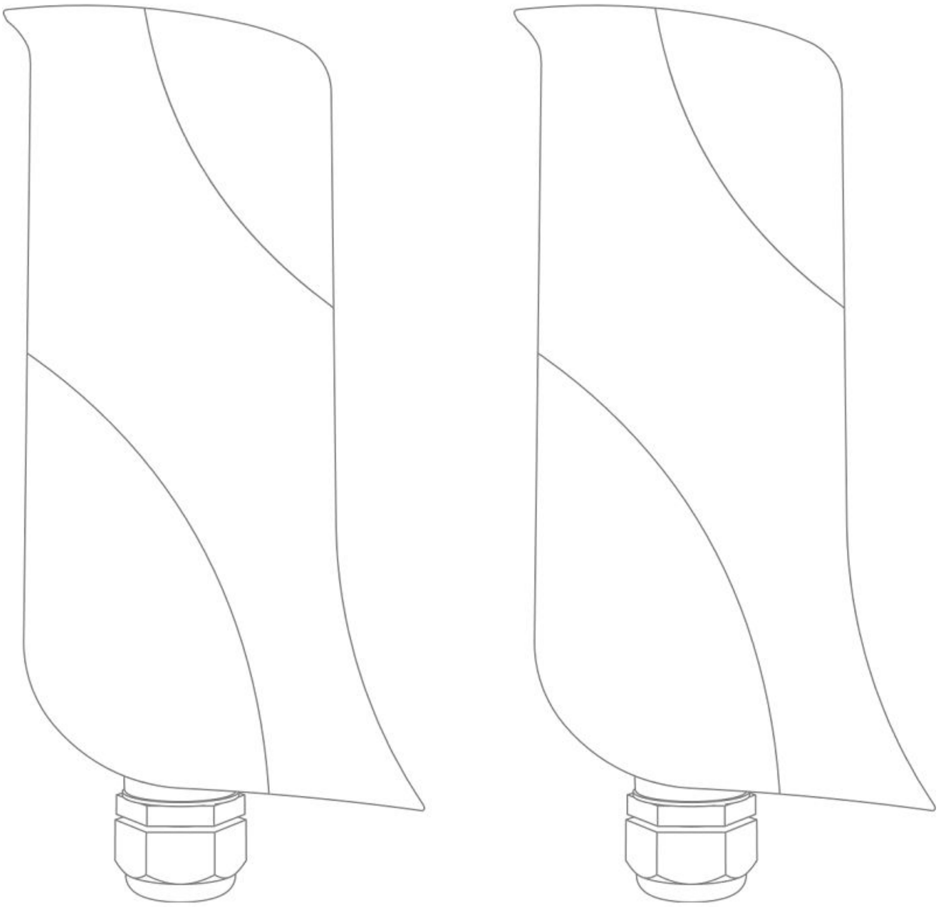


Cisco Ultra-Reliable Wireless Backhaul FM Ponte kit

Installation and Configuration Manual

(Formerly Fluidmesh)
Model FM1200V-HW | Edition 1.9 | Firmware 1.1 and 1.2.6

Table of Contents

1. HAZARDOUS CONDITION WARNINGS

Like all other global technology vendors, Cisco is required to complywith all local health and government regulations in the locations in whichwe operate. This includes meeting radio frequency (RF) exposure limitsfor our products.

Our equipment is tested in accordance with regulatory requirements as a condition to our ability to market and sell in any given jurisdiction. As an equipment manufacturer, Cisco defers to expert national and international health organizations responsible for guidance on the safety of RF signals, specifically the US Food and Drug Administration (FDA), Health Canada, the World Health Organization (WHO), and other national and global health agencies.

In May 2019, the FDA stated that there is "no link between adverse health effects and exposure at or under the current RF energy exposure limit", and that the current FCC RF exposure limits are sufficient to insure the safety of users.

If any Cisco hardware unit breaks down or malfunctions, emits smokeor an unusual smell, if water or other foreign matter enters the unit enclosure, or if the unit is dropped onto a hard surface or damaged in any way, power off the unit immediately and contact an authorized Cisco Networks dealer for assistance.

If you are adjusting and/or controlling a Cisco device using control software such as the RACER™ interface or the device's local Configurator interface, do not make configuration changes unless you know with certainty that your changes will not negatively impact people or animals in the vicinity of the device and its antennas.

1.1. Radio-frequency transmission hazard

WARNING

The system shown in this manual is designed to be installed and operated in a way that avoids contact with the antennas by human beings. The legislation quoted in this section is designed to reduce overall exposure of human beings to RF radiation.

This section gives minimum separation distances between antennas and humans. It is strongly recommended that the system be installed in a location where these minimum separation distances can be maintained at all times.

United States: This system has been evaluated for RF exposure for humans, in accordance with FCC regulation CFR 47 Part 2.1091. To maintain compliance, the minimum separation distance from the antenna to general bystanders is 20cm/7.9in. (all FM Ponte kit and x200 radio transceivers), or 21cm/8.3 in. (all FM1300 Otto and x500 radio transceivers).

Canada: This system has been evaluated for RF exposure for humans, in accordance with ISED regulation RSS-102. To maintain compliance, the minimum separation distance from the antenna to general bystanders is 20cm/7.9in. for all Cisco radio transceivers.

Europe / Australia / New Zealand: This system has been evaluated for RF exposure for humans, in accordance with standard EN 62232. To maintain compliance, the minimum separation distance from the antenna to general bystanders is 20cm/7.9in. for all Cisco radio transceivers.

Before activating any device capable of transmitting RF signals, make sure that all persons and animals are protected from possible RF exposure.

Make sure that all RF feeds are securely connected to an appropriate antenna. Never activate any RF-capable device that is not connected to an antenna.

2. Reporting mistakes and recommending improvements

You can help improve this manual.

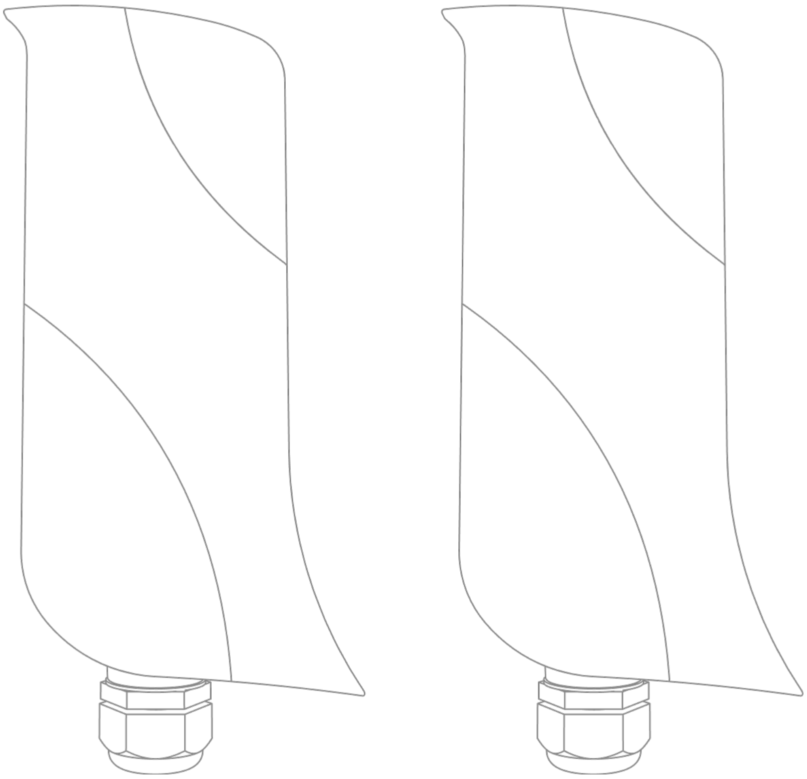
If you find any mistakes, or if you know of a way to improve the procedures that are given, please let us know by E-mailing your suggestions to documentation@cisco.com.

3. Getting Started

3.1. Introduction

3.1.1. Cisco FM Ponte kit

The Cisco FM Ponte kit radio transceiver



Introduction

The Cisco FM Ponte kit (model FM1200V-HW) is designed to operate in the sub-6 GHz range as a wireless data backhaul link. In non-technical terms, this means it is designed to function as an intermediate radio link between a core wired data network and a sub-network. The unit has an integrated, internally mounted 33° panel antenna capable of transmitting and receiving between 5.0 GHz and 6.0 GHz. A separate antenna cannot be installed or mounted.

IMPORTANT

Note that FM Ponte and FM1200 Volo transceivers utilize different communication protocols, and cannot communicate with each other.

Unit function and throughput speed

The unit is an entry-level networking solution consisting of two radio transceiver units. It is designed to handle video, voice, and data with extremely high reliability. It can be used to create point-to-point network links with real throughput of up to 50 Mbps (under optimal wireless link conditions), with a theoretical maximum distance between units of up to 3 miles (4.83 Km). The Cisco FM Ponte kit can be used to create parts of a wireless network architecture composed of point-to-point (P2P) links, with network activity 'transparent' to the network hosts. As a typical example, this type of operation allows two local networks to communicate with each other.

IMPORTANT
The Cisco FM Ponte kit cannot be switched to *Mesh Point* mode or *Mesh End* mode.

Unit configuration

The unit is programmed using a built-in Configurator interface. This is an offline interface that allows you to configure, monitor, and troubleshoot the unit.

Environmental rating

The unit is certified for outdoor usage, equipped with vibration-proof connectors, and designed for fast installation and enhanced reliability in harsh environments.

Product specifications

For detailed product specifications, refer to the product data sheet for the Cisco FM Ponte kit.

Transceiver and gateway unit power consumption

In service, Cisco transceiver units and gateway units consume electrical power at the rates given in the table below.

IMPORTANT
In service, transceiver and gateway units will consume power at various levels between the quoted lower limit and upper limit, depending on data traffic load, signal strength, environmental conditions such as line-of-sight and atmospheric moisture, and other factors.

Note that the power consumption of transceiver units tends to be affected in inverse proportion to the unit temperature (in other words, power consumption tends to rise when the temperature of the unit falls, and the other way around).

Table 1. Power consumption figures (transceiver units)

Unit series	Minimum power consumption	Nominal power consumption (typical conditions)	Maximum power consumption (realistic system-design assumption)
FM Ponte kit (Model FM1200V-HW)	4 Watts	6 to 7 Watts	10 Watts
FM1200 Volo (Model FM1200V-HW)	4 Watts	6 to 7 Watts	10 Watts
FM1300 Otto	8 Watts	10 to 12 Watts	15 Watts
FM3200-series (Model FM3200)	4 Watts	6 to 7 Watts	10 Watts
FM4200-series (Models FM4200F and FM4200)	4 Watts	6 to 7 Watts	10 Watts
FM3500 Endo (Model FM3500)	8 Watts	10 to 12 Watts	15 Watts
FM4500-series (Models FM4500F and FM4500)	8 Watts	10 to 12 Watts	15 Watts
FM 4800 Fiber	13 Watts	15 to 17 Watts	20 Watts

Table 2. Power consumption figures (gateway units)

Unit	Maximum power consumption (realistic system-design assumption)
FM1000 Gateway	60 Watts
FM10000 Gateway (Gen. 1)	275 Watts (redundant AC power supply) 250 Watts (non-redundant AC power supply)
FM10000 Gateway (Gen. 2)	300 Watts (redundant AC power supply)

3.2. Cisco Architecture

3.2.1. Overview

Wireless network architectures

The Cisco FM Ponte kit can be used to create wireless network architectures consisting of Point-to-point (P2P) links.

3.2.2. Cisco technologies

3.2.3. Point-to-point wireless bridge

A point-to-point wireless bridge allows two local networks to communicate with each other. A simplified example is shown in Figure 1 (page 12).

In context of the overall network architecture, the two local networks are called *network segments.*

IMPORTANT

For the Cisco FM Ponte kit, usable throughput is limited to 50 Mbps with a theoretical maximum distance between units of up to 3 miles (4.83 Km) under optimal wireless link conditions.

The Cisco FM Ponte kit cannot be switched to **Mesh Point** or **Mesh End** mode.

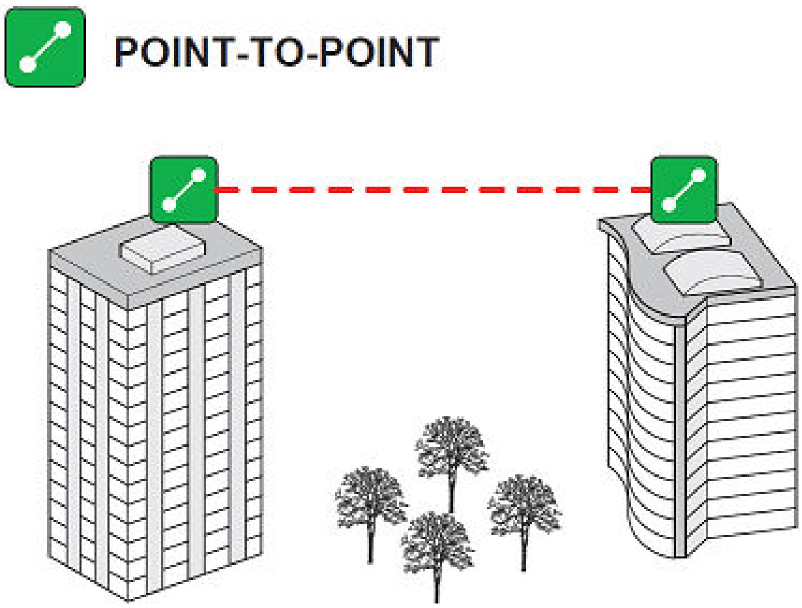


Figure 1. Point-to-point network architecture

All network activity that takes place on wireless bridges is 'transparent' to the network hosts. In other words, a wireless bridge forwards packets from one network segment to another according to a 'Forwarding table'. The forwarding table is built by learning the network topology from analysis of incoming traffic.

In this configuration, no explicit interaction takes place between the wireless bridge and the network hosts. The network segments on either side of the wireless bridge share the same IP subnet. Therefore, each network host must use a unique IP address within the subnet.

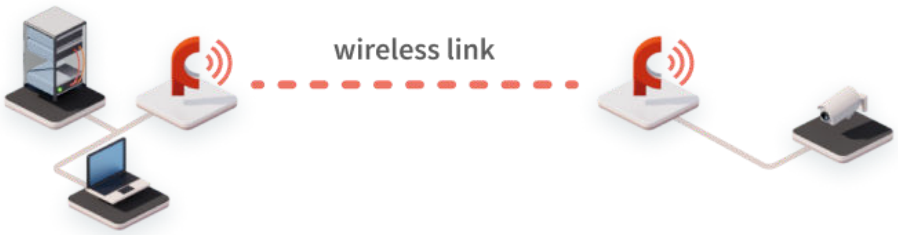
3.3. Cisco network addressing

3.3.1. Bridge IP addressing

The Cisco FM Ponte kit can only be operated in *Bridge mode*, creating a single point-to-point connection between two wireless network segments. A simplified example of a Bridge mode connection is shown in Figure 2 (page 13).

As shipped from the factory, the wired ethernet ports of all Cisco hardware components are assigned the same default IP address of **192.168.0.10/24**.

No default IP address is associated with the wireless interface.



192.168.0.10 is the default IP address of all Cisco Radios.

It is recommended to change the iP address of both units

Figure 2. Wireless network architecture (bridge configuration)

3.3.2. Unit identification and addressing

Bridge-capable radio transceiver identification

Regardless of its configuration and operating mode, every Cisco radio transceiver is shipped from the factory with a unique unit identification (ID) number. This number always takes the following form:

5.a.b.c

The triplet a.b.c uniquely identifies the individual physical hardware unit, and cannot be changed.

The unit ID number is used to identify the physical hardware units within the configurator interface that is used for configuration of the unit.

Network addressing

Cisco radio transceivers

Each Cisco radio transceiver unit has a factory-set IP address of **192.168.0.10**, and a Netmask of **255.255.255.0**.

NOTE

Each individual Cisco radio transceiver unit has a factory-set *5.a.b.c* Mesh identification number. Each unit is shipped from the factory with the same IP address, but with a unique Mesh identification number.

IMPORTANT

IP addresses must not be duplicated within a network. If addresses are duplicated, IP address conflicts will occur.

IMPORTANT

The Cisco FM Ponte kit is designed as a *Bridge* device only. It cannot be configured as a *Mesh Point* or *Mesh End* device.

4. Installing the radio

4.1. Installing the radio using the multi-axis mounting bracket

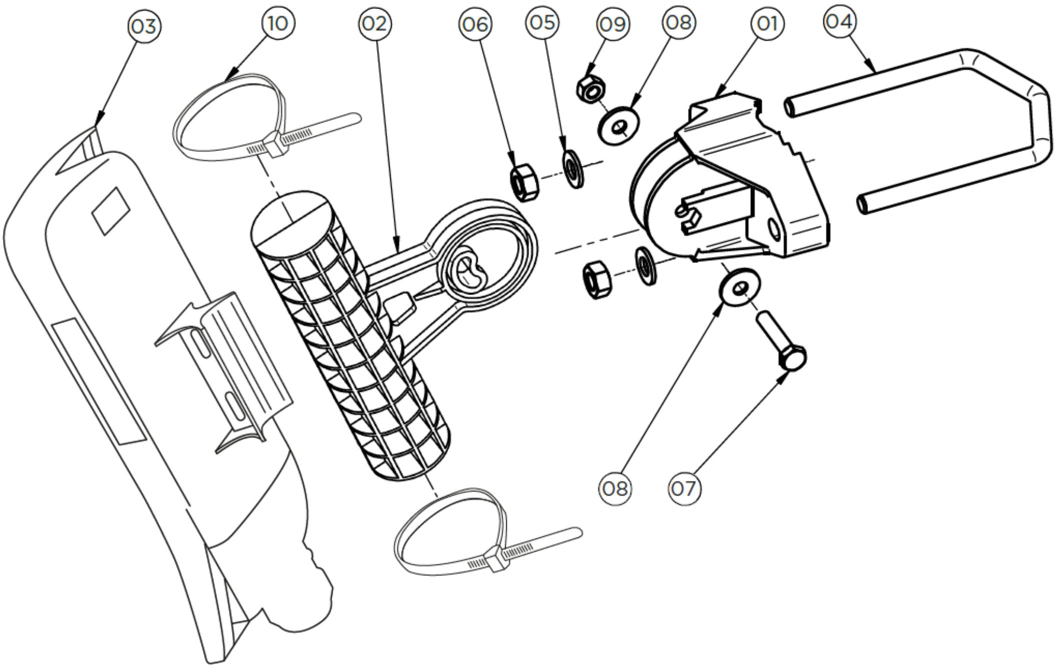
IMPORTANT

The FM Ponte transceiver kit includes two multi-axis mounting brackets (Cisco part number *FM-BRKT*).

The FM1200 Volo transceiver kit includes a single *FM-BRKT* mounting bracket.

The *FM-BRKT* mounting kits do not need to be purchased separately.

The diagram below shows the components and assembly sequence for installing the radio using the Cisco multi-axis mounting bracket.



The table below shows the components and quantities of each component used in each FM-BRKT assembly:

Component number	Description	Quantity
01	Pole Mount	1
02	Swivel Rod	1
03	Radio transceiver	1
04	U-bolt	1

Component number	Description	Quantity
05	8.4mm washer	2
06	M8 nut	2
07	M6x25 screw	1
08	6.4mm washer	2
09	M6 nut	1
10	Tie wrap	2

To install the radio transceiver on a wooden or metal utility pole using the Cisco multi-axis mounting bracket, do the following steps:

1. Decide where on the utility pole the unit must be mounted, taking access to the unit and antenna line-of-sight into account.
2. Place the U-bolt (04) around the utility pole at the chosen mounting point.
3. Place the Pole mount (01) over the two ends of the U-bolt, with the curved end of the mount aligned with the outer curve of the pole.
4. Place the 8.4mm flat washers (05) over the two ends of the U-bolt.
5. Screw the M8 nuts (06) onto the two ends of the U-bolt. Do not fully tighten the nuts at this time.
6. Insert the circular end of the Swivel rod (02) into the hollow part of the Pole mount (01).
7. Place a 6.4mm flat washer (08) over the shaft of the M6x25mm screw (07).
8. Push the M6x25mm screw through the securing hole of the Pole mount, making sure that the hexagonal end of the screw seats correctly on the casting of the Pole mount.
9. Place a second 6.4mm flat washer (08) over the threaded end of the M6x25mm screw (07).
10. Screw the M6 nut (09) onto the threaded end of the M6x25mm screw (07). Do not fully tighten the nut at this time.
11. Make sure that the transceiver unit faces the right way up.
12. Place the concave surface of the unit’s mounting lug securely against the cylindrical end of the Swivel rod (02).
13. Route the two tie-wraps (10) through the clamp holes of the unit’s mounting lug. Join the ends of the tie-wraps.
14. Securely fasten the transceiver unit to the Swivel rod by pulling the ends of the tie-wraps.
15. Aim and adjust the radio correctly. You can aim the unit in the vertical and horizontal planes.
16. Fully tighten the M6 nut and M8 nuts.

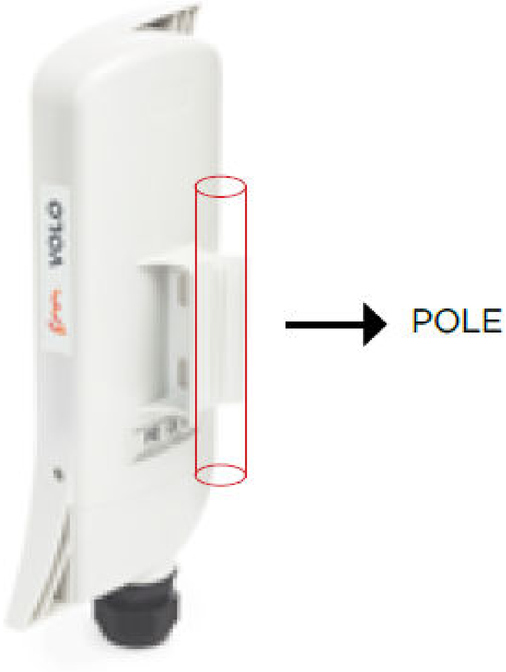
CAUTION

Do not over-tighten the nuts. Doing so could damage the bracket components.

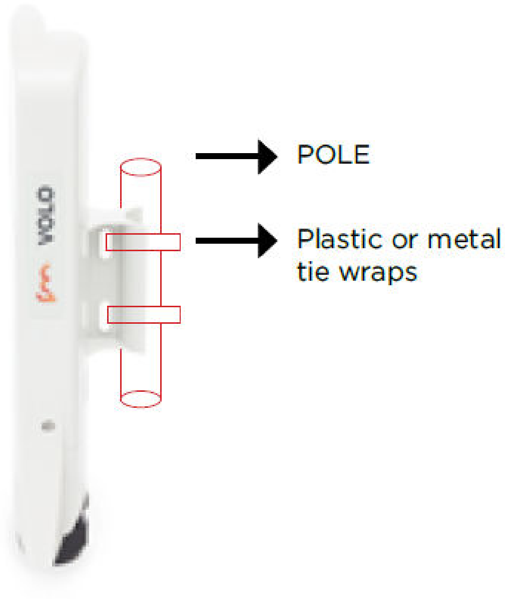
4.2. Installing the radio using tie-wraps

To install the radio transceiver on a wooden or metal utility pole using the included tie-wraps, do the following steps:

1. Decide where on the utility pole the radio must be mounted, taking access to the radio and line-of-sight into account.
2. Place the radio against the utility pole at the chosen mounting point (below).



3. Route the two tie-wraps through the clamp holes of the radio’s mounting lug (below).



4. Join the ends of the tie-wraps. Tighten the tie-wraps just enough that the radio can be easily moved in the horizontal plane.
5. Aim and adjust the radio correctly. You can aim the unit in the horizontal plane only.
6. Pull the ends of the tie-wraps until the radio assembly is secure.

5. Hardware installation

5.1. Cisco hardware installation

5.1.1. Installing the Cisco FM Ponte kit

Environmental rating and unit roles

The Cisco FM Ponte kit (model number FM1200V-HW) is a wireless radio transceiver unit.

The hardware is contained in an outdoor-rated metal enclosure that can be easily mounted on poles or walls.

The Cisco FM Ponte kit can operate in any of the following networking roles:

- As a point-to-point wireless bridge (see "Point-to-point wireless bridge" (page 12) for details).

Installation hardware

Metal clamps are supplied as part of the installation package, to allow mounting of the unit on utility poles. Refer to the Cisco FM Ponte kit installation instructions for details.

Removable bottom housing

The unit features a removable, water-tight bottom housing. The bottom housing is equipped with an NPT-1 standard-thread cable gland. The cable gland can house a dual-cable rubber seal that can accept two shielded Ethernet cables. Three different pre-cut rubber seals are provided to accept Ethernet cables of different diameter.

⚠ **CAUTION**

To prevent leaks and cable damage, tighten the cable gland by hand *only*. Do not use a wrench. No additional tape or sealing hardware is required.

If you are running only one Ethernet cable through the rubber seal, block the second cable hole with a one-inch cable stub *only*.

5.1.2. Best practice for shielded CAT5/6 connectors

⚠ **CAUTION**

To avoid the possibility of damage to network components due to electrostatic discharge (ESD), it is extremely important that all shielded CAT5/6 connectors are assembled according to the standards and directives in this section.

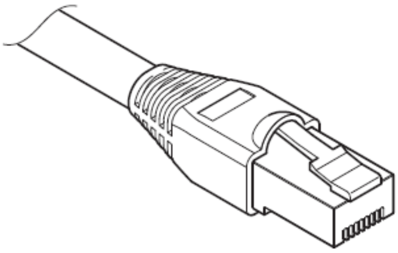


Figure 3. Shielded CAT5/6 connector

Use only professional-quality, outdoor-rated, RF-shielded cables in conjunction with Cisco radio transceivers.

Assemble all shielded CAT5/6 connectors to the following standards:

- Only use shielded RJ45 Ethernet connectors.
- When inserting each connector into a shielded Ethernet port, the connector's inner jacket must form a positive contact with the Ethernet port.
- When each RJ45 connector is plugged into the correct Ethernet port of the Cisco FM Ponte kit, lock the bottom of the RJ45 connector using the side retaining screws.
- When all RJ45 connectors are connected to the unit, make sure that the bottom cover of the unit is correctly secured to the unit enclosure.

5.1.3. Cisco FM Ponte kit Status and link LEDs

Unit and link quality status

The front panel of the Cisco FM Ponte kit (as seen below) contains seven LEDs. The panel is used to check the unit status and wireless link quality status.

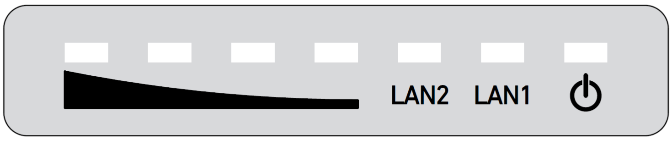


Figure 4. Status and link/boot LEDs

During normal operation, the seven LEDs indicate the following conditions:

- **Power:** The Cisco FM Ponte kit is receiving power.
- **LAN1:** Network activity on Ethernet port 1.
- **LAN2:** Network activity on Ethernet port 2.

- **SIGNAL STRENGTH (red):** Signal strength very poor.
- **SIGNAL STRENGTH (yellow):** Signal strength inadequate.
- **SIGNAL STRENGTH (green):** Signal strength acceptable.
- **SIGNAL STRENGTH (green):** Signal strength excellent.

TIP

During normal operation, the readings from the four **SIGNAL STRENGTH** LEDs can be used to do radio antenna alignment (see "Antenna-alignment tools and physical statistics" (page 49) for more information).

Boot sequence

During the unit's boot sequence, the four **SIGNAL STRENGTH** LEDs light up in sequence. During the boot sequence, the LEDs indicate the following conditions:

1. **Red:** Core system boot in progress.
2. **Yellow:** Wireless system boot in progress.
3. **First green:** Routing engine boot in progress.
4. **Second green:** Unit configuration boot in progress.

If the boot sequence above stops at any LED, an error has been detected during that stage of the boot sequence.

5.1.4. Supplying power to the Cisco FM Ponte kit

CAUTION

When connecting the Cisco FM Ponte kit to a power supply, be sure to follow the instructions in this section at all times.

Failure to follow these instructions may result in irreparable damage to the unit and/or other connected hardware, and will also invalidate the product warranty.

IMPORTANT

For technical data on which power sources are compatible with the Cisco FM Ponte kit, refer to "Electrical power requirements" (page 115).

The Cisco FM Ponte kit can be provided with power using the following methods:

- The included 24 Vdc passive PoE injector (90 Vac to 260 Vac, 50/60 Hz input).

- If connecting the unit to an Ethernet switch or router equipped with unmanaged PoE, an IEEE 802.3af-to-24 Vdc inline converter (model number *FM-POE-INL*).

CAUTION

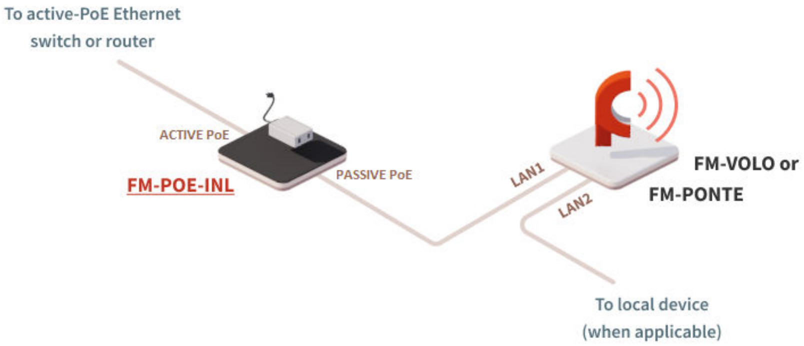
The Cisco FM Ponte kit is designed to accept power from the included 24 Vdc mode B passive PoE injector (model number *FM-POE-STD*) or from an IEEE 802.3af-to-24 Vdc inline converter (model number *FM-POE-INL*) only. Do not connect power supplies of any other voltage output, type or rating to the unit under any circumstances.

Do not connect an unmanaged PoE switch (in other words, a PoE switch on which DC power to the RJ45 ports cannot be switched off) to the Cisco FM Ponte kit under any circumstances. Connecting an unmanaged PoE switch to the unit will result in 48 Vdc power being supplied to the unit. This will irreparably damage the unit, and will invalidate the product warranty.

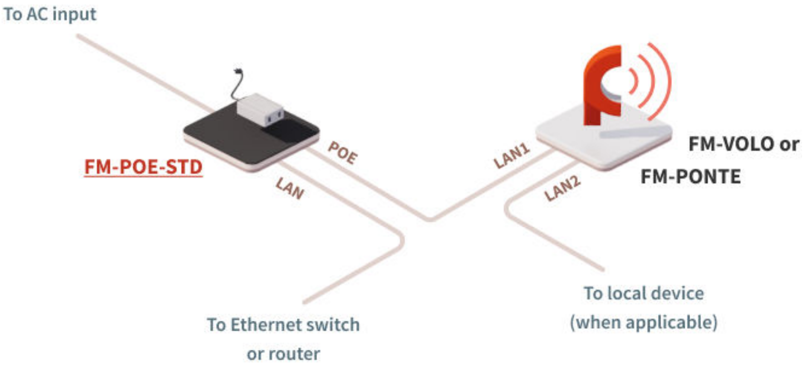
When providing the power source for the Cisco FM Ponte kit, remember the following important points:

- Install the power source as close to the unit as possible to minimize voltage drop. The maximum suggested distance is 50ft (15m).
- Ensure proper grounding (earthing) and reliable connectivity by using shielded CAT5/6 cables and connectors.
- If you are connecting the Cisco FM Ponte kit directly to a power source, only use the included 24 Vdc mode B passive PoE injector(s) (model number *FM-POE-STD*). If the included PoE injector(s) are non-functional, replacement injectors can be ordered from Cisco.
- If you are 'daisy-chaining’ (in other words, connecting the Cisco FM Ponte kit to a switch or a router through a 24 Vdc mode B passive PoE injector), note the following points:
    - The unit is designed to accept 24 Vdc passive mode B PoE power only. The RJ45 terminal assignments for mode B power are as follows:
        1. **Terminal 1:** Rx +
        2. **Terminal 2:** Rx -
        3. **Terminal 3:** Tx +
        4. **Terminal 4:** DC voltage +
        5. **Terminal 5:** DC voltage +
        6. **Terminal 6:** Tx -
        7. **Terminal 7:** DC voltage -
        8. **Terminal 8:** DC voltage -

- Do not connect the unit to an IEEE 802.3af or IEEE 802.3at PoE adapter, Ethernet switch or router through a passive PoE injector. The passive PoE injector included with the unit cannot regulate excessive voltages, and the DC power feed from switches of this type cannot be turned off. This will result in a damaging over-voltage being supplied to the unit.
- If connecting the unit to a switch or router equipped with unmanaged PoE, use the 802.3af-to-24 Vdc inline converter (model number *FM-POE-INL*) only (below). In this scenario, do not use the included 24 Vdc mode B passive PoE injector (model number *FM-POE-STD*), as the passive PoE injector will supply a damaging over-voltage to the unit.


To active-PoE Ethernet switch or router
ACTIVE PoE
FM-POE-INL
PASSIVE PoE
LAN1
LAN2
FM-VOLO or FM-PONTE
To local device (when applicable)

- If connecting the unit to an Ethernet switch or router equipped with power-management support, disable PoE on the RJ45 port of the Ethernet switch or router that is connected to the PoE injector (below).


To AC input
FM-POE-STD
POE
LAN
LAN1
LAN2
FM-VOLO or FM-PONTE
To Ethernet switch or router
To local device (when applicable)

- If connecting the PoE injector to a non-PoE switch or router (above), no special precautions need to be taken.

Connecting power to the Cisco FM Ponte kit

NOTE

For detailed comparative information on which Cisco hardware devices are capable of accepting power through IEEE 802.3at or IEEE 802.3af power sources, or through a DC IN power source, refer to "Electrical power requirements" (page 115).

Connecting power through a LAN RJ45 port

The Cisco FM Ponte kit radio transceiver unit has two Ethernet ports (Figure 5 (page 24)).

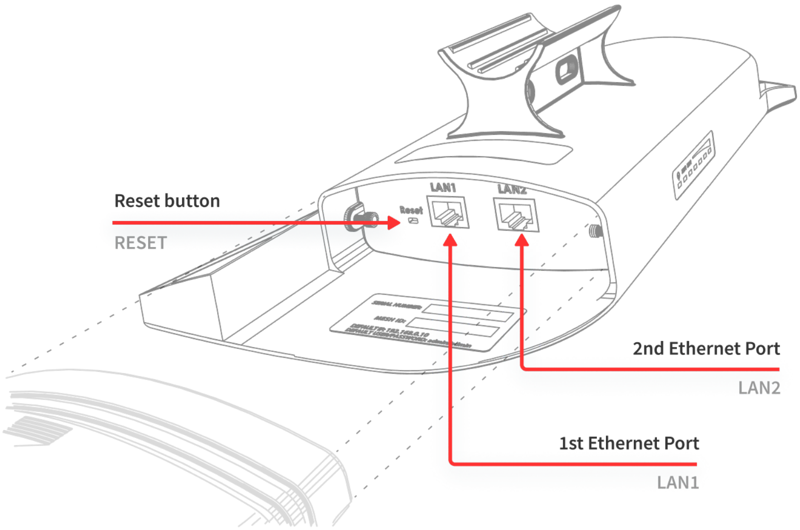


Figure 5. Device connector ports

CAUTION

The unit is designed to take power through 24 Vdc *Power-over-Ethernet* only, and does not have a dedicated power port. A 24 Vdc PoE injector is included with the unit. Do not connect any 48 Vdc PoE injector, and do not attempt to connect any other source of electrical power to the unit.

Connect the included 24 Vdc PoE injector to the unit by doing the following steps:

1. Only use a patch Ethernet cable to connect the PoE injector and the unit.
2. Insert the RJ45 connector leading from the PoE injector into the Ethernet port labelled *LAN1/POE*.

5.1.5. Rebooting the firmware and resetting the unit to factory defaults

The Cisco FM Ponte kit hardware can be rebooted and reset to factory default condition using the procedures in this section.

IMPORTANT
The following procedure shows how to do a 'hard' (device firmware) reboot. To do a 'soft' (device software) reboot, refer to "Resetting the unit to factory defaults" (page 98).

To do a 'hard' (device firmware) reboot under emergency conditions (for example, if the unit malfunctions), do the steps in the following sub-section.

Device firmware reboot

1. Remove the bottom cover from the main unit enclosure as shown in "Connecting LAN cables to the unit" (page 29).
2. Insert a long tool with a thin shaft, such as a paper clip or a thin screwdriver, into the **RESET** button port until the tool touches the bottom (Figure 6 (page 25)).

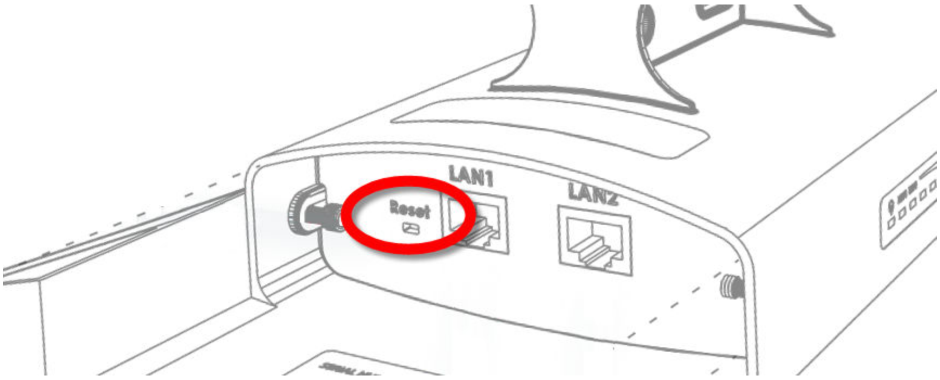


Figure 6. Cisco FM Ponte kit (Hardware RESET button port)

3. Press the **RESET** button for one second, then release the button immediately.
   - The unit will reboot.

Resetting the unit to factory settings

> **CAUTION**
>
> Do not do a factory reset unless the unit needs to be reconfigured using its factory configuration as a starting point.
>
> A factory reset will reset the unit's IP address and administrator password, and will disconnect the unit from the network.

The following methods are available to do a factory reset:

1. To do the reset using the offline Configurator interface, refer to "Resetting the unit to factory defaults" (page 98).
2. To do the reset by physically accessing the unit, follow the procedure below.

To reset the radio to its factory default settings, do the steps that follow:

1. Power ON the unit.
2. Wait approximately 40 seconds for the unit to boot up.
3. When the unit has completed its boot sequence, press the **RESET** button for 7 seconds.
    - The LEDs will blink.
    - The unit will be restored to factory default settings (including its default IP address of **192.168.0.10** and subnet mask of **255.255.255.0**).
    - The unit will reboot.
    - The administrator user name and password will both be reset to **admin**.

5.1.6. Suitability for outdoor installation

The Cisco FM Ponte kit was specifically designed for installation in harsh outdoor environments. Under operating conditions, the unit is completely sealed, and is capable of high-performance operation in outdoor environments, and under severe conditions such as water spray, salt, and extreme fluctuations in cold and heat.

The Cisco FM Ponte kit has an IP66 ingress protection rating.

5.2. Connecting the Cisco FM Ponte kit to networking and communications hardware

5.2.1. Terminal assignments for power and data connectors

IMPORTANT

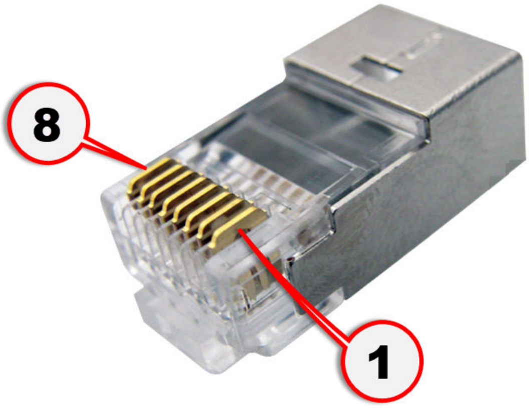
Always use outdoor-rated, RF-shielded Ethernet cables when connecting the Power and LAN ports of a Cisco hardware device to external hardware.

RJ45 Ethernet

IMPORTANT

Always use outdoor-rated, RF-shielded Ethernet cables, and RF-shielded RJ45 male connectors (a typical shielded connector can be seen in the image below).

The terminal assignments for male RJ45 connectors are as shown in the image below. With the connector in this orientation, the terminals are numbered 1, 2, 3, 4, 5, 6, 7 and 8 from right to left.



CAUTION

RJ45 connectors can be wired according to network cable wiring standards EIA/TIA T568A **or** EIA/TIA T568B.

To prevent device and/or network malfunctions:

- It is strongly recommended that wiring standard T568A **or** T568B be chosen at the network design stage, and applied to all relevant devices throughout the life of the project.
- Always use the same wiring standard at both ends of the same patch cable (for example, if a cable's RJ45 connector is wired according to T568A, the connector at the opposite end of the cable must also be wired according to T568A).

The terminal assignments for the different network cable wire standards are as follows:

Network cable wire standard T568A

- **Terminal 1**: Green wire with white tracer
- **Terminal 2**: Green wire
- **Terminal 3**: Orange wire with white tracer
- **Terminal 4**: Blue wire
- **Terminal 5**: Blue wire with white tracer
- **Terminal 6**: Orange wire
- **Terminal 7**: Brown wire with white tracer
- **Terminal 8**: Brown wire

Network cable wire standard T568B

- **Terminal 1**: Orange wire with white tracer
- **Terminal 2**: Orange wire
- **Terminal 3**: Green wire with white tracer
- **Terminal 4**: Blue wire
- **Terminal 5**: Blue wire with white tracer
- **Terminal 6**: Green wire
- **Terminal 7**: Brown wire with white tracer
- **Terminal 8**: Brown wire

5.2.2. Connecting LAN cables to the unit

Bottom housing and RJ45 LAN cabling

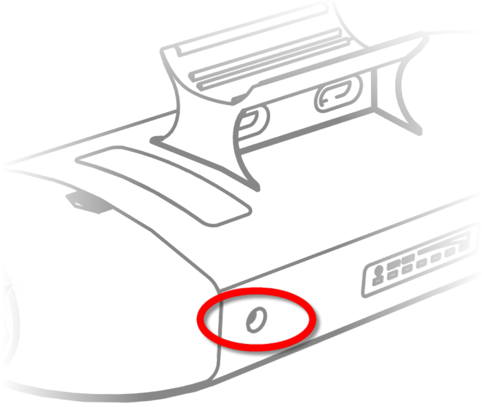
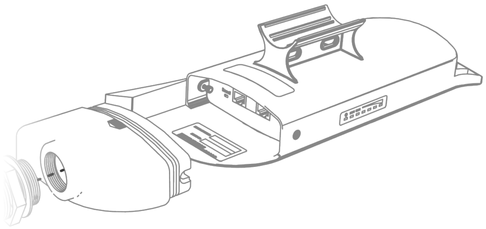
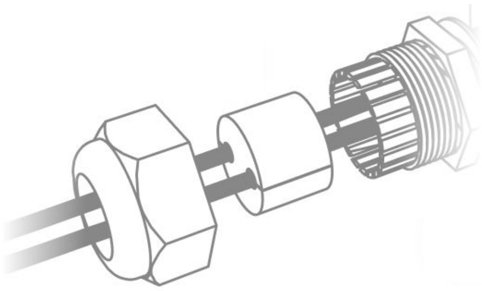
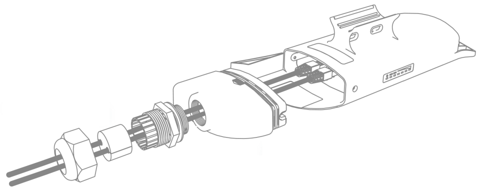
CAUTION

When loosening the screws that secure the bottom housing to the main body of the unit, do not remove the screws. Removing the screws will damage the main body.

When the Cisco FM Ponte kit is mounted in its final location, connect the unit to LAN connection(s) and a PoE power supply by doing the following steps:

1. Only use shielded CAT5/6 cables that terminate in RJ45 Ethernet connectors at both ends.
2. Make sure that the terminal pin assignments for the RJ45 plugs comply with the accepted standard for RJ45 LAN/PoE connectors.

Next, proceed to the steps in the following table:

	
3. Loosen the two screws that secure the bottom housing to the main housing. The location of one of the screws is shown above. The second screw is on the opposing side of the unit.	**4.** Separate the bottom housing from the main body of the unit.
	

5. Remove the hexagon nut and rubber seal from the cable gland.

IMPORTANT

The use of pre-made Ethernet cables is recommended. The rubber seal is pre-cut, allowing pre-made Ethernet cables to be used.

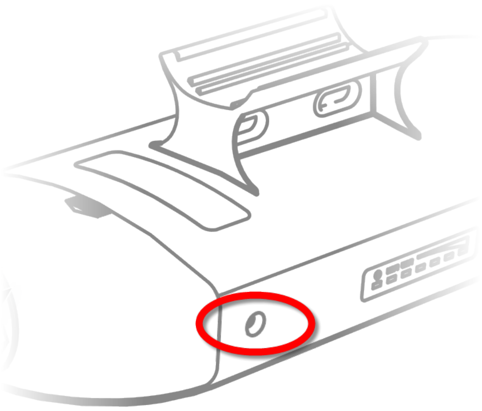
6. Make sure that the cable gland is securely screwed into the bottom housing.

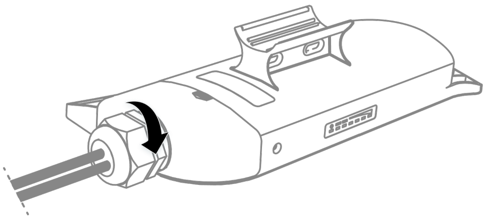
7. Route the LAN cables through the hexagon nut, the rubber seal, and the cable gland on the bottom housing.

CAUTION

If you are running only one Ethernet cable through the rubber seal, block the second cable hole with a one-inch cable stub *only*.

8. Connect the RJ45 connectors to the correct LAN ports as shown in “Connecting LAN cables to the unit” (page 29).





9. Correctly align the bottom housing with the main body of the unit. Press the bottom housing into the main body.

10. Tighten the two screws that secure the bottom housing to the main housing.

11. Slide the rubber seal toward the unit until it seats inside the cable gland.

12. Tighten the hexagon nut.

6. Using the Cisco Partner Portal

The Cisco Partner Portal is the main web-based portal through whichthe following activities are done:

1. Participating in Cisco E-learning
2. Using and sharing plug-in license codes for Cisco devices
3. Viewing the technical documentation for your Cisco devices

6.1. Accessing the Partner Portal

Access to the Partners Portal is granted only to Cisco's official partners and customers, and requires registration.

To access the Cisco Partner Portal, do the following steps:

1. Make sure a current web browser is installed on your computer. For detailed information on which browsers are supported, refer to Table 3 (page 31) below. If needed, upgrade your browser version.
2. Click this link.
   - The Cisco Partner Portal **Sign In** dialog will be shown.
3. Register as a portal user by clicking the **Create Account** link and following the software prompts.

Table 3. Supported web browsers

	Version	Computer operating systems	Compatibility	Reason
Mozilla Firefox	32 to 38	Linux, Windows 7, 8 and 10, OS X Mavericks	Partial	Icons and fonts do not display correctly in position modality
	39	Linux, Windows 7, 8 and 10, OS X Mavericks	Full	-
	40 onward	Linux, Windows 7, 8 and 10, OS X Mavericks	Full	-
Google Chrome	36 onward	Linux, Windows 7, 8 and 10, OS X Mavericks	Partial	Vertical scrolling in unit/template detail does not work correctly
	56 onward	Linux, Windows 7, 8 and 10, OS X Mavericks	Full	-

	Version	Computer operating systems	Compatibility	Reason
Microsoft Internet Explorer	11 onward	Windows 7, 8 and 10	Full	-
Microsoft Edge	13 onward	Windows 7, 8 and 10	Full	-
Apple Safari	8 onward	OS X Yosemite or later	Full	-

6.2. Enabling Two-Factor Authentication for security

To enhance cyber-security on the Partner Portal, Cisco uses two-factor authentication (2FA).

2FA works by providing an extra security layer that works independently of your Partner Portal login password. With 2FA activated, you will be asked to provide a secure one-time password (OTP) for each login.

To set up two-factor authentication, do the following steps:

1. Install an app capable of generating authentication codes on your mobile phone. Apps recommended for specific platforms are:
   - **Google Authenticator** or **Authy** (iPhone, Android)
   - **Microsoft Authenticator** (Windows Mobile)
2. Log into the Cisco Partner Portal using your normal access password.
3. Hover the mouse cursor over the Profile icon in the upper right-hand corner of the web page (Figure 7 (page 32)). Click the **Account** option.

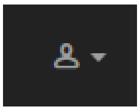


Figure 7. Partner Portal (Profile icon)

   - Your portal account page will be shown.
4. Click the **Two Factor Auth.** link on the left-hand side of the web page (Figure 8 (page 32)).

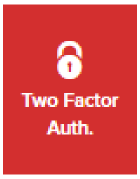


Figure 8. Partner Portal (Two Factor Auth. icon)

- The **Two Factor Authentication page** will be shown.
- The current two-factor authentication status of your portal account will be shown near the top of the page.

5. Click the **Set Up Two Factor Authentication** button.
    - A two-factor authentication dialog will ask to confirm your identity. If the name and E-mail address shown in the dialog are yours, enter your current portal password and click the **Validate identity** button.
6. An E-mail will be sent to your E-mail address with a verification code in the body of the mail. Enter the verification code in the **Verification code** field of the Two Factor Authentication web page.
    - The Two Factor Authentication web page will show a QR code.
7. Use the authentication app on your mobile phone to scan the QR code on the web page. Figure 9 (page 33) is a typical example of the QR code you will be shown.

Figure 9. Two Factor Authentication (typical QR code)

- The authenticator app will generate an authentication code. Enter this code in the **Authentication code** field of the Two Factor Authentication web page, and click the **Enable Two Factor Authentication** button.
- A list of ten *recovery codes* will be shown on the Two Factor Authentication web page. It is recommended that you save these codes in case you lose your mobile phone. Download the recovery codes as a *.TXT file by clicking the **Download** button, or print a hard copy of the codes by clicking the **Print** button.

6.3. Administering plug-in license codes

The Partner Portal Plug-ins page can be used to do the following tasks:

- Convert plug-in License codes to Activation codes
- Deactivate active plug-in License codes

- Reactivate deactivated plug-in License codes
- Export multiple Activation codes
- Share License codes with other Cisco device users• Accept shared License codes from other Cisco device users

To do the tasks above, refer to “Plug-In management” (page 90).

6.4. Viewing the technical documentation for your Cisco device

All documentation relating to your Cisco device (such as product brochures, technical data sheets, installation instructions and user manuals) can be found in the Documentation section of the Partner Portal.

To find documentation relating to your Cisco device, do the following steps:

1. Log in to the Cisco Partners Portal using your login credentials.
2. Click this link.
3. All documents are arranged by category. Browse the folders for the documentation you need.

7. Device configuration using the configurator interface

All Cisco radio transceiver devices are shipped with IP address **192.168.0.10**, and Netmask **255.255.255.0**.

The Cisco FM Ponte kit can be configured by using:

- The on-board Configurator interface.

The *Configurator* is a localized configuration software platform that resides on the Cisco device.

- Local configuration is done by connecting a computer to the device through a direct hardware connection, or through the internet.
- Using the Configurator, devices can be configured on an *Offline* basis only. A configuration (*.CONF) file can be manually applied to set the device parameters, or each device parameter can be manually set by the device user.
- Offline configuration settings for more than one Cisco device type can be integrated into a single configuration file. When the configuration file is uploaded to each device, the device automatically loads the correct configuration settings for its device type.

To configure the unit using the *Configurator*, refer to the following sub-sections.

IMPORTANT

The FM Racer Radio Configuration interface and command-line interface (CLI) contain device configuration parameters that are not available in the on-board Configurator interface.

Note that some configuration features may not be applicable to your specific Cisco device.

Configuration parameters and control tabs that are exclusive to FM Racer and the CLI include:

- **Project name** (The device has been assigned to the Project listed in this field.)
- **Position** (Shows the current physical location of the unit.)
- **Invoice No.** (Shows the Cisco sales invoice number for the unit.)
- **Shared With** (If responsibility for the unit is shared with other users, the details of the responsible users are shown in this field.)
- **Enable RTS Protection** (FM3500 Endo and FM4500-series transceivers only - shows the unit's current IEEE 802.11 request-to-send (RTS) setting.)
- **Promisc** ('Promiscuous' Mode: Shows the unit's current setting for backwards compatibility with legacy Cisco units that are no longer in production.)
- **Noise floor Calibration** (Shows the unit's current noise floorcalibration setting.)
- **MAX Transmission MCS** (Used to choose the modulation and coding scheme by which the unit automatically chooses its maximum data transmission rate.)
- **TX Power** (Controls the effective isotropic radiated power output of the unit.)
- **Automatic link distance** (Lets the system choose the maximum effective distance between the relevant wireless links.)
- **Ethernet speed** (Selects the correct data exchange speed for each Ethernet port.)
- **CISCO WI-FI** tab (Allows you to set up a second, segregated Wi-Fi interface that allows technicians access to the unit for configuration and maintenance purposes.)
- **FLUIDITY ADVANCED** tab (Allows you to adjust the load-balancing, handoff and network optimization characteristics of a transceiver unit.)
- **FLUIDITY POLE BAN** tab (Allows you to greatly reduce sudden degradations in bandwidth that happen when a mobile unit approaches, then leaves behind, a static unit.)

- **FLUIDITY FREQUENCY SCAN** tab (Used where mobile Fluidity units are configured with different frequencies.)
- **SPANNING TREE** tab (Allows you to build a logical topology for Ethernet networks, including backup links to provide fault tolerance if an active link fails.)
- **QOS** tab (Contains controls for Quality of Service and Class of Service settings.)
- **MPLS** tab (Contains controls for adjustment of the unit's multiprotocol label switching settings.)
- **FAST FAILOVER (TITAN)** tab (Contains controls to enable fast fail-over capability on networks where backup units are installed.)
- **ARP** tab (Contains controls for Address Resolution Protocol settings used for discovering MAC addresses that are associated with IP addresses.)
- **INTRA-CAR** tab (Contains controls to create and maintain a wireless backbone network throughout physically large, compartmentalized vehicles.)

For a detailed description of the configuration options featured in the FM Racer interface, refer to the *Available configuration parameters* section of the *Cisco Networks FM Racer User Manual*.

7.1. Software and hardware prerequisites

To access the Configurator graphical user interface (GUI) and use the Configurator to program the Cisco FM Ponte kit, you need the following:

- A desktop, laptop or tablet computer equipped with:
  - Any current web browser. For a list of compatible web browsers, refer to the *Supported web browsers* table in "Using the Cisco Partner Portal" (page 31).
  - Any Microsoft Windows, Mac OS or Linux operating system.
  - An integrated Ethernet port.
- A CAT5/6 Ethernet cable with an RJ45 connector at each end.

7.2. Accessing the Cisco FM Ponte kit for device configuration

Before the unit can be made part of a wireless network, it must be configured.

The on-board Configurator can be used to configure a Cisco devicein either of two ways:

- By connecting a control device directly to the Cisco device using an Ethernet cable (Local access)

- By connecting a control device to the Cisco device through an internet connection (Internet access)

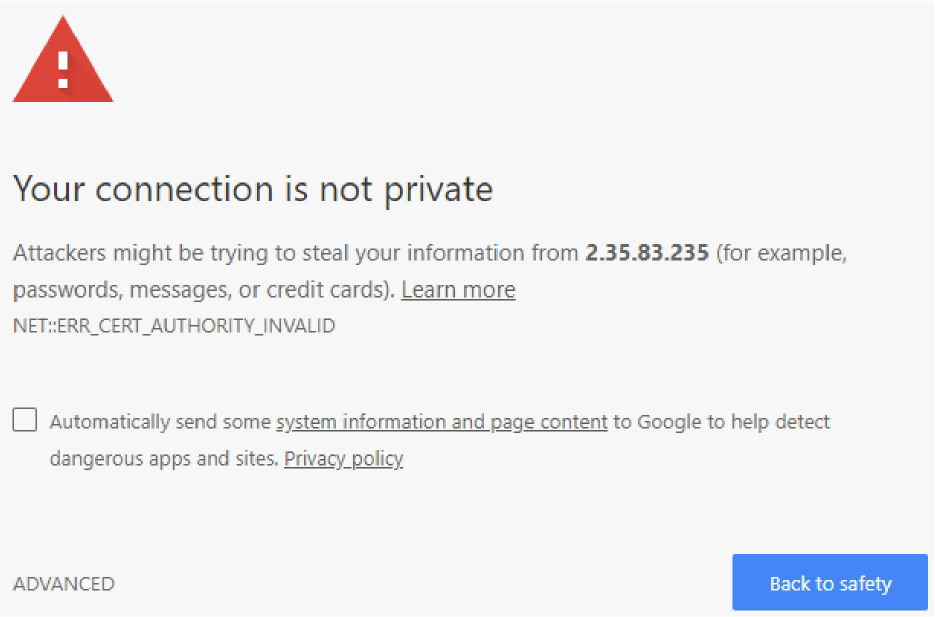
7.2.1. Local access and login for initial configuration

NOTE

If your computer has a wireless WiFi card, you may have to disable the card to avoid routing issues between the computer's wired and wireless network interfaces.

To use the Configurator interface to access the Cisco FM Ponte kit directly, do the steps that follow:

1. Power ON the unit.
2. Wait approximately one minute for the boot sequence to complete.
3. Connect one end of a CAT5/6 Ethernet cable to the computer that will be used to configure the Cisco FM Ponte kit.
4. Connect the other end of the Ethernet cable to the *Console* LAN port on the Cisco FM Ponte kit.
5. Manually set the computer's IP address and Netmask to be recognizable by the Cisco FM Ponte kit. The correct settings are as follows:
   - **IP address:** 192.168.0.10 (or any other IP address belonging to subnet 192.168.0.0/255.255.255.0)
   - **Netmask:** 255.255.255.0
6. Launch the computer's web browser.
7. Enter the IP address of the Cisco FM Ponte kit in the browser's URL entry field.
   - If the Configurator interface is shown immediately, proceed to Step 9 below.
   - Alternatively, you may see the following window:



Your connection is not private

Attackers might be trying to steal your information from **2.35.83.235** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

Figure 10. 'Connection Not Private' warning (Google Chrome)

IMPORTANT

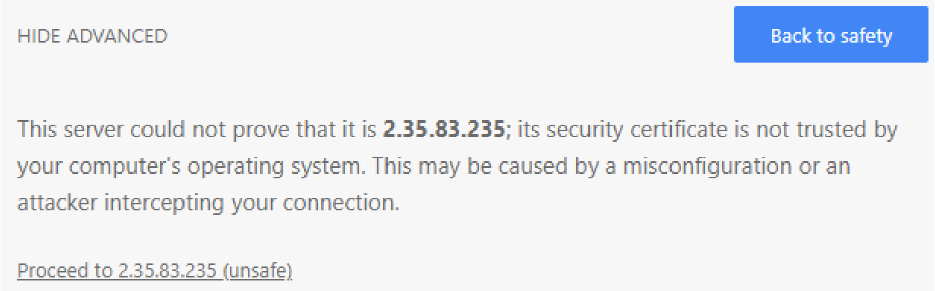
Due to rising levels of cyber crime, most modern web browsers are built to alert you to possible threats, such as hacking, spoofing and identity theft.

Because the Cisco FM Ponte kit is connected to the computer using an unsecured connection (in this case, a CAT5/6 cable), the web browser may show you security warnings like the one above.

This is normal and expected. During the configuration process, it is safe to ignore these warnings.

a. Click the **ADVANCED** link.

- You will see the following window:



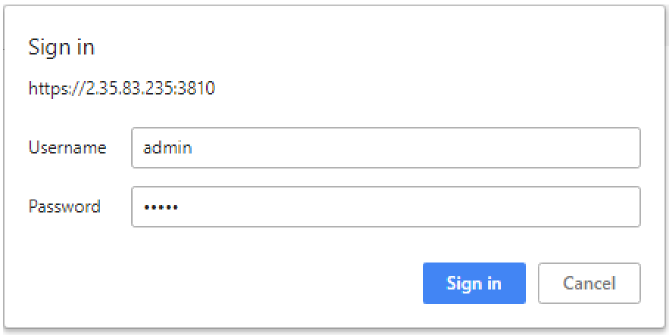
This server could not prove that it is **2.35.83.235**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 2.35.83.235 (unsafe)

Figure 11. Security certificate warning (Google Chrome)

b. Click **Proceed to [the URL] (unsafe)**.

- The device login window will be shown:



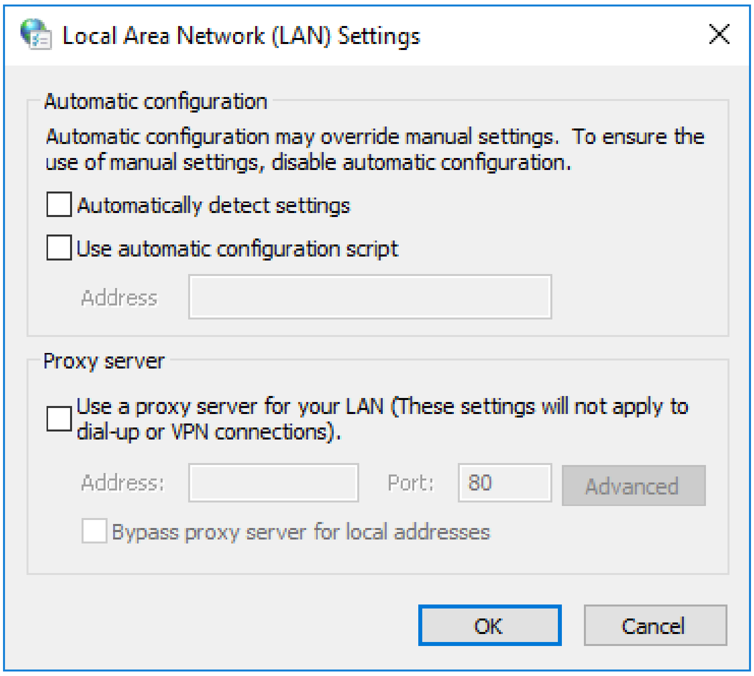
https://2.35.83.235:3810

Username: admin

Password: •••••

Figure 12. Cisco device login window

8. The factory-set login details are as follows:
   - Username: **admin**
   - Password: **admin**
9. Enter the correct username and password. Press 'Enter'.
   If your browser shows a time-out or similar message, the computer may be trying to access the Cisco device througha proxy server. To resolve the issue, do the following steps:
   1. Go to **Control Panel** > **Internet Options** > **Connections** > **LAN Settings**.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: 80

□ Bypass proxy server for local addresses

   2. Disable proxy connections by un-checking the check boxes for the following options:
      - **Automatically detect settings**
      - **Use automatic configuration script**
      - **Use a proxy server for your LAN**
   3. Click the **OK** button.
   4. Enter your user name and password in the device login window, and press 'Enter'.

10. To ensure system security, change the default password when the installation is completed. If the **Sign in** window does not appear, refer to “Changing the Administrator username and password” (page 86).

7.3. Using the MeshWizard™ configuration wizard

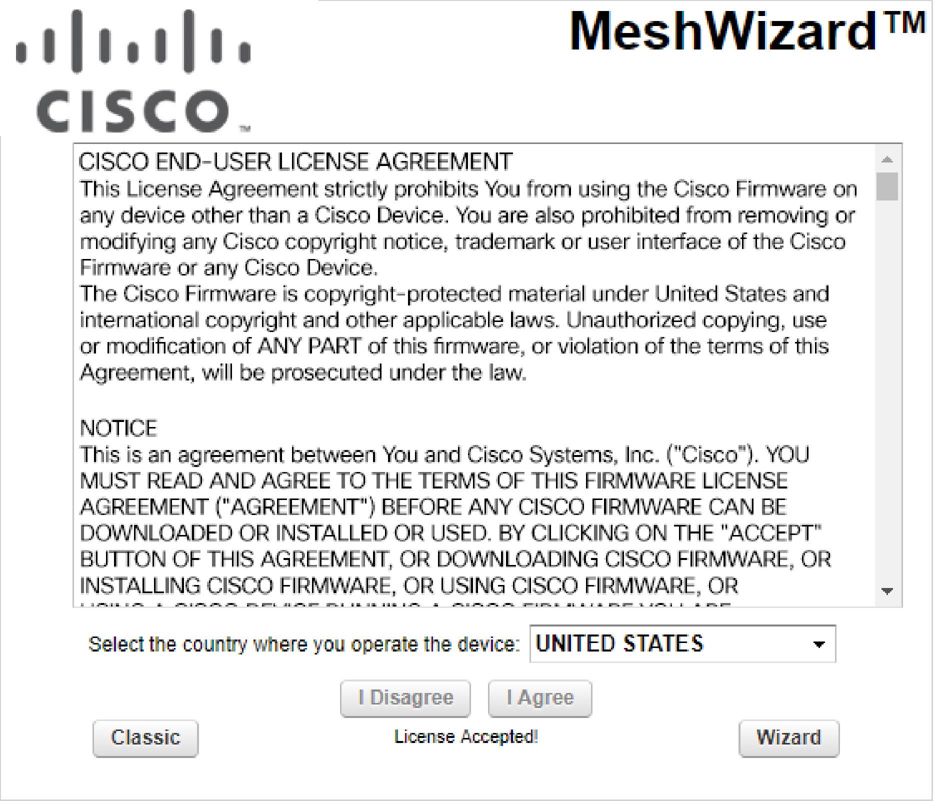
The Cisco FM Ponte kit is equipped with a configuration wizard that allows fast, easy configuration of the unit.

As an alternative to full configuration, the wizard can be completed before the first time the unit is used. If needed, the wizard settings can also be modified at any time after initial unit setup.

Open the Configuration Wizard by doing the following steps:

1. Connect the computer to be used for configuration directly to the Cisco FM Ponte kit as shown in “Accessing the Cisco FM Ponte kit for device configuration” (page 37).

2. Click the **-MeshWizard™** link under **Cisco PONTE** in the left-hand settings menu.
   - The MeshWizard end-user license agreement dialog will be shown (Figure 13 (page 42)).



CISCO END-USER LICENSE AGREEMENT
This License Agreement strictly prohibits You from using the Cisco Firmware on any device other than a Cisco Device. You are also prohibited from removing or modifying any Cisco copyright notice, trademark or user interface of the Cisco Firmware or any Cisco Device.
The Cisco Firmware is copyright-protected material under United States and international copyright and other applicable laws. Unauthorized copying, use or modification of ANY PART of this firmware, or violation of the terms of this Agreement, will be prosecuted under the law.

NOTICE
This is an agreement between You and Cisco Systems, Inc. ("Cisco"). YOU MUST READ AND AGREE TO THE TERMS OF THIS FIRMWARE LICENSE AGREEMENT ("AGREEMENT") BEFORE ANY CISCO FIRMWARE CAN BE DOWNLOADED OR INSTALLED OR USED. BY CLICKING ON THE "ACCEPT" BUTTON OF THIS AGREEMENT, OR DOWNLOADING CISCO FIRMWARE, OR INSTALLING CISCO FIRMWARE, OR USING CISCO FIRMWARE, OR

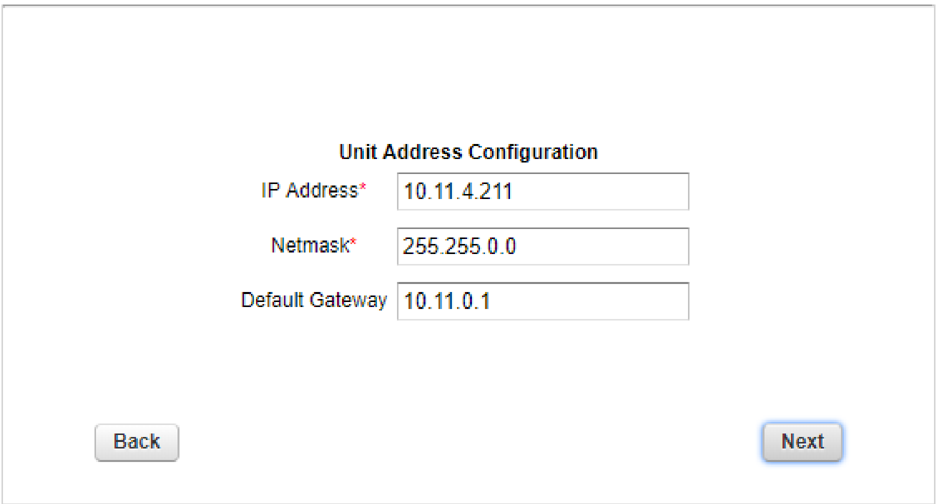
Select the country where you operate the device: UNITED STATES

License Accepted!

Figure 13. MeshWizard (End-user license agreement dialog)

3. Select the country in which the unit will be operated from the drop-down menu.
4. To enable operation of the Configurator interface and Cisco FM Ponte kit, you must click the **I Agree** button. Clicking this button confirms that you agree with, and consent to be bound by, the Cisco terms and conditions.
   - If you click the **I Agree** button, the **Classic** and **Wizard** buttons are shown on the dialog.
5. To configure the unit using the wizard, click the **Wizard** button. To configure the unit manually by using the Configurator interface, click the **Classic** button and configure the unit as shown in this manual.
6. If you clicked the **Wizard** button, the configuration wizard will proceed to the **Unit Address Configuration** window. The default IP address is **192.168.0.10** , and the default netmask is **255.255.255.0**. If needed, enter a different unit IP address,

netmask and/or default gateway in the relevant fields (Figure 14 (page 43)).



Unit Address Configuration

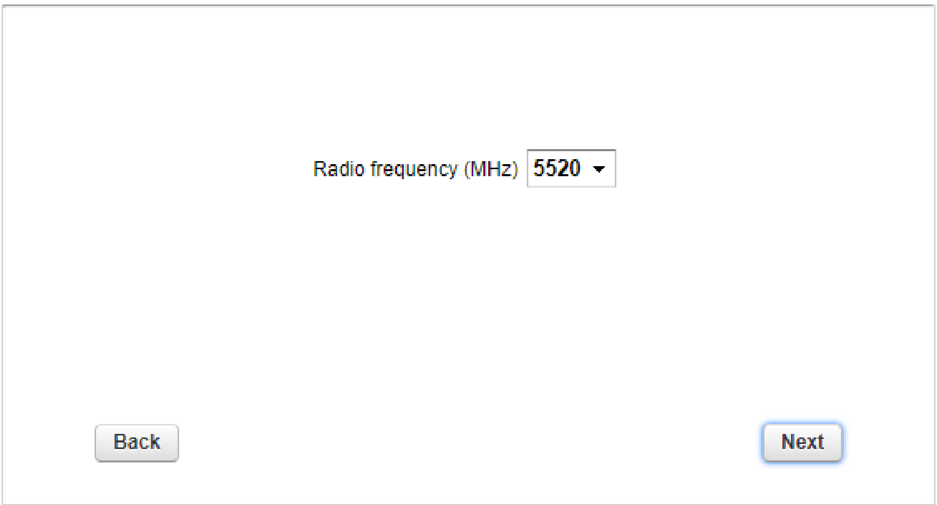
IP Address*: 10.11.4.211

Netmask*: 255.255.0.0

Default Gateway: 10.11.0.1

Figure 14. MeshWizard (Unit Address Configuration window)

7. Click the **Next** button.
   - The radio frequency window will be shown (Figure 15 (page 43)).



Radio frequency (MHz): 5520

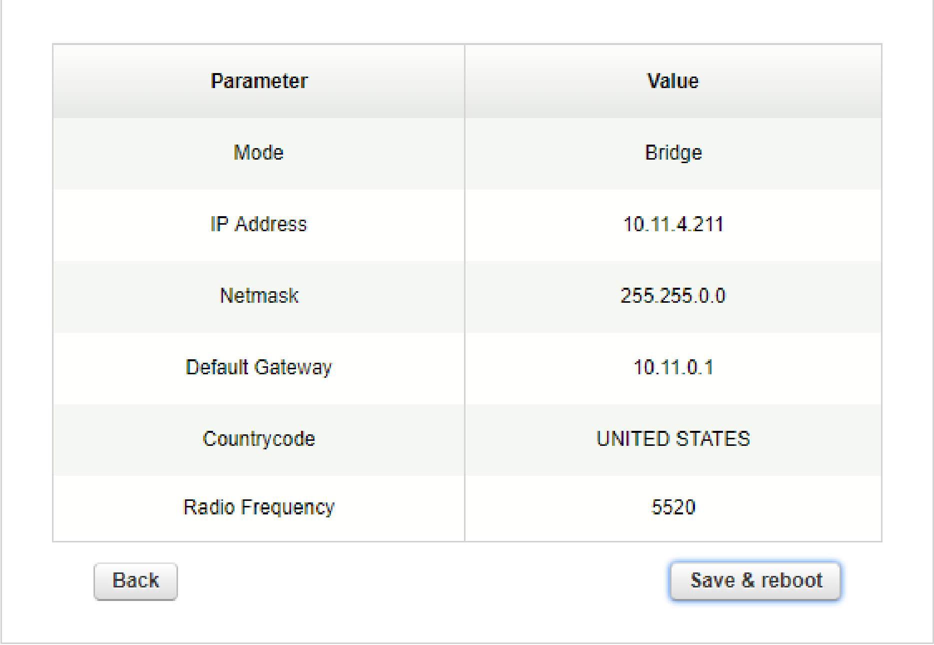
Figure 15. MeshWizard (Radio frequency window)

8. Select the frequency at which the unit must operate from the **Radio Frequency (MHz)** drop down list.

IMPORTANT

The radio units on both sides of a point-to-point wireless link must always be set to the same radio frequency value. A frequency mismatch will result in communication failure between the units.

9. Click the **Next** button.
   - The configuration confirmation dialog will be shown (Figure 16 (page 44)).



Parameter	Value
Mode	Bridge
IP Address	10.11.4.211
Netmask	255.255.0.0
Default Gateway	10.11.0.1
Countrycode	UNITED STATES
Radio Frequency	5520

Figure 16. MeshWizard (confirmation dialog)

10. Confirm that the values entered using the wizard are correct. If any values need to be changed, click the **Back** button. If all values are correct, click the **Save and reboot** button.
    - If you click the **Save and reboot** button, the configuration settings will be changed, and the unit will reboot.

7.4. General settings

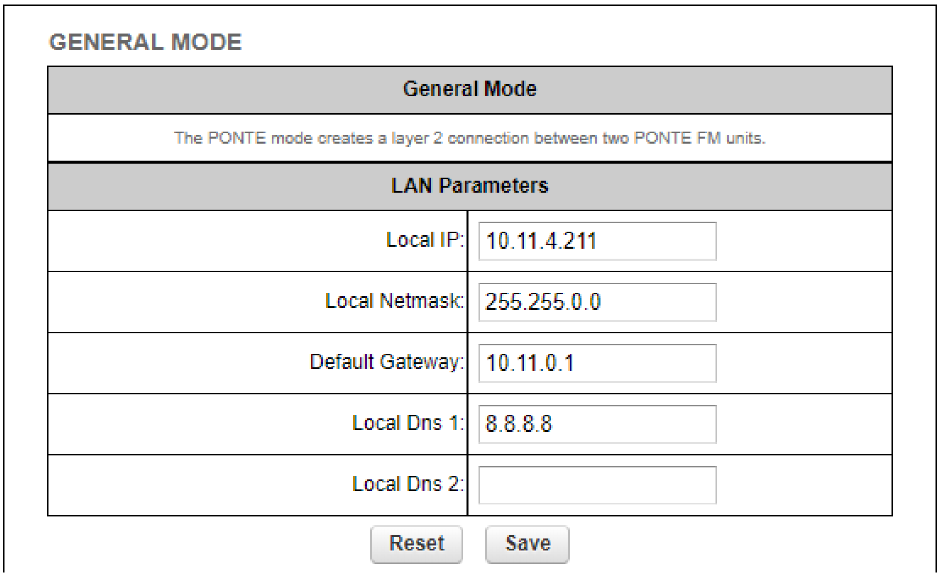
7.4.1. The General Mode window

The General Mode window contains controls to monitor and/or change the following settings:

- The unit's LAN parameters.

To change the General Mode settings, do the following steps:

- Click the **-general mode** link under **GENERAL SETTINGS** in the left-hand settings menu (below).



GENERAL MODE

General Mode

The PONTE mode creates a layer 2 connection between two PONTE FM units.

LAN Parameters

Local IP: 10.11.4.211

Local Netmask: 255.255.0.0

Default Gateway: 10.11.0.1

Local Dns 1: 8.8.8.8

Local Dns 2:

Figure 17. Configurator GUI (General Mode)

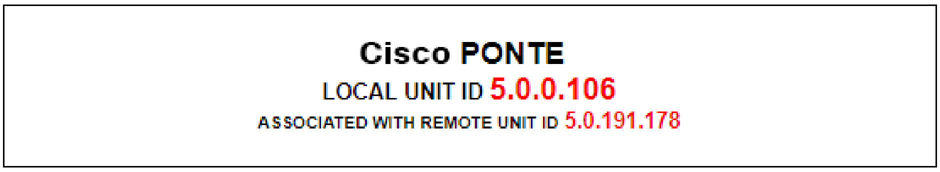
- The **GENERAL MODE** dialog will be shown (Figure 17 (page 45)).

Changing the operational mode

Operational mode settings on a bridge network-only unit

The Cisco FM Ponte kit kit contains two radio transceiver units. Both units can only be operated in *Bridge Mode*.

The Cisco device ID number of the unit that forms the opposite sideof the wireless bridge will be shown in the Configurator window heading block (Figure 18 (page 45)).



Cisco PONTE

LOCAL UNIT ID 5.0.0.106

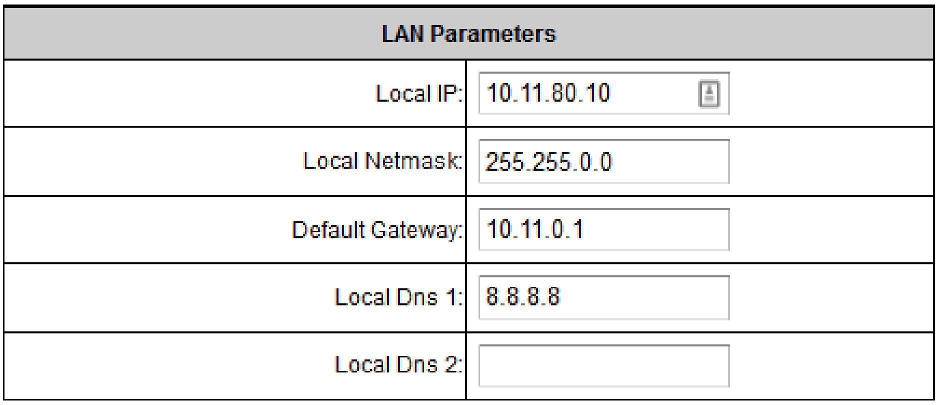
ASSOCIATED WITH REMOTE UNIT ID 5.0.191.178

Figure 18. Configurator window heading block

The Bridge ID of the remote unit to which the local unit must be linked is set at the factory and does not need configuration.

Changing the LAN parameters

The LAN Parameters box (below) contains the entry controls for local-address setting.



LAN Parameters	
Local IP:	10.11.80.10
Local Netmask:	255.255.0.0
Default Gateway:	10.11.0.1
Local Dns 1:	8.8.8.8
Local Dns 2:	

NOTE

When the **General Mode** window is opened for the first time, the **Local IP** and **Local Netmask** LAN parameters will be factory-set default values.

The information needed is self-explanatory. To enter a parameter, click the field and type the parameter.

If needed, enter the local primary DNS address in the **Dns 1** field, and enter the local secondary DNS address in the **Dns 2** field.

Save the LAN settings by clicking the **Save** button. Alternatively, clear the settings by clicking the **Reset** button.

7.4.2. Wireless settings

Modifying the wireless settings

IMPORTANT

If the Cisco FM Ponte kit was purchased in the USA or Canada, the Country selection is set to the country of purchase, and the **Country:** drop-down will be disabled.

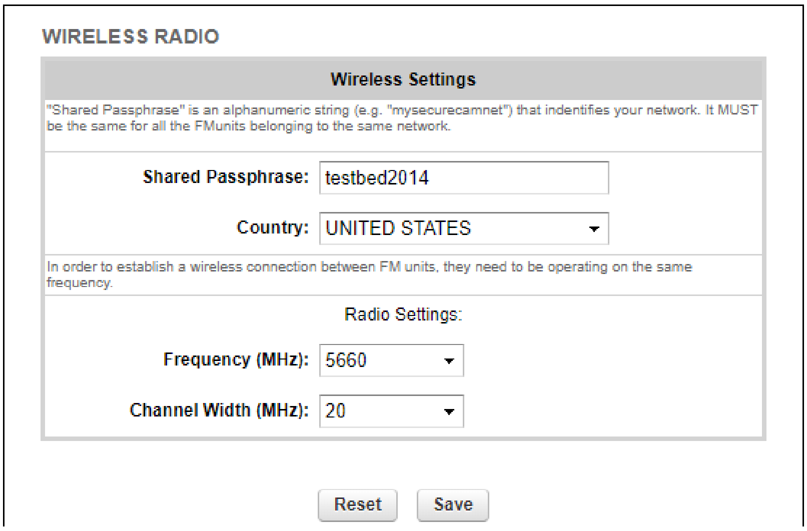
The **WIRELESS RADIO** window contains controls to change the following settings:

- The shared network passphrase.
- The national territory in which the wireless network is installed.
- The operational radio frequency and bandwidth settings.

To change the Wireless Settings, do the following steps:

1. Click the **-wireless radio** link under **GENERAL SETTINGS** in the left-hand settings menu.

- The **WIRELESS RADIO** dialog will be shown (Figure 19 (page 47)).



WIRELESS RADIO

Wireless Settings

"Shared Passphrase" is an alphanumeric string (e.g. "mysecurecamnet") that indentifies your network. It MUST be the same for all the FMunits belonging to the same network.

Shared Passphrase: testbed2014

Country: UNITED STATES

In order to establish a wireless connection between FM units, they need to be operating on the same frequency.

Radio Settings:

Frequency (MHz): 5660

Channel Width (MHz): 20

Figure 19. Configurator GUI (Wireless Radio dialog)

2. Enter a defined network passphrase in the Shared Passphrase field.

IMPORTANT

If a shared passphrase is defined, the same passphrase must be used for all Cisco units inthe same network.

The shared passphrase can be composed of any ASCII characters except the following: **'`"\$=**

3. Specify the country in which the unit is installed by selecting the correct option from the **Country** drop-down menu.

CAUTION

Different countries frequently have differing telecommunications regulations. If the Country listing is not set correctly, the unit may violate national telecommunications legislation.

4. Specify the unit's operating frequency by clicking the correct option in the **Frequency (MHz)** drop-down.

CAUTION

Make sure that the chosen country listing matches the country in which the unit is installed before changing the **Frequency (MHz)** value.

- You can change the frequency of each radio link in order to minimize interference with other wireless networks operating in the same area. The frequencies shown on the **Frequency (MHz)** selector are the carrier frequencies.

5. If **Advanced** configuration mode was selected, choose the required channel bandwidth from the **Channel Width (MHz)** drop-down. Note that the radio units on both sides of a wireless link must be set to the same channel width value. A channel width mismatch will result in degraded communication between the units.

> **CAUTION**
>
> Before finalizing the settings on the **WIRELESS RADIO** window, refer to "Important considerations for wireless settings" (page 48) below. This section contains important information that may influence your choice of wireless settings.

Important considerations for wireless settings

The following sub-sections contain important technical and regulatory information that influences the settings on the **WIRELESS RADIO** window.

- For information on how to avoid network co-location interference, refer to "Co-location considerations" (page 48).
- For information on the effects of channel width on data rate and throughput, refer to "Channel width considerations" (page 49).

Co-location considerations

To avoid radio interference caused by unit co-location, set the frequencies of co-located transceivers as far apart as practically possible.

Before a network is deployed, frequency allocations for every unit-to-unit link must be planned in advance. A safe method is to use the narrowest channel width that can realistically support the needed amount of data throughput whilst separating the individual channels as much as possible.

Even if two radios are not transmitting on the same channel, their side lobes may still cause them to interfere with each other. It is good practice to space the radios as far apart as practically possible in the vertical plane, with a minimum of 3ft/1m and an ideal distance of 5ft/1.5m between them.

Mounting radio transceiver units back-to-back or side by side may cause co-location interference that will degrade performance across your network.

Channel width considerations

Whenever practically possible, setting the unit to operate at a narrower channel width can help reduce overall network interference by increasing the number of available channels.

WARNING

Before changing the channel width value, make sure that the overall frequency range you will be using is legal for your territory. Changing the operating channel width may violate the local telecommunication authority's regulations, lead to illegal wireless operation, and have other harmful consequences.

The following table correlates different channel widths with their theoretical maximum data rates and achievable throughput, assuming that the unit is being used as part of a point-to-point configuration.

IMPORTANT

The following table shows theoretical values under ideal conditions. Actual throughput may vary depending on environmental and other conditions.

The Cisco FM Ponte kit is limited to a theoretical maximum of 50 Mbps usable Ethernet throughput (under optimal wireless link conditions).

Table 4. Available Radio Channel Widths

Channel width	Max.modulation speed	Max. throughput
5 MHz	37 Mb/s	8 Mb/s
10 MHz	75 Mb/s	16 Mb/s
20 MHz	150 Mb/s	90 Mb/s
40 MHz	300 Mb/s	150 Mb/s

7.4.3. Antenna-alignment tools and physical statistics

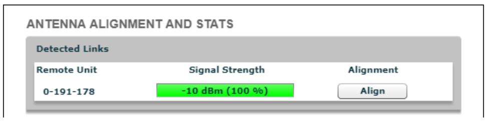
The **ANTENNA ALIGNMENT AND STATS** window contains controls to monitor current and average radio link status during operation of the unit, allowing you to easily adjust the alignment of the unit's antennas.

The window shows a list of wireless links to other Cisco units that have been detected by the local unit, and the relative strength of each wireless link in decibel-milliwatts (dBm).

To do an accurate alignment of a local antenna for a specific wireless link, do the following steps:

1. Click the **-antenna alignment and stats** link under **GENERAL SETTINGS** in the left-hand settings menu.

- The **ANTENNA ALIGNMENT AND STATS** window will be shown (Figure 20 (page 50)).



ANTENNA ALIGNMENT AND STATS

Detected Links

Remote Unit	Signal Strength	Alignment
0-191-178	-10 dBm (100 %)	Align

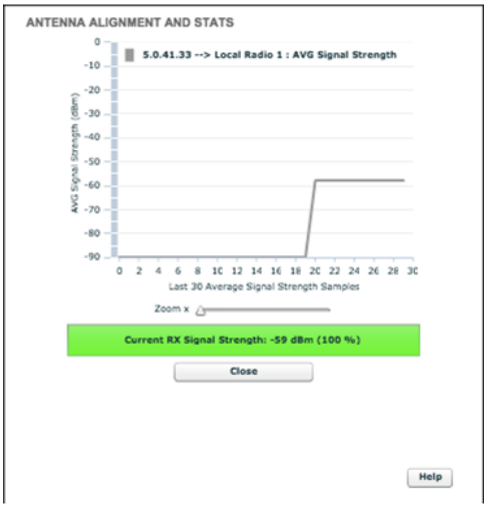
Figure 20. Configurator GUI (Antenna alignment and stats dialog)

2. More than one two-way wireless link may be shown in the **Detected Links** table. Find the two-way link for which the local antenna must be adjusted.

3. Click the **Align** button.

   - The **ANTENNA ALIGNMENT AND STATS** tool will be shown (Figure 21 (page 50)).

> **IMPORTANT**
>
> The Cisco Transmission Power Control (TPC) algorithm will be disabled during the antenna alignment process. This eliminates the possibility of false radio-transmission power readings.



ANTENNA ALIGNMENT AND STATS

5.0.41.33 --> Local Radio 1 : AVG Signal Strength
AVG Signal Strength (dBm)
0
-10
-20
-30
-40
-50
-60
-70
-80
-90
0
2
4
6
8
10
12
14
16
18
20
22
24
26
28
30
Last 30 Average Signal Strength Samples
Zoom x
Close
Help

Current RX Signal Strength: -59 dBm (100 %)

Figure 21. Antenna alignment and stats tool

4. The tool consists of:

   - A graph that reports average signal strength over the last 30 strength-sampling periods.
   - A bar that reports the quality of the signal currently being detected at the local unit receiver.

5. Do the physical antenna alignment by manually adjusting the location and direction of the relevant antenna. During the alignment, use the graph and bar readings to monitor variations in signal strength.
6. To increase the readability of the average signal strength graph, click-and-drag the **Zoom x** slider.
7. When the antenna alignment is complete, click the **Close** button.
   - The antenna alignment and stats tool will be closed.

7.5. Network control

7.5.1. Ping softdog

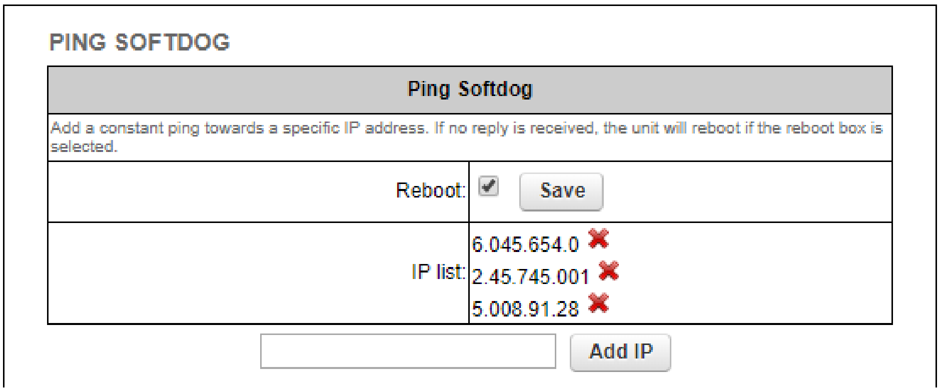
The **PING SOFTDOG** window contains controls to set up a constant series of pings to one or more IP addresses.

If connectivity is lost between the unit and any of the saved IP addresses, an option can also be set to automatically reboot the Cisco FM Ponte kit.

> **TIP**
> As well as being a fail-safe mechanism to monitor network connectivity, the constant ping can also be used as a 'keep-alive' message to devices that need uninterrupted connectivity, such as VoIP telephones.

To use the constant ping and automatic reboot functions, do the following steps:

1. Click the **-ping softdog** link under **NETWORK CONTROL** in the left-hand settings menu.
   - The **PING SOFTDOG** dialog will be shown (Figure 22 (page 51)).



PING SOFTDOG

Ping Softdog

Add a constant ping towards a specific IP address. If no reply is received, the unit will reboot if the reboot box is selected.

Reboot: ☑ Save

IP list: 6.045.654.0 ✖
2.45.745.001 ✖
5.008.91.28 ✖

Add IP

Figure 22. Configurator GUI (Ping Softdog dialog)

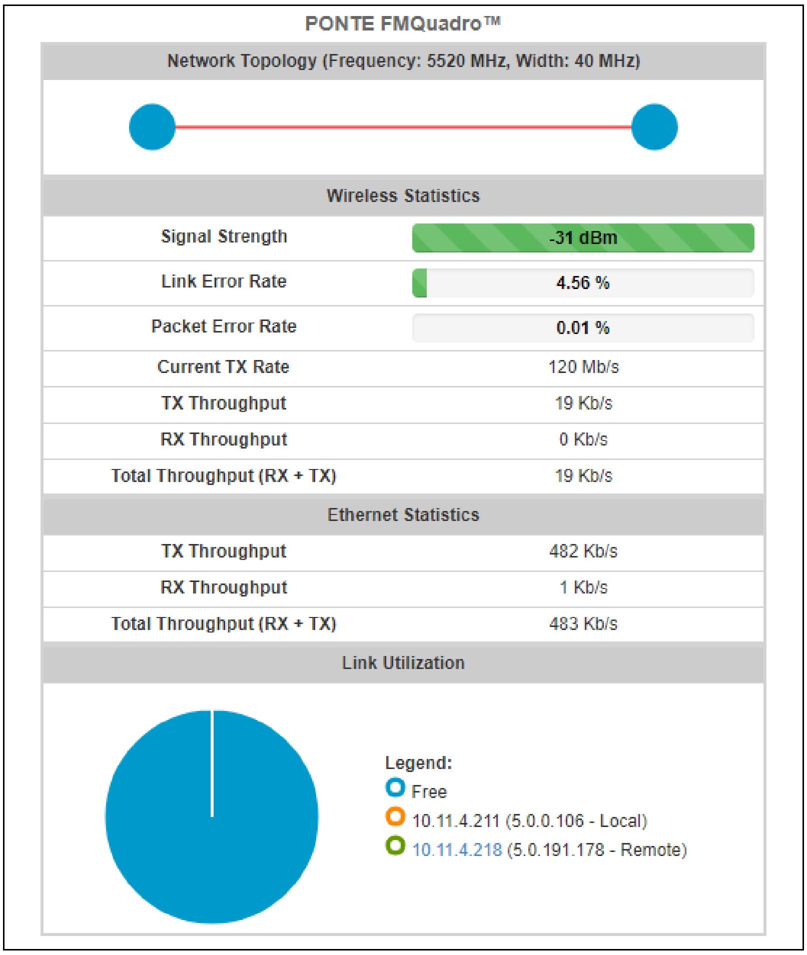
2. To set up a constant ping to one or more IP addresses, do the following steps:

    1. Enter the IP address in the field to the left of the **Add IP** button.
    2. Click the **Add IP** button.
        - The IP Address will be added to the IP list.
        - There is no limit on the number of IP addresses that can be entered.
    3. To delete an IP address from the IP list, click the red cross to the right of the IP address listing.
3. To automatically reboot the unit if connectivity is lost between the unit and any IP address, do the following steps:
    1. Check the **Reboot:** check-box.
    2. Click the **Save** button.

7.5.2. FM-QUADRO

FM-QUADRO for bridge network-capable devices

The *PONTE FMQuadro™* window (Figure 23 (page 53)) contains a dynamic information display that shows important information about the two Cisco FM Ponte kit bridge devices and the wireless link between them, and allows you to diagnose problems with the wireless link.



PONTE FMQuadro™

Network Topology (Frequency: 5520 MHz, Width: 40 MHz)

Wireless Statistics	
Signal Strength	-31 dBm
Link Error Rate	4.56 %
Packet Error Rate	0.01 %
Current TX Rate	120 Mb/s
TX Throughput	19 Kb/s
RX Throughput	0 Kb/s
Total Throughput (RX + TX)	19 Kb/s
Ethernet Statistics	
TX Throughput	482 Kb/s
RX Throughput	1 Kb/s
Total Throughput (RX + TX)	483 Kb/s

Link Utilization

Legend:
○ Free
○ 10.11.4.211 (5.0.0.106 - Local)
○ 10.11.4.218 (5.0.191.178 - Remote)

Figure 23. PONTE FMQuadro™ window

The *Network Topology* section shows:

- A stylized bridge network connection between the two Cisco FM Ponte kit units.
- The operating frequency and channel width of the two units.

The *Wireless Statistics* section shows real-time values for each of the following:

- **Signal Strength:** The current signal level being received, in dBm.
- **Link Error Rate:** The percentage of packet re-transmissions due to transmission errors.
- **Packet Error Rate:** The percentage of packets dropped due to excessive transmission errors.
- **Current TX Rate:** The current link transmission rate, in Mb/s.
- **TX Throughput:** Rate of successful message transmission by the unit over the wireless link.
- **RX Throughput:** Rate of successful message reception by the unit over the wireless link.

- **Total Throughput (RX + TX):** Rate of successful combined message delivery over the wireless link.

The *Ethernet Statistics* section shows real-time values for each of the following Ethernet-related values:

- **TX Throughput:** Rate of successful message transmission by the unit over the wireless link.
- **RX Throughput:** Rate of successful message reception by the unit over the wireless link.
- **Total Throughput (RX + TX):** Rate of successful combined message delivery over the wireless link.

The *Link Utilization* section shows a comparative graph and values for each of the following:

- *Blue:* Link bandwidth that is currently un-utilized.
- *Orange:* link bandwidth that is currently in use by the local Cisco FM Ponte kit unit.
- *Green:* link bandwidth that is currently in use by the remote Cisco FM Ponte kit unit.

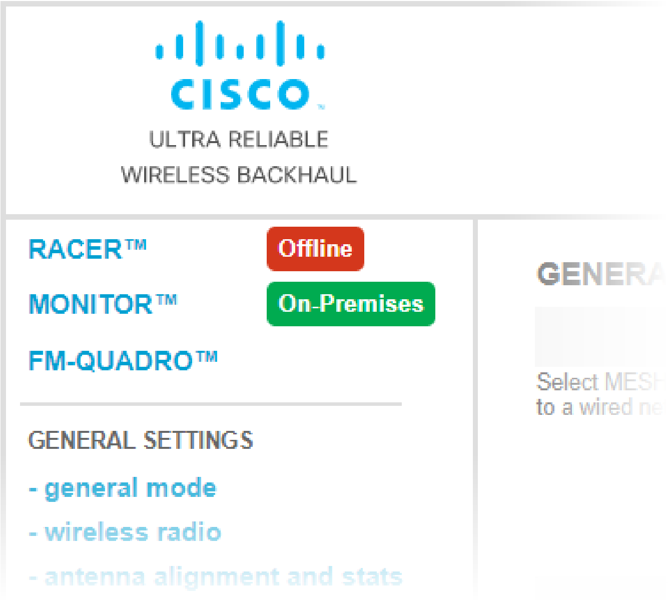
Plotting and interpreting the wireless links

NOTE

The statistical information refresh period is:

- One second for Fluidity (mobile) networks.
- Six seconds for stationary networks.

To plot and interpret all wireless links in the current network, click the **FM-QUADRO™** link in the upper left part of the settings menu (below).



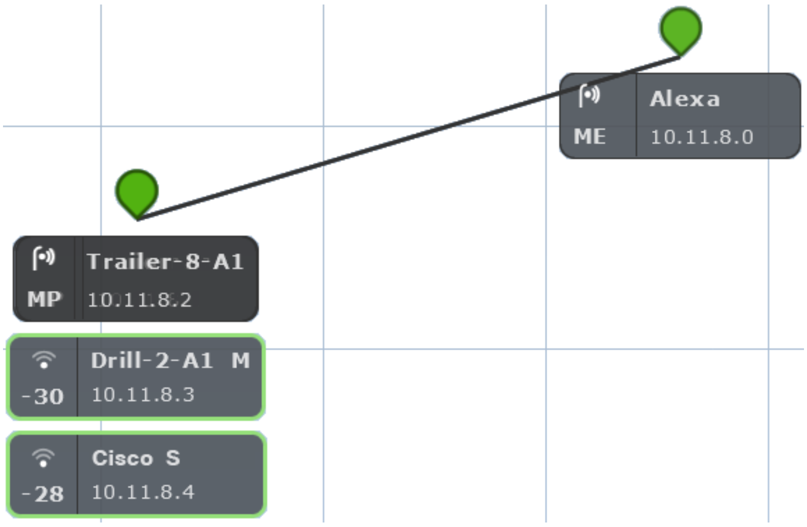
IMPORTANT

If you are working within a Fluidity Layer-3 network cluster, and the network cluster has more than one Mesh-end radio, access FM-QUADRO through the Configurator interface of the cluster's *Primary* Mesh-end.

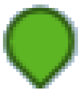
Find the Primary Mesh-end by comparing the Mesh ID values of the Mesh-end radios. The Primary Mesh-end will have a numerically lower Mesh ID value than the Secondary Mesh-end.

If you access the FM-QUADRO interface belonging to the cluster's *Secondary* Mesh-end, the network topology view will be shown, but some statistics and configuration information may not be available to view.

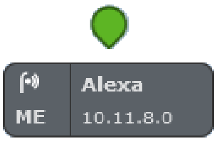
- A graphical view of the current network topology will be shown. A typical example is shown below.



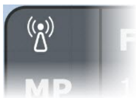
- Stationary (wayside, or infrastructure) Cisco radio transceivers are shown as colored icons (below).



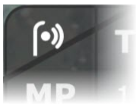
- Stationary radio transceiver icons are colored according to the performance of their data links relative to preset KPI thresholds:
  - If an icon is white, KPI checking is not currently enabled for the FM Quadro view.
  - If an icon is red, the performance of at least one link is below standard (red link line).
  - If an icon is orange, the performance of at least one link is acceptable, but not optimal (orange link line).
  - If an icon is green, the performance of all links is optimal (green link lines).
- A tooltip is shown below each stationary transceiver icon (below).



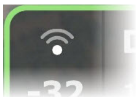
- In clockwise order, the tooltip shows the following information:
  - The *device type icon.* Depending on device type, any of three icons may be seen:
    - The icon below will be shown if the device is a stationary non-Fluidity radio device:



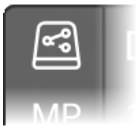
  - The icon below will be shown if the device is a stationary radiodevice that is part of a Fluidity network:



  - The dynamic Wi-Fi reception-style icon below will be shown if the radio device is a mobile device that is part of a Fluidity network. This icon shows whether the radio's current RSSI is weak, acceptable or strong.

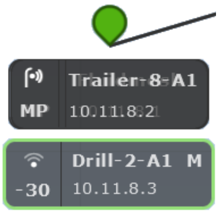


  - The icon below will be shown if the device is an Ultra-reliable Wireless Backhaul Gateway device.



- The device label, corresponding to the device’s name configuration parameter (*Alexa* in the image above).
- If the device is a mobile radio transceiver, the device’s Primary/Subordinate setting will be shown. A Primary device is marked M, and a Subordinate device is marked S.
- The device’s IP address.
- If the device is a stationary mesh end, it will be marked *ME*. If it is a stationary mesh point, it will be marked *MP*. If it is a mobile radio, the RSSI (in dBm) between the radio and the stationary radio to which it is connected will be shown.
- If the device does not currently have a configured IP address or device label, the device’s Cisco Mesh ID number willbe shown.
- If the network is a Fluidity network, mobile Cisco radio transceivers that are part of the network are shown as tooltips with colored borders. The tooltip representing a mobile Cisco radio is always shown below the tooltip of

the stationary transceiver to which it is currently connected (below).



- Mobile-radio tooltip borders are colored according to the radio's performance relative to its currently configured KPI thresholds:
  - If LER is less than or equal to 15%, PER is 0%, and RSSI is greater than or equal to -81 dBm, radio performance is optimal, and the tooltip border will be green.
  - If LER is between 15% and 30% or RSSI is between -86 dBm and -81 dBm, radio performance is acceptable, and the tooltip border will be orange.
  - If LER is greater than 30%, PER is greater than 0%, or RSSI is less than -86 dBm, radio performance is below standard, and the tooltip border will be red.

IMPORTANT

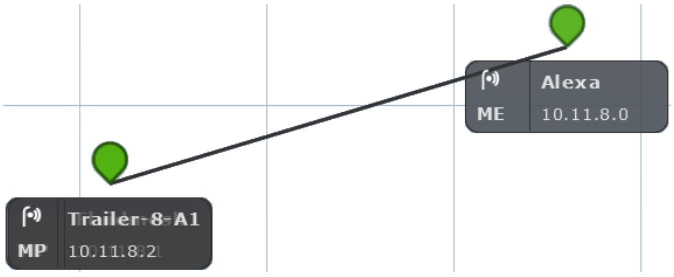
The KPI thresholds that govern tooltip border color cannot be changed.

If you need to adjust KPI thresholds to custom values, you must use FM Monitor as the primary network monitoring tool.

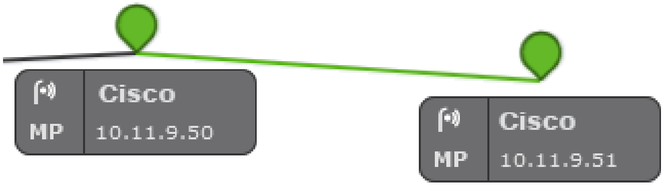
If a mobile radio connected to a stationary radio hands off to another stationary radio, the tooltip representing the mobile radio will move to a position underneath the tooltip of the connected stationary radio. If a stationary or mobile radio is disconnected from the network or cannot be reached, it will not be shown in the FM-QUADRO view.

Network connectivity links between stationary radio transceivers are shown as lines:

- A wired LAN link is shown as a solid black line (below).



- A wireless LAN link is shown as a colored line (a typical example is shown below).



Wireless LAN link lines are colored according to the link's performance relative to its currently configured KPI thresholds:

- If LER is less than or equal to 15%, PER is 0%, and RSSI is greater than or equal to -81 dBm, link performance is optimal, and the link line will be green.
- If LER is between 15% and 30% or RSSI is between -86 dBm and -81 dBm, link performance is acceptable, and the link line will be orange.
- If LER is greater than 30%, PER is greater than 0%, or RSSI is less than -86 dBm, link performance is below standard, and the link line will be red.
- If a wireless link is currently in use as a wireless route, but KPI checking is not enabled, the link will be shown as a solid light blue line.

IMPORTANT

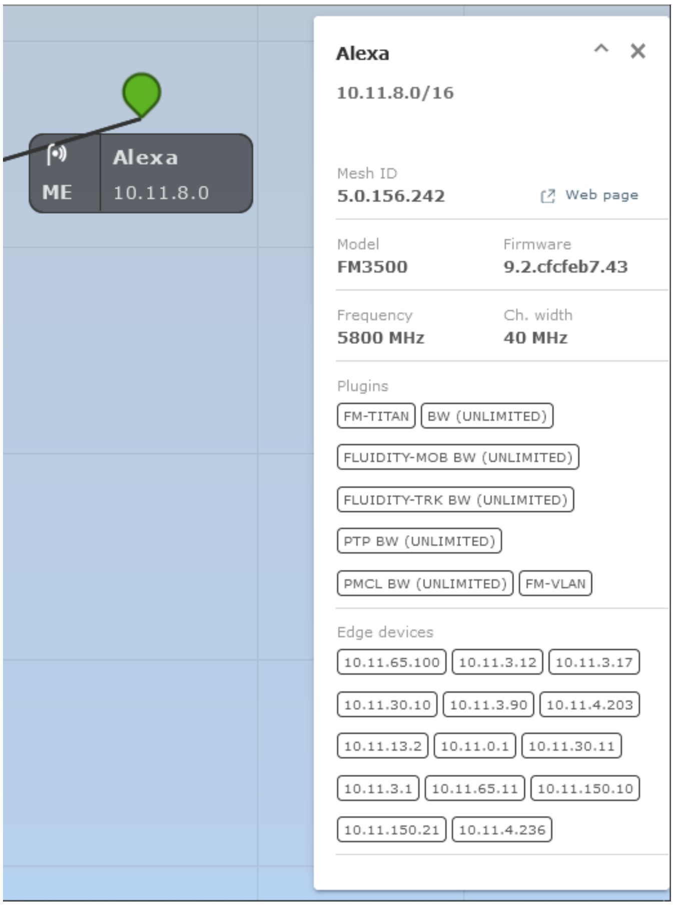
The KPI thresholds that govern wireless link line color cannot be changed.

If you need to adjust KPI thresholds to custom values, you must use FM Monitor as the primary network monitoring tool.

Viewing live data for a radio or wireless link

The device elements shown in the main view are interactive. To get additional real-time information on any Ultra-Reliable Wireless Backhaul device or wireless link, click its icon or tooltip.

- For stationary radio transceivers, an information sidebar will be shown on the right side of the view (a typical sidebar is shown below).



Alexa

10.11.8.0/16

Mesh ID
5.0.156.242

Web page

Model	Firmware
FM3500	9.2.cfcfeb7.43

Frequency	Ch. width
5800 MHz	40 MHz

Plugins

FM-TITAN | BW (UNLIMITED) | FLUIDITY-MOB BW (UNLIMITED) | FLUIDITY-TRK BW (UNLIMITED) | PTP BW (UNLIMITED) | PMCL BW (UNLIMITED) | FM-VLAN

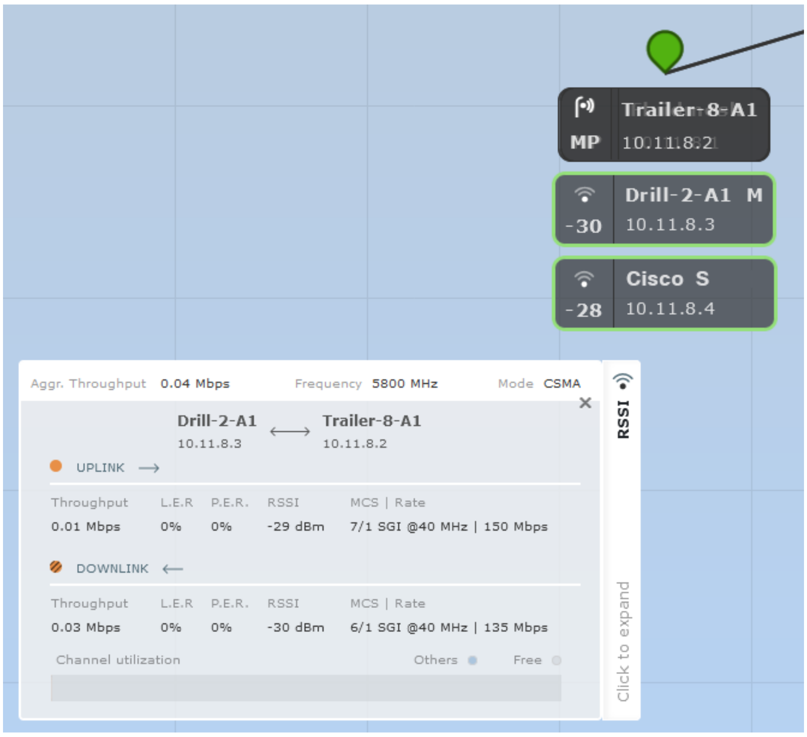
Edge devices

10.11.65.100 | 10.11.3.12 | 10.11.3.17 | 10.11.30.10 | 10.11.3.90 | 10.11.4.203 | 10.11.13.2 | 10.11.0.1 | 10.11.30.11 | 10.11.3.1 | 10.11.65.11 | 10.11.150.10 | 10.11.150.21 | 10.11.4.236

- When an information sidebar is shown for a stationary radio, the sidebar shows the following information:
  - The device name label.
  - The device's IP address and netmask (a typical example might be 10.11.8.0/16).
  - The device's Mesh ID number.
  - A **Web page** link. Clicking this link will open the device's offline Configurator interface in a new window.
  - The device model name.
  - The device's current firmware version.
  - The device's operating frequency.
  - The device's operating channel width.
  - A list of the software plug-ins currently installed on the device.
  - If the device is a stationary radio, a list of IP addresses belonging to all non-Cisco edge devices currently connected to the device will be shown.

NOTE
Only one device information sidebar can be shown at any time.

- For mobile radio transceivers, the same information sidebar will be shown on the right side of the view. An information widget will also be shown on the lower left part of the view.
- For wireless links, only the information widget will be shown. A typical information widget is shown below:



Aggr. Throughput 0.04 Mbps Frequency 5800 MHz Mode CSMA

Drill-2-A1 ⟷ Trailer-8-A1
10.11.8.3 10.11.8.2

● UPLINK ⟶

Throughput	L.E.R	P.E.R.	RSSI	MCS | Rate
0.01 Mbps	0%	0%	-29 dBm	7/1 SGI @40 MHz | 150 Mbps

▨ DOWNLINK ⟵

Throughput	L.E.R	P.E.R.	RSSI	MCS | Rate
0.03 Mbps	0%	0%	-30 dBm	6/1 SGI @40 MHz | 135 Mbps

Channel utilization Others ● Free ○

NOTE
A maximum of two radio information widgets can be shown at any time.

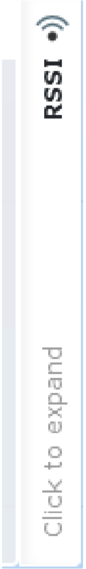
When an information widget is shown for a mobile radio or a wireless link, the widget shows the following information:

- The widget header shows the aggregate throughput, operating frequency, and channel-access mode of the link between the mobile transceiver and the stationary transceiver to which it is connected.
- The two radios connected by the wireless link are shown as name labels with IP addresses, connected by a double-pointed line.
- The main body of the widget contains live readings on uplink and downlink throughput, LER, PER, RSSI, MCS, and modulation rates.

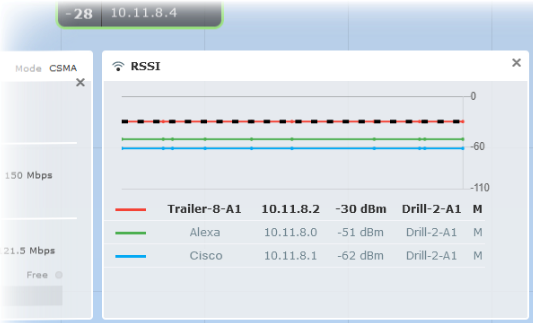
A channel-utilization bar shows uplink and downlink utilization for the selected pair of devices, as well as link utilization by other links.

Viewing live RSSI data for a wireless link

To see an RSSI information chart for any wireless link between a stationary radio and mobile radio, click the **Click to expand** link on the mobile radio's information widget (below).



A typical RSSI information chart is shown below:



🟥	**Trailer-8-A1**	**10.11.8.2**	**-30 dBm**	**Drill-2-A1**	**M**
🟩	Alexa	10.11.8.0	-51 dBm	Drill-2-A1	M
🟦	Cisco	10.11.8.1	-62 dBm	Drill-2-A1	M

When an RSSI information chart is shown for a wireless link, the chart shows the following information:

- The bold dashed line on the upper part of the graph is the RSSI envelope for the wireless link between the relevant mobile radio and the stationary radio to which it is currently connected.
- The solid lines on the upper part of the graph are RSSI readings for other stationary and mobile radios that are part of the network.

- The table on the lower part of the information chart contains device identification and real-time RSSI readings for other stationary and mobile radios that are part of the network.

Manipulating the FM-QUADRO view

FM-QUADRO can be manipulated and edited to make any network easy to view.

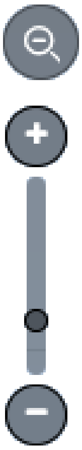
To change the overall position of the network view, click any blank part of the view, and drag the view to any position on the screen.

To very quickly zoom into or out of the network view, click any blank part of the view, and scroll back and forth with the mouse wheel.

- The view will snap between four pre-determined zoom settings.

To apply fine zoom adjustment to the network view, do the steps that follow:

1. Click the *Zoom* icon on the upper right part of the FM-QUADRO view (upper icon, below).



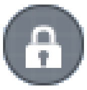
   - The Zoom slider and buttons will be shown (above).

2. Click the **+** button to zoom into the view, or click the **–** button to zoom out of the view. Alternatively, click-and-drag the zoom slider to adjust the zoom level.

Changing the relative position of device icons

All Ultra-Reliable Wireless Backhaul devices represented by icons or tooltips can be placed in any position on the FM-QUADRO view. To move any icon or tooltip, do the steps that follow:

1. Click the *Edit Mode* icon on the upper right part of the FM-QUADRO view (below).



Alternatively, enter Edit mode by clicking the *Settings* icon on the upper right part of the FM-QUADRO view, and clicking the **Edit Mode** switch in the *Appearance / Background* dialog from **Off** to **On**.

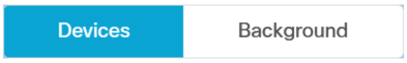
- The *Edit mode* dialog will be shown.

2. Click the **Continue to Edit Mode** button to enable Edit Mode.

   - An *Edit Mode: ON* notification will appear in the view.

To move any icon and its tooltip to a different position, do the steps that follow:

1. Click the *Devices* portion of the **Devices | Background** button (below).



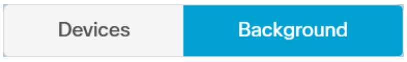
2. Click-and-drag any of the stationary device icons or tooltips to any needed position in the Topology view. Note that tooltips representing mobile radios do not appear in Edit mode.

   Alternatively, you can reset the Topology view to a strictly hierarchical structure by clicking the **Apply hierarchical view** link in the lower right part of the view.

If needed, you can add an aerial image to the Topology view. This allows you to superimpose the network view over a map of the terrain on which the network has been installed. For instructions on how to add an aerial image as a background to the Topology view, refer to "Adding an aerial map to the FM-QUADRO view" (page 66).

To move an uploaded background image to a different position, do the steps that follow:

1. Click the *Background* portion of the **Devices | Background** button (below).



2. Click-and-drag the background image to any needed position in the Topology view.
3. Adjust the scale of the background image by clicking-and-dragging the **Adjust background scale** slider.
4. Adjust the relative transparency of the background image by clicking-and-dragging the **Adjust background transparency** slider.

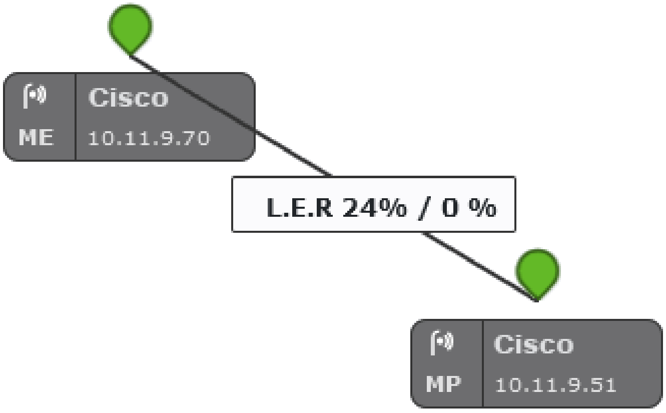
When you are finished editing, click the **Save changes** button to save your changes. Alternatively, click the **Discard changes** button to revert to your previous configuration.

- The Topology view will revert to View mode.

Showing KPI values for wireless links

To show an information ribbon containing key performance indicators next to all wireless link lines, do the steps that follow:

1. Click the *Settings* icon on the upper right part of the FM-QUADRO view (below).
   - The *Appearance / Background* dialog will be shown.
2. If the *Background* settings are shown, click the **Appearance** heading.
3. Click the **KPI values on routes** switch from **Off** to **On**.
4. Click the check-boxes for each KPI you want to see for all wireless links. Available options are:
   - L.E.R. (Current link error rate, shown as a percentage)
   - P.E.R. (Current packet error rate, shown as a percentage)
   - RSSI (Current received signal strength, shown in dBm)
   - Link Utilization (shown as a percentage)
5. To save your changes, click the **Save changes** button. Alternatively, click the **Discard** button to leave the dialog without saving any changes.
   - An information ribbon containing the chosen key performance indicators will be shown next to all wireless link lines (a typical example is shown below).



Showing real-time color codes for radio transceiver key performance indicators

To show performance status indications (in the form of colored device icons) for radio transceivers in real time, do the steps that follow:

1. Click the *Settings* icon on the upper right part of the FM-QUADRO view (below).

   - The *Appearance / Background* dialog will be shown.

2. If the *Background* settings are shown, click the **Appearance** heading.
3. Click the **Default Thresholds** switch from **Off** to **On**.
4. In the **Thresholds per KPI** section, click the check-boxes for each KPI you want to influence the device icon status coloring. Available options are:
   - L.E.R. (Current link error rate)
   - P.E.R. (Current packet error rate)
   - RSSI (Current received signal strength)

   > **NOTE**
   >
   > The KPI thresholds that determine device icon colors cannot be adjusted. The preset KPI thresholds are as follows:
   >
   > - Optimal radio performance (green icon): LER ≤15%, PER = 0%, RSSI ≥-81 dBm
   > - Acceptable radio performance (orange icon): LER 15 to 30%, PER = 0%, RSSI -86 to -81 dBm
   > - Sub-standard radio performance (red icon): LER ≥30%, PER >0%, RSSI <-86 dBm

5. To save your changes, click the **Save changes** button. Alternatively, click the **Discard** button to leave the dialog without saving any changes.
   - All device icons representing radio transceivers will be shown in the FM Quadro view as appropriately colored icons.

Adding an aerial map to the FM-QUADRO view

You can add an aerial image to the FM-QUADRO view. This allows you to superimpose the network map over a map of the actual terrain on which the network has been installed, making it easier to visualize component placement, line-of-sight between antennas, and other factors.

To add an aerial terrain map to the FM-QUADRO view, do the following steps:

1. Get an aerial image of the area in which the wireless network and LAN are installed. The image must conform to the following requirements:
    - *Image formats:* *.PNG, *.JPG, *.JPEG or *.SVG only.
    - *File size:* Less than or equal to 500 Kilobytes (FM1000 and FM10000 Gateways only), or less than or equal to 150 Kilobytes (all radio transceivers).

    > **TIP**
    >
    > Suitable aerial images can be created and downloaded using Google Earth. Basic instructions on how to use Google Earth are available here.

    - Images can be uploaded to FM-QUADRO using Google Chrome, Firefox, Safari or Microsoft Internet Explorer. Cisco recommends using the latest version of Google Chrome or Firefox.
2. Click the *Settings* icon on the upper right part of the FM-QUADRO view (below).
    - The *Appearance / Background* dialog will be shown.
3. If the *Appearance* settings are shown, click the **Background** heading.
4. Click the **Image** radio button.
    - **Upload your file** and **Preview** sections will be shown.
5. Use the **Upload your file** section to upload the aerial image.
6. To save your changes, click the **Save changes** button. Alternatively, click the **Discard** button to leave the dialog without saving any changes.
    - Your chosen aerial image will be shown as a visual layer underneath the current network view.
7. If needed, move the device icons and/or tooltips to suit the aerial image as shown in "Changing the relative position of device icons" (page 63).

Adjusting the transparency of the aerial map view

You can adjust the transparency level of the aerial map view. This is a useful way to increase the visual definition of device icons, tooltips and link lines against strong background colors.

To adjust the transparency of the current aerial map view, do the steps that follow:

1. Click the *Edit Mode* icon on the upper right part of the FM-QUADRO view (below).

   🔒

   Alternatively, enter Edit mode by clicking the *Settings* icon on the upper right part of the FM-QUADRO view, and clicking the **Edit Mode** switch in the *Appearance / Background* dialog from **Off** to **On**.

   - The *Edit mode* dialog will be shown.

2. Click the **Continue to Edit Mode** button to enable Edit Mode.

   - An *Edit Mode: ON* notification will appear in the view.
   - The **Devices | Background** switch control will appear in the view.

3. Click the switch to *Background*.
4. Click-and-drag the *Adjust background transparency* slider to the position that gives a comfortable level of visual contrast between the network representation and the uploaded map view.
5. When the visual contrast is correct, click the **Save changes** button.

   - The *Save new layout* dialog will be shown.

6. To save your changes, click the **Save changes** button. Alternatively, click the **Keep editing** button to return to Edit Mode, or click the **Discard** button to leave Edit Mode without saving any changes.

Exporting a network representation file

You can export a representation file of the current network layout. This allows Cisco Technical Support to visualize the network for troubleshooting purposes.

To export a representation file for the current network, do the steps that follow:

1. Click the *Export as JSON* icon on the upper right part of the FM-QUADRO view (below).

- The *Export as JSON* dialog will be shown.

> **IMPORTANT**
>
> The dialog contains important information regarding confidentiality and FM-QUADRO functionality. Read and understand the dialog before you click the **Export** button.

2. Click the **Export** button to export the network representation as a *.JSON file. Alternatively, click the **Cancel** button to leave the dialog without exporting.
   - If you clicked the **Export** button, the *.JSON file will be downloaded as a *.ZIP package. Open the *.ZIP package to access the *.JSON file.
3. Forward the *.JSON file, and the diagnostic file exported from the device status page, to Cisco Technical Support.

7.5.3. Advanced tools

The Advanced Tools window contains tools to diagnose the condition of the wireless network.

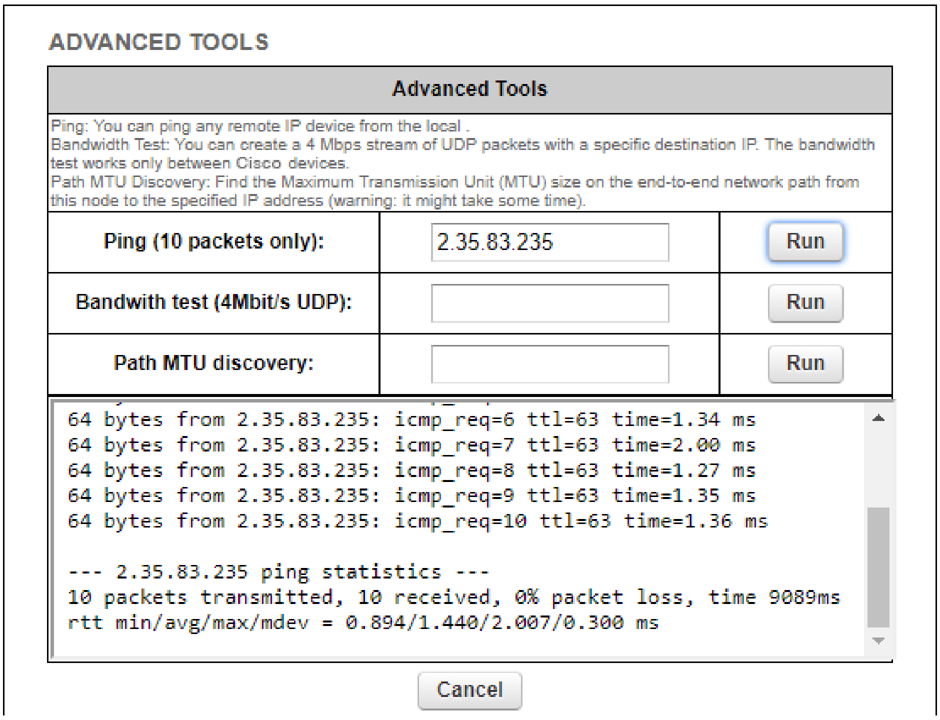
- The Ping test tool sends pings to a user-specified IP address.
- The Bandwidth test tool tests the bandwidth capacity of the wireless link between the Cisco unit and a user-specified IP address.
- The Path MTU tool tests the size of the maximum transmission unit.

To open the Advanced Tools dialog, click the **-advanced tools** link under **NETWORK CONTROL** in the left-hand settings menu.

Using the Ping test tool

The Ping test can be run while the network is under load (to test operational performance), or with the network unloaded (to test installed capacity). To use the Ping test tool, do the following steps:

1. Determine which wireless link is to be tested between the Cisco unit and another unit in the wireless network. Get theIP address of the other unit.
2. Enter the IP address of the other unit in the **Ping (10 packets only)** field (Figure 24 (page 70)).



ADVANCED TOOLS

Advanced Tools

Ping: You can ping any remote IP device from the local .
Bandwidth Test: You can create a 4 Mbps stream of UDP packets with a specific destination IP. The bandwidth test works only between Cisco devices.
Path MTU Discovery: Find the Maximum Transmission Unit (MTU) size on the end-to-end network path from this node to the specified IP address (warning: it might take some time).

Ping (10 packets only):	2.35.83.235	Run
Bandwith test (4Mbit/s UDP):		Run
Path MTU discovery:		Run

```
64 bytes from 2.35.83.235: icmp_req=6 ttl=63 time=1.34 ms
64 bytes from 2.35.83.235: icmp_req=7 ttl=63 time=2.00 ms
64 bytes from 2.35.83.235: icmp_req=8 ttl=63 time=1.27 ms
64 bytes from 2.35.83.235: icmp_req=9 ttl=63 time=1.35 ms
64 bytes from 2.35.83.235: icmp_req=10 ttl=63 time=1.36 ms

--- 2.35.83.235 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9089ms
rtt min/avg/max/mdev = 0.894/1.440/2.007/0.300 ms
```

Figure 24. Advanced Tools window (Ping test tool)

3. Click the **Run** button to the right of the IP address field.
    - The ping test result will be shown below the test controls.

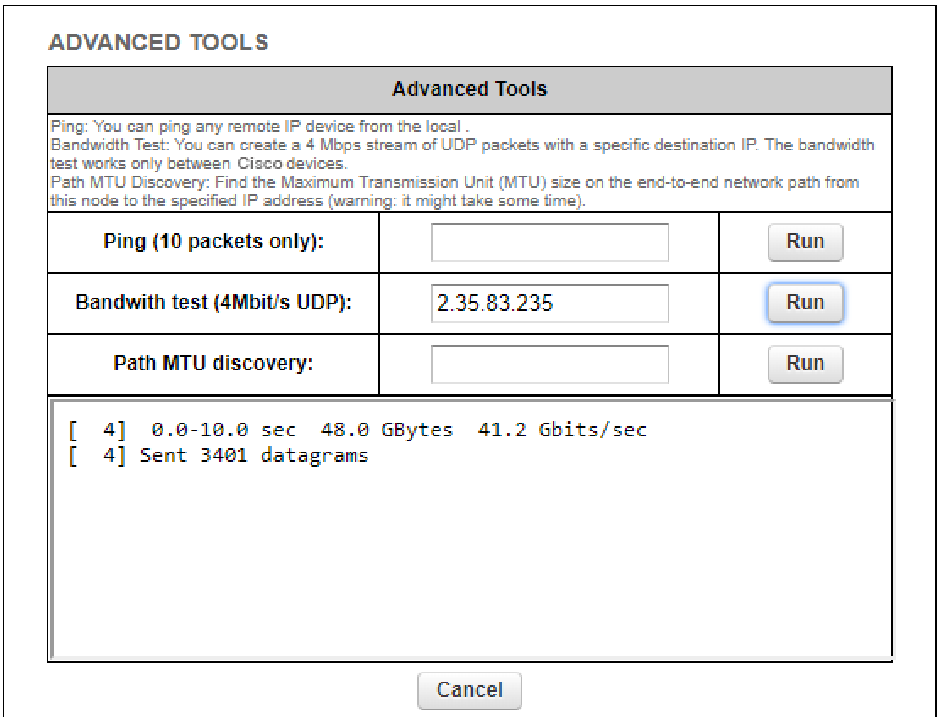
Using the Bandwidth Test tool

The Bandwidth test can be run with the network under load (to test operational performance), or with the network unloaded (to test installed capacity). The test tool generates a stream of packets at a rate of 4 Mbits/sec to test available network path throughput.

> **IMPORTANT**
>
> Bandwidth rate computation is CPU-intensive, and must be regarded as indicative only. Note that bandwidth testing tends to underestimate the actual link throughput.

To use the Bandwidth test tool, do the following steps:

1. Determine what wireless link is to be tested between the Cisco unit and another unit in the wireless network. Get theIP address of the other unit.
2. Enter the IP address of the other unit in the **Bandwith test (4Mbit/s UDP):** field (Figure 25 (page 71)).



ADVANCED TOOLS

Advanced Tools		
Ping: You can ping any remote IP device from the local . Bandwidth Test: You can create a 4 Mbps stream of UDP packets with a specific destination IP. The bandwidth test works only between Cisco devices. Path MTU Discovery: Find the Maximum Transmission Unit (MTU) size on the end-to-end network path from this node to the specified IP address (warning: it might take some time).		
Ping (10 packets only):		Run
Bandwith test (4Mbit/s UDP):	2.35.83.235	Run
Path MTU discovery:		Run

```
[  4]  0.0-10.0 sec  48.0 GBytes  41.2 Gbits/sec
[  4] Sent 3401 datagrams
```

Figure 25. Advanced Tools window (Bandwidth test tool)

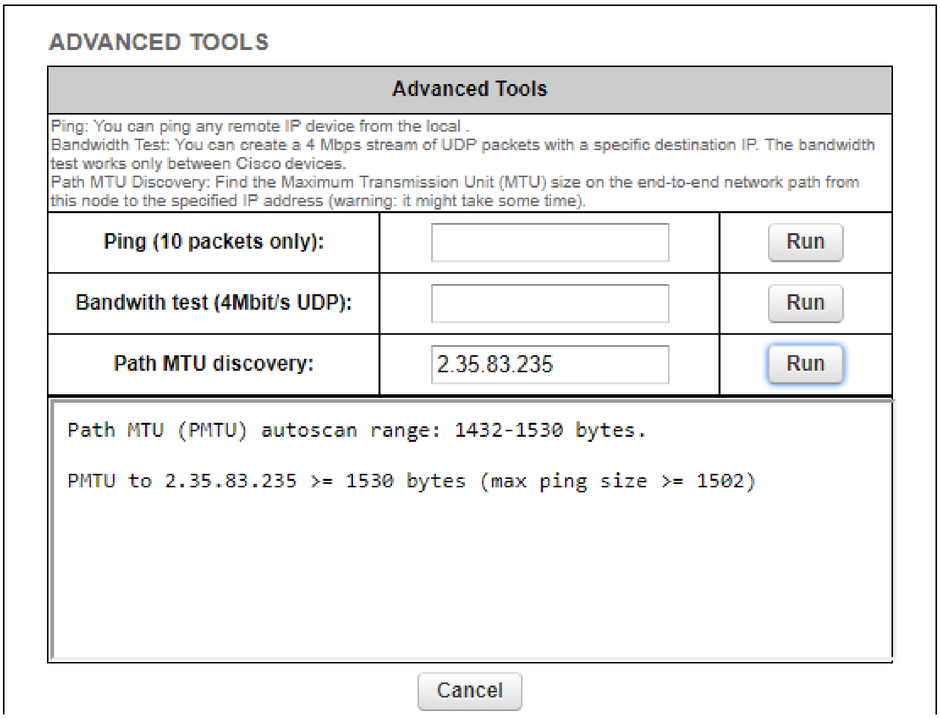
3. Click the **Run** button to the right of the IP address field.
    - The bandwidth test result will be shown below the test controls.

Using the Path MTU discovery tool

The Path MTU discovery tool tests the size of the maximum transmission unit (in other words, the largest protocol data unit that can be communicated in a single network layer transaction).

To use the Path MTU discovery tool, do the following steps:

1. Determine what wireless link is to be tested between the Cisco unit and another unit in the wireless network. Get theIP address of the other unit.
2. Enter the IP address of the second unit in the **Path MTU discovery** field (Figure 26 (page 72)).



ADVANCED TOOLS

Advanced Tools		
Ping: You can ping any remote IP device from the local . Bandwidth Test: You can create a 4 Mbps stream of UDP packets with a specific destination IP. The bandwidth test works only between Cisco devices. Path MTU Discovery: Find the Maximum Transmission Unit (MTU) size on the end-to-end network path from this node to the specified IP address (warning: it might take some time).		
Ping (10 packets only):		Run
Bandwith test (4Mbit/s UDP):		Run
Path MTU discovery:	2.35.83.235	Run

```
Path MTU (PMTU) autoscan range: 1432-1530 bytes.

PMTU to 2.35.83.235 >= 1530 bytes (max ping size >= 1502)
```

Figure 26. Advanced Tools window (Path MTU test tool)

3. Click the **Run** button to the right of the IP address field.
   - The Path MTU test result will be shown below the test controls.

7.6. Advanced settings

7.6.1. Ethernet settings

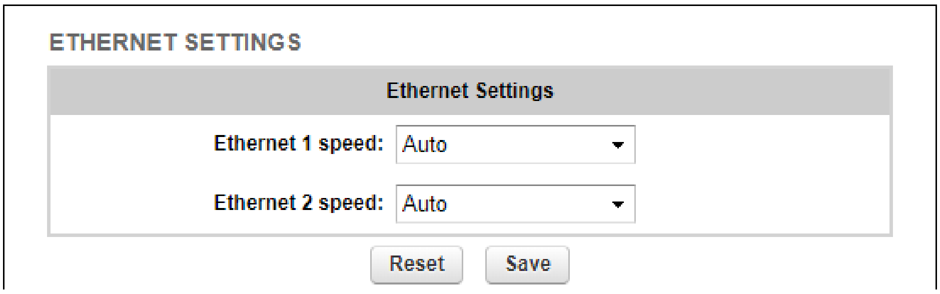
The Ethernet settings window contains controls to change the data exchange speeds of the unit's two RJ45 Ethernet ports.

IMPORTANT

By default, Ethernet speeds are set to Auto. It is strongly recommended that you do not change the Ethernet speed settings unless errors and/or unwanted behaviors are detected on the Ethernet connection.

To change the ethernet speed settings, click the **-ethernet settings** link under **ADVANCED SETTINGS** in the left-hand settings menu.

- The **Ethernet Settings** dialog will be shown (Figure 27 (page 73)).



ETHERNET SETTINGS

Ethernet Settings

Ethernet 1 speed: Auto

Ethernet 2 speed: Auto

Figure 27. Configurator GUI (Ethernet settings window)

To change the ethernet settings, do the following steps:

- To choose the correct data exchange speed for each Ethernet port, click one of the following data exchange speeds:
  - **Auto** (The data exchange speed for the selected port will be chosen automatically).
  - **10 Mbit half duplex**.
  - **10 Mbit full duplex**.
  - **100 Mbit half duplex**.
  - **100 Mbit full duplex**.

7.6.2. Static routes

The Static routes window is used to set static routing rules (in other words, manually-configured routing entries, as opposed to routing instructions from a dynamic routing table) for a Cisco unit.

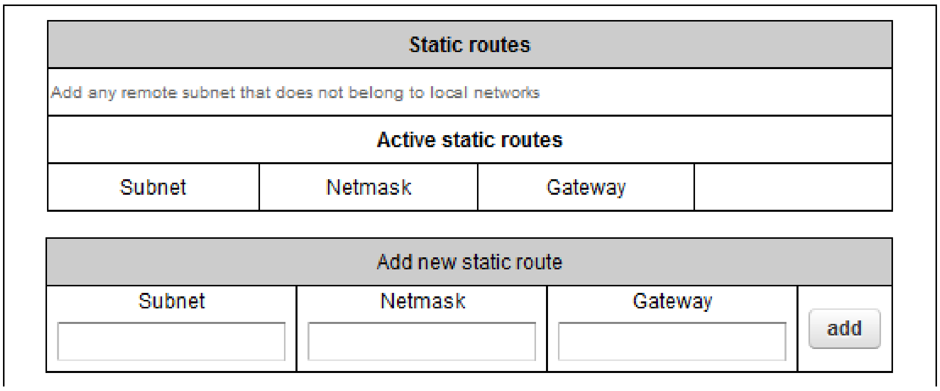
Static routes are typically used if there is a need to do any of the following in context of the network:

- Access a remote subnet that does not belong to a local network•

  Access other Cisco radio units or client devices across the local network
- Reach gateways (such as Internet gateways)
- Create networks that include 'fixed' devices (such as CCTV cameras)

To change the Static Routes settings, click the **-static routes** link under **ADVANCED SETTINGS** in the left-hand settings menu.

- The **Static Routes** dialog will be shown (Figure 28 (page 74)).



Static routes

Add any remote subnet that does not belong to local networks

Active static routes

Subnet	Netmask	Gateway	

Add new static route

Subnet	Netmask	Gateway	
			add

Figure 28. Configurator GUI (Static Routes window)

To enter a new static route, do the following steps:

1. Enter the **Subnet**, **Netmask** and **Gateway** designators in the correct fields of the **Add new static route** section.
2. Click the **add** button.
    - If the new static route is valid, it will be added to the **Active static routes** list.

7.6.3. Multicast

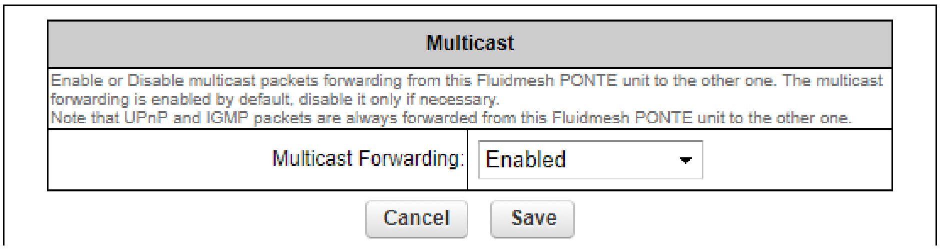
Multicast management for bridge network-capable devices

Multicast is a group-communication method in which data transmissions are addressed simultaneously to more than one destination computer.

Multicast traffic can only be forwarded *through* the local Cisco FM Ponte kit unit to the remote Cisco FM Ponte kit unit, and through the remote unit to the local unit.

To enable or disable multicast traffic forwarding on a Cisco FM Ponte kit unit, do the following steps:

1. Click the **-multicast** link under **ADVANCED SETTINGS** in the left-hand settings menu.
    - The **MULTICAST** dialog will be shown (Figure 29 (page 74)).



Multicast

Enable or Disable multicast packets forwarding from this Fluidmesh PONTE unit to the other one. The multicast forwarding is enabled by default, disable it only if necessary.
Note that UPnP and IGMP packets are always forwarded from this Fluidmesh PONTE unit to the other one.

Multicast Forwarding: Enabled

Figure 29. Multicast dialog

2. Click the **Multicast Forwarding** drop-down.
3. Click the **Enabled** option to enable multicast traffic forwarding, or click the **Disabled** option to disable forwarding

7.6.4. SNMP configuration

The SNMP window can be used to configure an SNMP v2c or SNMP v3 service to run on the Cisco FM Ponte kit.

Walk-throughs (no agent-to-manager notifications) and traps (agent-to-manager notifications enabled) are both supported. If SNMP traps are enabled, you can specify the server address to which monitoring information must be sent.

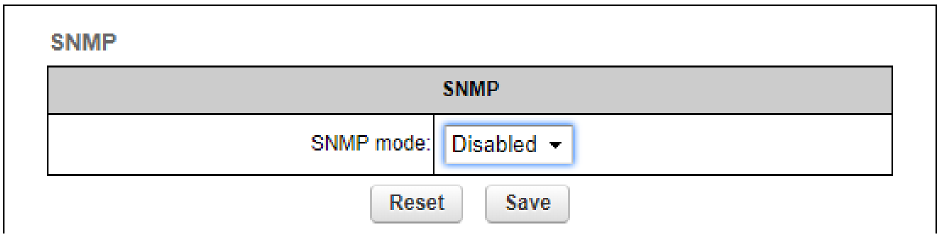
IMPORTANT

The same SNMP configuration must be set for all Cisco units in the wireless network.

For detailed information on Cisco unit SNMP configuration, refer to the *Cisco SNMP FM-MIB OID Table* and MIB configuration files. These can be downloaded from the Cisco Partner Portal (**Documentation** section > **User Manuals** > **Advanced Manuals**.)

To change the SNMP settings, do the following steps:

- Click the **-snmp** mode link under **ADVANCED SETTINGS** in the left-hand settings menu.
  - The default **SNMP** dialog will be shown (Figure 30 (page 75)).



SNMP

SNMP mode: Disabled

Figure 30. SNMP dialog (SNMP disabled)

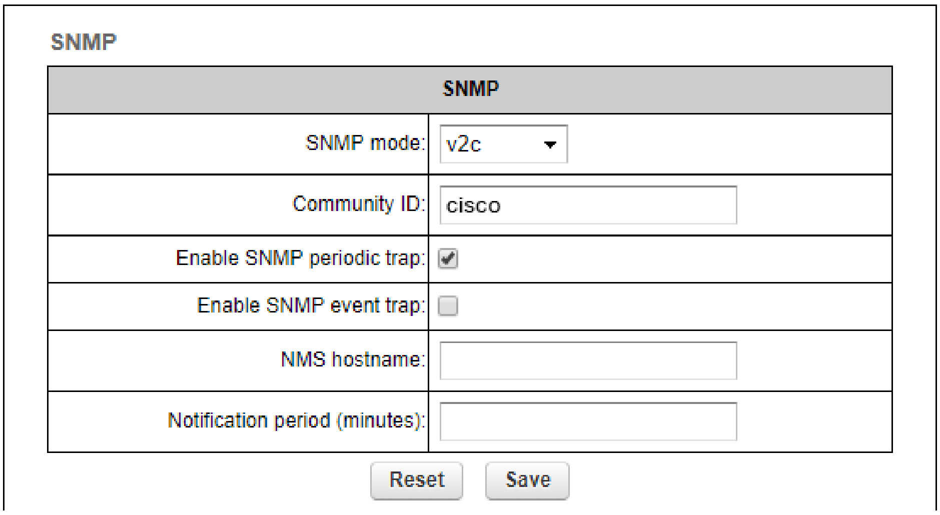
NOTE

By default, Cisco units are shipped from the factory with SNMP disabled.

Using SNMP v2c

To change the unit's SNMP mode to **v2c** and configure the unit accordingly, do the following steps:

1. Click the **SNMP mode** drop-down, and click the **v2c** option.
   - The **SNMP** v2c settings dialog will be shown (Figure 31 (page 76)).



SNMP

SNMP	
SNMP mode:	v2c ▾
Community ID:	cisco
Enable SNMP periodic trap:	☑
Enable SNMP event trap:	□
NMS hostname:	
Notification period (minutes):	

Figure 31. SNMP dialog (v2c selected)

2. Enter a community identity value in the **Community ID:** field.

> **IMPORTANT**
> The same community identity value must be set for all Cisco units in the wireless network.

3. SNMP traps can be enabled for significant system-related events. If needed, enable SNMP event traps by checking the **Enable SNMP event trap:** check-box, and enter the name of the network management station (NMS) host in the **NMS hostname:** field.

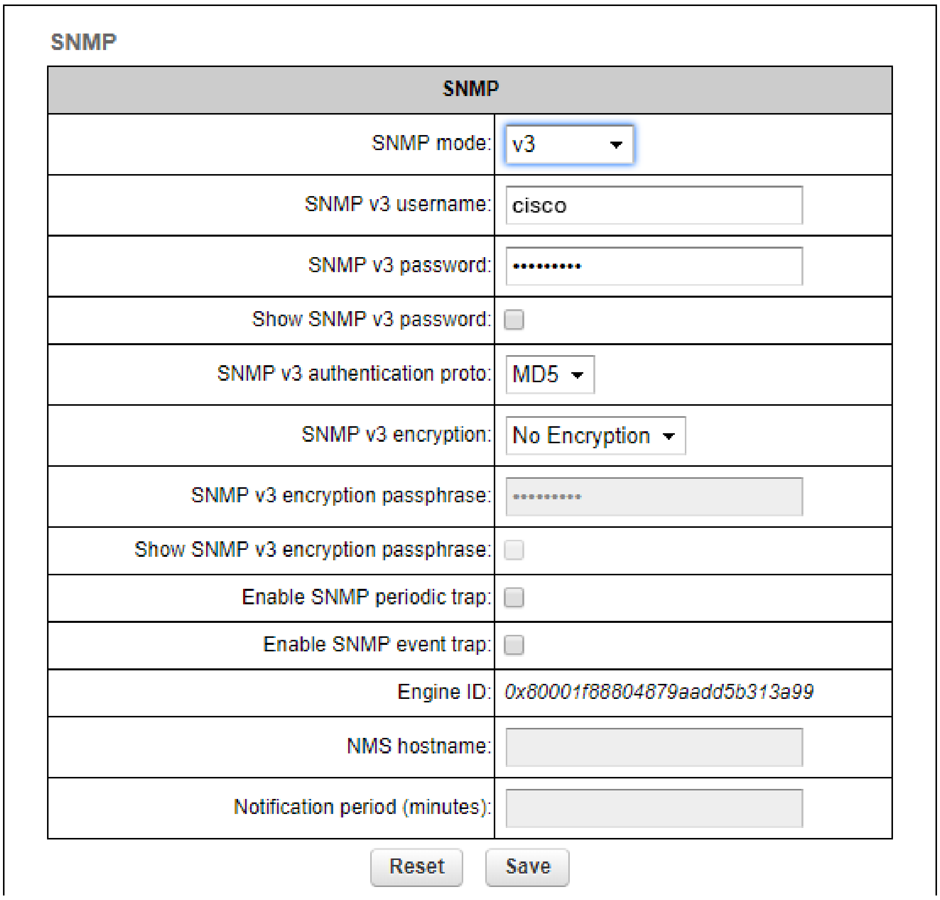
> **IMPORTANT**
> The NMS host to which traps are sent must have an SNMP agent that is configured to collect SNMP v2c traps.

4. You can also configure the unit to send SNMP traps at defined periodic intervals. If needed, enable periodic SNMP traps by checking the **Enable SNMP periodic trap:** check-box, and enter the name of the network management station (NMS) host in the **NMS hostname:** field.
5. Save the SNMP settings by clicking the **Save** button. Alternatively, clear the settings by clicking the **Reset** button.

Using SNMP v3

To change the unit's SNMP mode to **v3** and configure the unit accordingly, do the following steps:

1. Click the **SNMP mode** drop-down, and click the **v3** option.
   - The **SNMP** v3 settings dialog will be shown (Figure 32 (page 77)).



SNMP

SNMP	
SNMP mode:	v3 ▾
SNMP v3 username:	cisco
SNMP v3 password:	•••••••••
Show SNMP v3 password:	□
SNMP v3 authentication proto:	MD5 ▾
SNMP v3 encryption:	No Encryption ▾
SNMP v3 encryption passphrase:	•••••••••
Show SNMP v3 encryption passphrase:	□
Enable SNMP periodic trap:	□
Enable SNMP event trap:	□
Engine ID:	*0x80001f88804879aadd5b313a99*
NMS hostname:	
Notification period (minutes):	

Figure 32. SNMP dialog (v3 selected)

2. Enter an SNMP v3 user name in the **SNMP v3 username:** field.

IMPORTANT

The same SNMP v3 user name must be set for all Cisco units in the wireless network.

3. To change the current SNMP v3 password, enter a new password in the **SNMP v3 password:** field. The default password is ***cisco***. To show the password as it is being typed, checkthe **Show SNMP v3 password:** check-box.

4. Choose the correct authentication protocol from the **SNMP v3 authentication proto:** drop-down. The available options are **MD5** and **SHA**.

> **IMPORTANT**
>
> The same SNMP authentication protocol must be set for all Cisco units in the wireless network.

5. If needed, choose the correct encryption protocol from the **SNMP v3 encryption:** drop-down. The available options are **No Encryption**, **DES** (Data Encryption Standard) and **AES** (Advanced Encryption Standard).

> **IMPORTANT**
>
> The same encryption protocol must be set for all Cisco units in the wireless network.

6. To change the current encryption passphrase, enter a new passphrase in the **SNMP v3 encryption passphrase:** field. The default encryption passphrase is ***cisco***. To show the passphrase as it is being typed, check the **Show SNMP v3 encryption passphrase:** check-box.
7. SNMP traps can be enabled for significant system-related events. If needed, enable SNMP event traps by checking the **Enable SNMP event trap:** check-box, and enter the name of the network management station (NMS) host in the **NMS hostname:** field.

> **IMPORTANT**
>
> The NMS host to which traps are sent must have an SNMP agent configured to collect v2c traps.

8. You can also configure the unit to send SNMP traps at defined periodic intervals. If needed, enable periodic SNMP traps by checking the **Enable SNMP periodic trap:** check-box, and enter the name of the network management station (NMS) host in the **NMS hostname:** field.
9. Save the SNMP settings by clicking the **Save** button. Alternatively, clear the settings by clicking the **Reset** button.

7.6.5. VLAN settings

VLAN configuration

The **VLAN SETTINGS** window contains controls to connect the Cisco FM Ponte kit to one or more virtual local area networks (VLANs) that are part of the local wireless network.

IMPORTANT

The VLAN feature must be enabled using a software plug-in (Cisco part number *FM-VLAN*). Contact your Cisco Networks representative for details.

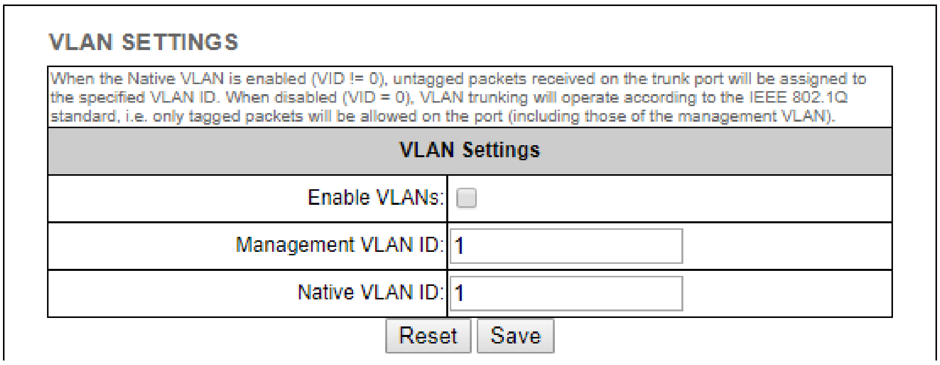
The Cisco FM Ponte kit features smart self-management of integration with connected VLANs, with minimal configuration time and avoidance of potential configuration errors. This is done by A) relying on the data-processing configuration of a connected network switch, and B) obeying predefined rules for management of incoming and outgoing data packets.

IMPORTANT

For detailed information on the predefined rules for packet management, refer to the "Rules for packet management" (page 80) table at the bottom of this section.

To connect the unit to a VLAN that is part of the local wireless network, do the following steps:

1. Click the **-vlan** settings link under **ADVANCED SETTINGS** in the left-hand settings menu.
   - The **VLAN SETTINGS** dialog will be shown (Figure 33 (page 79)).



VLAN SETTINGS

When the Native VLAN is enabled (VID != 0), untagged packets received on the trunk port will be assigned to the specified VLAN ID. When disabled (VID = 0), VLAN trunking will operate according to the IEEE 802.1Q standard, i.e. only tagged packets will be allowed on the port (including those of the management VLAN).

VLAN Settings	
Enable VLANs:	□
Management VLAN ID:	1
Native VLAN ID:	1

Figure 33. Configurator GUI (VLAN SETTINGS dialog)

2. Connect the unit to a VLAN that is part of the local wireless network by checking the **ENABLE VLANs:** check-box.
3. Enter the management identification number of the VLAN (used to communicate with the device's operating system) in the **Management VLAN ID:** field.

> **NOTE**
>
> The same Management VLAN ID number must be used on all Cisco FM Ponte kit devices that are part of the same bridge network.

4. Enter the native identification number (the VLAN ID implicitly assigned to untagged packets received on trunk ports) in the **Native VLAN ID:** field.
5. Save the VLAN settings by clicking the **Save** button. Alternatively, clear the settings by clicking the **Reset** button.

Rules for packet management

Parameter	Default value
Default VLAN configuration The factory-set VLAN parameters for the unit are as follows:	
Management VLAN ID (MVID)	1
Native VLAN ID (NVID)	1
Native VLAN processing	Enabled
Port mode (all Ethernet ports)	Smart
Traffic classes The system classifies incoming data packets according to the following definitions:	
Signaling	Ethernet protocol type $8847 or $09xx
User	All other traffic
Packet tagged with MVID	Packet passed
Access port rules for incoming packets (Case and Action)	
Untagged packet from Cisco device	Packet passed
Untagged packet, VID not configured	Packet passed
Untagged packet, VID configured	Packet tagged with specified VID
Tagged packet with valid VID	Packet dropped
Tagged packet with null (0) VID	Packet dropped
Access port rules for outgoing packets (Case and Action)	
Tagged packet with configured and allowed VID	Packet passed
Packet from Cisco device	Packet passed
Tagged packet, port VID not configured	Packet passed
Tagged packet with valid but disallowed VID	Packet dropped
Tagged packet with null (0) VID	Packet dropped
Access port rules for incoming packets with unit in Smart Mode (Case and Action)	

Parameter	Default value
Untagged packet	If native VLAN = ON: Packet passed (tagged with NVID) If native VLAN = OFF: Packet dropped
Tagged packet (any VID, no checks)	Packet passed with original tag
Access port rules for outgoing packets with unit in Smart Mode (Case and Action)	
Packets originating from Cisco devices (for example: FM Racer interface)	Packet implicitly tagged with MVID, next rules apply
Signalling traffic	Packet implicitly tagged with MVID, next rules apply
Tagged with valid VID (1 – 4095), not NVID	Packet passed (tagged)
Tagged with null VID (0) or NVID	Packet passed (untagged)
Access port rules for incoming packets with unit in Bridge Mode (Case and Action) The Native VLAN enable setting is used to control whether the *Management VLAN* should be tagged or not.	
Untagged packet, to remote devices	Pass packet to remote peer
Tagged packet (any VID), to remote devices	Pass packet to remote peer with original tag
Untagged packet, to local unit kernel	If native VLAN = ON: Packet passed to kernel, tagged with NVID If native VLAN = OFF: Packet not passed to kernel
Tagged packet (any VID), to local unit kernel	If native VLAN = ON: Packet not passed to kernel If native VLAN = OFF: Packet passed to kernel if VID = NVID
Access port rules for outgoing packets with unit in Bridge Mode (Case and Action)	
Tagged packet with valid VID from remote peer	Packet passed (tagged)
Tagged packet with null (0) VID from remote peer	Packet passed (untagged)
Packet from local unit kernel	If native VLAN not equal to MVID: Packet passed, tagged with MVID If native VLAN = MVID: Packet passed, untagged

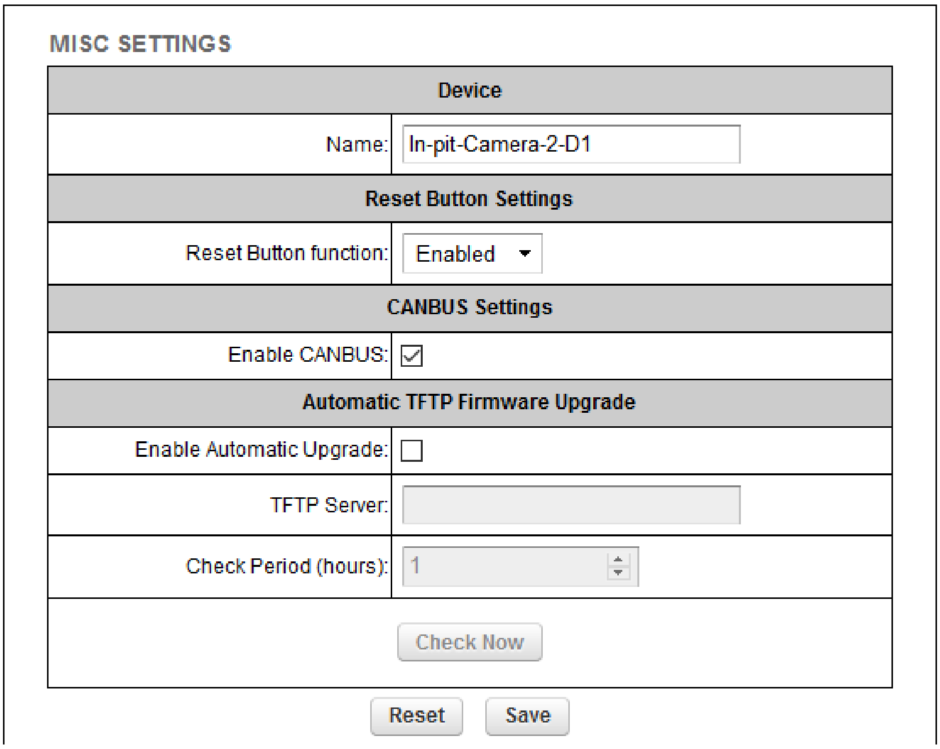
7.6.6. Miscellaneous settings

The **MISC SETTINGS** window contains controls to change the following settings:

- The device name, as used to identify the Cisco FM Ponte kit within the FMQuadro network map and to other Cisco utilities.
- The operation of the physical Reset button on the unit.

To change any of the miscellaneous settings, do the following steps:

1. Click the **-misc settings** link under **ADVANCED SETTINGS** in the left-hand settings menu.
    - The **MISC SETTINGS** dialog will be shown (Figure 34 (page 82)).



MISC SETTINGS

Device	
Name:	In-pit-Camera-2-D1
Reset Button Settings	
Reset Button function:	Enabled
CANBUS Settings	
Enable CANBUS:	☑
Automatic TFTP Firmware Upgrade	
Enable Automatic Upgrade:	□
TFTP Server:	
Check Period (hours):	1

Figure 34. Configurator GUI (MISC SETTINGS dialog)

2. Set the device name by typing it in the **Name:** field.

NOTE

It is not essential to specify the device name, but it is strongly recommended. Failure to specify the device name may make the unit difficult to recognize in situations where more than one unit is being dealt with at the same time (for example, when using utilities such as the FMQuadro network map).

3. Set the functionality of the unit's hardware **Reset** button by clicking the **Reset Button function:** drop-down and clicking the needed option as described below:
    - **Disabled:** The hardware **Reset** button will be disabled.

NOTE

If the **Disabled** option is chosen, you can still reboot or do a hard reset of the unit using the Configurator GUI. See "Resetting the unit to factory defaults" (page 98) for more information.

- **Enabled:** The hardware **Reset** button will be enabled.
- **Factory:** The hardware **Reset** button functionality will be set to its factory default configuration (enabled).

4. To enable CANBUS support for the unit, make sure the FM-CANBUS plug-in is installed, then check the **Enable CANBUS:** check-box.
5. Save the miscellaneous settings by clicking the **Save** button. Alternatively, clear the settings by clicking the **Reset** button.

7.7. Management settings

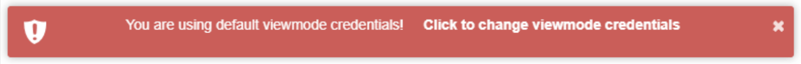
7.7.1. View Mode settings

The View Mode window allows the system administrator to grant and prohibit access to device configuration settings by category.

IMPORTANT

Changing the default password to a strong password is an extremely important step in preventing security breaches.

If you have logged into the configurator interface using default login credentials, you will see a notification banner at the bottom of the screen (Figure 35 (page 83)).



You are using default viewmode credentials! **Click to change viewmode credentials**

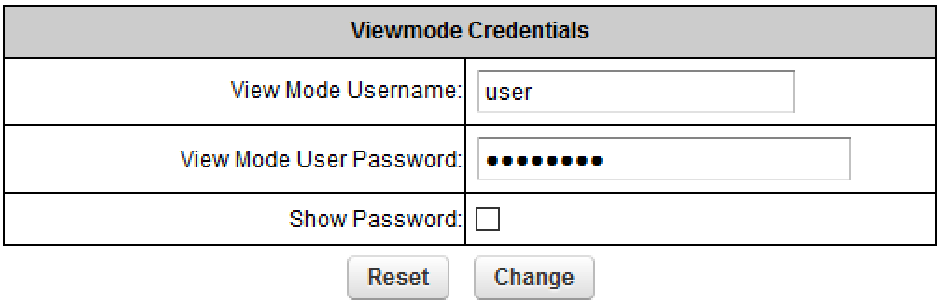
Figure 35. Default credentials notification banner

Click the banner to change the view mode credentials. You will be taken to the **VIEW MODE SETTINGS** section.

To gain editing privileges for the View Mode settings window requires the correct administrator user name and password. To change the administrator user name and password for the current user, do the following steps:

1. Click the **-view mode settings** link under **MANAGEMENT SETTINGS** in the left-hand settings menu. **VIEW MODE SETTINGS**

- The **Viewmode Credentials** section will be shown (Figure 36 (page 84)).



Viewmode Credentials

View Mode Username:	user
View Mode User Password:	●●●●●●●●●
Show Password:	□

Figure 36. VIEW MODE SETTINGS dialog (Viewmode Credentials section)

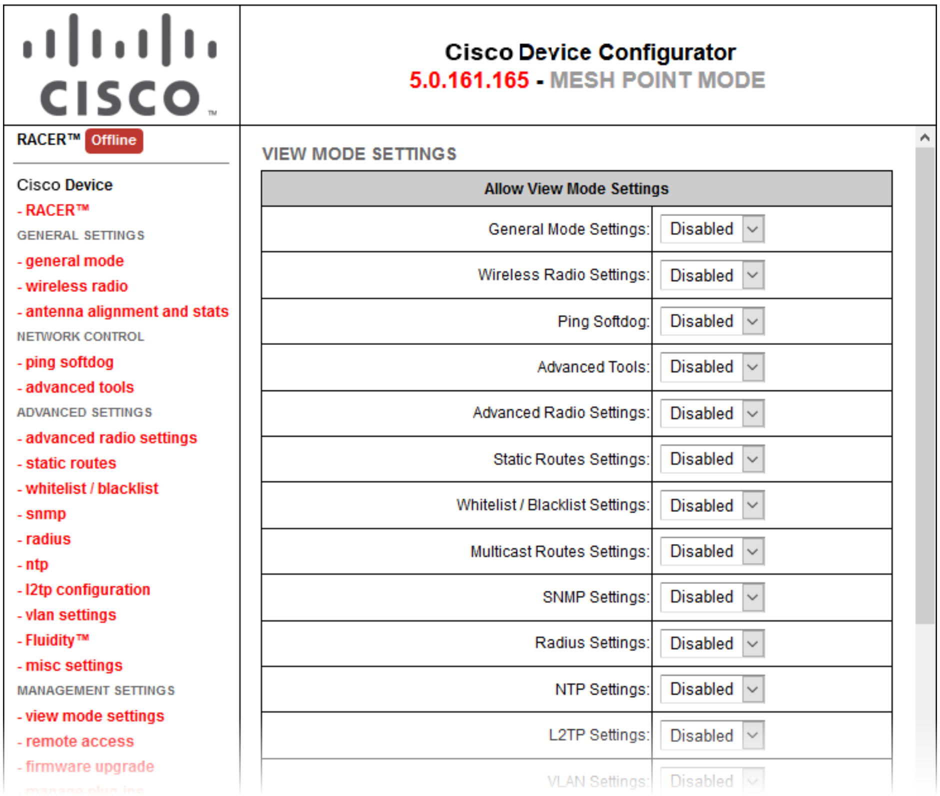
2. Enter the new user name in the **View Mode Username:** field.
3. The default password is *viewmode*. Enter the new password in the **View Mode User Password:** field.

> **NOTE**
> The new password must be a minimum of eight characters, and include at least one capital letter and one number.

4. To show the password as it is being typed, check the **Show Password** check-box.
5. Save the Viewmode Credentials settings by clicking the **Change** button. Alternatively, clear the settings by clicking the **Reset** button.

To change the View Mode settings, do the following steps:

1. Log in to the unit's Configurator GUI with Administrator credentials. See “Accessing the Cisco FM Ponte kit for device configuration” (page 37) for more information.
2. Click the **-view mode settings** link under **MANAGEMENT SETTINGS** in the left-hand settings menu (Figure 37 (page 85)).



Allow View Mode Settings	
General Mode Settings:	Disabled
Wireless Radio Settings:	Disabled
Ping Softdog:	Disabled
Advanced Tools:	Disabled
Advanced Radio Settings:	Disabled
Static Routes Settings:	Disabled
Whitelist / Blacklist Settings:	Disabled
Multicast Routes Settings:	Disabled
SNMP Settings:	Disabled
Radius Settings:	Disabled
NTP Settings:	Disabled
L2TP Settings:	Disabled
VLAN Settings:	Disabled

Figure 37. Configurator GUI (VIEW MODE SETTINGS dialog)

- The **VIEW MODE SETTINGS** dialog will be shown.

3. To allow or prohibit access to any device-configuration settings, click the relevant drop-down, and click the **Disabled** or **Enabled** setting:
   - If the **Disabled** option is selected for a device-configuration setting, the setting for that category will be visible but not accessible to ordinary users.
   - If the **Enabled** option is selected for a device-configuration setting, the setting can be modified by ordinary users.

IMPORTANT

If you are logged in to the Configurator interface with Administrator credentials, you can enable or disable any device-configuration setting.

If you are logged in to the Configurator interface as an ordinary user, you will be able to view the device-configuration settings, but cannot change the settings.

4. Save the view mode settings by clicking the **Save** button in the **Allow View Mode Settings** section. Alternatively, clear the settings by clicking the **Reset** button.

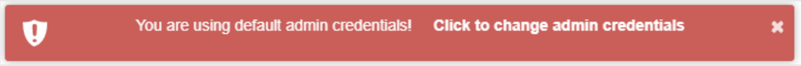
7.7.2. Changing the Administrator username and password

The **CHANGE USERNAME AND PASSWORD** section contains controls to change the Administrator's user name and password for the Cisco unit.

IMPORTANT

Changing the default password to a strong password is an extremely important step in preventing security breaches.

If you have logged into the configurator interface using default administrator's credentials, you will see a notification banner at the bottom of the screen (Figure 38 (page 86)).



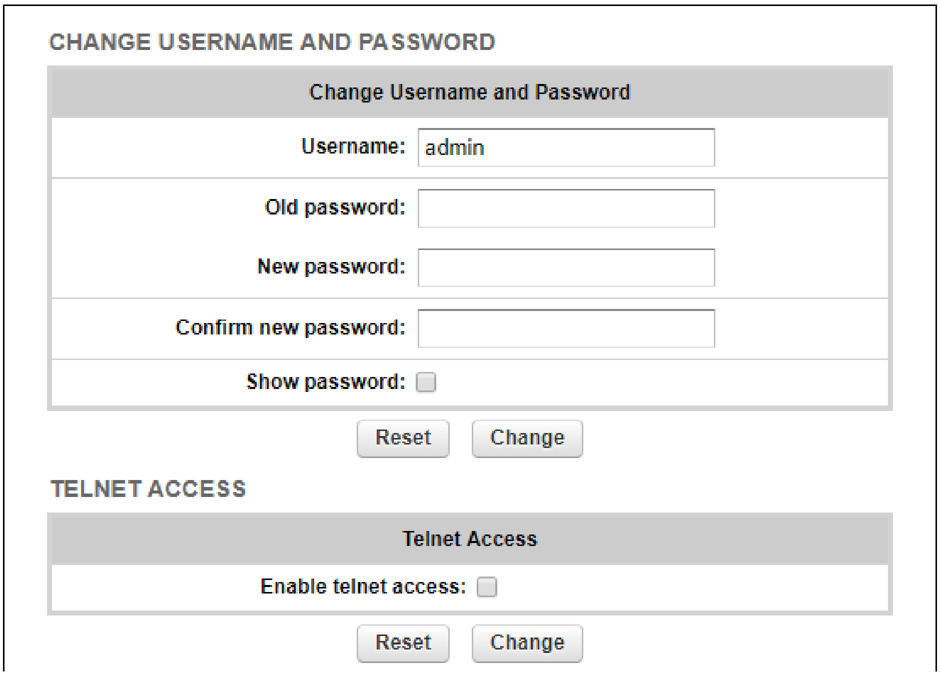
You are using default admin credentials! **Click to change admin credentials**

Figure 38. Default admin credentials notification banner

Click the banner to change the admin credentials. You will be taken to the **CHANGE USERNAME AND PASSWORD** section.

To change the Administrator's user name and password for the unit, do the following steps:

1. Click the **-remote access** link under **MANAGEMENT SETTINGS** in the left-hand settings menu.
   - The **CHANGE USERNAME AND PASSWORD** dialog will be shown (Figure 39 (page 87)).



CHANGE USERNAME AND PASSWORD

Change Username and Password

Username: admin

Old password:

New password:

Confirm new password:

Show password: □

TELNET ACCESS

Telnet Access

Enable telnet access: □

Figure 39. Management Settings dialog (Change Username and Password)

2. Enter the new administrator user name in the **Username:** field.
3. Enter the current password in the **Old password:** field.
4. Enter the new password in the **New password:** field.
5. Confirm that the new password is correctly spelled by checking the **Show Password:** check-box to show the text of the password, then re-entering the password in the **Confirm New password:** field.
6. Save the changed password settings by clicking the **Change** button. Alternatively, revert to the old password settings by clicking the **Reset** button.

> **IMPORTANT**
>
> Keep the Administrator name and password in a safe place. If the Administrator name and password are lost, the only way to log in to the unit is to do a hard reset.
>
> If you need to do a hard reset, refer to "Resetting the unit to factory defaults" (page 98) for more information.

Enabling remote access to the unit by Telnet

The **TELNET ACCESS** section contains controls to enable remote access to the unit using Telnet.

IMPORTANT

The Telnet protocol suffers from serious security weaknesses that limit its usefulness in environments where the network cannot be fully trusted.

Telnet is used at your own risk.

To enable Telnet access to the unit, do the following steps:

1. Click the **-remote access** link under **MANAGEMENT SETTINGS** in the left-hand settings menu.
    - The **TELNET ACCESS** dialog will be shown (see Figure 39 (page 87) in the previous section).
2. Enable Telnet access by checking the **Enable telnet access:** check-box.
3. Save the changed Telnet settings by clicking the **Change** button. Alternatively, revert to the old password settings by clicking the **Reset** button.

7.7.3. Overwriting and upgrading the unit firmware

The **FIRMWARE UPGRADE** window contains controls to overwrite the device firmware of the Cisco FM Ponte kit, or upgrade the firmware to the latest available version.

CAUTION

Overwriting the firmware of any electronic device must be done with great care, and always contains an element of risk.

It is not advisable to overwrite the firmware on a functioning Cisco unit unless a specific firmware-related issue needsto be resolved.

IMPORTANT

To access firmware image files, you need an approved Cisco extranet account. To create an extranet account, register for free at the Cisco Partner Portal.

To download the needed firmware image file to your computer, do the following steps:

1. Navigate to the Documentation section of the Cisco Partner Portal.
2. Find and open the device sub-folder for your specific Cisco device in the **FIRMWARE AND TOOLS** folder.
3. Download the firmware image (*.BIN) file to your computer.

CAUTION

Make sure that you download the specific *.BIN file for your device type. Uploading incorrect firmware for the device type will cause the firmware overwrite to fail, and may damage the unit.

The following procedure describes how to overwrite the existing firmware on a Cisco device. This procedure assumes that the wireless networkis currently active.

To overwrite the existing firmware on the Cisco device, do the following steps:

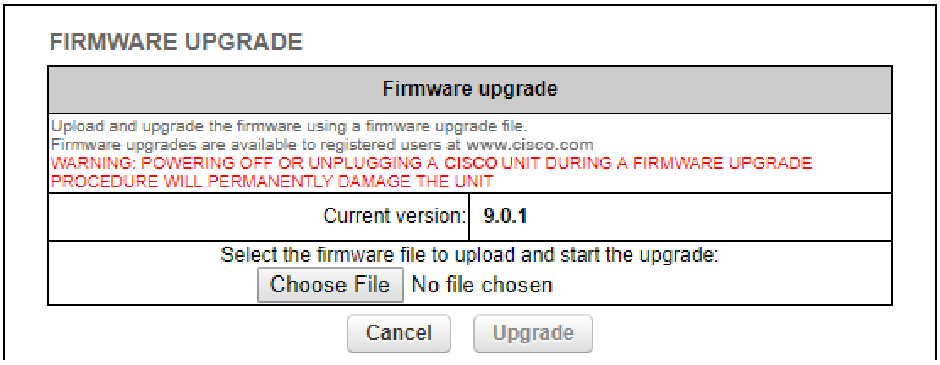
1. Power OFF all Cisco devices connected to the wireless network.
2. Disconnect all Ethernet cables from the Cisco device.
3. With the Cisco device disconnected from the wireless network, power ON the device.

CAUTION

Do not restart or power OFF the device while firmware overwriting is in progress.

Restarting or powering OFF the unit before overwriting is complete will permanently damage the unit.

4. Connect the computer containing the firmware image file directly to the Cisco unit, using an Ethernet cable. For detailed information on direct connection, refer to "Accessing the Cisco FM Ponte kit for device configuration" (page 37).
5. As a precaution, save the unit's existing device configuration file to the computer. For detailed information on how to save the existing configuration file, refer to "Saving and restoring the unit settings" (page 96).
6. Click the **-firmware upgrade** link under **MANAGEMENT SETTINGS** in the left-hand settings menu.
   - The **FIRMWARE UPGRADE** dialog will be shown (Figure 40 (page 90)).



FIRMWARE UPGRADE

Firmware upgrade	
Upload and upgrade the firmware using a firmware upgrade file. Firmware upgrades are available to registered users at www.cisco.com WARNING: POWERING OFF OR UNPLUGGING A CISCO UNIT DURING A FIRMWARE UPGRADE PROCEDURE WILL PERMANENTLY DAMAGE THE UNIT	
Current version:	9.0.1
Select the firmware file to upload and start the upgrade: Choose File No file chosen	

Figure 40. Configurator GUI (typical FIRMWARE UPGRADE dialog)

7. Upload the firmware image file to the unit by clicking the **Choose File** button and following the software prompts.
   - The **Upgrade** button will become available.
8. Click the **Upgrade** button. Follow the software prompts until the firmware overwrite is complete.
   - When the overwrite is complete, the unit will automatically reboot.

If the previous firmware was overwritten with a newer version of firmware, check that the firmware upgraded correctly by doing the following steps:

- When the overwrite is complete, make sure that the upgraded firmware has a greater version number than the firmware that was previously installed.
  - If the firmware version has not changed, the firmware upgrade has failed. Repeat the overwrite from step Step 1 above.

7.7.4. Plug-In management

IMPORTANT

For a complete list of software plug-ins that are currently available for the Cisco FM Ponte kit, refer to "Available plug-ins" (page 101).

The MANAGE PLUG-INS page shows which software plug-ins are currently active on the unit, and contains controls that allow you to do the following functions:

- Upload activation codes that allow the unit's accessory software plug-ins to function.
- Activate uploaded software plug-ins for use with the unit.
- Deactivate uploaded software plug-ins so they can be used on other Cisco units.

- Activate a non-repeatable Demo mode that allows full 4.9 GHz, AES and unlimited plug-in functionality for an 8-hour trial period.

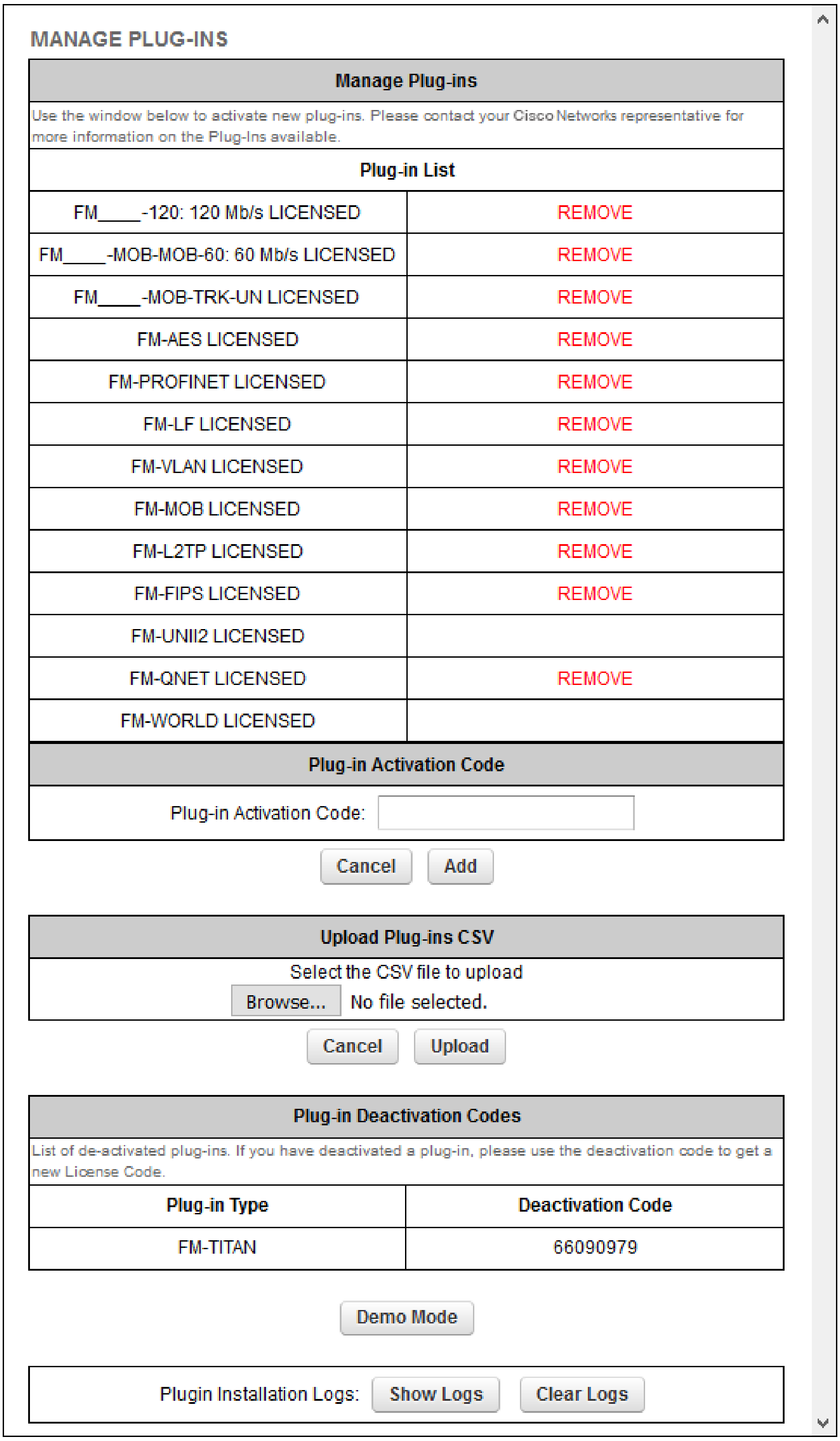
  NOTE

  4.9 GHz functionality is not available for the Cisco FM Ponte kit.

- Show and erase the log files for plug-in installation.

To open the **MANAGE PLUG-INS** dialog, do the following steps:

- Click the **-manage plug-ins** link under **MANAGEMENT SETTINGS** in the left-hand settings menu.
  - The **MANAGE PLUG-INS** dialog will be shown (Figure 41 (page 92)).



MANAGE PLUG-INS

Manage Plug-ins

Use the window below to activate new plug-ins. Please contact your Cisco Networks representative for more information on the Plug-Ins available.

Plug-in List

FM____-120: 120 Mb/s LICENSED	REMOVE
FM____-MOB-MOB-60: 60 Mb/s LICENSED	REMOVE
FM____-MOB-TRK-UN LICENSED	REMOVE
FM-AES LICENSED	REMOVE
FM-PROFINET LICENSED	REMOVE
FM-LF LICENSED	REMOVE
FM-VLAN LICENSED	REMOVE
FM-MOB LICENSED	REMOVE
FM-L2TP LICENSED	REMOVE
FM-FIPS LICENSED	REMOVE
FM-UNII2 LICENSED	
FM-QNET LICENSED	REMOVE
FM-WORLD LICENSED	

Plug-in Activation Code

Plug-in Activation Code:

Upload Plug-ins CSV

Select the CSV file to upload

No file selected.

Plug-in Deactivation Codes

List of de-activated plug-ins. If you have deactivated a plug-in, please use the deactivation code to get a new License Code.

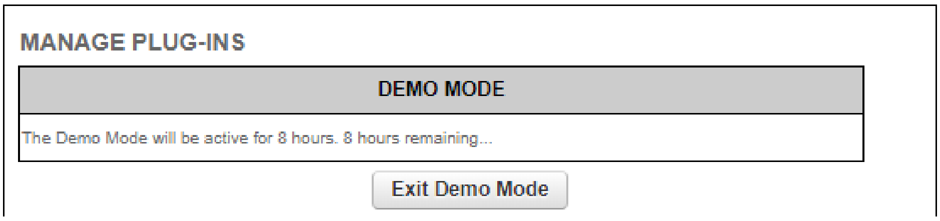
Plug-in Type	Deactivation Code
FM-TITAN	66090979

Plugin Installation Logs:

Figure 41. Configurator GUI (typical MANAGE PLUG-INS dialog)

To activate Plug-in Demo mode, do the following steps:

1. Click the **Demo Mode** button at the bottom of the **MANAGE PLUG-INS** dialog.
   - The **Demo Mode** activation dialog will be shown (Figure 42 (page 93)). A countdown timer shows how much Demo time remains.



MANAGE PLUG-INS

DEMO MODE

The Demo Mode will be active for 8 hours. 8 hours remaining...

Figure 42. MANAGE PLUG-INS dialog (Demo Mode activated)

2. To leave Demo mode before expiry of the 8-hour trial period, click the **Exit Demo Mode** button.
   - Demo mode will be deactivated, and the unit will reboot.
3. If the 8-hour Demo mode limit is reached, the unit will reboot and Demo mode will not be accessible again.

To upload one or more plug-in activation codes, refer to “Plug-in management procedures” (page 105).

To assign a software plug-in on the Partner Portal to the unit, do the following steps:

1. Enter the activation code for the plug-in in the **Plug-in Activation Code:** field.
2. Click the **Add** button.
   - The plug-in will be activated, and the plug-in functionality can be used.
   - A **REMOVE** link will be shown in red to the right of the relevant plug-in description in the **Plug-in List**.

To deactivate an uploaded software plug-in for use with another Cisco unit, refer to “Plug-in management procedures” (page 105).

To show and erase the plug-in installation log files, do the following steps:

1. Click the **Show Logs** button in the **Plug-in Installation Logs:** section.
   - The log files for plug-in installation will be shown in the **Plug-in Installation Logs**: section.
2. If needed, erase the log files for plug-in installation by clicking the **Clear Logs** button in the **Plug-in Installation Logs:** section.

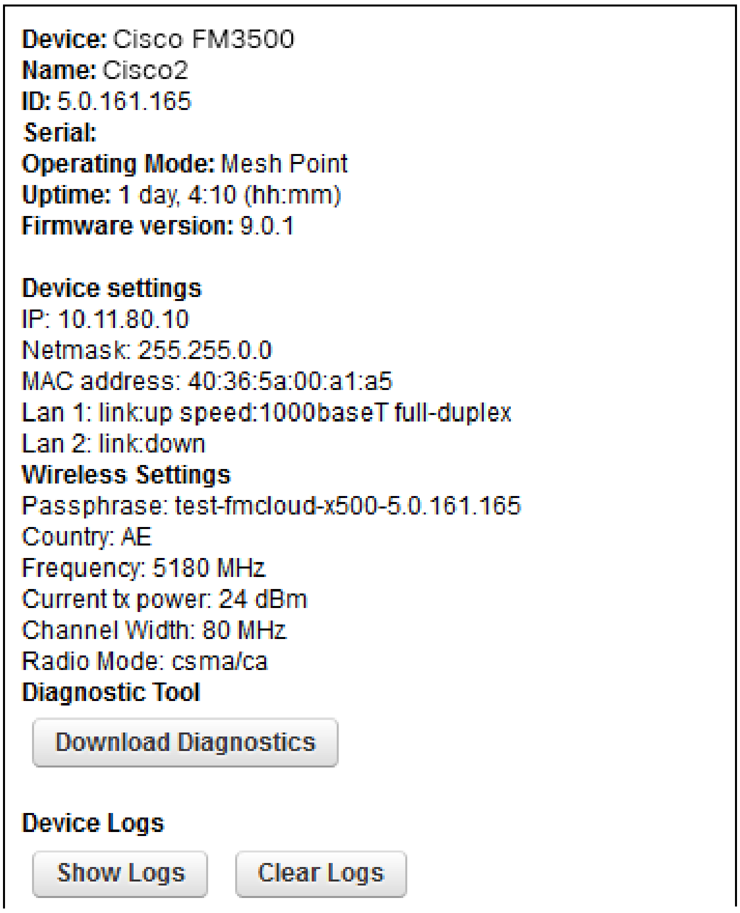
7.7.5. The device status view

The device status window

The device status window contains information on basic Cisco device settings (including the unit's MAC address), and controls that allow you to download diagnostic data files and view device-event logs.

To use the status window, do the following steps:

- Click the **-status** link under **MANAGEMENT SETTINGS** in the left-hand settings menu.
    - The status dialog will be shown (below).

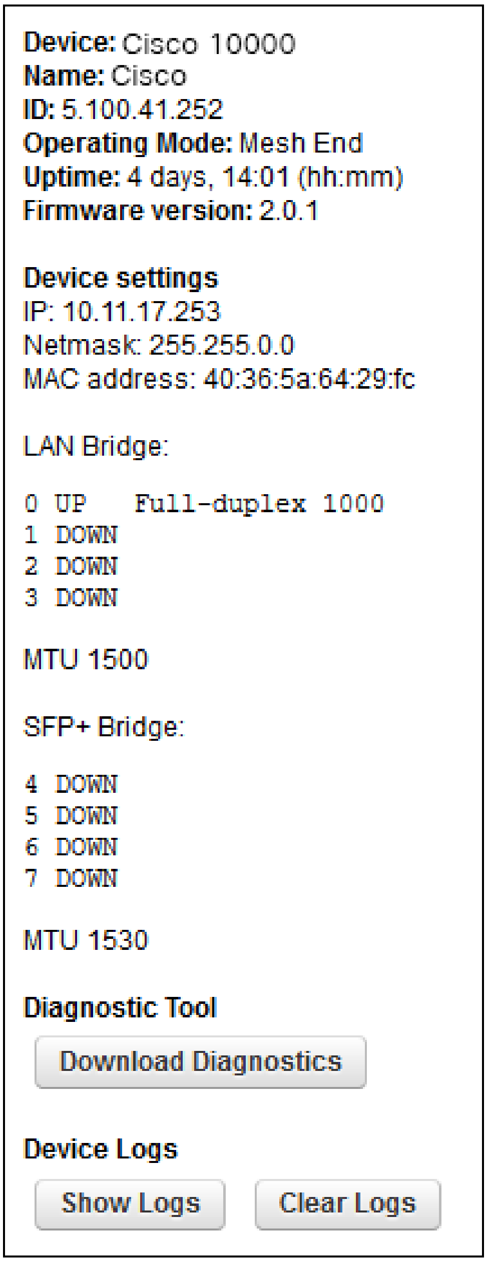


Device: Cisco FM3500
Name: Cisco2
ID: 5.0.161.165
Serial:
Operating Mode: Mesh Point
Uptime: 1 day, 4:10 (hh:mm)
Firmware version: 9.0.1

Device settings
IP: 10.11.80.10
Netmask: 255.255.0.0
MAC address: 40:36:5a:00:a1:a5
Lan 1: link:up speed:1000baseT full-duplex
Lan 2: link:down
Wireless Settings
Passphrase: test-fmcloud-x500-5.0.161.165
Country: AE
Frequency: 5180 MHz
Current tx power: 24 dBm
Channel Width: 80 MHz
Radio Mode: csma/ca
Diagnostic Tool

Device Logs

Figure 43. Configurator GUI (typical Status dialog)



Device: Cisco 10000
Name: Cisco
ID: 5.100.41.252
Operating Mode: Mesh End
Uptime: 4 days, 14:01 (hh:mm)
Firmware version: 2.0.1

Device settings
IP: 10.11.17.253
Netmask: 255.255.0.0
MAC address: 40:36:5a:64:29:fc

LAN Bridge:

```
0  UP    Full-duplex 1000
1  DOWN
2  DOWN
3  DOWN
```

MTU 1500

SFP+ Bridge:

```
4  DOWN
5  DOWN
6  DOWN
7  DOWN
```

MTU 1530

Diagnostic Tool

Device Logs

Figure 44. Typical Status dialog (second-generation FM1000 gateway gateway)

- Status information on the unit's basic characteristics, device settings and wireless settings is shown in the upper part of the window.

To download and forward the current diagnostic file for the unit, do the following steps:

1. Click the **Download Diagnostics** button.
2. Follow the software prompts to download the *.FM diagnostic file to your computer.

3. Log a support call with the Cisco Help desk. Ask for a reference number.
4. Attach the *.FM diagnostic file to an E-mail, and enter the support call reference number in the subject line of the E-mail. Send the mail to support@cisco.com.

> **IMPORTANT**
>
> Do not forward diagnostic files unless the Cisco Help desk requests them. If diagnostic files arrive when they have not been requested, they cannot be traced to specific problems.

To show the current device log for the unit, click the **Show Logs** button.

- The current device log will be shown in the Device Logs window above the **Show Logs** button.
- The status messages shown in the log relate to possible Ethernet port flapping, and will also alert you if duplicate IP addresses are present in the LAN. Refer to the text below for a description of the log messages.

> **NOTE**
>
> Ethernet port flapping is an issue in which the Ethernet port goes offline and comes back online at an excessively high rate within a given time period.
>
> Some possible causes of this problem may be auto-negotiation issues, chipset incompatibility, or faulty CAT5/6 cabling.

Some status messages that may be shown in the log have the following meanings:

- *ethX phy:X is up/down:* Ethernet port X is currently online/offline.
- *chatter: VBR: duplicate IP A? MACX --> MAXY at &lt;timestamp>:* Possible duplicate IP address 'A' has migrated from MAC address 'X' to MAC address 'Y', at the time shown.

7.7.6. Saving and restoring the unit settings

> **IMPORTANT**
>
> Device software configuration (*.CONF) files are not interchangeable with FM Racer configuration setup (*.FMCONF) files.

The **LOAD OR RESTORE SETTINGS** window contains controls that allow you to:

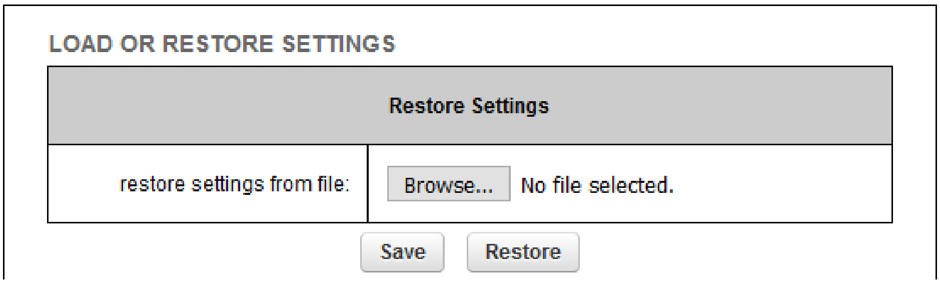
- Save the unit's existing software configuration as a configuration (*.CONF) file.

- Upload and apply a saved configuration file to the current unit.

> **TIP**
>
> Saved configuration files can be copied and distributed for use on more than one Cisco unit of the same type, simplifying the configuration of other deployed units.
>
> Saved configuration files can also be used for configuration backup. This can greatly speed up re-deployment if a damaged unit must be replaced with a unit of the same type.

To download the unit's existing configuration settings to your computer, do the following steps:

1. Click the **-configuration settings** link under **MANAGEMENT SETTINGS** in the left-hand settings menu.
   - The **LOAD OR RESTORE SETTINGS** dialog will be shown (Figure 45 (page 97)).


LOAD OR RESTORE SETTINGS

Restore Settings	
restore settings from file:	Browse... No file selected.

Figure 45. Configurator GUI (LOAD OR RESTORE SETTINGS dialog)

2. Download the unit's configuration (*.CONF) file to your computer by clicking the **Save** button and following the software prompts.

To upload a saved configuration file to the Cisco unit, do the following steps:

1. Find the configuration (*.CONF) file that must be uploaded to the unit by clicking the **Browse...** button and following the software prompts.
   - The name of the configuration file to be uploaded will be shown to the right of the **Browse...** button.
2. Apply the configuration settings to the unit by clicking the **Restore** button.
   - The configuration will be applied, and the unit will reboot.

7.7.7. Resetting the unit to factory defaults

The **reset factory default** window contains controls that allow you to restore the Cisco FM Ponte kit to its default factory settings (in other words, to do a 'hard reset').

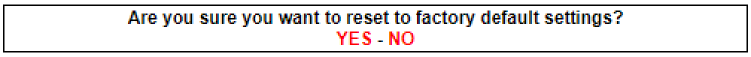
IMPORTANT

Doing a hard reset will revert all unit configuration settings, including the unit's IP address and administrator password, to factory defaults.

If you want to reboot the unit instead, refer to "Rebooting the unit" (page 98) below.

To reset the unit to its factory defaults, do the following steps:

1. Click the **-reset factory defaults** link under **MANAGEMENT SETTINGS** in the left-hand settings menu.
   - The unit reset dialog will be shown (Figure 46 (page 98)).



Are you sure you want to reset to factory default settings?
YES - NO

CAUTION

Do not do a hard reset unless the unit needs to be reconfigured using its factory configuration as a starting point.

A hard reset will reset the unit's IP address and administrator password, and will disconnect the unit from the network.

Figure 46. Configurator GUI (unit reset dialog)

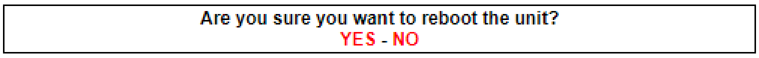
2. Reset the unit to its factory defaults by clicking the **YES** link. Alternatively, abort the factory reset by clicking the **NO** link.
   - If the **YES** link was clicked, the unit will do a factory reset, and will reboot.
3. If you have previously saved a device configuration file for the unit, you can restore the saved configuration settings to the unit as shown in "Saving and restoring the unit settings" (page 96).

Rebooting the unit

The **reboot** window contains controls that allow you to reboot the Cisco FM Ponte kit (in other words, to re-start the unit's operating system).

To reboot the unit, do the following steps:

1. Click the **-reboot** link under **MANAGEMENT SETTINGS** in the left-hand settings menu.
   - The unit reboot dialog will be shown (Figure 47 (page 99)).



Are you sure you want to reboot the unit?
YES - NO

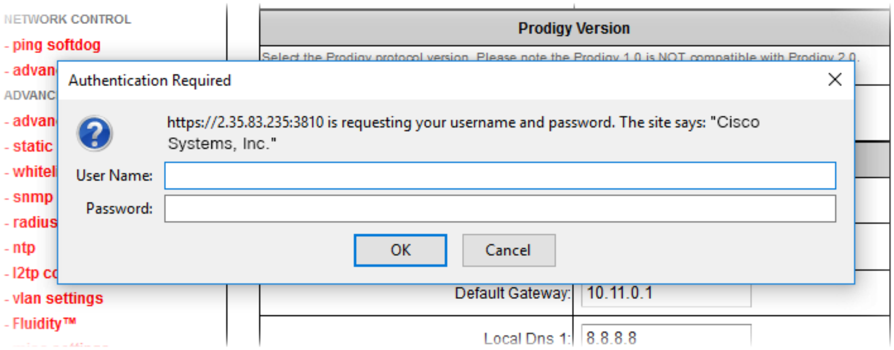
Figure 47. Configurator GUI (unit reboot dialog)

2. Reboot the unit by clicking the **YES** link. Alternatively, abort the reboot by clicking the **NO** link.
   - If the **YES** link was clicked, the unit will reboot.

7.7.8. Logging out

If clicked, the logout option logs the current user off the unit, and out of the Configurator interface.

- To log out, click the **-logout** link under **MANAGEMENT SETTINGS** in the left-hand settings menu.
  - You will be logged off the unit and out of the Configurator interface with no further prompting.
  - The web browser will show the **Authentication Required** dialog (Figure 48 (page 99)). If needed, use the dialog to log in again.



Authentication Required

https://2.35.83.235:3810 is requesting your username and password. The site says: "Cisco Systems, Inc."

User Name:
Password:

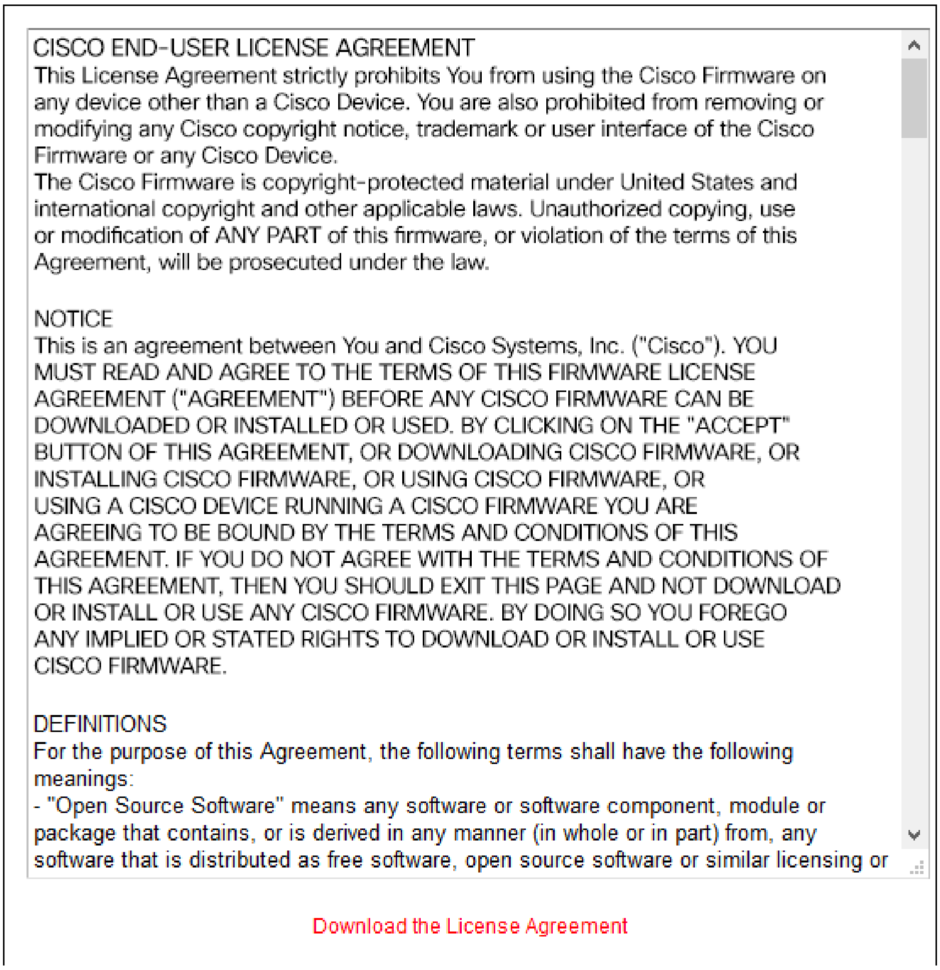
Figure 48. Web browser (Authentication Required dialog)

7.7.9. Viewing the end-user license agreement

The **License Agreement** window contains the Cisco end-user license agreement for the Cisco FM Ponte kit, its firmware and control software.

To view the terms and conditions of the license agreement, click the **License Agreement** link under **MANAGEMENT SETTINGS** in the left-hand settings menu.

- The license agreement dialog will be shown (Figure 49 (page 100)).



CISCO END-USER LICENSE AGREEMENT
This License Agreement strictly prohibits You from using the Cisco Firmware on any device other than a Cisco Device. You are also prohibited from removing or modifying any Cisco copyright notice, trademark or user interface of the Cisco Firmware or any Cisco Device.
The Cisco Firmware is copyright-protected material under United States and international copyright and other applicable laws. Unauthorized copying, use or modification of ANY PART of this firmware, or violation of the terms of this Agreement, will be prosecuted under the law.

NOTICE
This is an agreement between You and Cisco Systems, Inc. ("Cisco"). YOU MUST READ AND AGREE TO THE TERMS OF THIS FIRMWARE LICENSE AGREEMENT ("AGREEMENT") BEFORE ANY CISCO FIRMWARE CAN BE DOWNLOADED OR INSTALLED OR USED. BY CLICKING ON THE "ACCEPT" BUTTON OF THIS AGREEMENT, OR DOWNLOADING CISCO FIRMWARE, OR INSTALLING CISCO FIRMWARE, OR USING CISCO FIRMWARE, OR USING A CISCO DEVICE RUNNING A CISCO FIRMWARE YOU ARE AGREEING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT, THEN YOU SHOULD EXIT THIS PAGE AND NOT DOWNLOAD OR INSTALL OR USE ANY CISCO FIRMWARE. BY DOING SO YOU FOREGO ANY IMPLIED OR STATED RIGHTS TO DOWNLOAD OR INSTALL OR USE CISCO FIRMWARE.

DEFINITIONS
For the purpose of this Agreement, the following terms shall have the following meanings:
- "Open Source Software" means any software or software component, module or package that contains, or is derived in any manner (in whole or in part) from, any software that is distributed as free software, open source software or similar licensing or

Figure 49. Configurator GUI (End-user license agreement)

To read the end-user license agreement as an *.HTML web page in your browser, left-click the **Download the License Agreement** link.

- The end-user license agreement will be shown under a new tab in your web browser.

To download the end-user license agreement as a standard text (*.TXT) file, do the following steps:

1. Right-click the **Download the License Agreement** link.
2. Click the **Save Link as...** option and follow the software prompts to download the agreement as a text file.

8. Software Plug-Ins

8.1. Available plug-ins

Like other Cisco radio transceivers, the Cisco FM Ponte kit is able totake advantage of plug-in software upgrades that add features and enhance the performance of the unit.

The following table lists all available software plug-ins for all Cisco hardware devices, their specific functions, and their plug-in part numbers.

The tables that follow this table describe which plug-ins are compatible with specified Cisco devices.

Table 5. Available Cisco software plug-ins

Plug-in	Is the plug-in package removable and re-installable?	Function	Part number
Bandwidth	**Yes**	A range of plug-ins are available to enable increased traffic forwarding bandwidth, up to and including the amount of bandwidth specified in the part number (including unlimited bandwidth).	FM[model number]-[bandwidth limit]
Bandwidth upgrade	**Yes**	If an existing bandwidth plug-in is installed, this plug-in allows bandwidth to be upgraded to a higher, specified value. Note that if a bandwidth upgrade plug-in is removed, the unit's bandwidth capability is not restored to the level of the previous upgrade (if any). Rather, the bandwidth capability is restored to the factory default level.	FM[model number]-UPG-[existing bandwidth limit/new bandwidth limit]

Plug-in	Is the plug-in package removable and re-installable?	Function	Part number
Fluidity-Bandwidth (Mobile)	**Yes**	Enables Fluidity capability for mobile Cisco devices. Allows traffic forwarding up to and including the amount of bandwidth specified in the part number.	FM[model number]-MOB-MOB-[bandwidth limit] (FMx200 models) FM[model number]-FLU-MOB-[bandwidth limit] (FMx500 models)
Fluidity-Bandwidth (Trackside)	**Yes**	Enables Fluidity capability for static-mount Cisco devices. Allows traffic forwarding up to and including the amount of bandwidth specified in the part number.	FM[model number]-MOB-TRK-[bandwidth limit] (FMx200 models) FM[model number]-FLU-TRK-[bandwidth limit] (FMx500 models)
4.9 GHz band	**Yes**	Enables operation in the 4.9 GHz emergency band. Note that the 4.9 GHz band is not available in Brazil and Canada.	FM-49
Licensed Frequencies	**Yes**	Enables the use of any operating frequency, regardless of country selection.	FM-LF
World Frequencies	No	Unlocks the country drop-down selector on units sold in territories where the selector is locked.	FM-WORLD
AES	**Yes**	Enables data exchange according to the regular Advanced Encryption Standard.	FM-AES
Cisco Access Points	**Yes**	Enables WiFi access-point capability.	FM-AP
VLAN	**Yes**	Enables virtual LAN capability.	FM-VLAN
Virtual Gigabit	**Yes**	Enables Cisco Virtual Gigabit capability.	FM-VGBE
L2TP	**Yes**	Enables layer 2 transfer protocol capability.	FM-L2TP

Plug-in	Is the plug-in package removable and re-installable?	Function	Part number
PROFINET	**Yes**	Enables process field net capability.	FM-PROFINET
QNET	**Yes**	Enables Neutrino Qnet capability.	FM-QNET
FIPS	Yes	Enables Federal Information Processing Standards capability.	FM-FIPS
TITAN	Yes	Enables fast fail-over capability on networks where redundant (backup) units are installed.	FM-TITAN
UNII2	No	Enables use of frequencies in the Unlicensed National Information Infrastructure (U-NII) bands. Supported bands are U-NII-2A (5.250 to 5.350 GHz) and U-NII-2C / U-NII-2E (5.470 to 5.725 GHz).	FM-UNII2

The following tables describe which plug-ins are compatible with specified Cisco devices.

Table 6. Device plug-in compatibility (FM1000 Gateway to FM FM1300 Otto)

Plugin	FM1000 Gateway Gateway FM10000 Gateway Gateway	FM Ponte kit	FM FM1200 Volo	FM FM1300 Otto
Bandwidth	**Available**	Not available	**Available**	**Available**
Bandwidth upgrade	**Available**	Not available	**Available**	**Available**
Fluidity-Bandwidth (Mobile)	Not available	Not available	Not available	Not available
Fluidity-Bandwidth (Trackside)	Not available	Not available	Not available	Not available
Fluidity	***Firmware embedded***	Not available	Not available	Not available
4.9 GHz band	Not available	Not available	**Available**	Not available

Plugin	FM1000 Gateway Gateway FM10000 Gateway Gateway	FM Ponte kit	FM FM1200 Volo	FM FM1300 Otto
Licensed frequencies	Not available	Not available	**Available**	Not available
World frequencies	Not available	Not available	**Available**	Not available
AES	Not available	Not available	**Available**	**Available**
Cisco Access Points	Not available	Not available	**Available**	Not available
VLAN	***Firmware embedded***	**Available**	**Available**	Not available
Virtual Gigabit	Not available	Not available	**Available**	Not available
L2TP	***Firmware embedded***	Not available	**Available**	Not available
PROFINET	***Firmware embedded***	Not available	**Available**	Not available
QNET	***Firmware embedded***	Not available	**Available**	Not available
FIPS	Not available	Not available	**Available**	Not available
TITAN	**Available**	Not available	**Available**	Not available
UNII2	Not available	Not available	**Available**	Not available

Table 7. Device plug-in compatibility (FM Cisco 3200-series to FM 4800)

Plugin	FM FM3200 Base FM FM3200 Endo	FM Cisco FM3500 Endo	FM FM4200 Fiber FM FM4200 Mobi	FM FM4500 Fiber FM FM4500 Mobi	FM 4800
Bandwidth	**Available**	**Available**	**Available**	**Available**	**Available**
Bandwidth upgrade	**Available**	**Available**	**Available**	**Available**	**Available**
Fluidity-Bandwidth (Mobile)	**Available**	**Available**	**Available**	**Available**	**Available**
Fluidity-Bandwidth (Trackside)	**Available**	**Available**	**Available**	**Available**	**Available**
Fluidity	**Available**	**Available**	**Available**	**Available**	**Available**
4.9 GHz band	**Available**	**Available**	**Available**	**Available**	Not available

Plugin	FM FM3200 Base FM FM3200 Endo	FM Cisco FM3500 Endo	FM FM4200 Fiber FM FM4200 Mobi	FM FM4500 Fiber FM FM4500 Mobi	FM 4800
Licensed frequencies	**Available**	**Available**	**Available**	**Available**	**Available**
World frequencies	**Available**	**Available**	**Available**	**Available**	**Available**
AES	**Available**	**Available**	**Available**	**Available**	**Available**
Cisco Access Points	**Available**	Not available	**Available**	Not available	Not available
VLAN	**Available**	**Available**	**Available**	**Available**	**Available**
Virtual Gigabit	Not available	Not available	Not available	Not available	Not available
L2TP	**Available**	**Available**	**Available**	**Available**	**Available**
PROFINET	**Available**	**Available**	**Available**	**Available**	**Available**
QNET	**Available**	**Available**	**Available**	**Available**	**Available**
FIPS	**Available**	**Available**	**Available**	**Available**	**Available**
TITAN	**Available**	**Available**	**Available**	**Available**	**Available**
UNII2	**Available**	**Available**	**Available**	**Available**	**Available**

To purchase any of the software plug-ins, please contact your Cisco Networks representative.

8.2. Plug-in management procedures

8.2.1. Plug-in activation

The Plug-in management procedure has been standardized, and is the same for all Cisco hardware devices.

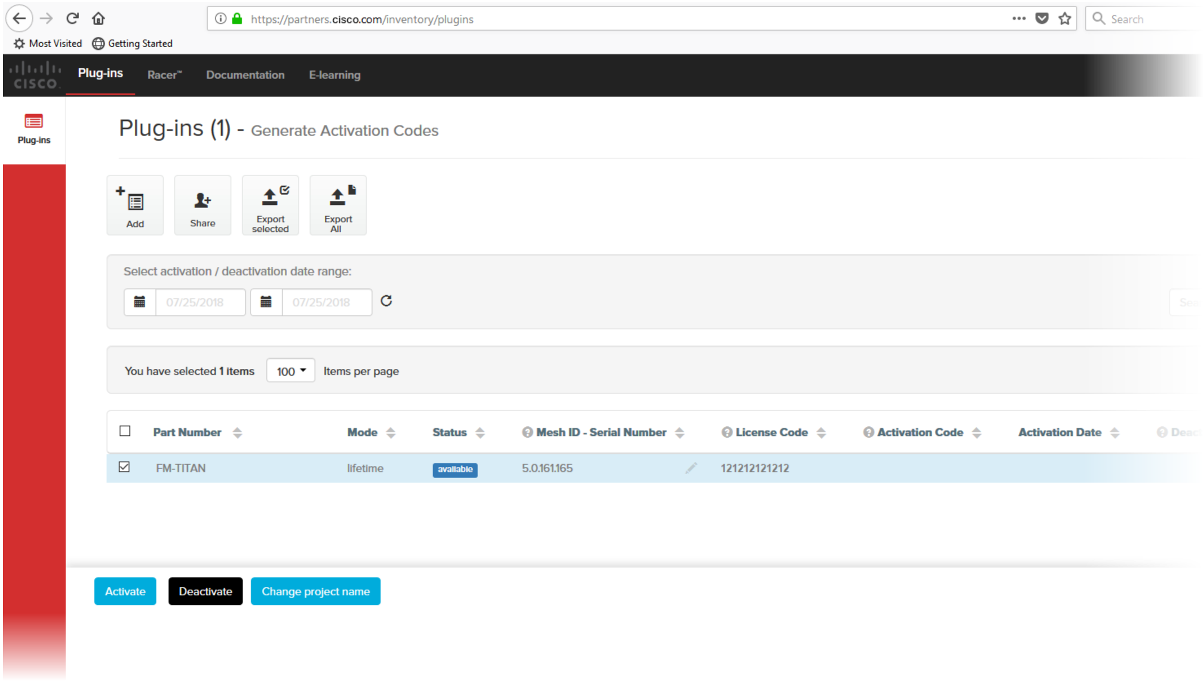
To obtain a plug-in activation code for a Cisco device, do the following steps:

1. Contact your Cisco Networks representative to purchase a generic 16-digit *License code* for plug-in activation.
2. Quote the unique mesh unit identification number (**5.a.b.c**) of the Cisco hardware device.
3. Using the Cisco Partner Portal, associate the *License code* with the quoted Cisco device to get an *Activation code*.
4. Enter the Activation code on the **MANAGE PLUG-INS** window for the unit.

You can also deactivate a plug-in Activation code that is currently in use so it can be used with a different Cisco unit. To deactivate an active plug-in, refer to The PLUGINS sub-tab.

To convert a License code into an Activation code for a Cisco device,do the following steps:

1. Log on to the Cisco Partner Portal.
2. Click the **Plug-ins** link.
   - When you purchase a generic 16-digit *License code*, the License code and corresponding plug-in will be listed on the Plug-ins page (Figure 50 (page 106)).



Plug-ins (1) - Generate Activation Codes

Select activation / deactivation date range: 07/25/2018 07/25/2018

You have selected 1 items 100 Items per page

□	Part Number	Mode	Status	Mesh ID - Serial Number	License Code	Activation Code	Activation Date	Deac
☑	FM-TITAN	lifetime	available	5.0.161.165	121212121212			

Figure 50. Partner Portal Plug-ins page (License code plug-in)

   - When the generic License code was purchased, you will have received an E-mail from *plugins@cisco.com* containing the License code. If the License code and corresponding plug-in are *not* listed on the Plug-ins page, click the **Add** button in the upper left-hand corner of the Plug-ins web page, and enter the License code using the dialog.

3. Enter the unit identification number (**5.a.b.c**) *or* the unit serial number of the Cisco unit in the **Mesh ID - Serial Number** field.
4. If needed, enter the name of the relevant technical project in the **Project Name** field.

TIP

If you cannot see the **Project Name** field, reduce the magnification on the Plug-ins web page until all the headings are visible.

5. Click the **Activate** button on the Plug-ins web page.
    - The **Plug-in Activation** dialog will be shown. Check that the given E-mail address is correct, and click the **Activate** button.
    - You will receive an E-mail from *plugins@cisco.com* containing the Activation code.
    - The **Activation Code** and **Activation Date** will be shown in the relevant fields on the Plug-ins web page.
    - The plug-in Status will change from **available** to **active**.
6. Use the Activation code to activate the plug-in. Refer to "Plug-In management" (page 90) for details.
    - The plug-in will be activated, and the relevant functionality can be used.

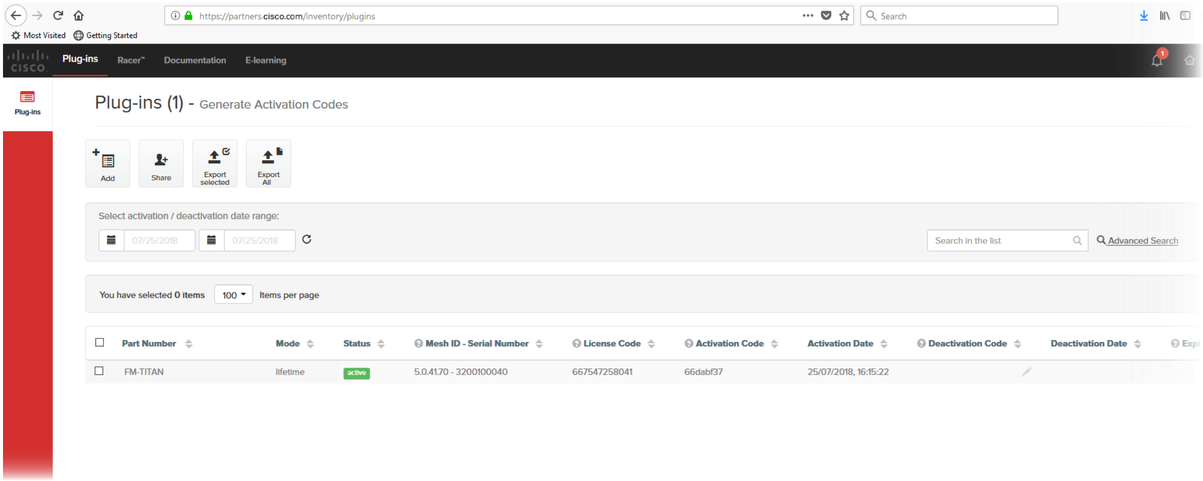
8.2.2. Deactivating an active plug-in

A plug-in *Activation code* that is currently in use can be *deactivated*. This allows the corresponding *License code* to be used in a different Cisco unit, or transferred to another Cisco user.

To deactivate an activated License code for use with another Cisco unit, do the following steps:

1. On the Configurator interface, click the **PLUGINS** sub-tab under the **SERVICES** tab (FM FM1300 Otto only) or click the **-manage plug-ins** link under **MANAGEMENT SETTINGS** in the left-hand settings menu (all other devices).
    - The **Manage Plugins** dialog will be shown (see below).
2. Click the red **REMOVE** link to the right of the correct plug-in listing.
    - The web browser will inform you that deactivating the plug-in will reboot the unit, and ask for confirmation that you want to deactivate.
3. Confirm the deactivation.
    - The unit will reboot.
    - The Deactivation code for the plug-in will be shown to the right of the plug-in listing, in the **Plug-in Deactivation Codes** section (see below).
4. Make a note of the Deactivation code.

5. Log on to the Cisco Partner Portal.
6. Click the **Plug-ins** link.
    - The Plug-ins web page will be shown (Figure 51 (page 108)).



Plug-ins (1) - Generate Activation Codes

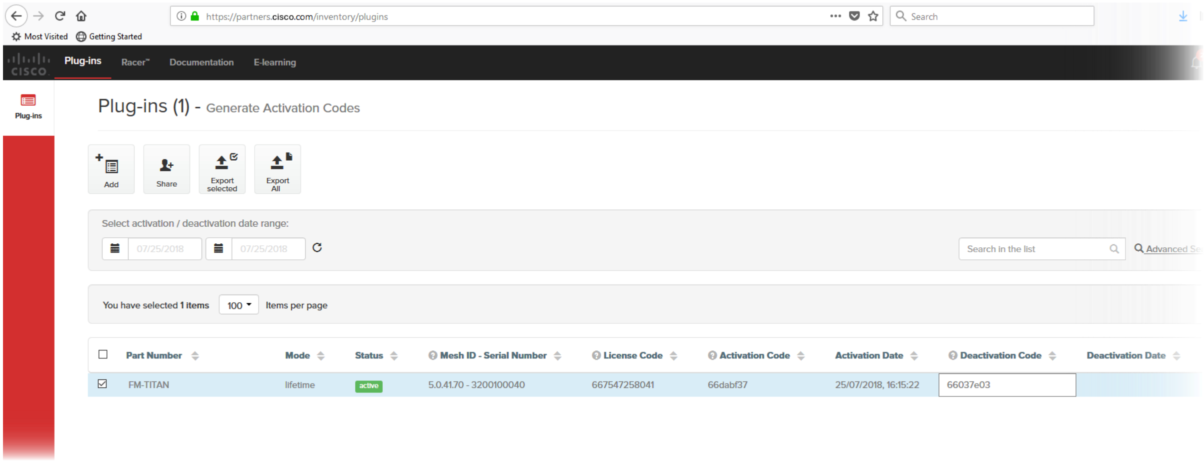
Select activation / deactivation date range: 07/25/2018 07/25/2018

You have selected **0** items 100 Items per page

□	Part Number	Mode	Status	Mesh ID - Serial Number	License Code	Activation Code	Activation Date	Deactivation Code	Deactivation Date
□	FM-TITAN	lifetime	active	5.0.41.70 - 3200100040	667547258041	66dabf37	25/07/2018, 16:15:22		

Figure 51. Partner Portal Plug-ins page (License code deactivation)

7. Check the selection check-box to the left of the relevant plug-in listing.
    - The plug-in control buttons will be shown at the bottom of the web page.
8. Enter the Deactivation code for the plug-in in the Deactivation Code field (Figure 52 (page 108)).



Plug-ins (1) - Generate Activation Codes

Select activation / deactivation date range: 07/25/2018 07/25/2018

You have selected **1** items 100 Items per page

□	Part Number	Mode	Status	Mesh ID - Serial Number	License Code	Activation Code	Activation Date	Deactivation Code	Deactivation Date
☑	FM-TITAN	lifetime	active	5.0.41.70 - 3200100040	667547258041	66dabf37	25/07/2018, 16:15:22	66037e03	

Figure 52. Partner Portal Plug-ins page (deactivation code entry)

9. Click the **Deactivate** button at the bottom of the web page.

- The **PLUG-IN DEACTIVATION** dialog will be shown.

10. To do a normal deactivation, click the **Deactivate** button. If for any reason it is not possible to retrieve the deactivation code, click the **Force Deactivation** button.

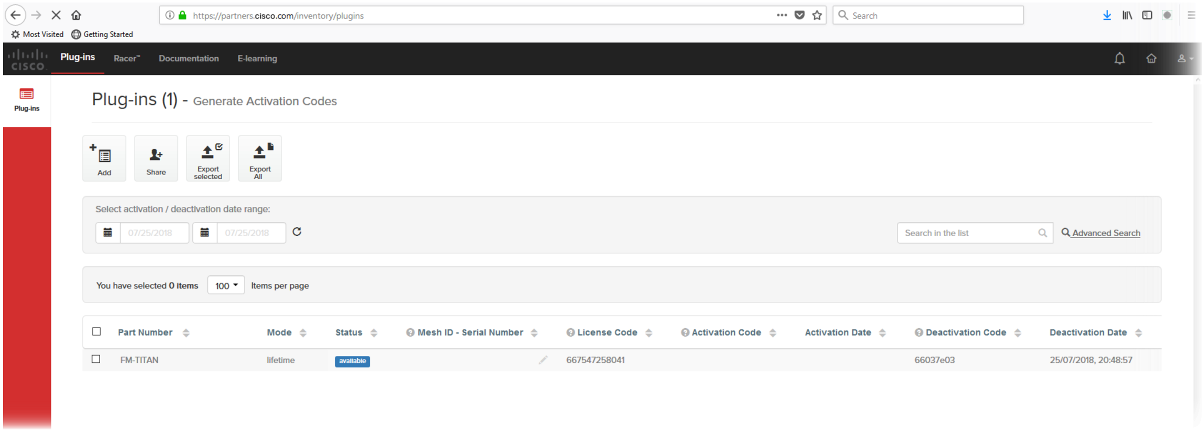
> **IMPORTANT**
>
> Only click the **Force Deactivation** button if you have no way to retrieve the deactivation code (for example, if the unit's boot sequence cannot be completed, or if the unit is damaged and cannot be powered ON).

- The plug-in will be deactivated.
- The Deactivation code will be shown in the **Deactivation Code** column of the plug-in listing.
- The Deactivation code will remain on the Partner Portal, and can be used to generate a new Activation code if needed.

8.2.3. Reactivating a deactivated plug-in

To use a Deactivation code to generate an new Activation code, do the following steps:

1. Log on to the Cisco Partner Portal.
2. Click the **Plug-ins** link.
    - The Plug-ins web page will be shown (Figure 53 (page 109)).



Plug-ins (1) - Generate Activation Codes

Select activation / deactivation date range: 07/25/2018 07/25/2018

Search in the list

You have selected **0 items** 100 Items per page

□	Part Number	Mode	Status	Mesh ID - Serial Number	License Code	Activation Code	Activation Date	Deactivation Code	Deactivation Date
□	FM-TITAN	lifetime	available		667547258041			66037e03	25/07/2018, 20:48:57

Figure 53. Partner Portal (Plug-ins web page)

3. Check the selection check-box to the left of the relevant plug-in listing.
    - The plug-in control buttons will be shown at the bottom of the web page.

4. Enter the unit identification number (**5.a.b.c**) or the unit serial number of the Cisco unit in the **Mesh ID - Serial Number** field.
5. Complete the plug-in activation process as shown in "Plug-in activation" (page 105).

8.2.4. Exporting and uploading multiple Activation codes

If more than one plug-in Activation code must be uploaded to a Cisco radio transceiver unit at the same time, the need to upload codes one by one can be avoided by exporting multiple codes, or all codes, from the Partner Portal as a *.CSV file.

To export a collection of Activation codes from the Partner Portal as a *.CSV file, do the following steps:

1. Log on to the Cisco Partner Portal.
2. Click the **Plug-ins** link.
   - The Plug-ins web page will be shown.
3. Convert all needed License codes and/or Deactivation codes to Activation codes as shown in "Plug-in activation" (page 105)
4. To export only selected Activation codes, check the selection check-boxes to the left of each plug-in that must be included in the *.CSV file, then click the **Export selected** button. Alternatively, export all Activation codes by clicking the **Export All** button (Figure 54 (page 110)).

IMPORTANT

If all Activation codes are exported, only the Activation codes that are linked to the unit identification number (**5.a.b.c**), or the unit serial number of the target unit, will be assigned to the unit.

All codes that are not relevant to the unit will remain unused.

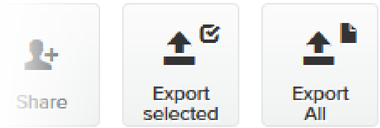
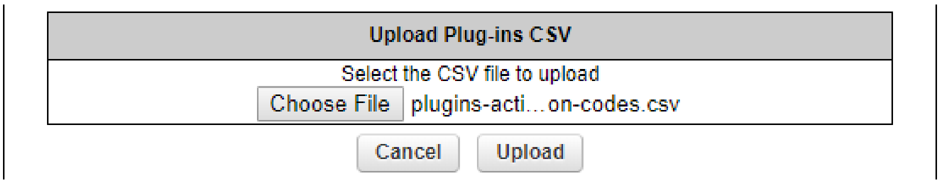


Figure 54. Plug-ins web page (code export controls)

5. Follow the software prompts to download the exported *.CSV file to your computer. Save the file in a safe place.
6. On the configurator interface, click the **-manage plug-ins** link under **MANAGEMENT SETTINGS** in the left-hand settings menu.

- The **MANAGE PLUG-INS** dialog will be shown.

7. Upload the *.CSV file to the unit by clicking the **Choose File** button in the **Upload Plug-ins CSV** section (Figure 55 (page 111)) and following the software prompts.



Upload Plug-ins CSV

Select the CSV file to upload

Figure 55. MANAGE PLUG-INS DIALOG (Upload Plug-ins CSV section)

- The chosen *.CSV file will be listed to the right of the **Choose File** button.

8. Click the **Upload** button.

- The plug-ins will be uploaded to the unit and activated, and the relevant functionality can be used.

8.2.5. Sharing License codes and accepting shared License codes

If needed, you can share license codes with other Cisco device users, and also have other Cisco device users share their license codes with you.

To share one or more license codes with another Cisco device user,do the steps that follow:

1. Log on to the Cisco Partner Portal.
2. Click the **Plug-ins** link.
   - The Plug-ins web page will be shown.
3. Check the selection check-boxes to the left of the plug-ins that must be shared.
4. Click the **Share** button in the upper left-hand corner of the **Plug-ins** web page (Figure 56 (page 111)).

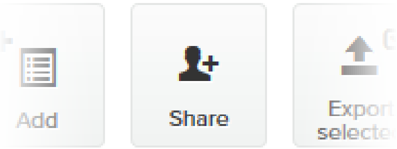


Figure 56. Plug-ins web page (Share button)

- The **Share License Codes** dialog will be shown.

5. Enter one or more E-mail addresses to which the License codes must be sent. Click the **Share** button.
    - An E-mail containing the selected License codes will be sent to the specified E-mail addresses.
    - The License codes contained in the E-mail can be converted to plug-in Activation codes in the normal way.

If needed, you can also ask another device user to share one or more license codes with you. If a License code is shared with you, it will be listed on your Partner Portal Plug-ins web page.

9. Troubleshooting

This section contains information that will allow you to solve common problems associated with configuration and installation of Cisco products.

9.1. I cannot get the Log-in screen

If you have directly connected a Windows computer to your Cisco device for device configuration, but you cannot access the log-in form on your web browser, check the following points:

Are you trying to access the unit using a valid IP address?

You must manually set the computer's IP address and Netmask to be recognizable by the Cisco device. The correct settings are as follows:

- **IP address:** 192.168.0.10 (or any other IP address belonging to subnet 192.168.0.0/255.255.255.0)
- **Netmask:** 255.255.255.0

Have you disabled the 'Access the Internet using a proxy server' function?

If your browser shows a time-out or similar message, the computer may be trying to access the Cisco device through a proxy server. To stopthe computer from trying to access the unit through a proxy connection, refer to “Accessing the Cisco FM Ponte kit for device configuration” (page 37).

9.2. I forgot the Administrator password

If you have forgotten the Administrator user name and/or password for the Configurator interface, and you must access the unit to configure it using the Configurator interface, do the following steps:

1. Physically access the unit.
2. Use the hardware **Reset** button to reset the unit to its factory default settings. Refer to “Resetting the unit to factory defaults” (page 98) for more information.

9.3. The wireless link is poor or non-existent in Bridge mode

If the unit is set to **Bridge** mode, and is showing any or all of the following symptoms:

- There is no wireless link
- The link LED on the device enclosure shows constant red
- The wireless link is constantly below 60% signal strength

Check the following points to improve the wireless link strength:

1. **Antenna alignment:** The antennas belonging to both units forming part of the affected link must face each other as directly as possible.
2. **Line-of-sight:** The antennas belonging to both units forming part of the affected link must have clear line-of-sight (in other words, there must be no physical obstructions between the two antennas).
3. **Power:** Verify that both units forming part of the affected link are receiving enough power from their Ethernet connections or PoE injectors.
4. **Frequency value and channel width:** Both units forming part of the affected link must be set to the same frequency value, and to the same channel width.

10. Electrical power requirements

The following table describes:

- The electrical power requirements for each Cisco hardware device type.
- Which Cisco hardware devices are capable of receiving power through an IEEE 802.3 Ethernet port (whether from a power-supplying device like a compatible network switch, or from a power-over-Ethernet (PoE) injector), or through a DC IN power supply port, or both.
- The specific voltage-variation tolerances of each Cisco radio transceiver unit type.

Table 8. Individual power requirements (FM1000 Gateway and FM10000 Gateway)

	Required input power	**FM1000 Gateway**	**FM10000 Gateway**
DC IN	12 Vdc (from mains AC power adapter producing a minimum of 60W (12V/5A)).	**X**	
First-generation FM10000 Gateway: unit may be equipped with single 250W non-redundant AC power supply unit (input power: 100 Vac to 240 Vac at 50 Hz to 60 Hz).		**X**	

Table 9. Individual power requirements (FM Ponte kit to FM4200 Mobi)

		FM Ponte kit (model FM1200V-HW)	**FM1200 Volo (model FM1200V-HW)**	**FM1300 Otto**	**FM3200 Base (model FM3200)**	**FM3200 Endo (model FM3200)**	**FM4200 Mobi (model FM4200)**
PoE	24V passive PoE	**X**	**X**				
	48V passive PoE				**X**	**X**	**X**

	IEEE 802.3af PoE (voltage range at PD: 37V to 57V)			X	X	X	X
	IEEE 802.3at PoE (voltage range at PD: 42.5V to 57V)			X	X	X	X
DC IN	Permanent DC power, min. 24V max. 60V						X
	EN 50155 compliance at 48V						X

Table 10. Individual power requirements (FM4200 Fiber to FM4800 Fiber)

		FM4200 Fiber (model FM4200F)	FM3500 Endo (model FM3500)	FM4500 Mobi (model FM4500)	FM4500 Fiber (model FM4500F)	FM4800 Fiber
PoE	24V passive PoE					
	48V passive PoE	X	X	X	X	X
	IEEE 802.3af PoE (voltage range at PD: 37V to 57V)	X				
	IEEE 802.3at PoE (voltage range at PD: 42.5V to 57V)	X	X	X	X	X

		FM4200 Fiber (model FM4200F)	FM3500 Endo (model FM3500)	FM4500 Mobi (model FM4500)	FM4500 Fiber (model FM4500F)	FM4800 Fiber
DC IN	Permanent DC power, min. 24V max. 60V	X		X	X	X
	EN 50155 compliance at 48V	X		X	X	X

11. Heat radiation data

When in use, all Cisco gateway units and radio transceivers generateheat as a by-product of electrical activity.

Heat radiated by a Cisco device may be of concern in confined locations such as server rooms (where the cumulative heat generated by a collection of electrical and electronic devices may cause damage to sensitive electronic components) and outdoor equipment enclosures (in which electronic components may overheat if the enclosure is not properly ventilated).

WARNING

The outer surfaces of some Cisco units may become hot during normal operation. Such units have a 'Hot Surfaces' warning triangle on their outer enclosures.

During normal operation, do not touch or handle such unit enclosures without personal protective equipment.

The following table shows nominal heat-radiation figures for all Cisco devices under idle conditions, and under full-load conditions.

All heat-radiation figures are given in British Thermal Units (BTU) per hour.

Device	Fiber-optic module installed	Idle @ 115 Vac / 60 Hz	Idle @ 230 Vac / 60 Hz	Full load @ 115 Vac / 60 Hz	Full load @ 230 Vac / 60 Hz
FM1000 Gateway		25.590	33.780	25.250	33.100
FM10000 Gateway (first and second generations)		271.595	267.159	436.395	437.078
FM Ponte kit (model FM1200V-HW)		6.479	6.138	19.778	19.437
FM1200 Volo (model FM1200V-HW)		6.479	6.138	19.778	19.437
All 3200-series transceivers (model FM3200)		10.230	10.230	24.552	24.552
FM3500 Endo (model FM3500)		9.889	9.889	26.939	26.939
FM4200 Mobi (model FM4200)		10.230	10.230	24.552	24.552
FM4200 Fiber (model FM4200F)	No	12.617	12.617	26.939	26.939

Device	Fiber-optic module installed	Idle @ 115 Vac / 60 Hz	Idle @ 230 Vac / 60 Hz	Full load @ 115 Vac / 60 Hz	Full load @ 230 Vac / 60 Hz
	Yes	15.004	15.004	29.326	28.985
FM4500 Mobi (model FM4500)		9.889	9.889	26.939	26.939
FM4500 Fiber (model FM4500F)	No	9.889	9.889	26.598	26.257
	Yes	12.958	12.958	29.326	29.326
FM4800 Fiber	No	23.529	23.529	47.399	47.058
	Yes	27.280	26.939	51.832	50.468

12. Federal Communications Commission (FCC) radio interference statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

FCC Caution: to assure continued compliance, use only shielded interface cables when connecting to computer or peripheral devices. You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This device has been assembled using components that comply with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Industry Canada

The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations.

Industry Canada Statement

This device complies with RSS-247 of Industry Canada.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Avis d'industrie Canada

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence.

L'exploitation est autorisee aux deux conditions suivantes:

(1) l'appareil ne doit pas produire de brouillage, et, and (2) l'utilisateur de l'appareil doit accepter tout brouillage radioelectrique subi, meme si le brouillage est susceptible d'en compromettre le fonctionnement.

IC RF Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

EC Declaration of Conformity

Cisco Systems Inc. declares under its sole responsibility that the Cisco FM Ponte kit is compliant with the following directives, and has been designed and manufactured to the following specifications:

EMC	EN 61000-6-1; EN 61000-6-2; EN 61000-6-3; EN 61000-6-4; EN 489-17
R&TTE	EN 300 328-1 V. 1.3.1; EN 300 328-2 V. 1.2.1; EN 301 893-1 V. 1.2.1; EN 300 440-2 V. 1.3.1
Safety	EN 60950-1:2001

Caution: This equipment is intended to be used in all EU and EFTA countries. Contact local Authority for procedure to follow.

Note:

Class A ITE is a category of all other ITE which satisfies the class A ITE but not the class B ITE limits.

Such equipment should not be restricted in its sale but the following warning shall be included in the instruction for use:

WARNING: this is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

For more details on legal combinations of power levels and antennas, contact Cisco Systems Inc.

Belgique

Dans le cas d’une utilisation privee, `a l’exterieur d’un batiment, au-dessus d’un espace public, aucun enregistrement n’est necessaire pour une dis-tance de moins de 300m. Pour une distance sup´erieure `a 300m un enregistrement aupr`es de l’IBPT est requise. Pour une utilisation publque a l’exterieur de batiments, une licence de l’IBPT est requise. Pour les enregistrements et licences, veuillez contacter l’IBPT.

France

Vous pouvez contacter l’Autorite de Regulation des Telecommunications (http://www.art-telecom.fr) pour de plus amples renseignements.

13. Notices and copyright

WARNING

Installation of Cisco hardware devices and their supporting infrastructure must be done by suitably qualified personnel only. In some countries, installation by a certified electrician may be required.

Hardware installations must comply with all applicable local legislation.

WARNING

Never disassemble a Cisco hardware device to any extent that is not described in the relevant device user's manual. Cisco devices contain no user-serviceable parts. Disassembling a Cisco hardware device will invalidate the device warranty, and may compromise the operational integrity of the device.

On some Cisco radio transceiver devices, the lower access cover must be removed to gain access to the hardware *Reset* button. Do not operate a radio transceiver device for extended periods if its lower access cover has been removed.

WARNING

To avoid danger from non-ionizing radiation and/or electric shock and/or high-intensity laser or LED light sources, be sure to install the unit only in a location with restricted access.

WARNING

To avoid danger from electric shock, do not expose the unit to water or high humidity if the unit is powered ON, or if any access covers have been removed from the unit enclosure.

Do not place liquid-filled objects on or above the unit.

NOTICE TO THE USER

Copyright © 2021 Cisco and/or its affiliates. All rights reserved. This manual and the software described herein shall not, in whole or in part, be reproduced, translated or reduced to any machine-readable form without the prior written consent of Cisco Systems.

Cisco and/or its affiliates provides no warranty with regard to this manual, software or other information contained herein, and hereby expressly disclaims any implied warranties of merchantability or fitness for any particular purpose with regard to this manual, the software or such other information. In no event shall Cisco Systems be held liable for any incidental, consequential or special damages, whether based on tort, contract or otherwise, arising out of or in connection with this manual, the software or other information contained herein, or use thereof.

Cisco Systems reserves the right to make any modification to this manual or the information contained herein at any time, without notice. The software described herein may also be governed by the terms of a separate end-user license agreement.

Cisco is a registered trademark of Cisco Systems. MeshWizard, EasyMesh, FMQuadro, FluidThrottle, VOLO, Fluidity, Virtual Gig, ENDO and MOBI are trademarks of Cisco Systems Inc.

Microsoft, Windows, Internet Explorer and Microsoft Edge are registered trademarks of the Microsoft Corporation in the United States and/or other countries.

Ethernet is a registered trademark of the Xerox Corporation.

Adobe and Flash Player are registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

All other brands and product names that appear in this manual may be trademarks or registered trademarks. Such brands and product names are the property of their respective owners.

14. Cisco end-user license agreement

14.1. Preamble

This License Agreement strictly prohibits you from using the Cisco Firmware on any device other than a Cisco Device. You are also prohibited from removing or modifying any Cisco or Cisco copyright notice, trademark or user interface of the Cisco Firmware or any Cisco Device.

The Cisco Firmware is copyright-protected material under United States and international copyright and other applicable laws. Unauthorized copying, use or modification of any part of this firmware, or violation of the terms of this Agreement, will be prosecuted to the maximum extent allowable under law.

14.2. Notice

This is an agreement between you and Cisco, a division of Cisco (hereafter known as 'Cisco').

You must read and agree to the terms of this firmware license agreement (hereafter known as the 'agreement') before any Cisco firmware canbe downloaded, installed or used. By clicking the 'Accept' button on any Cisco firmware download web page, or by downloading, installing or using Cisco firmware and/or by using any Cisco device running Cisco firmware, you are agreeing to be bound by the terms and conditions of this agreement. If you do not agree with the terms and conditions of this agreement, then you should not download, install or use any Cisco firmware, and you agree to forego any implied or statedrights to download, install or use Cisco firmware.

14.3. Definitions

For the purpose of this Agreement, the following terms shall have the following meanings:

'Open Source Software' means any software or software component, module or package that contains, or is derived in any manner (in whole or in part) from, any software that is distributed as free software, open source software or similar licensing or distribution models, including, without limitation, software licensed or distributed under any of the following licenses or distribution models, or licenses or distribution models similar to any of the following: (a) GNU's General Public License (GPL) or Lesser/Library GPL (LGPL); (b) the Artistic License (e.g., PERL); (c) the Mozilla Public License; (d) the BSD License; and (e) the Apache License;

'Cisco Device' means a Cisco networking device that youpurchase or otherwise rightfully acquire;

'Cisco Firmware' means the firmware in object code form made available by Cisco for Cisco Devices; and

'You' and 'Your' mean the company, entity or individual who owns or otherwise rightfully acquires the Cisco Device into which the Cisco Firmware will be incorporated.

14.4. License grant

Cisco grants you a non-exclusive, non-transferable license to use a copy of the Cisco Firmware and accompanying documentation and any updates or upgrades thereto provided by Cisco according to the terms set forth below. You are authorized by this license to use the Cisco Firmware in object code form only, and solely in conjunction with applicable and permitted Cisco-branded products and/or services and in accordance with the applicable documentation. You are granted a limited and non-exclusive license (without the right to sub-license) to use the software solely for the Cisco Devices that you own and control, and solely for use in conjunction with the Cisco Firmware.

14.5. Uses and restrictions on use

You may:

(a) download and use Cisco Firmware for use in Cisco Devices,and make copies of the Cisco Firmware as reasonably necessary for such use, provided that you reproduce, unaltered, all proprietary notices that exist on or in the copies.

You may not, and shall not permit others to:

(a) use the Cisco Firmware on any devices or products that are not owned by you or your business organization;

(b) use the Cisco Firmware on any non-Cisco Devices;

(c) copy the Cisco Firmware (except as expressly permitted above), or copy the accompanying documentation;

(d) modify, translate, reverse engineer, decompile, disassemble or otherwise attempt (i) to defeat, avoid, bypass, remove, deactivate, or otherwise circumvent any software protection mechanisms in the Cisco Firmware, including without limitation any such mechanism used to restrict or control the functionality of the Cisco Firmware, or (ii) to derive the source code or the underlying ideas, algorithms, structure or organization from the Cisco Firmware (except that the foregoing limitation does not apply to the extent that such activities may not be prohibited under applicable law); or

(e) distribute, rent, transfer or grant any rights in the Cisco Firmwareor modifications thereof or accompanying documentation in any form to any person without the prior written consent of Cisco.

(f) remove any Cisco or Cisco copyright notice, or Cisco or Ciscobranding from the Cisco Firmware or modify any user interface of the Cisco Firmware or Cisco Device.

Cisco Devices must be properly installed and they are sold for installation by a professional installer only. Cisco Devices must be installed by a professional installer of wireless networking products certified by Cisco, and they are not designed for installation by the general public. It is your responsibility to follow local country regulations, including operation within legal frequency channels, output power, and Dynamic Frequency Selection (DFS) requirements. You are responsible for keeping the devices working according to these rules.

(g) The Cisco Firmware contains technological protection or other security features designed to prevent unauthorized use of the Cisco Firmware, including features to protect against use of the Cisco Fimrware beyond the scope of the license granted herein, or in a manner prohibited herein. You agree that you shall not, and shall not attempt to, remove, disable, circumvent or otherwise create or implement any workaround to, any such copy protection or security features.

This license is not a sale. Title and copyrights to the Cisco Firmware,and any copy made by you, remain with Cisco and its suppliers. Unauthorized copying of the Cisco Firmware or the accompanying documentation, or failure to comply with the above restrictions, will result in automatic termination of this license and will make other legal remedies available to Cisco.

14.6. Open-source software

You hereby acknowledge that the Cisco Firmware may contain Open Source Software. You agree to review any documentation that accompanies the Cisco Firmware or is identified in the documentation for the Cisco Firmware, in order to determine which portions of the Cisco Firmware are Open Source Software and are licensed under an Open Source Software license. To the extent that any such license requires that Cisco provide you with rights to copy, modify, distribute or otherwise use any Open Source Software that are inconsistent with the limited rights granted to you in this Agreement, then such rights in the applicable Open Source Software license shall take precedence over the rights and restrictions granted in this Agreement, but solely with respect to such Open Source Software. You acknowledge that the Open Source Software license is solely between you and the applicable licensor of the Open Source Software. You shall comply with the terms of all applicable Open Source Software licenses, if any. Copyrights to the Open Source Software are held by the copyright holders indicated in the copyright notices in the corresponding source files, or as disclosed at www.cisco.com.

14.7. Termination

This license will continue until terminated. Unauthorized copying of the Cisco Firmware or failure to comply with the above restrictions will result in automatic termination of this Agreement and will make other legal remedies available to Cisco. This license will also automatically terminate if you go into liquidation, suffer or make any winding-up petition, make an arrangement with your creditors, or suffer or file any similar action in any jurisdiction in consequence of debt.

Furthermore, Cisco may immediately terminate this Agreement if (i)you fail to cure a breach of this Agreement (other than a breach pursuantto Cisco intellectual property rights) within thirty (30) calendar daysafter its receipt of written notice regarding such breach, or (ii) you breachany Cisco intellectual property right. Upon termination of this licensefor any reason, you agree to destroy all copies of the Cisco Firmware. Any use of the Cisco Firmware after termination isunlawful.

14.8. Feedback

You may provide suggestions, comments or other feedback ('Feedback') with respect to Cisco Firmware, and Cisco Devices. Feedback,even if designated as confidential by you, shall not impose any confidentiality obligations on Cisco. You agree that Cisco is freeto use, disclose, reproduce, license or otherwise distribute and exploit any Feedback provided by you as Cisco sees fit, entirely without obligation or restriction of any kind on account of intellectual property rights, or otherwise.

14.9. Consent to use of data

You acknowledge and agree that Cisco may, directly or indirectly through the services of third parties, collect and store information regarding the use and performance of the Cisco Firmware and Cisco Devices, and about equipment through which it otherwise is accessed and used.

You further agree that Cisco may use such information for any purpose related to any use of the Cisco Firmware and Cisco Devices by you, including, without limitation, improving the performance ofthe Cisco Firmware or developing updates and verifying your compliance with the terms of this Agreement and enforcing Cisco's rights, including all intellectual property rights in and to the Cisco Firmware.

Cisco shall have the right to collect and analyze data and other information relating to the provision, use and performance of various aspects of the Cisco Firmware and Cisco Devices and relatedsystems and technologies ('Data'), and you give Cisco the right touse and disclose such Data (during and after the term of this Agreement)in accordance with Cisco's Privacy Policy. If you choose to allow diagnostic and usage collection, you agree that Cisco and its subsidiaries and agents may collect, maintain, process and use diagnostic, technical, usage and related information, including but not limited to unique system or hardware identifiers, information about your device, system and software, that is gathered periodically to provide and improve Cisco's products and services, facilitate the provision of software updates, product support and other services to you (if any) related to Cisco products, and to verify compliance with the terms ofthis license. Cisco may use this information, as long as it is collectedin a form that does not personally identify you, for the purposes described above.

To enable Cisco's partners and third-party developers to improvetheir software, hardware and services designed for use with Cisco products, Cisco may also provide any such partner or third-partydeveloper with a subset of diagnostic information that is relevant to that partner’s or developer’s software, hardware and/or services, as long asthe diagnostic information is in a form that does not personally identify you.

14.10. Warranty disclaimer

Cisco Firmware, including without limitation any open source software, any Cisco Device, and any accompanying documentation are provided 'As is', and Cisco and its suppliers make, and you receive, no warranties or conditions, whether express, implied, or otherwise, or in any communication with you, and Cisco and its suppliers specifically disclaim any implied warranty of merchantability,satisfactory quality, fitness for a particular purpose, or non-infringementand their equivalents.

Cisco does not warrant that the operation of the Cisco Firmware will be uninterrupted or error-free or that the Cisco Firmware will meet your specific requirements. You acknowledge that Cisco has nosupport or maintenance obligations for the Cisco Firmware.

14.11. Limitation of liability

Except to the extent that liability may not by law be limited or excluded, in no event will Cisco or its suppliers be liable for loss of, or corruption to data, lost profits or loss of contracts, cost of procurement of substitute products or other special, incidental, punitive, consequential or indirect damages arising from the supply or use of the Cisco Firmware, howsoever caused and on any theory of liability (including without limitation negligence).

This limitation will apply even if Cisco or an authorized distributor or authorized reseller has been advised of the possibility of such damages, and notwithstanding the failure of essential purpose of any limited remedy. In no event shall Cisco's or its suppliers' or its resellers’ liability exceed five hundred United States dollars (US$ 500). You acknowledge that this provision reflects a reasonable allocation of risk.

14.12. Exclusion of liability for emergency services

Cisco does not support, nor are the services intended to support or carry, emergency calls to any emergency services, including but not limited to 911 dialing.

Cisco will not be held responsible for any liability or any losses, andyou, on behalf of yourself and all persons using the services through the licensed products, hereby waive any and all such claims or causes of action for losses arising from, or relating to, any party's attempts to contact emergency service providers using the licensed products, including but not limited to calls to public safety answering points.

Cisco will not be held liable for any losses, whether in contract, warranty, tort (including negligence), or any other form of liability, for any claim, damage, or loss, (and you hereby waive any and all such claims or causes of action), arising from or relating to your (i) inability to use the services to contact emergency services, or (ii) failure to make additional arrangements to access emergency services.

The parties expressly acknowledge and agree that Cisco has set its prices and entered into this agreement in reliance upon the limitations of liability and disclaimers of warranties specified herein, which allocate the risk between Cisco and the end user and form a basis of the bargain between the parties.

14.13. Export control

You acknowledge that the Cisco Devices, Cisco Firmware, documents, technical data, and any other materials delivered under this Agreement are subject to U.S. export control laws, and may also be subject to export or import regulations in other countries. You agree to comply strictly with these laws and regulations and acknowledge that you have the responsibility to obtain any licenses to export, re-export, or import as may be required after delivery to you. You shall not, directly or indirectly, export, re-export or release the Cisco Devices and Cisco Firmware, to, or make the Cisco Devices and Cisco Firmware accessible from any jurisdiction or country to which export, re-export or release is prohibited by law, rule or regulation. In particular, butwithout limitation, the Cisco Devices and Cisco Firmware maynot be exported or re-exported (a) into any U.S. embargoed countries or (b) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Department of Commerce Denied Person's List or Entity List.

By using the Cisco Devices and Cisco Firmware, you represent and warrant that you are not located in any such country or on any such list. You acknowledge and agree that you shall strictly comply with all applicable laws, regulations and rules, and complete all required undertakings (including obtaining any necessary export license or other governmental approval), prior to operating the Cisco Devices and

Cisco Firmware, or exporting, re-exporting, releasing or otherwise making the Cisco Devices and Cisco Firmware available outside the U.S. You acknowledge and agree that Cisco has no furtherresponsibility after the initial delivery to you, and you hereby agree to indemnify and hold Cisco harmless from and against all claim, loss,liability or damage suffered or incurred by Cisco resulting from, or related to your failure to comply with all export or import regulations.

14.14. General

This Agreement shall not be governed by the 1980 U.N. Convention on Contracts for the International Sale of Goods. Rather, this Agreement shall be governed by the laws of the State of Illinois, including its Uniform Commercial Code, without reference to conflicts of laws principles. You agree to the exclusive jurisdiction and venue of the State and Federal courts in Illinois, United States.

This Agreement is the entire agreement between you and Cisco, and supersedes any other communications or advertising with respect to the Cisco Firmware and accompanying documentation. If any provision of this Agreement is held invalid or unenforceable, such provision shall be revised to the extent necessary to cure the invalidity or unenforceability, and the remainder of the Agreement shall continue in full force and effect.

This Agreement and all documents, notices, evidence, reports, opinions and other documents given or to be given under this Agreement (collectively with this Agreement, 'Documents') are and will be written in the English language only. In the event of any inconsistency between any Document in the English language and any translation of it into another language, the English-language Document shall prevail. If you are acquiring the Cisco Firmware on behalf of any part of the U.S. Government, the following provisions apply: The Cisco Firmware and accompanying documentation are deemed to be 'commercial computer software' and 'commercial computer software documentation' respectively, pursuant to DFAR Section 227.7202 and FAR 12.212(b), as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Cisco Firmware and/or the accompanying documentation by the U.S. Government or any of its agencies shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement. Any technical data provided that is not covered by the above provisions is deemed to be 'technical data-commercial items' pursuant to DFAR Section 227.7015(a). Any use, modification, reproduction, release, performance, display or disclosure of such technical data shall be governed by the terms of DFAR Section 227.7015(b).

Cisco is a trademark of Cisco Systems in the United States and worldwide.

15. Contact us

Worldwide Headquarters:

Cisco Systems Inc

81 Prospect Street

Brooklyn, New York 11201

United States of America

Tel. +1 (617) 209 -6080

Fax. +1 (866) 458-1522

info@fluidmesh.com info@cisco.com

Technical Support desk: support@fluidmesh.com

www.fluidmesh.com www.cisco.com support@cisco.com

Regional headquarters for Europe, the Middle East and Africa:

Tel. +39 02 0061 6189

Regional headquarters for the United Kingdom:

Tel. +44 2078 553 132

Regional headquarters for France:

Tel. +33 1 82 88 33 6

Regional headquarters for Australia and New Zealand:

Tel: +61 401 747 403