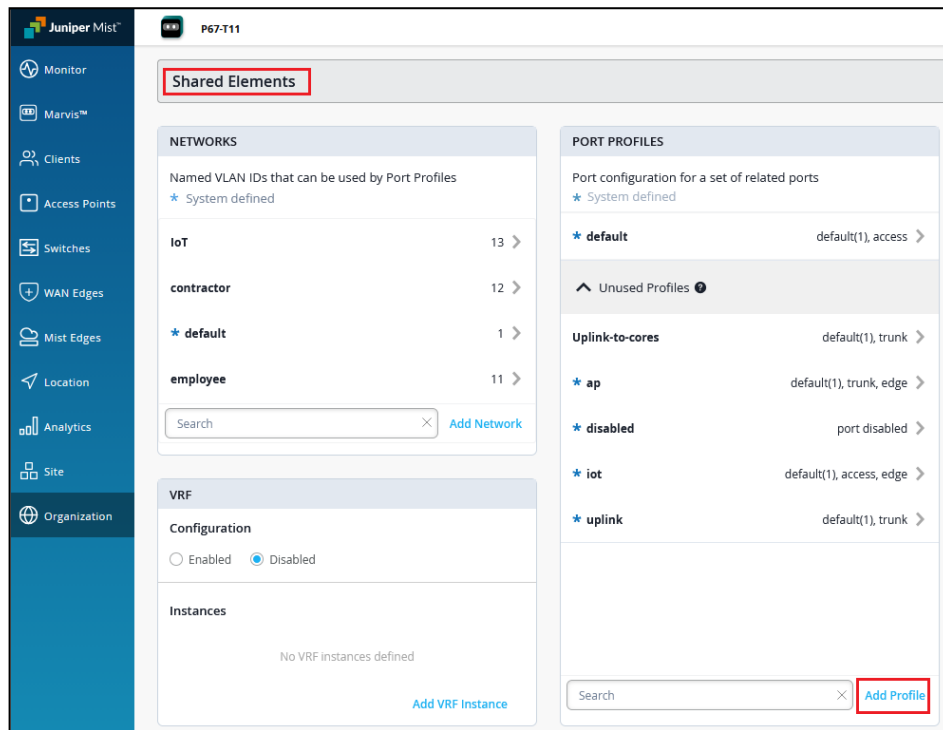
Close Remote Shell window and scroll the page down to Networks & Port Profiles section where you can see now “Uplink-to-cores” not listed in Unused Profiles.



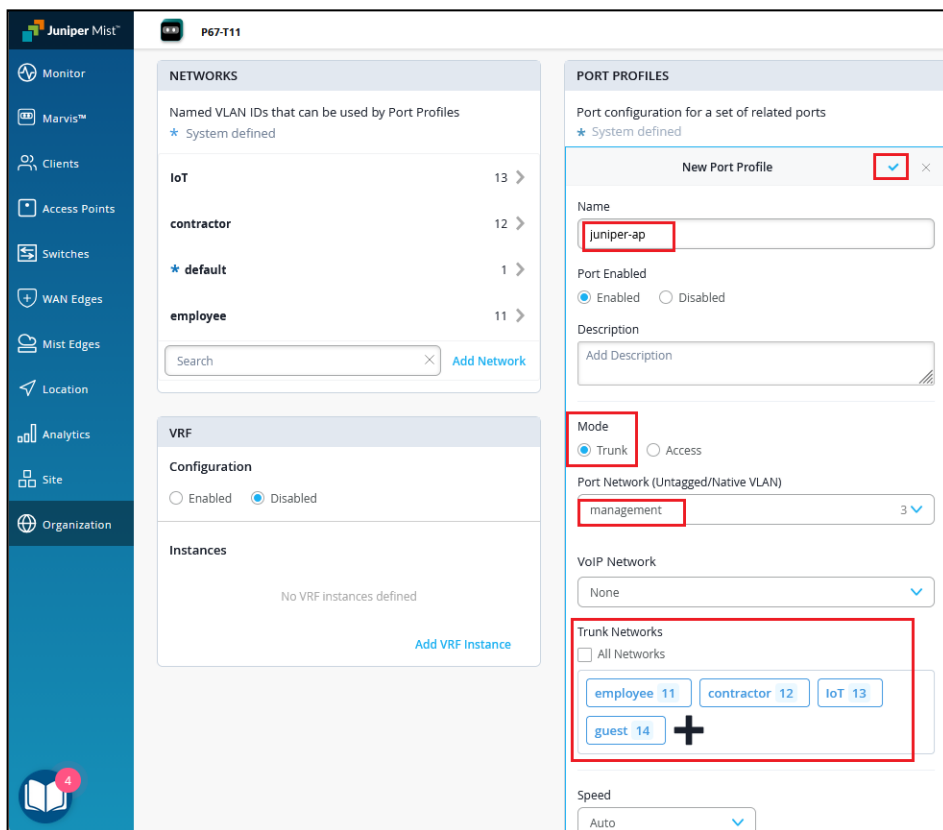
Create one more Port Profile for Juniper Access Point connected to port 2. Navigate to Organization > Wired > Switch Templates and select your template name or click on your Switch template in the properties.



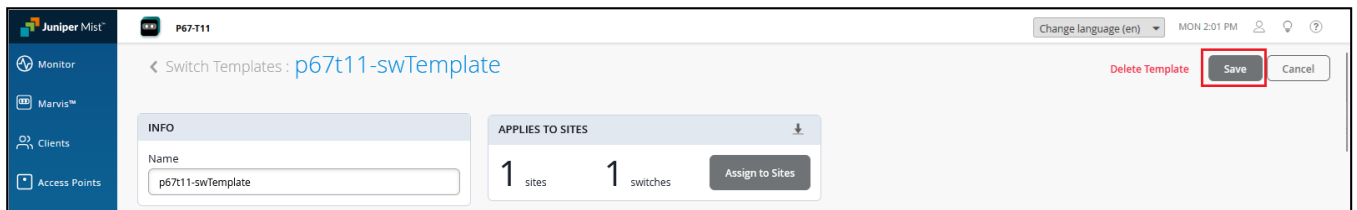
Scroll the page down to the Shared Elements and click Add Profile.



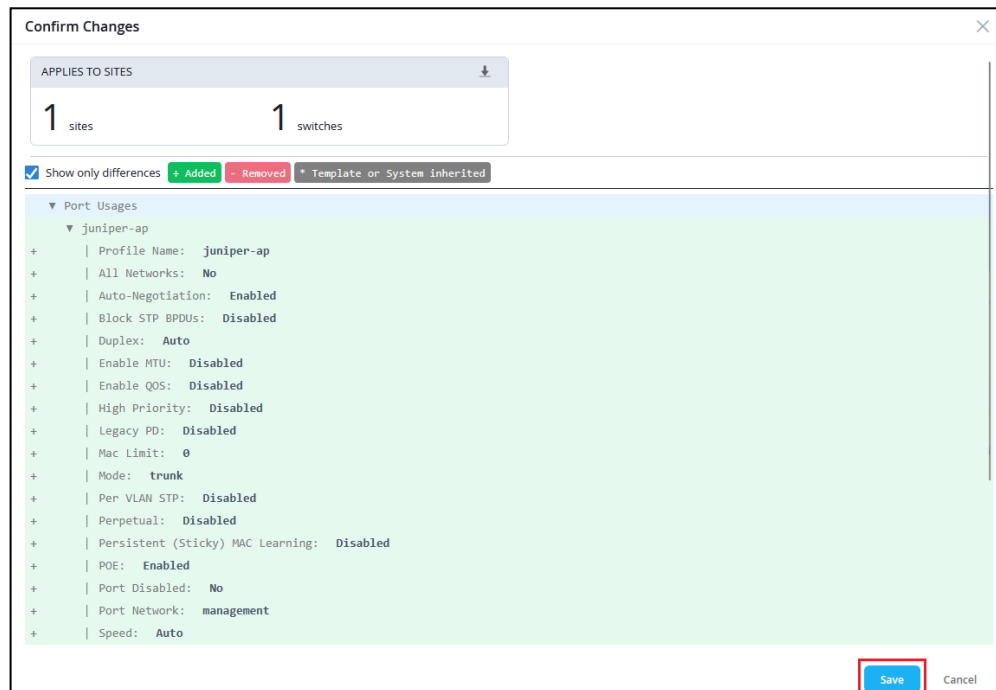
Give this profile name “juniper-ap”, select Mode Trunk, Native VLAN management, Trunk Networks: employee, contractor, IoT and guest. Then click on a check mark to create new profile.



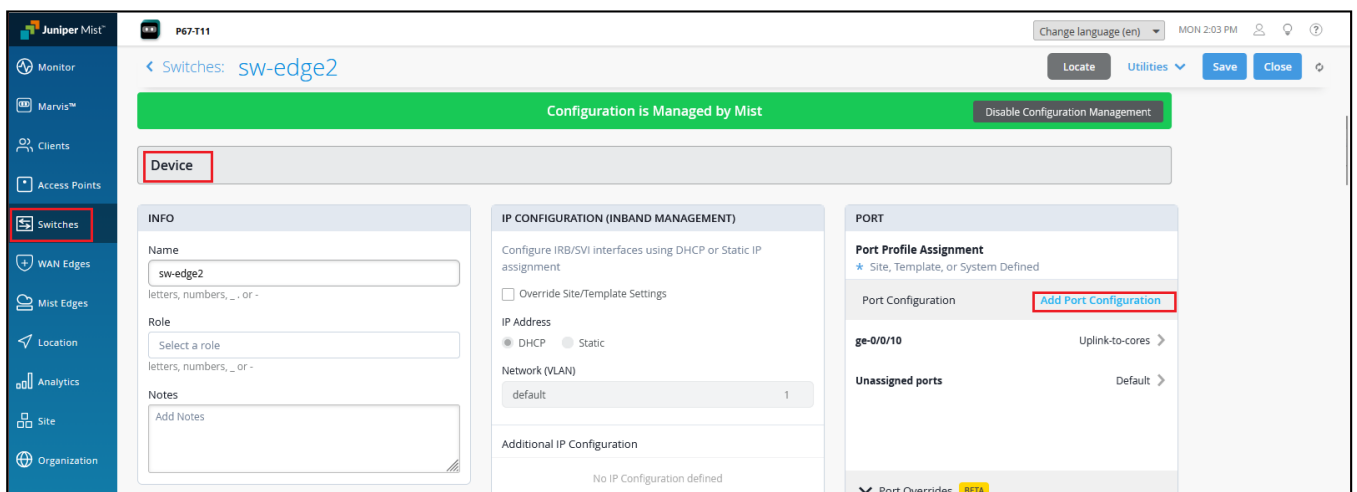
Click Save at the top of the page to save new settings in the Switch template.



Confirm changes by clicking **Save** again.



Navigate to Switches > sw-edge2, scroll the page down to Device section and click **Add Port Configuration**.



Select port 2 and click Done, then select juniper-ap profile. Click on the check mark to create new port configuration.

PORT

Port Profile Assignment

★ Site, Template, or System Defined

New Port Configuration

✓

×

Port IDs

ge-0/0/2

(ge-0/0/1, ge-0/0/4, ge-0/1/1-23, etc)

Interface

☒ L2 interface
 ☐ L3 interface
 ☐ L3 sub-interfaces

Configuration Profile

juniper-ap

management(3), trunk

☐ Enable Dynamic Port Configuration

Description

Add Description

Up / Down Port Alerts

☐ Enabled
 ☒ Disabled

Manage Alert Types in Alerts Page

Port Aggregation

☐ Enabled
 ☒ Disabled

Allow switch port operator to modify port profile

☐ Yes
 ☒ No

Click **Save** at the top of the page and then **Save** again to confirm new changes.

Juniper Mist

P67-T11

Change language (en)

MON 2:06 PM

Locate

Utilities

Save

Close

Switches: sw-edge2

INFO

Name

sw-edge2

letters, numbers, _ or -

Role

Select a role

letters, numbers, _ or -

Notes

Add Notes

IP CONFIGURATION (INBAND MANAGEMENT)

Configure IRB/SVI interfaces using DHCP or Static IP assignment

☐ Override Site/Template Settings

IP Address

☒ DHCP
 ☐ Static

Network (VLAN)

default

1

Additional IP Configuration

PORT

Port Profile Assignment

★ Site, Template, or System Defined

Port Configuration

Add Port Configuration

ge-0/0/2

juniper-ap

ge-0/0/10

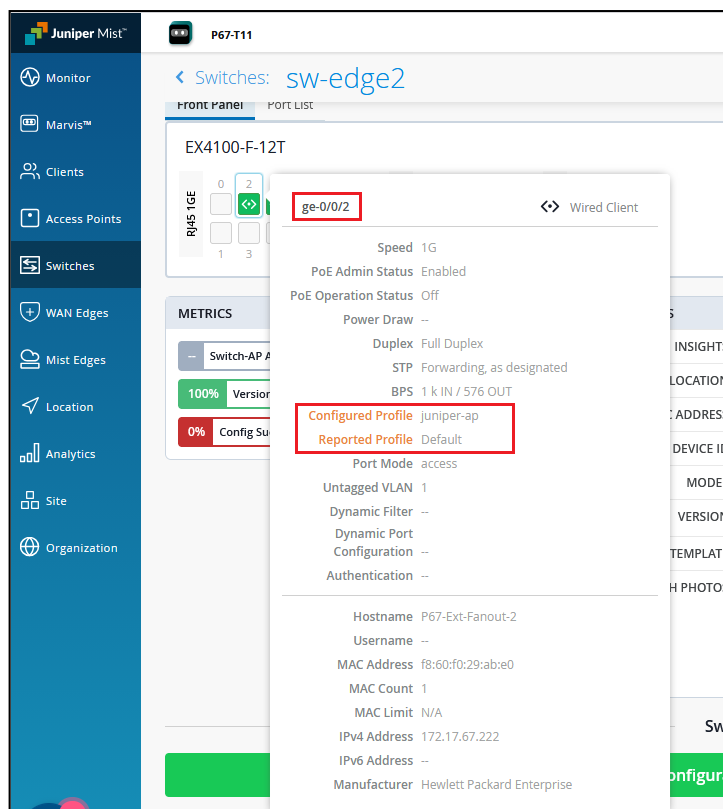
Uplink-to-cores

Unassigned ports

Default

Hover your mouse over port 2 where you will temporarily see “Configured Profile juniper-ap” and “Reported Profile Default”. This will be changed “Profile juniper-ap” once configuration is applied. This might take a couple of minutes.

NOTE: Refresh the web page entirely to update this information.



After refreshing the web page, confirm that new profile was applied.

Juniper Mist P67-T11

Switches: sw-edge2

Front Panel Port List

EX4100-F-12T

ge-0/0/2 Trunked Wired Client

Speed 1G

PoE Admin Status Enabled

PoE Operation Status Off

Power Draw --

Duplex Full Duplex

STP Forwarding, as designated

BPS 1 k IN / 664 OUT

Profile **juniper-ap**

Port Mode trunk

Native VLAN 3

Dynamic Filter --

Trunk VLANs 11, 12, 13, 14

Dynamic Port Configuration --

Authentication --

Hostname P67-Ext-Fanout-2

Username --

MAC Address 88:60:f0:29:ab:e0

MAC Count 1

MAC Limit N/A

IPv4 Address 172.17.67.222

IPv6 Address --

Manufacturer Hewlett Packard Enterprise

Switch Configuration

Configuration is Managed by Mist

Task 3-2: LAG configuration

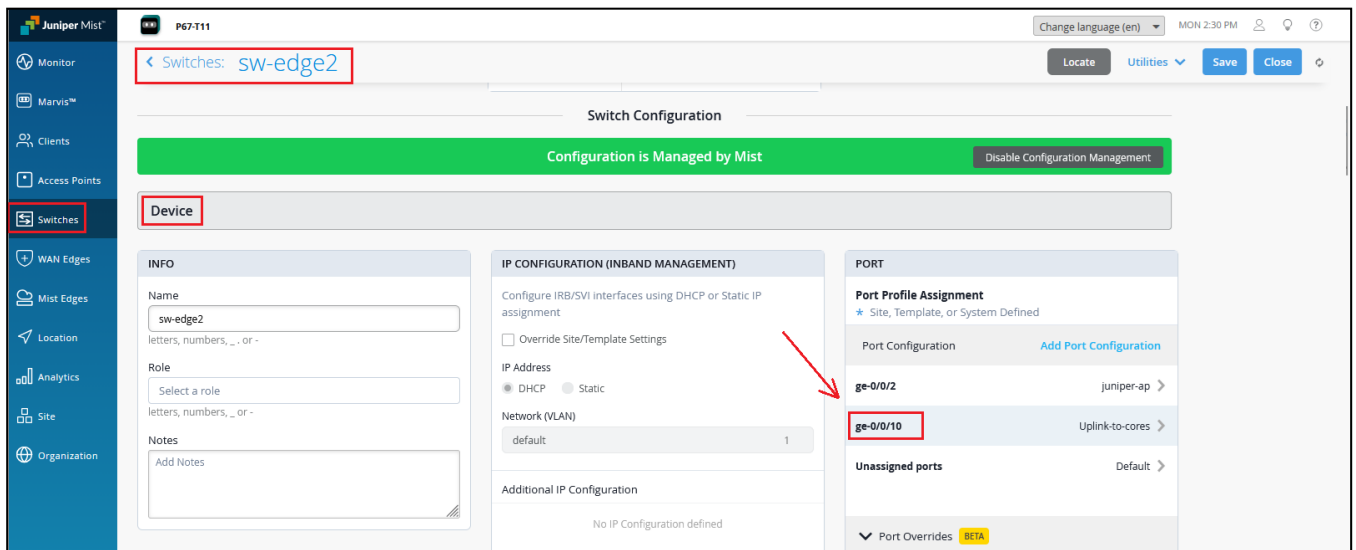
Objectives

Configure LAG on Juniper EX switch uplink ports.

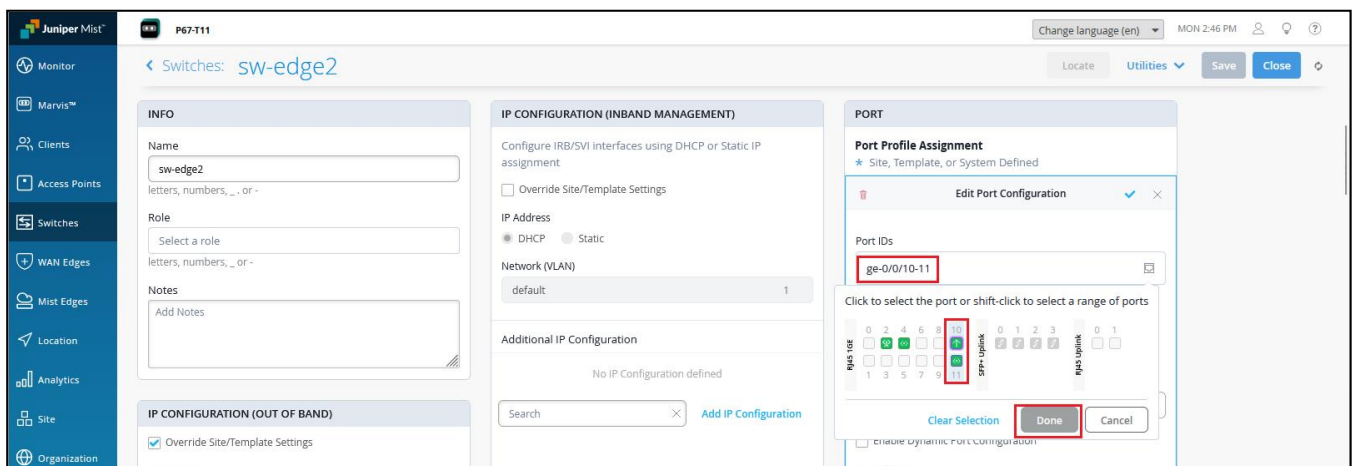
Validate LAGs with Port Panel and Port list views, and CLI commands.

Steps

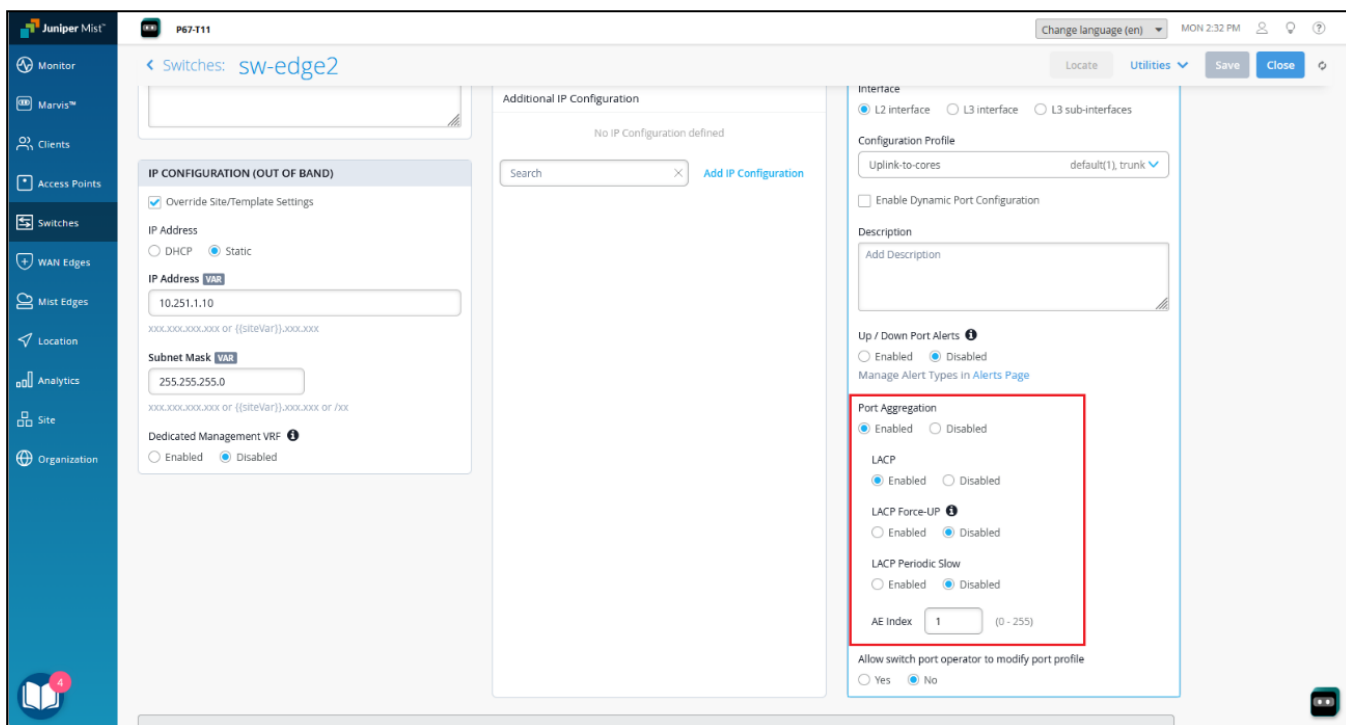
In Mist AI navigate to Switches > sw-edge2 and scroll to the Port configuration. Click on ge-0/0/10.



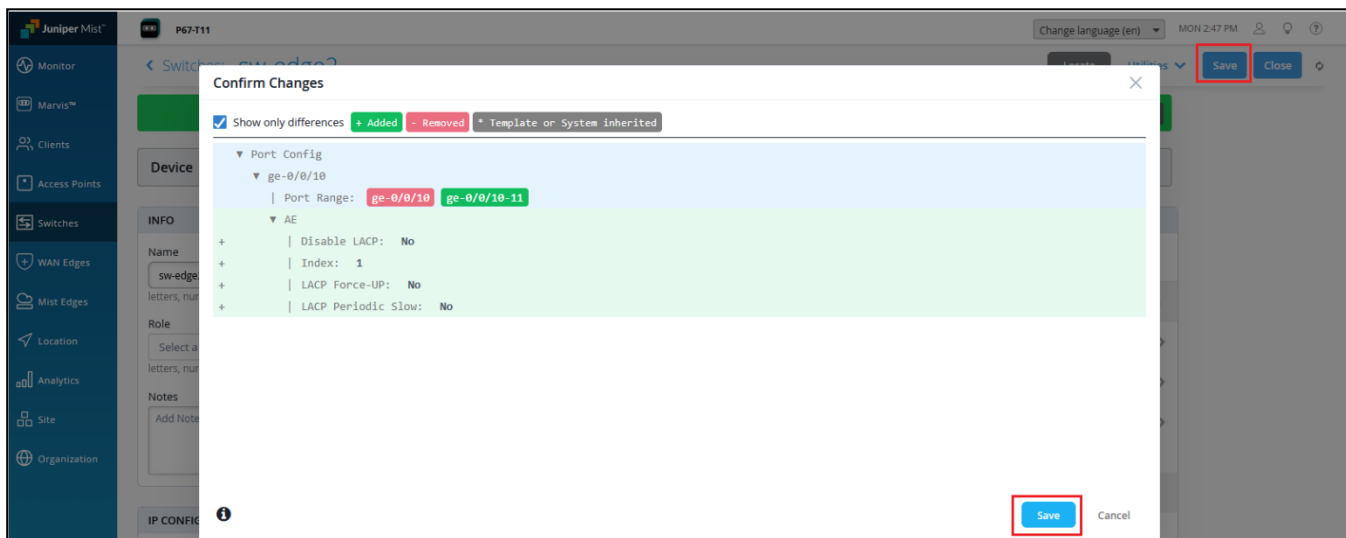
Select second interface ge-0/0/11 and click Done.



Enable Port Aggregation with LACP and AE index 1. Then click on the check mark to update the port configuration.



Click **Save** at the top of the page then **Save** again to confirm changes.

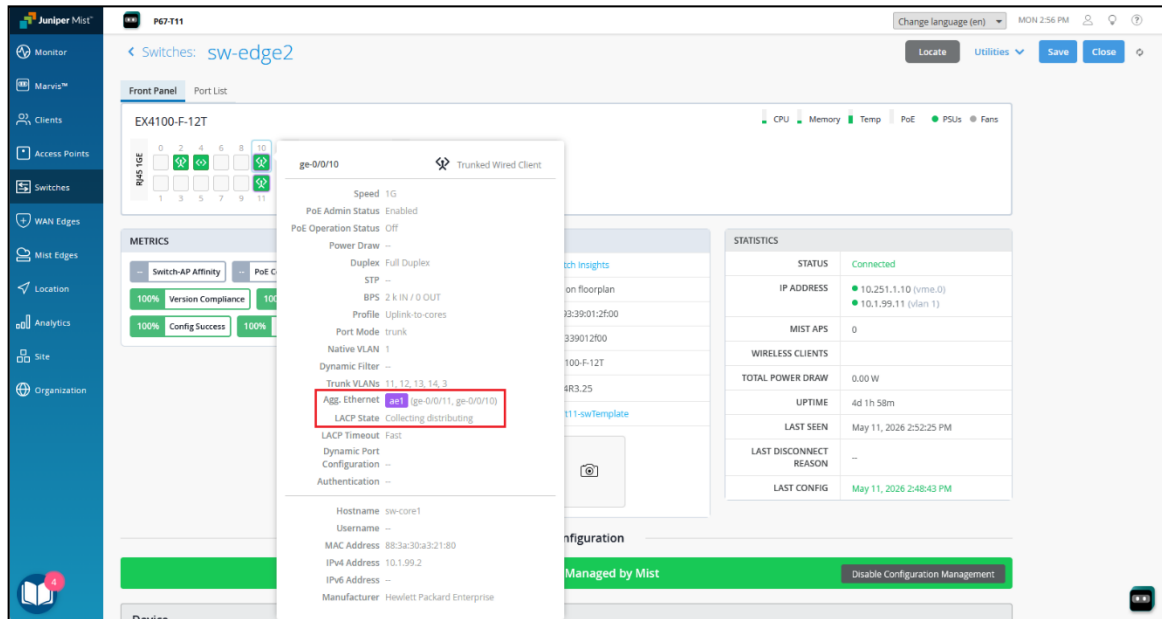


Wait several minutes and refresh the page. You should see 100% Config Success and icons changes for interfaces 10 and 11 like on the screenshot below.

NOTE: You will briefly see 0% Config Success which should be changed to 100% Config Success.



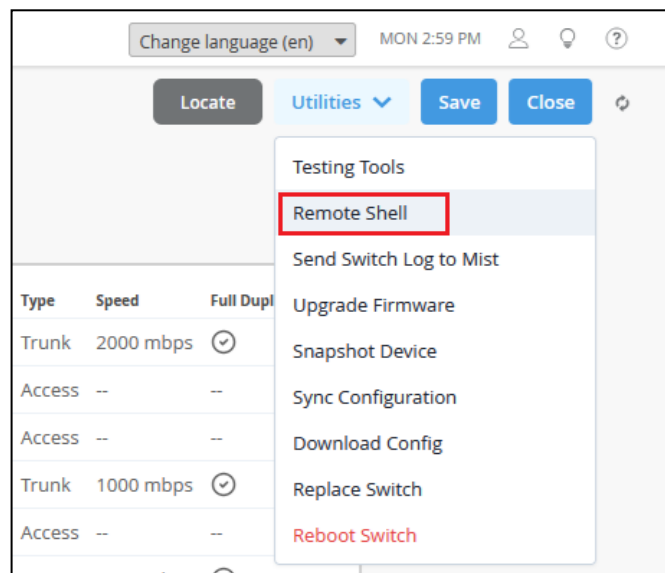
Hover your mouse over interface 10 or 11. You should see that these interfaces are members of LAG ae1.



Switch to Port List, confirm that ae1 interface is listed and ports ge-0/0/10 and ge-0/0/11 are members of ae1.

Port	Status	Agg. Ethernet	Wired Client	Manufacturer	Wireless Clients	Power Draw	Profile (Configured / Reported)	Type	Speed	Full Duplex	RX
ae1	up	--	--	--	--	--	Uplink-to-cores	Trunk	2000 mbps	⊙	0.8
ge-0/0/0	down	--	--	--	--	--	Default	Access	--	--	0.8
ge-0/0/1	down	--	--	--	--	--	Default	Access	--	--	0.8
ge-0/0/2	up	--	88:60:f0:29:ab:e0	Hewlett Packard Enterprise	--	--	juniper-ap	Trunk	1000 mbps	⊙	27
ge-0/0/3	down	--	--	--	--	--	Default	Access	--	--	0.8
ge-0/0/4	up	--	00:50:56:b1:29:bd	VMware, Inc.	--	--	Default	Access	1000 mbps	⊙	83
ge-0/0/5	down	--	--	--	--	--	Default	Access	--	--	0.8
ge-0/0/6	down	--	--	--	--	--	Default	Access	--	--	0.8
ge-0/0/7	down	--	--	--	--	--	Default	Access	--	--	0.8
ge-0/0/8	down	--	--	--	--	--	Default	Access	--	--	0.8
ge-0/0/9	down	--	--	--	--	--	Default	Access	--	--	0.8
ge-0/0/10	up	ae1	88:3a:30:a3:21:80	Hewlett Packard Enterprise	--	--	Uplink-to-cores	Trunk	1000 mbps	⊙	26
ge-0/0/11	up	ae1	88:3a:30:a5:06:40	--	--	--	Uplink-to-cores	Trunk	1000 mbps	⊙	4.5
xe-0/1/0 (vcp-0/1/0)	--	--	--	--	--	--	Default	Access	--	--	0.8
xe-0/1/1 (vcp-0/1/1)	--	--	--	--	--	--	Default	Access	--	--	0.8
xe-0/1/2 (vcp-0/1/2)	--	--	--	--	--	--	Default	Access	--	--	0.8
xe-0/1/3 (vcp-0/1/3)	--	--	--	--	--	--	Default	Access	--	--	0.8

Click Utilities > Remote Shell



Check LACP interfaces with “show lacp interfaces” command. You should see both interfaces ge-0/0/10 and ge-0/0/11 listed with Collecting distributing state. This confirms that LAG ae1 is functioning properly.

```
mist@sw-edge2> show lacp interfaces
Aggregated interface: ae1
LACP state:
  Role    Exp  Def  Dist  Col  Syn  Aggr  Timeout  Activity
  ge-0/0/10 Actor No   No   Yes  Yes  Yes   Yes     Fast    Active
  ge-0/0/10 Partner No   No   Yes  Yes  Yes   Yes     Slow    Active
  ge-0/0/11 Actor No   No   Yes  Yes  Yes   Yes     Fast    Active
  ge-0/0/11 Partner No   No   Yes  Yes  Yes   Yes     Slow    Active
LACP protocol:
  Receive State  Transmit State  Mux State
  ge-0/0/10     Current        Slow periodic  Collecting distributing
```

ge-0/0/11	Current	Slow periodic	Collecting distributing
-----------	---------	---------------	-------------------------

Use “show lacp interfaces extensive” command to collect more details about system identifier and port numbers on actor and partner sides. Notice that the Partner system ID is virtual system MAC address configured on VSX peers.

```
mist@sw-edge2> show lacp interfaces extensive
Aggregated interface: ae1
LACP state:      Role  Exp  Def  Dist  Col  Syn  Aggr  Timeout  Activity
ge-0/0/10        Actor  No   No   Yes   Yes  Yes   Yes    Fast    Active
ge-0/0/10        Partner No   No   Yes   Yes  Yes   Yes    Slow    Active
ge-0/0/11        Actor  No   No   Yes   Yes  Yes   Yes    Fast    Active
ge-0/0/11        Partner No   No   Yes   Yes  Yes   Yes    Slow    Active
LACP protocol:   Receive State  Transmit State  Mux State
ge-0/0/10        Current    Slow periodic  Collecting distributing
ge-0/0/11        Current    Slow periodic  Collecting distributing
LACP info:      Role  System priority  System identifier  Port priority  Port number  Port key
ge-0/0/10        Actor  127  20:93:39:01:2f:00  127  1  2
ge-0/0/10        Partner 65534 02:00:00:02:00:01  1  3  3
ge-0/0/11        Actor  127  20:93:39:01:2f:00  127  2  2
ge-0/0/11        Partner 65534 02:00:00:02:00:01  1  1003 3
```

Jump to MGMT PC Desktop and open SSH session to **sw-core2**. Disable interface 1/1/3 on sw-core2.

```
sw-core2# configure terminal
sw-core2(config)# interface 1/1/3
sw-core2(config-if)# shutdown
sw-core2(config-if)#
```

Repeat “show lacp interfaces extensive” command in Mist AI remote shell. You should see now interface ge-0/0/11 has Detached state and Partner System ID is all zeroes.

```
mist@sw-edge2> show lacp interfaces extensive
Aggregated interface: ae1
LACP state:      Role  Exp  Def  Dist  Col  Syn  Aggr  Timeout  Activity
ge-0/0/10        Actor  No   No   Yes   Yes  Yes   Yes    Fast    Active
ge-0/0/10        Partner No   No   Yes   Yes  Yes   Yes    Slow    Active
ge-0/0/11        Actor  No   Yes  No   No   No   Yes    Fast    Active
ge-0/0/11        Partner No   Yes  No   No   No   Yes    Fast    Passive
LACP protocol:   Receive State  Transmit State  Mux State
ge-0/0/10        Current    Slow periodic  Collecting distributing
ge-0/0/11        Port disabled  No periodic    Detached
LACP info:      Role  System priority  System identifier  Port priority  Port number  Port key
ge-0/0/10        Actor  127  20:93:39:01:2f:00  127  1  2
ge-0/0/10        Partner 65534 02:00:00:02:00:01  1  3  3
ge-0/0/11        Actor  127  20:93:39:01:2f:00  127  2  2
ge-0/0/11        Partner 1  00:00:00:00:00:00  1  2  2
```

Enable interface 1/1/3 on Core-2.

```
sw-core2(config)# interface 1/1/3
sw-core2(config-if)# no shutdown
```

Confirm in Mist AI Remote Shell that both ports 10 and 11 are in Collecting distributing state.

```
mist@sw-edge2> show lacp interfaces
Aggregated interface: ae1
LACP state:      Role  Exp  Def  Dist  Col  Syn  Aggr  Timeout  Activity
```


ge-0/0/10	Actor	No	No	Yes	Yes	Yes	Yes	Fast	Active
ge-0/0/10	Partner	No	No	Yes	Yes	Yes	Yes	Slow	Active
ge-0/0/11	Actor	No	No	Yes	Yes	Yes	Yes	Fast	Active
ge-0/0/11	Partner	No	No	Yes	Yes	Yes	Yes	Slow	Active
LACP protocol:		Receive State		Transmit State		Mux State			
ge-0/0/10		Current		Slow periodic		Collecting distributing			
ge-0/0/11		Current		Slow periodic		Collecting distributing			

In Mist AI Remote Shell review interface ge-0/0/10, ge-0/0/11 and ae1 configuration with “show configuration interfaces” command.

```
mist@sw-edge2> show configuration interfaces ae1
apply-groups Uplink-to-cores;
aggregated-ether-options {
    lacp {
        active;
    }
}

{master:0}
mist@sw-edge2> show configuration interfaces ge-0/0/10
ether-options {
    802.3ad ae1;
}

{master:0}
mist@sw-edge2> show configuration interfaces ge-0/0/11
ether-options {
    802.3ad ae1;
}
```

Task 3-3: Dynamic port configuration

Objectives

Add rules to Dynamic port configuration in Switch Template

Use Dynamic port configuration with MAC addresses.

Validate configuration and port profiles with Front Panel View and CLI commands.

Steps

Navigate to Mist AI Switches > sw-edge2 and open **Remote Shell**. Check Juniper EX switch MAC address table entry on interface 4 with “show ethernet-switching table interface ge-0/0/4” command. This is VM MAC-Address which is connected to your table switch. Note this MAC OUI (first half) for the following steps.

```
mist@sw-edge2> show ethernet-switching table interface ge-0/0/4

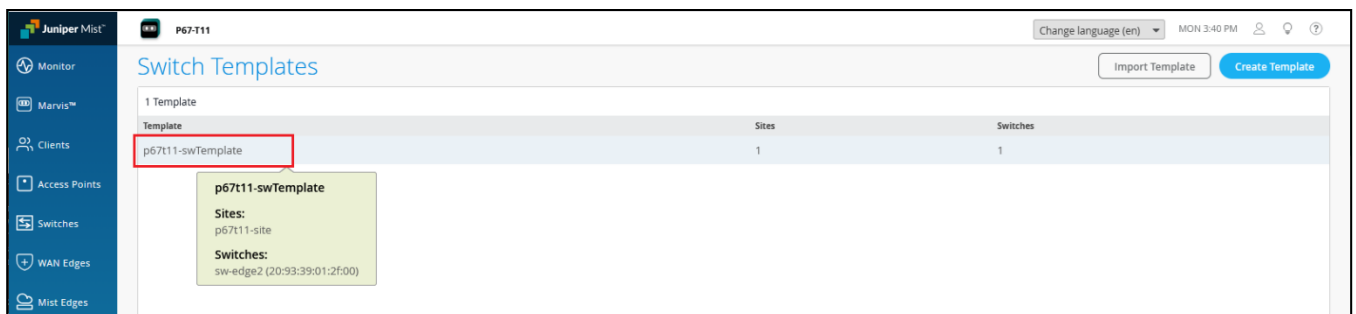
MAC database for interface ge-0/0/4

MAC database for interface ge-0/0/4.0

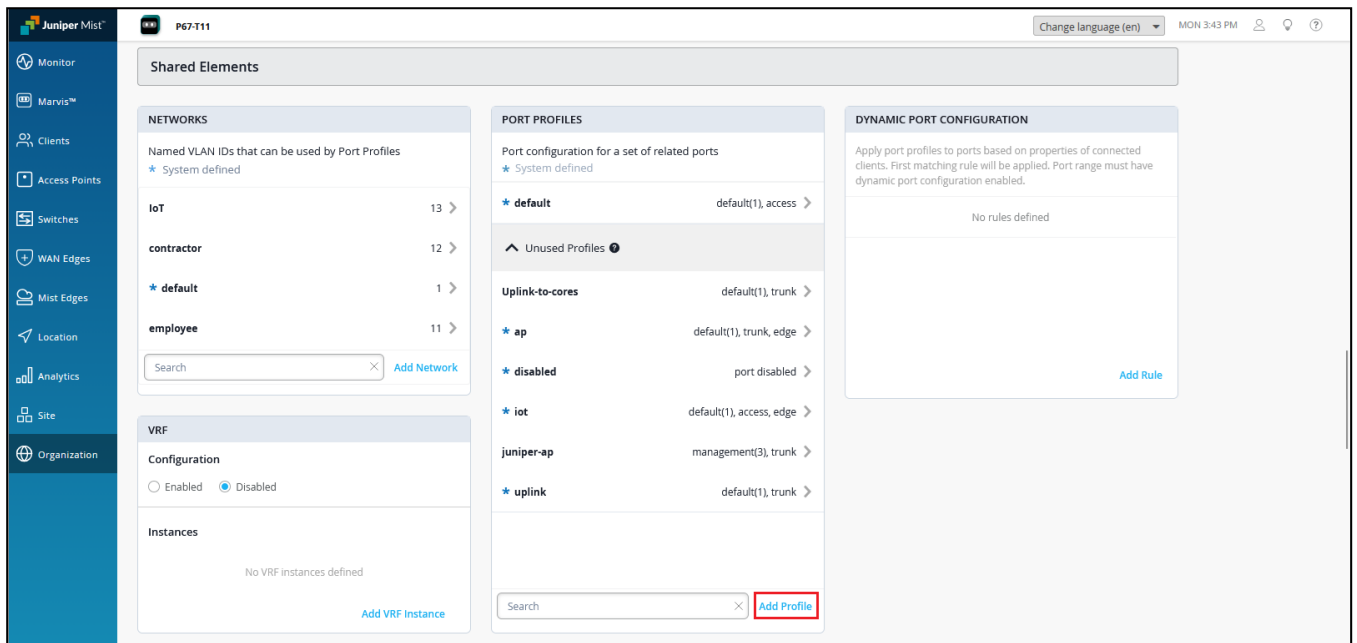
MAC flags (S - static MAC, D - dynamic MAC, L - locally learned, P - Persistent static, C
- Control MAC
          SE - statistics enabled, NM - non configured MAC, R - remote PE MAC, O - ovsdb
MAC
          GBP - group based policy)

Ethernet switching table : 1 entries, 1 learned
Routing instance : default-switch
  Vlan      MAC      MAC  Age  GBP   Logical   NH    RTR
  name      address flags   Tag   interface Index  ID
  default   00:50:56:b1:29:bd D    -    ge-0/0/4.0  0     0
```

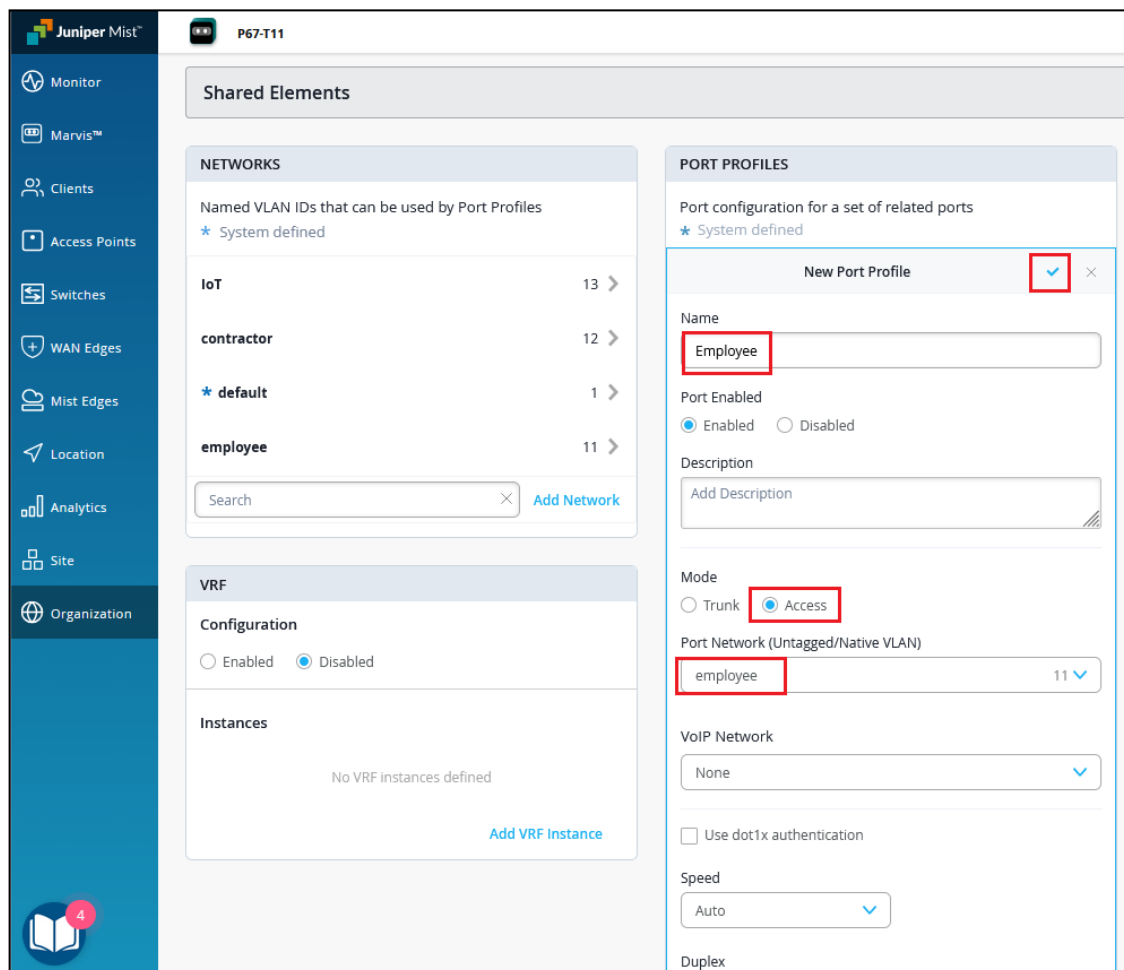
Navigate to Organization > Wired > Switch Templates and select your template.



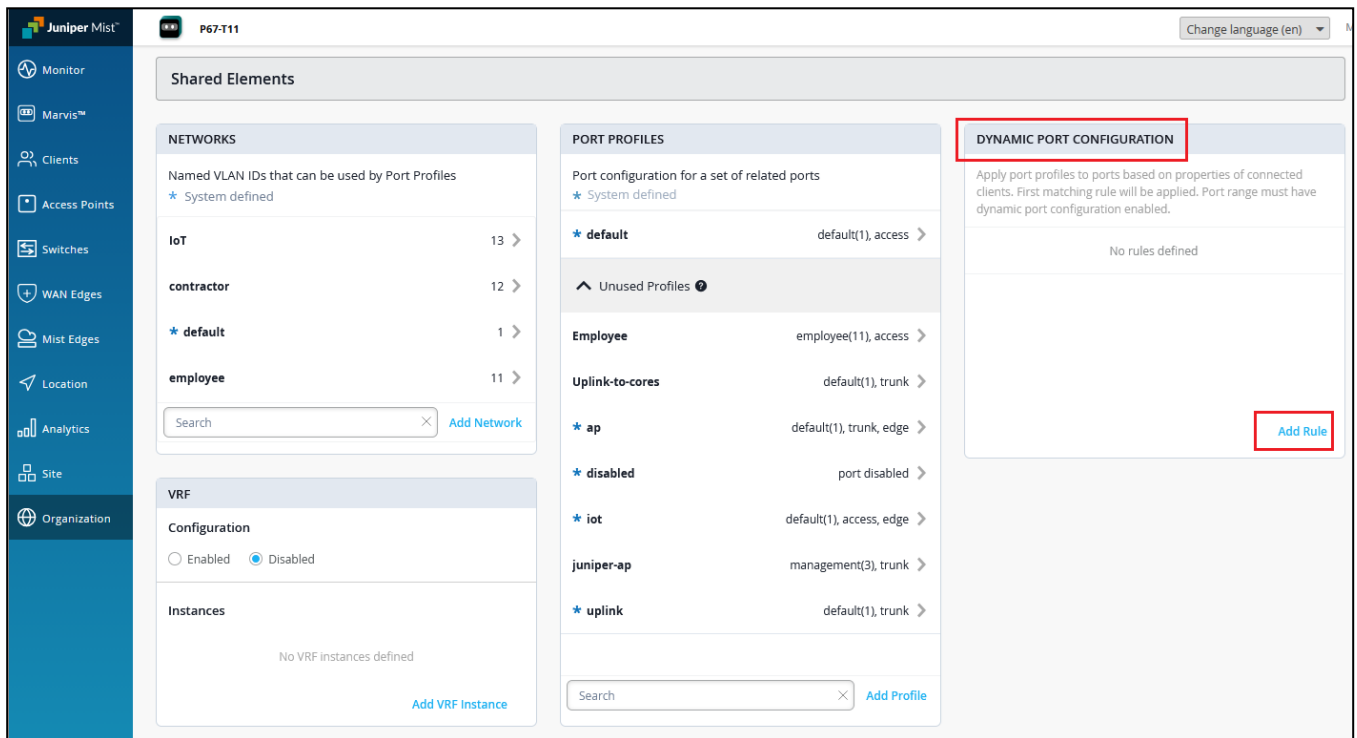
Scroll the page down to the Shared Elements section and click **Add Profile** to add a new Port Profile.



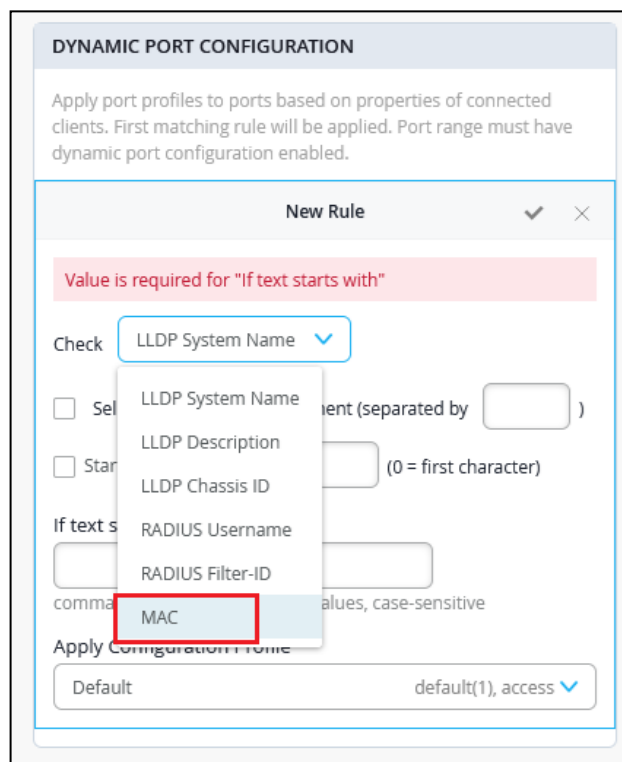
Give this new profile name “Employee”, keep Access Mode and select Network “employee”. Verify your configuration and click the check mark at the top.



Next, click **Add Rule** in Dynamic Port Configuration.



Click "Check", review available options and select MAC for this lab activity.



In "if text starts with" field enter MAC OUI you noted in step 1 and select Employee in "Apply Configuration Profile" drop-down menu. Then click the check mark to save new configuration.

DYNAMIC PORT CONFIGURATION

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

New Rule

Check

MAC

☐ Select the

1st

segment (separated by)

☐ Start at character offset

0

(0 = first character)

If text starts with

00:50:56

comma-separated same length values, case-sensitive

Apply Configuration Profile

Employee

employee(11), access

NOTE: You might have multiple rules configured for dynamic Port Configuration which will be evaluated from top to down and you can rearrange this order of rules with drag-and-drop. In the next Task you will configure additional rule.

Scroll the page up to the top and click **Save** to Apply new configuration and then **Save** again to confirm changes.

Juniper Mist

P67-T11

Change language (en)

MON 4:10 PM

Monitor

Marvis™

Clients

Access Points

Switches

WAN Edges

Mist Edges

Location

Analytics

Site

Organization

INFO

Name

p67t11-s

All Switches

Dynamic Port Config

Rules

00:50:56

Starts With: 00:50:56

Config Profile: Employee

Sort Order: 1

Source: link_peermac

Port Usages

Employee

Profile Name: Employee

Auto-Negotiation: Enabled

Block STP BPDUs: Disabled

Duplex: Auto

Enable MTU: Disabled

Enable QOS: Disabled

High Priority: Disabled

Legacy PD: Disabled

Mac Limit: 0

Mode: access

Per VLAN STP: Disabled

APPLIES TO SITES

1 sites

1 switches

Show only differences

+ Added

- Removed

* Template or System inherited

Save

Cancel

Navigate to Switches > sw-edge2. Notice the message at the top of the page.

Juniper Mist P67-T11

Change language (en) MON 4:12 PM

Locate Utilities Save Close

Switches: **sw-edge2**

Please select Enable Dynamic Configuration on a L2 interface for DPC rules to take effect.

Front Panel Port List

EX4100-F-12T

CPU Memory Temp PoE PSUs Fans

Metrics: Switch-AP Affinity PoE Compliance VLANs

100% Version Compliance 100% Switch Uptime

100% Config Success 100% Potential Anomalies

Properties:

INSIGHTS	Switch Insights
LOCATION	not on floorplan
MAC ADDRESS	20:93:39:01:2f:00
DEVICE ID	209339012f00
MODEL	EX4100-F-12T
VERSION	22.4R3.25
TEMPLATE	p67t11-swTemplate
SWITCH PHOTOS	

Statistics:

STATUS	Connected
IP ADDRESS	10.251.1.10 (vme.0) 10.1.99.11 (vlan 1)
MIST APS	0
WIRELESS CLIENTS	
TOTAL POWER DRAW	0.00 W
UPTIME	4d 3h 16m
LAST SEEN	May 11, 2026 4:11:25 PM
LAST DISCONNECT REASON	--
LAST CONFIG	May 11, 2026 4:11:07 PM

Switch Configuration

Configuration is Managed by Mist

Disable Configuration Management

NOTE: It's possible to enable Dynamic Configuration for multiple ports and multiple switches through Switch Template or Site Select Switches Configuration, but in this task, you will enable it for a single port.

In Switch Configuration section click **Add Port Configuration**.

Juniper Mist P67-T11

Change language (en) MON 4:15 PM

Locate Utilities Save Close

Switches: **sw-edge2**

Switch Configuration

Configuration is Managed by Mist

Disable Configuration Management

Device

INFO

Name: sw-edge2

Role: Select a role

Notes: Add Notes

IP CONFIGURATION (INBAND MANAGEMENT)

Configure IRB/SVI interfaces using DHCP or Static IP assignment

☐ Override Site/Template Settings

IP Address: DHCP Static

Network (VLAN): default

Additional IP Configuration

No IP Configuration defined

PORT

Port Profile Assignment

Port Configuration: Add Port Configuration

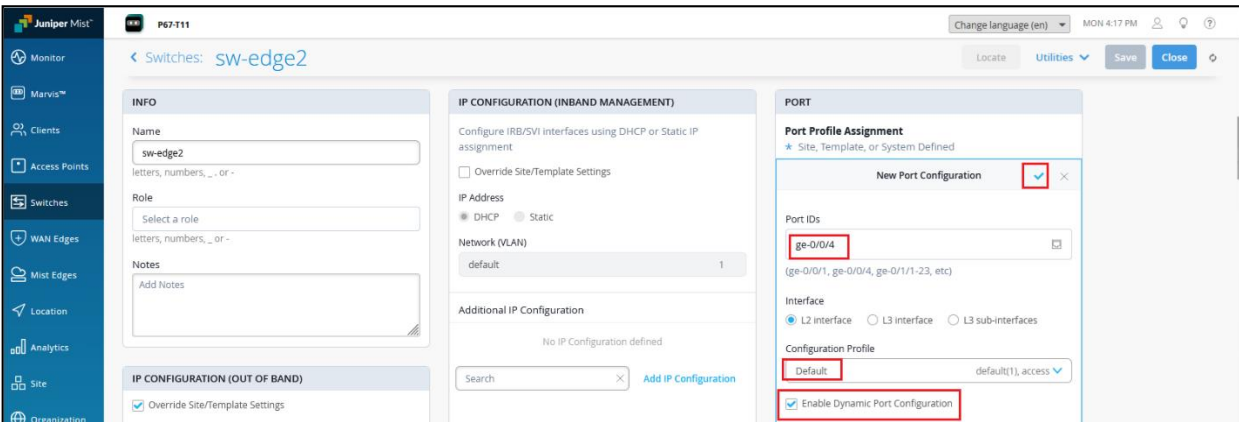
ge-0/0/2: juniper-ap

ge-0/0/10-11: Uplink-to-cores

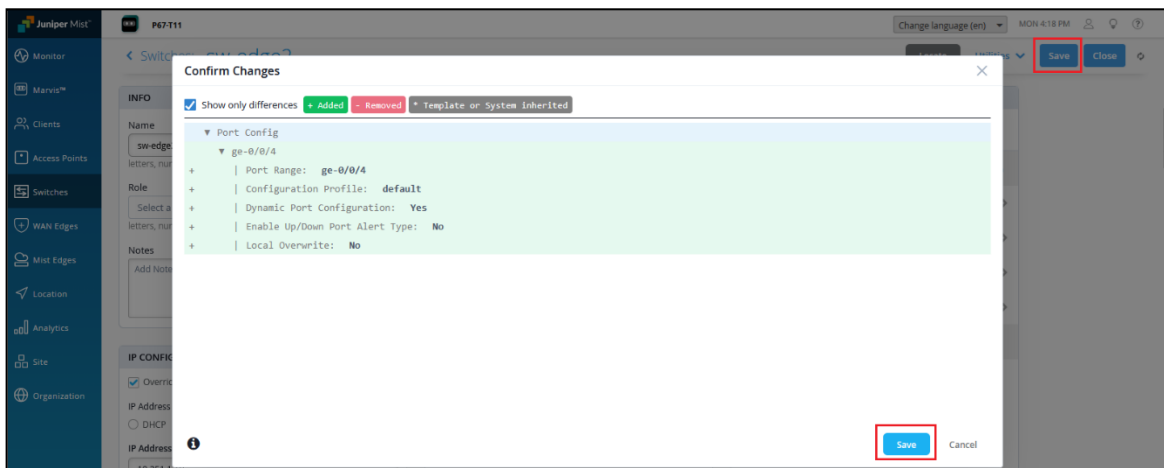
Unassigned ports: Default

Port Overrides BETA

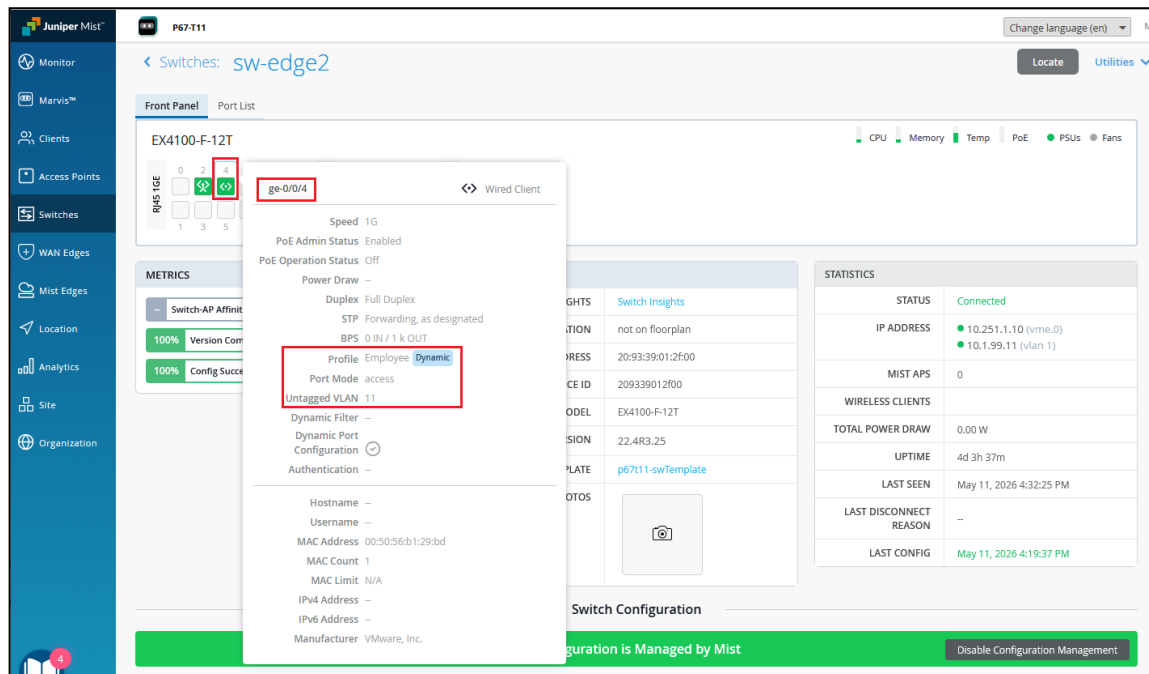
Select Port ID ge-0/0/4, Default Configuration Profile and enable check box "Enable Dynamic Port Configuration", then click on check mark to save new settings.



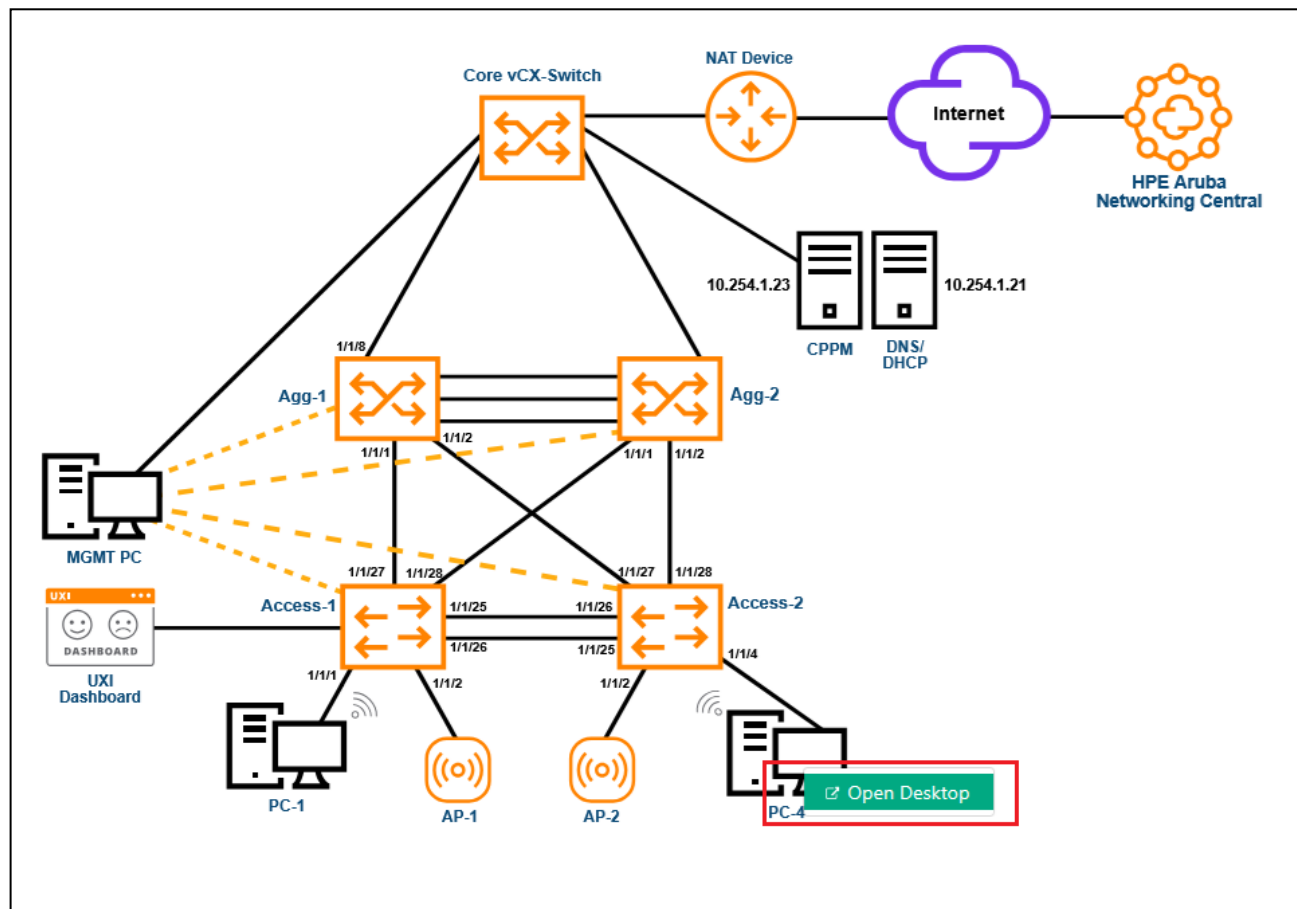
Click **Save** to apply a new configuration and **Save** again to confirm changes.



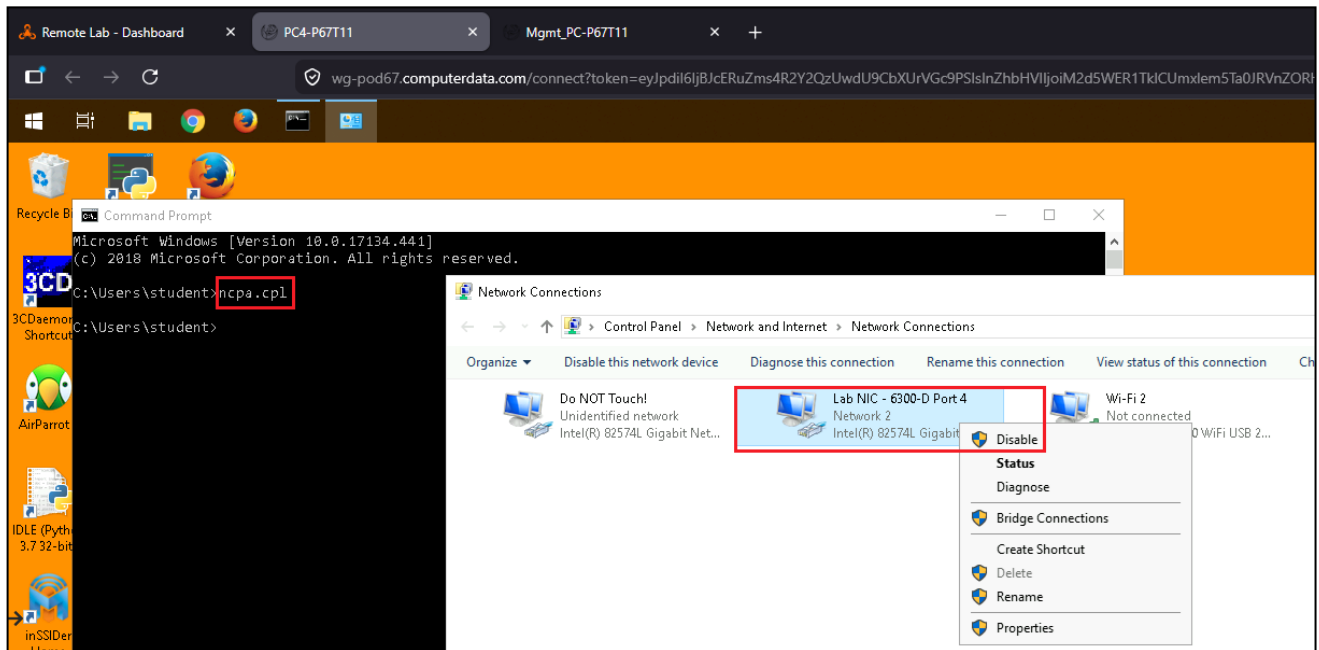
Wait about 5 minutes and refresh the page. You should see 100% Config Success. Hover your mouse over port 4. You should see Employee Profile Dynamically applied and untagged VLAN 11 in use.



Navigate to WebGate network diagram and connect to PC4 Remote Desktop.



Open CMD and type “**ncpa.cpl**” to access Network Connections settings. Then bounce Lab NIC (right mouse button then disable/enable).



Type “**ipconfig**” in CMD and confirm PC4 received IP address in 10.1.11.0/24 subnet used in VLAN 11.

```
C:\Users\student>ipconfig

Windows IP Configuration

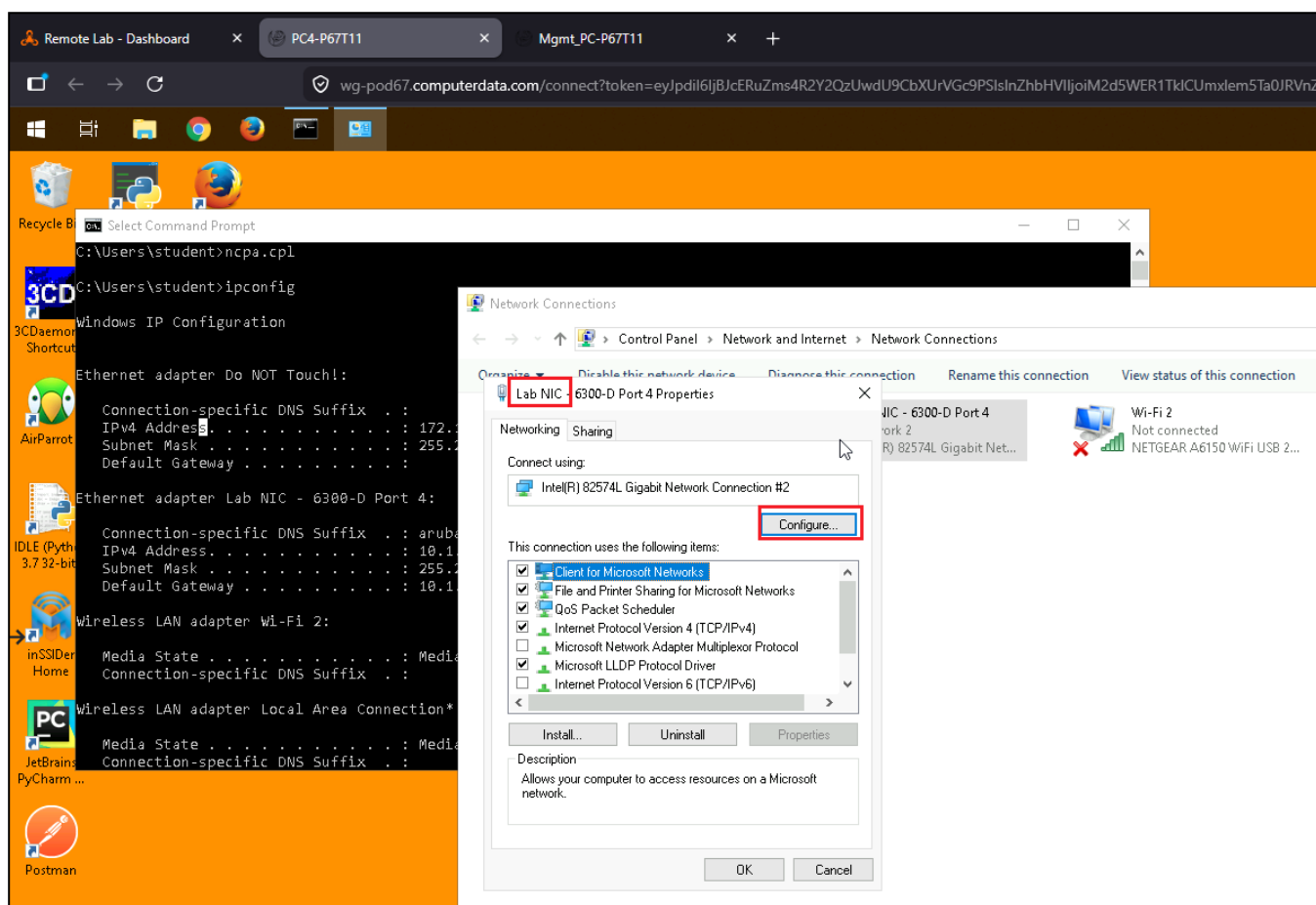
Ethernet adapter Do NOT Touch!:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 172.17.67.81
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

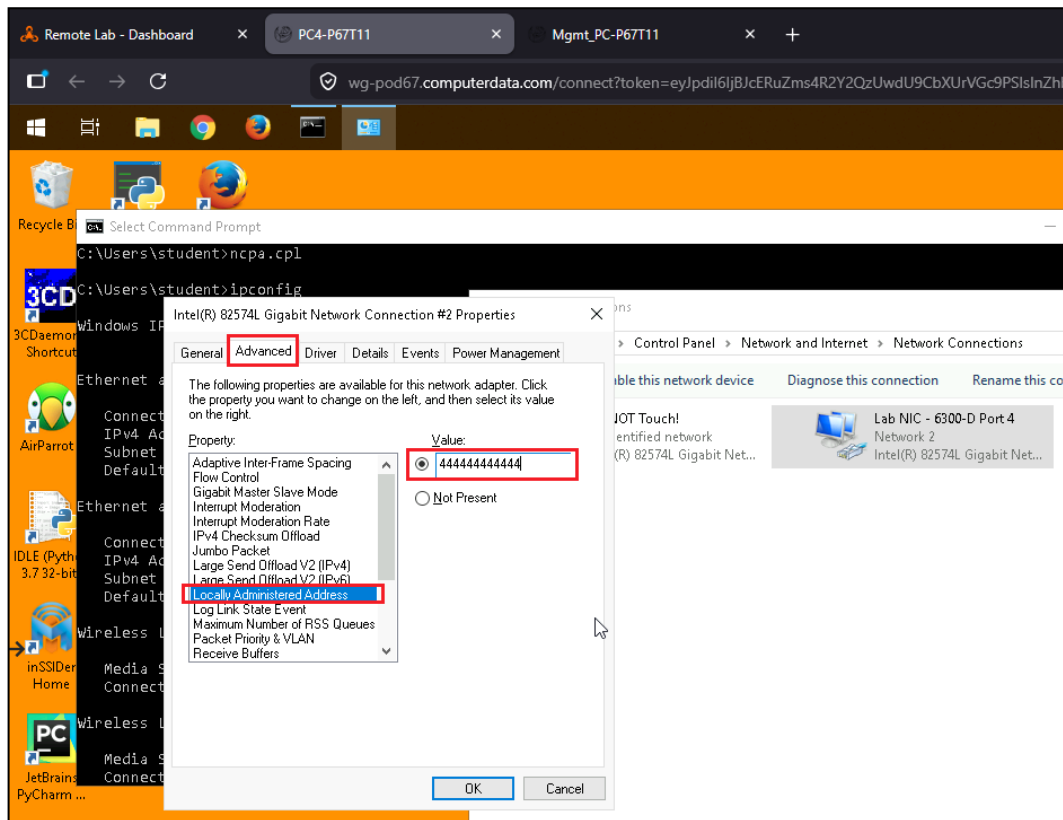
Ethernet adapter Lab NIC - 6300-D Port 4:

    Connection-specific DNS Suffix  . : aruba-training.com
    IPv4 Address. . . . . : 10.1.11.50
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.1.11.1
```

Click right-mouse button on Lab Nic, then click **Configure**.

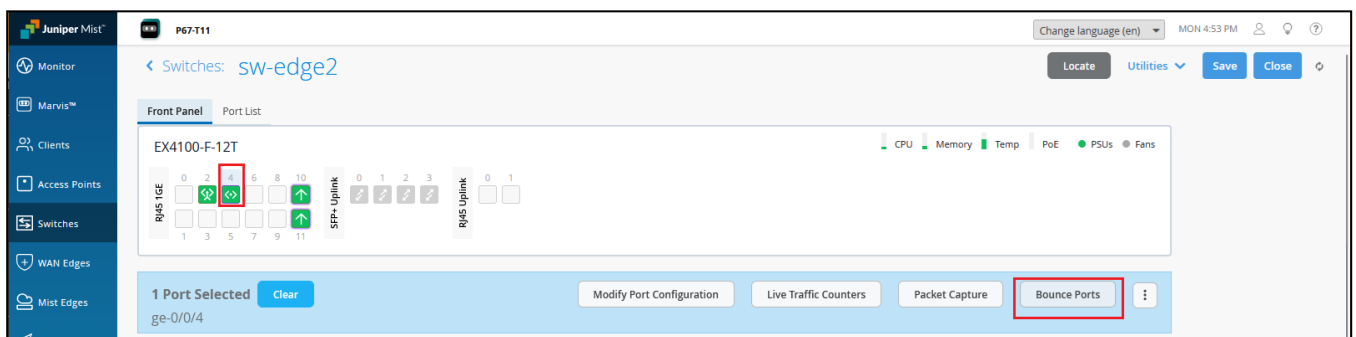


Switch to Advanced tab, select Locally Administered Address, click on Value and enter 4 x12 times to set PC4's MAC address to 44:44:44:44:44:44. Click OK.



Wait about 5-10 minutes. Navigate to Mist AI Switches > sw-edge2, select port 4 and click Bounce Port.

NOTE: You need to bounce port 4 on Juniper EX4100 switch to speed up dynamic Port Configuration. In our lab it takes longer time because PC4 is not directly connected to sw-edge2, but through intermediate fanout switch and vDS.



Confirm that Bounce Port ge-0/0/4 was successful.

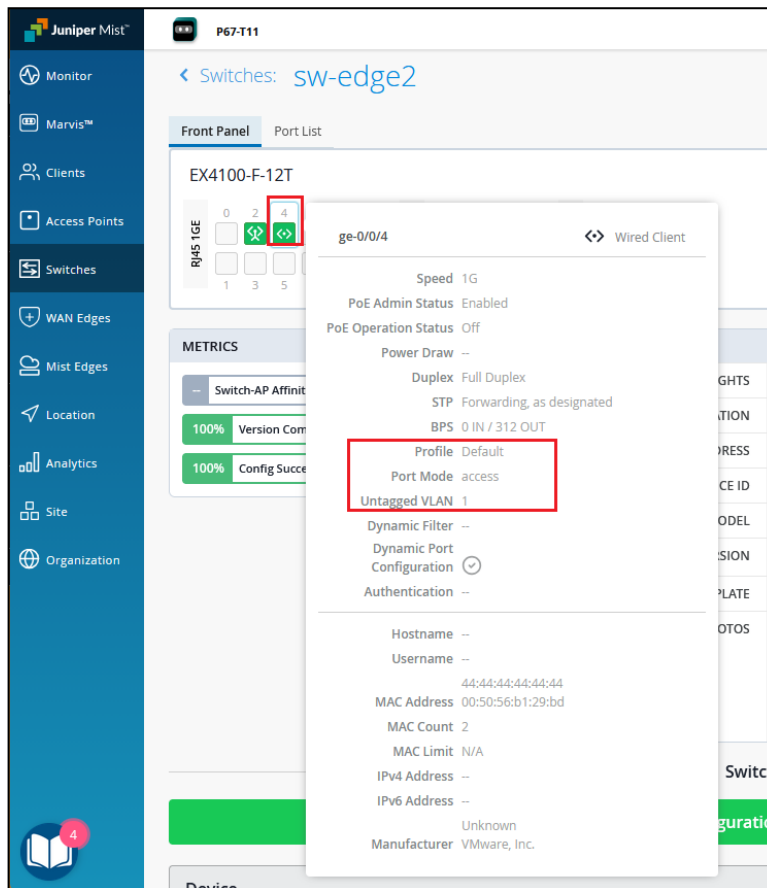
Bounce Port ge-0/0/4

May 11, 2026 4:53:59 PM

Bouncing port...

Port bounce complete.

Refresh the page and check applied Profile. It should show Default profile.



Jump to PC4, bounce interface Lab NIC and confirm with CMD “ipconfig” that it has IP in 10.1.99.0/24 now.

```
C:\Users\student>ipconfig
```

Windows IP Configuration

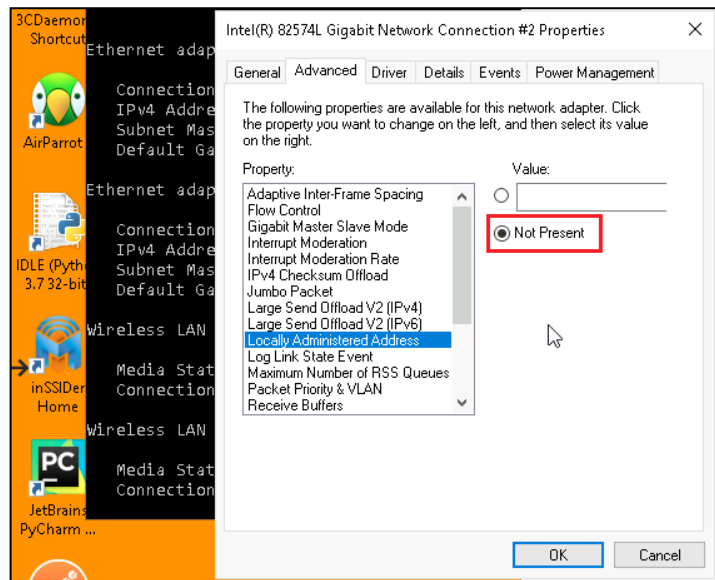
Ethernet adapter Do NOT Touch!:

```
Connection-specific DNS Suffix  . : 
IPv4 Address. . . . . : 172.17.67.81
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Ethernet adapter Lab NIC - 6300-D Port 4:

```
Connection-specific DNS Suffix  . : training.arubanetworks.com
IPv4 Address. . . . . : 10.1.99.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.1.99.2
```

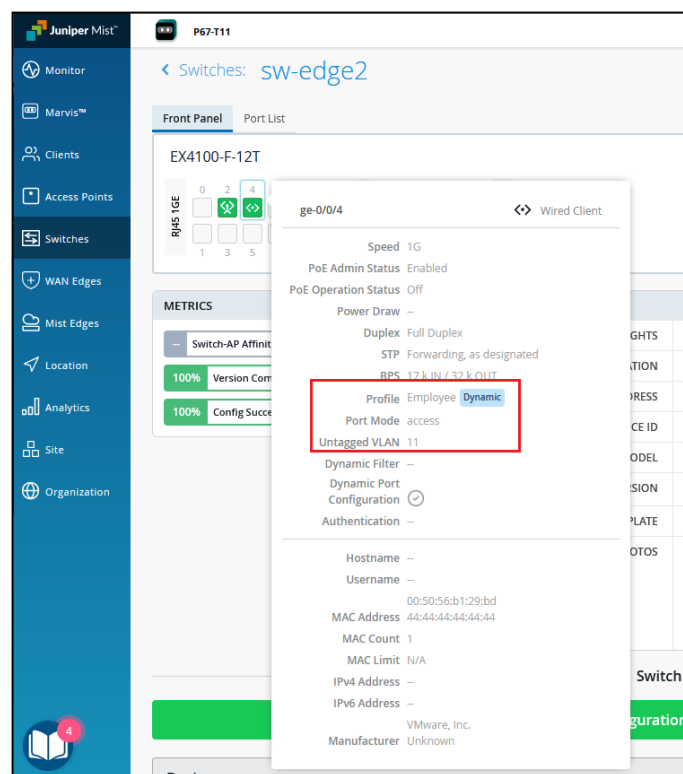
Repeat steps 17-18 on PC4 to set locally administered Address to Not Present and click OK.



In Mist AI, on sw-edge2 page with Front Panel bounce port 4 again. Close the window with Bounce Port result.

Bounce Port ge-0/0/4
May 11, 2026 5:00:53 PM
Bouncing port...
Port bounce complete.

Wait 5-10 minutes and refresh Mist AI page with sw-edge2 Front Panel. Hover mouse over port 4 and confirm that you see Profile Employee Dynamic.



On PC4 bounce Lab NIC and confirm with CMD “ipconfig” that it received IP from 10.1.11.0/24.

```
C:\Users\student>ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Do NOT Touch!:
```

```
Connection-specific DNS Suffix  . :  
IPv4 Address. . . . . : 172.17.67.81  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :
```

```
Ethernet adapter Lab NIC - 6300-D Port 4:
```

```
Connection-specific DNS Suffix  . : aruba-training.com  
IPv4 Address. . . . . : 10.1.11.50  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.1.11.1
```

Task 3-4: Network Access Control

Objectives

Configure RADIUS server with Switch Profiles

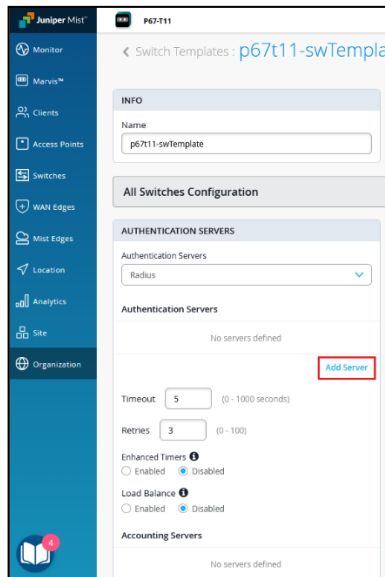
Enable 802.1X authentication in Port Profiles.

Use Dynamic Port Configuration with RADIUS attributes.

Validate configuration and applied profiles with Front Panel view and CLI commands.

Steps

Navigate to Organization > Wired > Switch templates and select your template. Then click Add server in Authentication Servers section.



Enter “cppm.aruba-training.com” in hostname field and “Aruba123!” in Shared Secret field. Then click on the check mark to save new settings.

Authentication Servers

Edit Server ✓ ×

Hostname / IP Address VAR

xxxx.xxx.xxx.xxx or {{siteVar}}.xxx.xxx

Port

Shared Secret ⓘ
 [Hide](#)

Timeout (0 - 1000 seconds)

Retries (0 - 100)

Enhanced Timers ⓘ
☐ Enabled ☒ Disabled

Load Balance ⓘ
☐ Enabled ☒ Disabled

Click Add Server next to Accounting Servers.

Juniper Mist P67-T11

All Switches Configuration

AUTHENTICATION SERVERS

Authentication Servers
 Radius ▼

Authentication Servers
 cppm.aruba-training.com : 1812 ➤

[Add Server](#)

Timeout (0 - 1000 seconds)

Retries (0 - 100)

Enhanced Timers ⓘ
☐ Enabled ☒ Disabled

Load Balance ⓘ
☐ Enabled ☒ Disabled

Accounting Servers

No servers defined

[Add Server](#)

Interim Interval (0 - 86400 seconds)

Source Address ⓘ
 ▼

Enter the same values as in step 2 and click the check mark.

Accounting Servers

New Server

Hostname / IP Address VAR
cppm.aruba-training.com

Port
1813

Shared Secret ?
Aruba123! Hide

Interim Interval 0 (0 - 86400 seconds)

Source Address ?
None

Set interim interval to 60 seconds, select source address from management network and enable CoA.

Accounting Servers

cppm.aruba-training.com : 1813

Add Server

Interim Interval 60 (0 - 86400 seconds)

☐ Immediate-Update ?

Source Address ?
management 3

Dynamic Request Port
☒ Enabled ☐ Disabled

CoA Port 3799 (1 - 65535)

Click **Save** at the top of the page to apply new settings and click **Save** again to confirm changes.

Confirm Changes

APPLIES TO SITES

1 sites 1 switches

☒ Show only differences Added Removed Template or System inherited

▼ AUTHENTICATION SERVER

- Immediate Update: No
- Interim Interval: 0 60
- Source Address: management

▼ Accounting Servers

- Host: cppm.aruba-training.com
- Secret: ***** @
- Port: 1813

▼ Authentication Servers

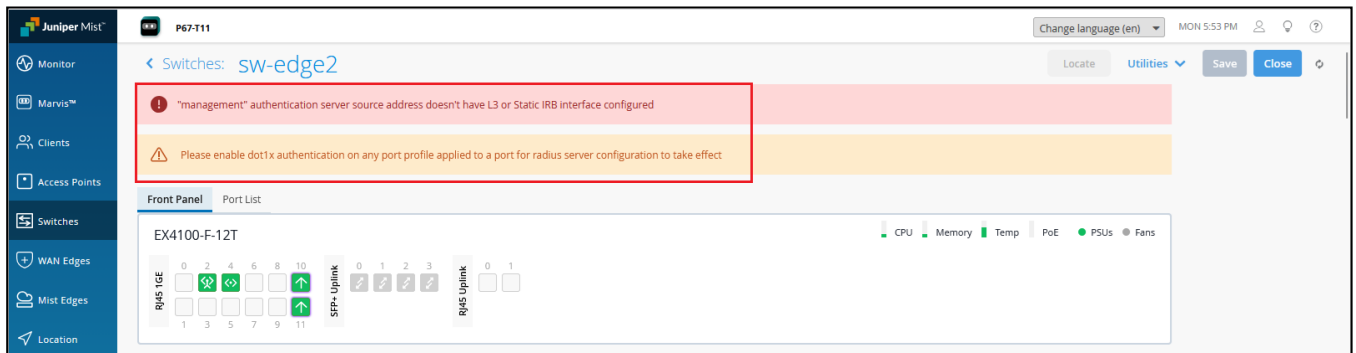
- Host: cppm.aruba-training.com
- Secret: ***** @
- Port: 1812

▼ Dynamic Request Port

- CoA Port: 3799
- Enabled: Yes

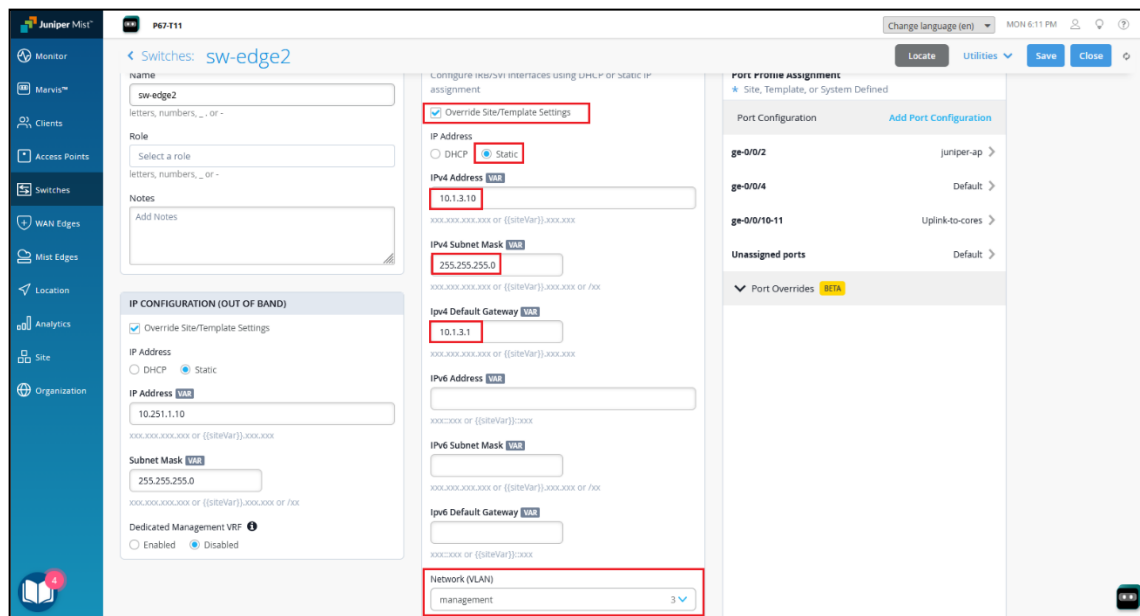
Save Cancel

In this lab we are going to use ClearPass Policy Manager as RADIUS server which is preconfigured to communicate with NAD (Network Access Device) in 10.1.3.0/24 MGMT subnet. RADIUS configuration requires to assign a static IP to SVI 3 on Juniper switch. Navigate to Switches > sw-edge2 and notice two messages at the top of the page.

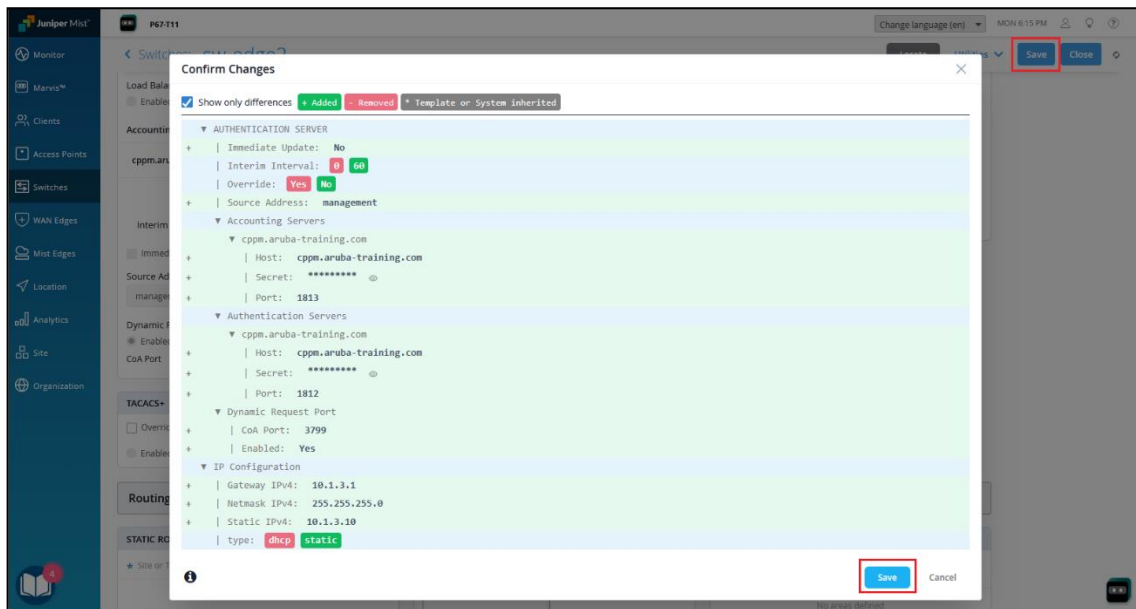


Scroll the page down to IP configuration (INBAND MANAGEMENT), enable checkbox “Override Site/Template Settings”, set Static IP address, set IPv4 Address to **10.1.3.10**, IPv4 Subnet Mask to **255.255.255.0**, IPv4 Default Gateway to **10.1.3.1** and select **management** network.

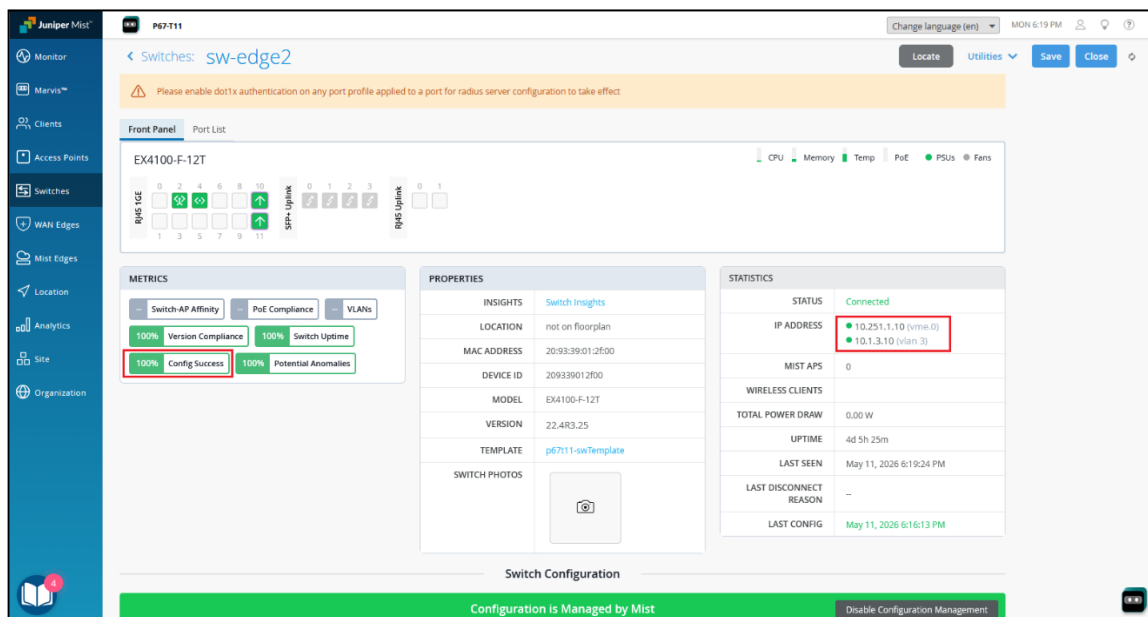
NOTE: It is possible to configure static IP address using variables. This will be explained in Lab 5.



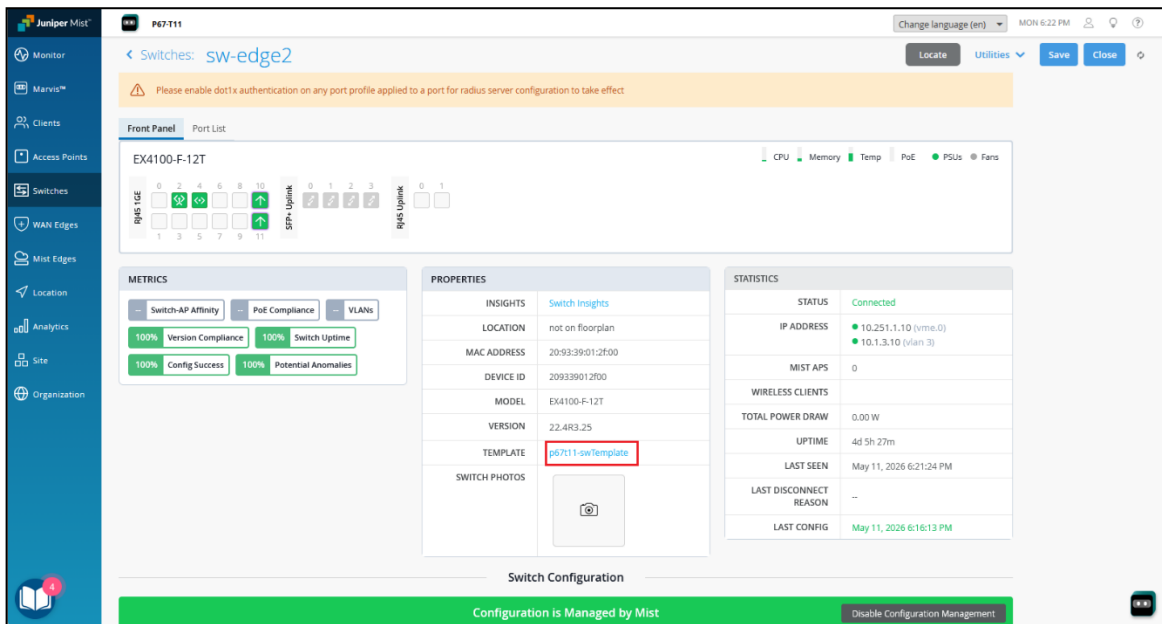
Click **Save** to apply new changes and click **Save** again to confirm changes.



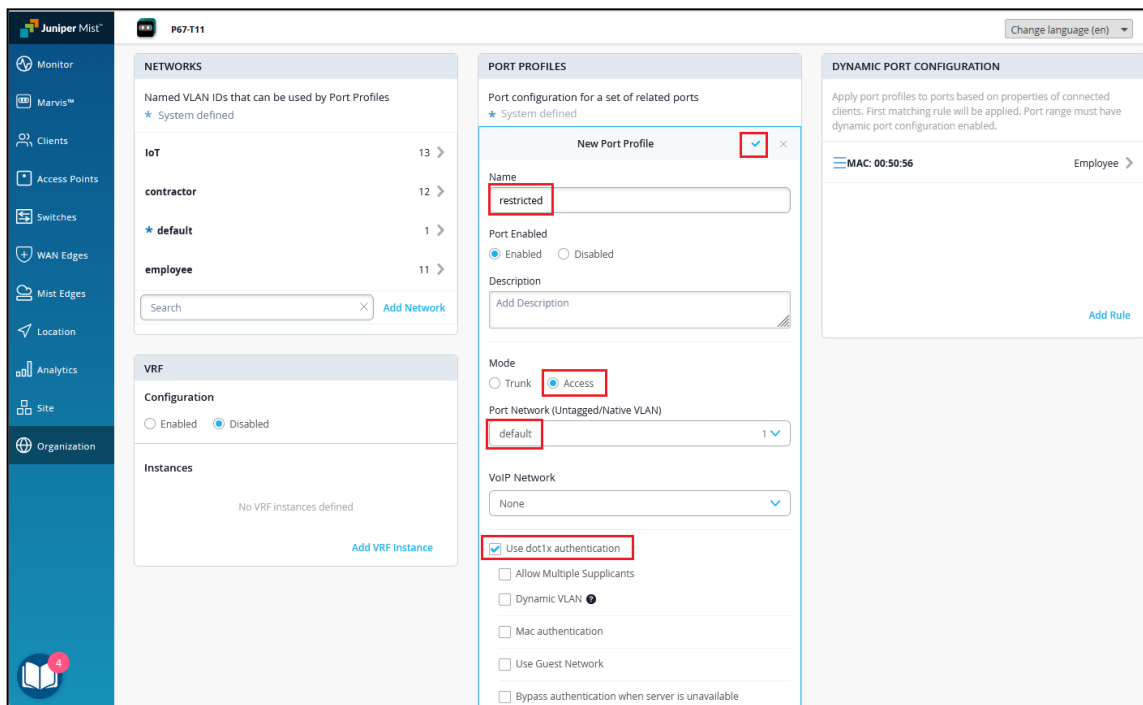
Wait 3-5 minutes and refresh the page. You should see 100% Config Success and new IP address assigned from 10.1.3.0/24.



Scroll the page up to the Properties and click on your template name.



Click Add Profile in Port Profiles. Name new profile as “restricted”, leave Access Mode and default Untagged VLAN, enable dot1x authentication and click the check mark to save these settings.



Edit Dynamic Port Configuration rule you added previously.

DYNAMIC PORT CONFIGURATION

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

MAC: 00:50:56	Employee >
---------------	------------

[Add Rule](#)

Change the settings to check RADIUS User-Name and text to employee instead of MAC address. Leave the configuration profile as Employee then click the check mark.

DYNAMIC PORT CONFIGURATION

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

✖
Edit Rule
✓
×

Check **RADIUS Username** ▼

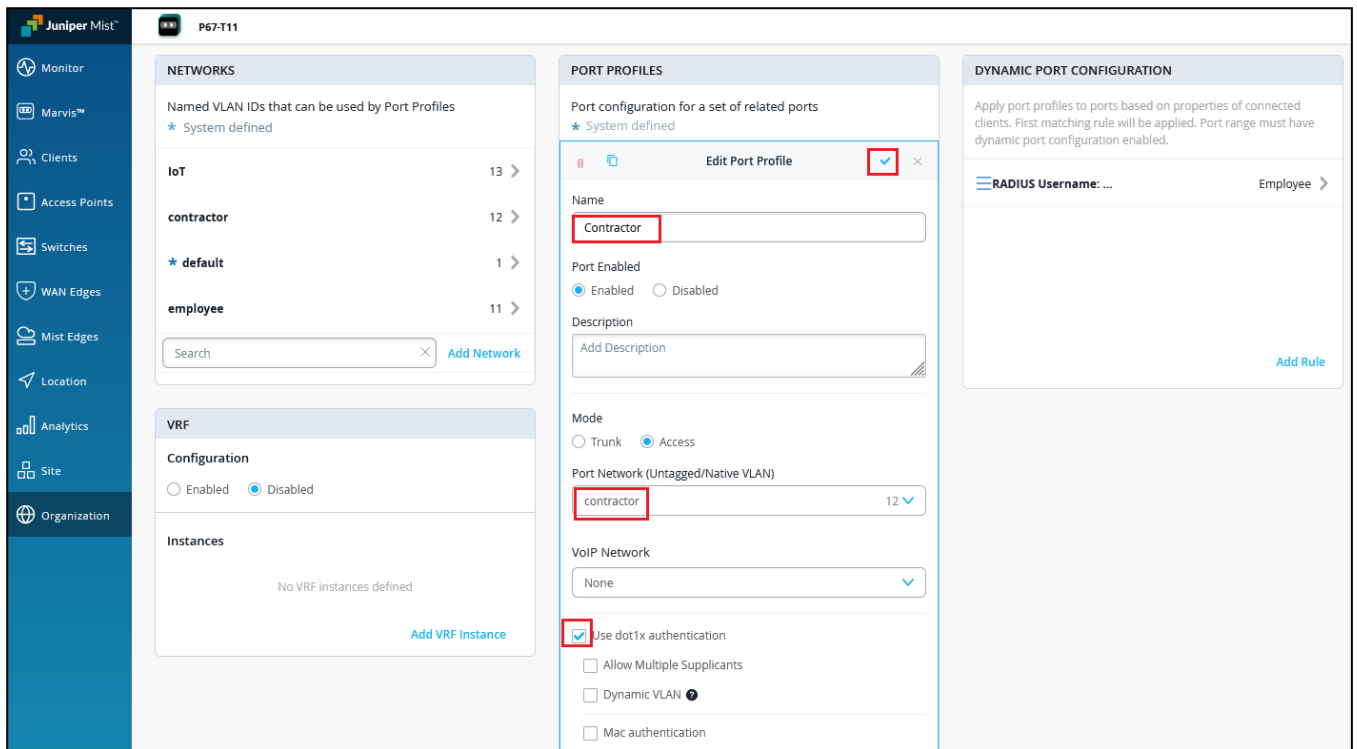
☐ Select the 1st ▼ segment (separated by)

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

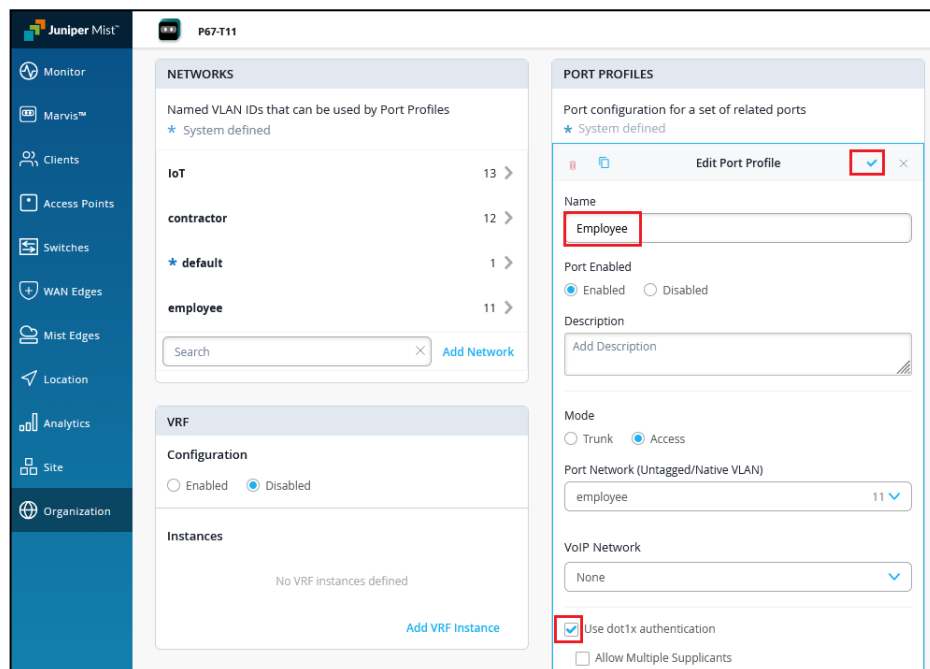
If text starts with
employee
comma-separated same length values, case-sensitive

Apply Configuration Profile
Employee employee(11), access ▼

Add new Port profile “Contractor” with “contractor” network and dot1x enabled. Click the check mark to add it.



Edit Employee Port Profile and enable dot1x. Click the check mark to save new settings.



Add a second rule to the Dynamic Port Configuration for contractor users. Use RADIUS User-Name with text contractor and apply Configuration Profile Contractor. Click the check mark to add new rule.

DYNAMIC PORT CONFIGURATION

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

New Rule

Check

RADIUS Username

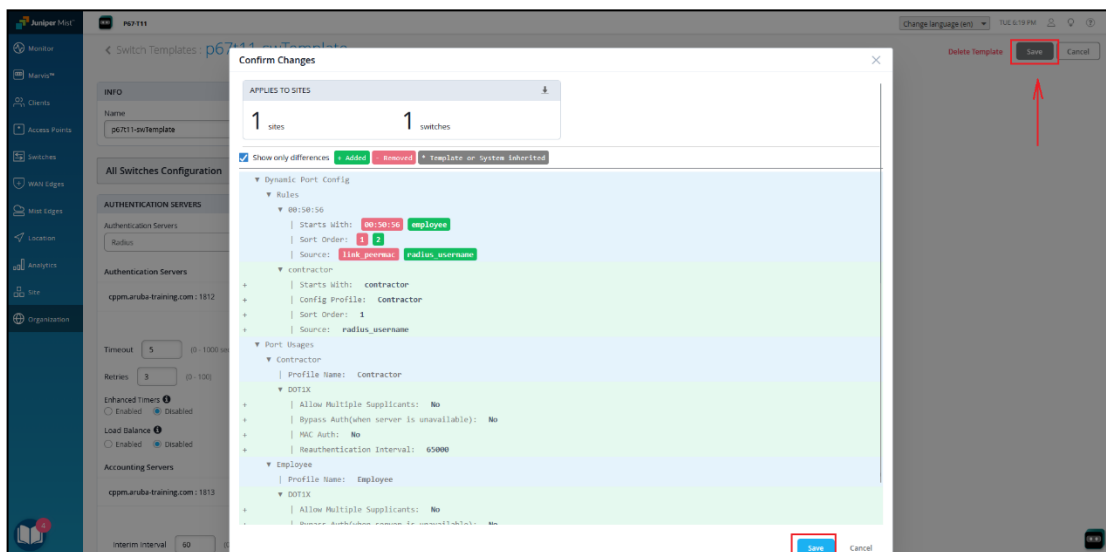
☐ Select the 1st segment (separated by)

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

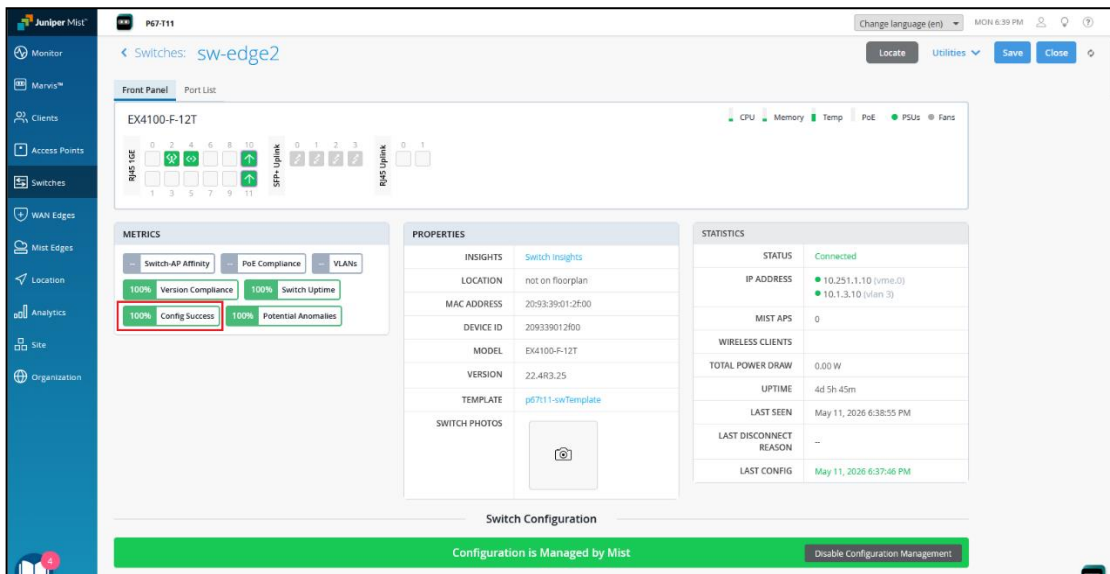
If text starts with
 contractor
comma-separated same length values, case-sensitive

Apply Configuration Profile
 Contractor contractor(12), access

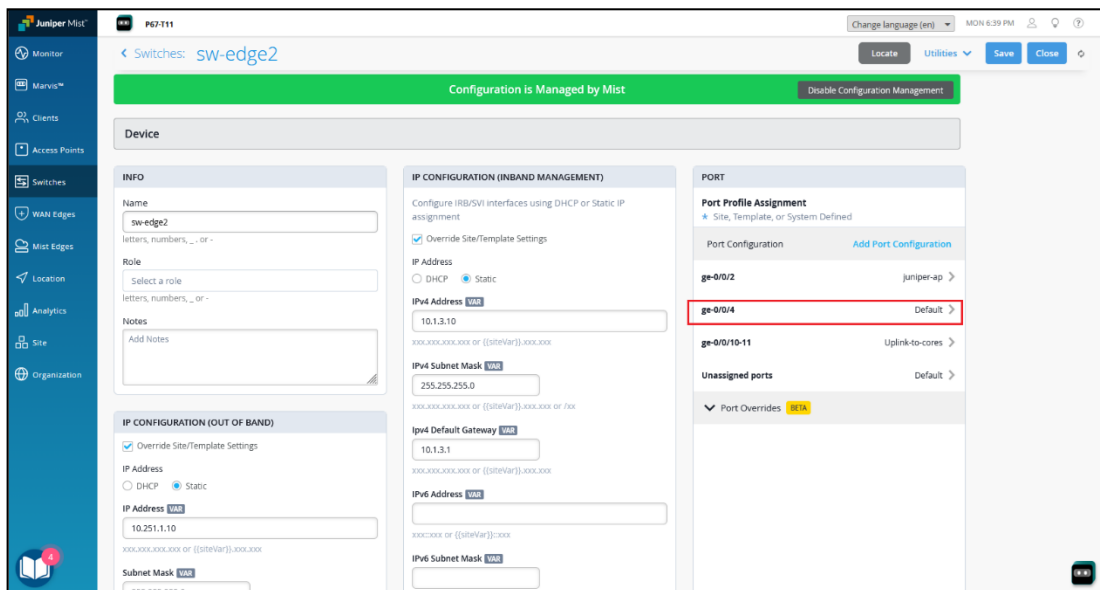
Scroll to the top of the page and click **Save** two times to apply and confirm changes.



Navigate to Switches > sw-edge2, wait 2-3 minutes to confirm that you have 100% Config Success.



Scroll the page down to Port settings and select ge-0/0/4.



Change the Configuration Profile from Default to restricted and click the check mark.

PORT

Port Profile Assignment
★ Site, Template, or System Defined

Edit Port Configuration [Save] [X]

Port IDs
ge-0/0/4
(ge-0/0/1, ge-0/0/4, ge-0/1/1-23, etc)

Interface
☒ L2 interface ☐ L3 interface ☐ L3 sub-interfaces

Configuration Profile
restricted default(1), access

☒ Enable Dynamic Port Configuration

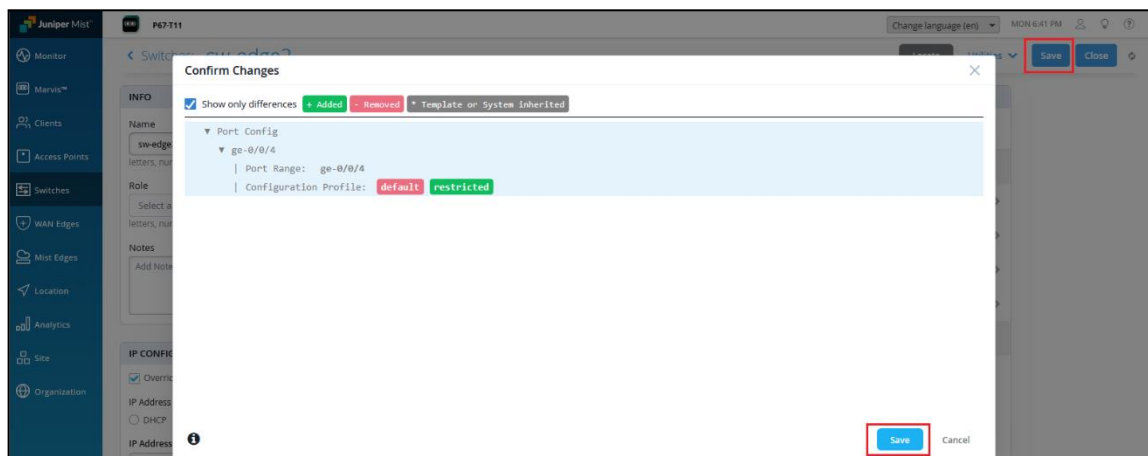
Description
Add Description

Up / Down Port Alerts ⓘ
☐ Enabled ☒ Disabled
[Manage Alert Types in Alerts Page](#)

Port Aggregation
☐ Enabled ☒ Disabled

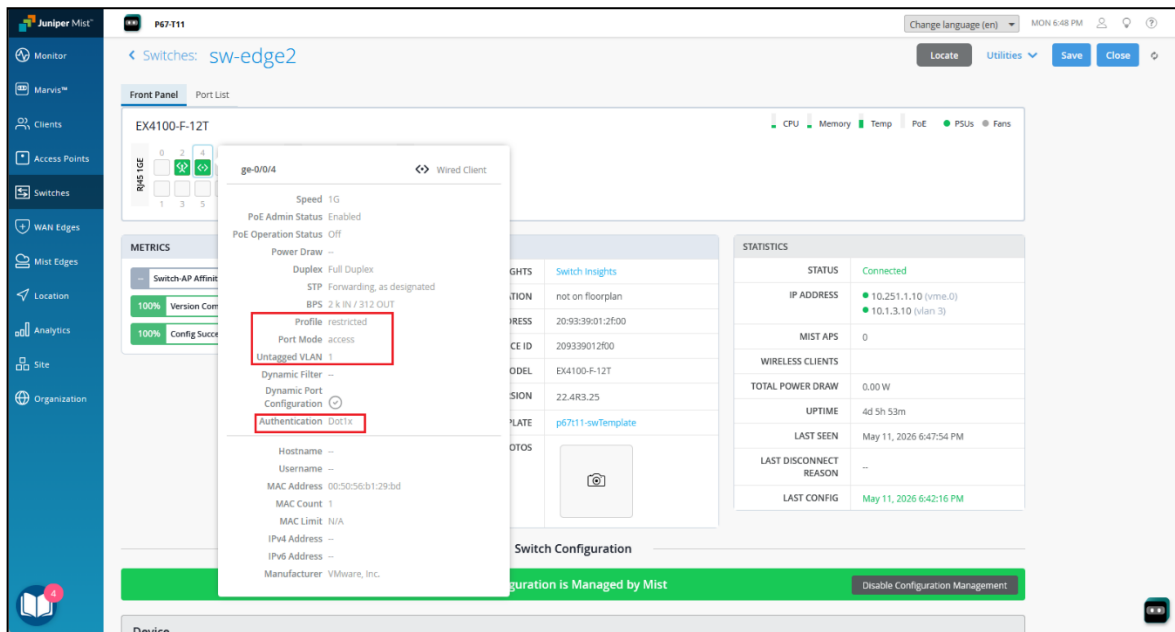
Allow switch port operator to modify port profile
☐ Yes ☒ No

Click Save two times to apply and confirm changes.

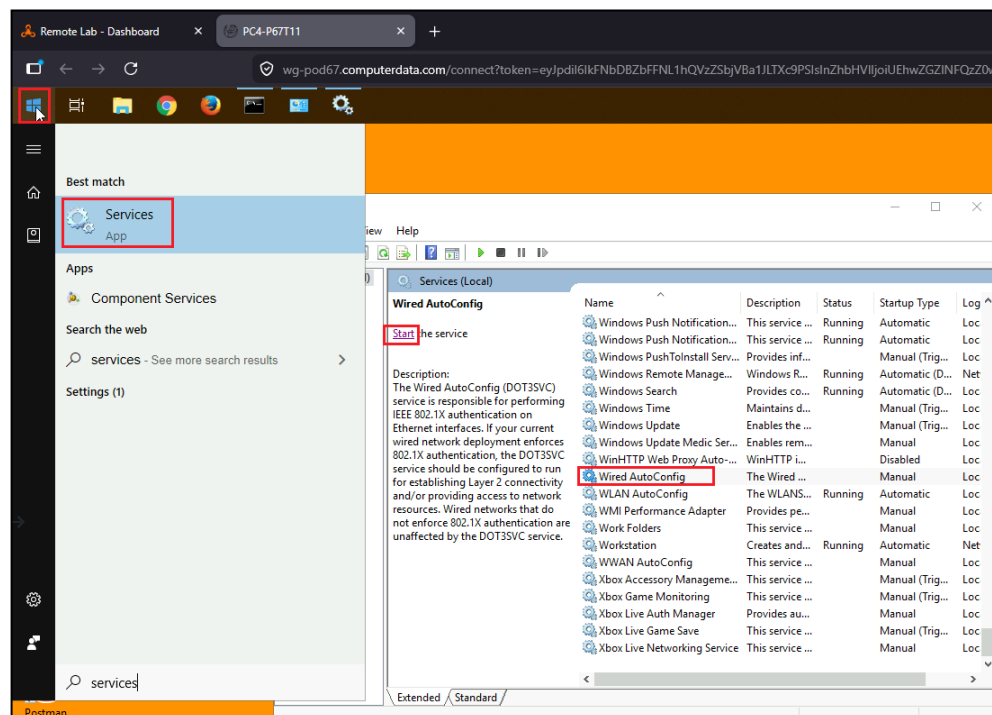


Wait 3-5 minutes, refresh the page and confirm that port 4 has restricted profile applied and 100% config Success.

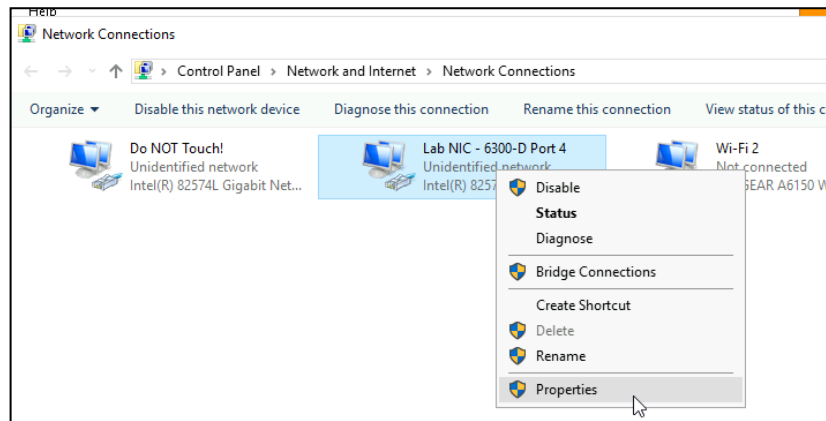
NOTE: To speed up this process, you might need to disable Lab NIC on PC4, then bounce port 4 in Mist AI then enable Lab NIC on PC4 and refresh the page in Mist AI.



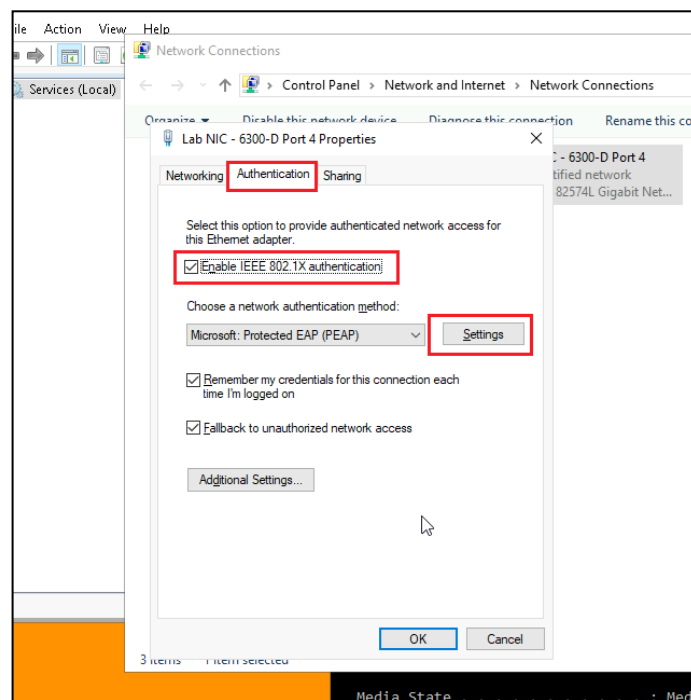
Navigate to PC4, click Windows Start button and type services. Click Services App and in services window search for “Wired AutoConfig” service. You can type wired to quickly find it. Then select this service and start it.



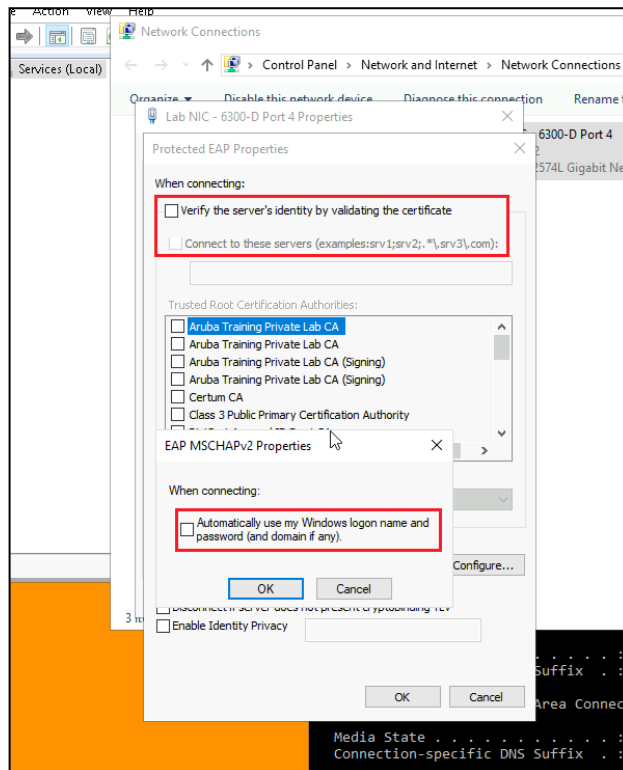
Open network connections window (type ncpa.cpl in CMD or in Windows Start), then open Lab NIC properties.



Switch to Authentication tab and enable 802.1X authentication. Then click Settings.

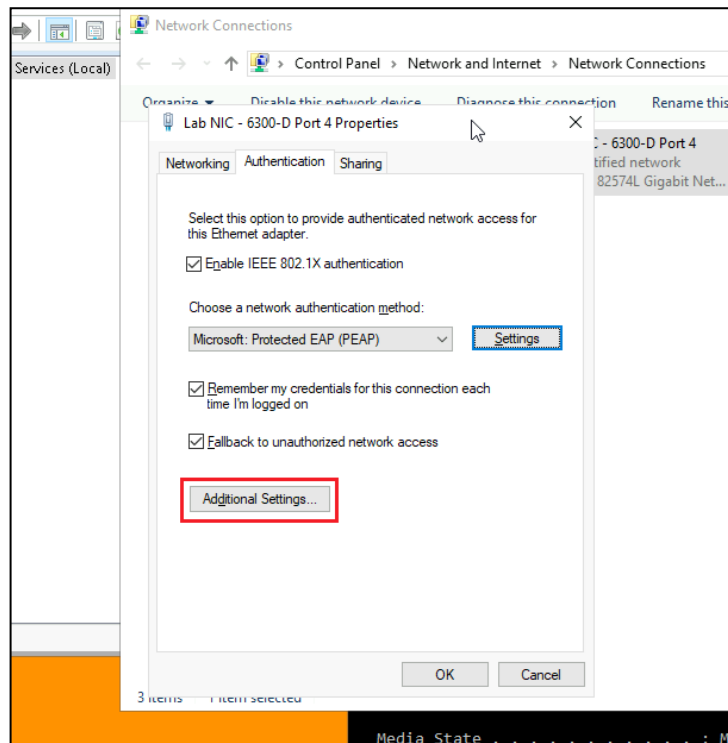


Disable “Verify the server’s identity by validating the certificate” check box, Click “Configure” and disable “Automatically use my Windows logon name and password”. Click “OK” two times to return to the Authentication tab.

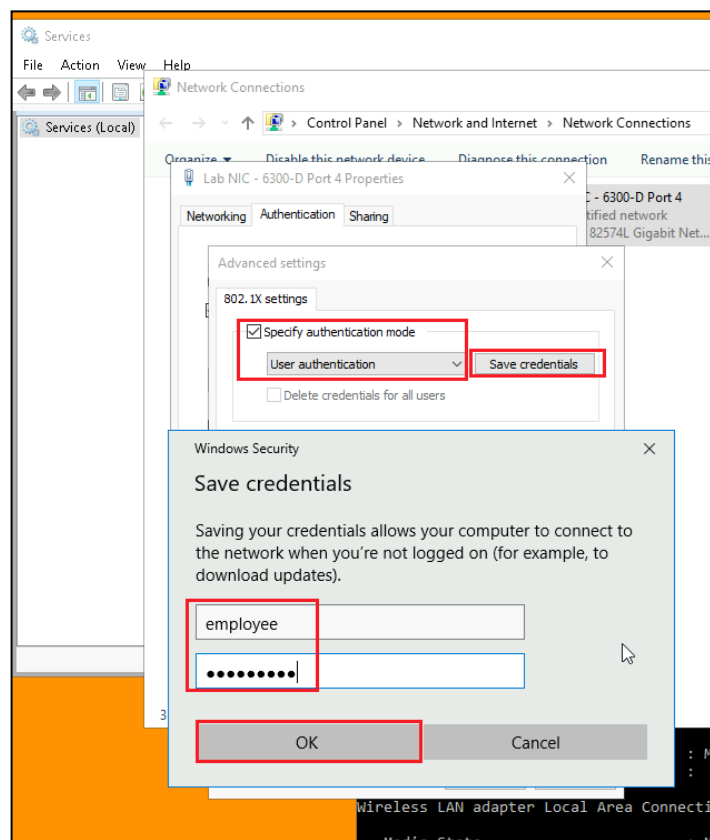


NOTE: Never disable RADIUS server verification in production network. In this lab client doesn't trust CA used to sign RADIUS certificate and to save your time we can disable it.

Click "Additional Settings".



Enable “Specify authentication mode” and set to “User authentication”. Click “Save credentials” and enter “**employee/Aruba123!**” credentials. Click “OK” three times to save your settings.



Your PC4 client is authenticated as employee now and should receive IP from 10.1.11.0/24. Check your client IP address with “ipconfig” command in CMD.

```
C:\Users\student>ipconfig
```

Windows IP Configuration

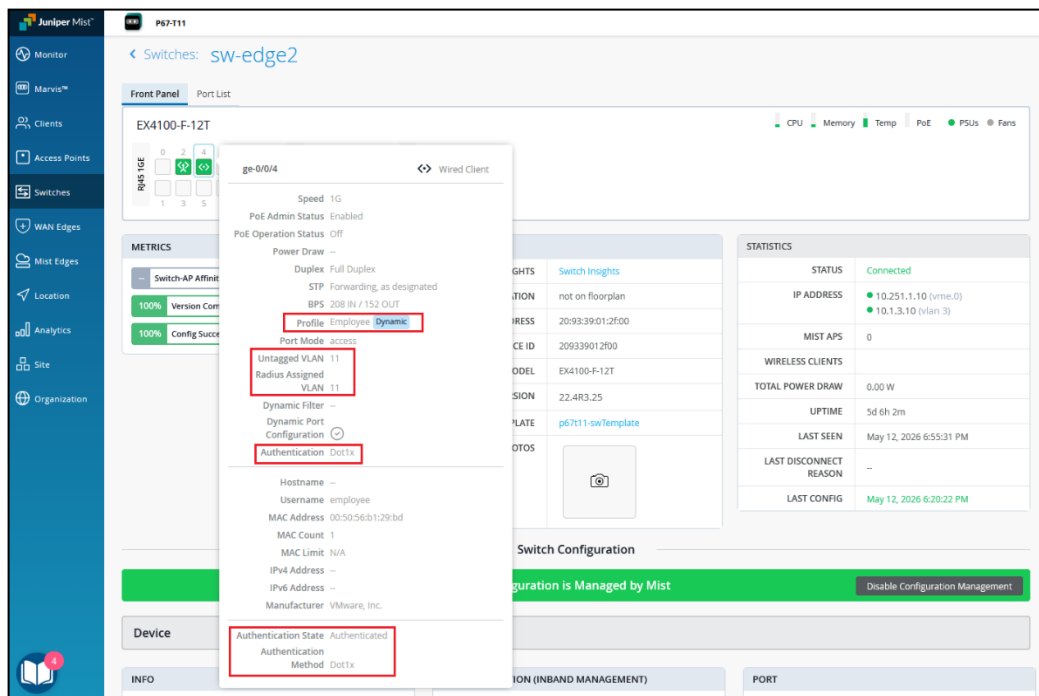
Ethernet adapter Do NOT Touch!:

```
Connection-specific DNS Suffix  . :  
IPv4 Address. . . . . : 172.17.67.81  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :
```

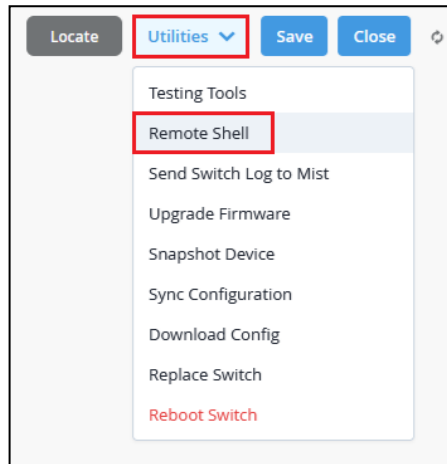
Ethernet adapter **Lab NIC** - 6300-D Port 4:

```
Connection-specific DNS Suffix  . : aruba-training.com  
IPv4 Address. . . . . : 10.1.11.50  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.1.11.1
```

Navigate to Mist AI Switches > sw-edge2, wait 5 minutes and refresh the page. Then hover your mouse over port 4. You should see your client authenticated as employee with Employee Dynamic profile applied, Radius assigned VLAN 11, and Dot1X successfully authenticated.



Click Utilities > **Remote Shell** in the top-right corner.

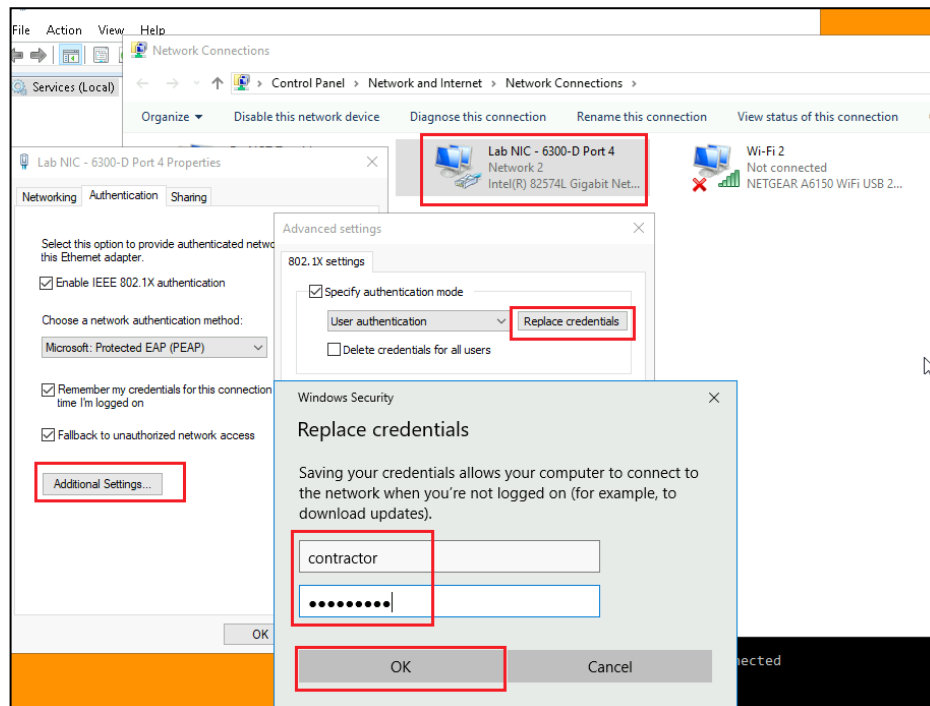


Type “show dot1x interface detail” command to check client authentication status on your switch.
You should see your client authenticated as employee. **Close** Remote Shell window.

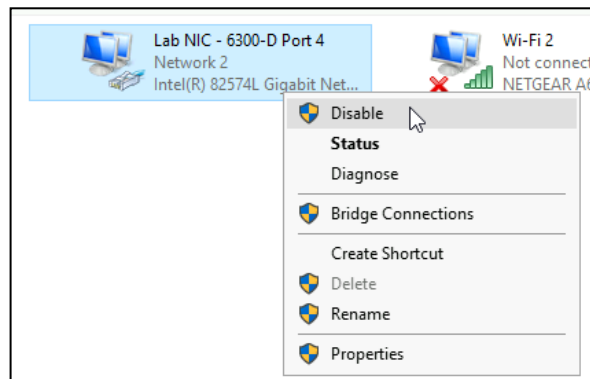
```
{master:0}
mist@sw-edge2> show dot1x interface detail
ge-0/0/4.0
Role: Authenticator
Administrative state: Auto
Supplicant mode: Single
Number of retries: 3
Quiet period: 60 seconds
Transmit period: 30 seconds
Mac Radius: Disabled
Mac Radius Restrict: Disabled
Reauthentication: Enabled
Reauthentication interval: 65000 seconds
Supplicant timeout: 30 seconds
Server timeout: 30 seconds
Maximum EAPOL requests: 2
Guest VLAN member: not configured
Number of connected supplicants: 1
  Supplicant: employee, 00:50:56:B1:29:BD
    Operational state: Authenticated
    Backend Authentication state: Idle
    Authentication method: Radius
    Authenticated VLAN: employee
    Session Reauth interval: 65000 seconds
    Reauthentication due in 64480 seconds
    Session Accounting Interim Interval: 600 seconds
    Accounting Update due in 80 seconds
    Eapol-Block: Not In Effect
    Domain: Data

{master:0}
mist@sw-edge2>
```

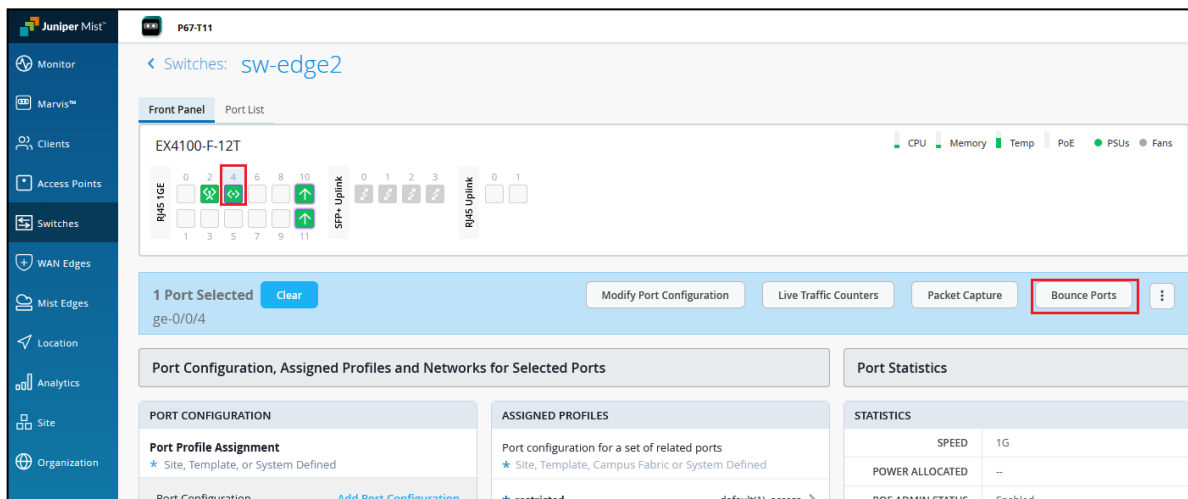
Switch to PC4, open Lab NIC properties, click Additional Settings, then Replace credentials and enter “**contractor/Aruba123!**” credentials. Click OK three times to save your settings.



Disable interface Lab NIC.



Navigate to Mist AI Switches > sw-edge2, select port 4 and click Bounce Ports.



Return to PC4 and **enable Lab NIC**. Your client is now authenticated as contractor. Check IP address assigned to PC4 with “ipconfig” in CMD.

```
C:\Users\student>ipconfig
```

Windows IP Configuration

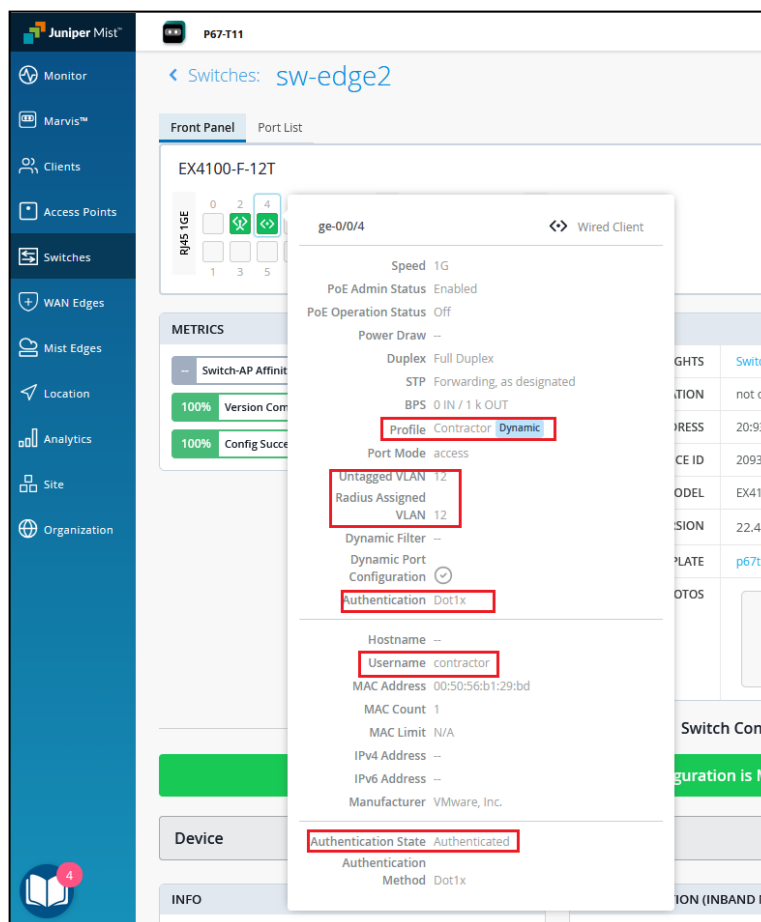
Ethernet adapter Do NOT Touch!:

```
Connection-specific DNS Suffix  . :  
IPv4 Address. . . . . : 172.17.67.81  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :
```

Ethernet adapter **Lab NIC** - 6300-D Port 4:

```
Connection-specific DNS Suffix  . : aruba-training.com  
IPv4 Address. . . . . : 10.1.12.50  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.1.12.1
```

Navigate to Mist AI Switches > sw-edge2. Wait 5 minutes, refresh the page and hover your mouse over port 4. You should see user contractor authenticated with dot1x, Dynamic Profile Contractor applied and RADIUS assigned VLAN 12.

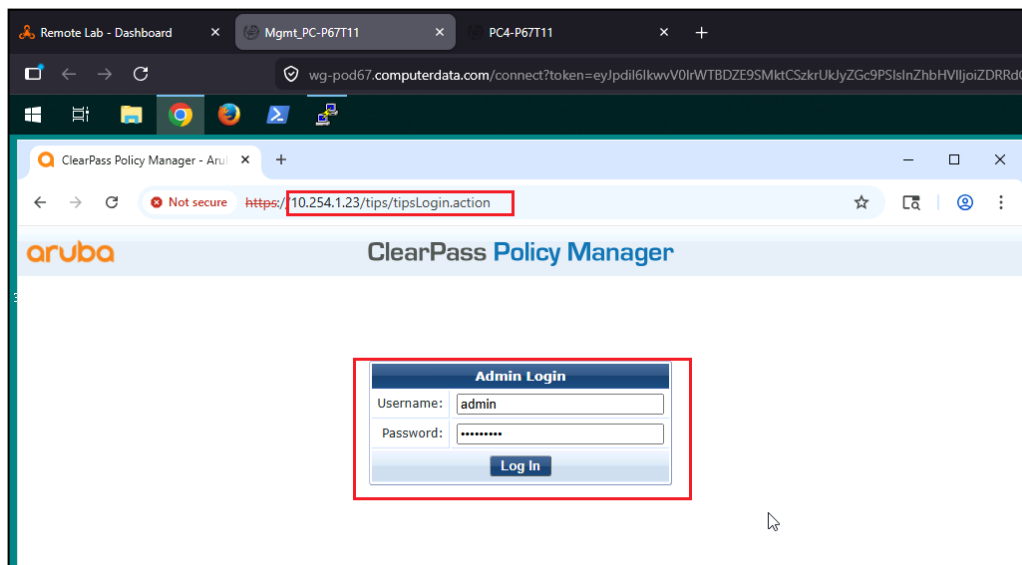


Click Utilities > **Remote Shell** and type command “show dot1x interface detail”.

```
{master:0}
mist@sw-edge2> show dot1x interface detail
ge-0/0/4.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Reauthentication interval: 65000 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: not configured
  Number of connected supplicants: 1
  Supplicant: contractor, 00:50:56:B1:29:BD
  Operational state: Authenticated
  Backend Authentication state: Idle
  Authentication method: Radius
  Authenticated VLAN: contractor
  Session Reauth interval: 65000 seconds
  Reauthentication due in 64578 seconds
  Session Accounting Interim Interval: 600 seconds
  Accounting Update due in 72 seconds
  Eapol-Block: Not In Effect
  Domain: Data

{master:0}
mist@sw-edge2>
```

Open MGMT PC Remote Desktop, launch VM browser and navigate to <https://10.254.1.23/tips>. Log in with “**admin/Aruba123!**” credentials.



Navigate to Monitoring > Access Tracker and review authentication attempts for employee and contractor in ClearPass Policy Manager Access Tracker.

The screenshot shows the ClearPass Policy Manager interface. The left sidebar has a 'Monitoring' section with 'Access Tracker' selected. The main panel displays 'Access Tracker May 12, 2026 23:21:55 UTC'. A table lists requests, with the first one selected. A 'Request Details' modal is open, showing the following information:

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R000000a7-01-6a03b2ef		
Date and Time:	May 12, 2026 23:08:32 UTC		
End-Host Identifier:	00-50-56-B1-29-BD		
Username:	contractor		
Access Device IP (Port):	10.1.3.10 (565)		
Access Device Name:	sw-edge2		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Juniper - wired - dot1x		
Authentication Method:	EAP-PEAP,EAP-MSCHAPV2		
Authentication Source:	Local:localhost		
Authorization Source:	[Local User Repository]		
Roles:	[Other], [User Authenticated]		
Enforcement Profiles:	RADIUS-Username		

The screenshot shows the ClearPass Policy Manager interface. The left sidebar has a 'Monitoring' section with 'Access Tracker' selected. The main panel displays 'Access Tracker May 12, 2026 23:22:26 UTC'. A table lists requests, with the first one selected. A 'Request Details' modal is open, showing the following information:

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R000000a4-01-6a03af3b		
Date and Time:	May 12, 2026 22:52:43 UTC		
End-Host Identifier:	00-50-56-B1-29-BD		
Username:	employee		
Access Device IP (Port):	10.1.3.10 (565)		
Access Device Name:	sw-edge2		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Juniper - wired - dot1x		
Authentication Method:	EAP-PEAP,EAP-MSCHAPV2		
Authentication Source:	Local:localhost		
Authorization Source:	[Local User Repository]		
Roles:	[Other], [User Authenticated]		
Enforcement Profiles:	RADIUS-Username		

You have completed this lab!

Lab 4: Day 2: Wired network Monitoring and Troubleshooting

Objectives

After completing this lab, you will be able to:

- Wired Visibility
- Monitor with Service Levels
- Marvis Actions
- Packet Capture for Wired client traffic

Overview

After completing this lab, you will learn how to monitor and troubleshoot Wired Clients and switches in Mist AI. Juniper Mist web UI could be changed over the time and will not match screenshots in this workshop. Ask your instructor for assistance if you struggle finding required settings in Juniper Mist.

Task 4-1: Wired Visibility

Objectives

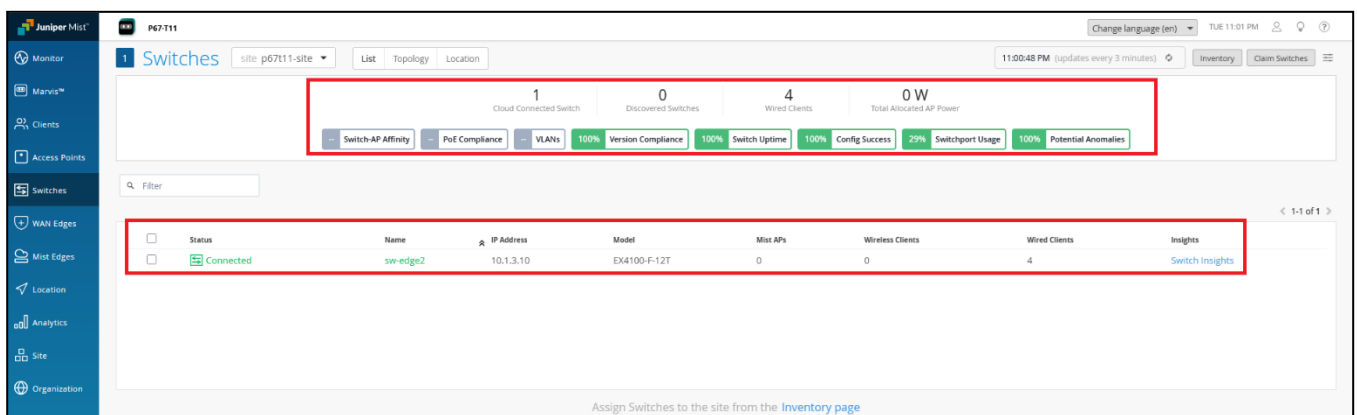
Switches page and switch metrics.

Switch details.

Wired Client Insights.

Steps

Navigate to Mist AI Switches page and observe switch metrics and details about cloud connected switches. Hover your mouse over different metrics to read the explanation.



Switch-AP Affinity – weighted percentage of switches that have more than 12 access points connected.

PoE Compliance – percentage of access points that have the required power

VLANs – percentage of access points for which all wired VLANs are active

Version Compliance – percentage of switches that have the same software version (per switch model)

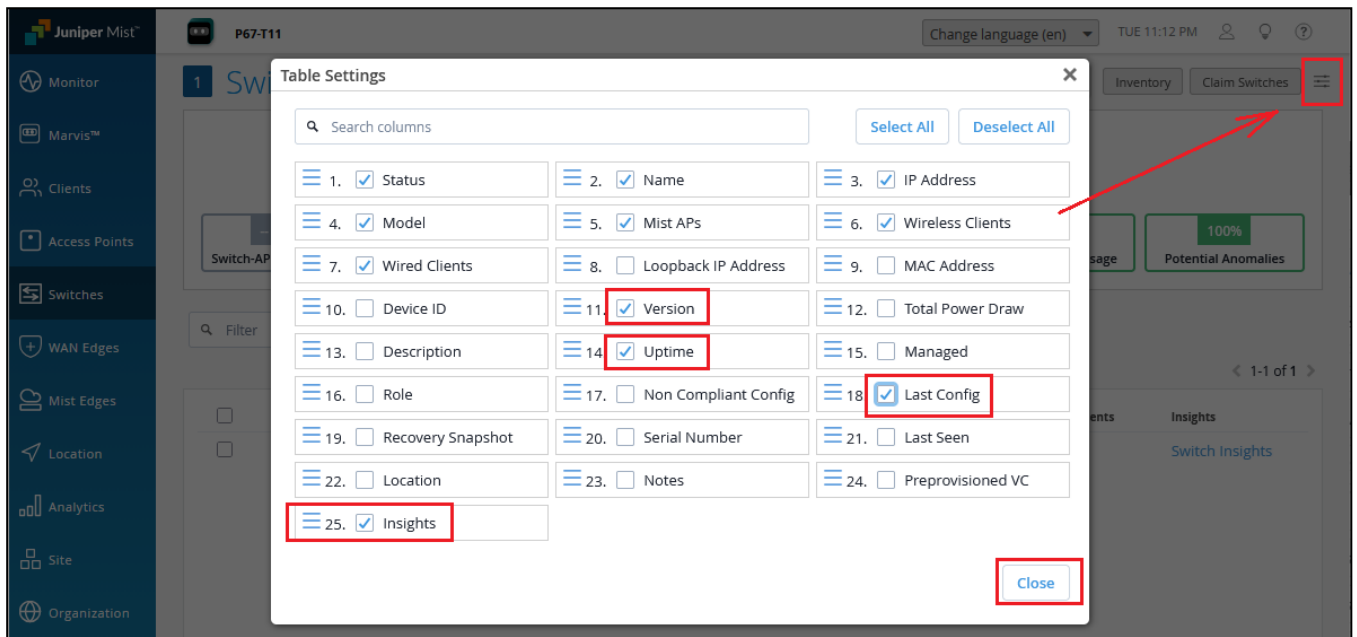
Switch Uptime – percentage of time the switch was up during the past 7 days, average across all switches

Config Success – percentage of online switches that are not in config failed state

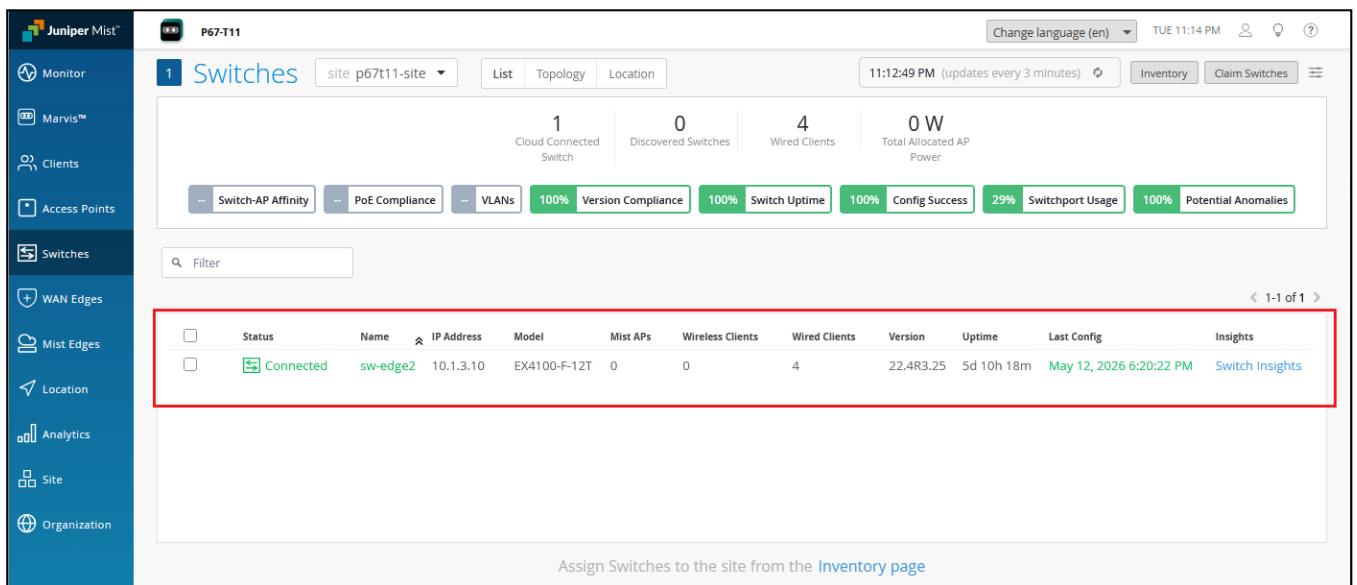
Switchport Usage – 4 of 14 ports active (10 ports inactive)

Potential Anomalies – percentage of switches without any potential anomalies

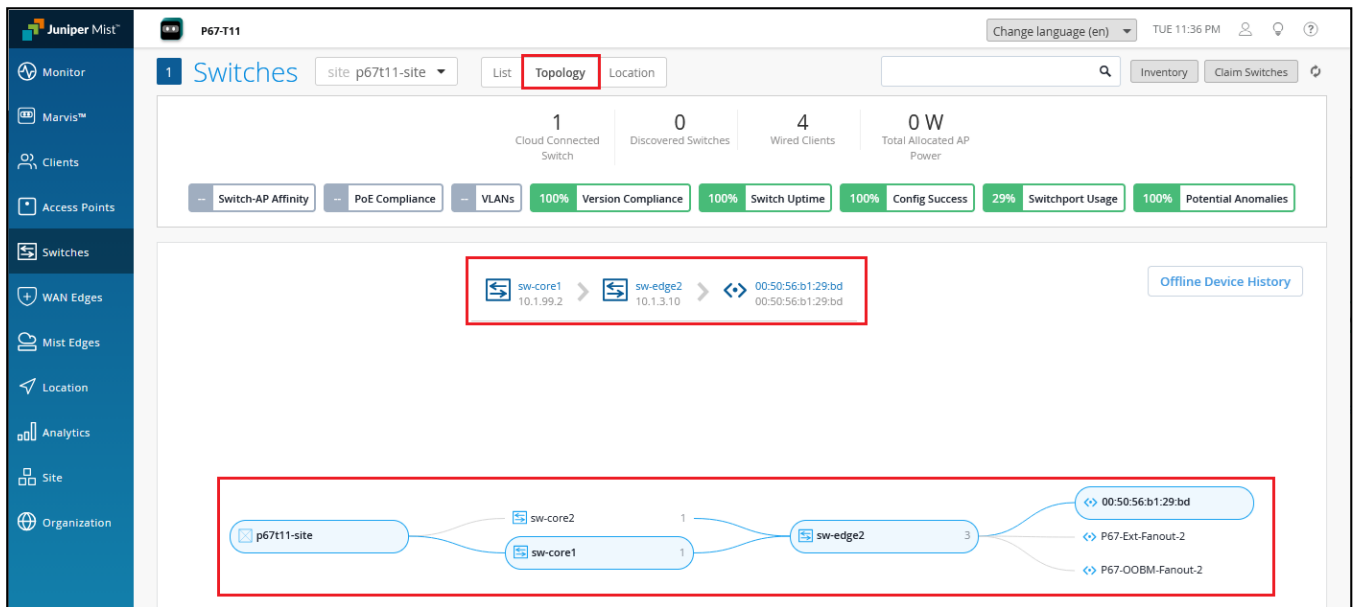
Click the settings icon in the top-right corner. Enable Last Config, version and uptime columns. Drag and drop Insights to the last place. Then click close.



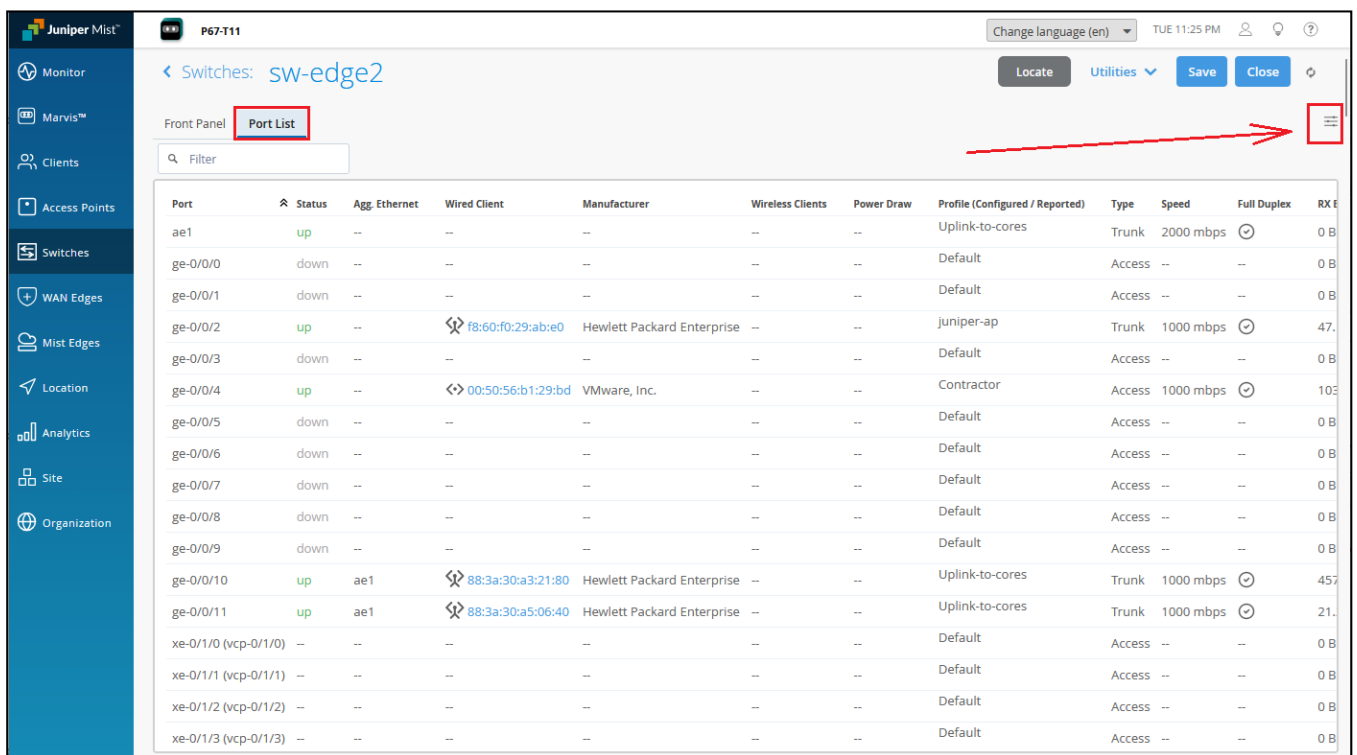
Switches page now display versions, uptime and Last Config columns.



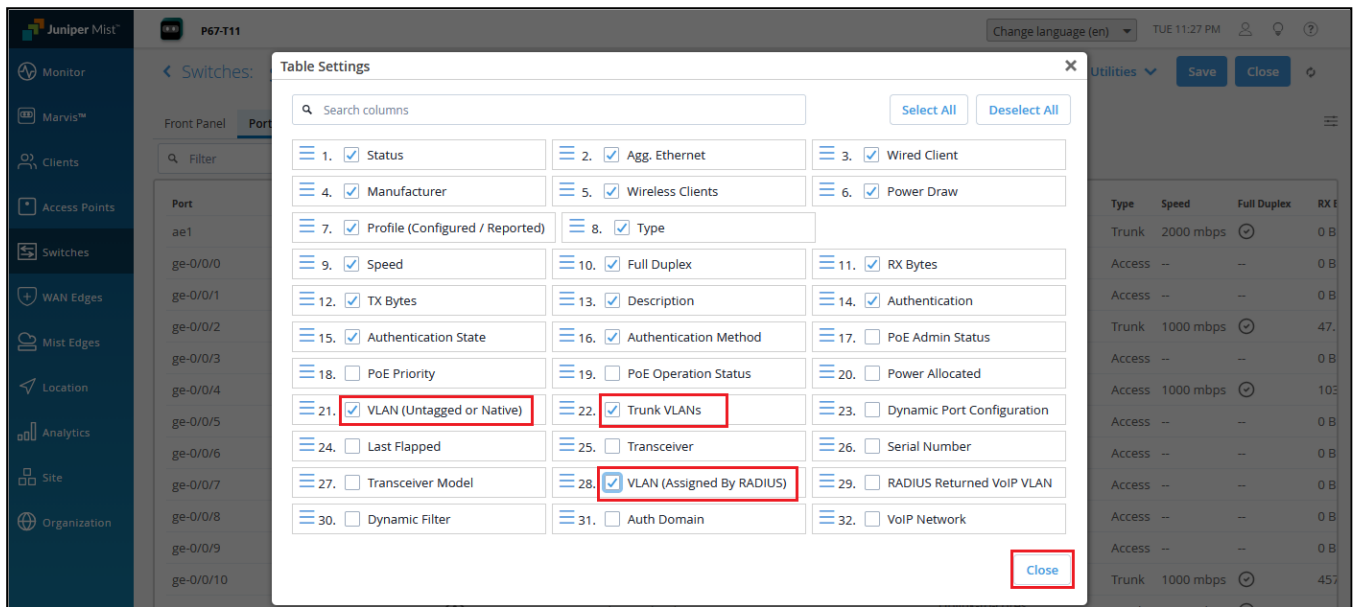
Click on the topology view and then click on each device in the topology to reveal the entire path.



Click on your table switch name **sw-edge2** at the top of the page (or switch back to the List view and click on your switch name) and switch to Port List view. Click on settings icon at the top-right corner.



Enable VLAN (Untagged or Native), Trunk VLANs and VLAN (Assigned by RADIUS) columns. Click Close.

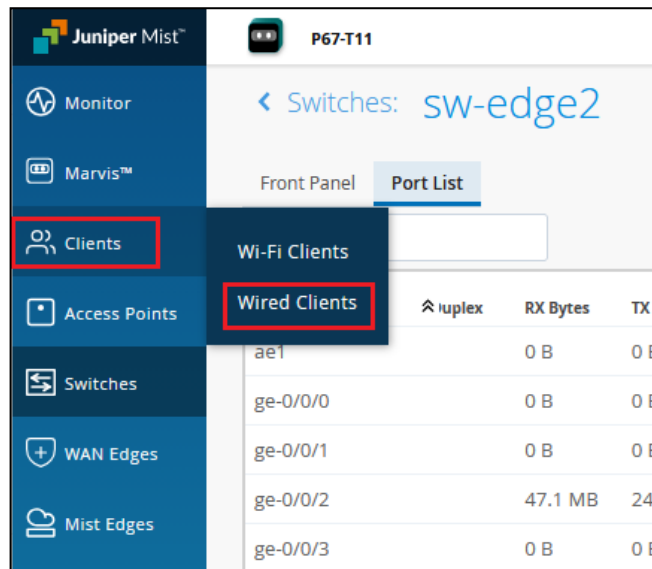


Scroll the page to the right and observe details about VLANs on interface ge-0/0/2, ge-0/0/4 and uplinks ge-0/0/10 and ge-0/0/11.

The screenshot shows the 'Port List' table for switch sw-edge2. The table has the following columns: Port, Duplex, RX Bytes, TX Bytes, Description, Authentication, Authentication State, Authentication Method, VLAN (Untagged or Native), Trunk VLANs, and VLAN (Assigned By RADIUS). The following rows are highlighted with red boxes:

Port	Duplex	RX Bytes	TX Bytes	Description	Authentication	Authentication State	Authentication Method	VLAN (Untagged or Native)	Trunk VLANs	VLAN (Assigned By RADIUS)
ge-0/0/2	47.1 MB	24.3 MB	--	--	--	--	--	3	11, 12, 13, 14	--
ge-0/0/4	103.6 MB	351.9 MB	--	Dot1x	Authenticated	Dot1x	12	--	12	--
ge-0/0/10	457.6 MB	163.6 MB	--	--	--	--	1	11, 12, 13, 14, 3	--	--
ge-0/0/11	21.2 MB	51.2 MB	--	--	--	--	1	11, 12, 13, 14, 3	--	--

Navigate in Mist AI to Clients > Wired Clients.

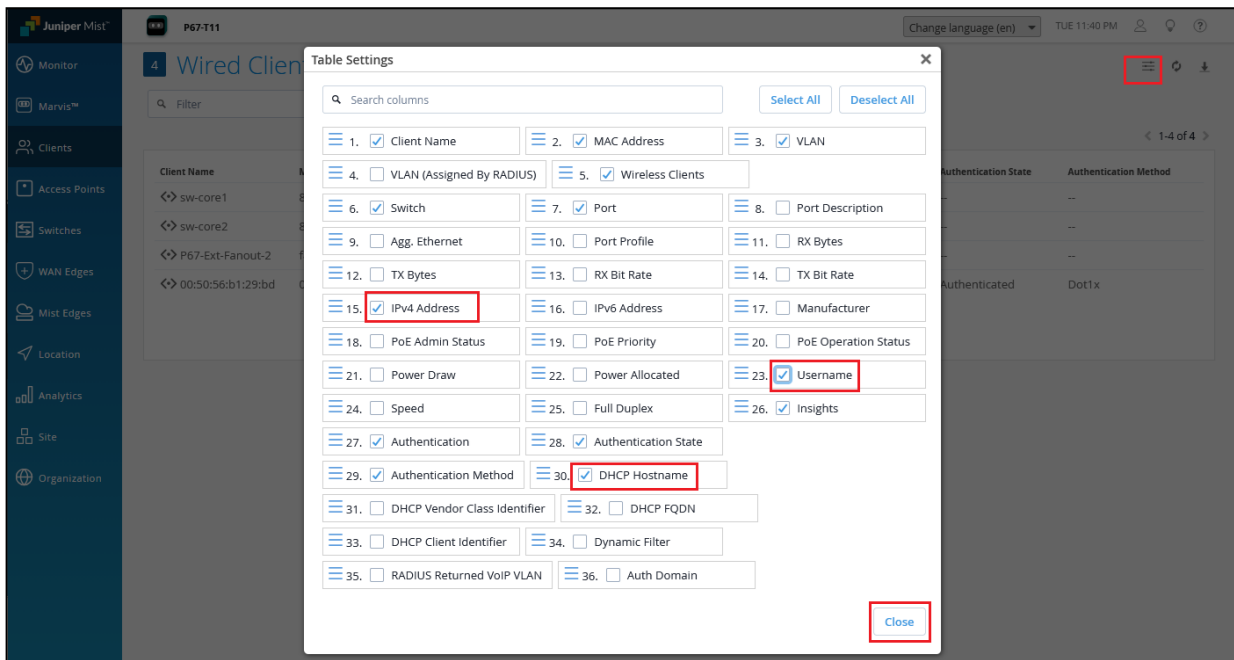


Review the page with Wired Clients. You should have two core switches listed, fanout switch listed and PC4's MAC address on port ge-0/0/4.

The screenshot shows the 'Wired Clients' page in the Juniper Mist interface. The page title is '4 Wired Clients' with a filter dropdown set to 'site p67t11-site'. A search filter box is present. The table below lists the wired clients, with the entire table highlighted by a red border.

Client Name	MAC Address	VLAN	Wireless Clients	Switch	Port	Insights	Authentication	Authentication State	Authentication Method
<> sw-core1	88:3a:30:a3:21:80	1	--	sw-edge2	ge-0/0/10	Wired Client Insights	--	--	--
<> sw-core2	88:3a:30:a5:06:40	1	--	sw-edge2	ge-0/0/11	Wired Client Insights	--	--	--
<> P67-Ext-Fanout-2	f8:60:f0:29:ab:e0	311	--	sw-edge2	ge-0/0/2	Wired Client Insights	--	--	--
<> 00:50:56:b1:29:bd	00:50:56:b1:29:bd	12	--	sw-edge2	ge-0/0/4	Wired Client Insights	Dot1x	Authenticated	Dot1x

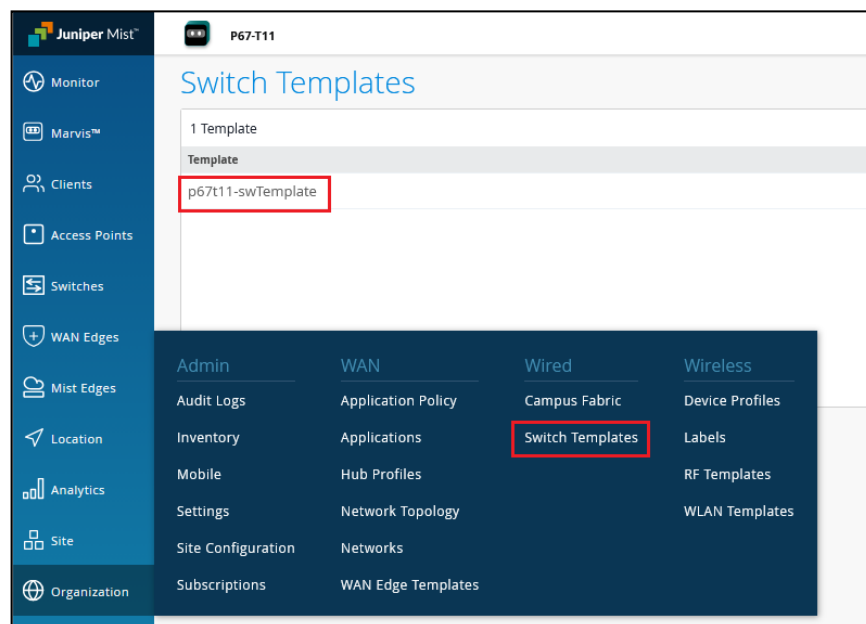
Click on Table settings icon at the top-right corner. Enable "IPv4 Address", "Username", "DHCP Hostname" and click Close.



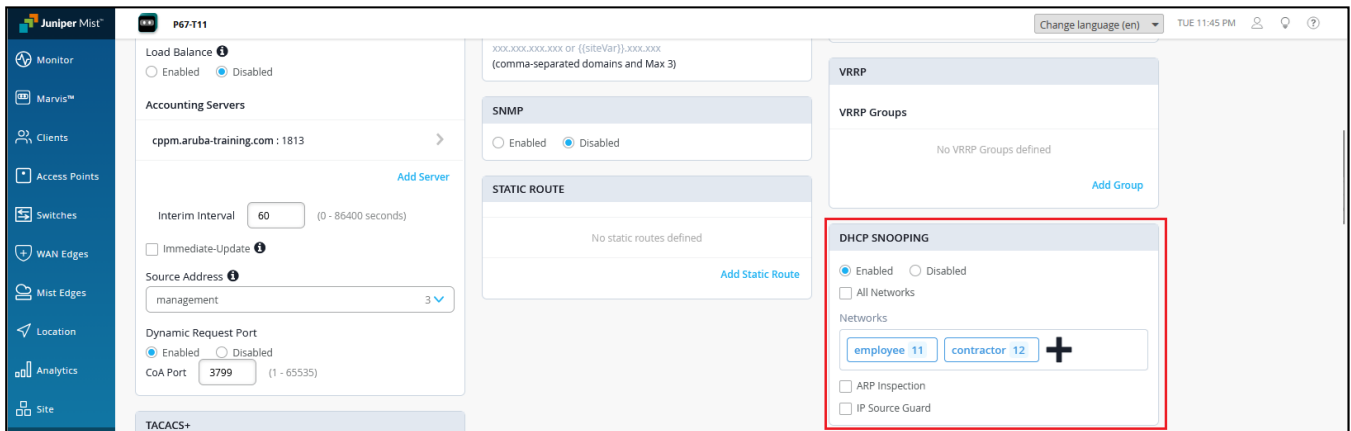
Review new columns, then hover your mouse over “IPv4 Address” and read the text.

Client Name	MAC Address	VLAN	Wireless Clients	Switch	Port	IPv4 Address	Username	Insights	Authentication	Authentication State	Authentication Method	DHCP Hostname
P67-Ext-Fanout-2	f8:60:f0:29:ab:e0	311	--	sw-				ights	--	--	--	--
sw-core1	88:3a:30:a3:21:80	1	--	sw-				ights	--	--	--	--
sw-core2	88:3a:30:a5:06:40	1	--	sw-edge2	ge-0/0/11	10.1.3.3	--	Wired Client Insights	--	--	--	--
00:50:56:b1:29:bd	00:50:56:b1:29:bd	12	--	sw-edge2	ge-0/0/4	--	contractor	Wired Client Insights	Dot1x	Authenticated	Dot1x	--

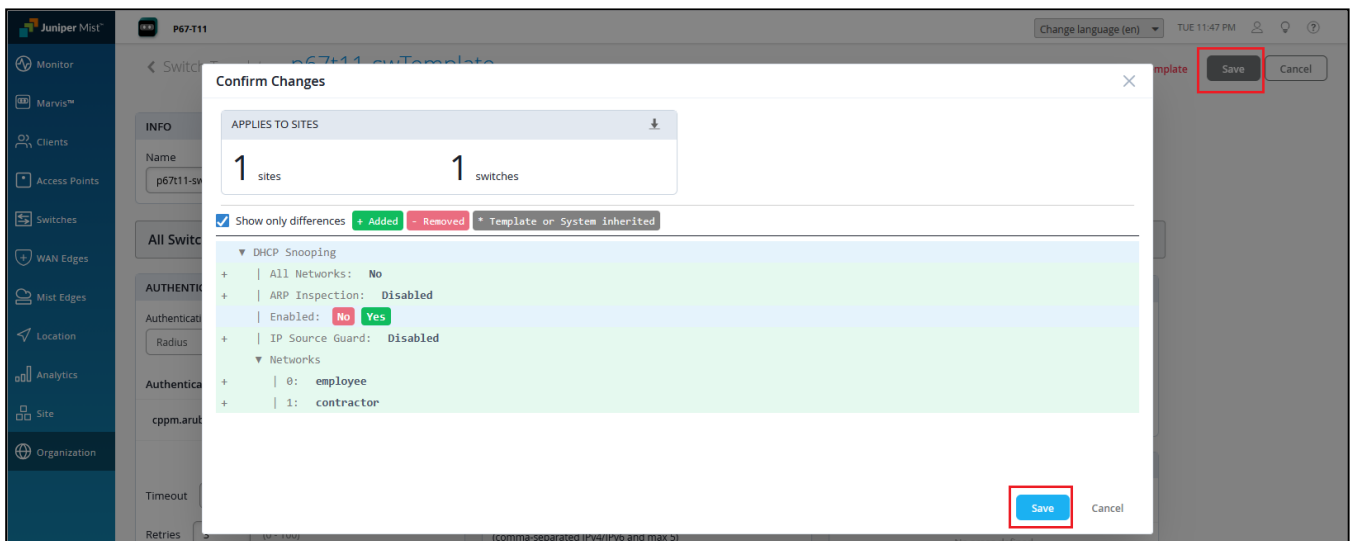
Navigate to Organization > Wired > Switch Templates and select your template.



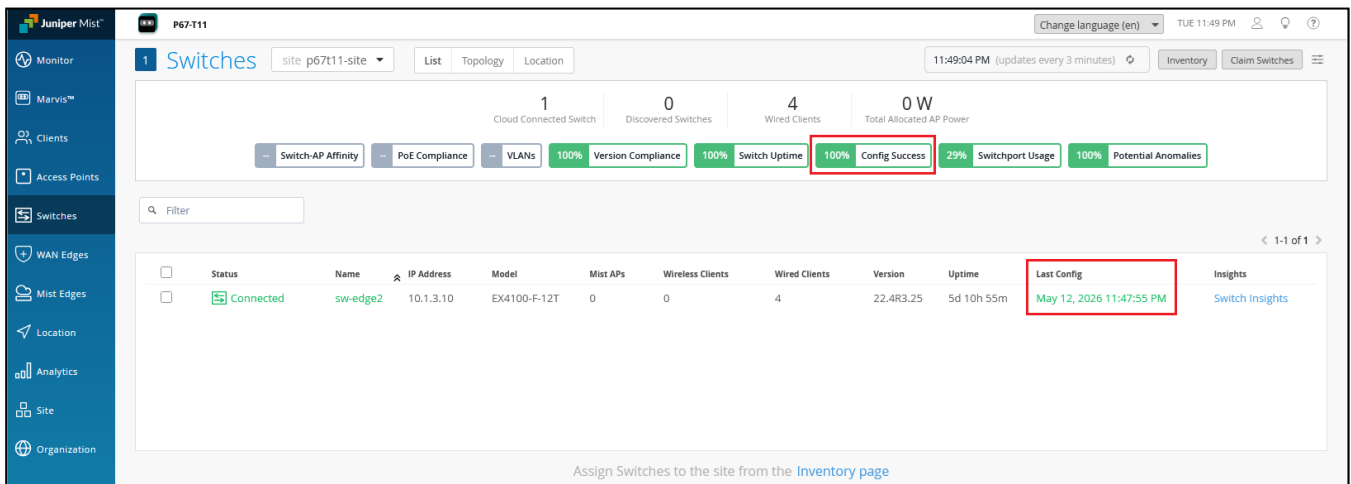
Scroll the page down to DHCP Snooping settings. Enable DHCP Snooping and add employee and contractor networks.



Scroll the page up, click Save to apply new settings and Save again to confirm changes.

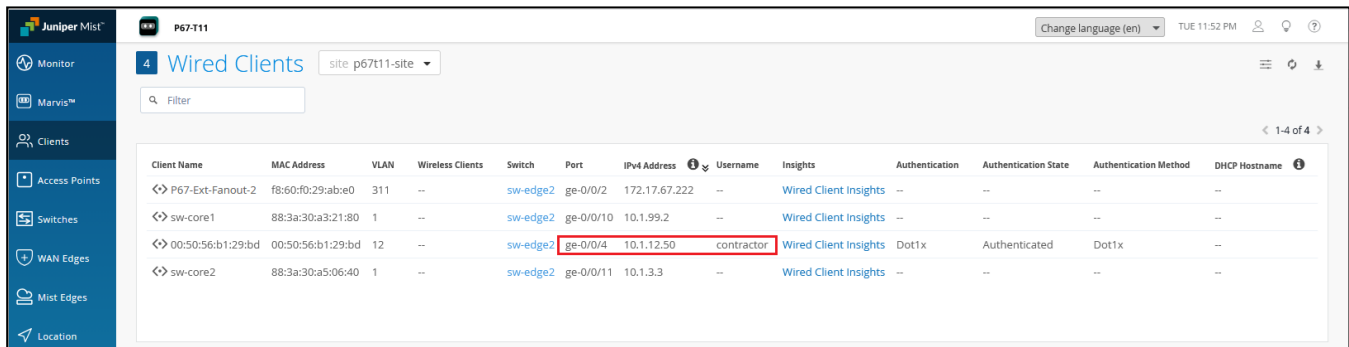


Navigate to Mist AI Switches page and wait several minutes until new configuration is synchronized and refresh the page. You should see 100% Config Success.



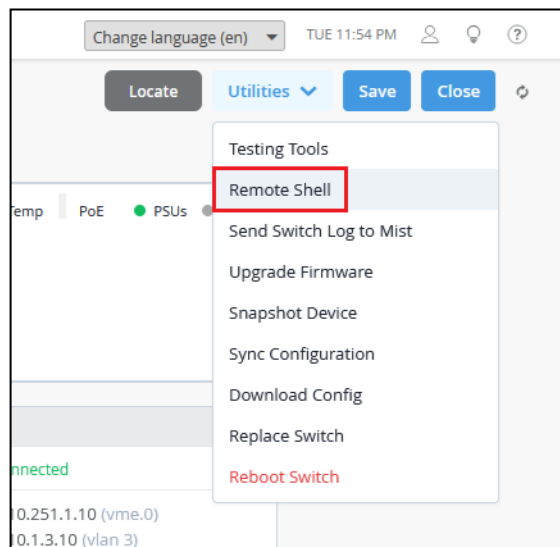
Connect to PC4 Remote Desktop and bounce Lab NiC (right-mouse click disable/enable).

Navigate to Mist AI Clients > Wired Clients page. Wait a couple of minutes and refresh the page. PC4 IP address must be displayed now.



Client Name	MAC Address	VLAN	Wireless Clients	Switch	Port	IPv4 Address	Username	Insights	Authentication	Authentication State	Authentication Method	DHCP Hostname
P67-Ext-Fanout-2	f8:60:f0:29:ab:e0	311	--	sw-edge2	ge-0/0/2	172.17.67.222	--	Wired Client Insights	--	--	--	--
sw-core1	88:3a:30:a3:21:80	1	--	sw-edge2	ge-0/0/10	10.1.99.2	--	Wired Client Insights	--	--	--	--
00:50:56:b1:29:bd	00:50:56:b1:29:bd	12	--	sw-edge2	ge-0/0/4	10.1.12.50	contractor	Wired Client Insights	Dot1x	Authenticated	Dot1x	--
sw-core2	88:3a:30:a5:06:40	1	--	sw-edge2	ge-0/0/11	10.1.3.3	--	Wired Client Insights	--	--	--	--

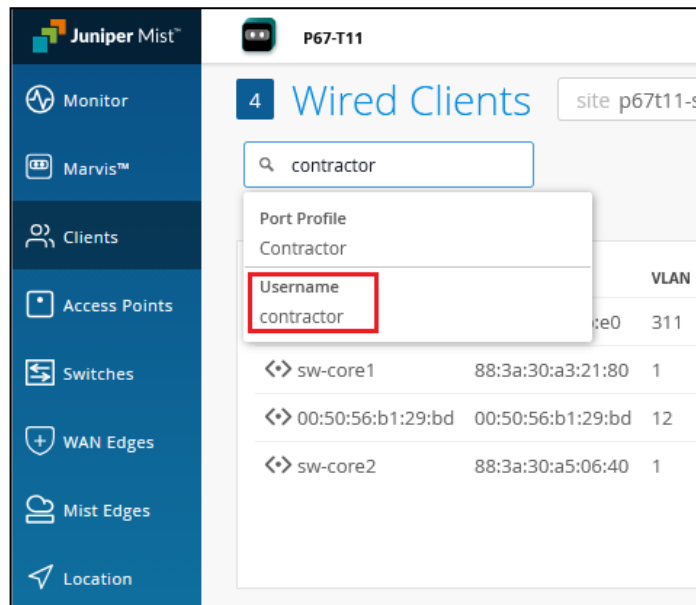
Click on sw-edge2 > Utilities > Remote Shell.



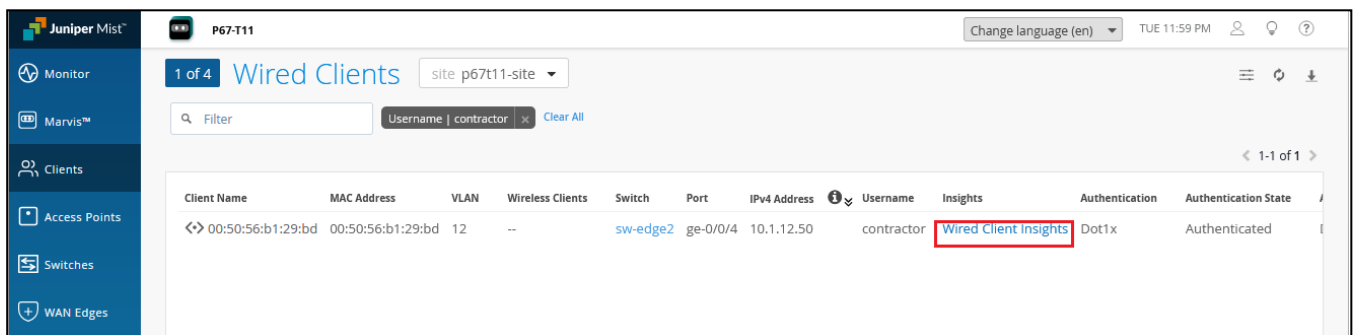
Type CLI command “show dhcp-security binding”. Review the output and close Remote Shell.

```
mist@sw-edge2> show dhcp-security binding
IP address      MAC address      Vlan    Expires State  Interface
10.1.12.50      00:50:56:b1:29:bd  contractor 690911 BOUND  ge-0/0/4.0
{master:0}
```

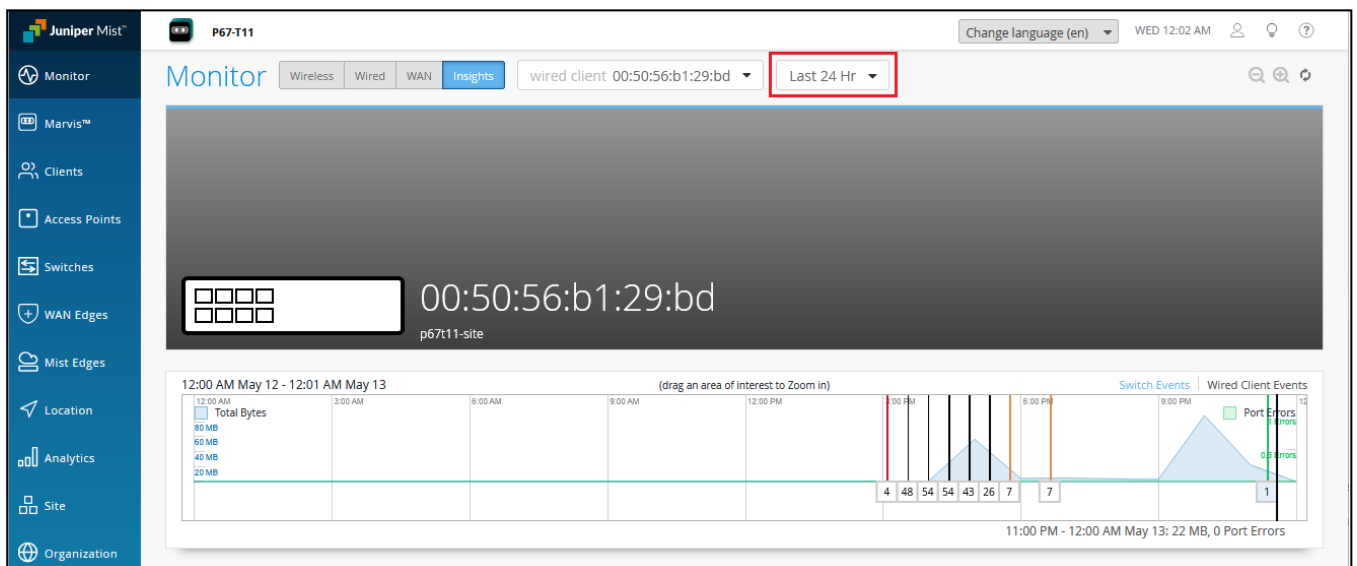
Navigate to Clients > Wired Clients and type “contractor” in a search field. Click on Username contractor. This will filter Wired Clients and display only contractor user.



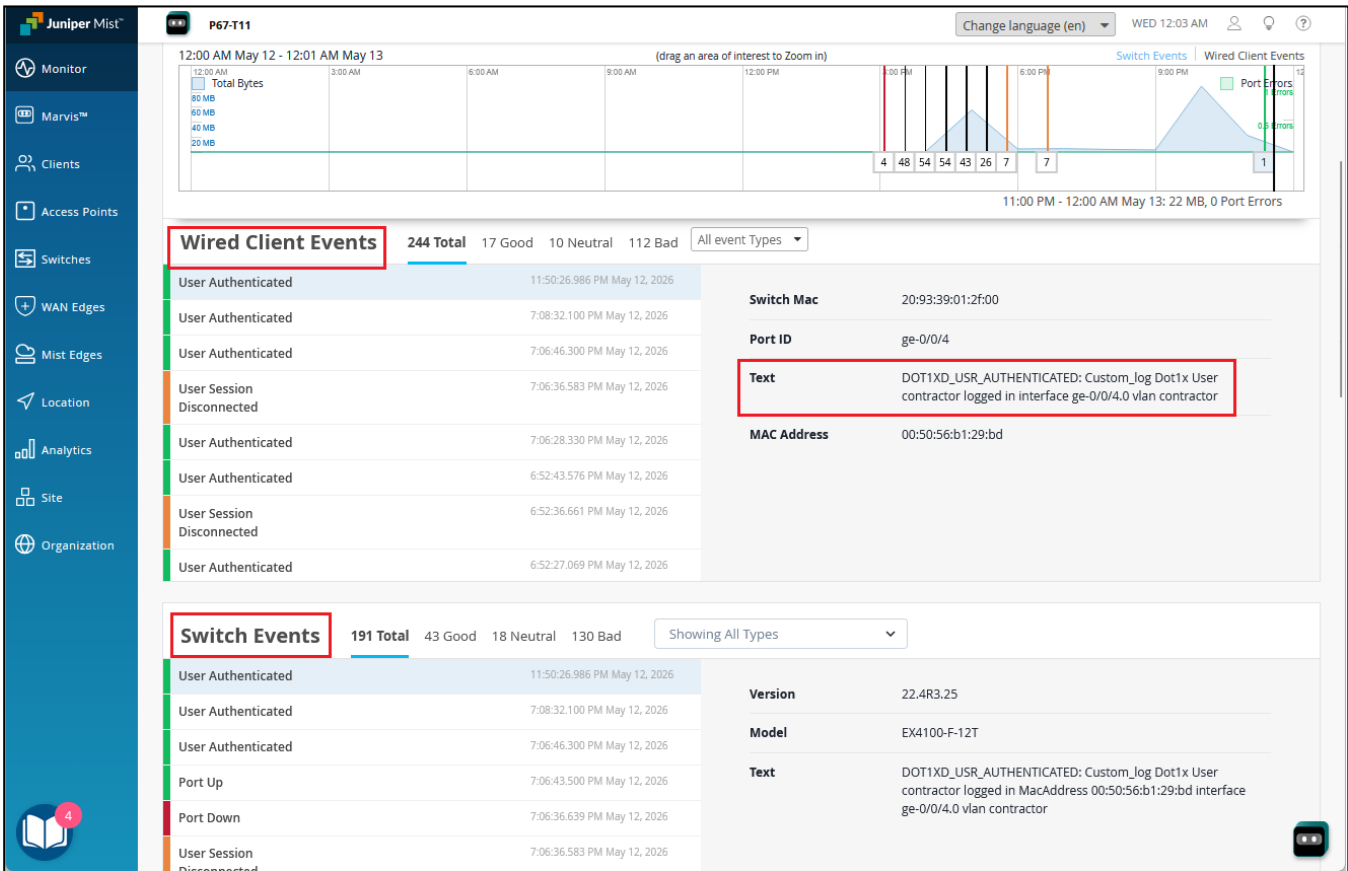
Click on Wired Client Insights.



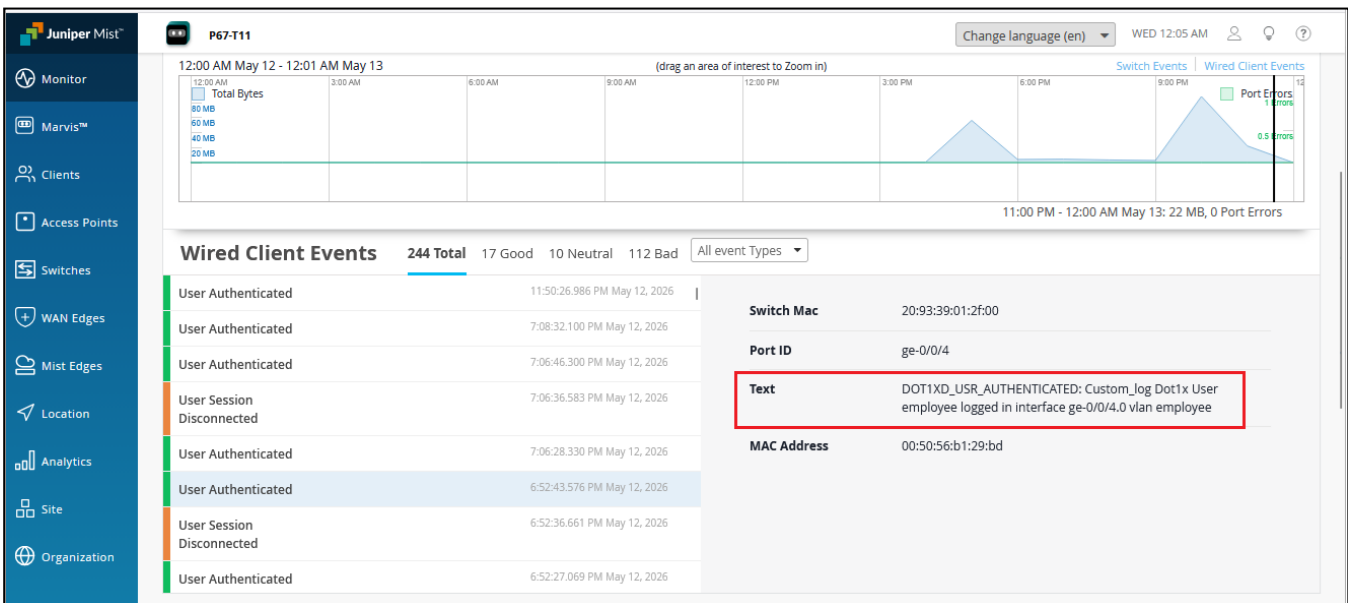
On Wired Client Insights page select Last 24 Hr filter at the top of the page.



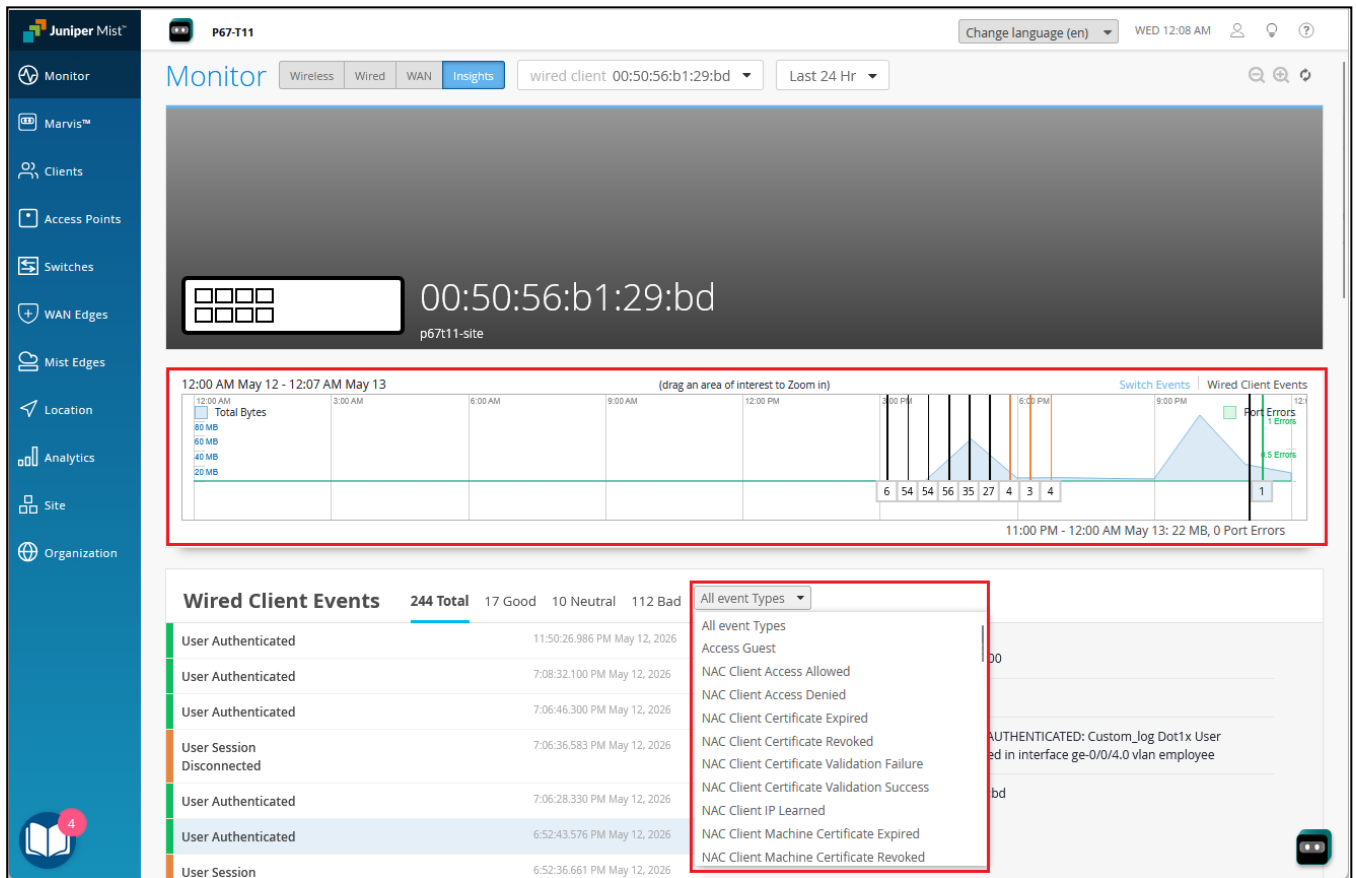
Scroll the page down to review Wired Client Events and Switch Events where this client is connected.
Find Event where contractor user was authenticated with DOT1X in interface ge-0/0/4.0 vlan contractor.



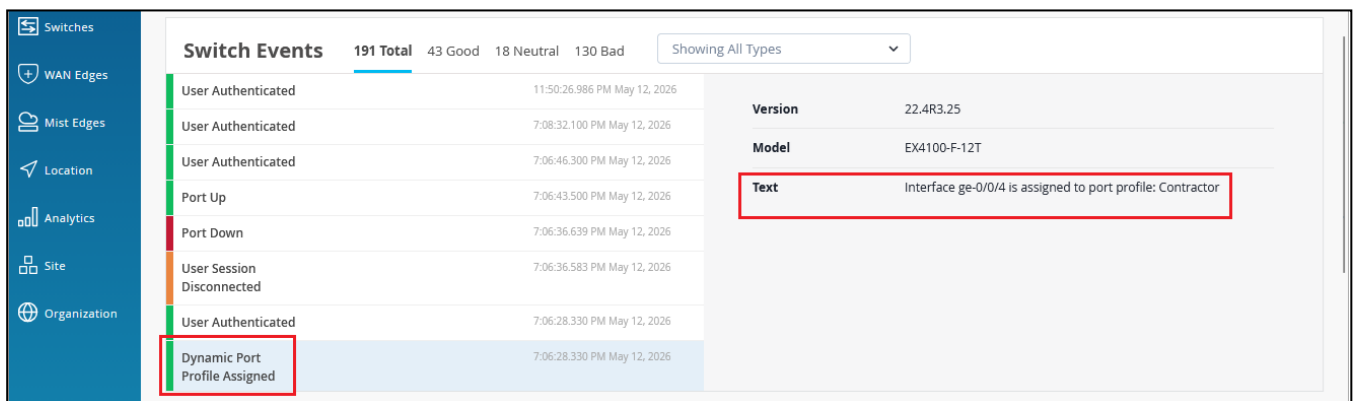
Find Wired Client Event where employee user was authenticated with DOT1X in interface ge-0/0/4.0 vlan employee.



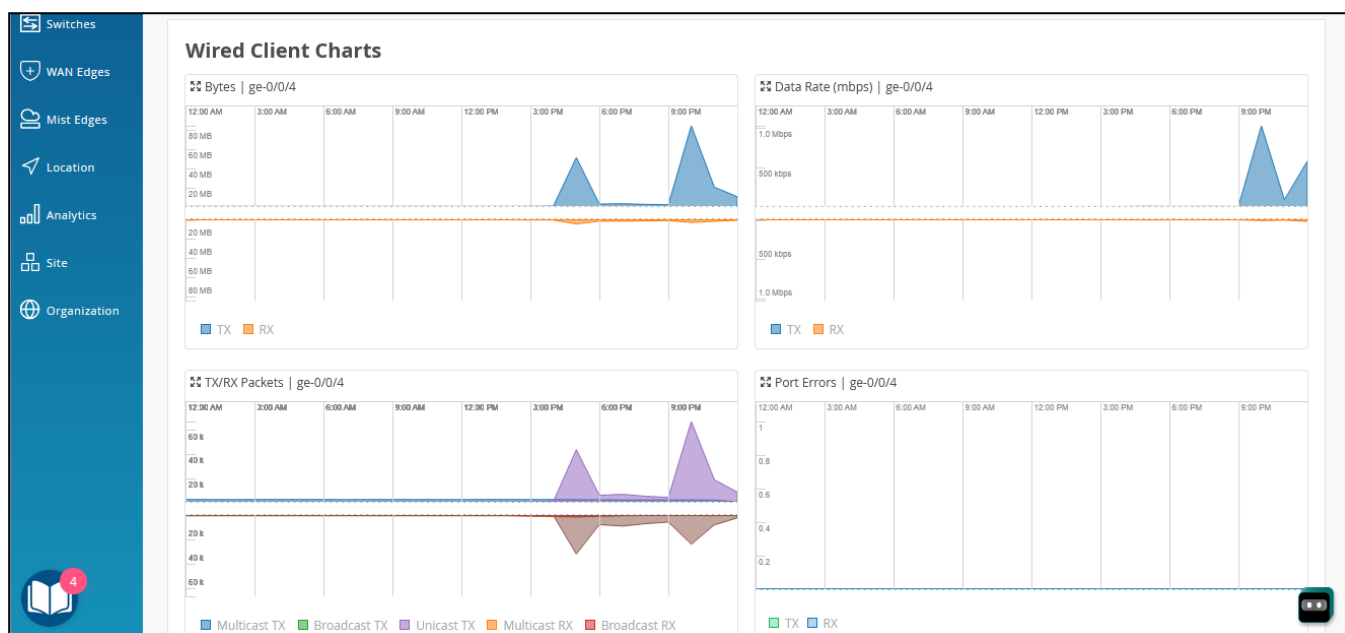
You can filter events based on event type or drag an area of interest to Zoom in. To Zoom out, scroll the page up to the top and select Last 24 Hr or other option.



Review Switch Event below with Dynamic Port Profile Assignment.



Scroll down the page to see your Wired Client Charts with Bytes TX/RX, Data Rate (mbps), TX/RX packets, Port Errors and Power Draw.



Task 4-2: Monitor with Service Levels

Objectives

Use Service Levels to troubleshoot DHCP issues.

Use Service Levels to troubleshoot 802.1X issues.

User Mist Alerts.

Steps

At the beginning of this task PC4 should be connected, authenticated as contractor and has IP from 10.1.12.0/24. Connect to PC4 Remote Desktop to confirm this. Run CMD command “ipconfig” and then “ping 10.254.1.21”.

```
C:\Users\student>ipconfig

Windows IP Configuration

Ethernet adapter Do NOT Touch!:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 172.17.67.81
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Lab NIC - 6300-D Port 4:

    Connection-specific DNS Suffix  . : aruba-training.com
    IPv4 Address. . . . . : 10.1.12.50
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.1.12.1

<Output omitted>

C:\Users\student>ping 10.254.1.21

Pinging 10.254.1.21 with 32 bytes of data:
Reply from 10.254.1.21: bytes=32 time=2ms TTL=126
Reply from 10.254.1.21: bytes=32 time=2ms TTL=126
Reply from 10.254.1.21: bytes=32 time=2ms TTL=126
Reply from 10.254.1.21: bytes=32 time=2ms TTL=126

Ping statistics for 10.254.1.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\Users\student>
```

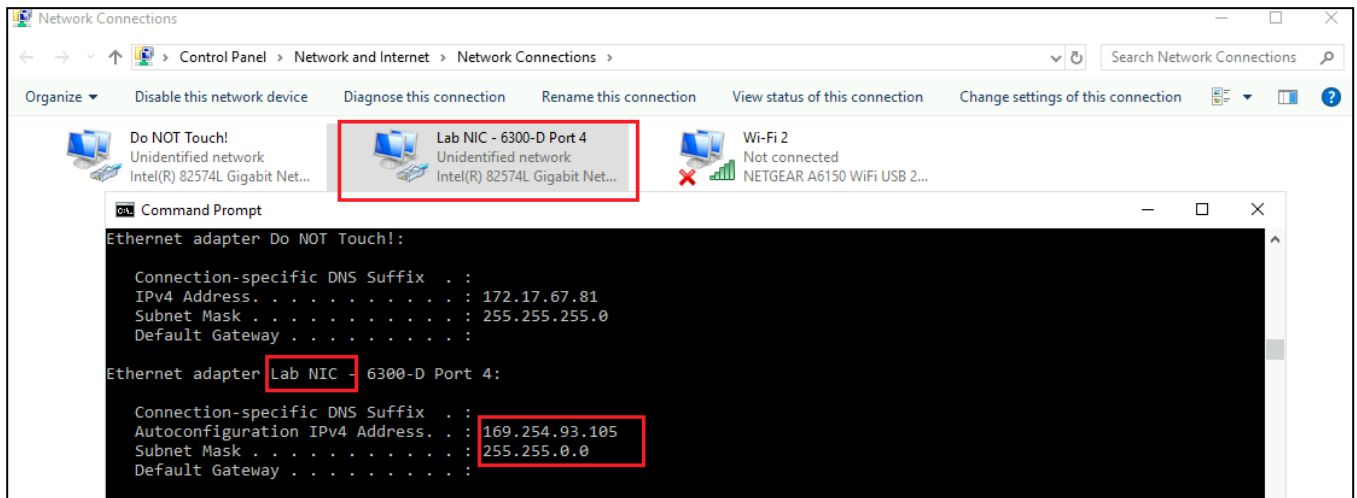
Connect to **MGMT PC** Remote Desktop and open SSH session to Core-1. Remote DHCP relay settings from SVI 12.

```

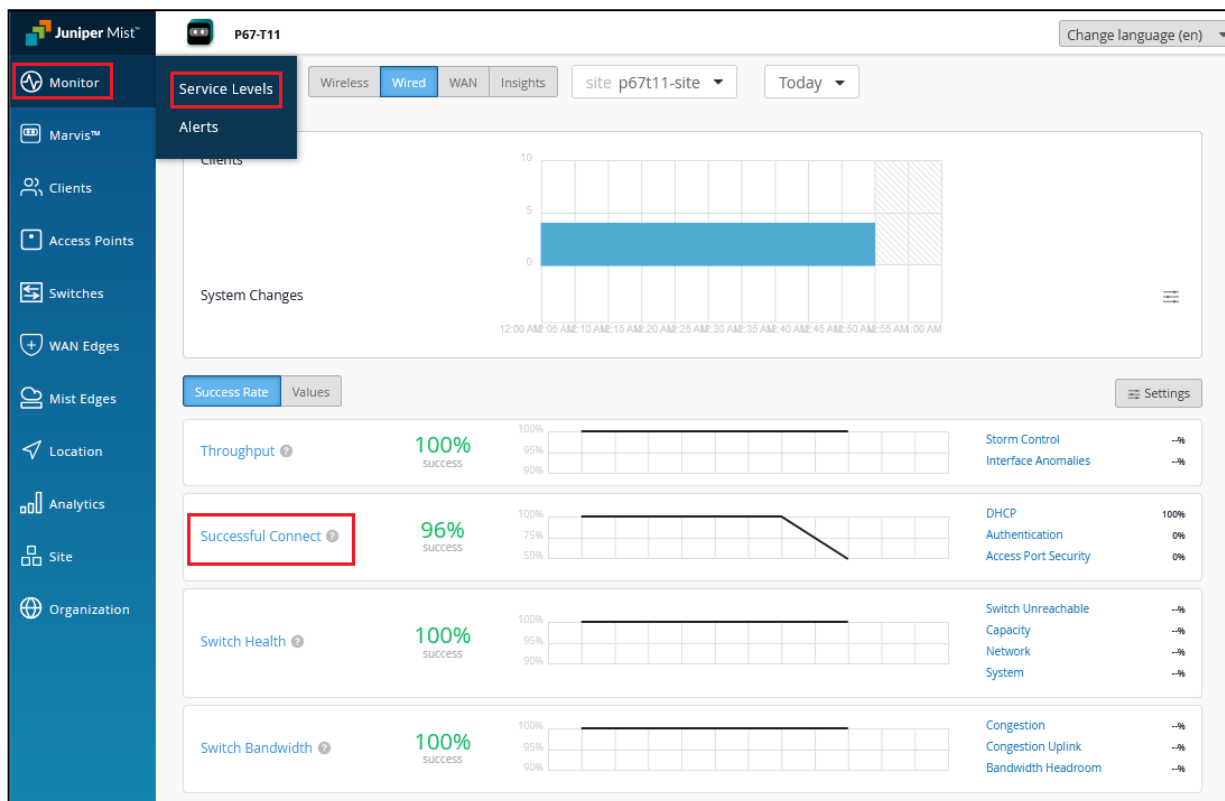
sw-core1# configure terminal
sw-core1(config)# interface vlan 12
sw-core1(config-if-vlan)# no ip helper-address 10.254.1.21
sw-core1(config-if-vlan)# show running-config current-context
interface vlan 12
ip address 10.1.12.2/24
active-gateway ip mac 02:00:00:01:00:00
active-gateway ip 10.1.12.1

```

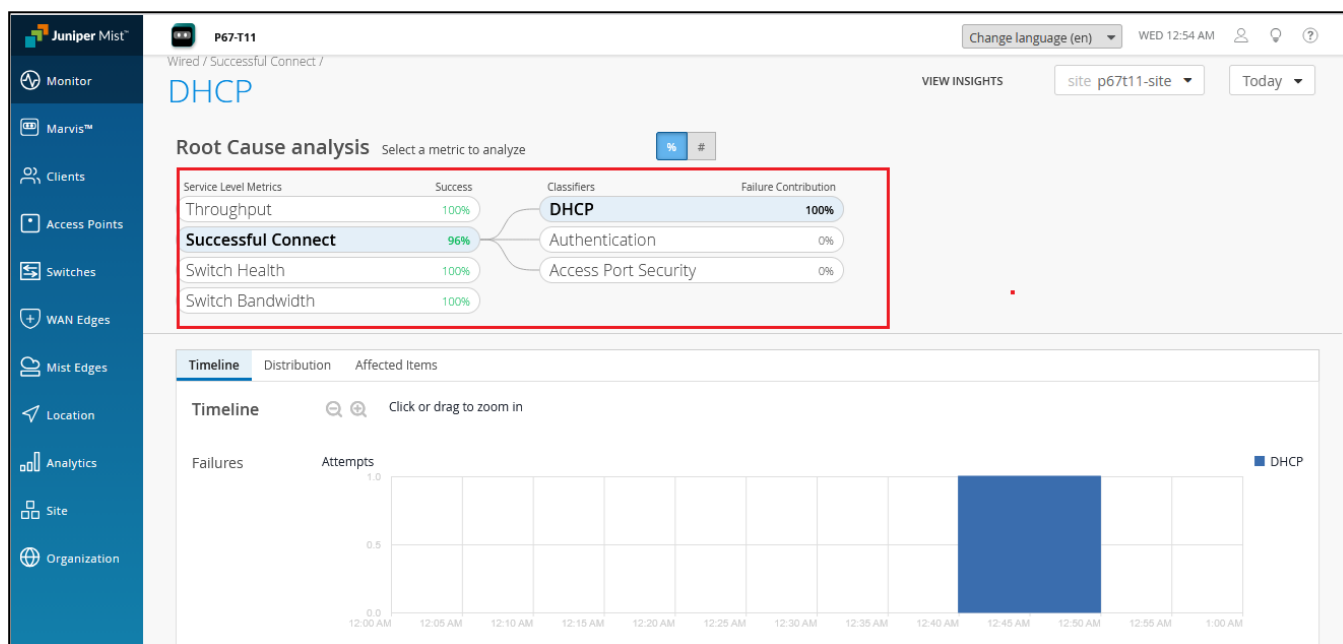
Connect to **PC4** Remote Desktop and bounce Lab NIC. It will fail to receive IP address from DHCP server. This could take 20 minutes to be detected on Mist AI side.



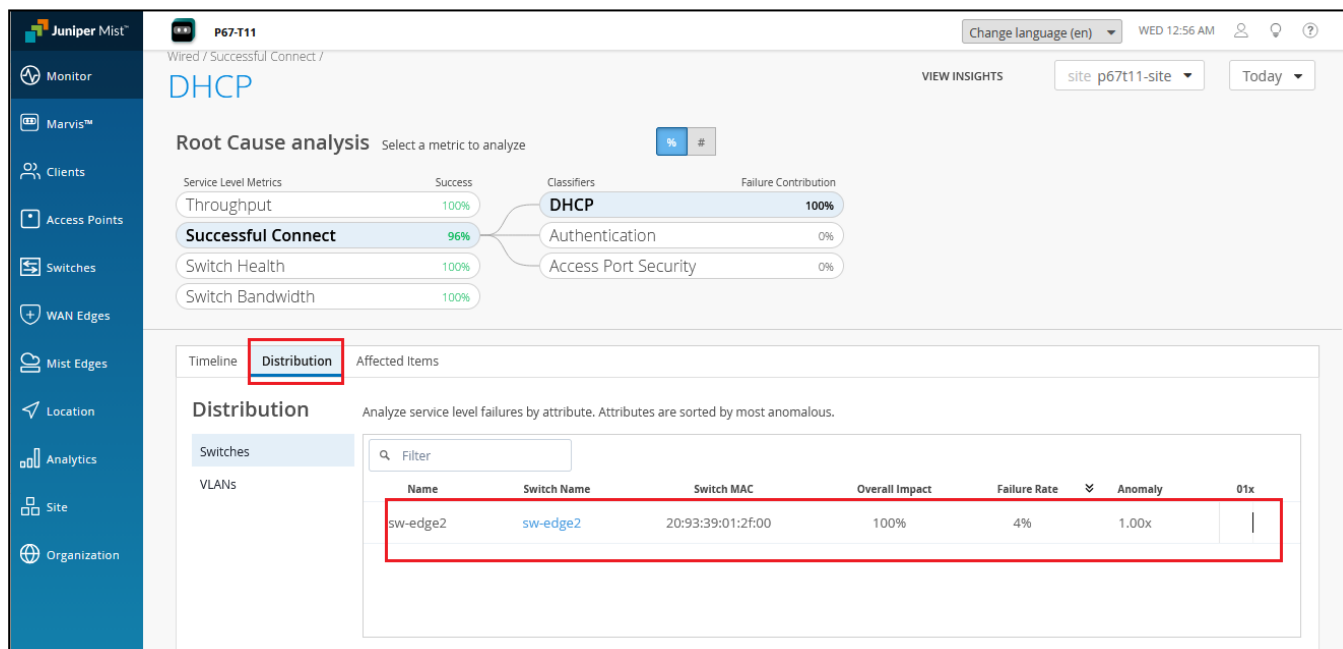
Navigate to Mist AI Monitor > Service Levels and click Successful Connect.



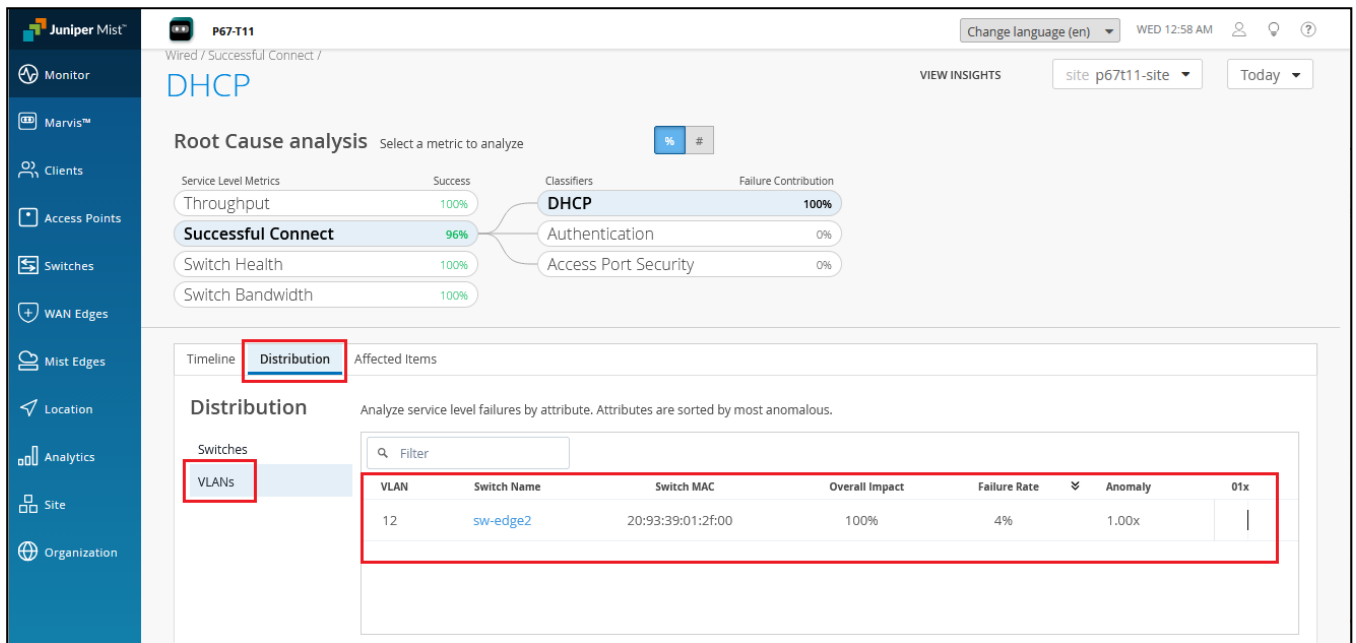
You should see DHCP 100% failure contribution.



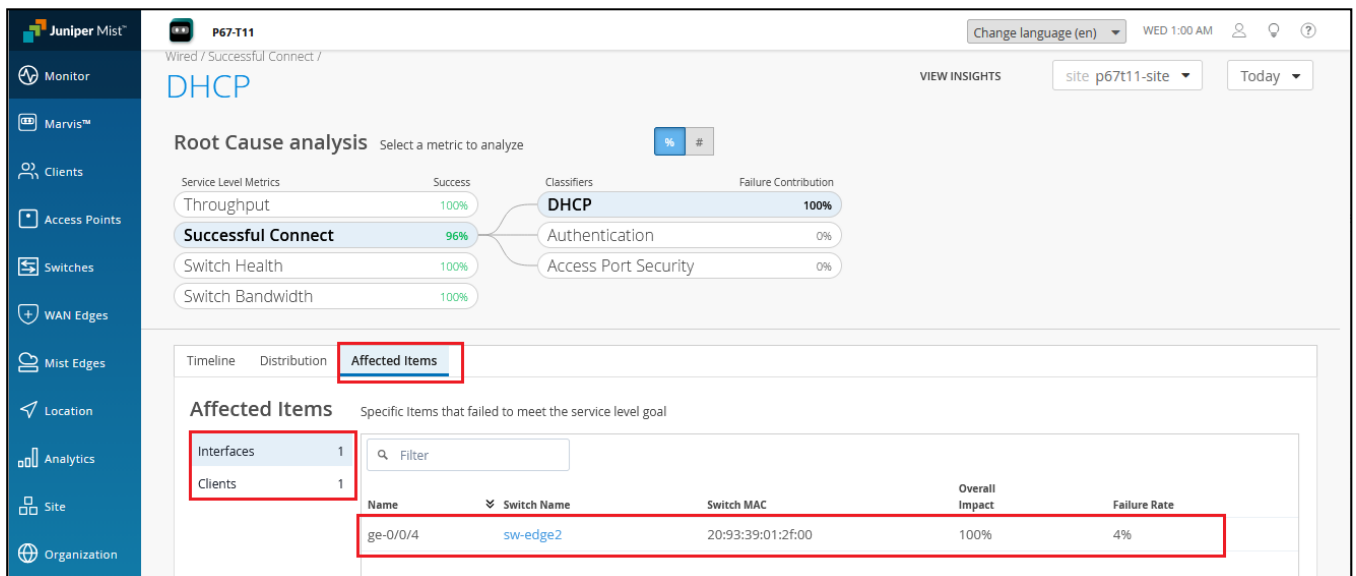
Switch to Distribution tab to analyze impact. As you can see from the output anomaly repeated with a single client connected to sw-edge2.



Switch to VLANs to see more details about impact. This output reveals that VLAN 12 is affected by a single client.



Click Affected items to check more details about interfaces where failed clients are connected.



Return to MGTP PC Remote Desktop and fix the issue with DHCP on sw-core1.

```
sw-core1# configure terminal
sw-core1(config)# interface vlan 12
sw-core1(config-if-vlan)# ip helper-address 10.254.1.21
sw-core1(config-if-vlan)# end
sw-core1# show running-config interface vlan 12
interface vlan 12
  ip address 10.1.12.2/24
  active-gateway ip mac 02:00:00:01:00:00
  active-gateway ip 10.1.12.1
  ip helper-address 10.254.1.21
exit
sw-core1#
```

Connect to PC4 Remote Desktop and bounce Lab NIC. It should receive IP address now. You can double-check it with “ipconfig” CMD command.

```
C:\Users\student>ipconfig
```

Windows IP Configuration

Ethernet adapter Do NOT Touch!:

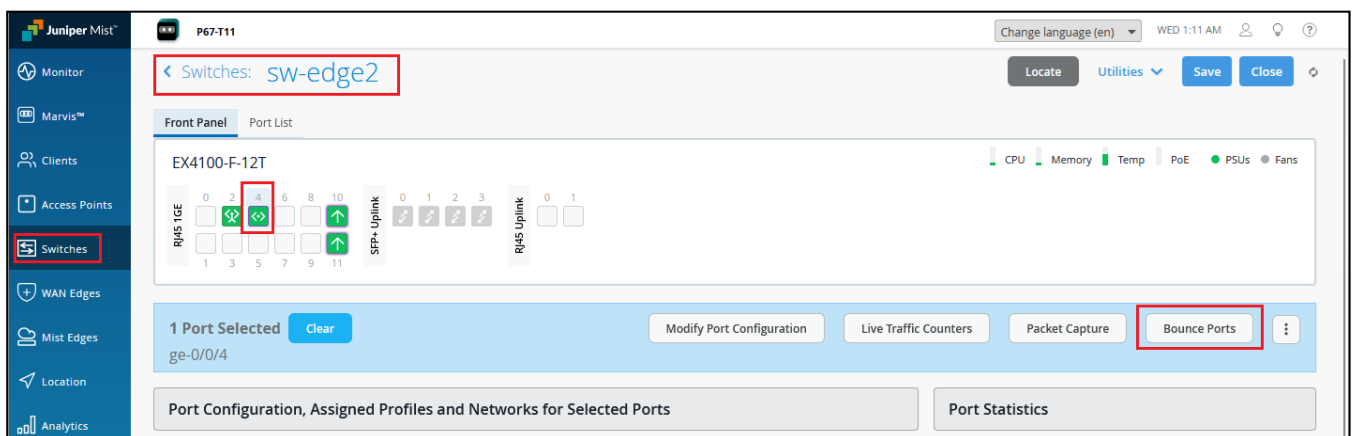
```
Connection-specific DNS Suffix  . :  
IPv4 Address. . . . . : 172.17.67.81  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :
```

Ethernet adapter Lab NIC - 6300-D Port 4:

```
Connection-specific DNS Suffix  . : aruba-training.com  
IPv4 Address. . . . . : 10.1.12.50  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.1.12.1
```

This time you will simulate an issue with client authentication. On PC4 open Lab NIC properties, then Authentication tab, click Additional Settings and Replace credentials. Enter incorrect credentials “**contractor/aruba123**”. Click OK three times to save new settings.

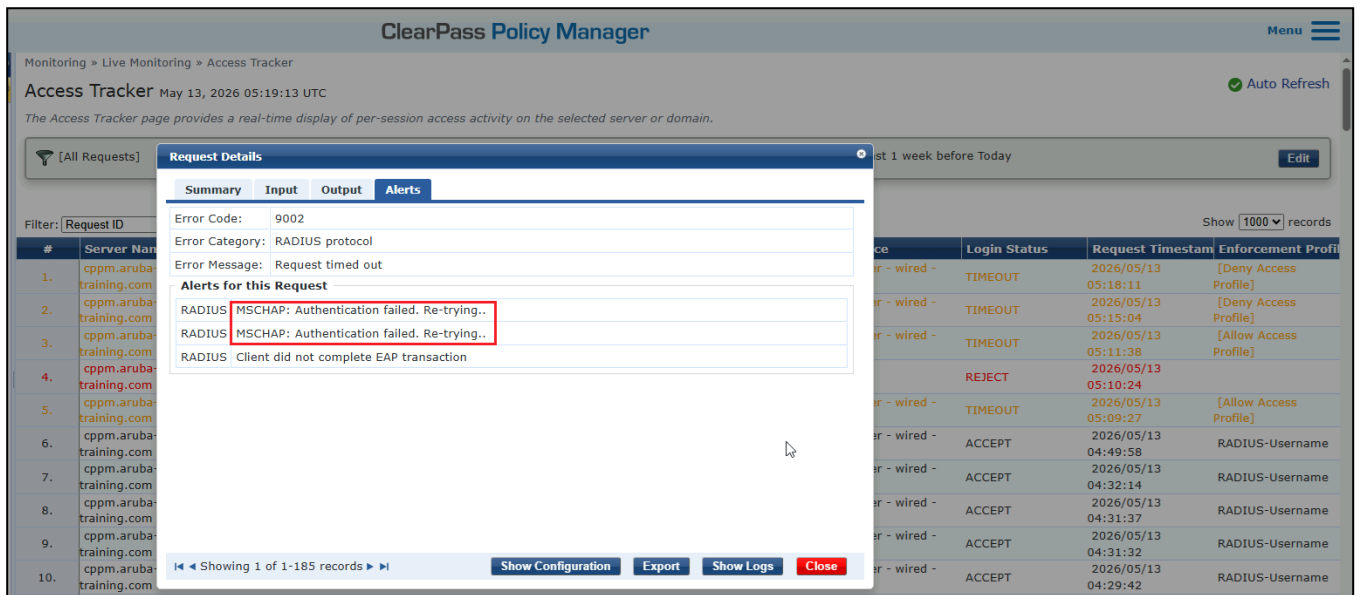
Navigate to Mist AI Switches > sw-edge2, select port 4 and click Bounce Ports.



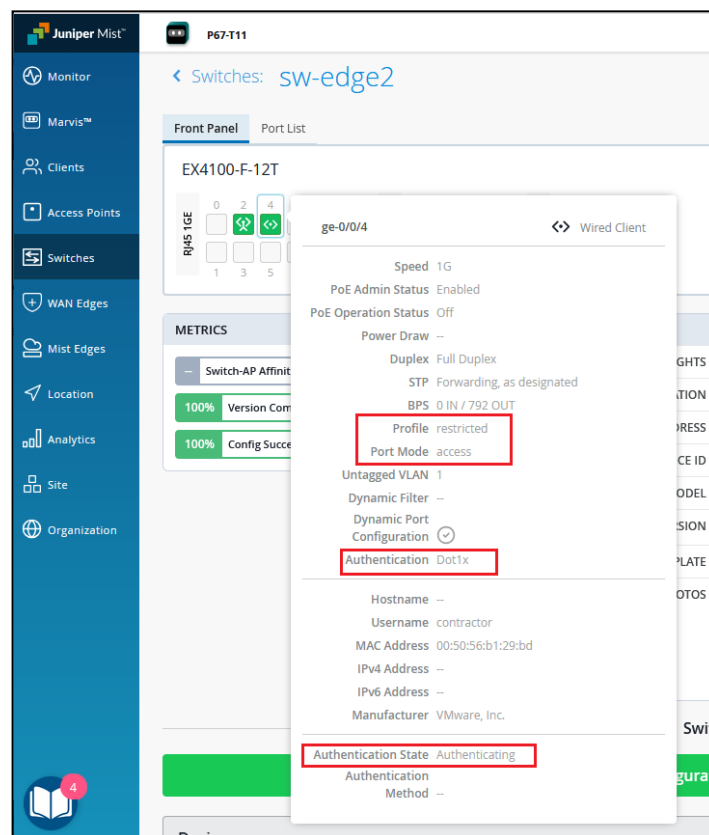
```
Bounce Port ge-0/0/4  
May 13, 2026 1:09:35 AM  
Bouncing port...
```

Port bounce complete.

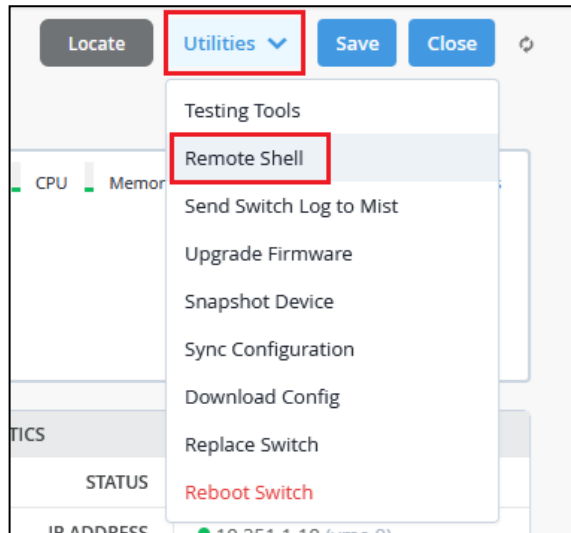
On MGMT PC, navigate to <https://10.254.1.23/tips> and log in with “**admin/Aruba123!**” credentials. Open Access Tracker where you should see multiple timeouts with failed authentication.



Navigate to Mist AI Switches > sw-edge2 and hover your mouse over port 4 in Front Panel. You should see restricted Profile applied.



Click Utilities > Remote Shell and type “show dot1x authentication-failed-users” command and then “show dot1x interface detail”. Review the output and close Remote Shell.

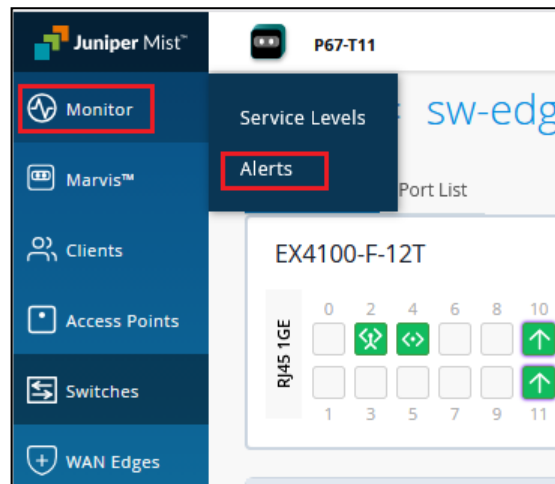


```
mist@sw-edge2> show dot1x authentication-failed-users
Interface      MAC address      User              Failure Count
-----
ge-0/0/4.0     00:50:56:b1:29:bd contractor        5

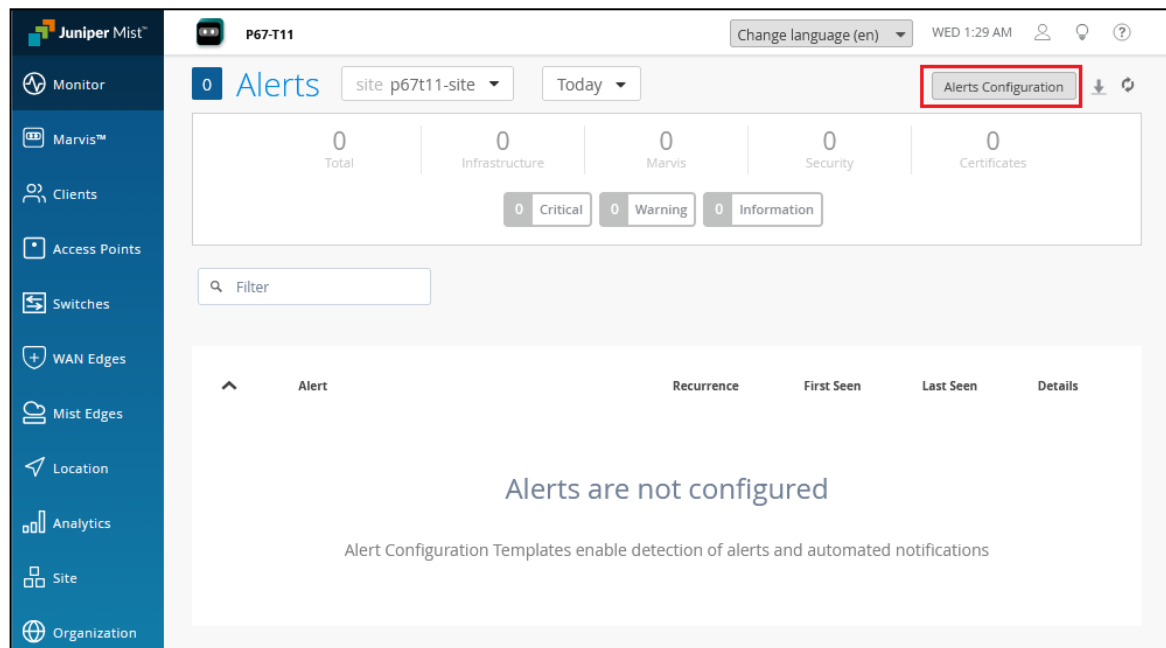
{master:0}
mist@sw-edge2> show dot1x interface detail
ge-0/0/4.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Reauthentication interval: 65000 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: not configured
  Number of connected supplicants: 1
  Supplicant: contractor, 00:50:56:B1:29:BD
  Operational state: Connecting
  Backend Authentication state: Idle
  Authentication method: None
  Session Reauth interval: 65000 seconds
  Reauthentication due in 0 seconds
  Session Accounting Interim Interval: 600 seconds
  Accounting Update due in 0 seconds
  Eapol-Block: Not In Effect
  Domain: Data

{master:0}
mist@sw-edge2>
```

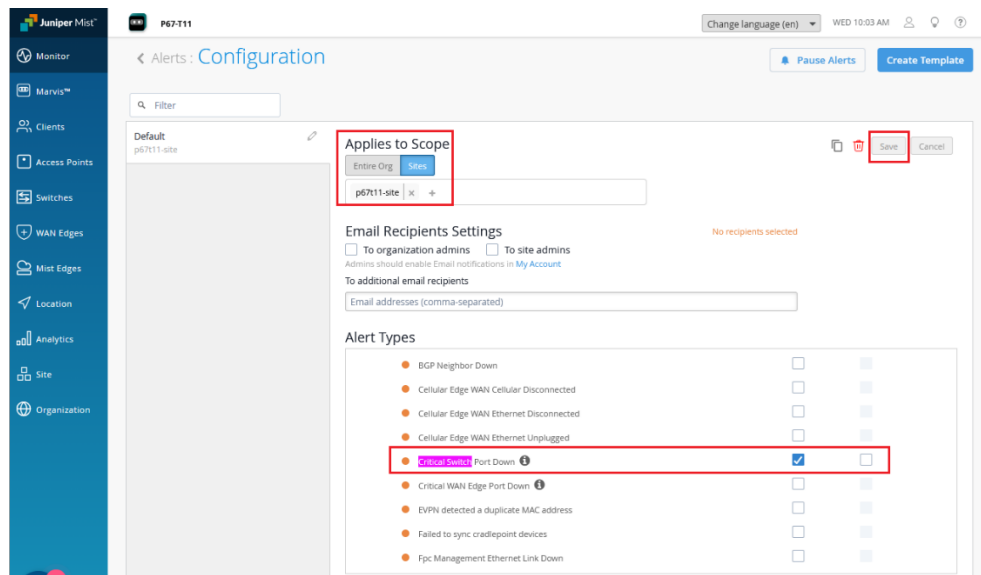
Navigate to Mist AI Monitor > Alerts



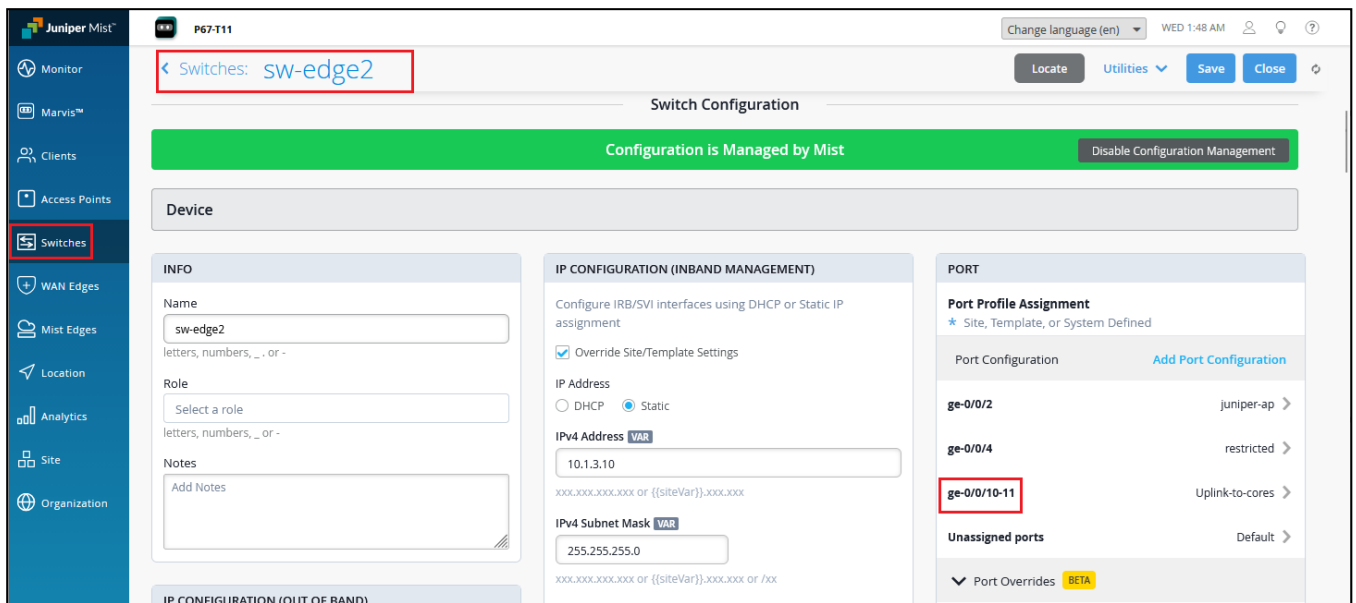
Click Alert Configuration in the top-right corner.



Search with Ctrl+F “Critical Switch Port Down”, enable checkbox, select “Applies to Scope Sites” and add your site, then click Save to apply and confirm changes.



Navigate in Mist AI to Switches > sw-edge2 and scroll down the page till Port Profile Assignment section. Click on ge-0/0/10-11.



Enable UP/Down Port Alerts and click the check mark.

Port Profile Assignment
 * Site, Template, or System Defined

Edit Port Configuration [Save] [Close]

Port IDs
 ge-0/0/10-11
 (ge-0/0/1, ge-0/0/4, ge-0/1/1-23, etc)

Interface
☒ L2 interface ☐ L3 interface ☐ L3 sub-interfaces

Configuration Profile
 Uplink-to-cores default(1), trunk

☐ Enable Dynamic Port Configuration

Description
 Add Description

Up / Down Port Alerts ⓘ
☒ Enabled ☐ Disabled
[Manage Alert Types in Alerts Page](#)

Port Aggregation
☒ Enabled ☐ Disabled

LACP
☒ Enabled ☐ Disabled

Then click Save at the top of the page to apply new settings and click Save again to confirm changes.

Juniper Mist P67-T11

Change language (en) WED 1:51 AM

[Save] [Close]

Confirm Changes

☒ Show only differences + Added - Removed * Template or System inherited

▼ Port Config

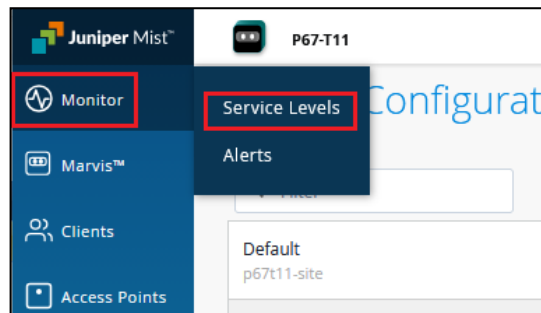
▼ ge-0/0/10-11

| Port Range: ge-0/0/10-11

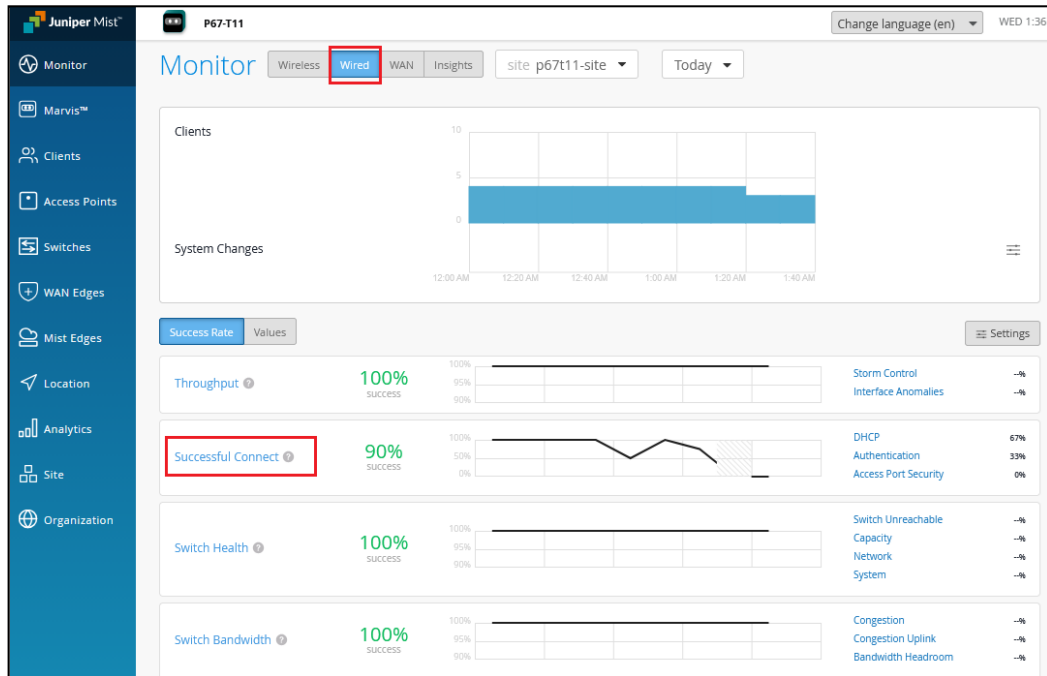
| Enable Up/Down Port Alert Type: No Yes

[Save] Cancel

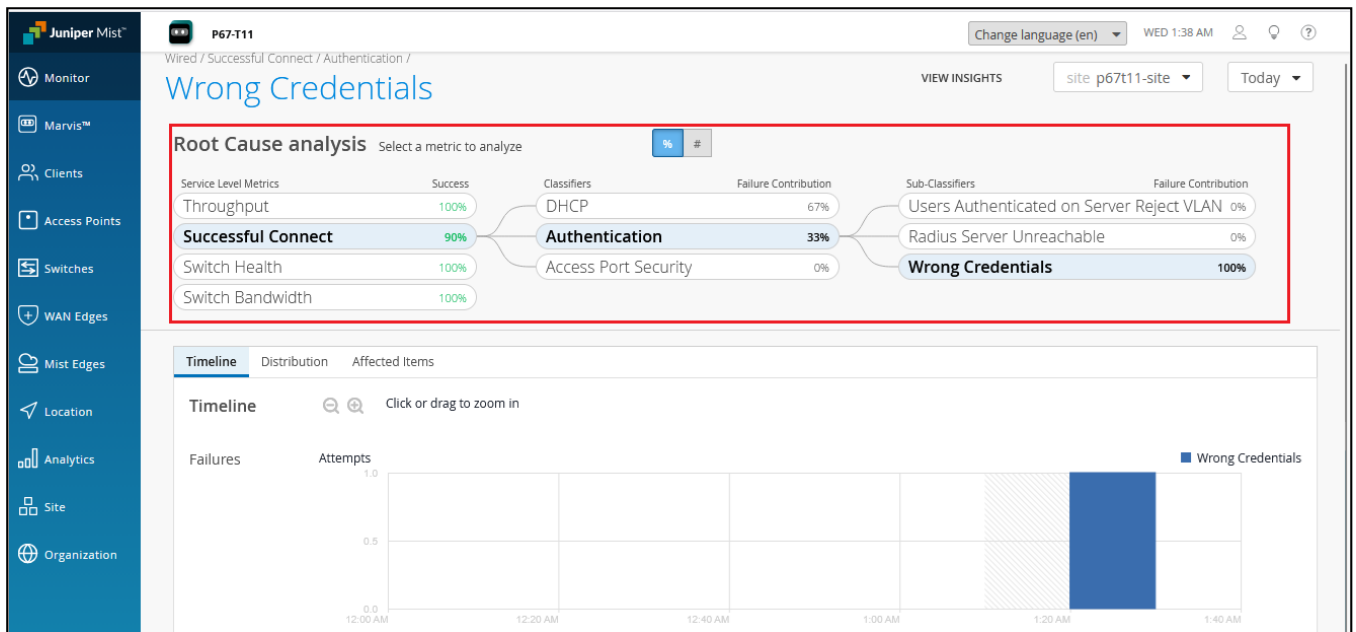
Navigate to Mist AI Monitor > Service Levels



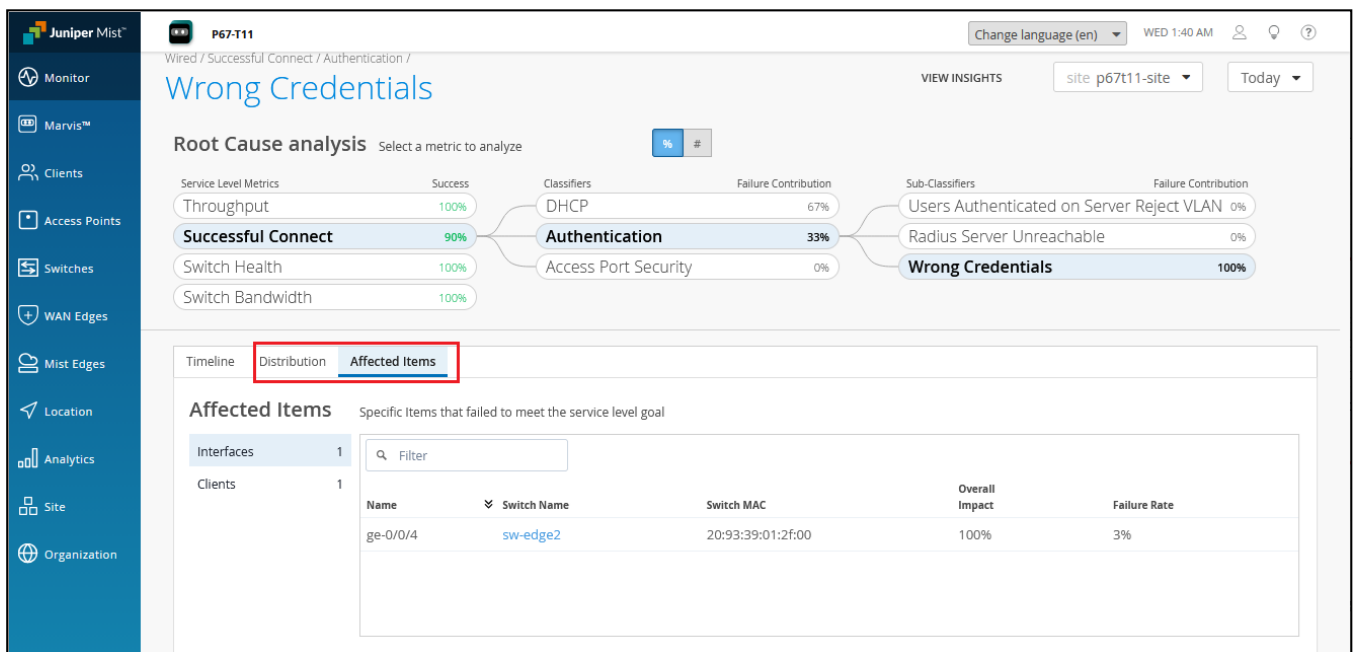
Click on Successful Connect in Wired Monitor.



You should see Authentication percentage in failure contribution and Wrong Credentials in sub-classifiers. It might take more time to reveal this issue. Wait 10-15 more minutes and refresh the browser.



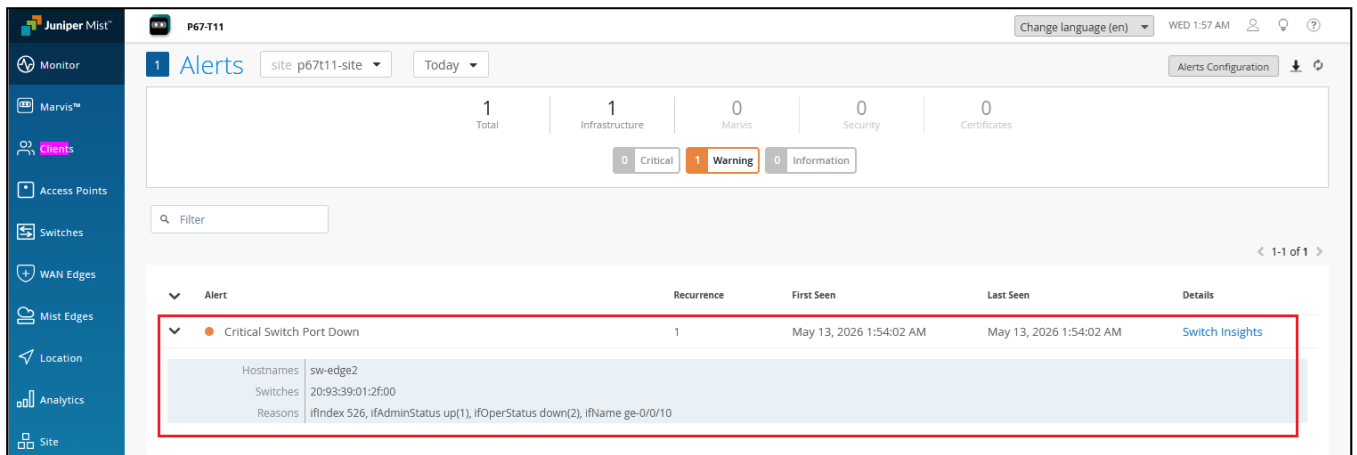
Check Distribution and Affected items tabs to investigate the incident.



Connect to MGMT PC and open SSH session to sw-core2. Disable interface 1/1/3 connected to sw-edge2. This will disable one of two uplinks on sw-edge2.

```
sw-core1# configure terminal
sw-core1(config)# interface 1/1/3
sw-core1(config-if)# shutdown
sw-core1(config-if)# end
```

Navigate to Mist AI Monitor > Alerts. You should see Critical Switch Port Down alert.



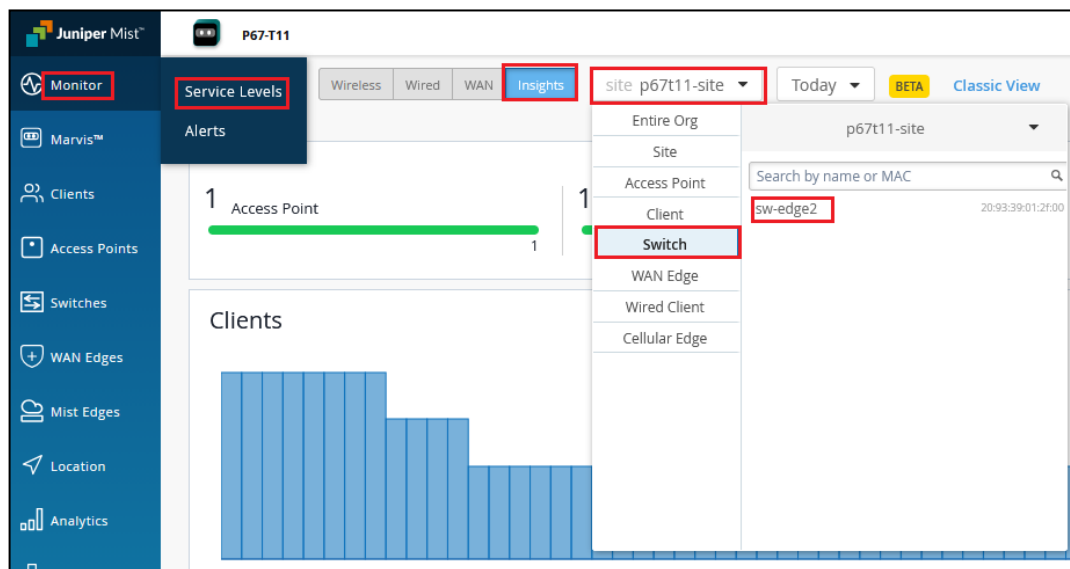
Connect to MGMG PC Remote Desktop and enable interface 1/1/3.

```
sw-core1# configure terminal
sw-core1(config)# interface 1/1/3
sw-core1(config-if)# no shutdown
sw-core1(config-if)# end
```

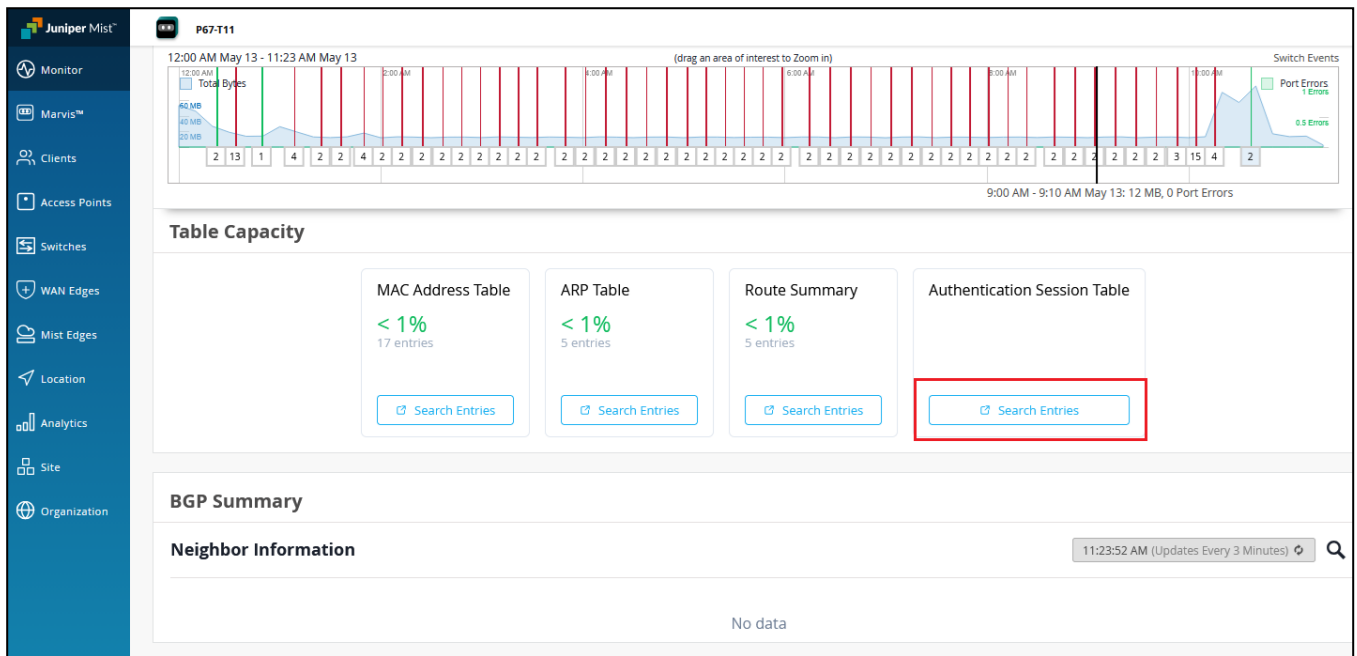
Connect to **PC4** Remote Desktop, open Lab NIC properties, then Authentication tab, click Additional Settings and Replace credentials. Enter correct credentials "**contractor/Aruba123!**". Click OK three times to save new settings.

NOTE: You might need to bounce port 4 in Mist AI Switches > sw-edge2 and then renew IP on PC4 with "ipconfig/renew" CMD command.

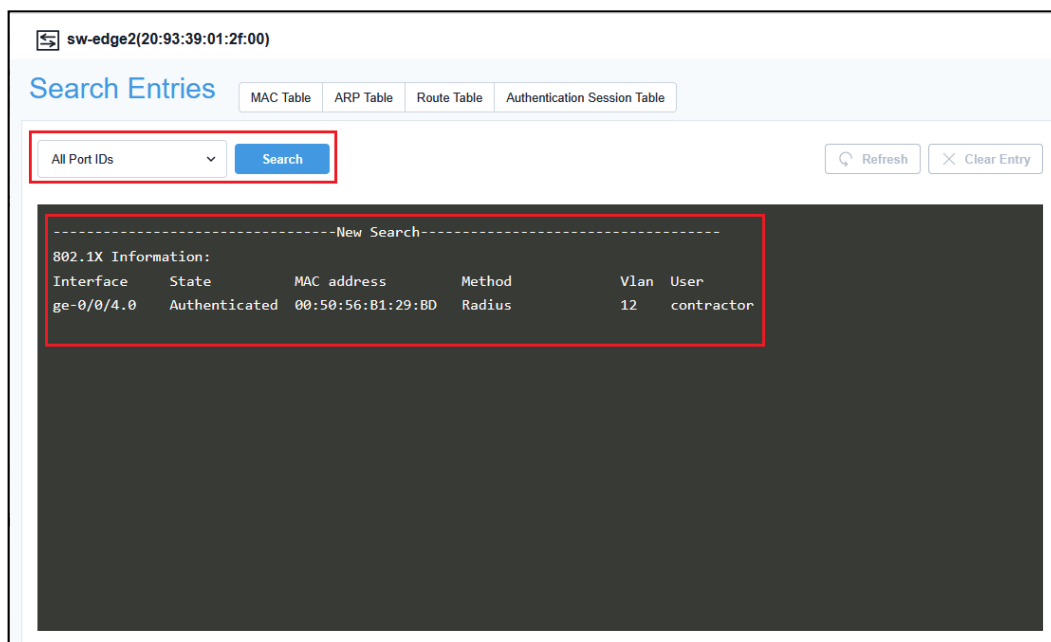
Navigate to Mist AI Monitor > Service Levels, select Insights and click site name next to Insights at the top of the page, then select Switch and click your switch name.



Scroll down the page to Table Capacity. And click Search Entries in Authentication Session Table.



Leave “All Port IDs” selected and click Search. It should display your contractor user authenticated on port ge-0/0/4



Select port ge-0/0/4 and click Search to see authentication details for client connected to port ge-0/0/4.

sw-edge2(20:93:39:01:2f:00)

Search Entries

MAC Table ARP Table Route Table Authentication Session Table

ge-0/0/4 Search Refresh Clear Entry

```

Reauthentication interval: 65000 seconds
Supplicant timeout: 30 seconds
Server timeout: 30 seconds
Maximum EAPOL requests: 2
Guest VLAN member: not configured
Number of connected supplicants: 1
Supplicant: contractor, 00:50:56:B1:29:BD
Operational state: Authenticated
Backend Authentication state: Idle
Authentication method: Radius
Authenticated VLAN: contractor
Session Reauth interval: 65000 seconds
Reauthentication due in 60436 seconds
Session Accounting Interim Interval: 600 seconds
Accounting Update due in 237 seconds
Eapol-Block: Not In Effect
Domain: Data

```

Clear Screen

Switch to MAC Table, then select port ge-0/0/4 and click Search. You should see your table PC4 MAC address.

sw-edge2(20:93:39:01:2f:00)

Search Entries

MAC Table ARP Table Route Table Authentication Session Table

MAC Address All VLANs ge-0/0/4 Search Refresh Clear Entry

```

-----New Search-----

MAC database for interface ge-0/0/4.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned, P - Persistent static, C - Control MAC
SE - statistics enabled, NM - non configured MAC, R - remote PE MAC, O - ovsdb MAC
GBP - group based policy)

Ethernet switching table : 1 entries, 1 learned
Routing instance : default-switch

Vlan      MAC      MAC      Age  GBP   Logical      NH      RTR
name      address  flags
contractor  00:50:56:b1:29:bd  D      -      ge-0/0/4.0    0      0

```

Clear Screen

Close the Search Entries window.

Task 4-3: Marvis Actions

Objectives

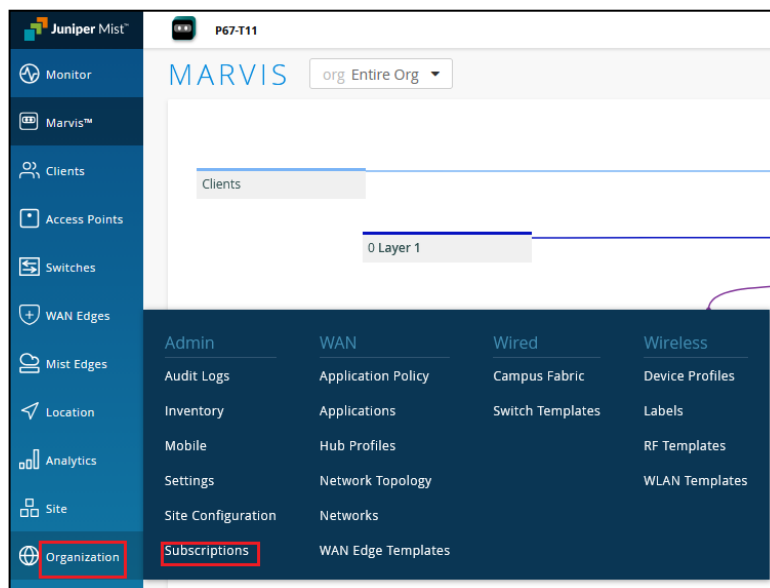
Review Marvis Actions.

Communicate with Marvis using conversational language.

Communicate with Arvis using queries.

Steps

Navigate to Organization > Admin > Subscriptions.

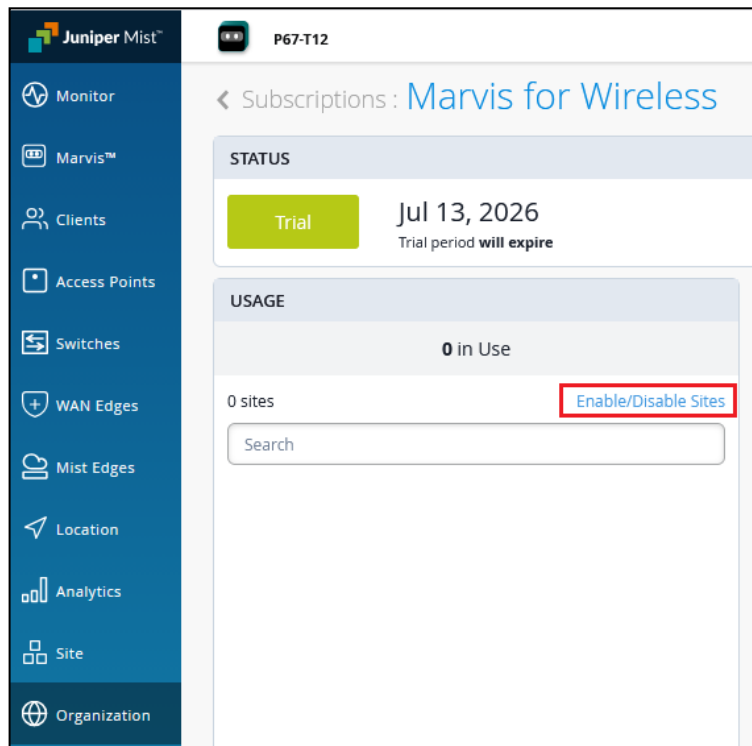


Click Marvis for Wireless.

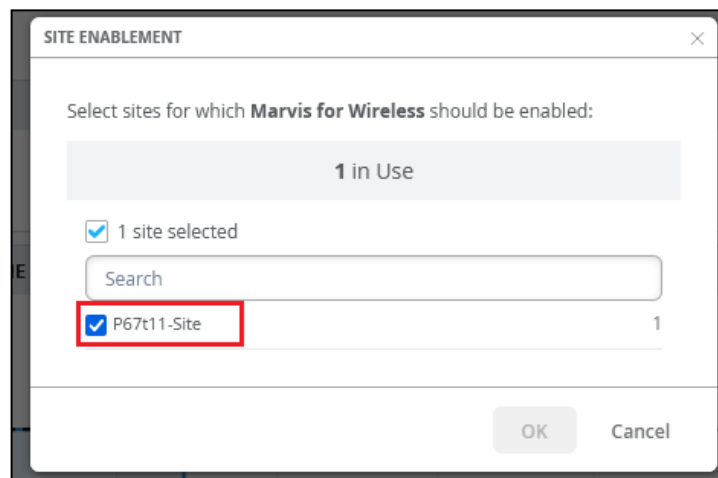
The screenshot shows the Juniper Mist P67-T11 interface with the 'Subscriptions' page open. The 'Organization' menu item is highlighted in the sidebar. The 'Subscriptions' table is displayed with the following data:

Subscription Type	Status	Usage	Sites with Usage
Asset Visibility	Trial	--	0 of 1
Marvis for WAN	Trial	--	0 of 1
Marvis for Wired Network	Trial	--	0 of 1
Marvis for Wireless	Trial	--	0 of 1
vBLE Engagement	Trial	--	0 of 1
WAN Assurance	Trial	--	0 of 1
WAN Assurance for Class 1	Trial	--	0 of 1
WAN Assurance for Class 2	Trial	--	0 of 1
WAN Assurance for Class 3	Trial	--	0 of 1
WAN Assurance for Class 4	Trial	--	0 of 1
WAN Assurance for Class 5	Trial	--	0 of 1
WAN Assurance for Class 6	Trial	--	0 of 1
Wi-Fi Management and Assurance	Trial	1	1 of 1
Wired Assurance 12	Trial	--	0 of 1
Wired Assurance 24	Trial	--	0 of 1
Wired Assurance 48	Trial	--	0 of 1

Click Enable/Disable Sites.



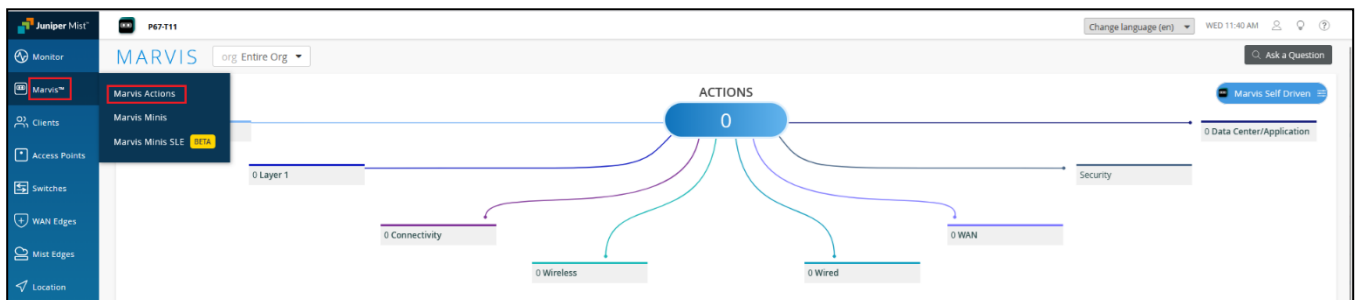
Select your site and click OK.



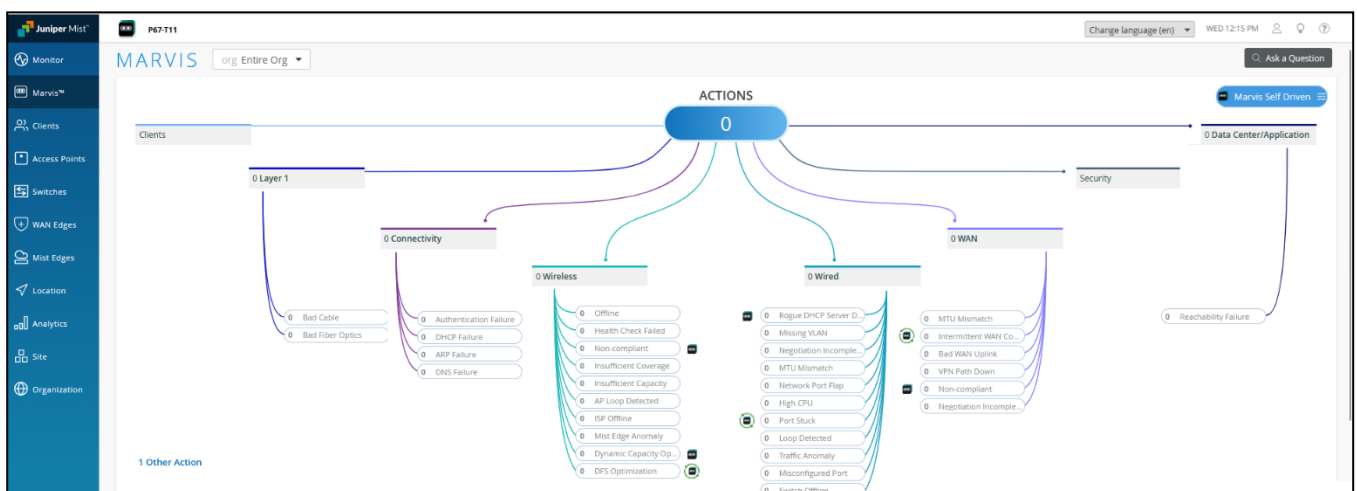
Return to Subscriptions and click Marvis for Wired Networks. Repeat previous steps to enable it for your site. Check that Marvis for Wireless and Marvis for Wired Networks are in use.

Subscription Type	Status	Usage	Sites with Usage
Asset Visibility	Trial	--	0 of 2
Marvis for WAN	Trial	--	0 of 2
Marvis for Wired Network	Trial	1	1 of 2
Marvis for Wireless	Trial	1	1 of 2
vBLE Engagement	Trial	--	0 of 2
WAN Assurance	Trial	--	0 of 2
WAN Assurance for Class 1	Trial	--	0 of 2
WAN Assurance for Class 2	Trial	--	0 of 2
WAN Assurance for Class 3	Trial	--	0 of 2
WAN Assurance for Class 4	Trial	--	0 of 2
WAN Assurance for Class 5	Trial	--	0 of 2
WAN Assurance for Class 6	Trial	--	0 of 2
Wi-Fi Management and Assurance	Trial	1	1 of 2
Wired Assurance 12	Trial	1	1 of 2
Wired Assurance 24	Trial	--	0 of 2
Wired Assurance 48	Trial	--	0 of 2

Navigate to Mist AI Marvis > Marvis Actions. You should have 0 Actions now.



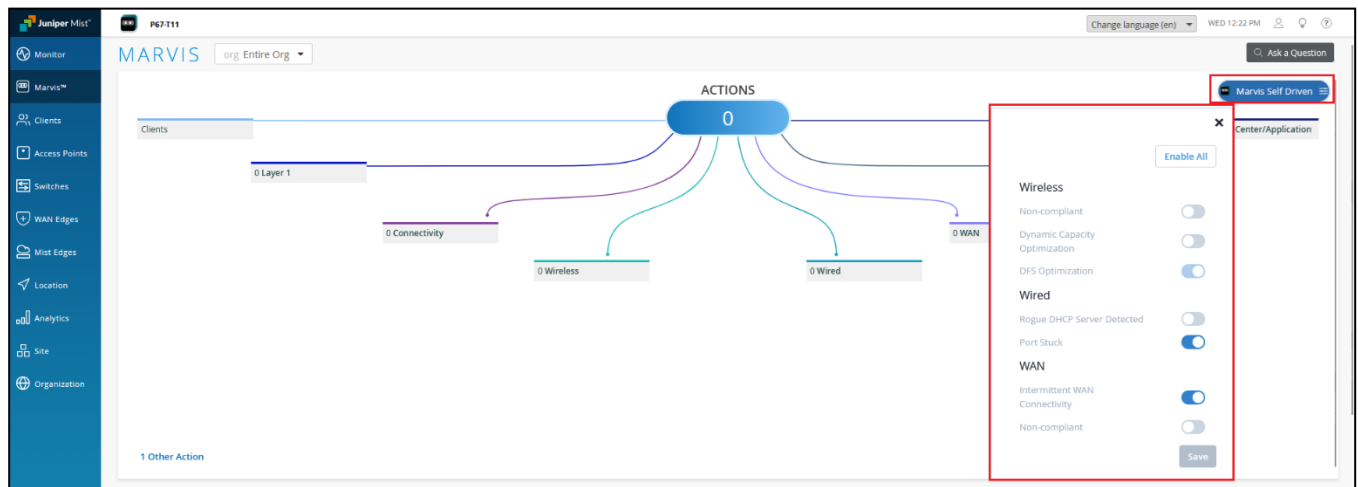
Observe available Actions by clicking on each group of Actions and then click each individual Action.



Marvis leverages the Mist AI to identify the root cause of issues. Marvis can automatically fix issues (self-driving mode) or recommend actions that require user intervention (driver-assist mode). The

Marvis Actions page lists the high-impact network issues that Marvis detects. Marvis Actions also displays the recommended actions for your organization's network. Marvis Actions provides insight into issues across the wired, WAN, and wireless networks, at the managed service provider (MSP) level, organization level, and site level. With Marvis Actions, you can track firmware compliance on APs, identify bad cables, locate L2 loops, detect WAN link outages, and more—all from a single page.

Click Marvis Self Driven setting to review available options.



Marvis actions provide both driver-assist and self-driving actions. Driver-assist actions require user intervention based on the details and recommendations provided by Marvis. When you grant permissions to Marvis, it autonomously initiates self-driving actions to execute corrective measures without any user involvement. This effectively automates the process of identifying and resolving issues. For example, a driver-assist action involves a network administrator having to manually upgrade the firmware on an AP. Conversely, a self-driving action automatically initiates the firmware upgrade when Marvis detects a firmware non-compliance on an AP.

By utilizing the self-driving capabilities, you can automate simple repetitive tasks, streamline troubleshooting processes, minimize downtime, and enhance overall network efficiency.

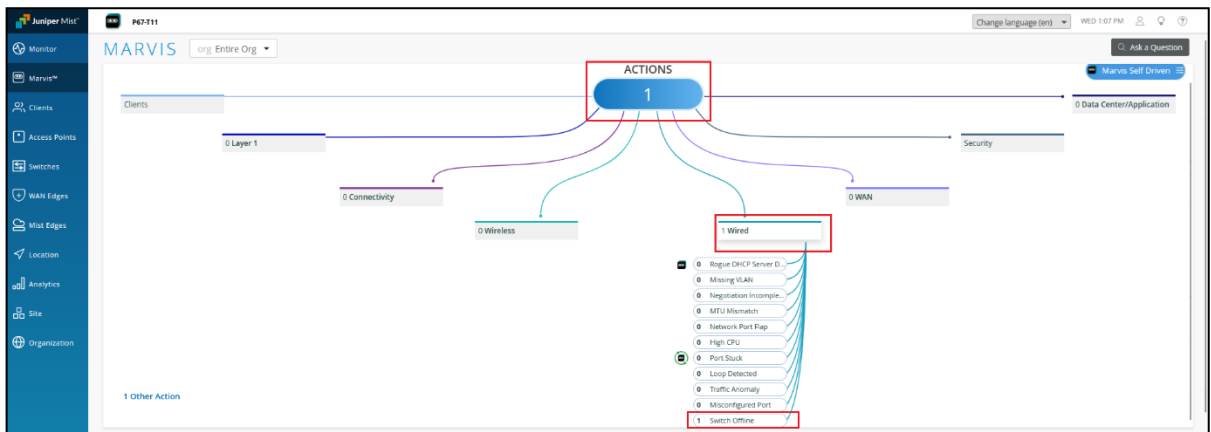
Open MGMT PC Remote Desktop and connect to **sw-core1** with SSH. Shutdown interface 1/1/3 which is connected to sw-edge2.

```
sw-core1# configure terminal
sw-core1(config)# interface 1/1/3
sw-core1(config-if)# shutdown
sw-core1(config-if)# end
```

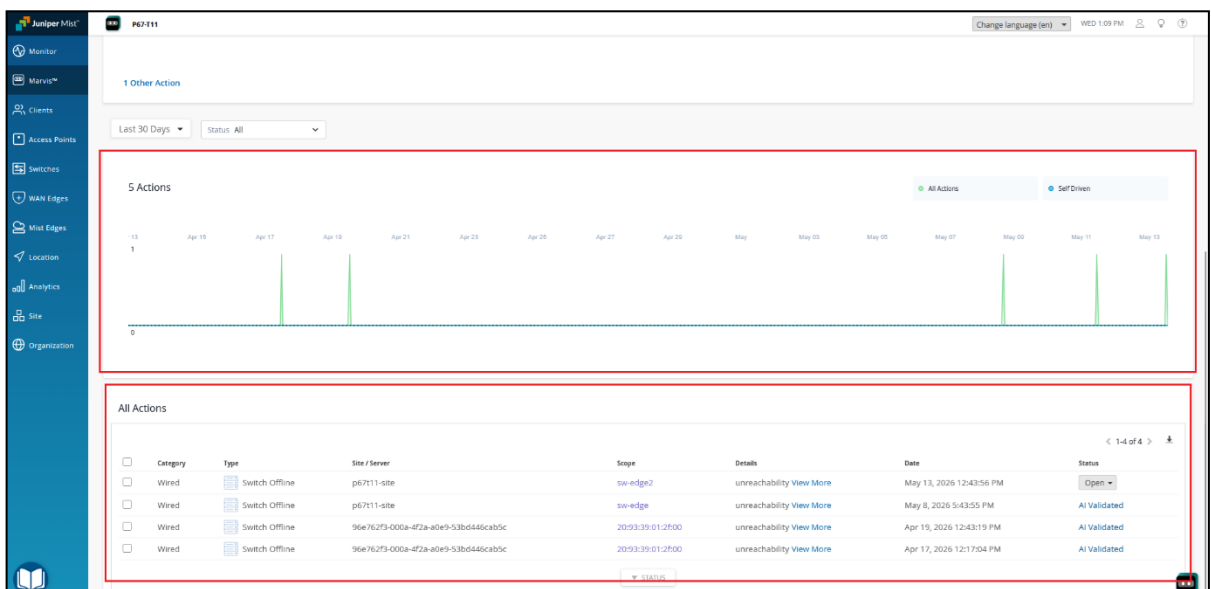
Open SSH session to **sw-core2** and disable interface 1/1/3. This way you disconnect both Juniper switch and AP from Mist AI.

```
sw-core2# configure terminal
sw-core2(config)# interface 1/1/3
sw-core2(config-if)# shutdown
sw-core2(config-if)# end
```

Return to Mist AI Marvis > Marvis Actions page. It might take 10-15 minutes to see one action appear, feel free to continue with the following steps instead of waiting.



Scroll down the page to observe the Time Series Graph. You may see several actions triggered.



Click View More next to unreachability. A new window will appear with Switch details.

Switch Offline

Switch Details

Site ID	28d12c58-c070-4399-bbe2-9063eacbefa6	Impacted Site	p6711-site
Model	EX4100-F-12T	Start Time	May 13, 2026 12:43:56 PM

Connect to MGMT PC, open SSH session to **sw-core1** and enable interface 1/1/3.

```
sw-core1# configure terminal
sw-core1(config)# interface 1/1/3
sw-core1(config-if)# no shutdown
sw-core1(config-if)# end
```

Connect to MGMT PC, open SSH session to **sw-core2** and enable interface 1/1/3.

```
sw-core2# configure terminal
sw-core2(config)# interface 1/1/3
sw-core2(config-if)# no shutdown
sw-core2(config-if)# end
```

Navigate to Mist AI Switches and confirm that your table switch is connected.

The screenshot shows the Juniper Mist web interface for the 'p67t11' site. The 'Switches' tab is selected. At the top, there are summary cards for Cloud Connected Switches (1), Discovered Switches (0), Wired Clients (2), and Total Allocated AP Power (0W). Below these are various compliance and status indicators, all showing 100% except for Switchport Usage at 21%. A table lists the switches, with one entry highlighted in red: 'sw-edge2' with IP address 10.1.3.10, model EX4100-F-12T, and status 'Connected'.

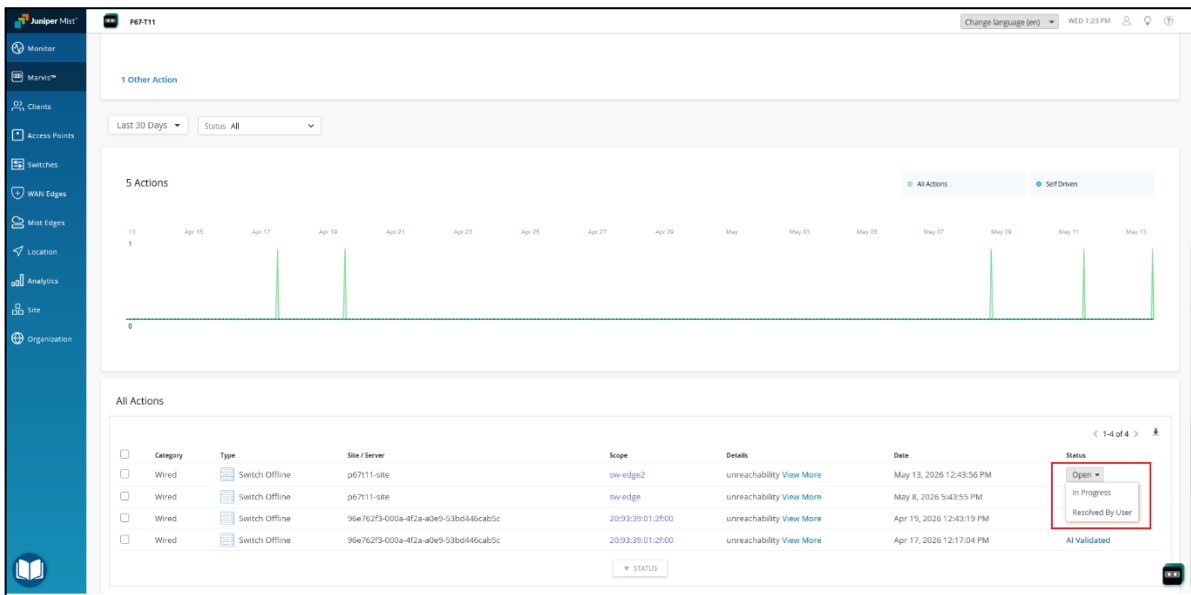
Status	Name	IP Address	Model	Mist APs	Wireless Clients	Wired Clients	Version	Uptime	Last Config	Insights
Connected	sw-edge2	10.1.3.10	EX4100-F-12T	0	0	2	22.4R3.25	6d 22m	May 13, 2026 11:36:40 AM	Switch Insights

Navigate to Mist AI Access Points and confirm that your table access point is connected.

The screenshot shows the Juniper Mist web interface for the 'p67t11' site. The 'Access Points' tab is selected. At the top, there are summary cards for Access Points (1), Wireless Clients (0), and AP12 (1). Below these are various compliance and status indicators, all showing 100%. A table lists the access points, with one entry highlighted in red: 'AP12' with MAC address 70:90:41:40:5a:60, IP address 10.1.3.50, model AP12, and status 'Connected'.

Status	Name	MAC Address	IP Address	Version	Model	Eth Port Speed	Last Seen	No. Clients	Total Bytes	2.4 GHz Channel	5 GHz Channel	6 GHz Channel	2.4 GHz TxPower	5 GHz TxPower	6 GHz TxPower	LLDP Role
Connected	AP12	70:90:41:40:5a:60	10.1.3.50	0.12.27458	AP12	eth0 1000mbps	May 13, 2026 1:17:00 PM	0	0 B							

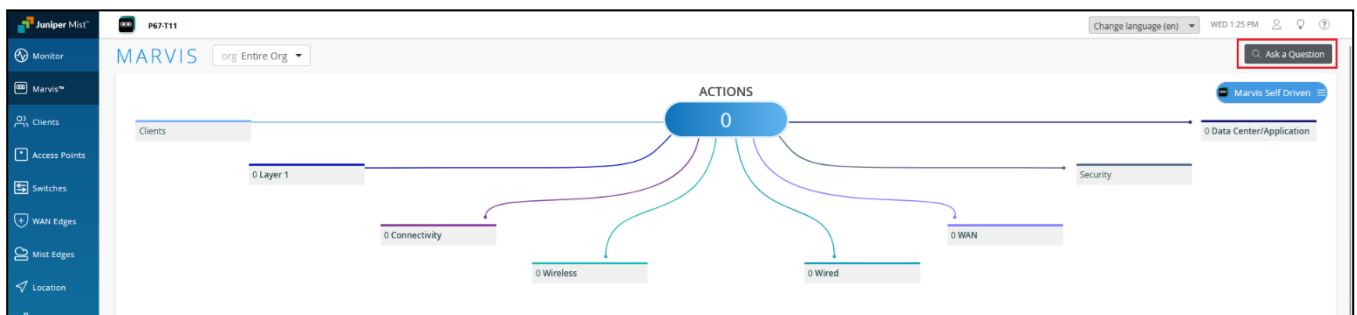
Navigate to Mist AI Marvis > Marvis Actions, scroll down the page and if you have an Action with Open status. Click on Open and select Resolved by User.



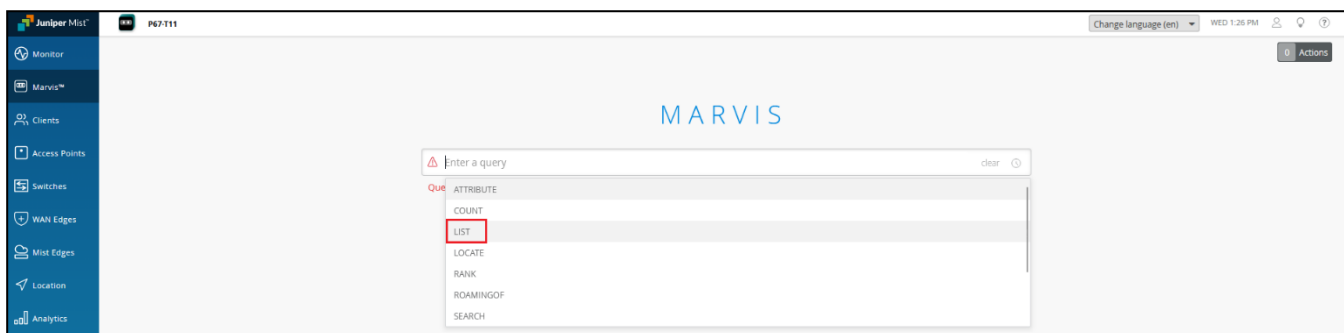
Select Solved using the Mist suggestion action, type a comment and click OK.

The 'Resolve Action' dialog box is shown. Under the 'RESOLUTION' section, the radio button 'Solved using the Mist suggested action' is selected. The 'COMMENT' field contains the text 'Uplink disconnected'. The 'OK' button is highlighted.

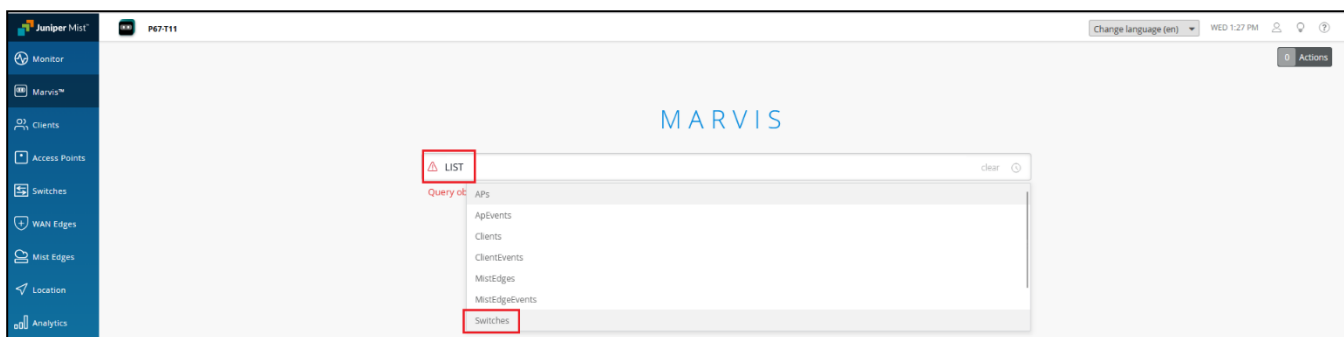
Scroll up the page to the top and click Ask a Question.



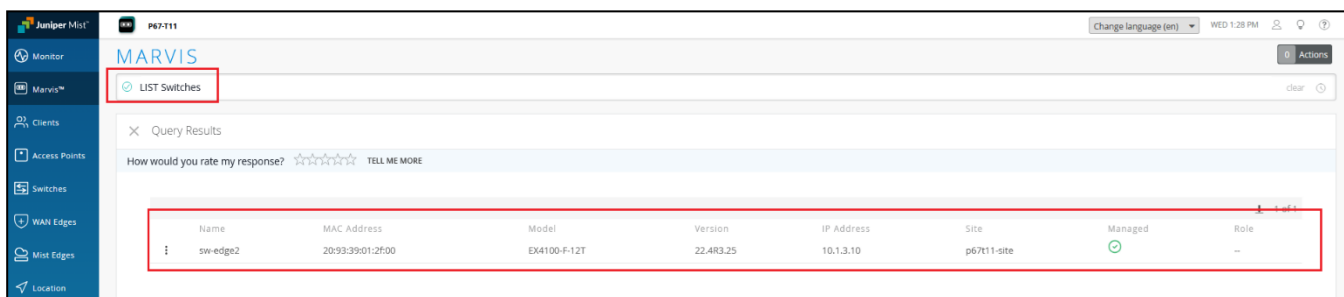
Click in the field with "Enter a query" text and select LIST.



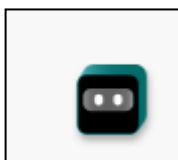
Then hit space and select Switches



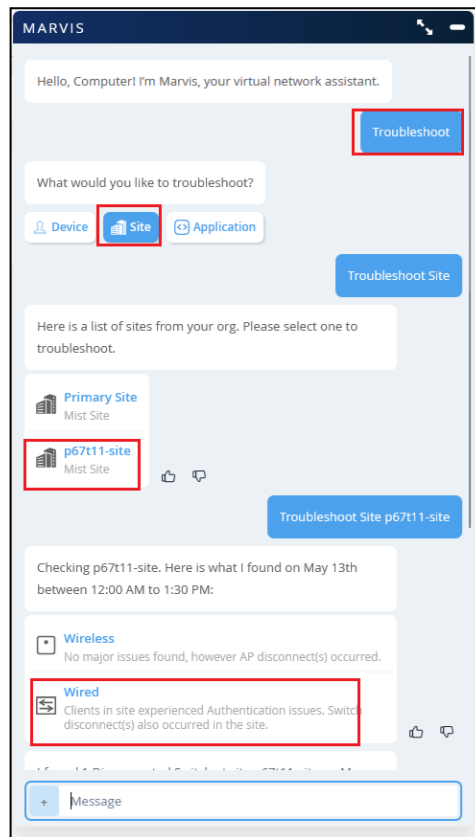
Hit Enter and review the output which should contain your table switch.



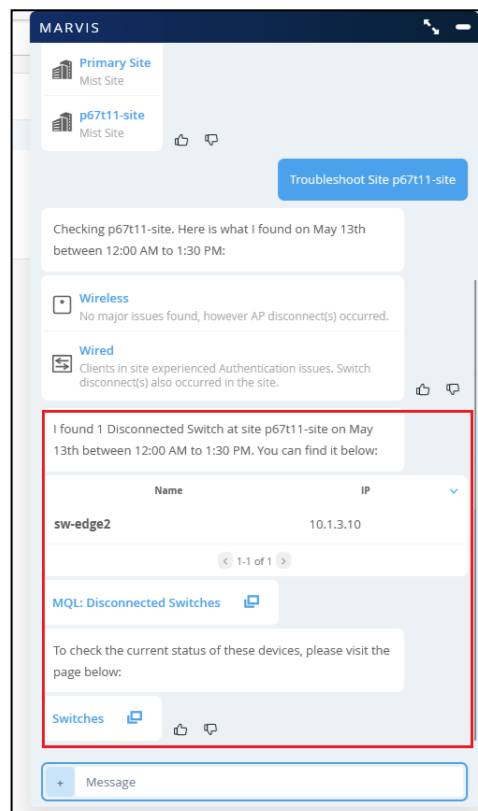
Click Marvis icon in the top-left corner or bottom-right corner.



Click or type troubleshoot, then select Site, select your site and Wired.



Select Disconnected switches or otherwise you can access Switch Insights.



Click MQL: Disconnected Switches.

The screenshot shows the Juniper Mist MARVIS interface. On the left is a navigation sidebar with icons for Monitor, Marvis™, Clients, Access Points, Switches, WAN Edges, and Mist Edges. The main panel has a header with the MARVIS logo and a search bar. The search bar contains the query: `LIST SwitchEvents WITH SwitchEventType Switch-Disconnected AND Site 'p67111-site' DURING '12:00 AM May 13, 2026 - 1:30 PM May 13, 2026'`. Below the search bar, there is a 'Query Results' section with a feedback prompt: 'How would you rate my response?' followed by five stars and a 'TELL ME MORE' link. A table displays the results with columns: Time, Type, Switch, and Event Detail. The table shows one result: May 13, 2026 12:32:29 PM, Switch Disconnected, sw-edge2, and chassis mac: 209339012f00 ...

Time	Type	Switch	Event Detail
May 13, 2026 12:32:29 PM	Switch Disconnected	sw-edge2	chassis mac: 209339012f00 ...

Task 4-4: Packet Capture for Wired client traffic

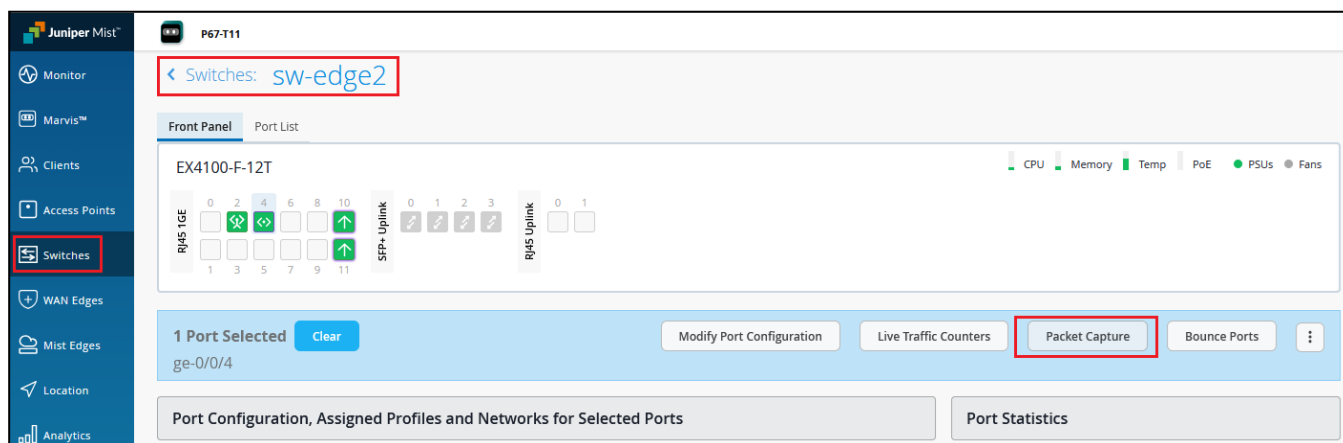
Objectives

Use Packet Capture for Wired Clients.

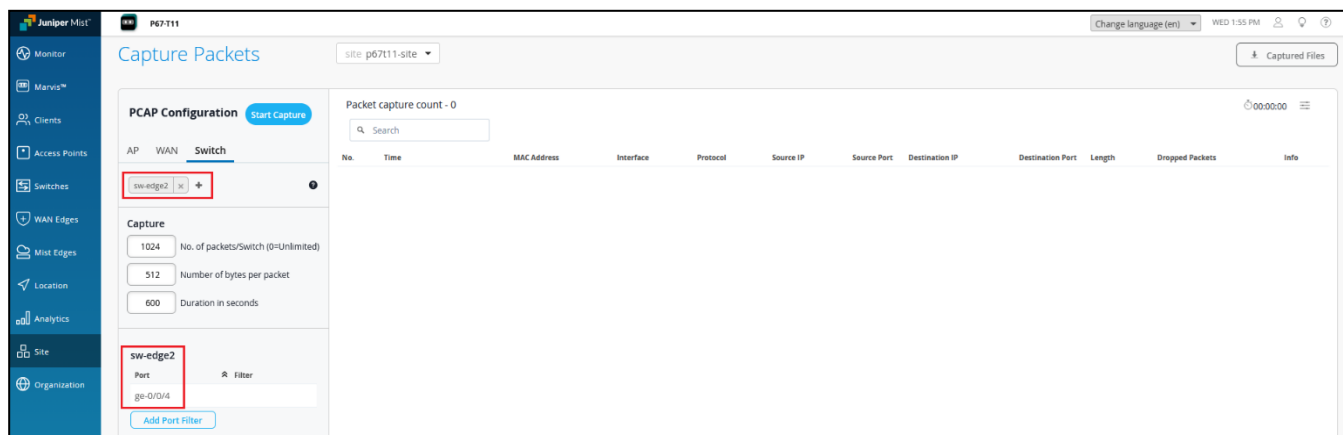
Analyze Wired Client Traffic.

Steps

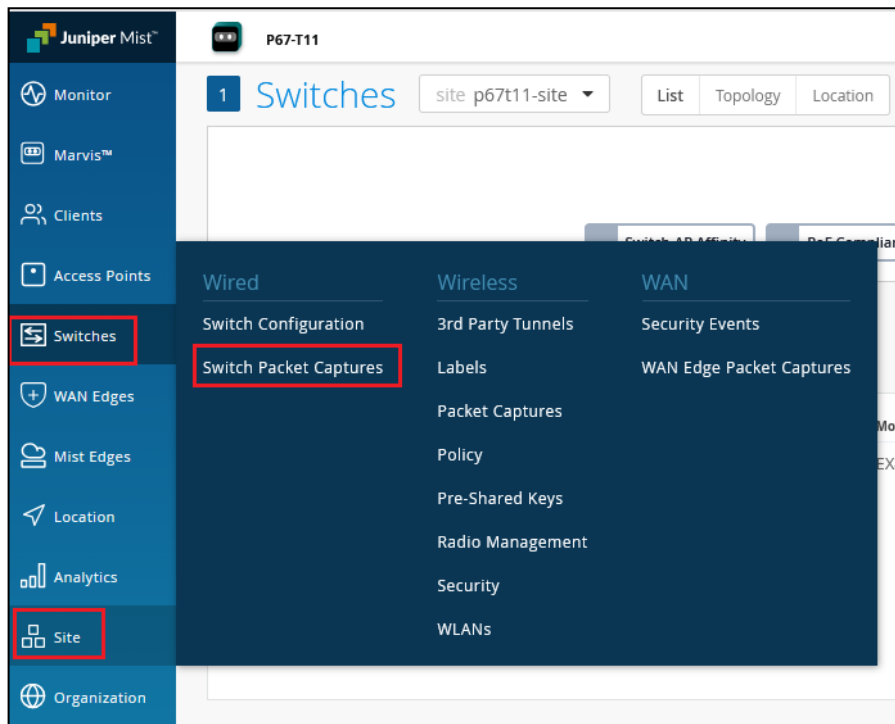
You can navigate to Wired Packet Capture in several ways. Try the first option through Switch Front Panel. Navigate to Mist AI Switches > sw-edge2, then select Port 4 on the Front Panel.



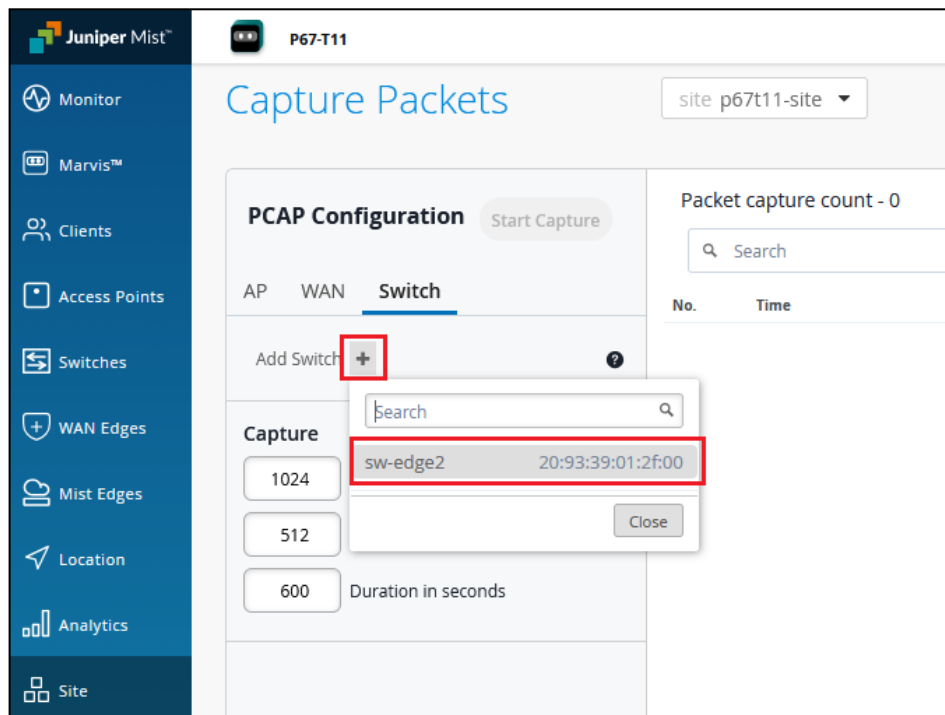
This will bring you to Capture Packets page where your switch and port are already selected.



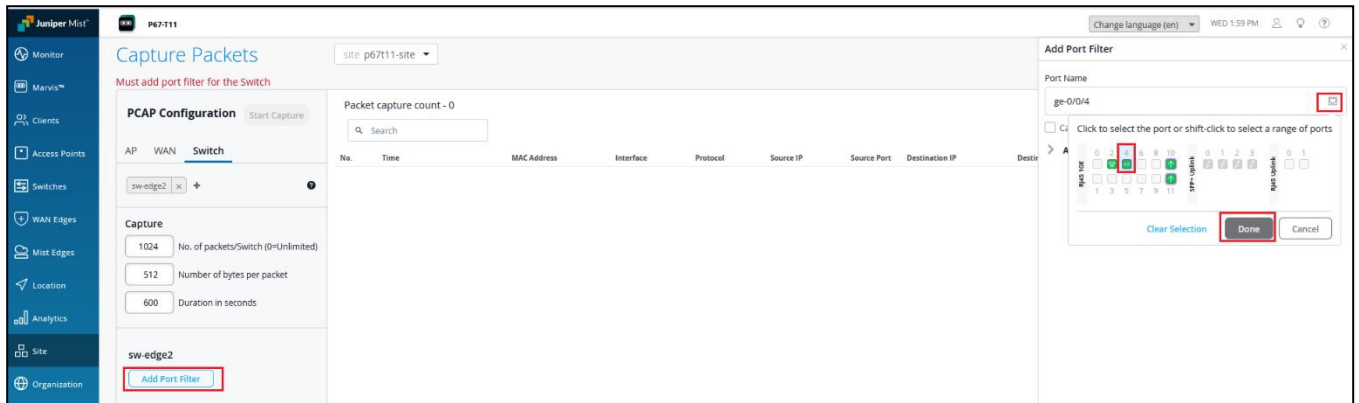
Now try a second option. Navigate first to Mist AI Switches. And after that navigate to Site > Wired > Switch Packet Captures.



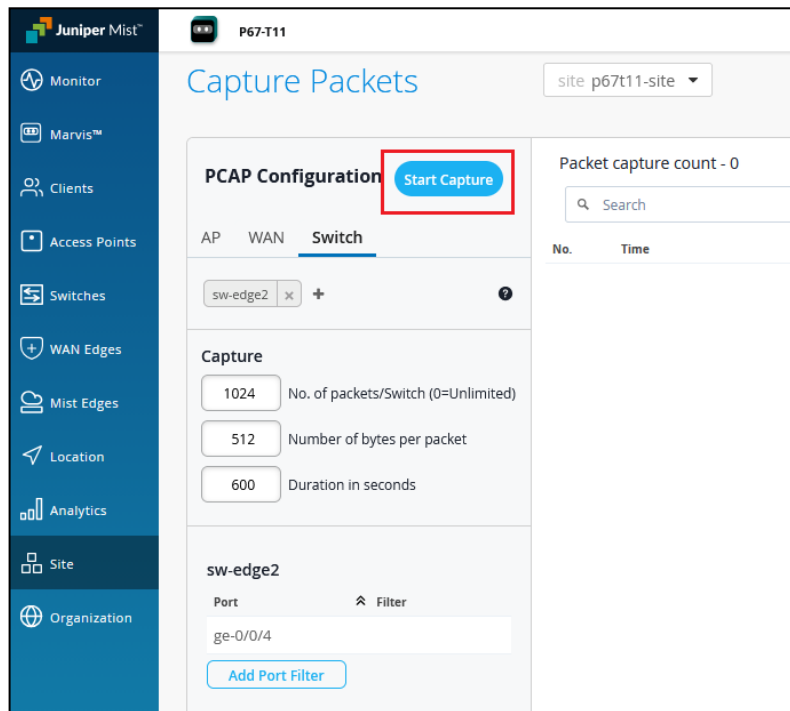
You need to select your switch first.



Then click Add Port Filter, click small port icon and then select port 4. Click **Done** and **Save**.



Click Start Capture.



In several seconds you will start seeing some packets captured.

Connect to **PC4** Remote Desktop, open CMD and **ping 10.254.1.21**.

```
C:\Users\student>ping 10.254.1.21
```

```
Pinging 10.254.1.21 with 32 bytes of data:
Reply from 10.254.1.21: bytes=32 time=2ms TTL=126
Reply from 10.254.1.21: bytes=32 time=2ms TTL=126
Reply from 10.254.1.21: bytes=32 time=2ms TTL=126
Reply from 10.254.1.21: bytes=32 time=1ms TTL=126
```

```
Ping statistics for 10.254.1.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

On **PC4**, renew IP address with **ipconfig/renew** CMD command.

```
C:\Users\student>ipconfig/renew
```

Windows IP Configuration

<Output omitted>

Ethernet adapter Lab NIC - 6300-D Port 4:

```
Connection-specific DNS Suffix  . : aruba-training.com
IPv4 Address. . . . . : 10.1.12.50
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.1.12.1
```

<Output omitted>

On **PC4**, open a browser and navigate to **google.com**

Return to Mist AI Wired Packet Capture. Make sure it was still running and click **Stop Capture**. Otherwise repeat previous steps on **PC4**.

PCAP Configuration **Stop Capture**

Packet capture count - 202

Search

No.	Time	MAC Address	Interface	Protocol	Source IP	Source Port	Destination IP	Destination Port	Length	Dropped Packets	Info
1	2:06:11.769 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61126	10.254.1.21	443	66	0	HTTPS, (61126) -> (443), se
2	2:06:11.769 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61126	10.254.1.21	443	60	0	HTTPS, (61126) -> (443), se
3	2:06:11.769 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61126	10.254.1.21	443	253	0	HTTPS, (61126) -> (443), se
4	2:06:11.772 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61126	10.254.1.21	443	412	0	HTTPS, (61126) -> (443), se
5	2:06:11.774 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61127	10.254.1.21	443	66	0	HTTPS, (61127) -> (443), se
6	2:06:11.774 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61127	10.254.1.21	443	60	0	HTTPS, (61127) -> (443), se
7	2:06:11.774 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61127	10.254.1.21	443	183	0	HTTPS, (61127) -> (443), se
8	2:06:11.774 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61127	10.254.1.21	443	396	0	HTTPS, (61127) -> (443), se
9	2:06:11.777 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61128	10.254.1.21	443	66	0	HTTPS, (61128) -> (443), se
10	2:06:11.777 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61128	10.254.1.21	443	60	0	HTTPS, (61128) -> (443), se
11	2:06:11.777 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61128	10.254.1.21	443	183	0	HTTPS, (61128) -> (443), se
12	2:06:11.780 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61128	10.254.1.21	443	380	0	HTTPS, (61128) -> (443), se
13	2:06:11.780 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61129	10.254.1.21	443	66	0	HTTPS, (61129) -> (443), se
14	2:06:11.780 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61129	10.254.1.21	443	60	0	HTTPS, (61129) -> (443), se
15	2:06:11.780 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61129	10.254.1.21	443	106	0	HTTPS, (61129) -> (443), se
16	2:06:11.783 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61129	10.254.1.21	443	384	0	HTTPS, (61129) -> (443), se
17	2:06:13.172 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	DNS	10.1.12.50	55790	224.0.0.251	5353	83	0	Transaction Id: 0x8743, res
18	2:06:14.749 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	UDP	10.1.12.50	58532	142.251.154.119	443	961	0	HTTPS, (58532) -> (443)
19	2:06:14.769 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	UDP	10.1.12.50	58532	142.251.154.119	443	75	0	HTTPS, (58532) -> (443)
20	2:06:14.800 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	UDP	10.1.12.50	58532	142.251.154.119	443	79	0	HTTPS, (58532) -> (443)
21	2:06:14.749 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	UDP	10.1.12.50	58532	142.251.154.119	443	383	0	HTTPS, (58532) -> (443)

Type "icmp" in search field and hit enter.

PCAP Configuration **Start Capture**

Packet capture count - 8

Search **Filter | icmp** **Clear All**

No.	Time	MAC Address	Interface	Protocol	Source IP	Source Port	Destination IP	Destination Port	Length	Dropped Packets	Info
26	2:06:17.909 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	ICMP	10.1.12.50		10.254.1.21		74	0	type= Echo Request, code= 0, se
27	2:06:17.910 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	ICMP	10.1.12.50		10.254.1.21		96	0	type= Echo Request, code= 0, se
29	2:06:18.920 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	ICMP	10.1.12.50		10.254.1.21		96	0	type= Echo Request, code= 0, se
30	2:06:19.937 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	ICMP	10.1.12.50		10.254.1.21		96	0	type= Echo Request, code= 0, se
32	2:06:18.920 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	ICMP	10.1.12.50		10.254.1.21		74	0	type= Echo Request, code= 0, se
33	2:06:19.937 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	ICMP	10.1.12.50		10.254.1.21		74	0	type= Echo Request, code= 0, se
34	2:06:20.952 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	ICMP	10.1.12.50		10.254.1.21		74	0	type= Echo Request, code= 0, se
35	2:06:20.952 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	ICMP	10.1.12.50		10.254.1.21		96	0	type= Echo Request, code= 0, se

Type "dhcp" and click on DHCP Protocol.

PCAP Configuration **Start Capture**

Packet capture count - 214

Search **dhcp**

Protocol
DHCP

Info
message_type= Boot Request, hops= 0, transaction_id= 0x3b40135f, unicast, DHCP Message Type (DHCP REQUEST)

No.	Time	MAC Address	Interface	Protocol	Source IP	Source Port	Destination IP	Destination Port	Length	Dropped Packets	Info
197	2:06:40.744 PM May 13, 2026										

Review DHCP requests sent by PC4.

The screenshot shows the Juniper Mist 'Capture Packets' interface. The 'PCAP Configuration' section on the left has 'Switch' selected. The main table shows two captured packets, both DHCP requests from 10.1.12.50 to 10.254.1.21. The 'Info' column for both packets contains the text 'message_type= Boot Request, hops=1'.

No	Time	MAC Address	Interface	Protocol	Source IP	Source Port	Destination IP	Destination Port	Length	Dropped Packets	Info
36	2:06:25.674 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4	DHCP	10.1.12.50	68	10.254.1.21	67	364	0	message_type= Boot Request, hops=1
37	2:06:25.676 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4	DHCP	10.1.12.50	68	10.254.1.21	67	364	0	message_type= Boot Request, hops=1

Type “https” and hit enter. You should see PC4 communication with internal and external IP addresses using TCP destination port 443.

Click on one of captured packets to see more details at the bottom of the page.

The screenshot shows the Juniper Mist 'Capture Packets' interface with a filter 'https' applied. The table lists 158 packets, mostly HTTPS traffic. The 'Info' column for many packets shows 'HTTPS, (61128) -> (443), se'. At the bottom, a detailed view of a packet is shown, including the 'Time', 'Switch', 'Switch MAC', 'Source', 'Destination', and 'Content'.

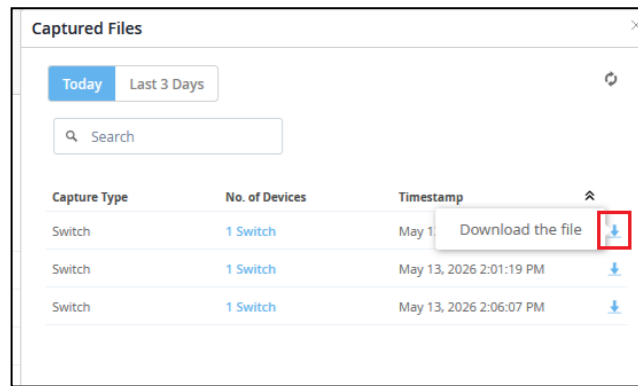
No	Time	MAC Address	Interface	Protocol	Source IP	Source Port	Destination IP	Destination Port	Length	Dropped Packets	Info
11	2:06:11.777 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61128	10.254.1.21	443	183	0	HTTPS, (61128) -> (443), se
12	2:06:11.780 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61128	10.254.1.21	443	380	0	HTTPS, (61128) -> (443), se
13	2:06:11.780 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61129	10.254.1.21	443	66	0	HTTPS, (61129) -> (443), se
14	2:06:11.780 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61129	10.254.1.21	443	60	0	HTTPS, (61129) -> (443), se
15	2:06:11.780 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61129	10.254.1.21	443	108	0	HTTPS, (61129) -> (443), se
16	2:06:11.783 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61129	10.254.1.21	443	394	0	HTTPS, (61129) -> (443), se
18	2:06:14.749 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	UDP	10.1.12.50	58532	142.251.154.119	443	361	0	HTTPS, (58532) -> (443)
19	2:06:14.760 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	UDP	10.1.12.50	58532	142.251.154.119	443	75	0	HTTPS, (58532) -> (443)
20	2:06:14.800 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	UDP	10.1.12.50	58532	142.251.154.119	443	79	0	HTTPS, (58532) -> (443)
21	2:06:14.749 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	UDP	10.1.12.50	58532	142.251.154.119	443	303	0	HTTPS, (58532) -> (443)
22	2:06:14.769 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	UDP	10.1.12.50	58532	142.251.154.119	443	97	0	HTTPS, (58532) -> (443)
23	2:06:14.801 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	UDP	10.1.12.50	58532	142.251.154.119	443	101	0	HTTPS, (58532) -> (443)
24	2:06:15.779 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	60063	172.217.68.188	443	82	0	HTTPS, (60063) -> (443), se
25	2:06:15.779 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	60063	172.217.68.188	443	60	0	HTTPS, (60063) -> (443), se
57	2:06:30.469 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	UDP	10.1.12.50	58532	142.251.154.119	443	378	0	HTTPS, (58532) -> (443)
58	2:06:30.512 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	UDP	10.1.12.50	58532	142.251.154.119	443	101	0	HTTPS, (58532) -> (443)
59	2:06:31.090 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	DNS	10.1.12.50	63810	10.254.1.21	53	99	0	Transaction Id= 0x6402, Mes
61	2:06:31.119 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	UDP	10.1.12.50	58971	142.250.111.04	443	1314	0	HTTPS, (58971) -> (443)

Click Captured Files in the top-right corner to download files.

The screenshot shows the Juniper Mist 'Capture Packets' interface. The 'Captured Files' button in the top-right corner is highlighted with a red box. The table below shows two captured packets, both HTTPS traffic from 10.1.12.50 to 10.254.1.21.

No	Time	MAC Address	Interface	Protocol	Source IP	Source Port	Destination IP	Destination Port	Length	Dropped Packets	Info
11	2:06:11.777 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61128	10.254.1.21	443	183	0	HTTPS, (61128) -> (443), se
12	2:06:11.780 PM May 13, 2026	20:93:39:01:2f:00	ge-0/0/4.0	TCP	10.1.12.50	61128	10.254.1.21	443	380	0	HTTPS, (61128) -> (443), se

Click on download icon next to one of your files.



If you have Wireshark installed on your PC you can open this file or you can try that from MGMT PC.

You have completed this lab!

Lab 5: Configuration Scalability

Objectives

After completing this lab, you will be able to:

- Use Site variables
- Use CLI Configuration in Mist AI
- Use Select Switches Configuration
- Use bulk upload of switch configuration

Overview

After completing this lab, you will become familiar with Juniper MIST Site variables, CLI Configuration, Select switches configuration and bulk upload of switch configuration. Juniper Mist web UI could be changed over the time and will not match screenshots in this workshop. Ask your instructor for assistance if you struggle finding required settings in Juniper Mist.

Task 5-1: Use Site variables

Objectives

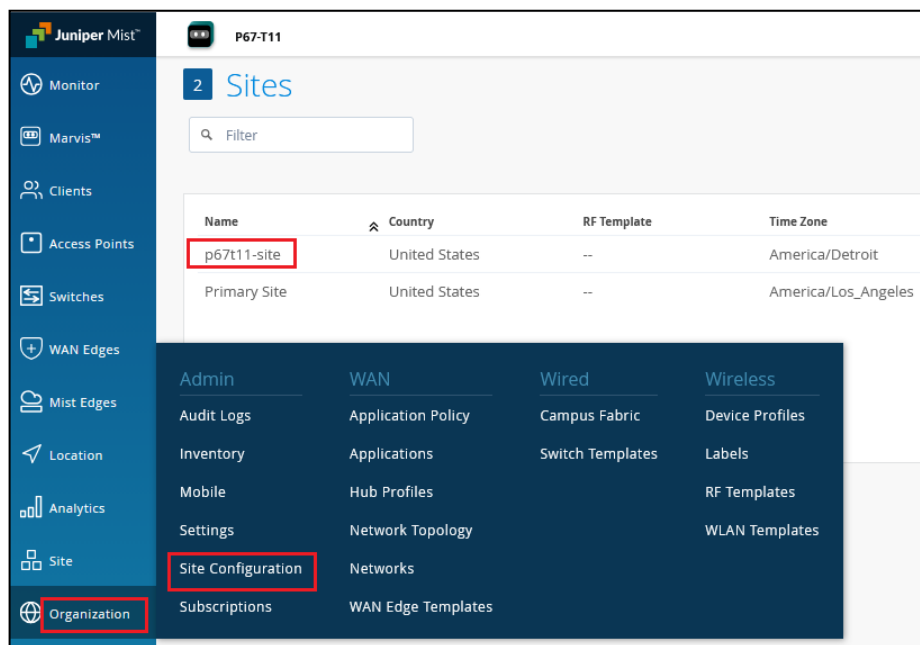
Define Site variables.

Configure Switch Templates with Site Variables.

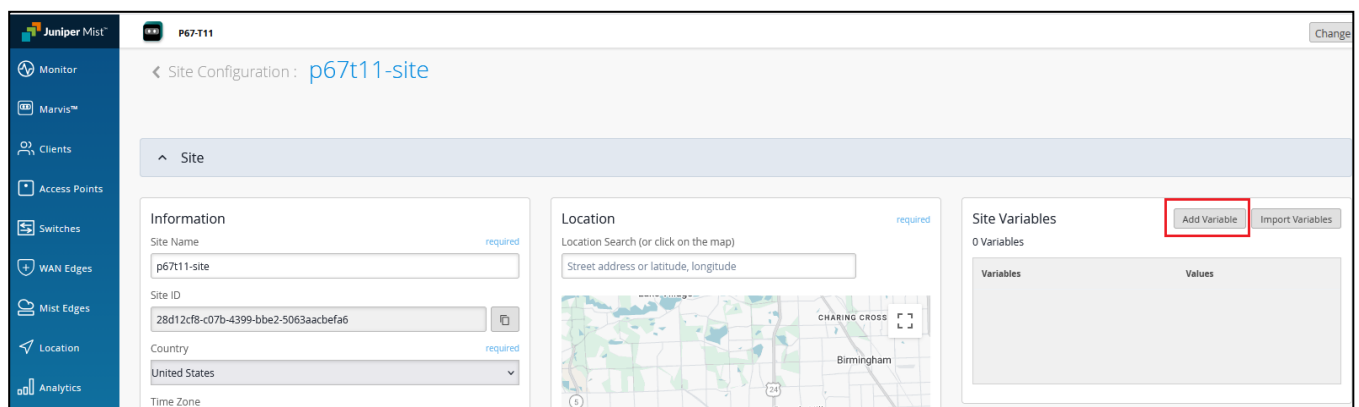
Change variables and validate configuration.

Steps

Navigate to Mist AI Organization > Admin > Site Configuration and select your site.



Click Add Variable in Site Variables section.



Define variable `{{dns}}` with value 10.254.1.21 and click **Save**.



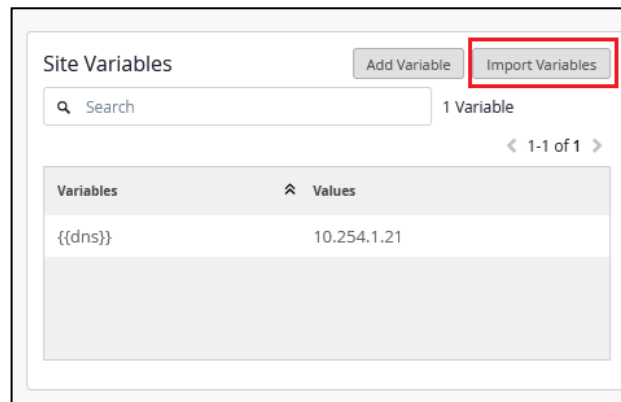
Add Variables [X]

Variable

Value

[Save] [Cancel]

Click Import Variables.



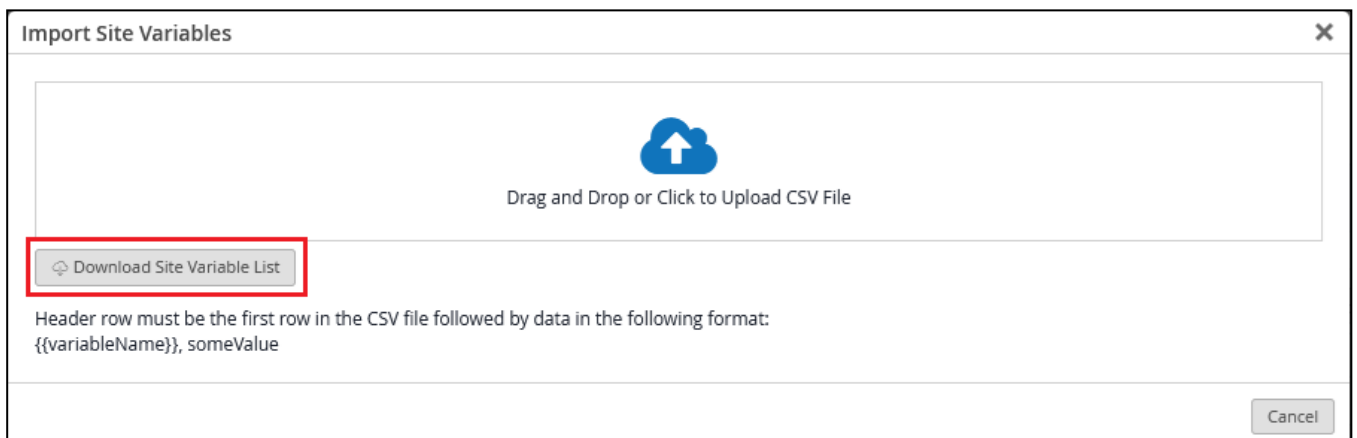
Site Variables [Add Variable] [Import Variables]

Search 1 Variable

< 1-1 of 1 >

Variables	Values
{{dns}}	10.254.1.21

Click Download Site Variable List.



Import Site Variables [X]

Drag and Drop or Click to Upload CSV File

[Download Site Variable List]

Header row must be the first row in the CSV file followed by data in the following format:
 {{variableName}}, someValue

[Cancel]

Open siteVariables.csv file and add these variables to the one you added previously:

Variable	Value
{{ntp}}	10.254.1.21
{{radius}}	10.254.1.23
{{vlan_emp}}	11
{{vlan_cont}}	12

{{vlan_iot}}	13
{{vlan_guest}}	14
{{vlan_mgmt}}	3

	A	B	C
1	Variable	Value	
2	{{dns}}	10.254.1.21	
3	{{ntp}}	10.254.1.21	
4	{{radius}}	10.254.1.23	
5	{{vlan_emp}}	11	
6	{{vlan_cont}}	12	
7	{{vlan_iot}}	13	
8	{{vlan_guest}}	15	
9	{{vlan_mgmt}}	3	

Save siteVariables.csv file, then drag and drop the file to Import Site Variables window. The warning message below says that you have a conflict variable (which is {{dns}}) which already exists and will be skipped. Click **Save**.

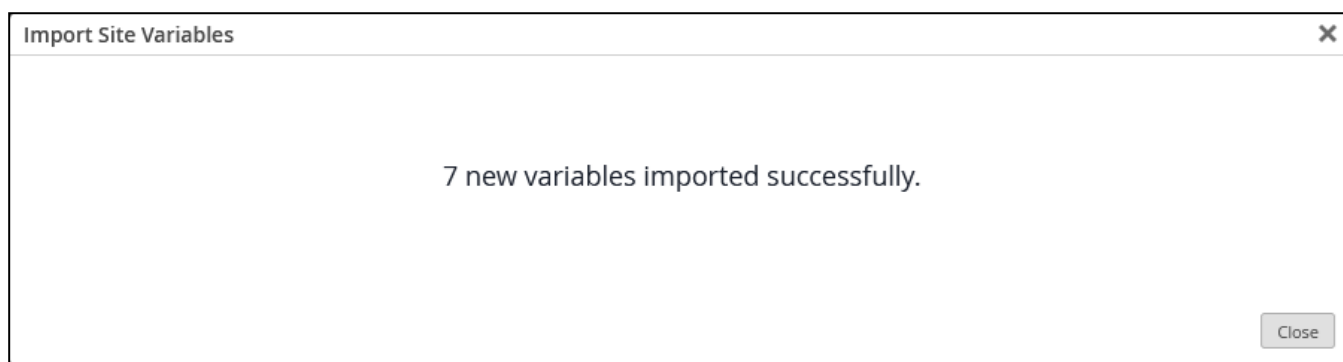
Import Site Variables
✕

Variable	Value
{{ntp}}	10.254.1.21
{{radius}}	10.254.1.23
{{vlan_emp}}	11
{{vlan_cont}}	12
{{vlan_iot}}	13
{{vlan_guest}}	15
{{vlan_mgmt}}	3

One or more site variables in the uploaded CSV conflict with existing site variables. The existing site variable values have been preserved in favor of the uploaded ones in the case of conflicts.

Save
Upload Again

Confirm that you see “7 new variables imported successfully” message. Click Close.



Review your site variables in Mist AI.

Site Variables

Add Variable Import Variables

Search 8 Variables

< 1-8 of 8 >

Variables	Values
{{dns}}	10.254.1.21
{{ntp}}	10.254.1.21
{{radius}}	10.254.1.23
{{vlan_cont}}	12
{{vlan_emp}}	11
{{vlan_guest}}	14
{{vlan_iot}}	13
{{vlan_mgmt}}	3

Click on `{{vlan_mgmt}}`. In a popup window you can change this variable or delete. Click **Cancel**.

Edit Variables

Variable

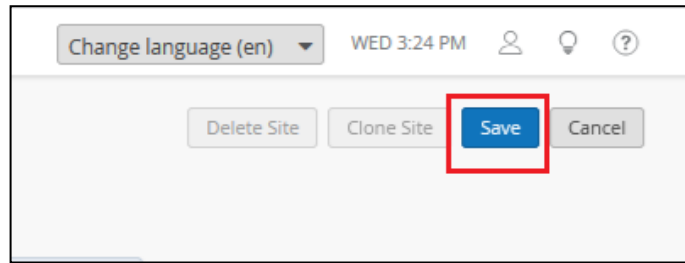
`{{vlan_mgmt}}`

Value

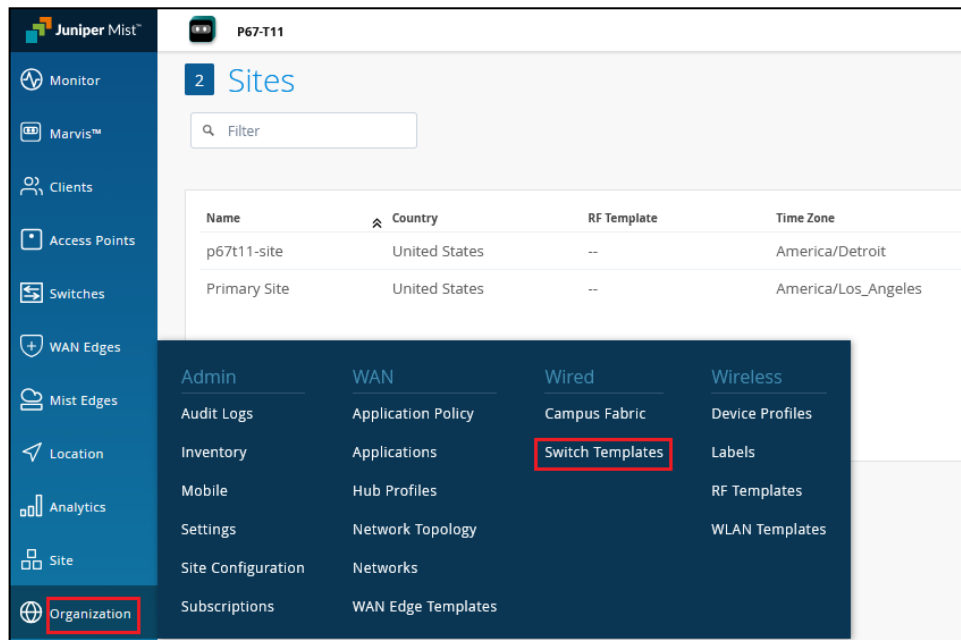
3

Delete Save Cancel

Click **Save** in the top-right corner.



Navigate to Mist AI Organization > Wired > Switch Templates and click on your template.



Replace NTP Server IP address with **{{ntp}}**, replace DNS Server IP address with **{{dns}}**. Then click on your authentication server hostname you added previously and replace with **{{radius}}**. Click the check mark.

Juniper Mist P67-T11

NAME: p67t11-swTemplate

APPLIES TO SITES: 1 sites 1 switches [Assign to Sites](#)

All Switches Configuration

AUTHENTICATION SERVERS

Authentication Servers: Radius

Authentication Servers

Edit Server ☒

Hostname / IP Address **VAR**: {{radius}}

Port: 1812

Shared Secret **ⓘ**: ***** [Reveal](#)

Timeout: 5 (0 - 1000 seconds)

Retries: 3 (0 - 100)

Enhanced Timers **ⓘ**: ☐ Enabled ☒ Disabled

Load Balance **ⓘ**: ☐ Enabled ☒ Disabled

Accounting Servers

cpm.aruba-training.com: 1813

NTP

NTP Servers **VAR**: {{ntp}}

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

DNS SETTINGS

DNS Servers **VAR**: {{dns}}

xxx.xxx.xxx.xxx or {{siteVar}}.xxx.xxx (comma-separated IPv4/IPv6 and max 5)

DNS Suffix **VAR**:

xxx.xxx.xxx.xxx or {{siteVar}}.xxx.xxx (comma-separated domains and Max 3)

SNMP

☐ Enabled ☒ Disabled

STATIC ROUTE

No static routes defined [Add Static Route](#)

CLI CONFIGURATION

Additional CLI Commands **ⓘ** **⌵**

OSPF

OSPF Areas

No areas defined [Add Area](#)

VRMP

VRMP Groups

No VRMP Groups defined [Add Group](#)

DHCP SNOOPING

☒ Enabled ☐ Disabled

☐ All Networks

Replace your accounting server hostname with **{{radius}}** variable. Click the check mark.

Juniper Mist P67-T11

All Switches Configuration

AUTHENTICATION SERVERS

Authentication Servers: Radius

Authentication Servers

{{radius}} : 1812 [Add Server](#)

Timeout: 5 (0 - 1000 seconds)

Retries: 3 (0 - 100)

Enhanced Timers **ⓘ**: ☐ Enabled ☒ Disabled

Load Balance **ⓘ**: ☐ Enabled ☒ Disabled

Accounting Servers

Edit Server ☒

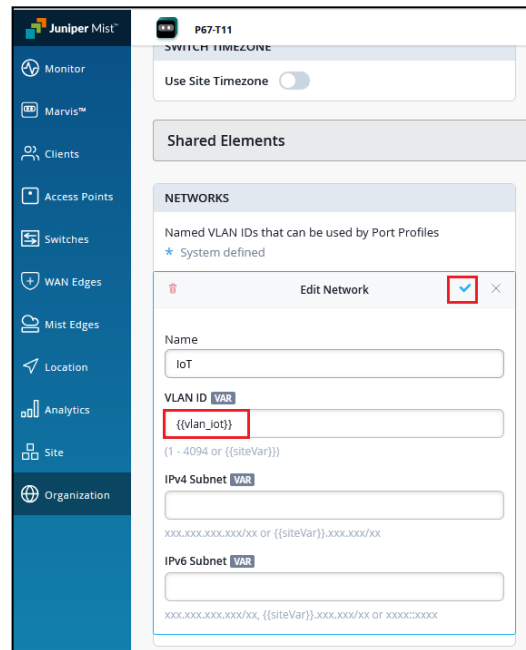
Hostname / IP Address **VAR**: {{radius}}

xxx.xxx.xxx.xxx or {{siteVar}}.xxx.xxx

Port: 1813

Shared Secret **ⓘ**: ***** [Reveal](#)

Scroll down the page to Shared Elements. Click on IoT network and replace VLAN ID 13 with **{{vlan_iot}}**. Click the check mark.



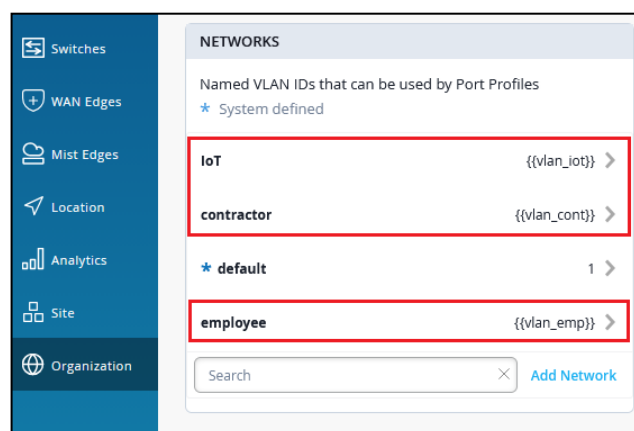
Edit contractor network and replace VLAN 12 with variable **{{vlan_cont}}**. Click the check mark.

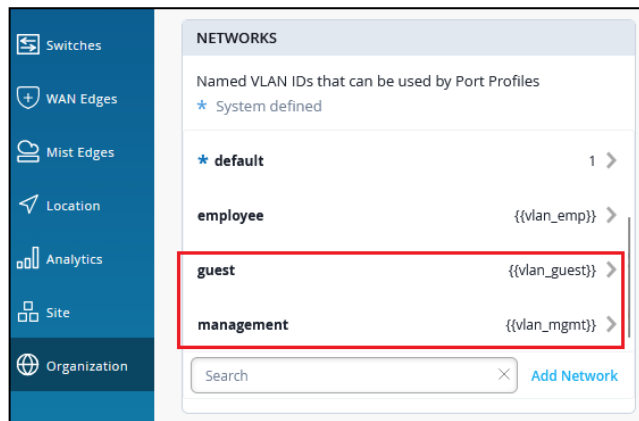
Edit employee network and replace VLAN 11 with variable **{{vlan_emp}}**. Click the check mark.

Edit guest network and replace VLAN 13 with variable **{{vlan_guest}}**. Click the check mark.

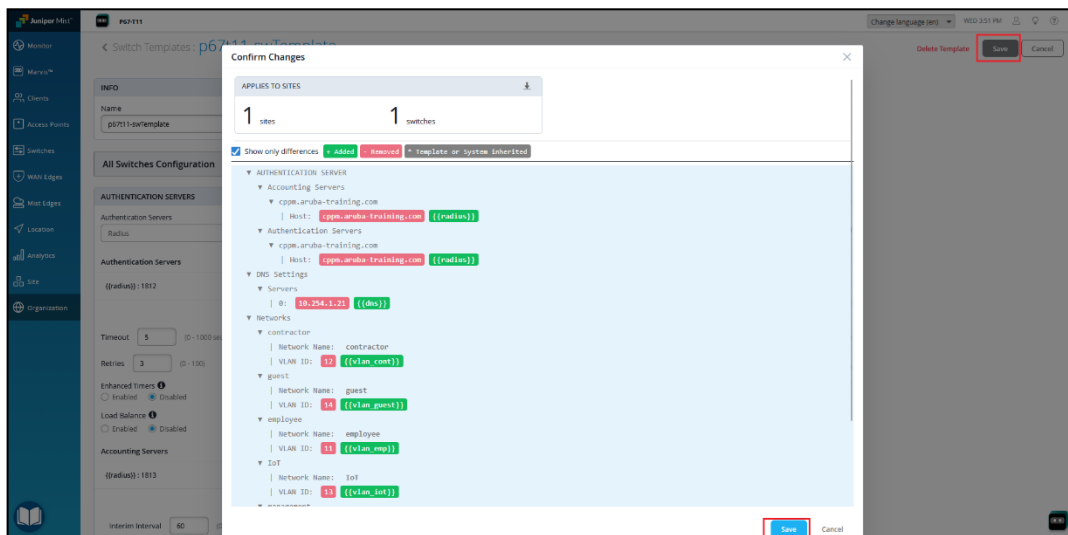
Edit management network and replace VLAN 3 with variable **{{vlan_mgmt}}**. Click the check mark.

Confirm that you changed all 5 networks to use variables.





Scroll up the page, click **Save** to apply new settings and click **Save** again to confirm changes.



Navigate to Mist AI Switches > sw-edge2, wait a couple of minutes, then refresh the page and confirm that it shows 100% Config Success.

Juniper Mist P67-T11

< Switches: sw-edge2

Front Panel Port List

EX4100-F-12T

CPU Memory Temp PoE PSUs Fans

Metrics: Switch-AP Affinity, PoE Compliance, VLANs, Version Compliance (100%), Switch Uptime (100%), Config Success (100%), Potential Anomalies (100%)

Properties:

INSIGHTS	Switch Insights
LOCATION	not on floorplan
MAC ADDRESS	20:93:39:01:2f:00
DEVICE ID	209339012f00
MODEL	EX4100-F-12T
VERSION	22.4R3.25
TEMPLATE	p67t11-swTemplate
SWITCH PHOTOS	

Statistics:

STATUS	Connected
IP ADDRESS	10.251.1.10 (vme.0) 10.1.3.10 (vlan 3)
MIST APS	0
WIRELESS CLIENTS	
TOTAL POWER DRAW	0.00 W
UPTIME	6d 2h 58m
LAST SEEN	May 13, 2026 3:52:54 PM
LAST DISCONNECT REASON	Default Gateway Unreachable
LAST CONFIG	May 13, 2026 3:52:16 PM

Switch Configuration

Configuration is Managed by Mist

Disable Configuration Management

Click Utilities > Remote Shell.

Change language (en) WED 3:57 PM

Locate Utilities Save Close

Testing Tools

Remote Shell

Send Switch Log to Mist

Upgrade Firmware

Snapshot Device

Sync Configuration

Download Config

Replace Switch

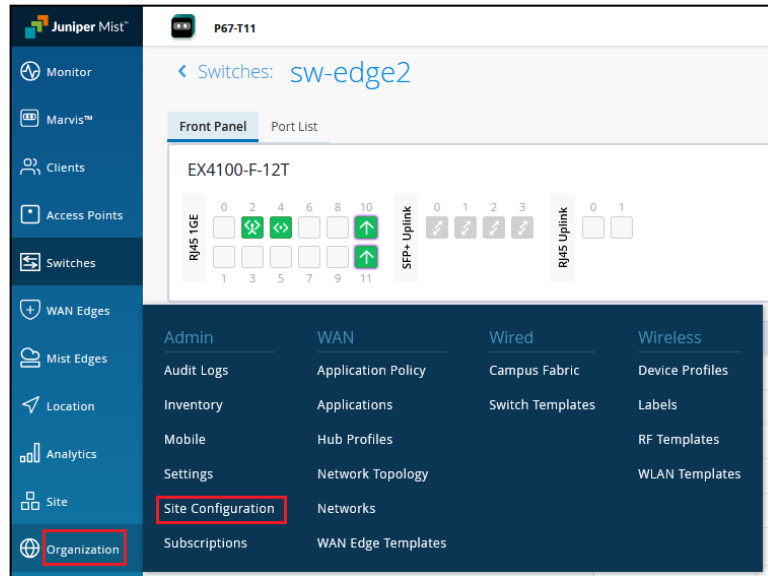
Reboot Switch

Type “show vlans” command and check VLAN ID used for guest VLAN name where you should see 14.
Close Remote Shell.

```
mist@sw-edge2> show vlans guest
```

Routing instance default-switch	VLAN name guest	Tag 14	Interfaces ae1.0* ge-0/0/2.0*
{master:0}			

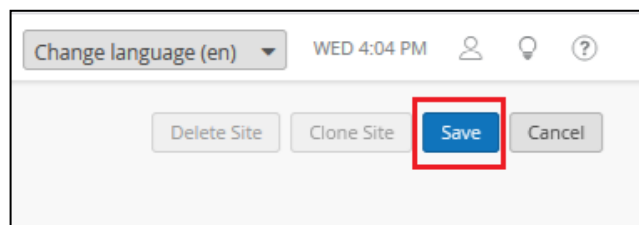
Navigate in Mist AI to Organization > Site Configuration and select your site.



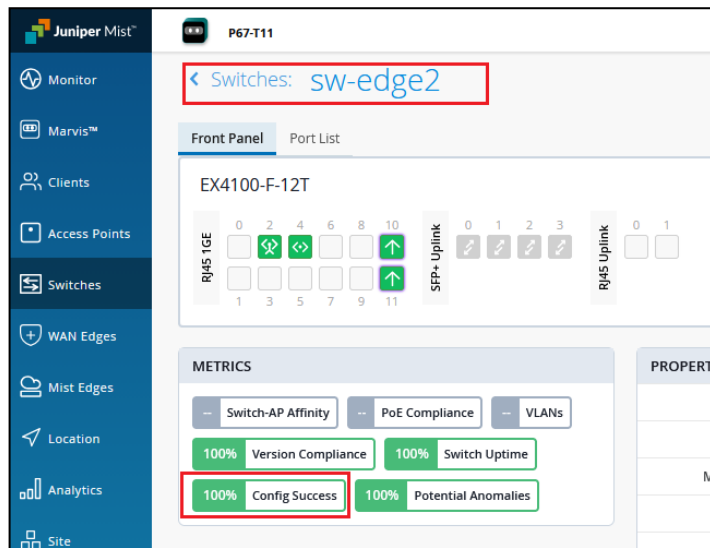
Click on {{vlan_guest}} variable and change the value to 15. Click **Save**.

 The screenshot shows a dialog box titled 'Edit Variables' with a close button (X) in the top right corner. Inside the dialog, there are two input fields. The first field is labeled 'Variable' and contains the text '{{vlan_guest}}'. The second field is labeled 'Value' and contains the number '15'. At the bottom right of the dialog, there are three buttons: 'Delete', 'Save' (highlighted with a red box), and 'Cancel'.

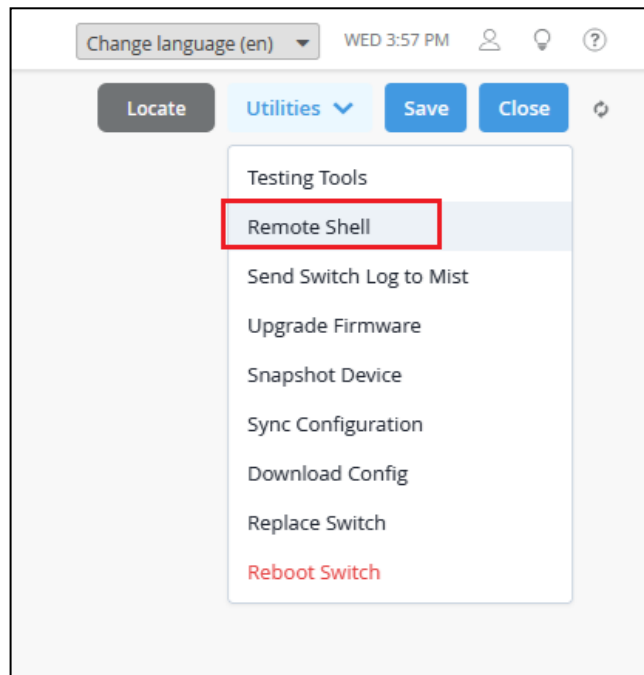
Click **Save** at the top of the page.



Navigate in Mist AI to Switches > sw-edge2 and confirm that it shows 100% Config Sync.



Click Utilities > Remote Shell.



Type Command “show vlans guest”. You should see that VLAN ID has changed to 15 and it’s tagged on the uplink and port 2. Close Remote Shell.

```
mist@sw-edge2> show vlans guest
```

Routing instance	VLAN name	Tag	Interfaces
default-switch	guest	15	ae1.0* ge-0/0/2.0*

```
{master:0}
```

Task 5-2: Use CLI Configuration in Mist AI

Objectives

Use Site/Template CLI Configuration.

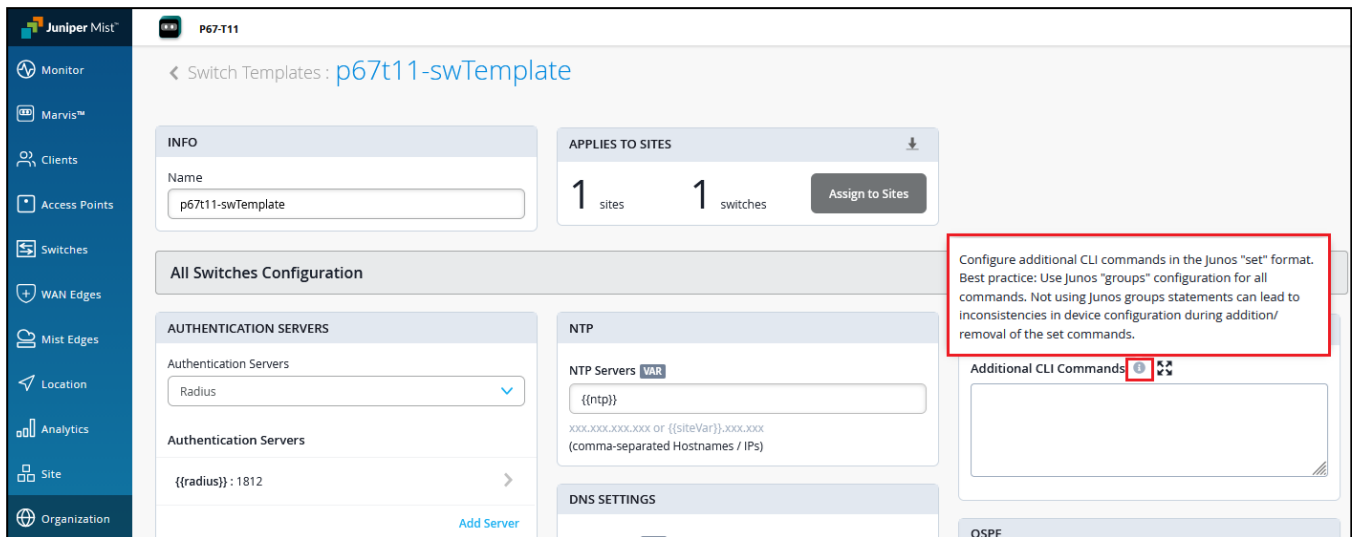
Use Additional CDLI configuration.

Validate CLI configuration applied with Junos groups.

Steps

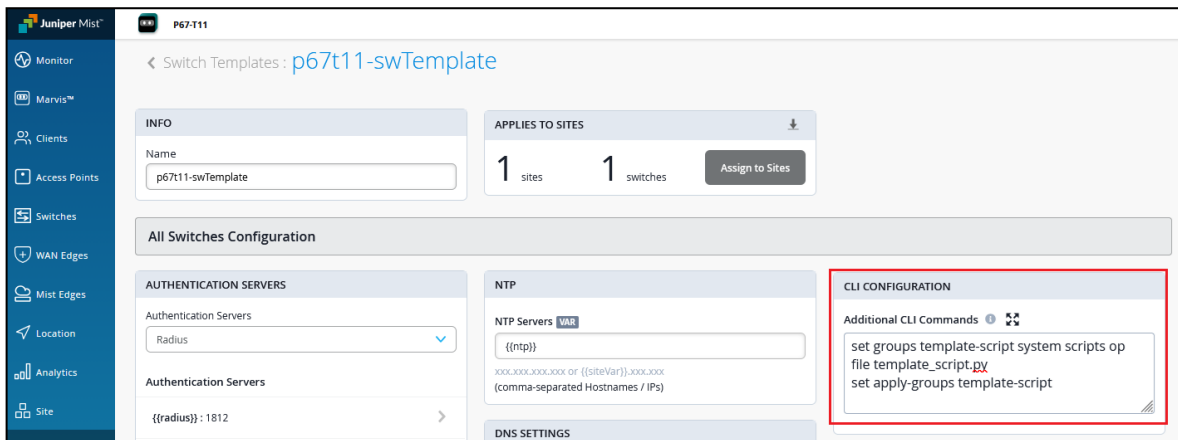
You can apply additional CLI commands to individual switch, or site, or organization switch template, or with select switches configuration (Rule-based). Navigate to Organization > Wired > Switch Templates and select your template. Hover your mouse over information icon next to Additional CLI Commands and read the text.

NOTE: Additional CLI commands in Juniper Mist allow you to configure settings beyond what's available in the GUI. Here are key use cases: Custom System Configuration, Advanced Networking Features such as custom QoS settings, Virtual Chassis Management, Port-Level Customization, Hierarchical Configuration, Integration & Extensibility. Additional CLI commands take precedence over GUI-based configurations, so manage them carefully to avoid conflicts with template-based settings.

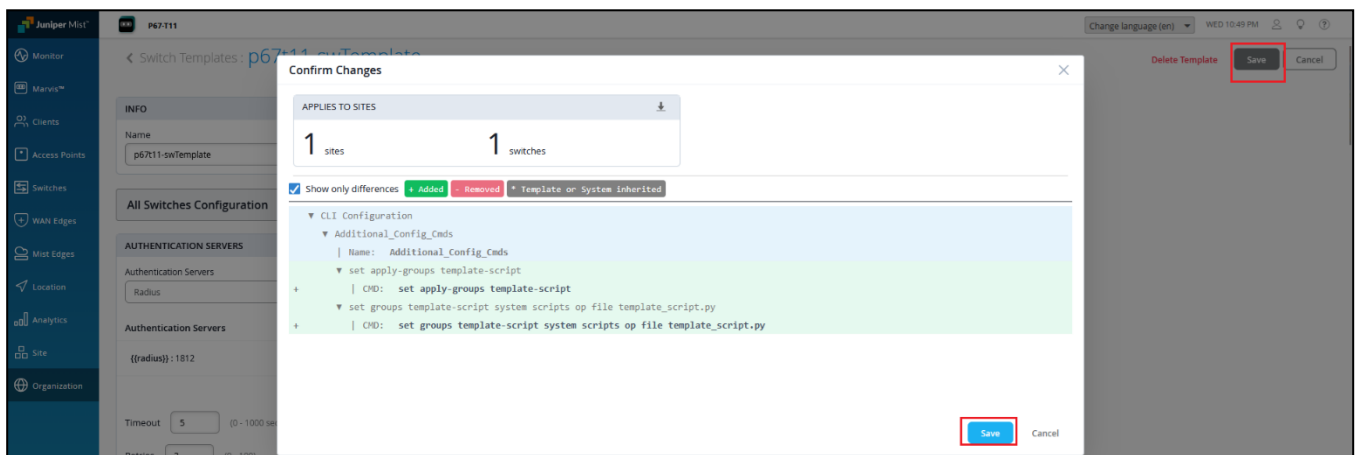


Enter following commands to CLI Configuration.

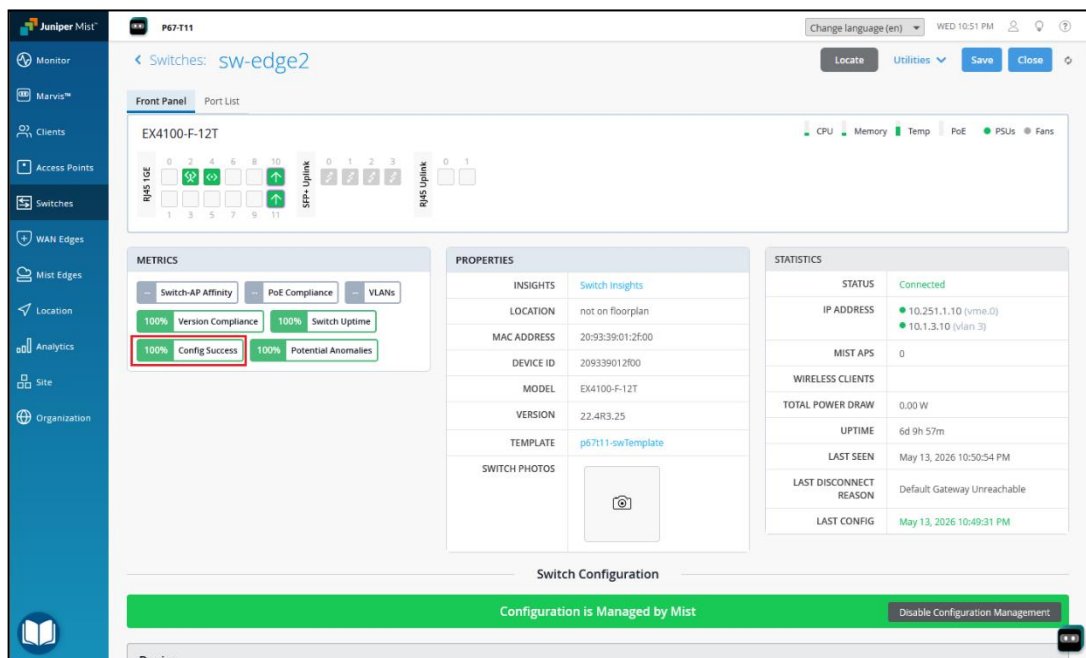
```
set groups template-script system scripts op file template_script.py
set apply-groups template-script
```



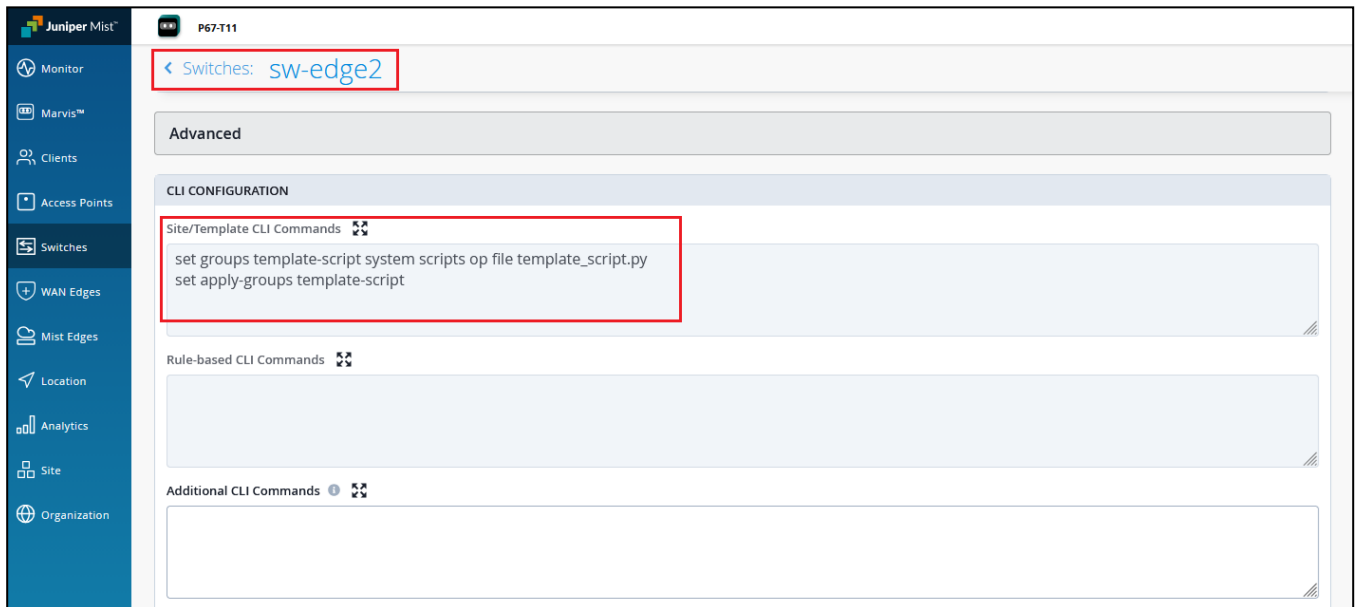
Click **Save** at the top of the page and then click **Save** again to confirm changes.



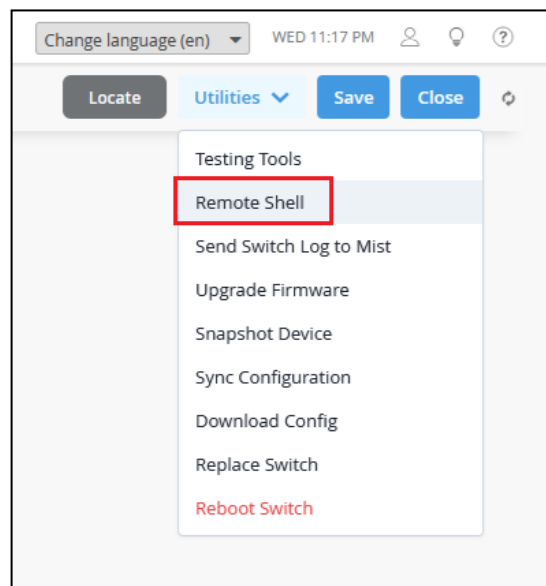
Navigate to Mist AI Switches > sw-edge2, wait a couple of minutes and refresh the page. You should see 100% Config Success.



Scroll down the page to Advanced section where you will find CLI configuration pushed from the switch template.



Click Utilities > Remote Shell



Check that your configuration was pushed to the switch with “show configuration groups template-script” command.

```
mist@sw-edge2> show configuration groups template-script
system {
  scripts {
    op {
      file template_script.py;
    }
  }
}
```

```
{master:0}
```

Confirm that group was applied with “show configuration apply-groups” command.

```
mist@sw-edge2> show configuration apply-groups
## Last commit: 2026-05-14 02:49:49 UTC by mist
apply-groups [ mist-script top template-script ];

{master:0}
```

Check system scripts configuration hierarchy. Group commands are not displayed in the configuration hierarchy.

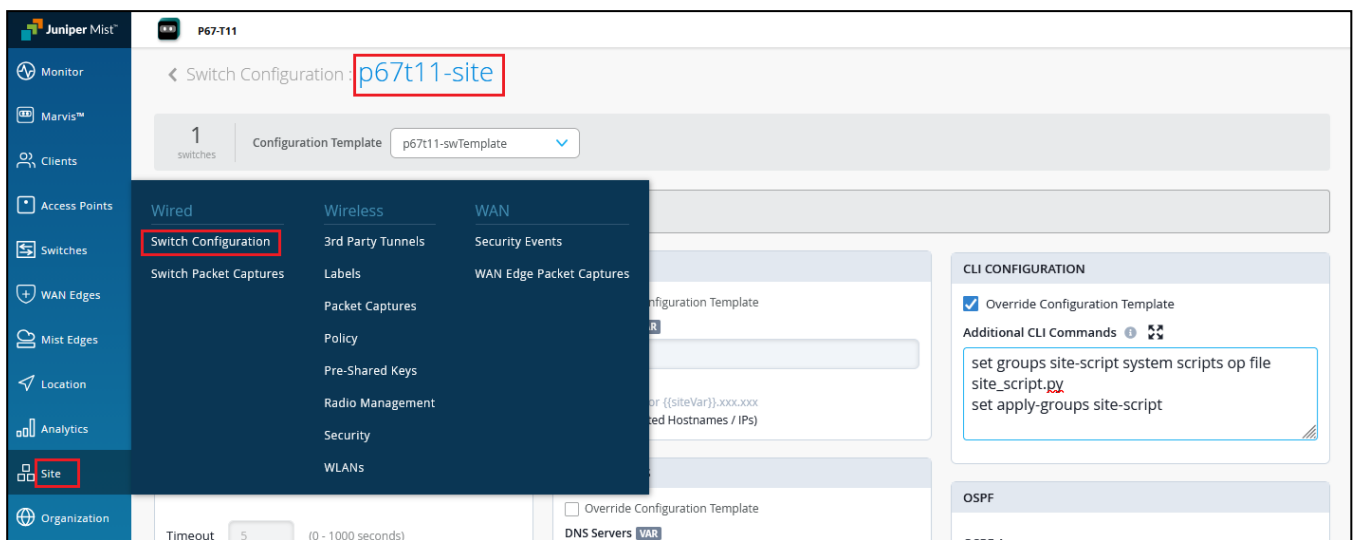
```
mist@sw-edge2> show configuration system scripts
language python3;
synchronize;

{master:0}
```

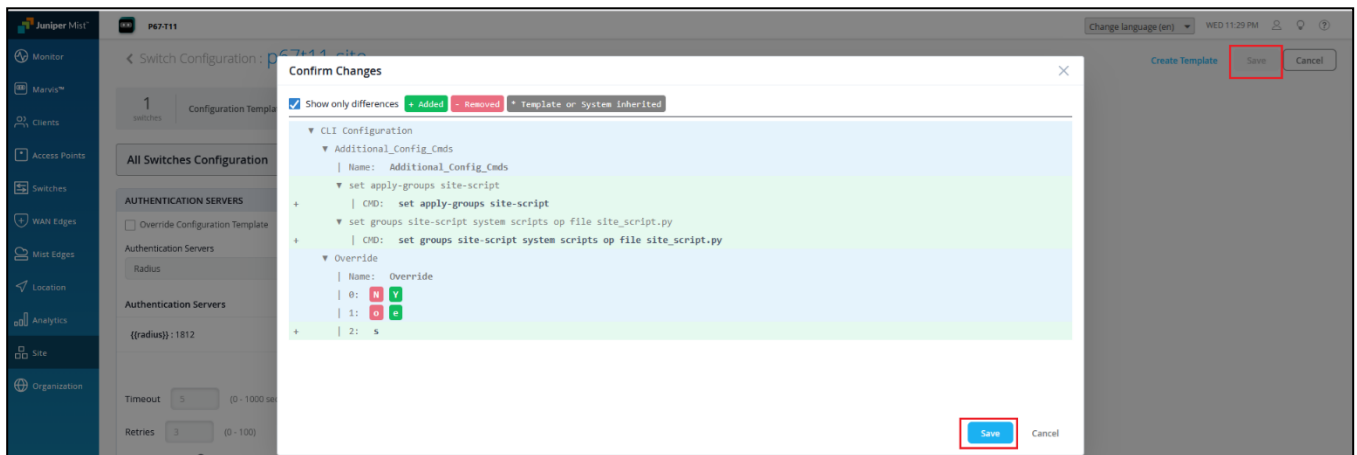
Check system scripts inherited configuration with “show configuration system scripts | display inheritance” command. Then close Remote Shell window.

```
mist@sw-edge2> show configuration system scripts | display inheritance
##
## 'commit' was inherited from group 'mist-script'
##
<Output omitted>
##
## 'template_script.py' was inherited from group 'template-script'
##
file template_script.py;
}
language python3;
synchronize;
```

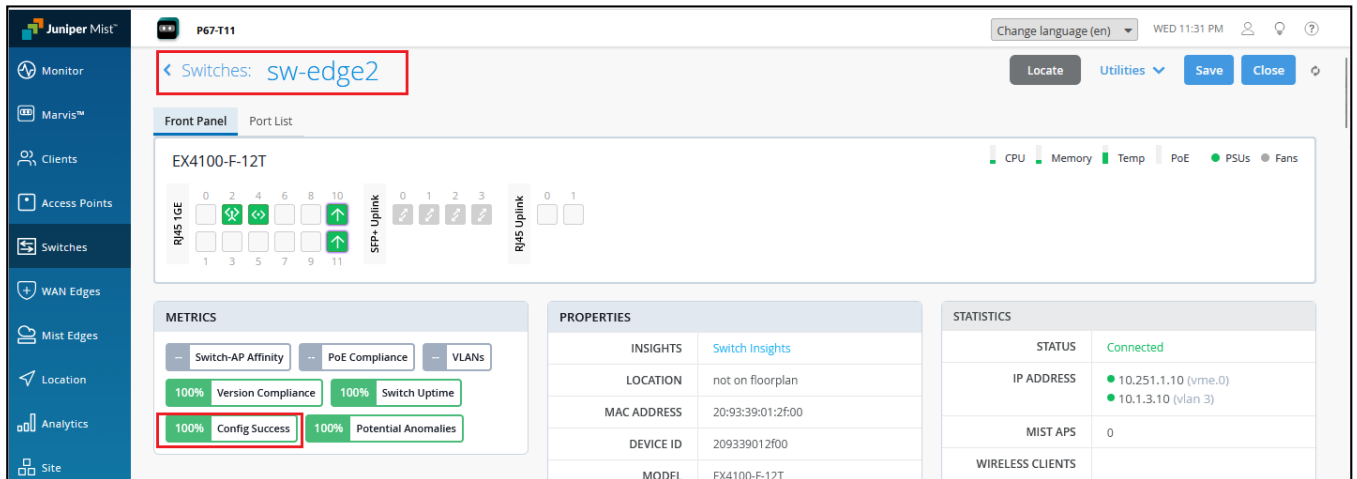
Navigate in Mist AI to Site > Wired > Switch Configuration. Enable checkbox Override Configuration Template and replace “template” with “site” three times. Compare your result with the screenshot below.



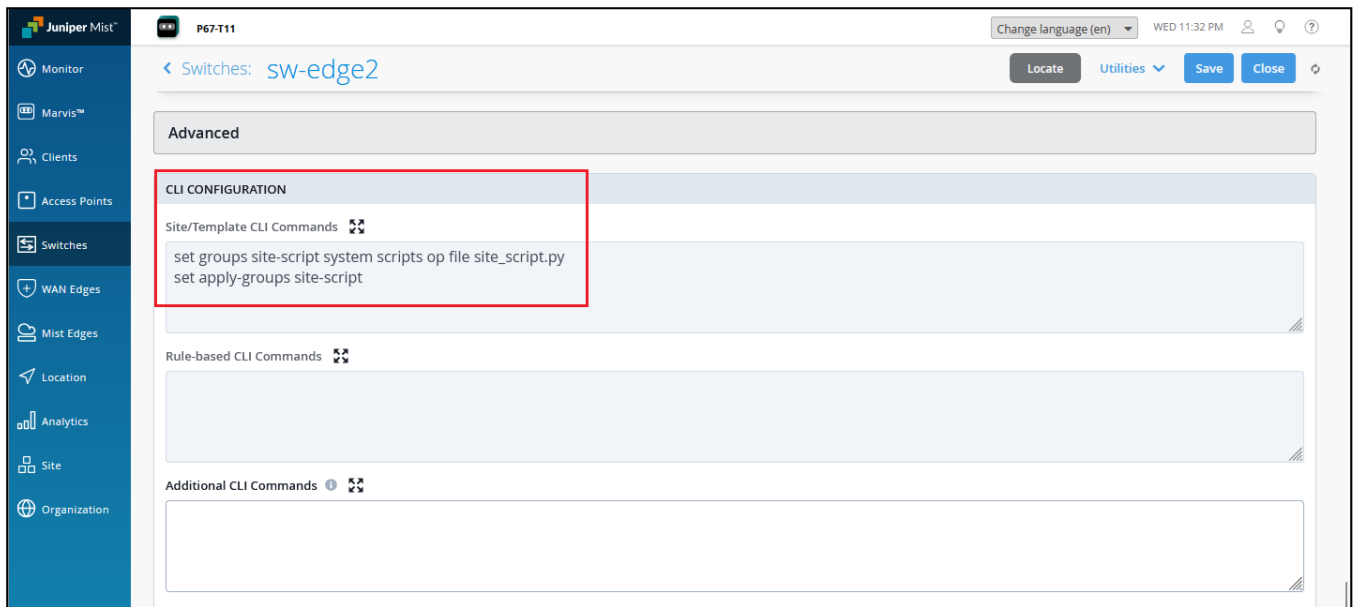
Click **Save** in the top-right corner to apply new settings and click **Save** again to confirm changes.



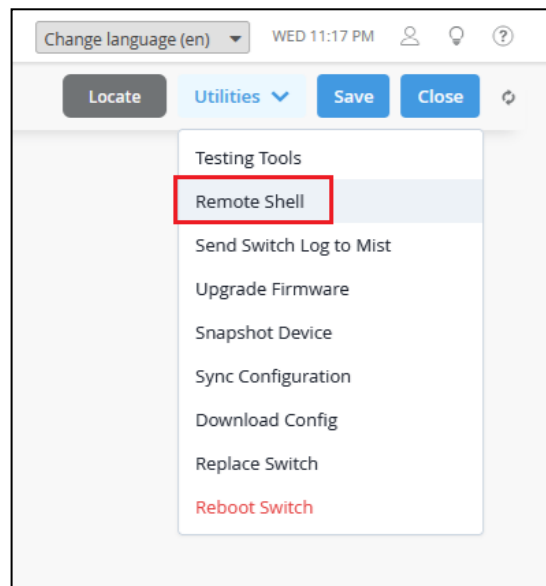
Navigate in Mist AI to Switches > sw-edge2, wait a couple of minutes and refresh the page. Confirm that you can see 100% Config Success.



Scroll down the page to Advanced section where you will see site-script replaced template-script.



Click Utilities > Remote Shell.



Check Groups configuration and search for “script” word with “show configuration groups | match script” command. As you should see, template-script was replaced with site-script.

```
mist@sw-edge2> show configuration groups | match script
mist-script {
  scripts {
    event-script mist_critical_events.py;
    event-script mist_redirect_to_oc_term.py;
  }
  event-script {
    python-script-user mist;
    python-script-user mist;
    file escript.log {
    file op-script.log {
  }
}
site-script {
```

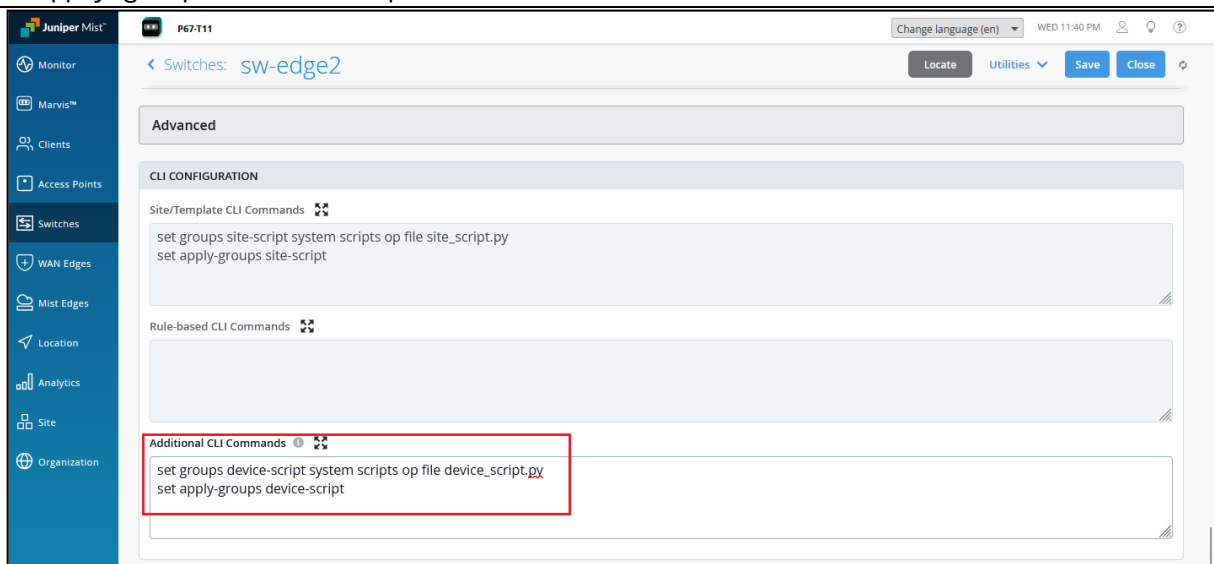
```
scripts {  
    file site_script.py;  
}  
{master:0}
```

Compare current configuration with previous version using “show configuration | compare rollback 1” command. Command lines with “-” symbol indicate deleted configuration. Close Remote Shell.

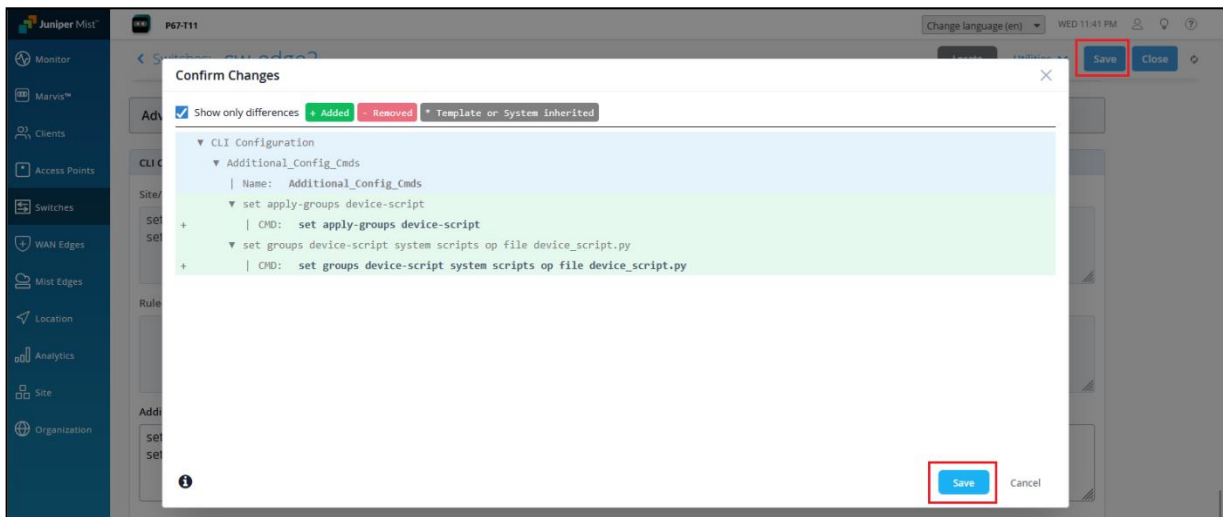
```
mist@sw-edge2> show configuration | compare rollback 1  
[edit groups]  
top { ... }  
+ site-script {  
+     system {  
+         scripts {  
+             op {  
+                 file site_script.py;  
+             }  
+         }  
+     }  
+ }  
- template-script {  
-     system {  
-         scripts {  
-             op {  
-                 file template_script.py;  
-             }  
-         }  
-     }  
- }  
[edit]  
- apply-groups [ mist-script top template-script ];  
+ apply-groups [ mist-script top site-script ];  
{master:0}
```

Add the following commands to the Additional CLI Commands field.

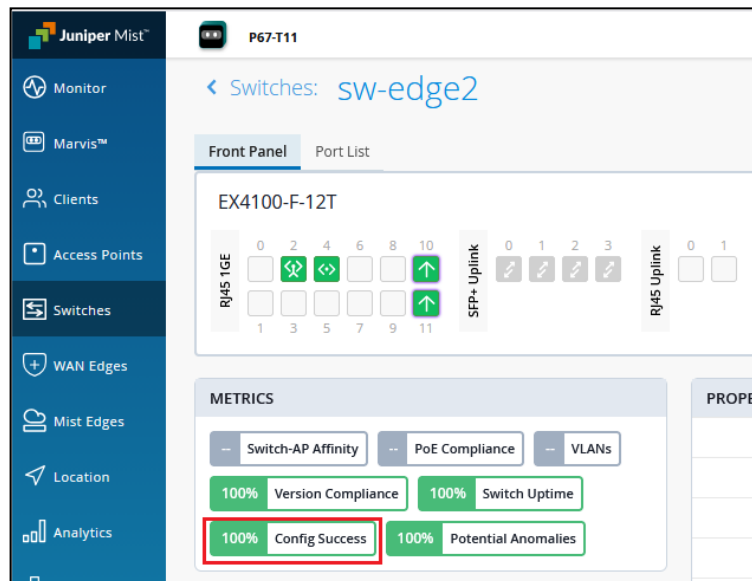
```
set groups device-script system scripts op file device_script.py  
set apply-groups device-script
```



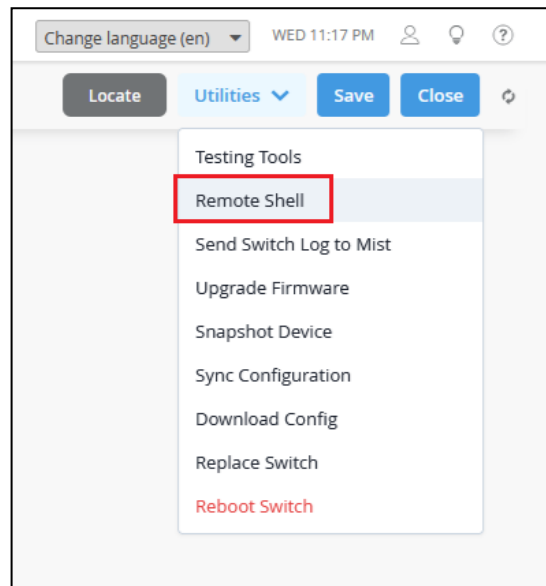
Click **Save** to apply new configuration and click **Save** again to confirm changes.



Wait a couple of minutes and refresh the page. Confirm that you can see 100% Config Success.



Click Utilities > Remote Shell.



Check Groups configuration and search for “script” word with “show configuration groups | match script” command. You should see both site-script and device-script listed.

```
mist@sw-edge2> show configuration groups | match script
mist-script {
    scripts {
        event-script mist_critical_events.py;
        event-script mist_redirect_to_oc_term.py;
    }
    event-script {
        python-script-user mist;
        python-script-user mist;
    }
    file escript.log {
    }
    file op-script.log {
    }
    site-script {
        scripts {
            file site_script.py;
        }
    }
    device-script {
        scripts {
            file device_script.py;
        }
    }
}
{master:0}
```

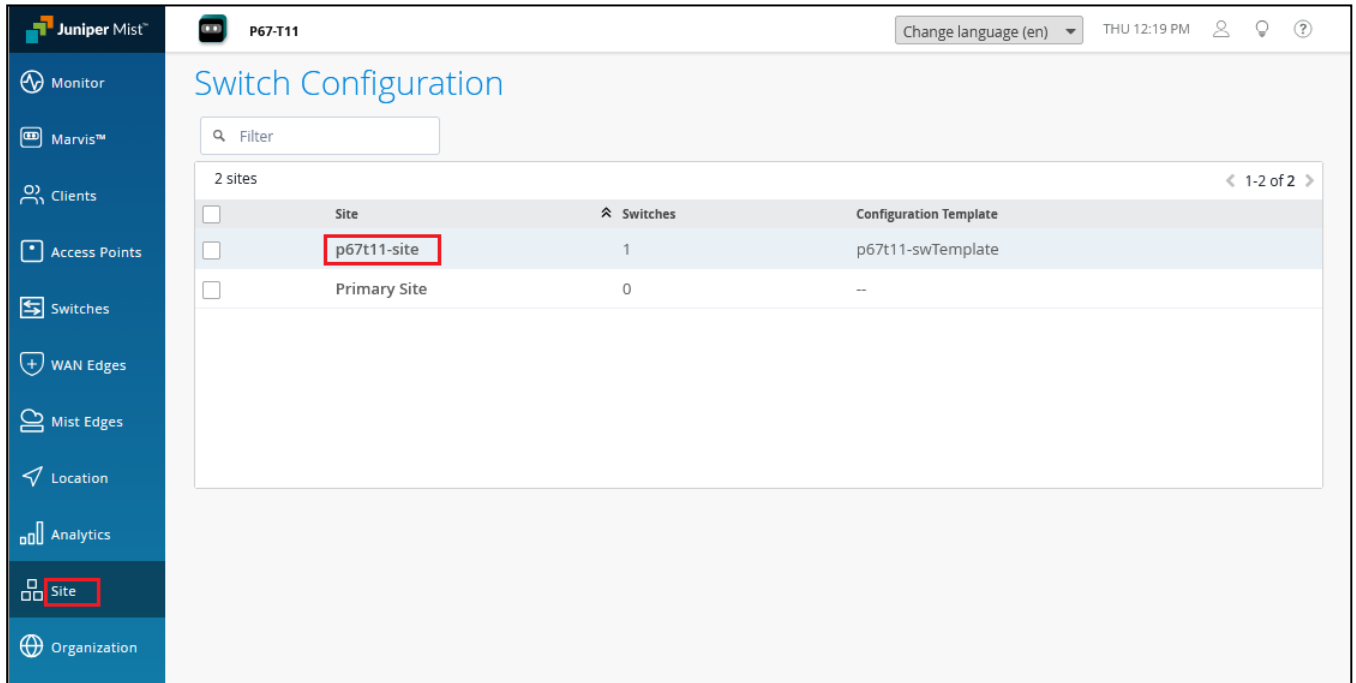
Check system scripts inherited configuration to confirm that you have both site and device scripts.
Close Remote Shell window.

```
mist@sw-edge2> show configuration system scripts | display inheritance
##
## 'commit' was inherited from group 'mist-script'
##
<Output omitted>

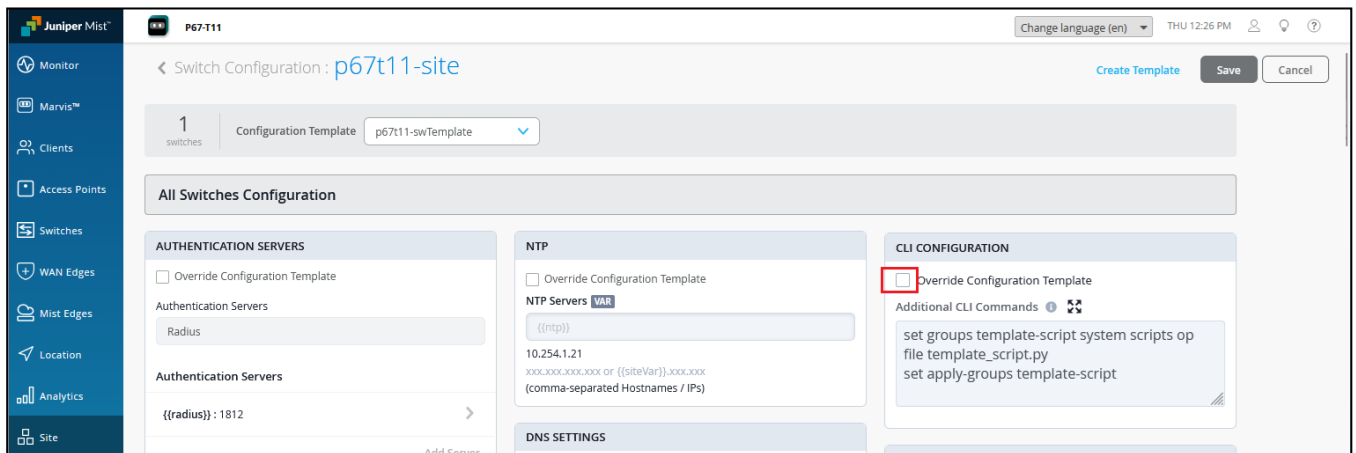
##
## 'site_script.py' was inherited from group 'site-script'
##
file site_script.py;
##
## 'device_script.py' was inherited from group 'device-script'
```

```
##
file device_script.py;
}
language python3;
synchronize;
```

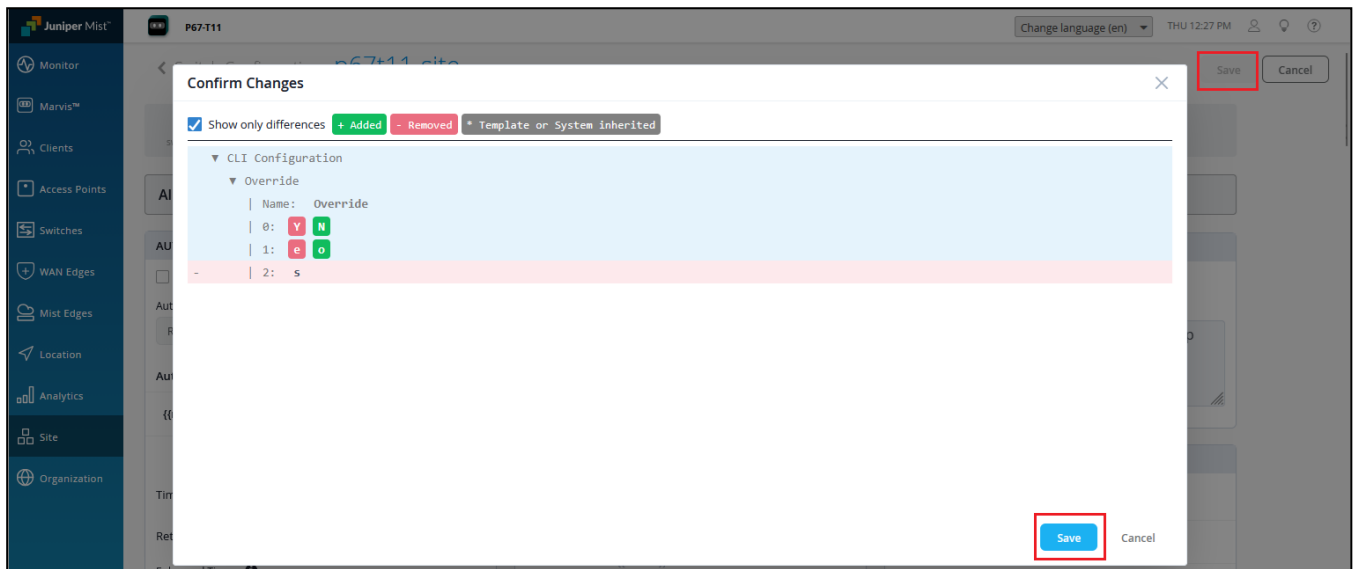
Navigate to Site > Wired > Switch Configuration



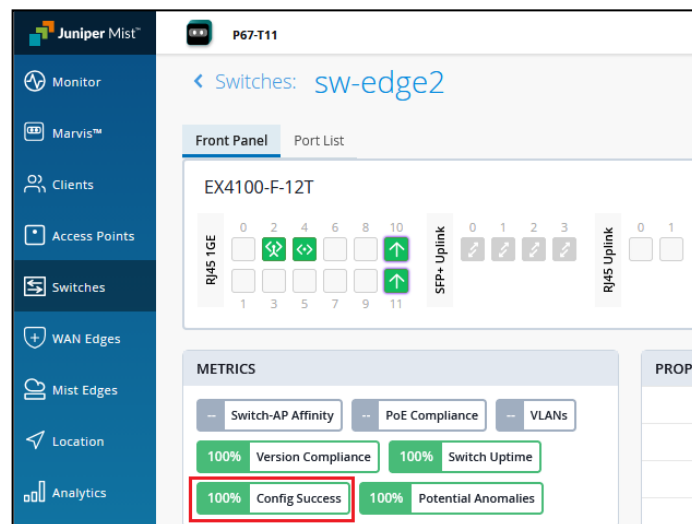
In CLI Configuration section uncheck the checkbox “Override Configuration Template”.



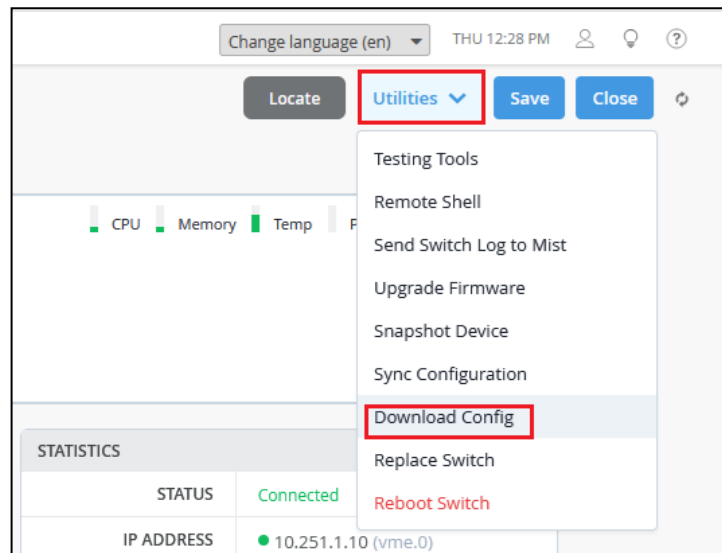
Click Save in the top-right corner and then click Save again to confirm changes.



Navigate in Mist AI to Switches > sw-edge2. Wait a couple of minutes, refresh the page and confirm that you see 100% Config Success.



Click Utilities > Download Config.



Open downloaded file and check CLI commands at the bottom. You should see that site-script was removed, and template-script was pushed to the switch.

```
set groups template-script system scripts op file template_script.py
set apply-groups template-script
set groups device-script system scripts op file device_script.py
set apply-groups device-script
```


Task 5-3: Use Select Switches Configuration

Objectives

Use Select Switches Configuration in Organization Switch Templates with switch roles.

Override Select Switches Configuration in Sites with switch model.

Apply Rule-based CLI configuration with Select Switches Configuration.

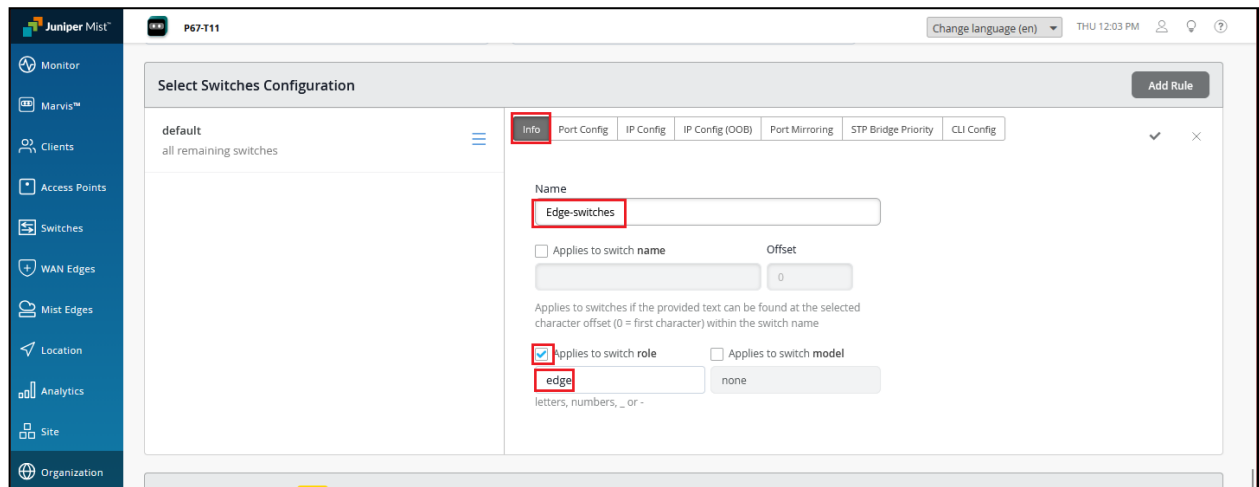
Steps

You can use Select Switches Configuration at the Organization level with Switch Templates or at the Site level. Navigate to Organization > Wired > **Switch Templates** and select your switch template. Scroll to the Select Switches Configuration section and click **Add Rule**.

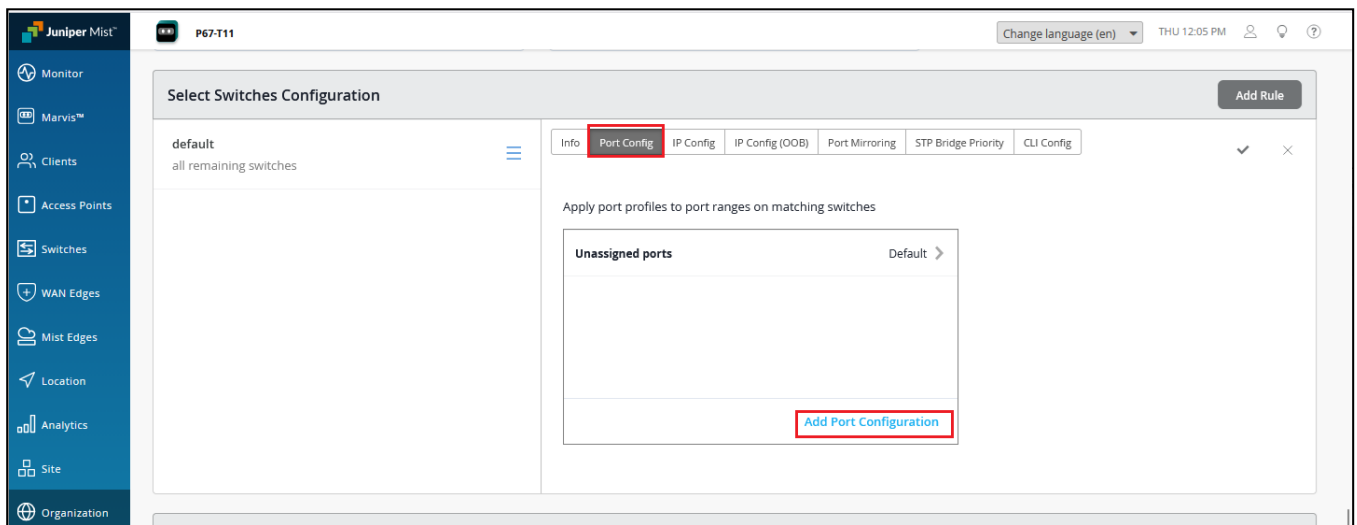
The screenshot shows the Juniper Mist web interface. On the left sidebar, the 'Organization' menu item is highlighted. The main content area is titled 'Select Switches Configuration'. A red box highlights the 'Add Rule' button in the top right corner. Below the title bar, there are tabs for 'Info', 'Port Config', 'IP Config', 'IP Config (OOB)', 'Port Mirroring', 'STP Bridge Priority', and 'CLI Config'. The 'Info' tab is selected. The form for creating a rule is displayed. It includes a 'Name' field with a placeholder 'Rule name'. Below this is a checkbox labeled 'Applies to switch name' and an 'Offset' field with a value of '0'. A note states: 'Applies to switches if the provided text can be found at the selected character offset (0 = first character) within the switch name'. There are two more checkboxes: 'Applies to switch role' and 'Applies to switch model'. The 'Applies to switch role' dropdown is set to 'edge'. The 'Applies to switch model' dropdown is set to 'none'. At the bottom of the form, there is a 'Switch Policy Labels' section with a 'BETA' tag.

You can apply Port Config, IP Config, Port Mirroring, STP Bridge Priority or CLI Config to a group of switches based on switch name, role or model.

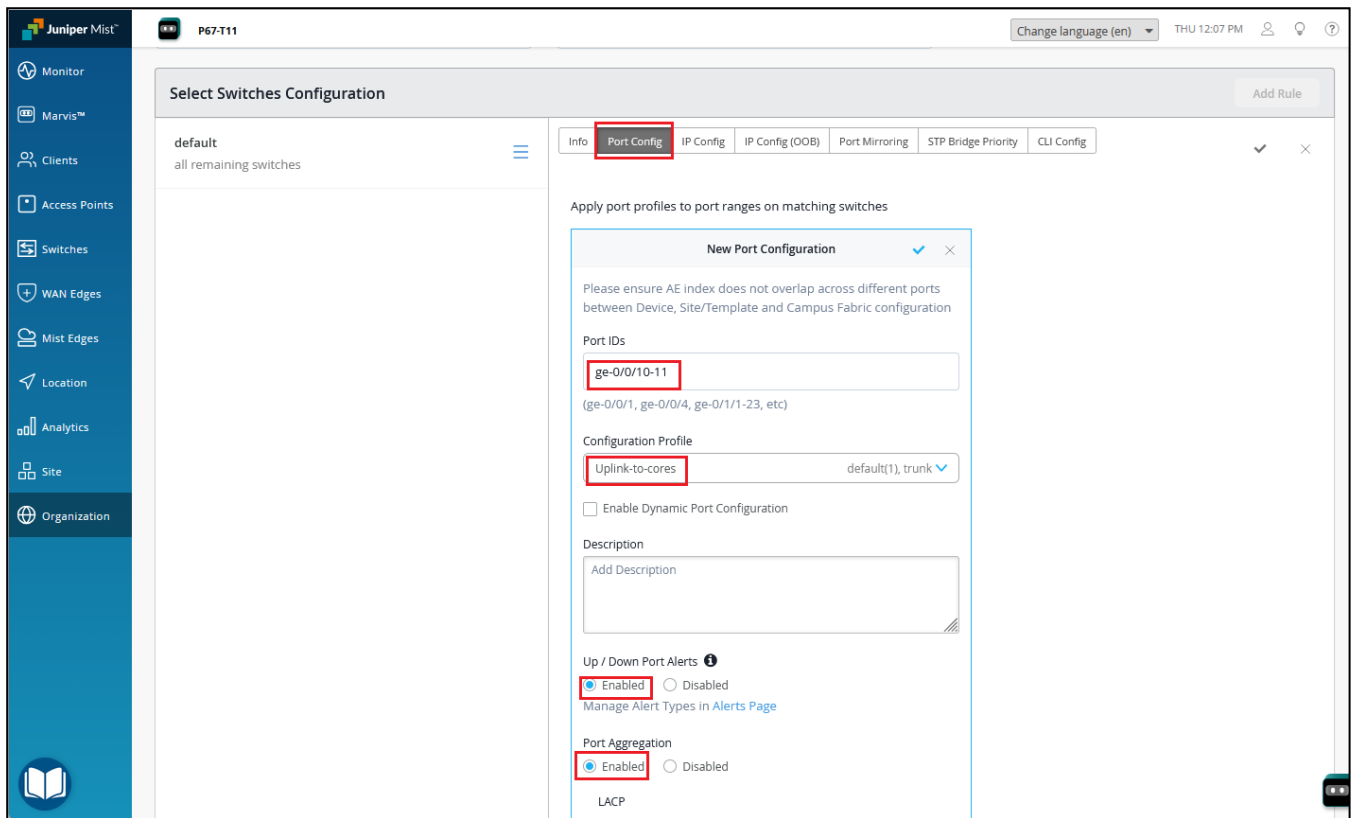
In this Lab you will use switch roles to select switches. In Info tab, give this rule name Edge-switches, enable checkbox “Applies to switch role” and select edge.



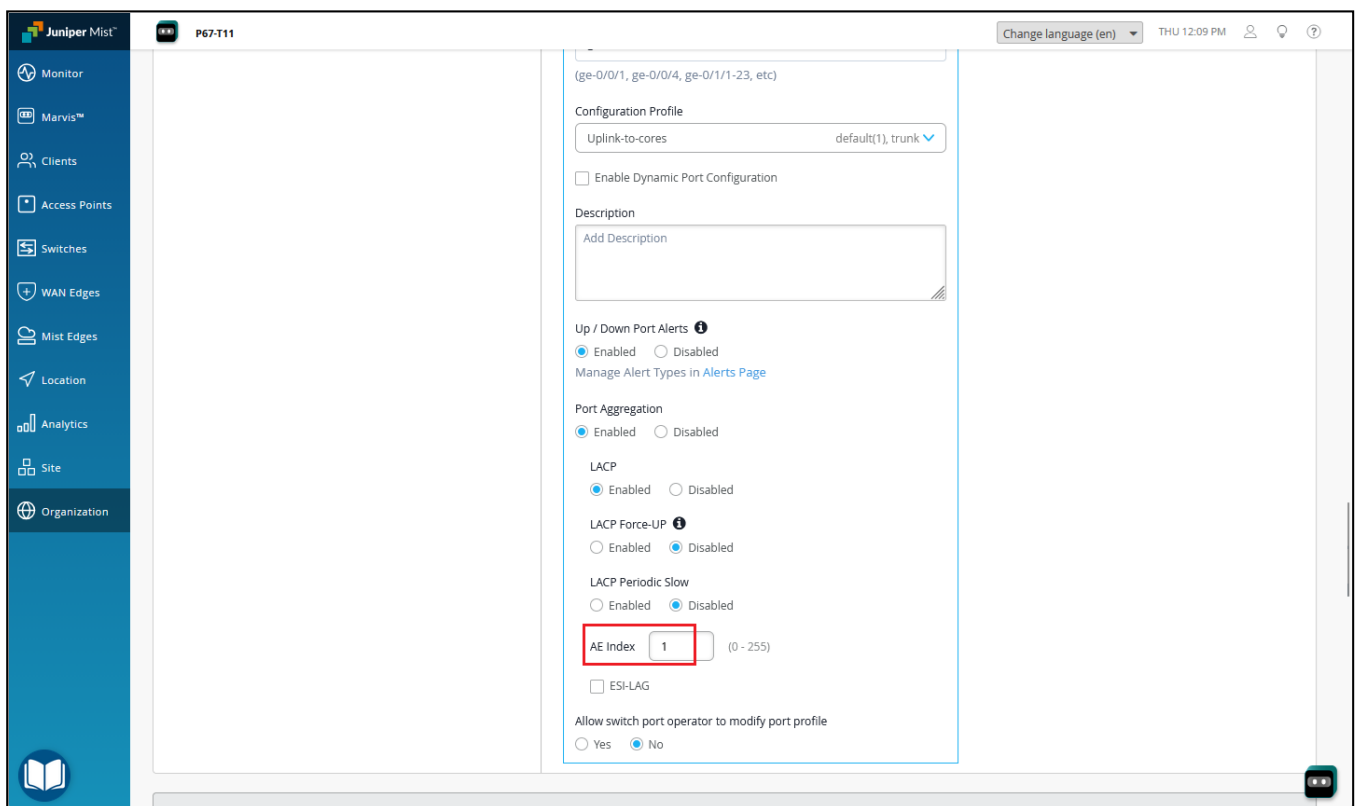
Switch to Port Config tab and click Add Port Configuration.



Add Port IDs ge-0/0/10-11 to configure your switch uplinks, select Configuration Profile “Uplinks-to-cores”, enable Up/Down Port Alerts and enable Port Aggregation.

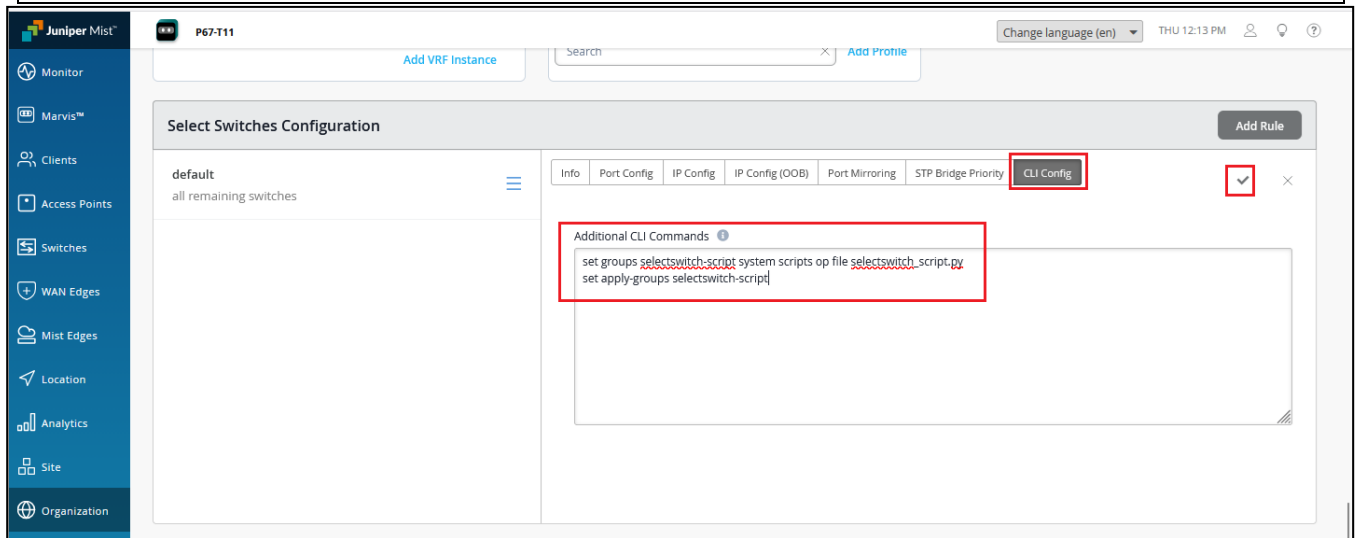


Scroll down the page and type 1 in AE Index. Then Scroll up and click the **check mark** in New Port configuration window.

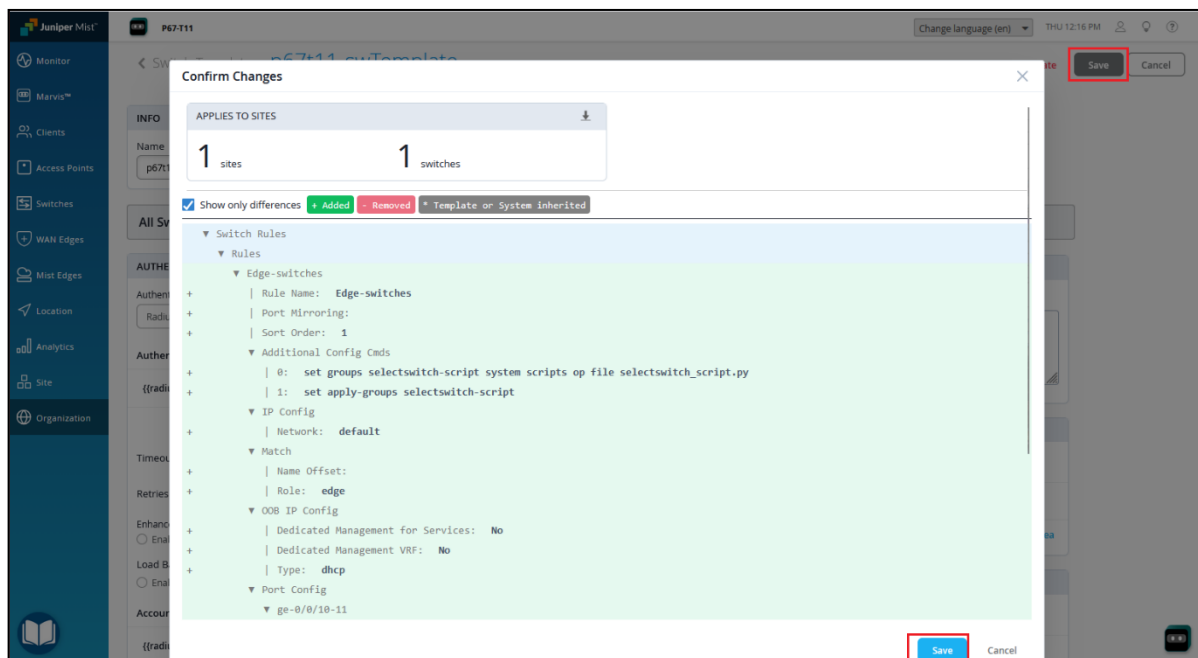


At this point you just added a single Port Configuration for uplinks and didn't add any settings for ports 4 and 2 where you have PC4 and Juniper access point connected. Switch to CLI Config tab and enter these CLI commands and click the check mark to save new rule.

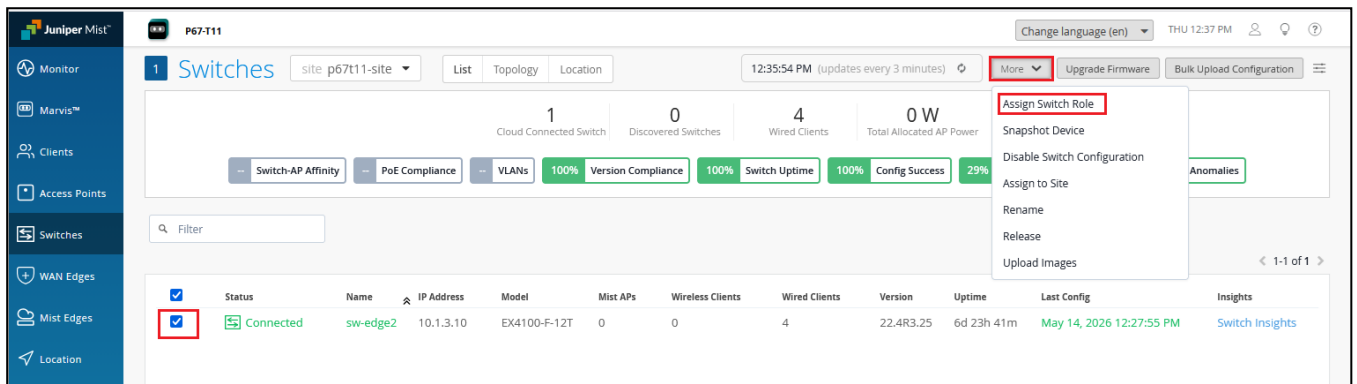
```
set groups selectswitch-script system scripts op file selectswitch_script.py
set apply-groups selectswitch-script
```



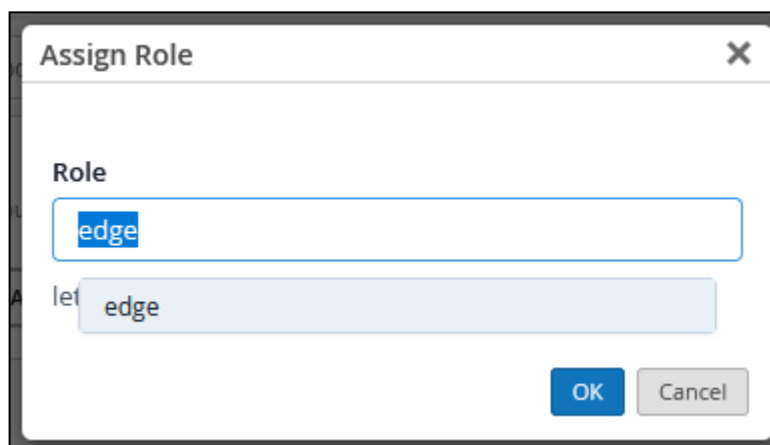
Scroll up the page to the top and click **Save** to apply new settings, then click **Save** to confirm changes.



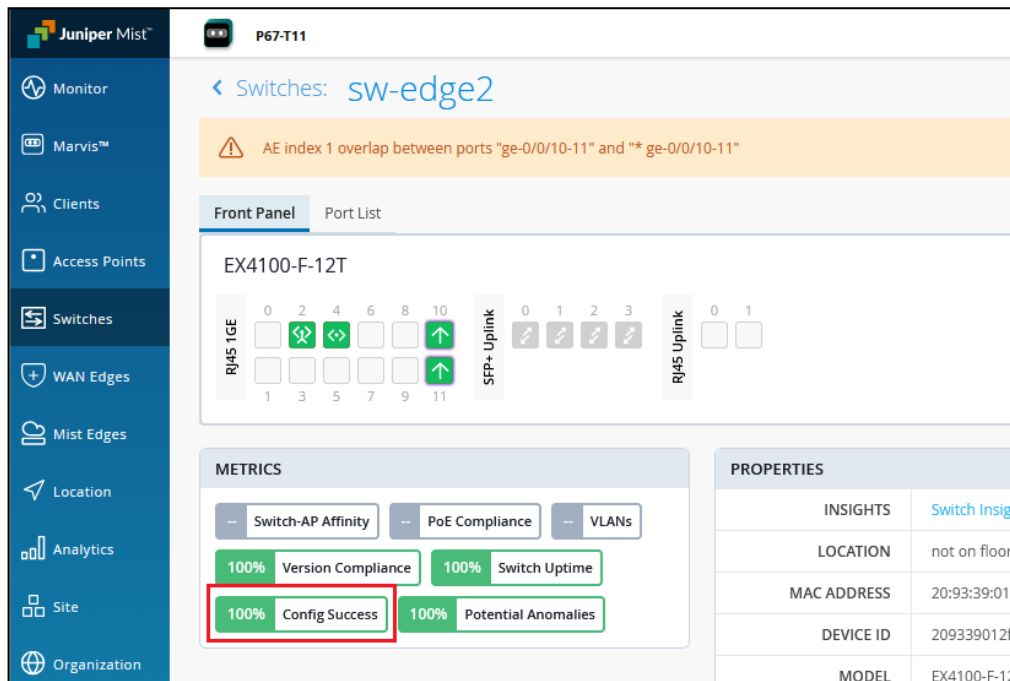
Navigate in Mist AI to Switches and click the checkbox next to your switch. Then click More at the top and select Assign Switch Role.



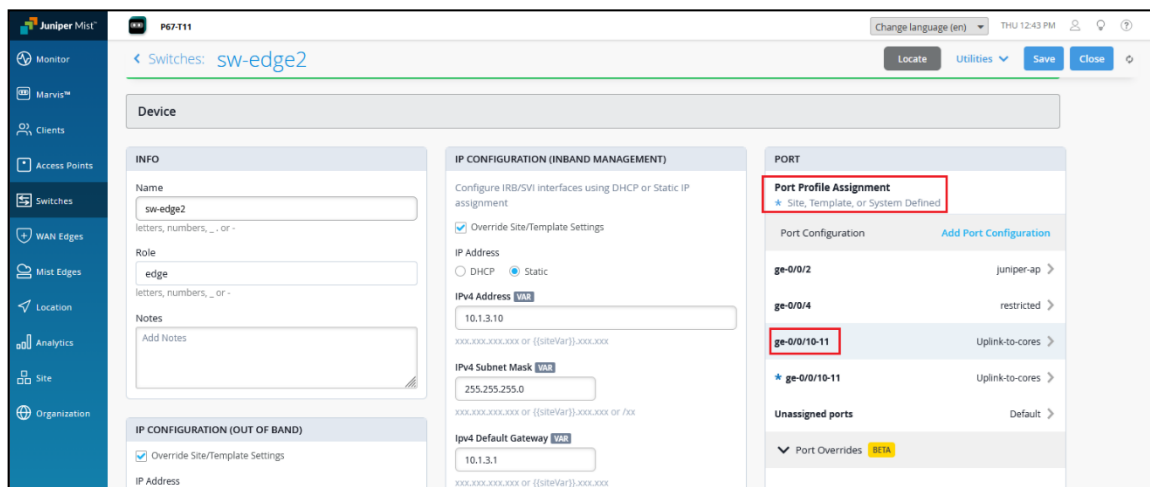
Start typing the role name edge and notice that it appears automatically allowing you to select it.
Click OK.



Click on your switch name, wait a couple of minutes and refresh the page. Confirm that you can see 100% Config Success. Notice message “AE index 1 overlap between ports “ge-0/0/10-11” and “*ge-0/0/10-11”. In other words, between the local switch configuration and inherited configuration from the template.



Scroll down the page to Port Profile Assignment section and click on ge-0/0/10-11 without * (locally configured).



Click on the trash icon to delete this local profile.

Juniper Mist P67-T11

Switches: sw-edge2

INFO

Name: sw-edge2

Role: edge

Notes: Add Notes

IP CONFIGURATION (INBAND MANAGEMENT)

Configure IRB/SVI interfaces using DHCP or Static IP assignment

☒ Override Site/Template Settings

IP Address: ☐ DHCP ☒ Static

IPv4 Address: 10.1.3.10

IPv4 Subnet Mask: 255.255.255.0

IPv4 Default Gateway: 10.1.3.1

IP CONFIGURATION (OUT OF BAND)

☒ Override Site/Template Settings

IP Address: ☐ DHCP ☒ Static

IP Address: 10.251.1.10

PORT

Port Profile Assignment

* Site, Template, or System Defined

Port IDs: ge-0/0/10-11

Interface: ☒ L2 interface ☐ L3 interface ☐ L3 sub-interfaces

Configuration Profile: Uplink-to-cores

☐ Enable Dynamic Port Configuration

Description: Add Description

Save

Confirm that you have * ge-0/0/10-11 Port Configuration and click Save in the top-right corner.

Juniper Mist P67-T11

Switches: sw-edge2

INFO

Name: sw-edge2

Role: edge

Notes: Add Notes

IP CONFIGURATION (INBAND MANAGEMENT)

Configure IRB/SVI interfaces using DHCP or Static IP assignment

☒ Override Site/Template Settings

IP Address: ☐ DHCP ☒ Static

IPv4 Address: 10.1.3.10

IPv4 Subnet Mask: 255.255.255.0

IPv4 Default Gateway: 10.1.3.1

IP CONFIGURATION (OUT OF BAND)

☒ Override Site/Template Settings

PORT

Port Profile Assignment

* Site, Template, or System Defined

Modified by a Port Operator

Port Configuration

ge-0/0/2: juniper-ap

ge-0/0/4: restricted

* ge-0/0/10-11: Uplink-to-cores

Unassigned ports: Default

Port Overrides: BETA

Save

Review changes and click Save to confirm it.

Confirm Changes

☒ Show only differences + Added - Removed * Template or System inherited

Port Config

ge-0/0/10-11

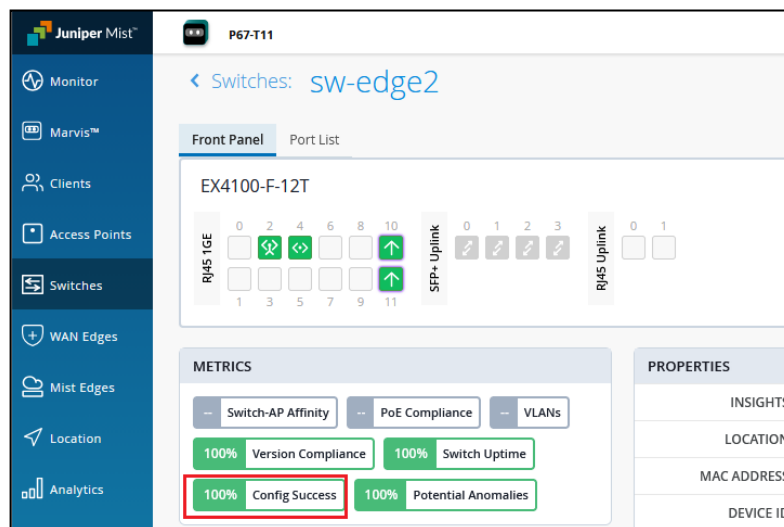
- Port Range: ge-0/0/10-11
- Configuration Profile: Uplink-to-cores
- Dynamic Port Configuration: No
- Enable Up/Down Port Alert Type: Yes
- Local Overwrite: No
- AE
 - Disable LACP: No
 - Index: 1
 - LACP Force-UP: No
 - LACP Periodic Slow: No

Save

Scroll down the page to Advanced section. Notice that you have three scripts pushed from different hierarchy levels: template-script from the template CLI configuration, selectswitch-script from the Select Switches Configuration in your template and device-script from the local configuration.



Scroll up to the top of the page, refresh the page and confirm that you see 100% Config Success.



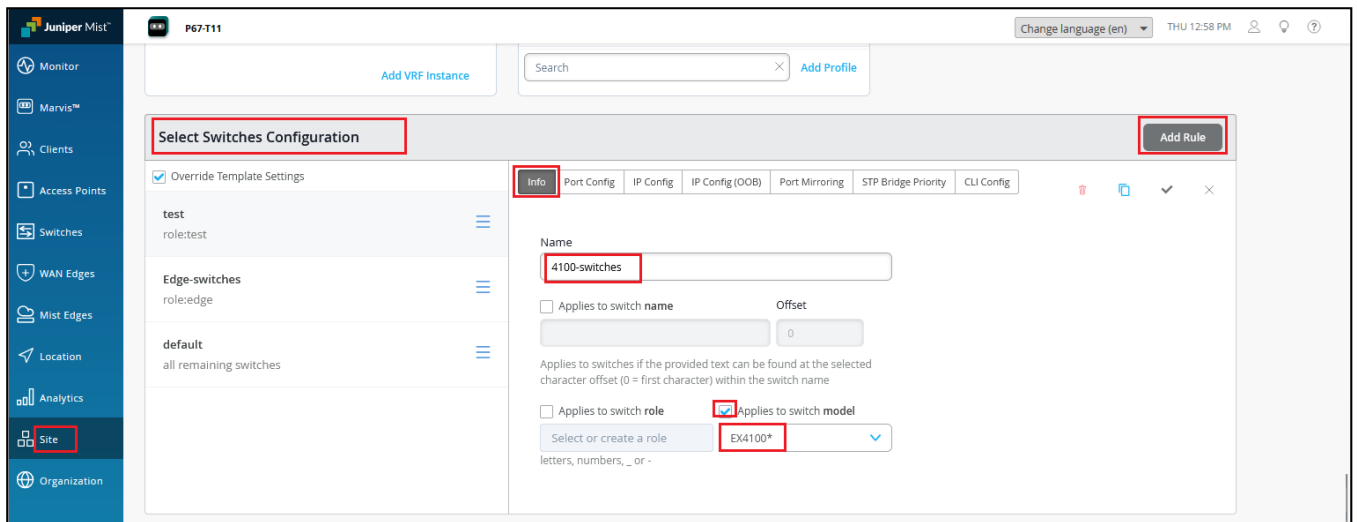
Click Port List to confirm that you have ae1 interface with ge-0/0/10 and ge-0/0/11 members configuration pushed to your switch from Organization Switch Template Select Switches Configuration.

Port	Status	Agg Ethernet	Wired Client	Manufacturer	Wireless Clients	Power Draw	Profile (Configured / Reported)	Type	Speed	Full Duplex	RX/TX
ae1	up	--	--	--	--	--	Uplink-to-cores	Trunk	2000 mbps	☑	0 B
ge-0/0/0	down	--	--	--	--	--	Default	Access	--	--	0 B
ge-0/0/1	down	--	--	--	--	--	Default	Access	--	--	0 B
ge-0/0/2	up	--	88:60:f0:29:ab:e0	Hewlett Packard Enterprise	--	--	juniper-ap	Trunk	1000 mbps	☑	68.
ge-0/0/3	down	--	--	--	--	--	Default	Access	--	--	0 B
ge-0/0/4	up	--	00:50:56:b1:29:bd	VMware, Inc.	--	--	Contractor	Access	1000 mbps	☑	142
ge-0/0/5	down	--	--	--	--	--	Default	Access	--	--	0 B
ge-0/0/6	down	--	--	--	--	--	Default	Access	--	--	0 B
ge-0/0/7	down	--	--	--	--	--	Default	Access	--	--	0 B
ge-0/0/8	down	--	--	--	--	--	Default	Access	--	--	0 B
ge-0/0/9	down	--	--	--	--	--	Default	Access	--	--	0 B
ge-0/0/10	up	ae1	88:3a:30:a3:21:80	Hewlett Packard Enterprise	--	--	Uplink-to-cores	Trunk	1000 mbps	☑	796
ge-0/0/11	up	ae1	88:3a:30:a5:06:40	Hewlett Packard Enterprise	--	--	Uplink-to-cores	Trunk	1000 mbps	☑	49.
xe-0/1/0 (vcp-0/1/0)	--	--	--	--	--	--	Default	Access	--	--	0 B
xe-0/1/1 (vcp-0/1/1)	--	--	--	--	--	--	Default	Access	--	--	0 B
xe-0/1/2 (vcp-0/1/2)	--	--	--	--	--	--	Default	Access	--	--	0 B
xe-0/1/3 (vcp-0/1/3)	--	--	--	--	--	--	Default	Access	--	--	0 B

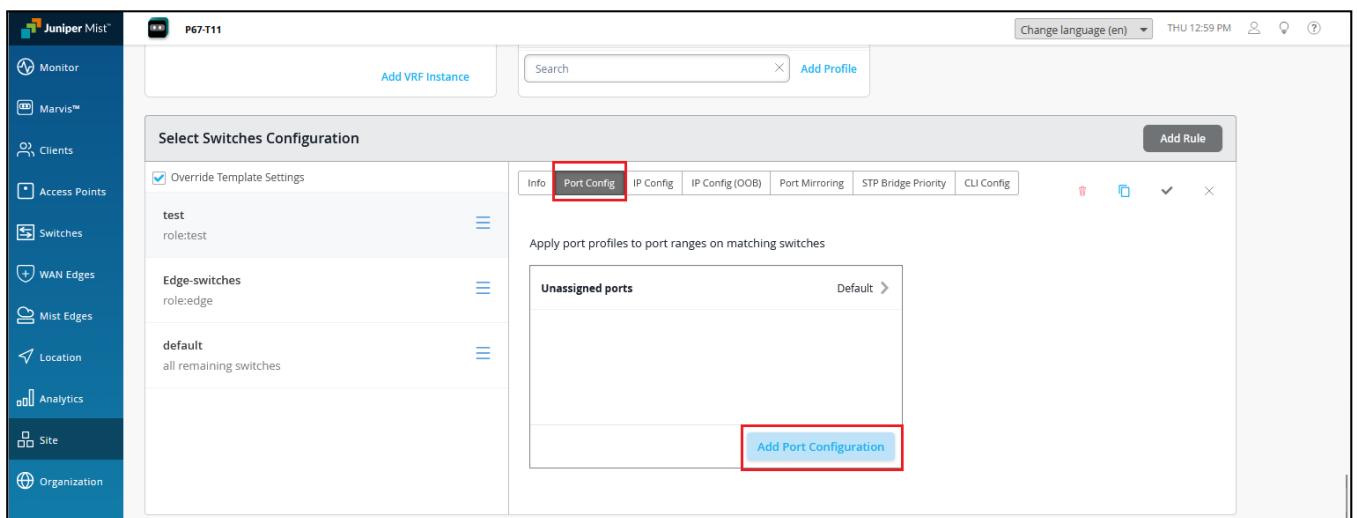
Now, let's repeat this for ports 2 and 4 but this time at the Site level. Navigate to Site > Wired > Switch Configuration and select your site.

Site	Switches	Configuration Template
p67t11-site	1	p67t11-swTemplate
Primary Site	0	--

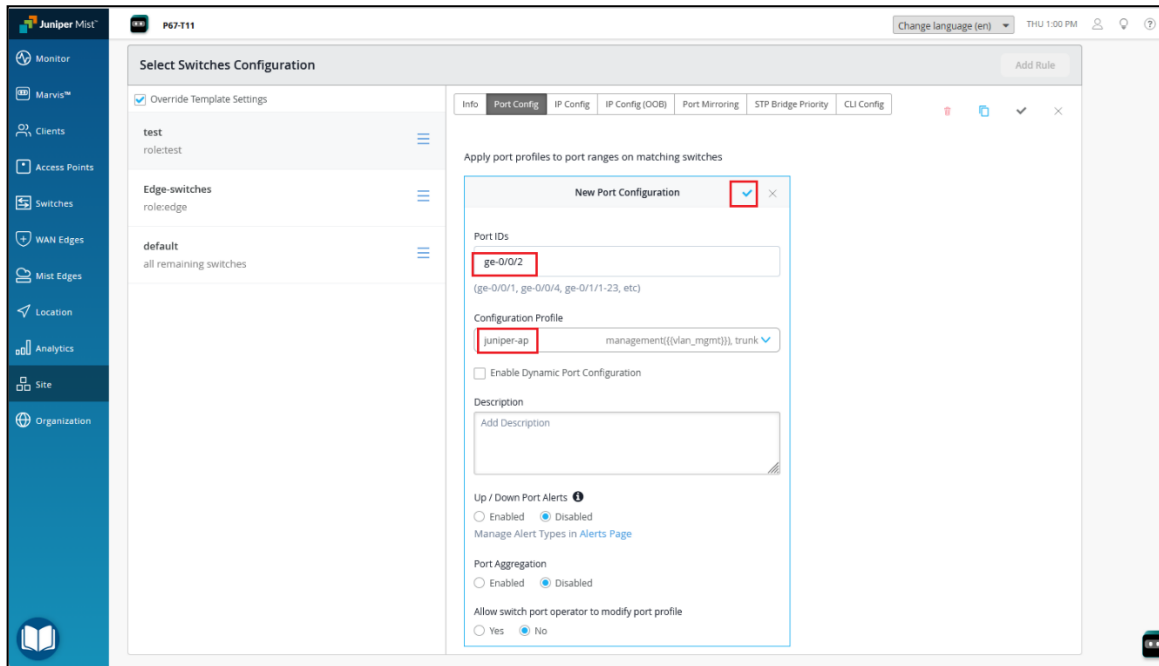
Scroll down the page to Select Switches Configuration, enable checkbox Override Template Settings and click Add Rule. In info tab enter 4100-switches rule name, then enable checkbox Applies to switch model and select EX4100* - all EX 4100 switch models.



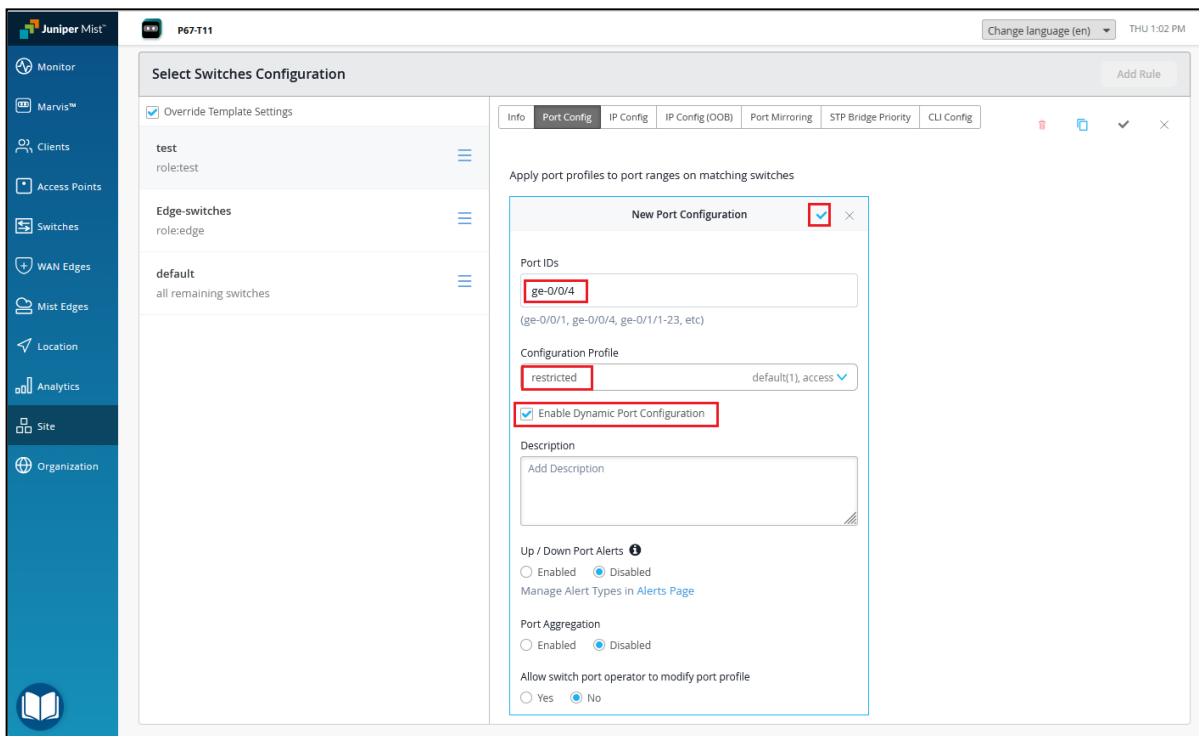
Switch to Port Config Tab and click Add Port Configuration.



Type ge-0/0/2 in Port IDs field, select juniper-ap Configuration Profile and click the check mark to save New Port Configuration.



Click Add Port Configuration, type ge-0/0/4 in Port IDs field, select restricted Configuration Profile, enable Dynamic Port Configuration and click the check mark to save New Port Configuration.



Click Add Port Configuration, type ge-0/0/10-11 in Port IDs field, select Uplink-to-cores Configuration Profile, enable Up/Down Port Alerts, enable Port Aggregation, **type 1 in AE Index** and click **Save**.

Juniper Mist P67-T11 Change language (en) THU 1:15 PM

Select Switches Configuration Add Rule

☒ Override Template Settings

Edge-switches
role:edge

default
all remaining switches

Info **Port Config** IP Config IP Config (OOB) Port Mirroring STP Bridge Priority CLI Config

Apply port profiles to port ranges on matching switches

New Port Configuration ☒ ×

Please ensure AE index does not overlap across different ports between Device, Site/Template and Campus Fabric configuration

Port IDs

(ge-0/0/1, ge-0/0/4, ge-0/1/1-23, etc)

Configuration Profile
 default(1), trunk ▼

☐ Enable Dynamic Port Configuration

Description

Up / Down Port Alerts ?
☒ Enabled ☐ Disabled
[Manage Alert Types in Alerts Page](#)

Port Aggregation
☒ Enabled ☐ Disabled

LACP
☒ Enabled ☐ Disabled

AE Index (0 - 255)

☐ ESI-LAG

Allow switch port operator to modify port profile
☐ Yes ☒ No

Review Port Configuration and click the check mark to save new Rule.

Juniper Mist P67-T11 Change language (en) THU 1:16 PM

Select Switches Configuration Add Rule

☒ Override Template Settings

Edge-switches
role:edge

default
all remaining switches

Info **Port Config** IP Config IP Config (OOB) Port Mirroring STP Bridge Priority CLI Config

Apply port profiles to port ranges on matching switches

ge-0/0/2 juniper-ap ➤

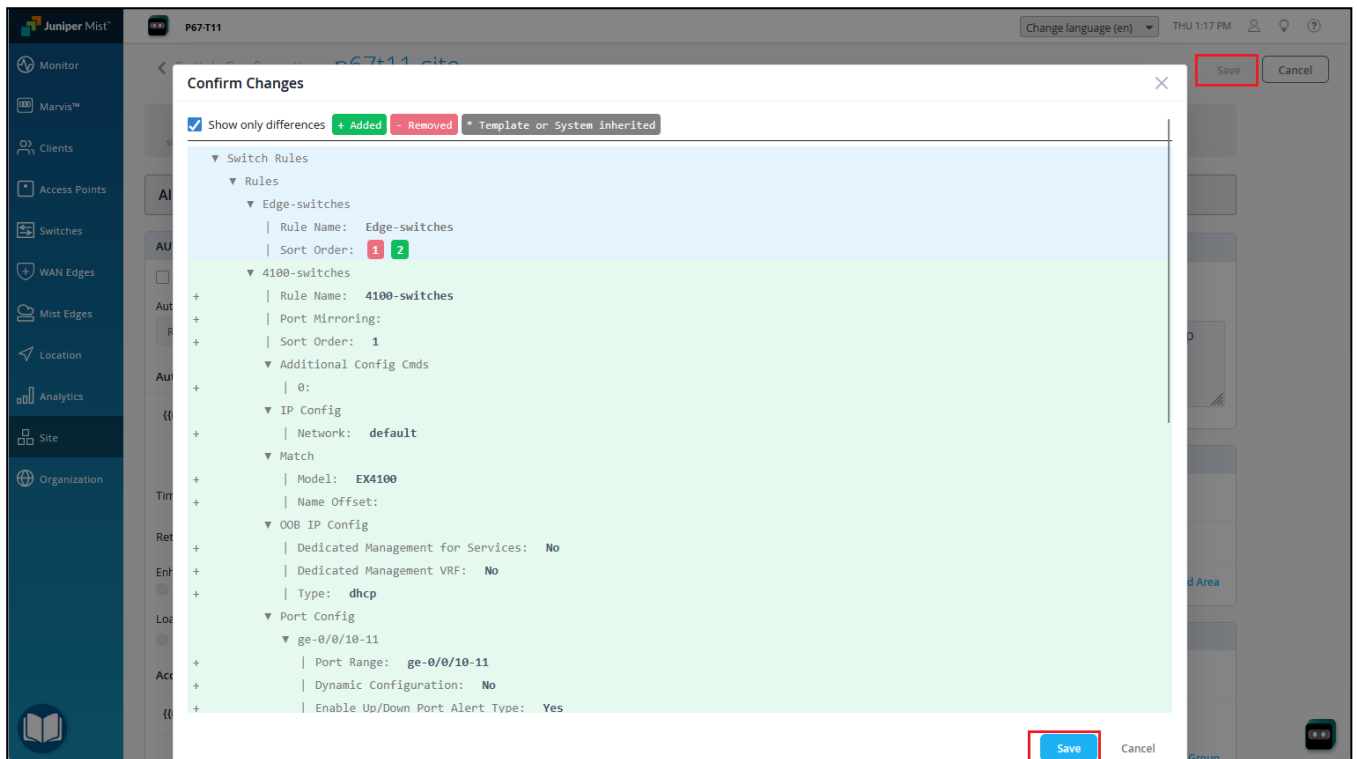
ge-0/0/4 restricted ➤

ge-0/0/10-11 Uplink-to-cores ➤

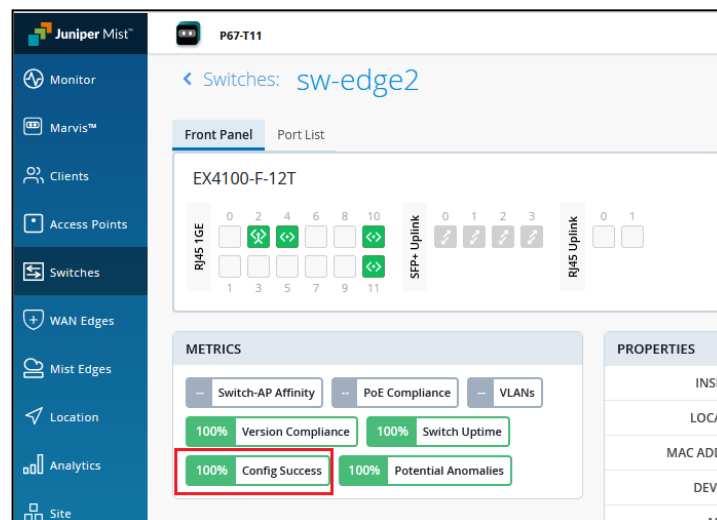
Unassigned ports Default ➤

[Add Port Configuration](#)

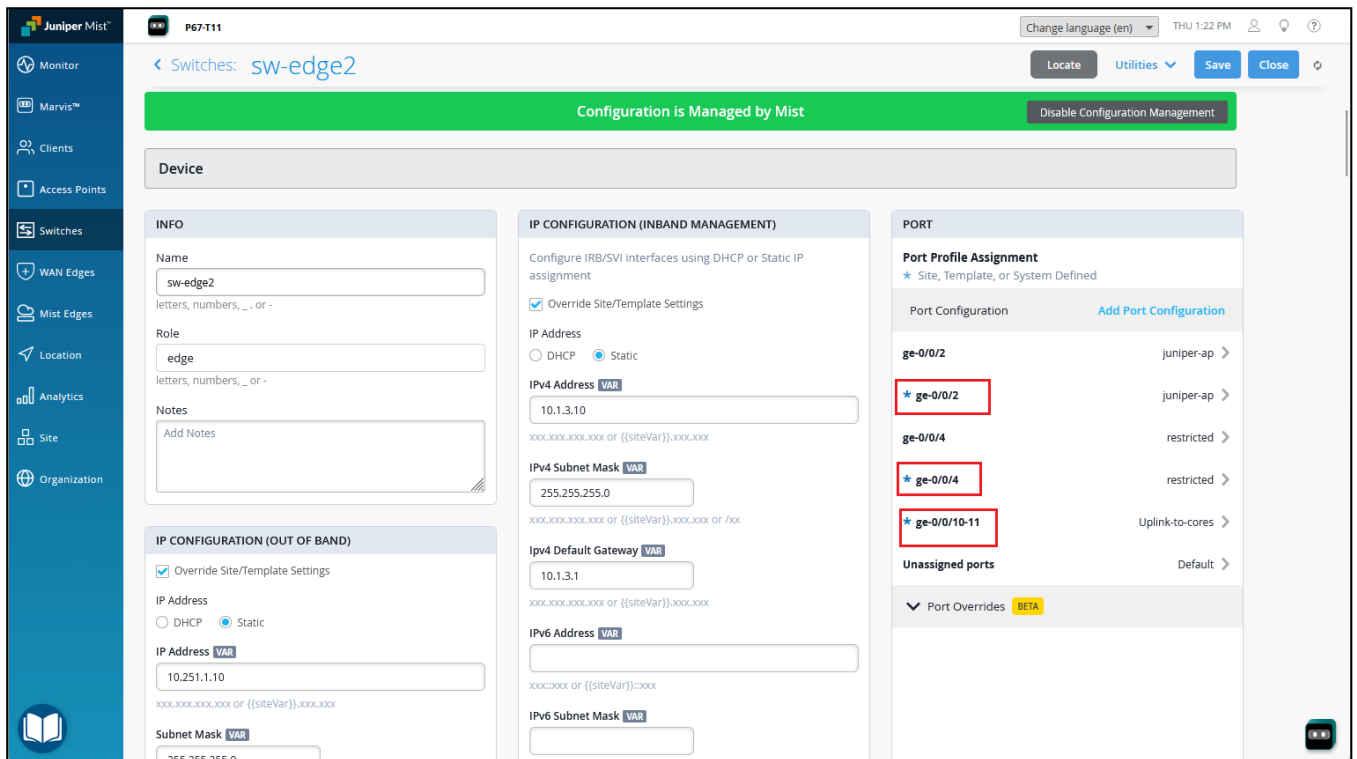
Scroll up the page and click Save, then click Save again to confirm changes.



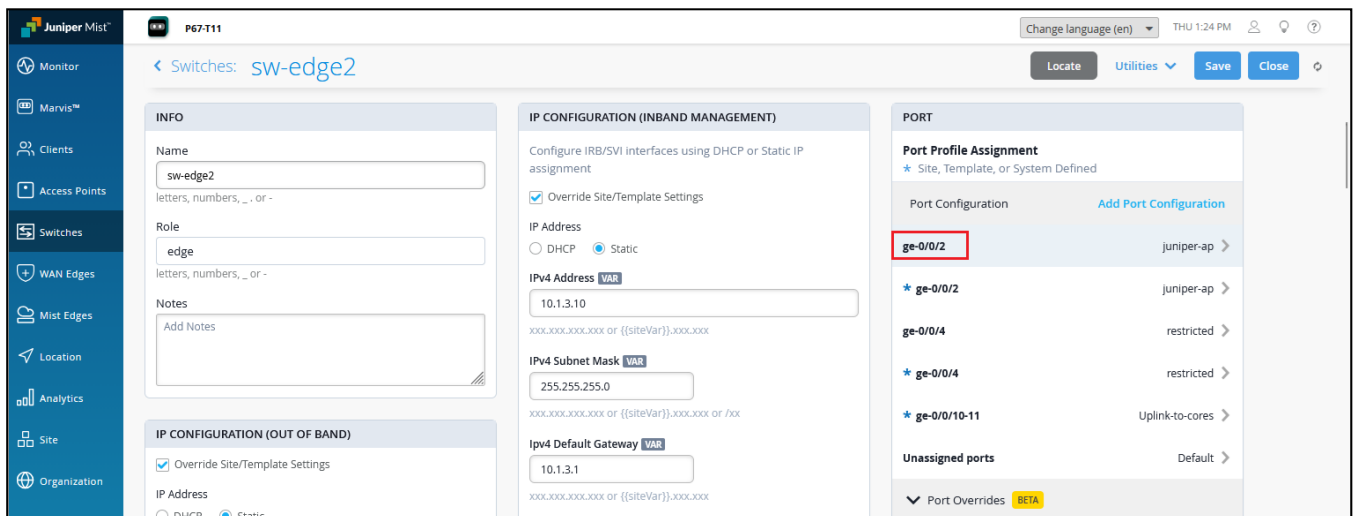
Navigate in Mist AI to Switches > sw-edge2, wait a couple of minutes and refresh the page. Confirm that you see 100% Config Success.



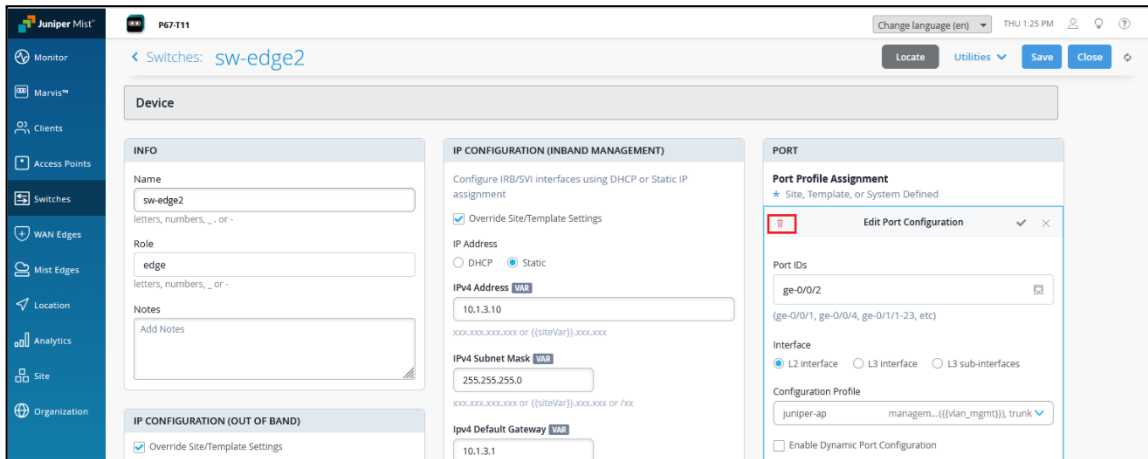
Scroll down the page to Port Profile Assignment where you should see three Port Profile assignments inherited from the site. This includes * ge-0/0/2, * ge-0/0/4 and * ge-0/0/10-11.



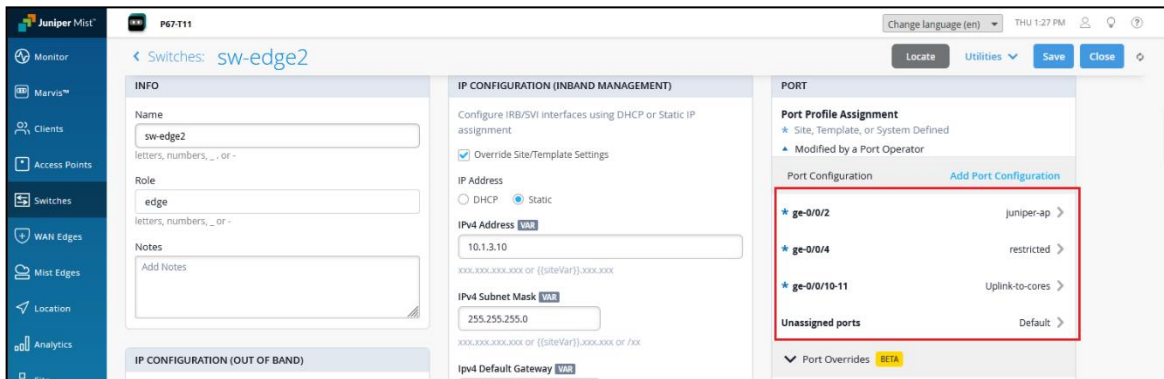
Click on local Port Profile Assignment ge-0/0/2 (without *).



Click on the trash icon to delete this local profile.

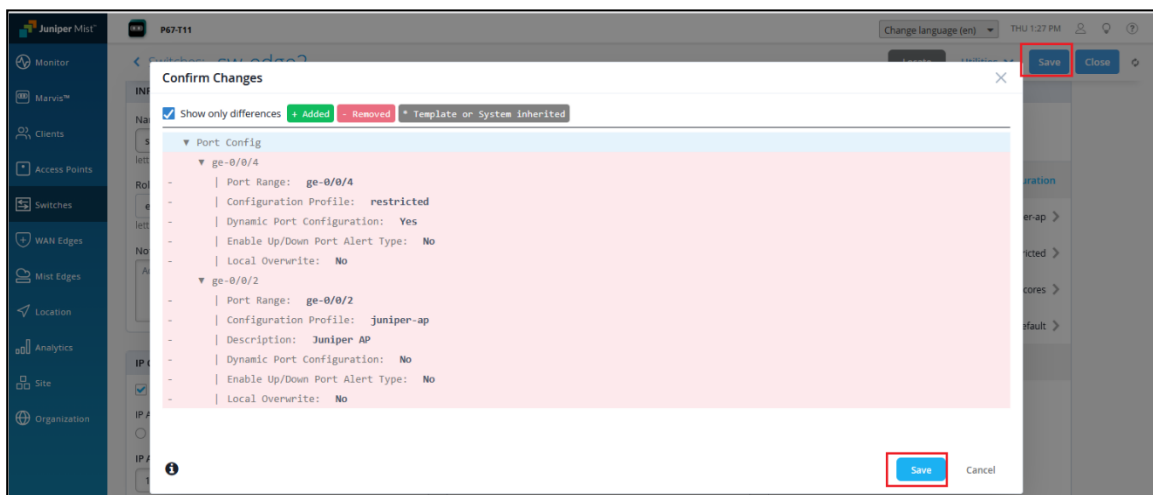


Delete local Port Profile Assignment ge-0/0/4 (without *) and check that all Port Profile Assignments are now inherited from your site.

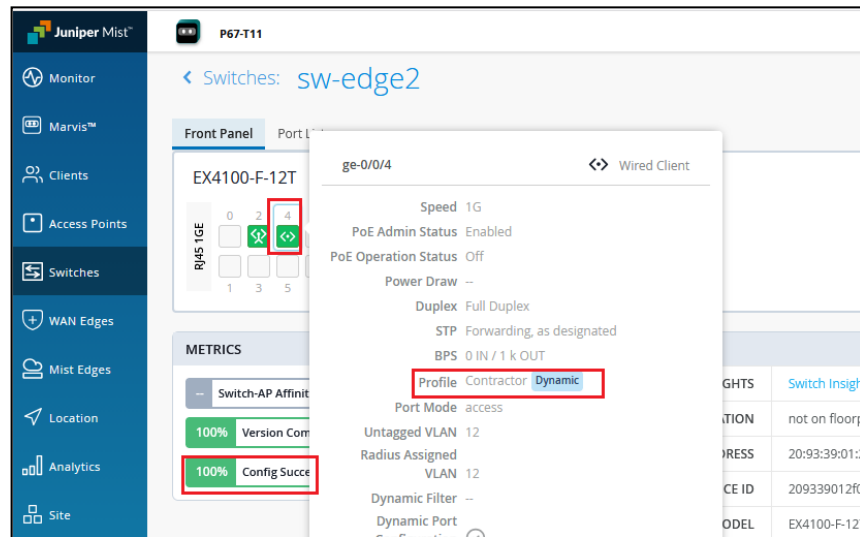


NOTE: You can override inherited configuration with a local Port Profile Assignment, or you can use Port Overrides to append parameters to existing local or inherited port configuration.

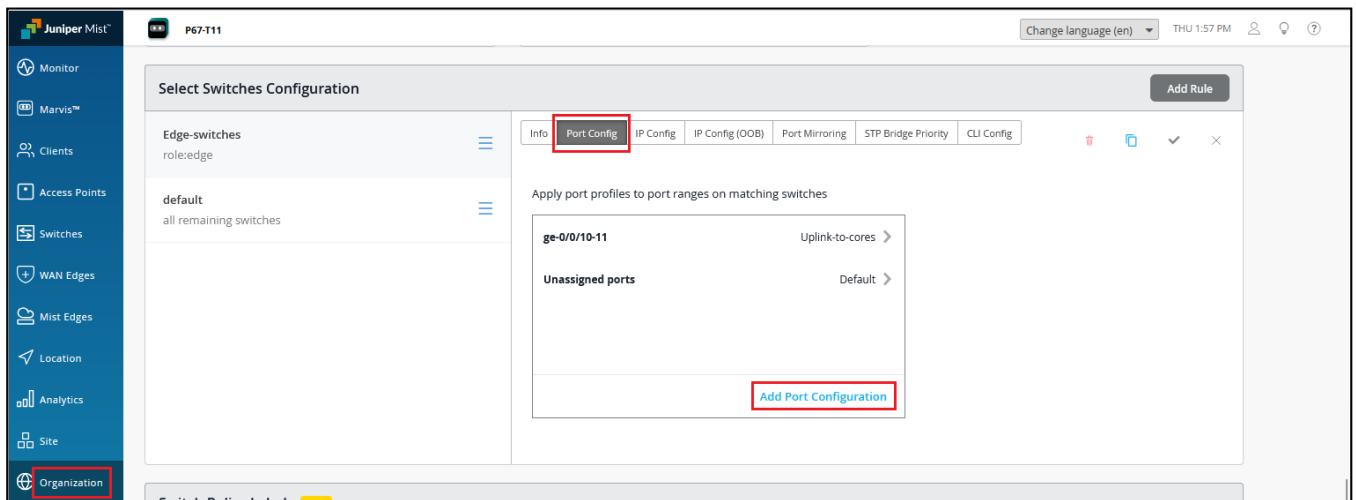
Click Save and then click Save again to confirm changes.



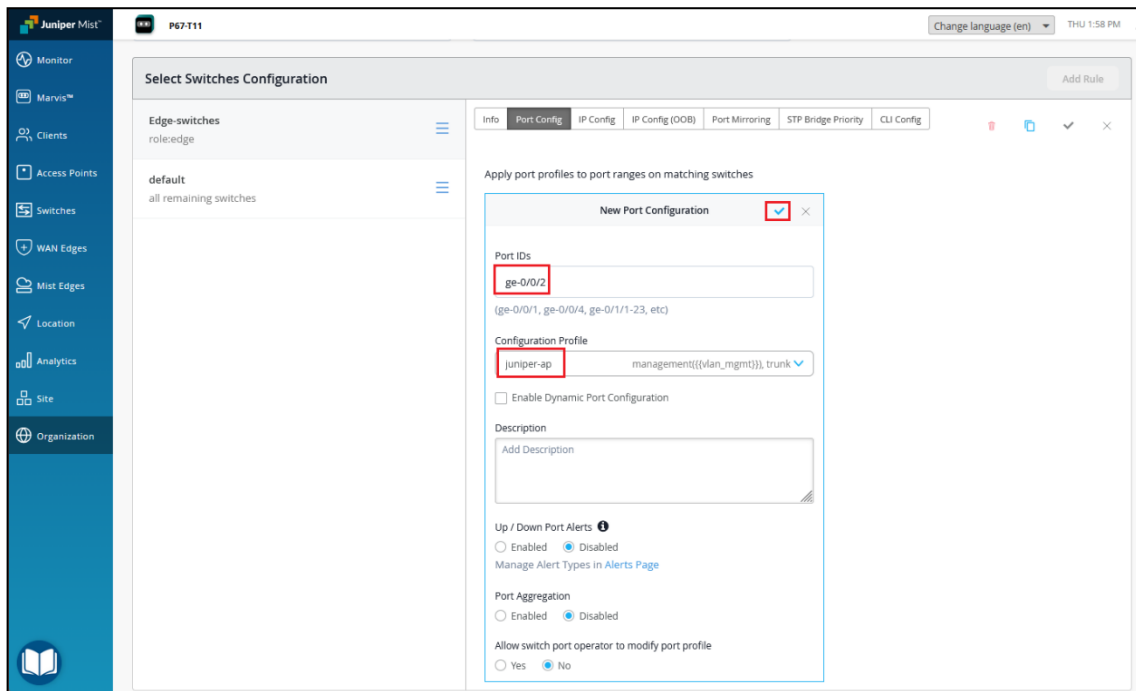
Wait a couple of minutes and refresh the page, then confirm that you have 100% Config Success and correct profiles applied to ports 2 (juniper-ap) and 4 (contractor).



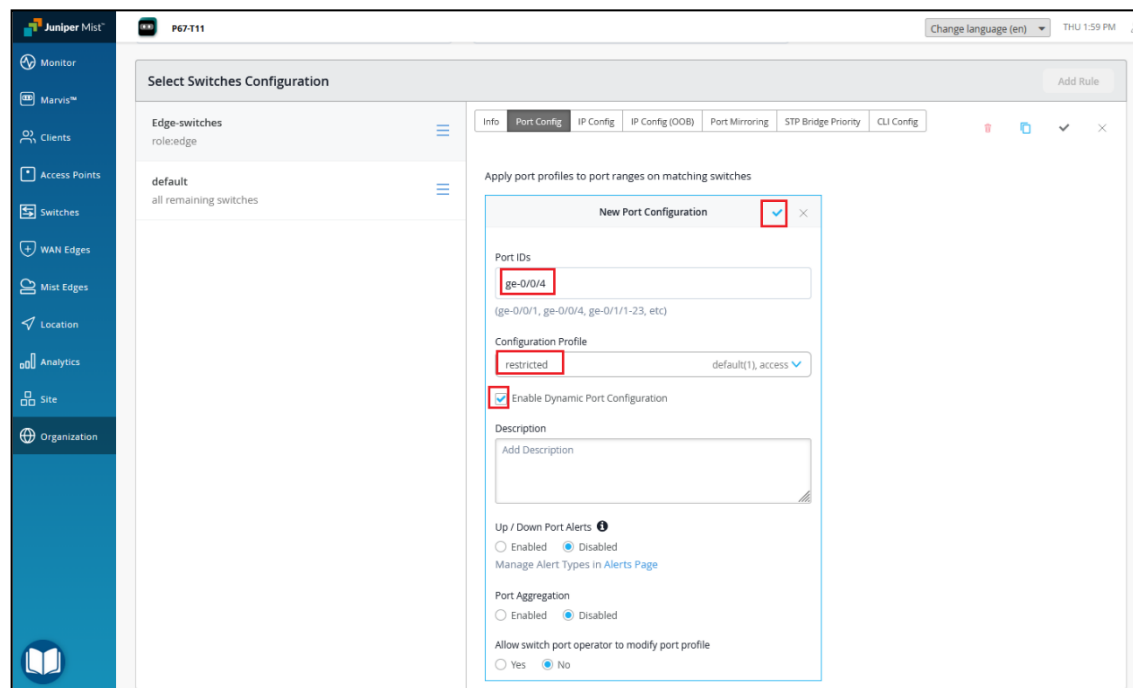
Navigate in Mist AI to Organization > Wired > Switch Templates and select your template. Scroll to Select Switches Configuration, click on Edge-switches rule, select tab Port Config and click Add Port Configuration.



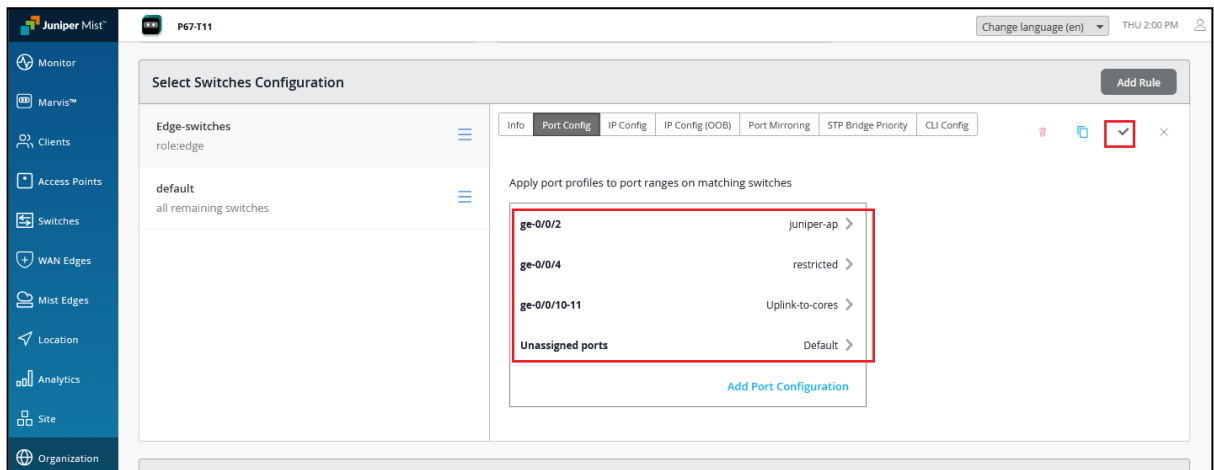
Type ge-0/0/2 in Port IDs field, select juniper-ap Configuration Profile and lick the check mark.



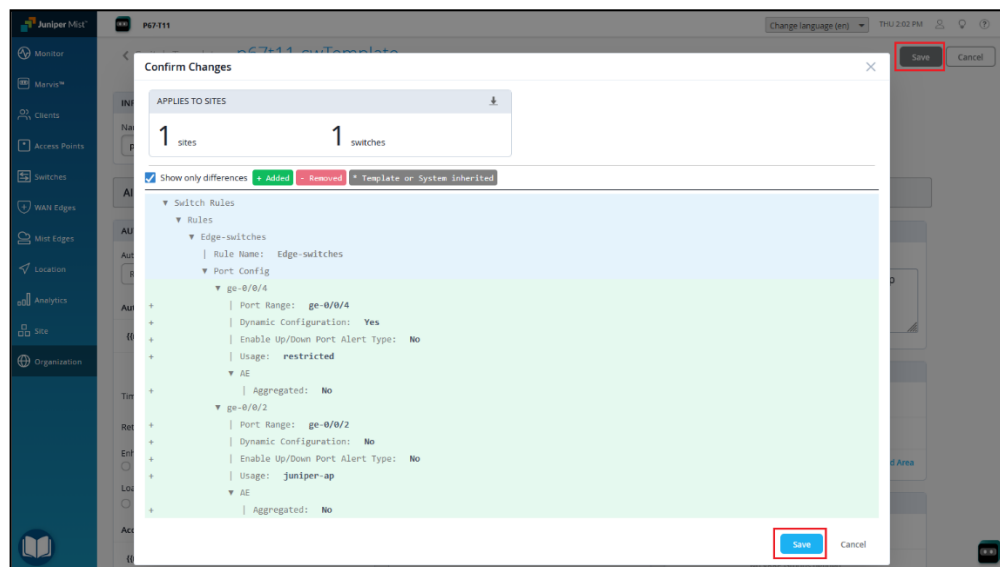
Click Add Port Configuration, type ge-0/0/4 in Port IDs field, select restricted Configuration Profile, enable Dynamic Port Configuration and click the check mark.



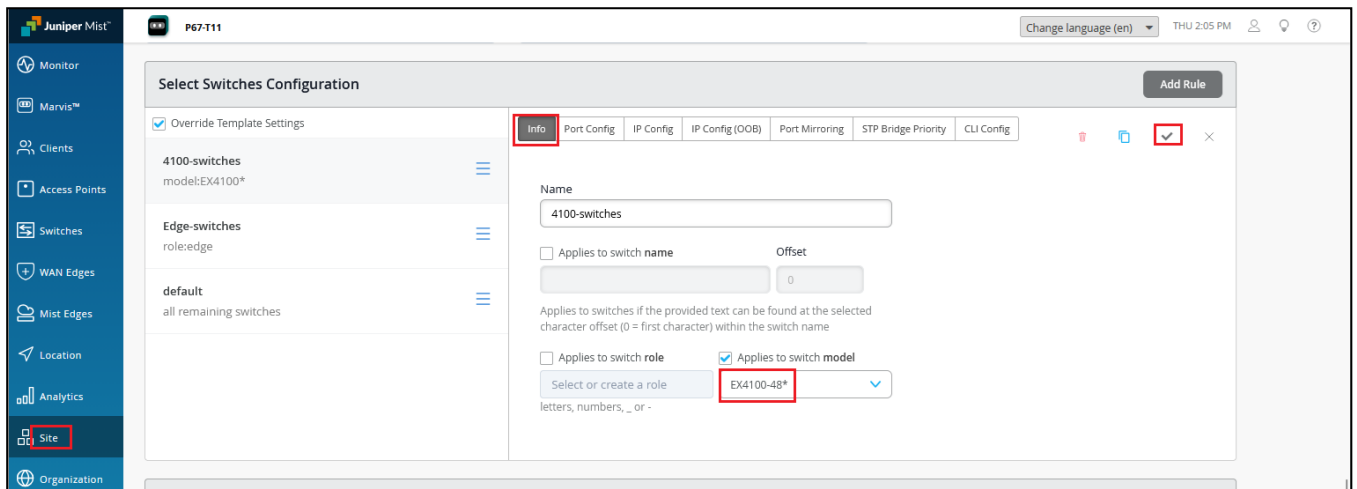
Confirm that you have three Port Configurations and click the check mark to update the rule.



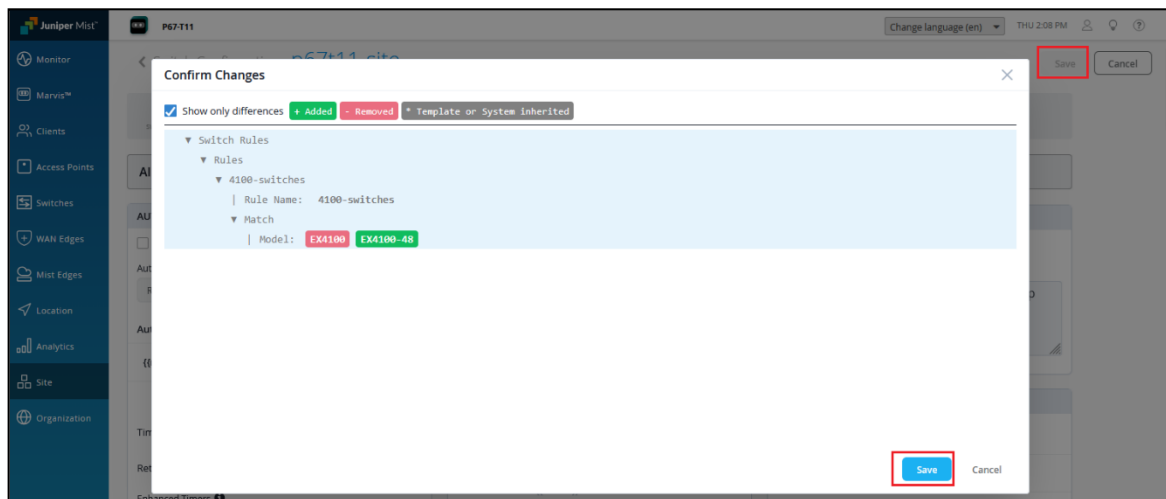
Scroll up to the top of the page and click Save then click Save again to confirm changes.



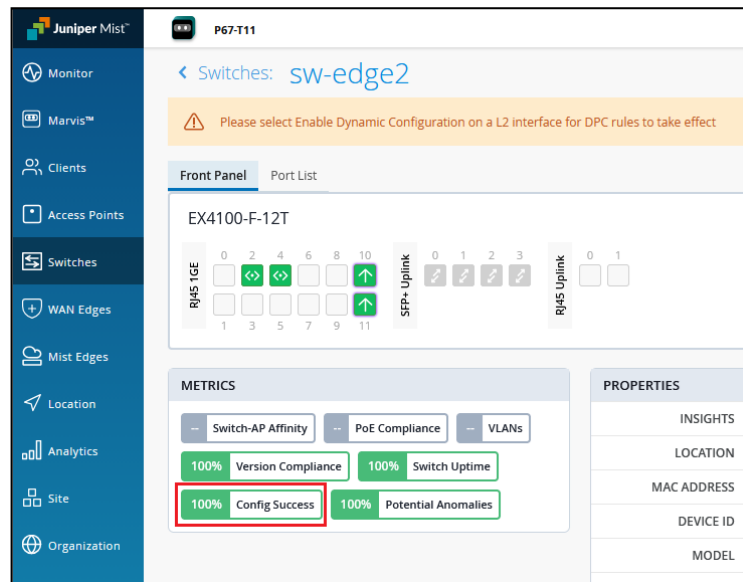
In Mist AI navigate to Site > Wired > Switch Configuration and select your site. Then click 4100-switches rule and change the switch model to EX4100-48* which will not match your table switch model (EX4100-F-12T). Click the check mark to save new rule settings.



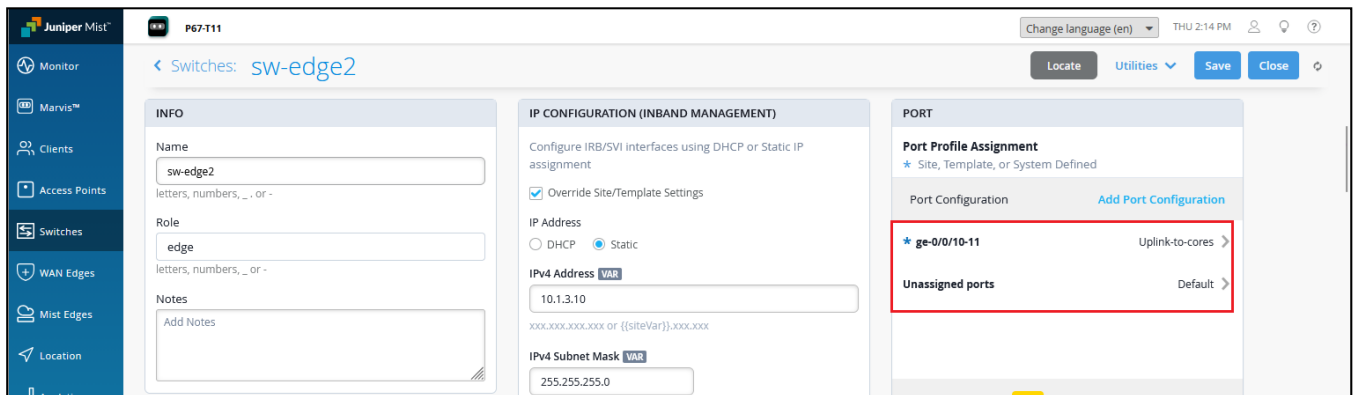
Scroll up the page to the top and click Save, then click Save again to confirm changes.



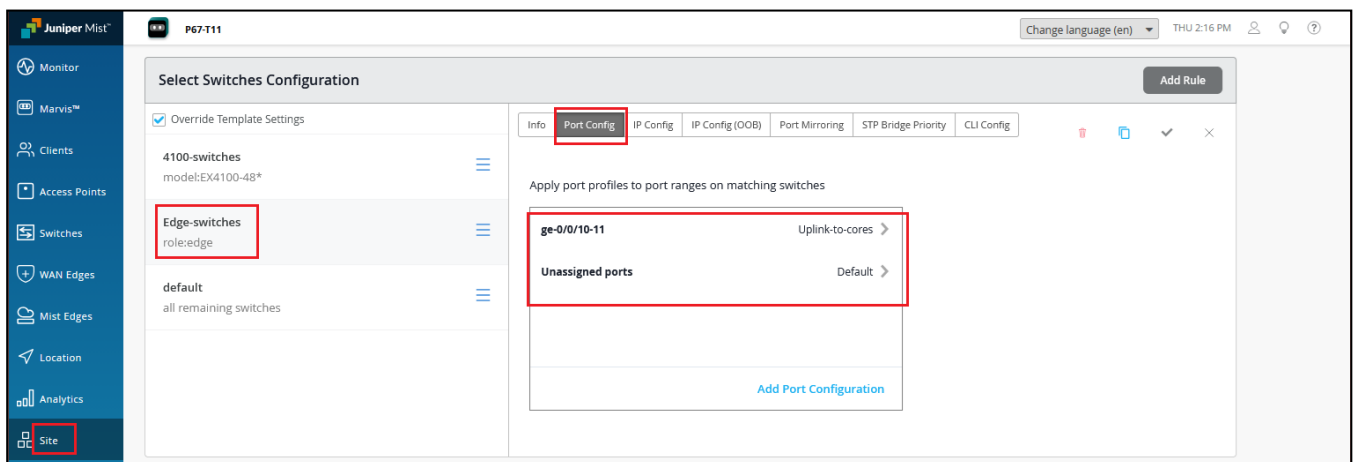
Navigate in Mist AI to Switches > sw-edge2, wait a couple of minutes and refresh the page. Confirm that you have 100% Config Success.



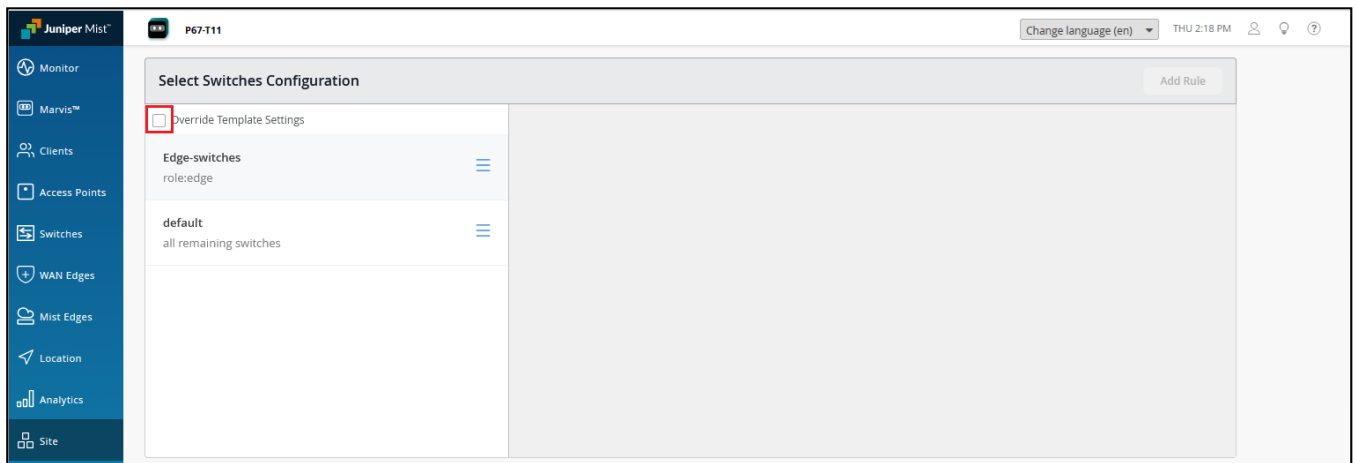
Scroll down the page to Port Profile Assignment and confirm that ge-0/0/2 and ge-0/0/4 disappeared.



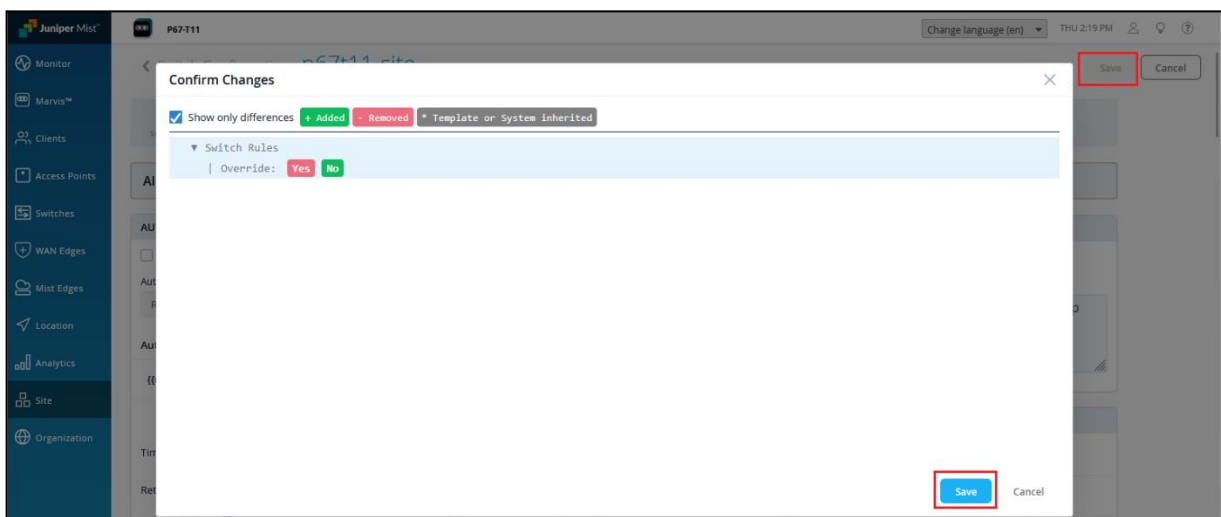
Navigate in Mist AI to Site > Wired > Switch Configuration and select your Site. Scroll down the page to Select Switches Configuration and lick on Edge-switches Rule, then switch to Port config tab. As you can see, your latest changes in Select Switches Configuration from Organization template were not applied to Site Overrides.



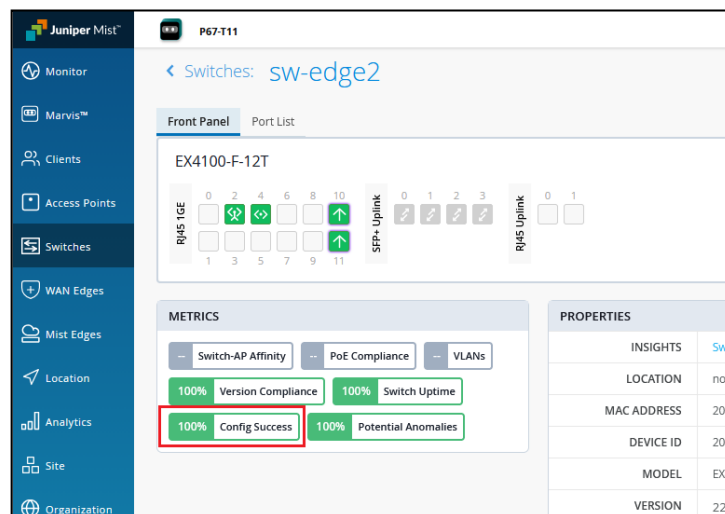
Uncheck Override Template Settings.



Scroll the page up to the top and click Save, then click Save again to confirm changes.



Navigate in Mist AI Switches > sw-edge2, wait a couple of minutes and refresh the page. Confirm that you can see 100% Config Success.



Scroll down the page to Port Profile Assignment section and confirm that you have three inherited Port Profile Assignments.

The screenshot shows the Juniper Mist configuration interface for a switch named 'sw-edge2'. The interface is divided into several sections:

- INFO:** Contains fields for Name (sw-edge2), Role (edge), and Notes.
- IP CONFIGURATION (INBAND MANAGEMENT):** Contains fields for IP Address (10.1.3.10), IPv4 Address (VAR), and IPv4 Subnet Mask (255.255.255.0).
- PORT:** Contains a section for Port Profile Assignment, which is highlighted with a red box. It lists three inherited assignments: ge-0/0/2 (juniper-ap), ge-0/0/4 (restricted), and ge-0/0/10-11 (Uplink-to-cores). Below this is a section for Unassigned ports (Default) and a Port Overrides section (BETA).

The top of the page shows the Juniper Mist logo, a navigation menu on the left, and a top bar with the switch name 'sw-edge2' and various utility buttons (Locate, Utilities, Save, Close). A green banner at the top indicates 'Configuration is Managed by Mist'.

Task 5-4: Use bulk upload of switch configuration

Objectives

Review Bulk Upload Configuration CSV sample.

Customize Bulk Upload Configuration CSV file.

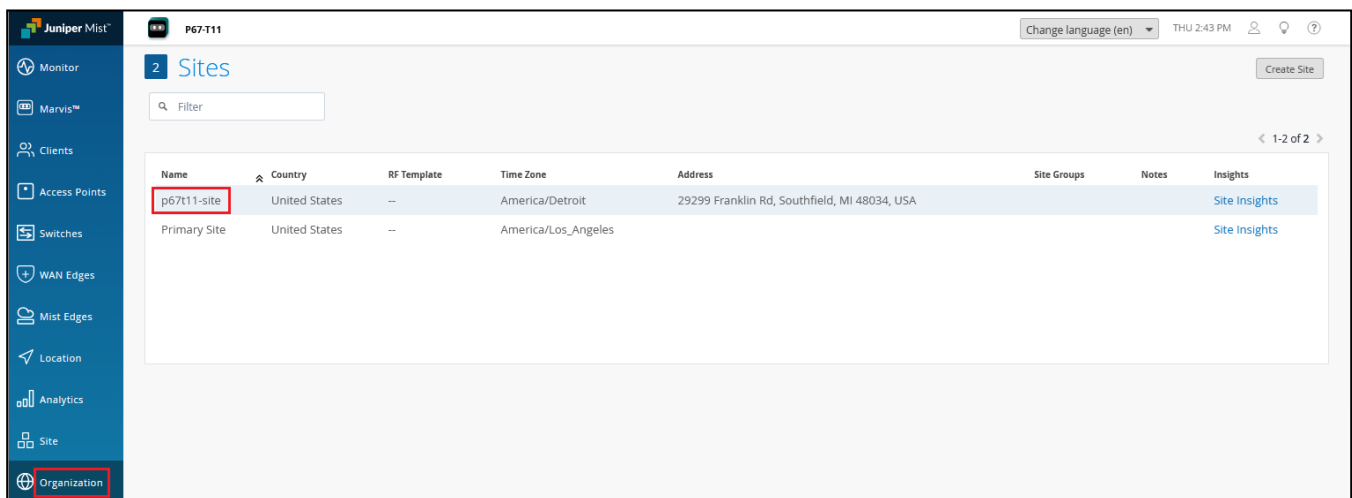
Update your switch configuration with Bulk Upload Configuration.

If you don't want to manually configure the switch-specific settings on each switch, you can configure the settings by uploading them through a CSV file. You can upload the settings for one or more switches at once. You can upload the following settings: MAC address, serial number, switch name, switch role, router-ID, IP configuration (OOB), Primary IP (In-Band), and Default Gateway (In-Band).

If you want any networks or L3 interfaces/sub Interfaces configuration to be present in the sample CSV downloaded, specify those on the Bulk Upload Configurations window before downloading the file. The downloaded sample file includes fields to configure settings for the specified networks and interfaces. The network selection allows you to configure additional IP addresses on individual devices as IRB interfaces.

Steps

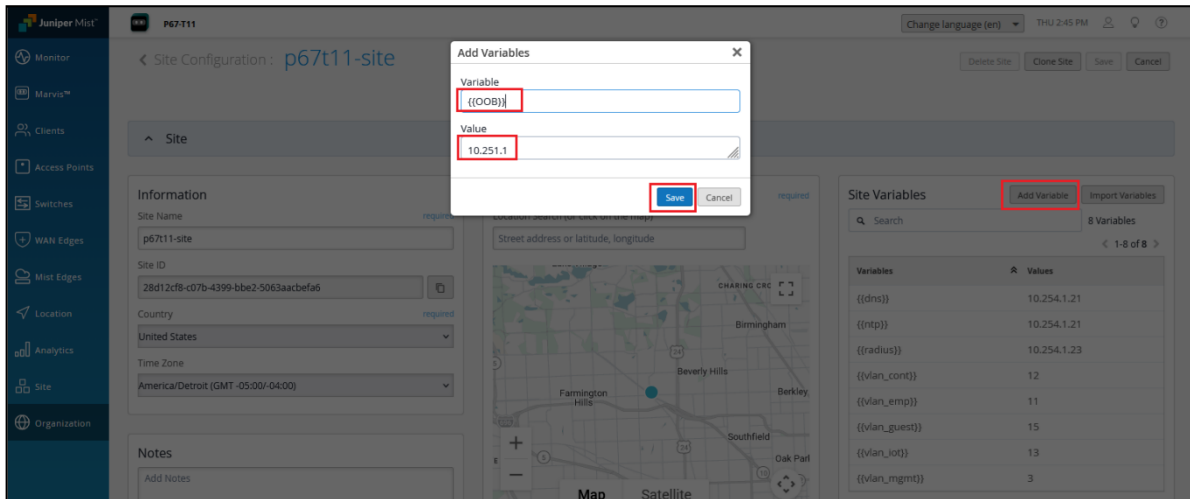
In this Lab you will change switch In-Band and OOB IP settings to use Site variables and you will update it with Bulk Upload Configuration. Start with defining Site variables. In Mist AI navigate to Organization > Admin > Site Configuration and select your site.



The screenshot shows the Juniper Mist web interface. On the left sidebar, the 'Organization' menu item is highlighted with a red box. The main content area displays the 'Sites' page, which includes a table of sites. The first row of the table, 'p67t11-site', is highlighted with a red box. The table has columns for Name, Country, RF Template, Time Zone, Address, Site Groups, Notes, and Insights. The second row is 'Primary Site'.

Name	Country	RF Template	Time Zone	Address	Site Groups	Notes	Insights
p67t11-site	United States	--	America/Detroit	29299 Franklin Rd, Southfield, MI 48034, USA			Site Insights
Primary Site	United States	--	America/Los_Angeles				Site Insights

In Site Variables, click Add Variable, type {{OOB}} in Variable field and "10.251.1" in Valued field then click Save.



Click Add Variable to add Variable `{{InBand}}` with value "10.1.3". Click Save.

Add Variables

Variable

Value

Save Cancel

Confirm that new variables are added correctly. Check dots and register.

Variables	Values
{{dns}}	10.254.1.21
{{InBand}}	10.1.3
{{ntp}}	10.254.1.21
{{OOB}}	10.251.1
{{radius}}	10.254.1.23
{{vlan_cont}}	12
{{vlan_emp}}	11
{{vlan_guest}}	15
{{vlan_iot}}	13
{{vlan_mgmt}}	3

Click Save in the top-right corner.

Change language (en) THU 2:56 PM

Delete Site Clone Site **Save** Cancel

Site Variables Add Variable Import Variables

Search 10 Variables

< 1-10 of 10 >

Variables	Values
{{dns}}	10.254.1.21
{{InBand}}	10.1.3
{{ntp}}	10.254.1.21
{{OOB}}	10.251.1

In Mist AI navigate to Switches, select sw-edge2 and click Bulk Upload Configuration.

Juniper Mist P67-T11

Change language (en) THU 2:57 PM

1 Switches site p67t11-site List Topology Location 2:57:25 PM (updates every 3 minutes) More Upgrade Firmware **Bulk Upload Configuration**

1 Cloud Connected Switch 0 Discovered Switches 4 Wired Clients 0 W Total Allocated AP Power

Switch-AP Affinity PoE Compliance VLANs 100% Version Compliance 100% Switch Uptime 100% Config Success 29% Switchport Usage 100% Potential Anomalies

Filter

	Status	Name	IP Address	Model	Mist APs	Wireless Clients	Wired Clients	Version	Uptime	Last Config	Insights
☒	Connected	sw-edge2	10.1.3.10	EX4100-F-12T	0	0	4	22.4R3.25	7d 2h 2m	May 14, 2026 2:55:31 PM	Switch Insights

Click Download Device List.

Bulk Upload Configurations

The recommended approach is to disable configuration management for devices before as it may overwrite the existing UI configuration and then enable after verifying the configurations

Drag and Drop or Click to Upload CSV File

Networks +

Networks displayed here are VLANs saved under Site > Switch Configuration or on a Switch Template assigned to this site. These networks can be selected to configure additional IP addresses on individual devices as IRB interfaces

L3 Interfaces/Sub Interfaces

Can be a range of a comma separated value e.g. xe-0/0/2, et-0/0/4-7

Download Device List

The CSV file should have the following format:
Header Row: MAC, Serial, Name, Role, Router-Id, IP configuration (OOB), Primary IP (In-Band), Default Gateway (In-Band), Notes
Note : Header Row must be the first row in the file and not be changed. The MAC and Serial must not be changed as well.

Cancel

Open downloaded “switch_configurations.csv” file. This file contains a sample switch and your selected switch. MAC, Serial, Name, Role, Router-ID, IP config (OOB), Primary IP (In-Band), Default Gateway (In-Band) and Notes.

	A	B	C	D	E	F	G	H	I
1	MAC	Serial	Name	Role	Router-Id	IP configuration (OOB)	Primary IP (In-Band)	Default Gateway (In-Band)	Notes
2	xxxxxxxxxxxx	serial001	sample_hostname	sample_role	x.x.x.x	x.x.x.x/y or {{siteVar}}.x.x/{{siteVarMask}} or dhcp	x.x.x.x/y or {{siteVar}}.x.x/{{siteVarMask}} or dhcp	xxx.xxx.xxx.xxx or {{siteVar}}.xxx.x	the switch notes
3	209339012f00	FK3124AV0065	sw-edge2	edge		10.251.1.10/255.255.255.0	10.1.3.10/255.255.255.0;management	10.1.3.1	

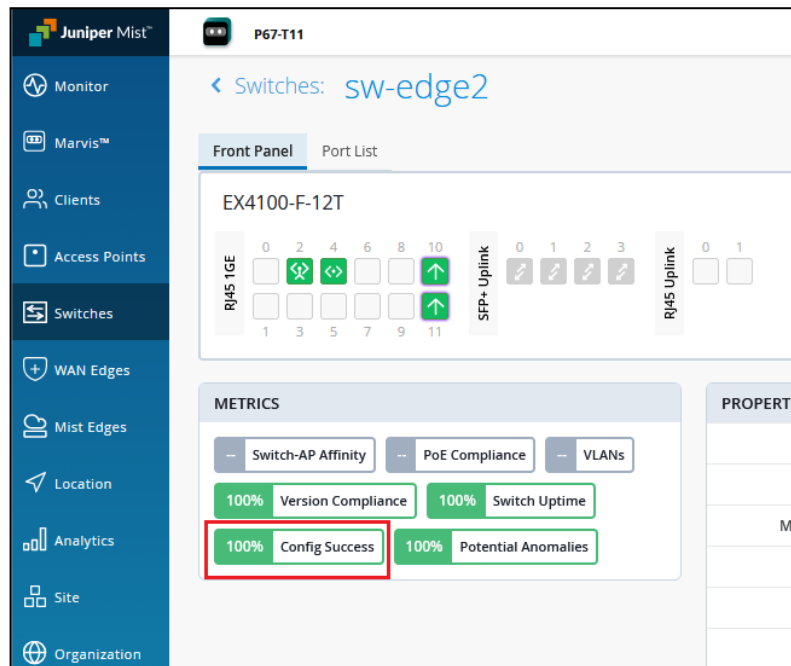
Replace IP config (OOB) 10.251.1.10/255.255.255.0 with {{OOB}}.10/24, replace Primary IP (In-Band) 10.1.3.10/255.255.255.0 with {{InBand}}.10/24 and replace Default Gateway (In-Band) 10.1.3.1 with {{InBand}}.1. Save your file.

	A	B	C	D	E	F	G	H	I
1	MAC	Serial	Name	Role	Router-Id	IP configuration (OOB)	Primary IP (In-Band)	Default Gateway (In-Band)	Notes
2	xxxxxxxxxxxx	serial001	sample_hostname	sample_role	x.x.x.x	x.x.x.x/y or {{siteVar}}.x.x/{{siteVarMask}} or dhcp	x.x.x.x/y or {{siteVar}}.x.x/{{siteVarMask}} or dhcp	xxx.xxx.xxx.xxx or {{siteVar}}.xxx.x	the switch notes
3	209339012f00	FK3124AV0065	sw-edge2	edge		{{OOB}}.10/24	{{InBand}}.10/24;management	{{InBand}}.1	

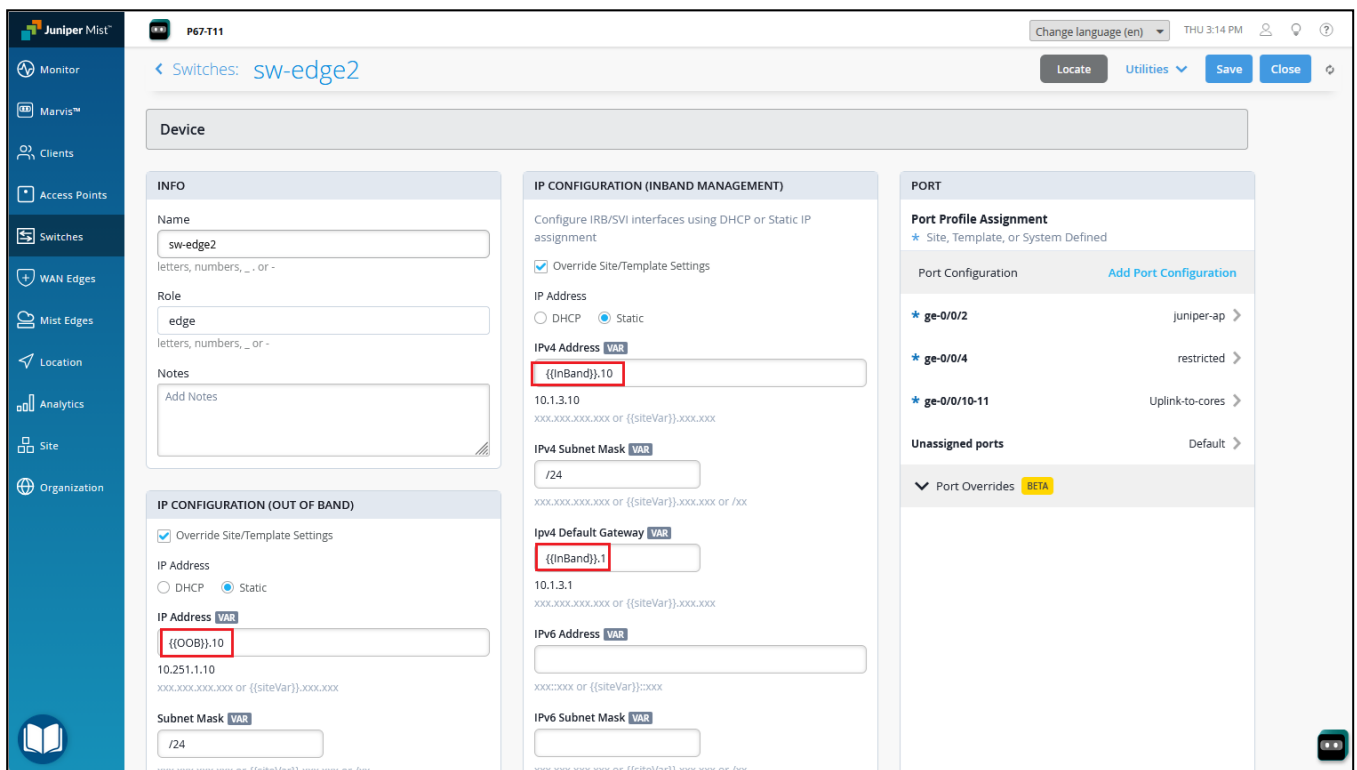
Drag and drop your switch_configurations.csv file to the Bulk Upload Configurations window. You can adjust some settings in this window and click **Save**.

In case of Success, you should see a message with successfully updated devices. Click **Close**.

Click on your switch name, wait a couple of minutes and refresh the page. Confirm that you have 100% Config Success.



Confirm that OOB and In-Band IP addresses and Default Gateway displayed with configured variables.



You have completed this lab!