



JUNIPER Mist Edge Teleworker Solution User Guide

[Home](#) » [JUNIPer](#) » JUNIPER Mist Edge Teleworker Solution User Guide 



Juniper Mist Edge Teleworker Solution Guide
RELEASE
Published
2024-01-11

About the Guide

Use this guide to learn about Juniper Mist™ Teleworker solution to extend the corporate network to remote office workers.

Contents

- [1 Juniper Mist Teleworker Overview](#)
- [2 Create a Site for Remote Office Workers](#)
- [3 Set Up Juniper Mist Edge and Configure the WLAN Template](#)
- [4 Wired Client Connection Through ETH1 or the Module Port of the AP](#)
- [5 Split Tunneling for a Corporate SSID](#)
- [6 Claim and Ship an AP to an Employee Location](#)
- [7 Documents / Resources](#)
 - [7.1 References](#)

Juniper Mist Teleworker Overview

IN THIS SECTION

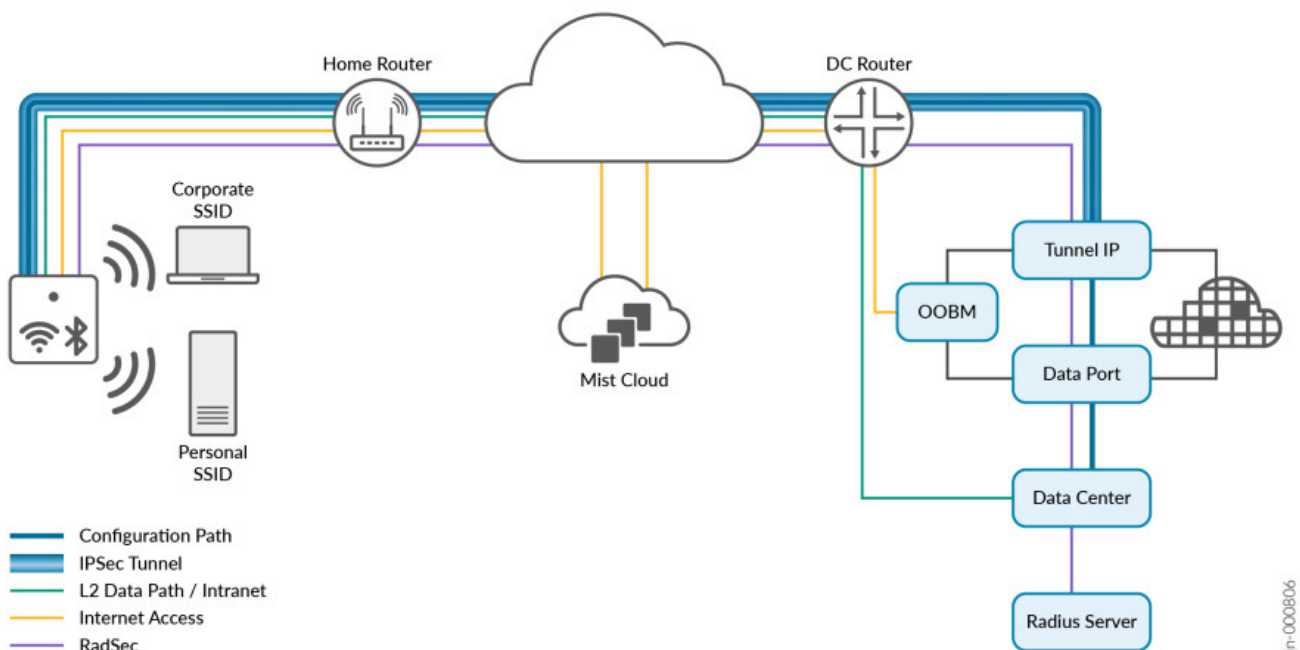
- Benefits of the Mist Teleworker Solution | 2

The Juniper Mist™ Teleworker solution leverages the Juniper Mist Edge architecture to extend the corporate network to remote office workers. Juniper Mist extends the network using an IPsec-secured L2TPv3 tunnel from a remote access point (AP). In addition, Juniper Mist Edge provides an additional RadSec service to securely proxy authenticated requests from remote APs. This feature facilitates the same user experience for remote workers as others have inside the office.

Juniper® cloud services, driven by Mist AI provide:

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

The following image illustrates the Juniper Mist Teleworker solution:



The components of the Juniper Mist Teleworker solution are:

- Juniper Mist access point (AP)
- Juniper Mist Edge appliance
- Juniper Mist Wireless Assurance subscription (1x per AP). SUB-1S-Y, where X is one, three, or five years of service.
- Juniper Mist Edge subscription (1x per AP). SUB-ME-1S-Y, where X is one, three, or five years of service.
- Juniper Mist Marvis subscription (1x per AP). SUB-ME-1S-Y, where X is one, three, or five years of service.

Benefits of the Mist Teleworker Solution

The Juniper Mist Teleworker solution offers the following benefits:

- Agility
- Zero-touch provisioning—Remove prior-staging requirement for APs.

- Network management with minimal effort—Leverage Marvis® Virtual Network Assistant and manage network performance with analytics about Juniper Mist service-level expectation (SLE) metrics.
- Firmware independence—Remove firmware dependency between an AP and Juniper Mist Edge. You can independently update the Juniper Mist Edge services in less than 3 seconds.
- Security
- Traffic isolation—The level of traffic control is similar to the level in the original wireless LAN controller architecture. Enable transparent movement of user traffic to a single central location, isolating it from your access switches.
- Automated security—Enable machine-driven site deployment without any credential exposure.
- Secure WebSocket to talk to the cloud.
- Endpoint Protection—Secure wireless and wired endpoints through PoE-out.
- Flexibility
- Reuse hardware.
- Support flexible all-home coverage with secure mesh capabilities.
- Enable employees to self-manage their home SSID.

Create a Site for Remote Office Workers

By using Juniper Mist to support remote workers, customers can extend their corporate WLAN to employees' homes whenever the employees work remotely.

You can create Sites in the Juniper Mist portal from the Organization>Site Configuration menu.

NOTE:

- For AP41 and AP43, the minimum AP firmware version required to support IPsec and split tunneling is 0.7.20289.
- For AP32/33 and AP12, the minimum AP firmware version required to support IPsec with split tunneling is 0.8.21022.

Set Up Juniper Mist Edge and Configure the WLAN Template

After the initial Juniper Mist™ configuration is complete, you do not need to pre-stage the access point (AP). You can ship the AP directly to the employee's house and be ready to serve clients within 20 seconds. Juniper Mist Edge typically resides in the DMZ where one arm connects to the Internet and another arm connects to trusted corporate network. Before you configure the WLAN templates to enable the corporate SSID, you must complete the following tasks:

Table 1:

Task	Refer to
Configure port connections and set up Juniper Mist Edge	Getting Started
Create the Juniper Mist Edge cluster	No Link Title
Create Mist tunnel	No Link Title
Enable RADIUS proxy service	No Link Title

To configure the WLAN template:

1. Configure WLAN template to enable a corporate service set identifier (SSID).
2. From the left menu of the Juniper Mist portal, select Organization > WLAN Templates.
3. In the WLAN Templates window, click Create Template.
4. In the New Template window, enter Name and assign the template to Entire Org or Site and Site groups.
Each remote home office site is placed into a Site Group called Remote Teleworker. If you prefer, you can place the entire organization in the site group and add physical office sites added as exceptions.
For example, the following template is assigned to all Sites except Sites “BranchA,” and “BranchB.”

Name

remote-teleworker

Applies to

Entire Org Sites and Site Groups

Except for these sites (exceptions)

Branch A × Branch B × +

5. Specify the security settings.
SSID settings depend on your organization's requirements. The following image illustrates the configuration of the 802.1X secure WLAN.

Security

Security Type

- ☐ MAC address authentication by RADIUS lookup
- ☐ Use EAPOL v1 (for legacy clients)
- ☐ Enable EAP-Reauth
- ☐ Prevent banned clients from associating

Edit banned clients in [Network Security Page](#)

Fast Roaming

- ☐ Default
- ☐ Opportunistic Key Caching (OKC)
- ☒ .11r
 - ☐ Zebra Compatibility

6. Specify the number of VLANs to be tunneled through the Edge appliance.

VLAN

☐ Untagged
 ☒ Tagged
 ☐ Pool
 ☐ Dynamic

VLAN ID ?

100

(1 - 4094)

A Juniper Mist access point (AP) does not tunnel a WLAN configured with an untagged VLAN.

7. For an organization-level deployment, specify Custom Forwarding to Mist and select a tunnel profile from the Tunnel drop-down menu. The Mist tunnel must specify the same VLANs that you want to tunnel.

Custom Forwarding

☒ Custom Forwarding to Mist ▼

Tunnel EAST-DC-Tunnel ▼

[Create and configure Mist Tunnels](#)

8. For site-level deployment, specify Custom Forwarding to Site Edge. The Site tunnel must specify the same VLANs that you want to tunnel.

Custom Forwarding

☒ Custom Forwarding to Site Edge ▼

Wired Client Connection Through ETH1 or the Module Port of the AP

IN THIS SECTION

- Example: AP12 Wired Port Configuration for Tunneling | 8
- Example: Second Port Configuration for AP41 | 11

Along with extending a corporate Juniper Mist network to remote office workers, you must also connect wired devices to the corporate network. For example, devices like a security camera and an IP phone require tight security policing on the firewall, after onboarding. Therefore, you must place these devices in a unique VLAN. You can configure the devices access point (AP) by AP or through AP overrides. If you prefer, you can create device profiles and assign these to the devices. In either case, the configuration is exactly the same.

Example: AP12 Wired Port Configuration for Tunneling

When multiple remote user APs require same port configuration, you can create a device profile and map the device profile to the APs. You can also configure individual APs as well.

The screenshot displays a network management interface with a blue sidebar on the left and a white configuration area on the right. The sidebar contains icons and labels for 'Clients', 'Access Points', 'Switches', 'Gateways', 'Location', 'Analytics', 'Network', and 'Organization'. The 'Access Points' section is currently selected. The main configuration area is titled 'Name' and contains a text box with 'Kumar-Home-AP12'. Below this is a 'Labels' section with a large empty box containing a '+' icon. The 'Site Assignment' section features a dropdown menu with 'Kumar-WFH' selected. The 'Device Profile' section has a dropdown menu with 'None' selected, and a tooltip is visible showing 'None' and 'AP12-Wired-Port' as options. The text 'for profile settings' is also visible.

Port configuration is as follows:

Port 0—AP management traffic is sent untagged. All local WLANs and VLANs are autotagged on Eth0. Therefore, you can configure Eth0 with List of VLAN ID(s) and set Port VLAN ID to 1.

Other ports— Map other ports to single VLAN or multiple VLAN as illustrated. If you map other port to single VLAN, the wired host receives IP address from that VLAN. If you configure other ports as a trunk with multiple allowed VLAN and one of them as native VLAN, it behaves as a trunk. Use the additional wired ports to extend a tunneled VLAN to a wired port.

Ethernet Properties

PoE Passthrough

☐ Enable ☒ Disable

Ethernet Port Configurations

☒ Enable ☐ Disable

Note: This will take over the automatically generated VLAN settings. Please ensure all necessary VLANs are specified on all ports.

Eth0

List of VLAN ID(s)

1

☒ Port VLAN ID (optional)

1

Eth1

☒ Enable interface ☐ Disable interface

List of VLAN ID(s)

5

☒ Port VLAN ID (optional)

5

Eth2

Note: This is only applicable for AP12

☒ Enable interface ☐ Disable interface

List of VLAN ID(s)

5,10

☒ Port VLAN ID (optional)

5

Eth3

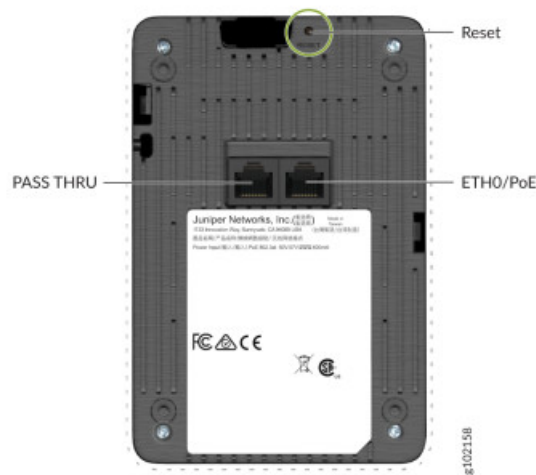
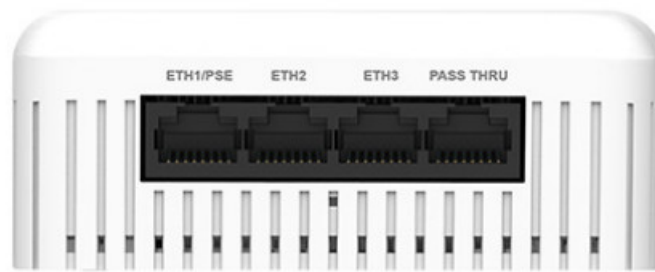
Note: This is only applicable for AP12

☐ Enable interface ☒ Disable interface

List of VLAN ID(s)

NOTE: Note: A wired port does not support split tunneling. Therefore, omit VLAN 1726 from the configuration. You can include VLAN 110 on a wired port, because it tunnels for the wired device. The following image illustrates the Eth0+PoE port and pass-through (Pass Thru) ports.

Figure 1: Eth0+PoE and Pass Thru Ports

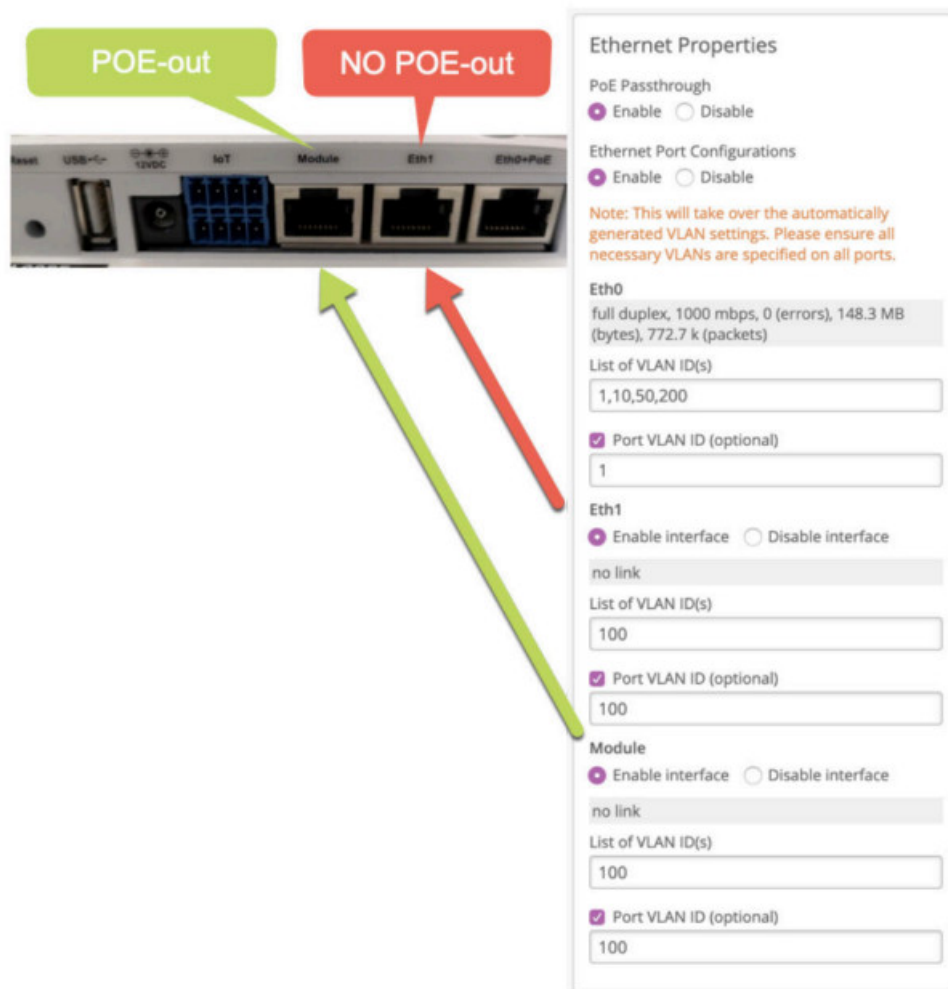


You can plug the Eth0+PoE port into the PoE switch or PoE brick to power on the AP12. The port uses a DHCP IP address for management. Pass-through ports marked Pass Thru act as a patch from the back to the side port. You can use a pass-through port in cases where you need to connect a device behind a wall mount, such as a TV in a hotel.

You can configure ports Eth1, Eth2, and Eth3 on the AP Details or Device Profile page in the Juniper Mist portal. You can map the ports to a management VLAN or a tunneled VLAN.

Example: Second Port Configuration for AP41

The following image shows the second port configuration for AP41.



In the example, Port VLAN ID is the same as Native VLAN ID or Untagged VLAN. Note that only the Module port is capable of providing power over Ethernet (PoE)-out to power a low-powered device, such as an IP phone. PoE Passthrough is supported only if a PoE injector—not a DC power supply—powers an AP.

NOTE: AP12, AP41, AP43 and AP45 can provide PoE-out. The following ports provide power over Ethernet (PoE)-out on different APs:

- Module port on AP41
- ETH1 on AP41 and AP43
- Passthrough port on AP12

Split Tunneling for a Corporate SSID

Juniper Mist Edge provides split-tunnel capability. This capability enables corporate clients to connect to local home devices (such as printers and media systems) while connected to the corporate network. You can enable this feature under the Mist Tunnel settings.

NOTE: Split-tunnel capability is applicable for a single remote AP at a site.

After you enable split tunneling, IP addresses listed in the Destination Subnet field are tunneled back to the Juniper Mist Edge. The rest IP addresses are locally bridged. Additionally, DNS Servers field, when configured, provides a way to use corporate DNS servers to resolve URLs/FQDNs for both tunneled and locally bridged traffic.

When you enable split tunneling, the AP serves the 192.168.157.X/27 IP address from a private subnet that it runs for clients. Traffic destined for the corporate office, defined in Destination Subnet, is translated to the corporate IP. The corporate IP is the IP that the AP receives from the VLAN of the corporate WLAN. The rest of the wireless client traffic is translated to the AP's management VLAN IP address.

Configure the Tunnel Gateway setting with the client subnet gateway. This is the gateway for the VLAN mapped to

the WLAN. Note that you can configure multiple destination subnets. You can also add the IP addresses and separate them by commas.

Make corporate DNS servers part of the Destination Subnet, or add the servers as a /32 entry.

The screenshot shows the Mist Edge configuration interface for a tunnel. The form is divided into several sections:

- Name:** A text field containing "ME-Tunnel1".
- VLAN ID(s):** A text field containing "20, 30" with a note "(1 - 4094)" below it.
- Cluster:** Two dropdown menus. The "Primary Cluster" is set to "ME-Cluster1" and the "Secondary Cluster" is set to "No Cluster".
- Tunnel Timers:** Two text fields. "Hello Interval" is set to "60" and "Hello Retries" is set to "7".
- Protocol:** Two radio buttons. "UDP" is unselected and "IP" is selected.
- MTU:** A text field containing "1300".
- IPsec:** A checkbox labeled "Enabled" which is checked.
- Connections Status:** A table showing connection status:

Connections Status	
Connected	0
Missing Connection	0
- Split Tunnel:** A section with a radio button set to "Enabled". Below it are three text fields:
 - DNS Servers:** "10.1.10.20, 10.20.12.15"
 - Destination Subnet:** "198.10.3.10/24"
 - Tunnel Gateway:** "198.16.20.30"

Claim and Ship an AP to an Employee Location

You can use the Juniper Mist™ AI app to claim an AP before shipping it to an employee's remote home office location. See <https://www.mist.com/documentation/mist-ai-mobile-app/>.

In the Mist AI app, select the site and Claim an AP to that site using the QR code on the back of the AP.

Then, still from the app, ship the AP to the employee's location. No need to connect it to the network before shipping!

For Remote Teleworker solution, ensure that the firewall is configured to allow the connection from remote AP. Consider the following guidelines:

- Allow port 500/4500 for IPsec and port 2083 for RadSec from remote APs
- Firewall must translate the destination IP of the packets from remote AP to the tunnel IP
- Obtain the external IP for the Mist Edge tunnel IP where a remote AP connects (usually a firewall IP), Append that IP to the hostname/IPs under tunnel termination services.

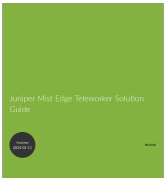
No additional configuration is required on Mist Edge or AP, other than selecting the tunnel type as IPsec and Radius to proxy through Mist Edge

Upon receiving the AP, the employee can now connect it to any of the Ethernet ports on the local home router (using a PoE injector or DC power). The AP is ready to serve the new, remote office in less than 20 seconds.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks,

Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Copyright © 2024 Juniper Networks, Inc. All rights reserved.

Documents / Resources

	<p>JUNIPER Mist Edge Teleworker Solution [pdf] User Guide</p> <p>Mist Edge Teleworker Solution, Mist, Edge Teleworker Solution, Teleworker Solution</p>
---	--

References

- [.:: Mist AI Mobile App - Mist](#)
- [User Manual](#)