Mist Edge General Config Guide

Document owners:

Robert Young – ryoung@juniper.net

Slava Dementyev – vdementyev@juniper.net

Jan Van de Laer – djanvan@juniper.net

Table of Contents

Solution Overview 3

How it works 6

Configuration Steps 7

Setup Mist Edge 7

Configure and prepare the SSID 19

Create a Site for Campus, Branches 21

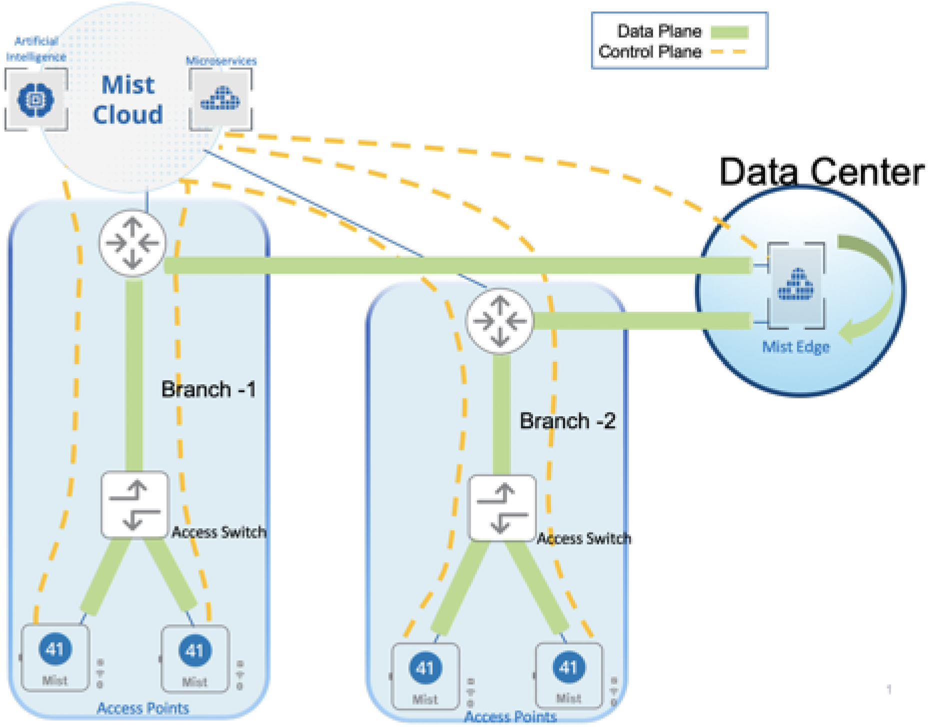
Mist Edge Insights 22

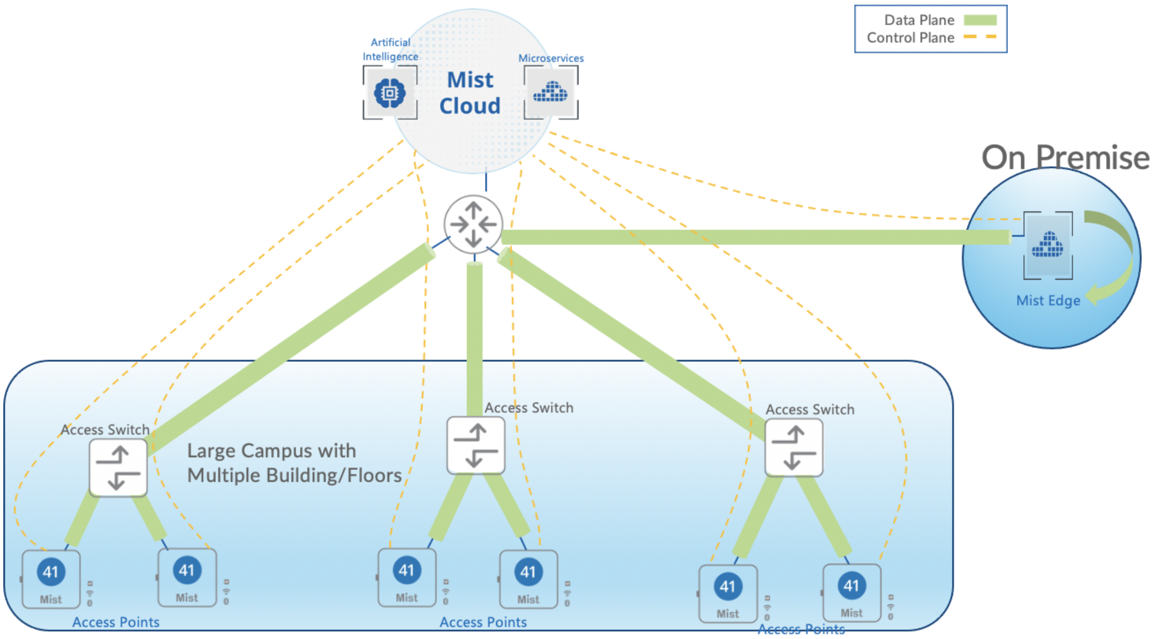
Troubleshooting 24

Packet Captures on the Mist Edge 24

Solution Overview

Mist solution leverages Mist Edge for cases that need to retain the Centralized Datapath Architecture for Campus/Branch deployments. Mist AP can form L2TPv3 Tunnel to extend one or multiple vlan from one or multiple Mist Edge located in Campus, DC or DMZ simultaneously. AP can support both local and Centralized Datapath together.





WIth Mist Edge solution customers can retain their centralized Datapath, providing the same level of redundancy and access to corporate resources, while extending visibility into user network experience and streamlining IT operations.

What are the benefits of the Mist Edge Centralized architecture solution with Mist Edge compared to all the other alternatives?

Agility:

- Zero Touch Provisioning - no AP pre-staging required, support for same AP to tunnel to multiple locations and any number of cluster support
- Exceptional support with minimal effort - leverage Mist SLEs and Marvis Actions
- No firmware dependency between AP and Mist Edge , Mist Edge services can be updated independently and takes 3 seconds at max to update.

Security:

- Traffic Isolation - same level of traffic control as original WLC architecture.
- Automated Security - machine-driven site deployment, no credential exposure.
- Support Dot1x and MPSK support.

Flexibility:

- Full re-usability of hardware
- Can add additional Mist Edges for horizontal scale increase of APs or users.

Scalability:

- Can scale from few branches to Thousands of them.

- Can support Campus with a few hundred APs to Thousands of them.
- A single Mist Edge can support 10000 AP and 100000 Clients.

The components of the Centralized Architecture solution include the following:

- Mist AP
- Mist Edge Appliance:

	Appliance				VM
Key Metrics	Mist Edge –X1	Mist Edge –X5	Mist Edge – X5-M	Mist Edge – X10	Mist Edge - VM
# AP	500	5000	5000	10000	500
# Clients	5000	50000	50000	100,000	5000
Throughput	2 Gbps	20 Gbps	40 Gbps	40 Gbps	2 Gbps

- Mist WiFi Assurance subscription (1x per AP) where X is 1,3 or 5 Years of service:

  SUB-1S-<**X**>Y

- Mist Edge subscription (1x per AP), where X is 1, 3 or 5 years service:

  SUB-ME-1S-<**X**>Y

Recommended additional components:

- Mist Marvis subscription (1x per AP) where X is 1, 3 or 5 years of service:

  SUB-1S-<**X**>Y

Note : Mist Edge VM has part number ME-VM that needs to be used for quotes. 1 ME-VM license allows any number of Mist Edge VM per org for a 1000 AP limit.

How it works

Mist solution leverages Mist Edge for extending centralized corporate/production/guest network vlan to APs using L2TPv3 tunnel. Mist Cloud orchestrates the Tunnel , Datapath continues to work even if Mist Edge or AP’s Cloud connectivity to Mist Cloud is lost.

Mist Edge is based on multi service architecture , so individual services can be upgraded as and when required and takes a maximum of 3 seconds and does not require a Mist Edge reboot.

AP firmware and Mist Edge service version are decoupled , upgrading a Mist Edge does not warrant an AP firmware upgrade.

APs can form Multiple Tunnels to different Mist Edge Cluster on Site, DMZ and Datacenter , user traffic can be mapped to be tunneled or local bridged based on Radius attribute returned for Dot1x authenticated wireless LAN.

APs can support Tunneled and Local Bridged Wireless LAN together and are not mutually exclusive.

Mist cloud-driven AI provides unprecedented user experience visibility via Service Level Expectations (SLE) framework, AI-driven Marvis engine with natural language processing for troubleshooting and root cause analysis and Marvis actions, which IT can leverage for remote troubleshooting of user issues without spending any additional resources.

Configuration Steps

The configuration process is very straightforward and consists of the following steps. Once the initial configuration is done, no pre-staging of the Access Points is required, they can be shipped directly to the branch or Campus and brought online.

Setup Mist Edge

Mist Edge typically resides in the DMZ/DC/Campus with one arm connected to the Internet and another arm going into a trusted corporate network. First, it is necessary to understand physical port connections before proceeding to the actual configuration.

<u>**Connect Cables - Physical Port Connections:**</u>

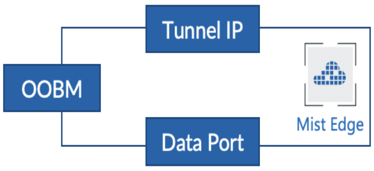
The following snippet outlines Mist Edge port configuration requirements:

Tunnel IP is the interface where AP communicates with to setup the L2TPv3 Tunnel between AP and Mist Edge. This IP needs to be configured from Tunnel IP section on Mist UI. If there is a firewall between AP management subnet and Mist Edge Tunnel IP , traffic destined to Tunnel IP on port 1701 needs to be allowed.

The Out-of-Band-Management (OOBM)

Interface communicates with the Mist cloud and is there to configure, send stats and check status of Mist Edge , Mist Edge Cluster and AP Tunnels.

Interface expects a DHCP IP address by default and can be configured with static IP address

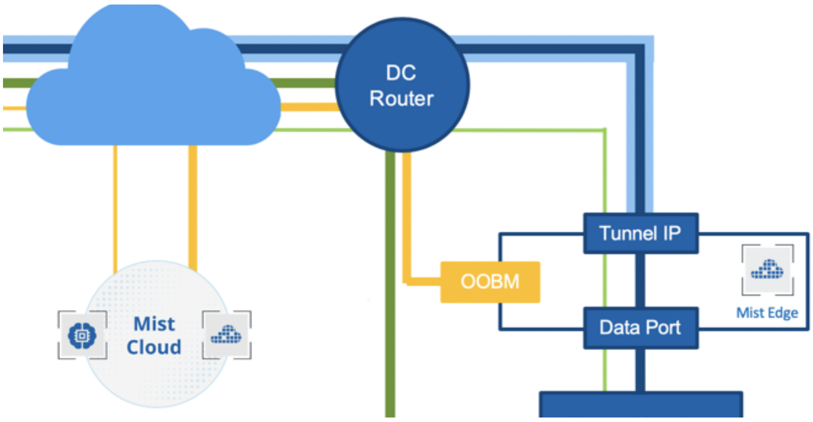


Data Port is connected to a trunk port that has all the VLANs configured where the WLAN need to be mapped to

Note : OOBM IP and Tunnel IP are different IP addresses and need to be from different subnets.

Request to Keep the Switch ports to which Data ports (ge0,ge1) on ME-X1 or (Xe0,Xe1) on ME-X5 and (Xe0,Xe1,Xe2,Xe3) on ME-X5-M and ME-X10 are connected shut down until Mist Edge is configured for Tunnel IP and Mist Tunnel details.

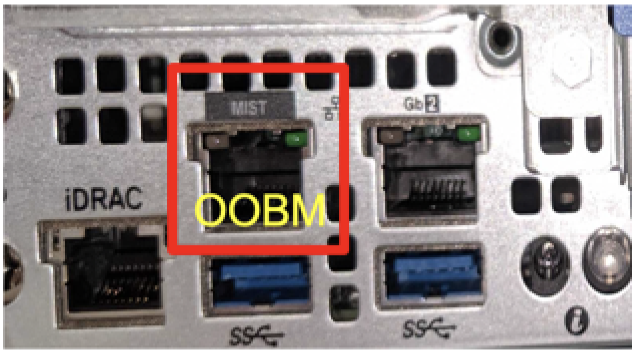
1. **Out of Band Management Port:**



Connect Out-Of-Band-Management Port (OOBM) of the Mist Edge to an untagged interface of your switch. OOBM port is used by the Mist Edge to communicate to the Mist Cloud:

Note: OOBM port on the Mist Edge appliance is marked as "MIST". By default OOBM port is configured to obtain an IP address via DHCP, it can be later changed to use static IP configuration.

The following figures shows OOBM port on X1 Mist Edge appliance:



Mist Edge comes pre-loaded with a custom debian linux installed. To configure static IP on the OOBM port, add the following lines to the interfaces config. Use iDrac interface or connect keyboard and monitor to the appliance for the OOBM initial staging if DHCP is not available. The default username and password for Mist Edge appliance is *mist* / *<Claim-code>*, default root (su -) password is *<Claim-code>*. Note the right interface id based on your MistEdge Appliance Model:

```
nano /etc/network/interfaces

iface eno1 inet static
        address 192.168.50.50/24
        gateway 192.168.50.1
        dns-nameservers 8.8.8.8 8.8.4.4
```

Please update the DNS entries as well.

```
nano /etc/resolv.conf

nameserver 8.8.8.8
nameserver 8.8.4.4
```

After saving the file, reboot the Mist Edge to apply the settings.

OOBM Interface ID per Mist Edge (ME) model:

Mist Edge Appliance Model	Interface Id
X1	eno1
X5	eno3
X5-M / X10	enp59s0f0 (for Deb9 based ME) , ens1f0 (for Deb-10 based ME)

Note: All ZTP capable Mist Edge shipped with claim code are Debian 10 based.

The 'OOBM IP' received through DHCP or assigned static while bringing up the Mist Edge is different from 'Tunnel IP' that is entered in the Mist Edge details on Mist Dashboard (Mist UI

So 2 IP addresses need to be set aside for Mist Edge , one for OOBM and other for Tunnel IP, they should be from different subnets.

In order for the Mist Edge to communicate to the Mist Cloud the following FQDNs and ports must be allowed for the OOBM interface.

For US cloud environment:

```
ep-terminator.mistsys.net : TCP port 443
```

For GCP cloud environment:

```
ep-terminator.gc1.mist.com : TCP port 443
```

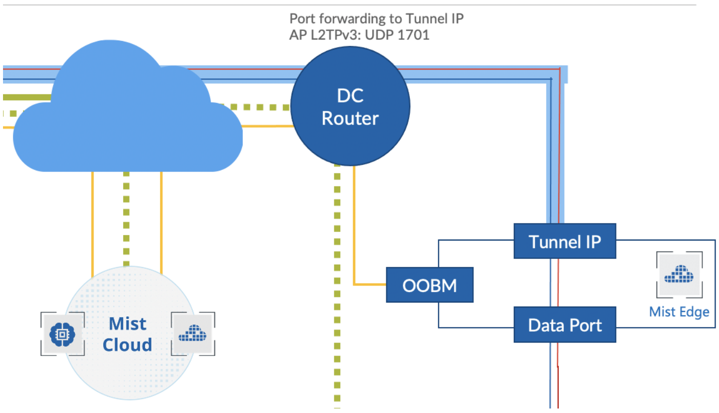
For EU cloud environment:

```
ep-terminator.eu.mistsys.net : TCP port 443
```

2. **Tunnel IP or Downstream Port**:

   Connect your Downstream port to the untrusted side of your network that typically goes to your firewall. Downstream Port must be connected to the *untagged* interface.

   Make sure that your router/FW either does Port Forwarding to the Tunnel Interface IP address (UDP port 1701) This is the interface/IP to which APs from a site or multiple site will be talking to in order to establish a L2TPv3 tunnel:

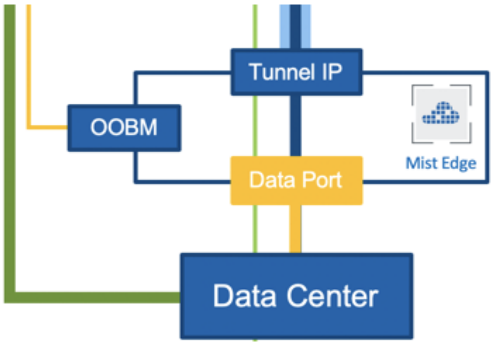


   Note: Tunnel IP SVI on Mist Edge is a protected interface , so even it its not connected to Firewall , it is only open for ports UDP: 1701 (L2TPv3) , 500 and 4500 (IPsec) and TCP port 2083 for Radsec.

   For Remote worker use case alone Mist Edge will be using UDP port 500,4500 and TCP port 2083 , all other Campus and Branch use cases it will just use UDP port 1701

3. **Upstream Data Port**:

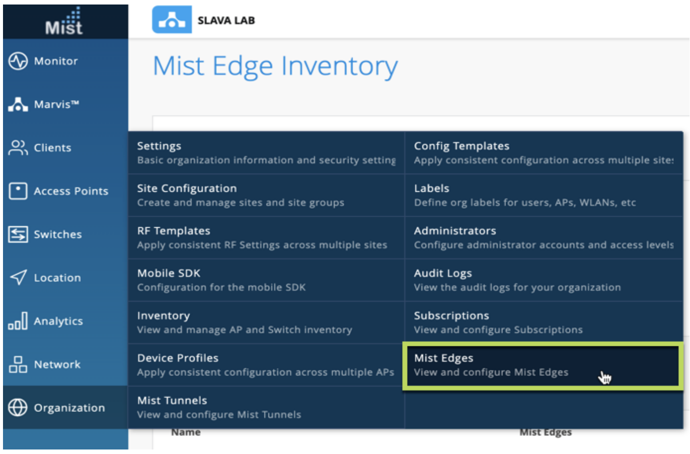
   Connect your Upstream port to the trusted side of the network. This interface would typically connect to your core/agg switch with all the necessary user VLANs *tagged*.



Now after all interfaces have been connected to the correct ports, it is time to register and configure Mist Edge in the Mist Cloud Dashboard.

Mist Edge Claim on the Mist Dashboard:

On the Mist Dashboard navigate to Organization ⟶ Mist Edges and Click 'Claim Mist Edge':



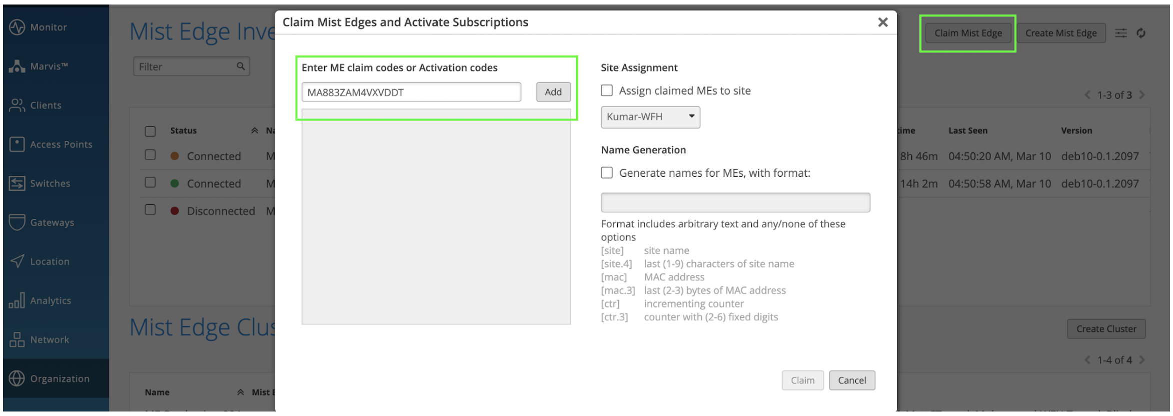
SLAVA LAB

Mist Edge Inventory

- Monitor
- Marvis™
- Clients
- Access Points
- Switches
- Location
- Analytics
- Network
- Organization

Settings Basic organization information and security setting	Config Templates Apply consistent configuration across multiple site:
Site Configuration Create and manage sites and site groups	Labels Define org labels for users, APs, WLANs, etc
RF Templates Apply consistent RF Settings across multiple sites	Administrators Configure administrator accounts and access levels
Mobile SDK Configuration for the mobile SDK	Audit Logs View the audit logs for your organization
Inventory View and manage AP and Switch inventory	Subscriptions View and configure Subscriptions
Device Profiles Apply consistent configuration across multiple APs	Mist Edges View and configure Mist Edges
Mist Tunnels View and configure Mist Tunnels	

Enter the claim code received in PO or present on the service Tag:



Claim Mist Edges and Activate Subscriptions

Enter ME claim codes or Activation codes

MA883ZAM4VXVDDT Add

Site Assignment

□ Assign claimed MEs to site

Kumar-WFH

Name Generation

□ Generate names for MEs, with format:

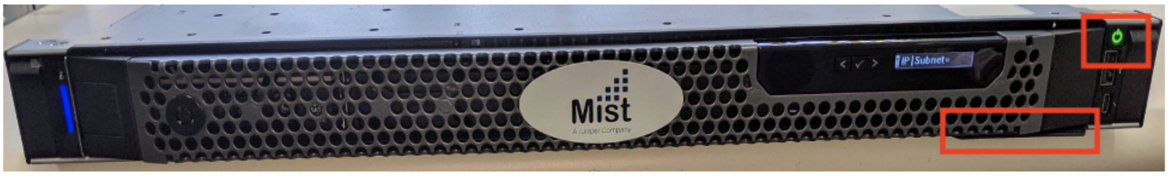
Format includes arbitrary text and any/none of these options

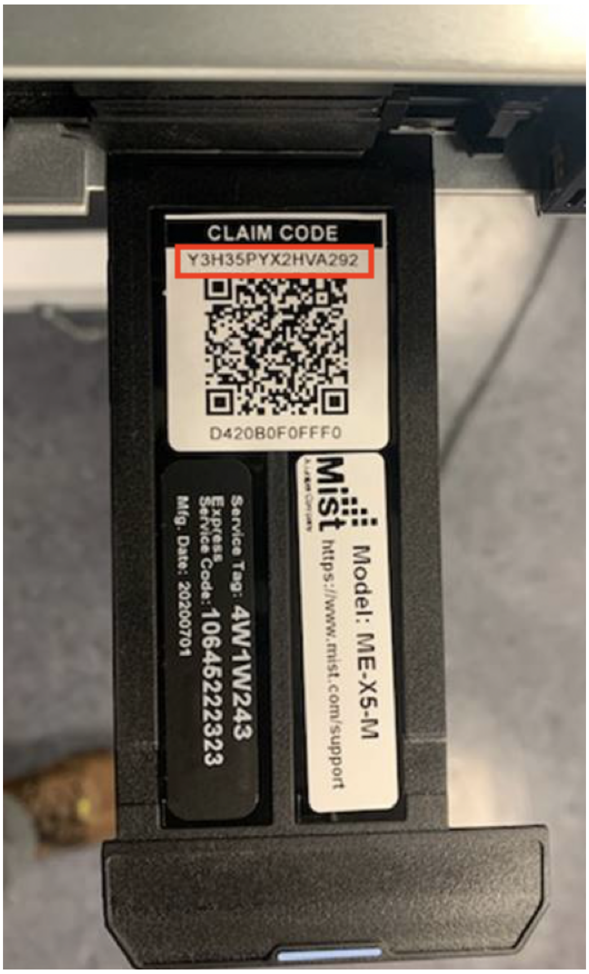
[site]	site name
[site.4]	last (1-9) characters of site name
[mac]	MAC address
[mac.3]	last (2-3) bytes of MAC address
[ctr]	incrementing counter
[ctr.3]	counter with (2-6) fixed digits

Claim Cancel

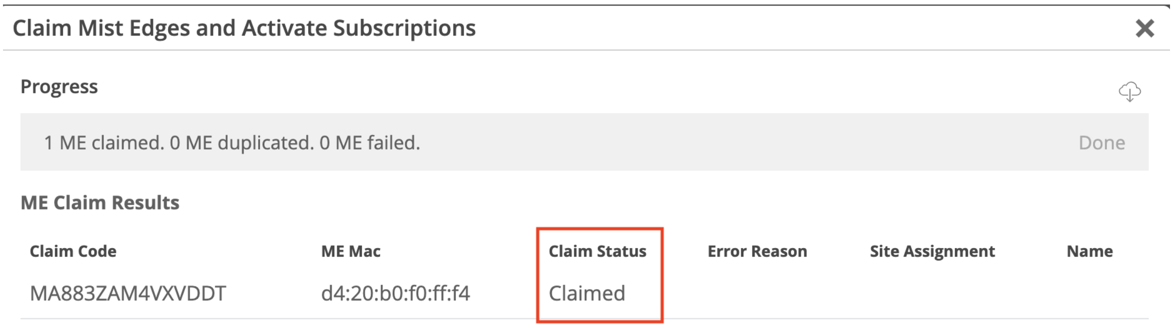
Claim Code can be found on the service Tag of Mist Edge located below the power button as shown below. Service Tag can be pulled out:

Ensure Mist Edge is powered on and the Power button shows Green.





After the Mist Edge is claimed it will show up as Disconnected and Registered, select it to edit settings:



Claim Mist Edges and Activate Subscriptions

Progress

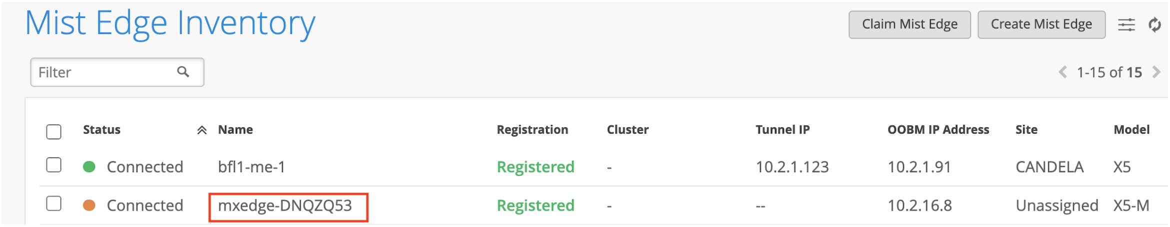
1 ME claimed. 0 ME duplicated. 0 ME failed.

ME Claim Results

Claim Code	ME Mac	Claim Status	Error Reason	Site Assignment	Name
MA883ZAM4VXVDDT	d4:20:b0:f0:ff:f4	Claimed			

Mist Edge will download Tunnel terminator service and Reboot in 3 minutes to show connected.

This reboot is only the first time when Mist Edge is brought online, future service upgrades only take 3 seconds and does not require Reboot.



Mist Edge Inventory

□	Status	Name	Registration	Cluster	Tunnel IP	OOBM IP Address	Site	Model
□	● Connected	bfl1-me-1	Registered	-	10.2.1.123	10.2.1.91	CANDELA	X5
□	● Connected	mxedge-DNQZQ53	Registered	-	--	10.2.16.8	Unassigned	X5-M

In case of Mist Edge not showing connected even after 5 minutes , one can SSH to the Mist Edge appliance using the Out-Of-Band management IP address that we have configured in the previous step. The default username and password for Mist Edge appliance is *mist* /<Claim-code>, default root password is <Claim-code>. Make sure you drop into root (`su –`) to issue a few debug commands . Issue the following commands to check connectivity to Mist Cloud:

a. Issue 'mxagent info' , which will show output similar to below:

   mxagent info

   Status: Registered

   IP: 10.2.10.224

   Mist Reachable: Yes

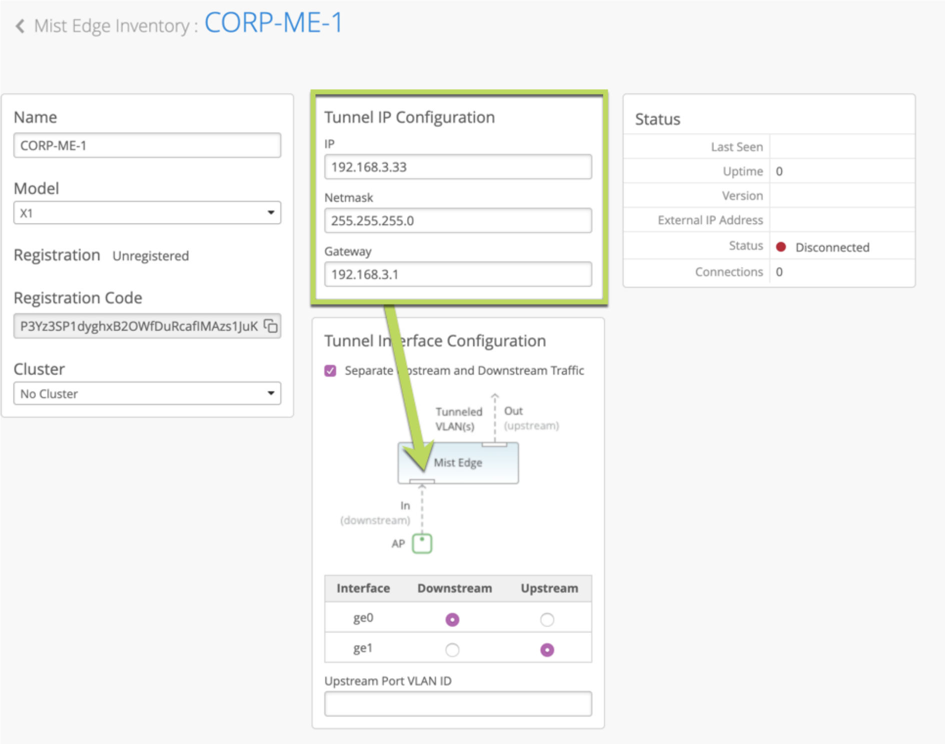
   Org ID: <Current-Org-Id to which it is Registered>

b. ping ep-terminator.mistsys.net

   If Ping is successful , request to ensure 443 outbound to ep-terminator.mistsys.net is allowed , which should ensure Mist Edge shows up connected.

Note: Above URL will be ep-terminator.gc1.mist.com or ep-terminator.eu.mistsys.net if its GCP or EU cloud instance that Mist Edge is being claimed against.

In the setting page first enable “Separate Upstream and Downstream Traffic”. Assign correct interface IDs to the correct interfaces. In the below example we are using X1 Mist Edge, where ge0 interface is connected to the public untrusted side and ge1 interface is connected to the corporate network with all the user VLANs tagged:



‹ Mist Edge Inventory : CORP-ME-1

Name: CORP-ME-1

Model: X1

Registration: Unregistered

Registration Code: P3Yz3SP1dyghxB2OWfDuRcafIMAzs1JuK

Cluster: No Cluster

Tunnel IP Configuration

IP: 192.168.3.33

Netmask: 255.255.255.0

Gateway: 192.168.3.1

Status

Last Seen	
Uptime	0
Version	
External IP Address	
Status	● Disconnected
Connections	0

Tunnel Interface Configuration

☑ Separate Upstream and Downstream Traffic

Interface	Downstream	Upstream
ge0	●	○
ge1	○	●

Upstream Port VLAN ID

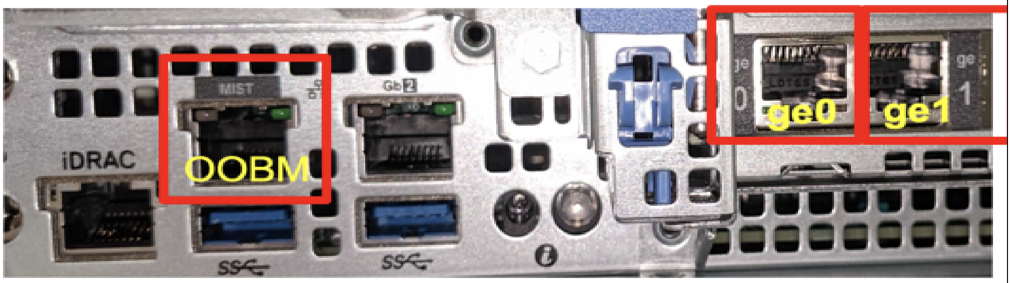
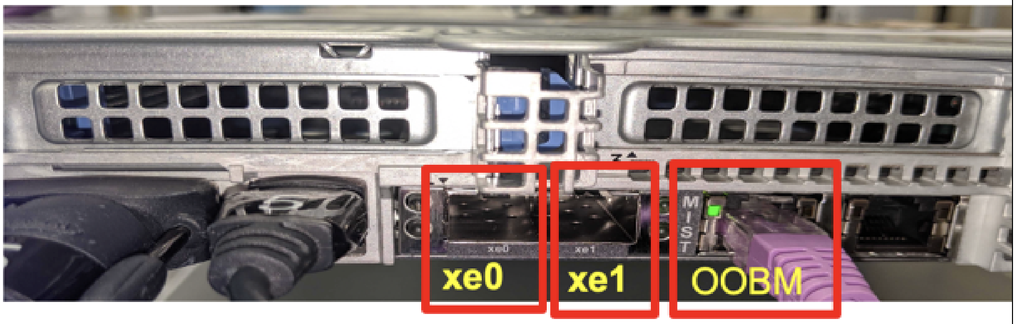
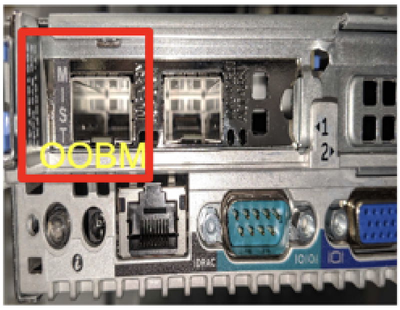
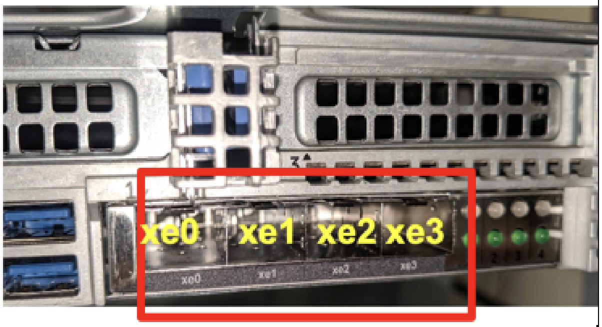
Note: a. Upstream Port VLAN ID is optional and should only be used whenever the upstream switchport is configured as an access port with a single VLAN untagged.

b. The ‘OOBM IP’ received through DHCP or assigned static while bringing up the Mist Edge is different from ‘Tunnel IP’ that is entered in the Mist Edge details on Mist Dashboard (Mist UI).

So 2 IP addresses need to be set aside for Mist Edge , one for OOBM and other for Tunnel IP, they need to be from different subnets.

Based on your Mist Edge model the interface IDs might be different. Please use the image below that show individual model port mappings:

Note: Request to keep the data ports on switch side , that is corresponding ports to ge0,ge1 or xe0,xe1 or xe0,xe1,xe2,xe3 shutdown until Mist Edge is configured with Tunnel IP and ‘Mist Tunnel vlan’.

X1	
X5	
X5-M and **X10**	 

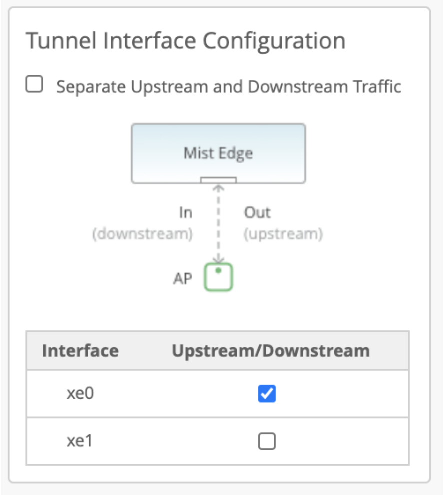
Note:

1. Instead of a Dual arm port config, that is separate port for Downstream and Upstream , one can useSingle arm - one port or multiple ports in the Port channel , where the corresponding switch port is trunk with Tunnel IP being native/untagged , rest of the client vlans are tagged.

If multiple ports are used they will be part of the port channel , listed below are those settings.

Mist Edge auto detects port channel.

Single Arm, Single port used

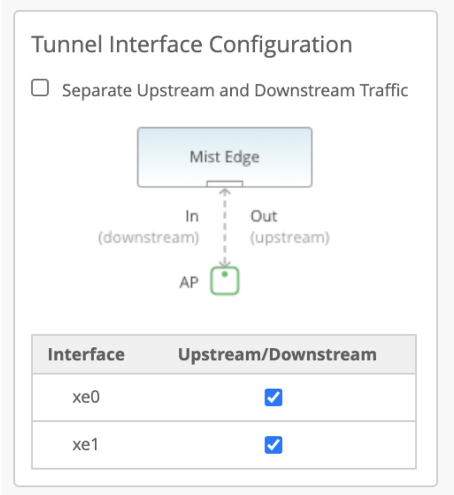


Tunnel Interface Configuration

□ Separate Upstream and Downstream Traffic

Interface	Upstream/Downstream
xe0	☑
xe1	□

Single Arm, Multiple ports in Port channel

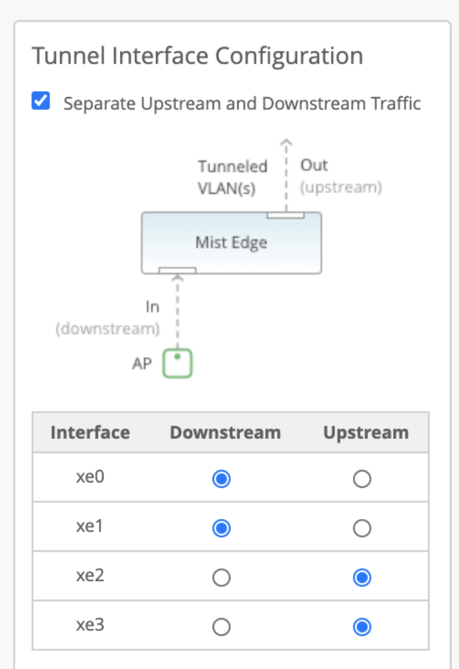


Tunnel Interface Configuration

□ Separate Upstream and Downstream Traffic

Interface	Upstream/Downstream
xe0	☑
xe1	☑

2. For a ME-X5-M and ME-X10 , one can do a port channel for Downstream and Upstream, where Downstream port channel is untagged Tunnel IP vlan and Upstream port channel is all tagged client vlan.



Tunnel Interface Configuration

☑ Separate Upstream and Downstream Traffic

Interface	Downstream	Upstream
xe0	●	○
xe1	●	○
xe2	○	●
xe3	○	●

3. For ME-X5, ME-X5-M and ME-X10 fiber ports;

   a. Request to use SFP Cable OM3 50/125µm / OM4.

      OS2 version is not supported.

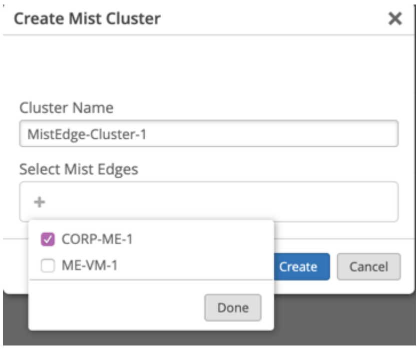
If the OS2 version is used, frequent LACP flap, packet errors, port not coming up will be observed.

The above issues get resolved once the SFP cable is replaced with OM3/OM4 type.

   b. If for ME-X5-M and ME-X10 , copper ports are required for OOBM (management port labelled as mist) , a Juniper Fiber to converter can be requested.

Create a Mist Edge Cluster:

Now that all the necessary services have been provisioned let's create a Mist Edge Cluster and add Mist Edge in there:



Create Mist Cluster

Cluster Name: MistEdge-Cluster-1

Select Mist Edges

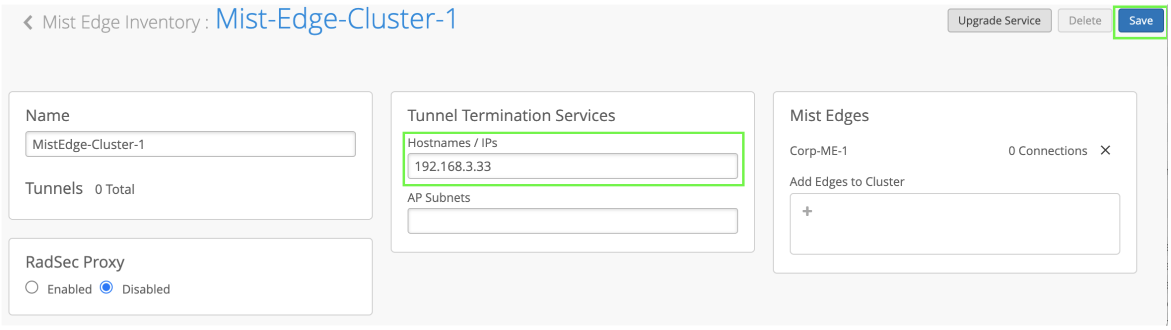
☑ CORP-ME-1

□ ME-VM-1

Under Mist Edge Cluster configuration, we will need to set our Cluster IP address(es) or FQDNs for the remote APs to communicate to.

In case your Firewall/Router is not doing a port forward to the Tunnel IP interface, IP specified on the Mist dge cluster will be the same IP configured on Mist Edge.

In case your Firewall/Router is doing a port forward to the Tunnel IP interface, you will need to specify the external IP address of your Firewall/Router that translates to Tunnel IP . In case multiple Mist Edges are part of the cluster, their respective IP addresses should be listed there, comma separated:



‹ Mist Edge Inventory : Mist-Edge-Cluster-1

Name: MistEdge-Cluster-1

Tunnels 0 Total

RadSec Proxy: ○ Enabled ● Disabled

Tunnel Termination Services

Hostnames / IPs: 192.168.3.33

AP Subnets:

Mist Edges

Corp-ME-1 0 Connections ✕

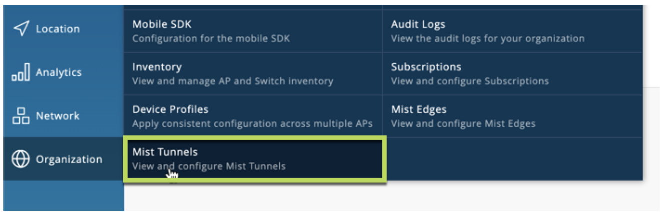
Add Edges to Cluster

+

Time to move to the next step and create a Mist Tunnel.

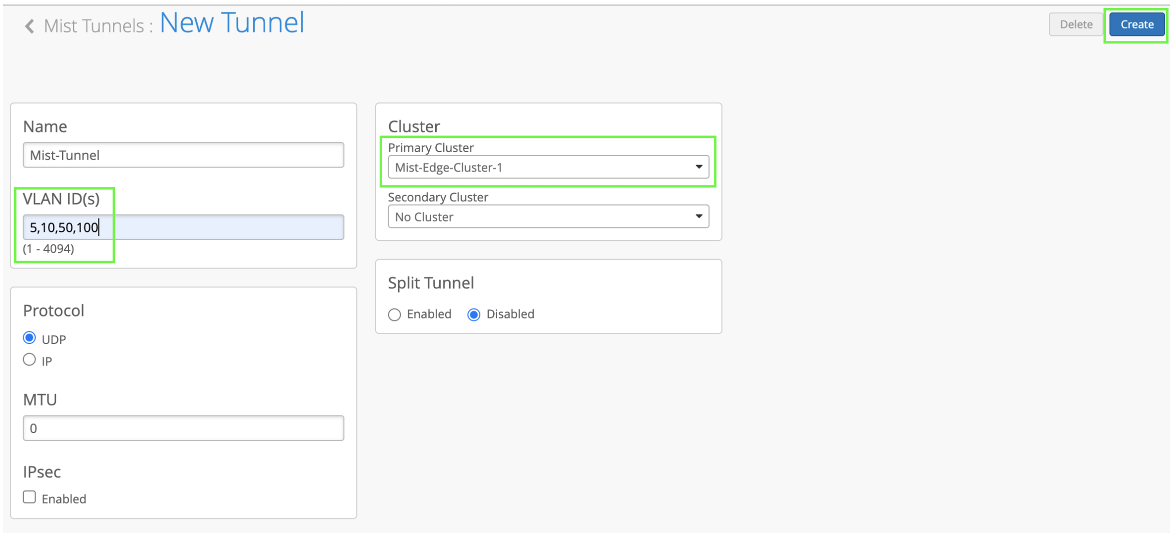
Setup the Mist Tunnel

Navigate to Organization → Mist Tunnels and Create a new Tunnel. Typically this is where you would list all your user VLANs (Client vlan) that you would like to extend from your corporate network to the APs . The VLAN list should be comma separated:



Location
Analytics
Network
Organization
Mobile SDK
Configuration for the mobile SDK
Audit Logs
View the audit logs for your organization
Inventory
View and manage AP and Switch inventory
Subscriptions
View and configure Subscriptions
Device Profiles
Apply consistent configuration across multiple APs
Mist Edges
View and configure Mist Edges
Mist Tunnels
View and configure Mist Tunnels

Once you create a Mist Tunnel, specify all user VLANs required to be tunneled back, assign the tunnel to the Mist Edge Cluster (s) we have created earlier, leave the rest of the setting as it is:



‹ Mist Tunnels : New Tunnel

Name: Mist-Tunnel

VLAN ID(s): 5,10,50,100 (1 - 4094)

Protocol: ● UDP ○ IP

MTU: 0

IPsec: □ Enabled

Cluster

Primary Cluster: Mist-Edge-Cluster-1

Secondary Cluster: No Cluster

Split Tunnel: ○ Enabled ● Disabled

Configure and prepare the SSID

The best way to provision your corporate SSID to extend vlan is to leverage Config Templates.

Navigate to Organization → Config Templates.

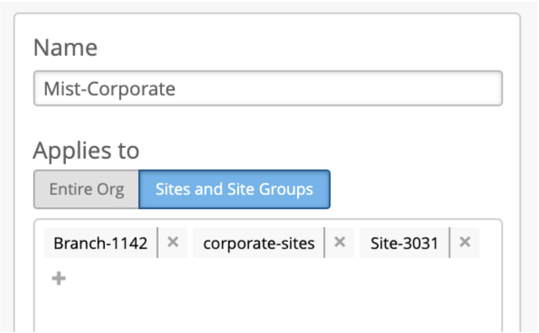
Create config template and use template assignment for either

a) Specific Sites or Site-Group, where individual sites will be mapped into a Site Group

or

b) Entire Org with actual office Sites added as exceptions. For example the following template will be assigned to all Sites, *except* Sites "HQ", "BranchA", and "BranchB".

Config Template assigned to Site/Site group

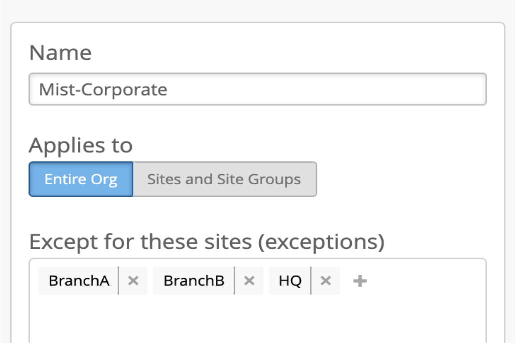


Name: Mist-Corporate

Applies to: Entire Org | [✓ Sites and Site Groups]

Branch-1142 ✕ corporate-sites ✕ Site-3031 ✕ +

Entire Org with some site exclusion.

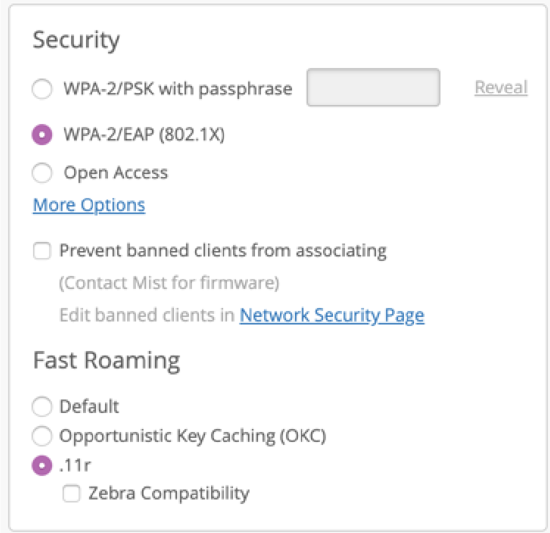


Name: Mist-Corporate

Applies to: [✓ Entire Org] | Sites and Site Groups

Except for these sites (exceptions): BranchA ✕ BranchB ✕ HQ ✕ +

SSID settings would depend upon particular customer requirements, but below are the most important parts with regards to vlan data tunneling back to the corporate network.



Security

○ WPA-2/PSK with passphrase Reveal

● WPA-2/EAP (802.1X)

○ Open Access

More Options

□ Prevent banned clients from associating (Contact Mist for firmware)

Edit banned clients in Network Security Page

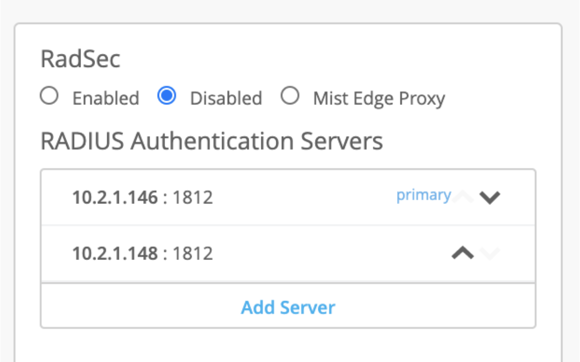
Fast Roaming

○ Default

○ Opportunistic Key Caching (OKC)

● .11r

□ Zebra Compatibility



RadSec

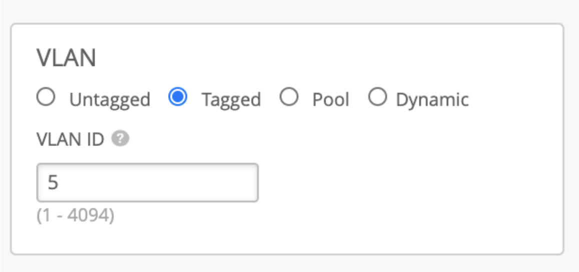
○ Enabled ● Disabled ○ Mist Edge Proxy

RADIUS Authentication Servers

10.2.1.146 : 1812 primary

10.2.1.148 : 1812

Add Server



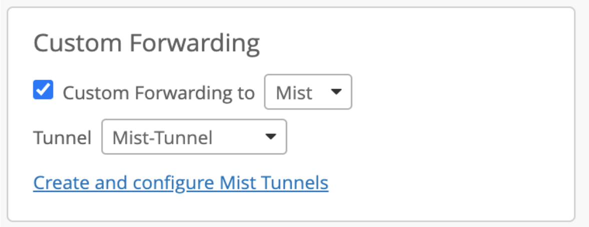
VLAN

○ Untagged ● Tagged ○ Pool ○ Dynamic

VLAN ID

5

(1 - 4094)



Custom Forwarding

☑ Custom Forwarding to Mist

Tunnel Mist-Tunnel

Create and configure Mist Tunnels

Note: Configuring one Config template per Wireless LAN makes it easier to manage SSIDs that need to be broadcast at a given site by using site and Site-groups.

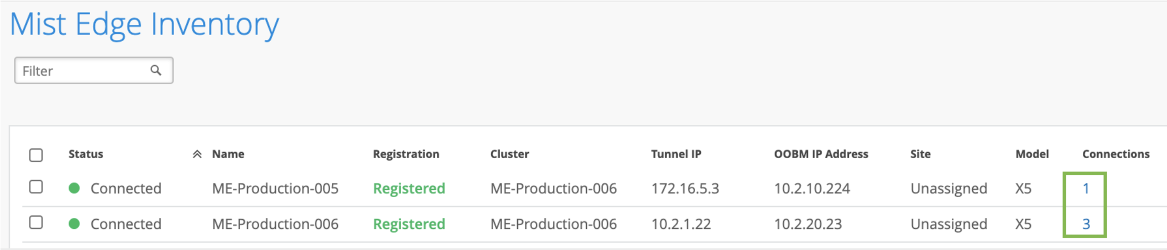
Create a Site for Campus, Branches

Sites can be created using UI under Organization → Site Configuration

Please note the following guidelines:

- For all APs, use AP firmware version 0.8.21301

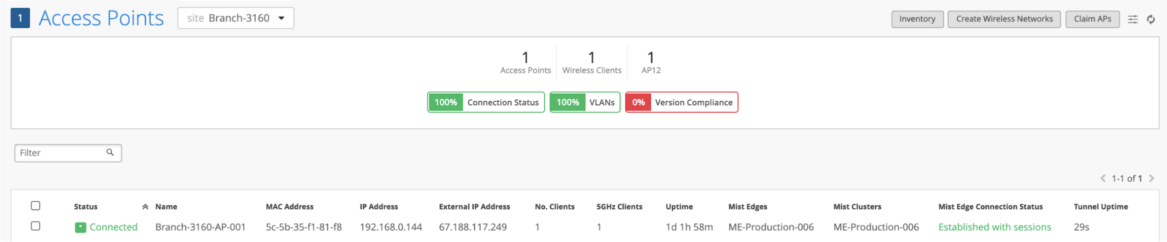
APs mapped to Tunneled Wireless LAN will form L2TPv3 tunnel and status can be confirmed on AP table as well as Mist Edge inventory.



Mist Edge Inventory

Filter

□	Status	Name	Registration	Cluster	Tunnel IP	OOBM IP Address	Site	Model	Connections
□	● Connected	ME-Production-005	Registered	ME-Production-006	172.16.5.3	10.2.10.224	Unassigned	X5	1
□	● Connected	ME-Production-006	Registered	ME-Production-006	10.2.1.22	10.2.20.23	Unassigned	X5	3



□	Status	Name	MAC Address	IP Address	External IP Address	No. Clients	5GHz Clients	Uptime	Mist Edges	Mist Clusters	Mist Edge Connection Status	Tunnel Uptime
□	Connected	Branch-3160-AP-001	5c-5b-35-f1-81-f8	192.168.0.144	67.188.117.249	1	1	1d 1h 58m	ME-Production-006	ME-Production-006	Established with sessions	29s

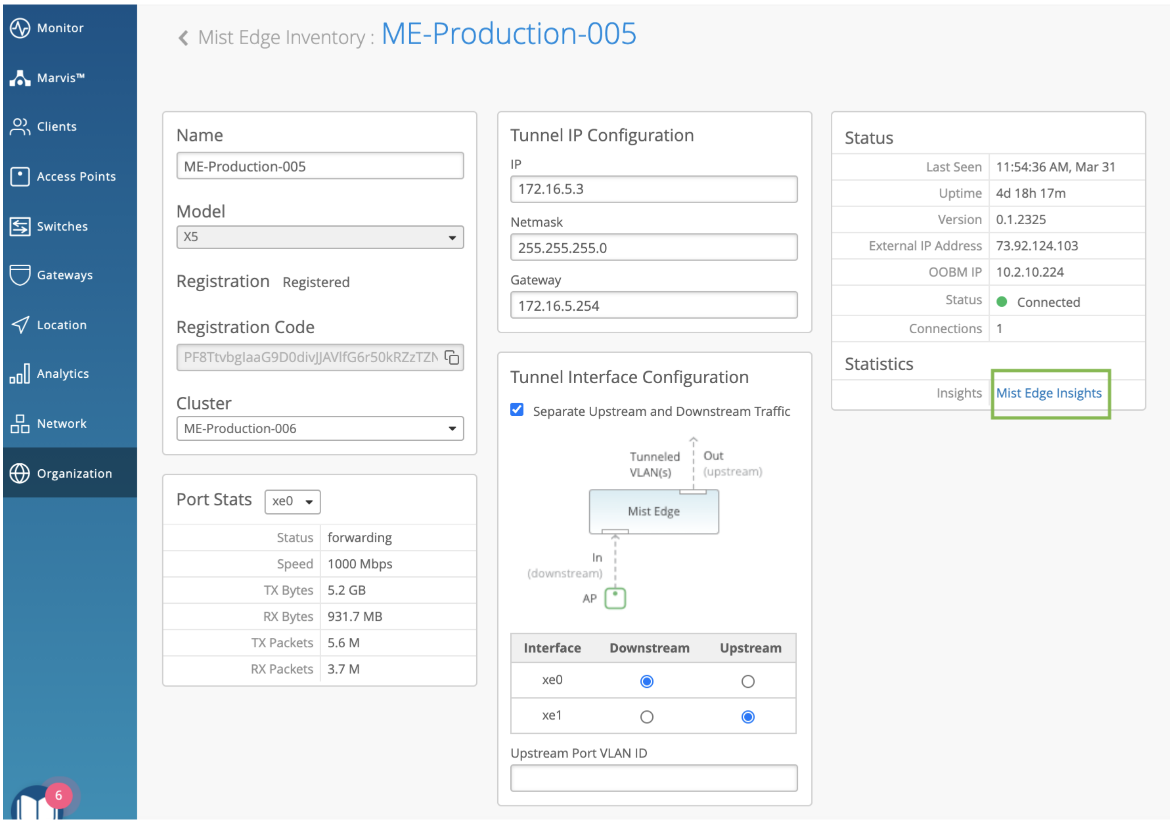
Mist Edge Insights

One can launch Mist Edge Insights from Mist Edge details.

Mist Edge Insights provide Insights into Tunnel trend, Mist Edge Events (service restarts, config changes, upgrade, Mist Edge reboots).

It also shows the Time series and list view of Data ports.

Provides LACP status and LACP neighbor info, makes it easier to verify the upstream switch port connections.



Mist Edge Inventory : ME-Production-005

Name: ME-Production-005

Model: X5

Registration: Registered

Registration Code: PF8TtvbglaaG9D0divJJAVlfG6r50kRZzTZN

Cluster: ME-Production-006

Port Stats: xe0

Status	forwarding
Speed	1000 Mbps
TX Bytes	5.2 GB
RX Bytes	931.7 MB
TX Packets	5.6 M
RX Packets	3.7 M

Tunnel IP Configuration

IP: 172.16.5.3

Netmask: 255.255.255.0

Gateway: 172.16.5.254

Tunnel Interface Configuration

☑ Separate Upstream and Downstream Traffic

Interface	Downstream	Upstream
xe0	●	○
xe1	○	●

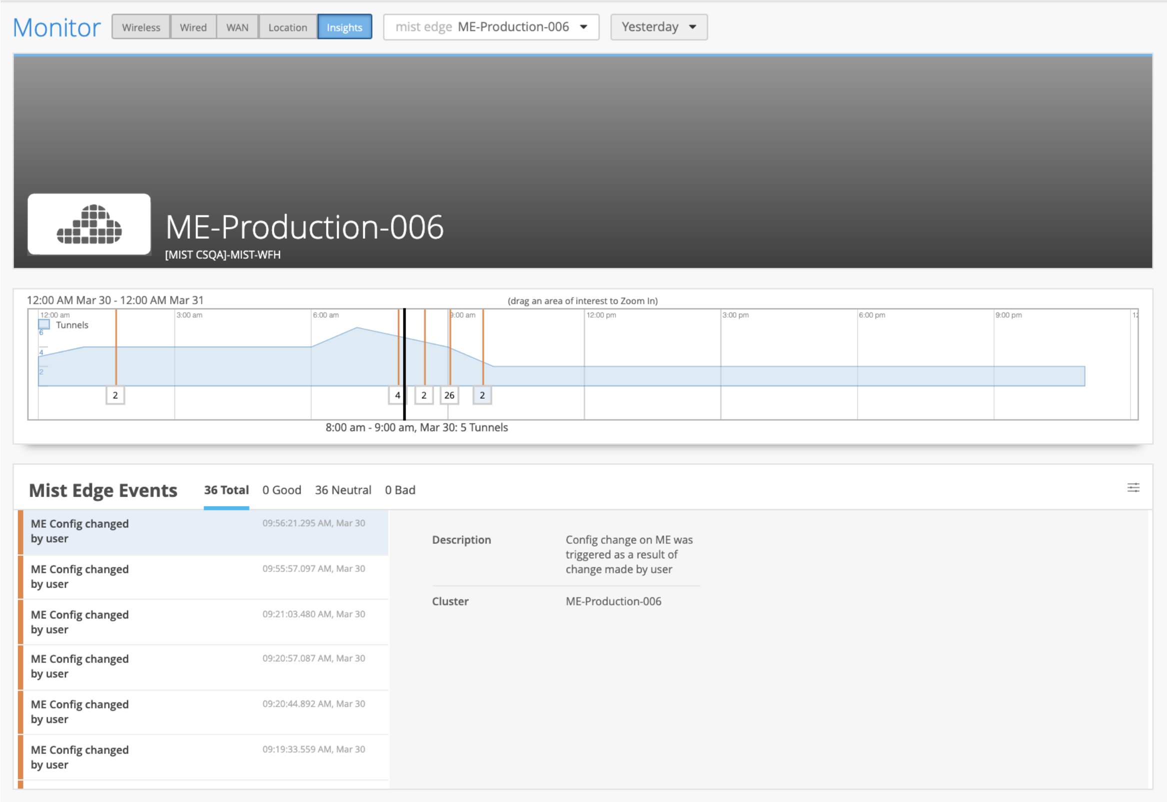
Upstream Port VLAN ID:

Status

Last Seen	11:54:36 AM, Mar 31
Uptime	4d 18h 17m
Version	0.1.2325
External IP Address	73.92.124.103
OOBM IP	10.2.10.224
Status	● Connected
Connections	1

Statistics

Insights	Mist Edge Insights



ME-Production-006

[MIST CSQA]-MIST-WFH

12:00 AM Mar 30 - 12:00 AM Mar 31

(drag an area of interest to Zoom In)

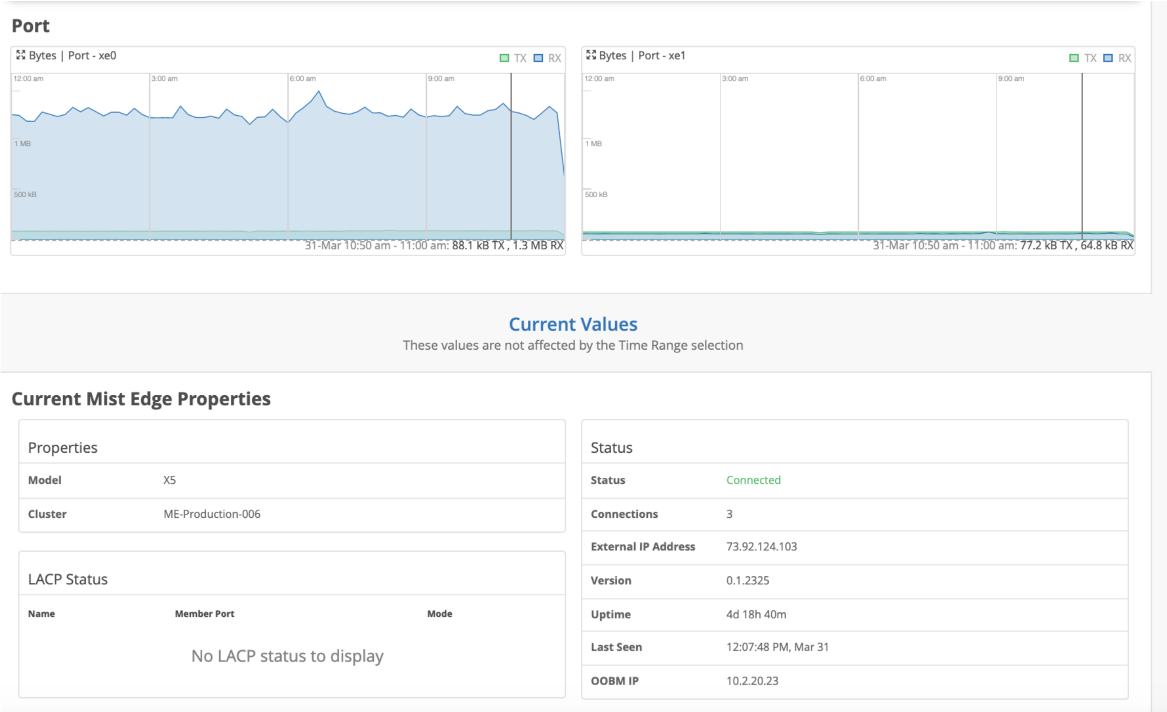
8:00 am - 9:00 am, Mar 30: 5 Tunnels

Mist Edge Events

36 Total 0 Good 36 Neutral 0 Bad

ME Config changed by user	09:56:21.295 AM, Mar 30
ME Config changed by user	09:55:57.097 AM, Mar 30
ME Config changed by user	09:21:03.480 AM, Mar 30
ME Config changed by user	09:20:57.087 AM, Mar 30
ME Config changed by user	09:20:44.892 AM, Mar 30
ME Config changed by user	09:19:33.559 AM, Mar 30

Description	Config change on ME was triggered as a result of change made by user
Cluster	ME-Production-006



Port

31-Mar 10:50 am - 11:00 am: 88.1 kB TX , 1.3 MB RX

31-Mar 10:50 am - 11:00 am: 77.2 kB TX , 64.8 kB RX

Current Values

These values are not affected by the Time Range selection

Current Mist Edge Properties

Properties

Model	X5
Cluster	ME-Production-006

LACP Status

Name	Member Port	Mode

No LACP status to display

Status

Status	Connected
Connections	3
External IP Address	73.92.124.103
Version	0.1.2325
Uptime	4d 18h 40m
Last Seen	12:07:48 PM, Mar 31
OOBM IP	10.2.20.23

Troubleshooting

To see established **L2TPv3 tunnels** from the MistEdge perspective:

Note: Ensure that '**curl** http://localhost:9110/debug/l2tp' shows a listener as shown below, if there isn't a listener that indicates Mist Cluster not updated with Tunnel IP.

```
root@ME-Production-005:~# curl http://localhost:9110/debug/l2tp

1 tunnels, 1 listeners.

Tunnels by state:

  State established-with-sessions: 1

tunnel between 10.137.70.14:43346 - Branch-3160-AP-001 - router-id
176.133.250.183 and 10.1.2.22:1701

 state established-with-sessions

.

.

listener at 10.1.2.22:1701
```

Packet Captures on the Mist Edge

Currently the packet capture facility on the Mist Edge is local to the appliance only, but it can be very useful to troubleshoot datapath at different entry points (inbound physical port, l2tpv3 tunnel, drop etc). In order to enable packet captures into the cli shell, it is necessary to instal tshark:

```
apt-get install tshark
```

After the tshark is installed you could use port debug command to list all the interfaces you can capture on:

```
root@ME-Production-005:~# curl http://localhost:9110/debug/ports

Port 0 "port0":

    PCI address: "0000:13:00.0"

    MAC: 00-0c-29-22-a4-d1

    PMD: "net_vmxnet3"

    link: true, duplex: true, Speed: 10000 Mbps

    state: Forwarding
    Rx: 314267822 bytes, 2253968 packets, 0+0 errors
    Tx: 282976995 bytes, 1947497 packets, 0 errors
    rx_good_packets: 2253968
    tx_good_packets: 1947497
    rx_good_bytes: 314267822
    tx_good_bytes: 282976995
    rx_q0packets: 2253968
    rx_q0bytes: 314267822
    tx_q0packets: 1947497
    tx_q0bytes: 282976995
Port 1 "port1":
    PCI address: "0000:1b:00.0"
    MAC: 00-0c-29-22-a4-db
    PMD: "net_vmxnet3"
    link: true, duplex: true, Speed: 10000 Mbps
    state: Forwarding
    Rx: 640727016 bytes, 1387326 packets, 0+79 errors
    Tx: 279571047 bytes, 1783598 packets, 0 errors
    rx_good_packets: 1387326
    tx_good_packets: 1783598
    rx_good_bytes: 640727016
    tx_good_bytes: 279571047
    rx_missed_errors: 79
    rx_q0packets: 1387326
    rx_q0bytes: 640727016
    tx_q0packets: 1783598
    tx_q0bytes: 279571047
```

```
Bridge port vlans:

[0] port0, PVID 1, Inactive Vlans [1]

[1] port1, Inactive Vlans [100]

[4] kni0, Inactive Vlans [1]

[11] L2TP session "mxtunnel" with 192.168.51.122:0 (d4-20-b0-02-63-5e),
Active Vlans [100]
```

Based on the example above, below are some sample packet capture syntax commands (more info available at `tt-pcap --help`)

```
root@ME-Production-005:~# tt-pcap -port=1 udp port 67 | tshark -nr -

Running as user "root" and group "root". This could be dangerous.

    1 0.000000000      0.0.0.0 ? 255.255.255.255 DHCP 346 DHCP Discover -
Transaction ID 0x12e3913a

    2 0.103353790 192.168.100.1 ? 192.168.100.135 DHCP 337 DHCP Offer    -
Transaction ID 0x12e3913a

    3 1.521102670      0.0.0.0 ? 255.255.255.255 DHCP 346 DHCP Request  -
Transaction ID 0x12e3913a

    4 2.133698590 192.168.100.1 ? 192.168.100.135 DHCP 337 DHCP ACK      -
Transaction ID 0x12e3913a
```