

Cisco Ultra-Reliable Wireless Backhaul FM10000 Gateway

Installation and Configuration Manual

(Formerly Fluidmesh)
Edition 1.7 | Firmware 1.5.0

Table of Contents

1. HAZARDOUS CONDITION WARNINGS	6
2. Reporting Mistakes And Recommending Improvements	7
3. Getting Started	8
3.1. Introduction	8
3.1.1. Cisco FM10000 Gateway	8
The Cisco FM10000 Gateway Gateway	8
Introduction	8
Product Specifications	9
Transceiver And Gateway Unit Power Consumption	9
3.2. Cisco Architecture	10
3.2.1. Overview	10
Wireless Network Architectures	10
3.2.2. Cisco Technologies	11
Prodigy	11
3.3. Cisco Network Addressing	11
3.3.1. Bridge IP Addressing	11
3.3.2. Unit Identification And Addressing	11
Mesh-Capable Gateway Identification	11
Network Addressing	13
Cisco Gateways	14
Configuring The Local Gateway Units	15
VLAN Tagging	17
Connecting And Configuring An Ethernet Edge Device	17
Cisco Gateway Devices	18
4. Hardware Installation	19
4.1. Cisco Hardware Installation	19
4.1.1. The Role Of The Gateway In A Cisco Network Architecture	19
4.1.2. Installing The Cisco FM10000 Gateway	20
Connecting To The Unit Hardware (First-Generation Devices)	20
4.1.3. Best Practice For Shielded CAT5/6 Connectors	22
4.1.4. Supplying Power To The Cisco FM10000 Gateway	22
Connecting Power To The Cisco FM10000 Gateway	23
Connecting Power Through The Device Power Ports	23
4.1.5. Rebooting The Firmware And Resetting The Unit To Factory Defaults	24
Device Firmware Reboot	24
5. Using The Cisco Partner Portal	26
5.1. Accessing The Partner Portal	26
5.2. Enabling Two-Factor Authentication For Security	27
5.3. Administering Plug-In License Codes	28
5.4. Using The RACER™ Radio Configuration Interface	29
5.5. Viewing The Technical Documentation For Your Cisco Device	29
6. Device Configuration Using The Configurator Interface	30
6.1. Software And Hardware Prerequisites	32
6.2. Accessing The Cisco FM10000 Gateway For Device Configuration	32
6.2.1. Local Access And Login For Initial Configuration	33
6.2.2. Initial Configuration With The Unit In Provisioning Mode	36
6.3. Switching Between Offline And Online Modes	42
Uploading A Device Configuration File From FM Racer	43
6.4. Viewing And Accessing The FM Monitor Settings	44
6.5. General Settings	45

6.5.1. The General Mode Window	45
Changing The Operational Mode	46
Operational Mode Settings On A Gateway Unit	46
Changing The LAN Parameters	46
6.6. Network Control	47
6.6.1. FM-QUADRO	47
FM-QUADRO For Mesh Network-Capable Devices	47
Plotting And Interpreting The Wireless Links	47
Viewing Live Data For A Radio Or Wireless Link	52
Viewing Live RSSI Data For A Wireless Link	55
Manipulating The FM-QUADRO View	56
Changing The Relative Position Of Device Icons	56
Showing KPI Values For Wireless Links	58
Showing Real-Time Color Codes For Radio Transceiver Key Performance Indicators	59
Adding An Aerial Map To The FM-QUADRO View	59
Adjusting The Transparency Of The Aerial Map View	61
Exporting A Network Representation File	61
6.6.2. Advanced Tools	62
Using The Ping Test Tool	62
Using The Bandwidth Test Tool	63
Using The Path MTU Discovery Tool	64
6.7. Advanced Settings	65
6.7.1. Static Routes	65
6.7.2. Pass Lists And Block Lists	66
6.7.3. Multicast	69
Multicast Management For Gateway Devices	69
Configuring Multicast Within A Layer-3 Network	71
6.7.4. SNMP Configuration	71
Using SNMP V2c	72
Using SNMP V3	73
6.7.5. RADIUS Configuration	75
6.7.6. NTP Configuration	78
6.7.7. L2TP Configuration	79
6.7.8. VLAN Settings	80
VLAN Configuration	80
Rules For Packet Management	81
6.7.9. Fluidity Settings	83
6.7.10. Miscellaneous Settings	84
6.8. Management Settings	85
6.8.1. View Mode Settings	85
6.8.2. Changing The Administrator Username And Password	88
6.8.3. Overwriting And Upgrading The Unit Firmware	89
6.8.4. Plug-In Management	92
6.8.5. The Device Status View	95
The Device Status Window	95
6.8.6. Saving And Restoring The Unit Settings	97
6.8.7. Resetting The Unit To Factory Defaults	99
Rebooting The Unit	99
6.8.8. Logging Out	100
6.8.9. Viewing The End-User License Agreement	100
7. Software Plug-Ins	102
7.1. Available Plug-Ins	102
7.2. Plug-In Management Procedures	106

7.2.1. Plug-In Activation	106
7.2.2. Deactivating An Active Plug-In	108
7.2.3. Reactivating A Deactivated Plug-In	110
7.2.4. Sharing License Codes And Accepting Shared License Codes	111
8. Troubleshooting	112
8.1. I Cannot Get The Log-In Screen	112
8.2. I Cannot Log In To The FM Racer Interface	112
8.3. I Forgot The Administrator Password	112
8.4. I Purchased A Cisco Device, But It Is Not Shown In FM Racer	113
8.5. I Cannot Connect My Cisco Device To The FM Racer Interface	113
8.6. I Applied Configuration Settings To The Device Using FM Racer, But I Have Lost Connection To The Device In FM Racer.	113
8.7. How Do I Connect An Existing Pre-FM Racer Device To FM Racer?	114
9. Electrical Power Requirements	115
10. Heat Radiation Data	118
11. FCC And CE Compliance Certificates	120
12. Notices And Copyright	123
13. Cisco End-User License Agreement	125
13.1. Preamble	125
13.2. Notice	125
13.3. Definitions	125
13.4. License Grant	126
13.5. Uses And Restrictions On Use	126
13.6. Open-Source Software	127
13.7. Termination	128
13.8. Feedback	128
13.9. Consent To Use Of Data	128
13.10. Warranty Disclaimer	129
13.11. Limitation Of Liability	129
13.12. Exclusion Of Liability For Emergency Services	130
13.13. Export Control	130
13.14. General	131
14. Contact Us	132

1. HAZARDOUS CONDITION WARNINGS

Like all other global technology vendors, Cisco is required to comply with all local health and government regulations in the locations in which we operate. This includes meeting radio frequency (RF) exposure limits for 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 smoke or 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.

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 FM10000 Gateway

The Cisco FM10000 Gateway Gateway

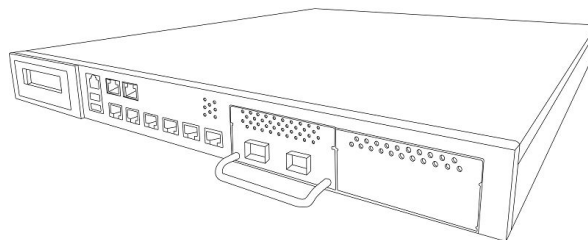


Figure 1. FM1000 gateway gateway (first generation)

Introduction

The Cisco FM10000 Gateway Gateway is an industrial-grade network switch, router and data-management center. One of its most important functions is to lower the load on a large-scale Fluidity-enabled wireless infrastructure (typically an infrastructure that is required to handle aggregate throughput of up to 10 Gigabits per second or higher) by balancing traffic from many connected Cisco transceiver units, all without impacting the performance of the connected network.

Note that two generations of the FM1000 gateway Gateway exist:

- First-generation devices have eight RJ45 Ethernet ports and two XCO/SFP ports on their front panel.
- Second-generation devices have four RJ45 Ethernet ports and four XCO/SFP+ ports on their front panel.

The first-generation Cisco FM10000 Gateway is equipped with eight Gigabit Ethernet interfaces, and is capable of being fitted with two SFP fiber-optic transceiver modules. The unit can handle up to 10 Gigabits per second of aggregate data traffic originating from a Fluidity-enabled radio

cluster. The Cisco FM10000 Gateway can also be used in conjunction with one or more Cisco FM1000 gateway Gateway Gateway units to create a hierarchical architecture for scalability purposes.

More than one unit can be installed as part of the same system to provide redundancy and improve automatic fault tolerance. Multiple units can be co-located within the same data center, or alternatively, installed in different data centers to provide geographic redundancy.

The unit is also able to connect clusters of Fluidity networks that are located within different broadcast domains. The unit acts as the aggregation point for all tunnels, and connects all portions of Fluidity infrastructure across layer 3 or wide-area networks. Roaming tasks across different clusters belonging to different broadcast domains are executed with zero hand-off time.

The unit is suitable for installation in conventional data centers, on a conventional server rack, and is capable of reliable operation in very high or low temperatures.



IMPORTANT

Fiber-optic transceiver modules and duplex fiber-optic connectors can easily be sourced as off-the-shelf parts.

If you experience difficulty in sourcing or ordering fiber-optic parts or accessories, please contact your local Cisco Networks representative for assistance.

Product specifications

For detailed product specifications, refer to the product data sheet for the Cisco FM10000 Gateway.

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

Depending on the network design and the type of components used, the Cisco FM10000 Gateway can be used to create wireless network architectures, including:

- Point-to-point (P2P) links.
- Mobility networks.

3.2.2. Cisco technologies

Prodigy

Prodigy is Cisco's proprietary implementation of the Multi-Protocol-Label-Switching (MPLS) standard.

Prodigy 2.0 offers greatly improved performance compared to Prodigy 1.0. New features include:

- Fluidity (through software plug-ins)
- Traffic engineering
- Advanced Quality of Service (QoS)



IMPORTANT

The Cisco FM10000 Gateway features exclusive support for Prodigy 2.0. The unit does **not** support Prodigy 1.0.

Also note that Prodigy 1.0 and Prodigy 2.0 are **not** compatible with each other. Do not implement the two protocol versions within the same network.

If you are expanding an existing network using a Cisco FM10000 Gateway Gateway, make sure all components that are part of the network are compatible with the Gateway by:

1. Upgrading all Cisco radio transceivers within the network to firmware version 6.5 or higher, and:
2. Configuring all Cisco radio transceivers within the network to operate using Prodigy 2.0.

3.3. Cisco network addressing

3.3.1. Bridge IP addressing

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.

3.3.2. Unit identification and addressing

Mesh-capable gateway identification

In contrast to Cisco products that can be set in *Mesh Point* and *MeshEnd* modes as needed, the Cisco FM10000 Gateway can only be set as a *Mesh End* point.

Regardless of its configuration and operating mode, every Cisco device is shipped from the factory with a unique mesh identification (ID) number (also called the Mesh ID). This number always takes the following form:

5.a.b.c

The triplet a.b.c uniquely identifies the individual physical hardware unit.

The Mesh ID number is used to identify the physical hardware units within the configurator interface that is used for configuration of the unit. Mesh ID numbers cannot be changed.

Simplified network diagrams demonstrating the relationship between a wired LAN and a linked mesh radio network containing a *mesh end* unit and *mesh point* units are shown below. [Figure 2 \(page 12\)](#) shows a typical Layer 2 network, while [Figure 3 \(page 13\)](#) shows a typical Layer 3 network.

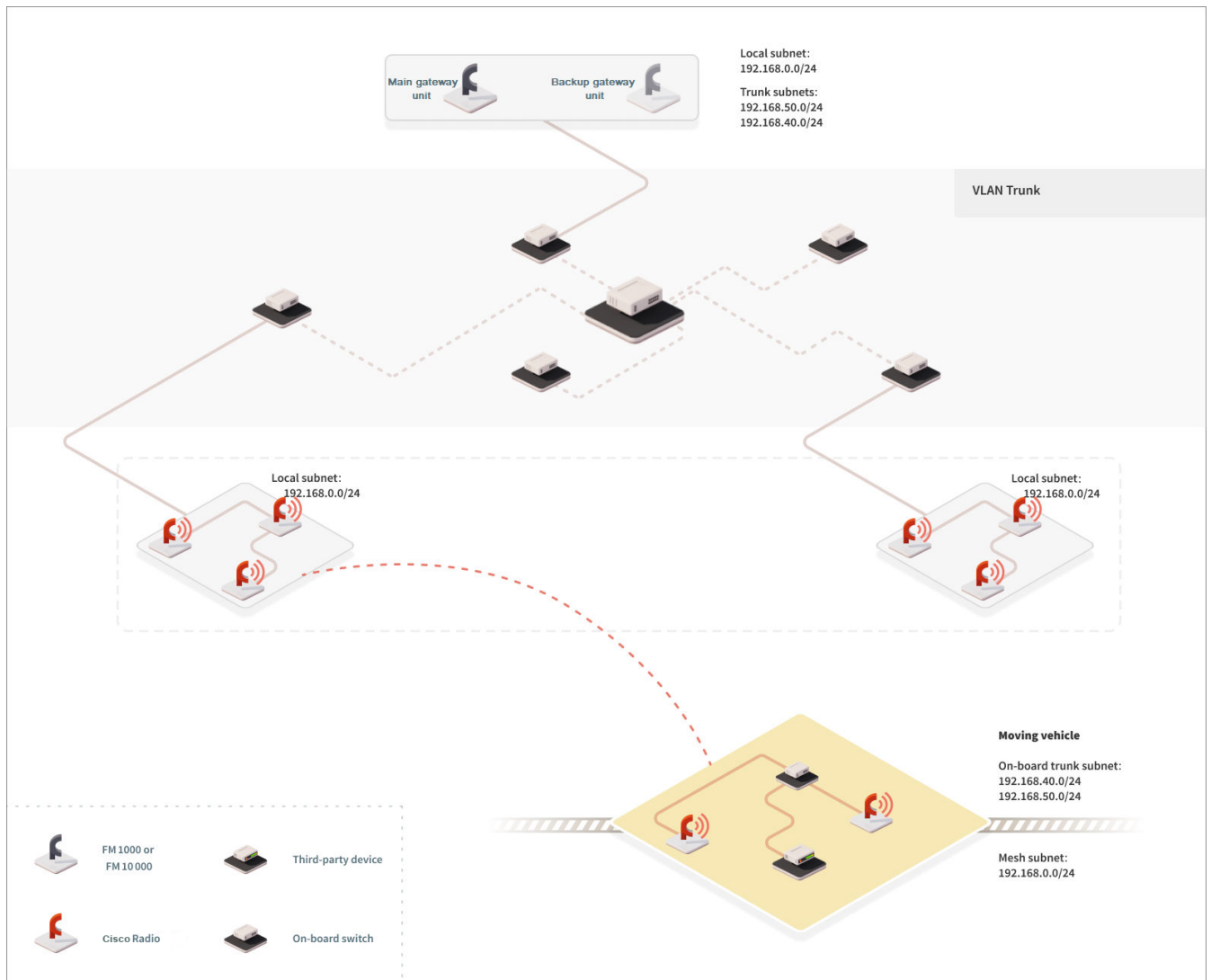


Figure 2. Cisco Network Addressing - Mesh End (Layer 2)

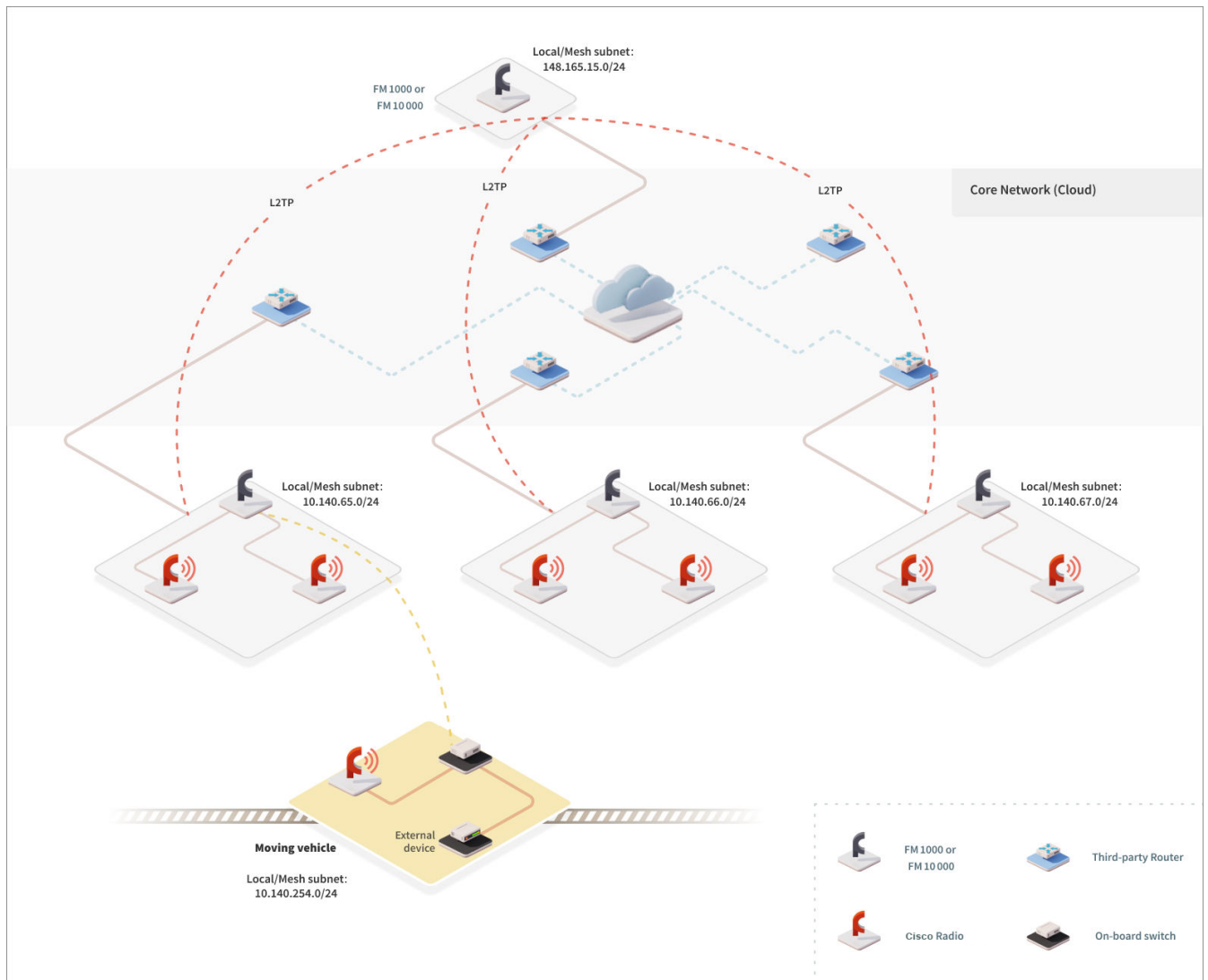


Figure 3. Cisco Network Addressing - Mesh End (Layer 3)

Network addressing

This section elaborates on the overall purpose and function of the Cisco FM10000 Gateway by explaining the role of the FM1000 Gateway (and, if included, the FM10000 Gateway) gateway device within a wireless network.

Cisco gateways

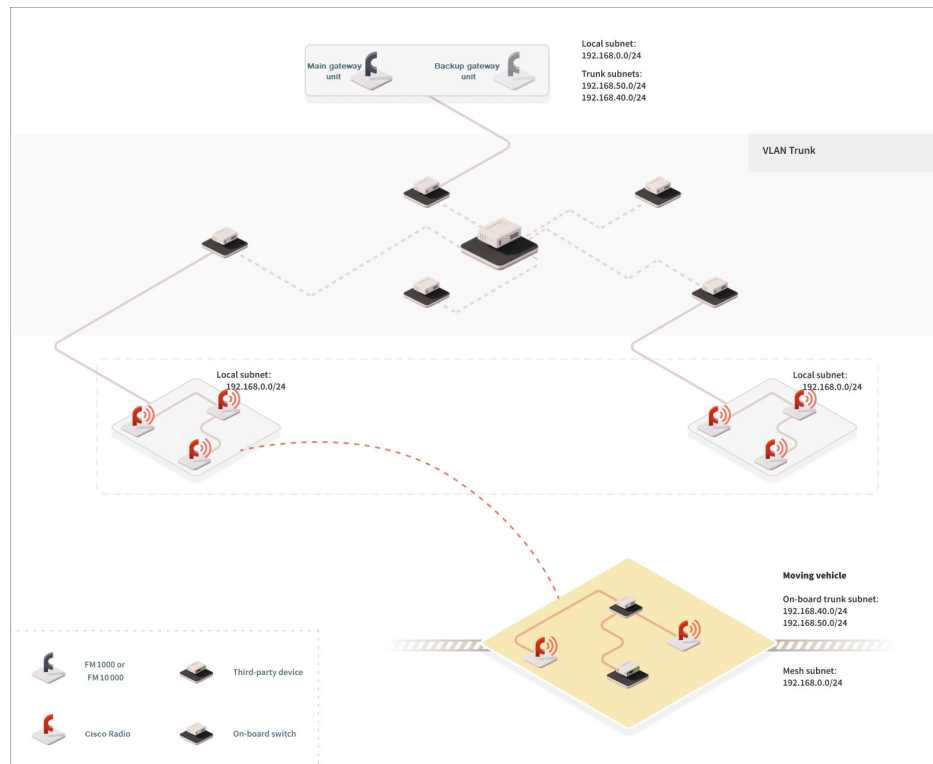



Figure 4. Hierarchical network architecture with relative IP addressing



NOTE

The system architecture shown above is to be regarded as indicative only.

The FM1000 Gateway is necessary for the cluster to function if the cluster aggregate throughput is greater than 350 Mbps, but less than 1 Gbps. If throughput is less than 350 Mbps, a Cisco radio transceiver may be used to facilitate an L2TP tunnel to the global gateway.

The FM10000 Gateway is only necessary as a global gateway if the overall aggregate throughput value is between 1 Gbps and 10 Gbps. If throughput is less than 1 Gbps, an FM1000 Gateway can replace an FM10000 Gateway as a global gateway unit.

Figure 4 (page 14) shows a typical hierarchical network architecture with relative IP addressing.

Within this schema:

- An FM1000 Gateway is used as an aggregate point within each single network cluster or broadcast domain.

- An FM1000 Gateway Gateway or FM10000 Gateway Gateway is used at data-center level to ensure IP address reachability across the entire network.
- L2TP tunnels must be enabled between each FM1000 Gateway at cluster level, and between each cluster-level FM1000 Gateway and the data-center FM1000 Gateway or FM10000 Gateway. The L2TP tunnels are used to exchange signaling information without physically modifying the pre-existing core network.

At a logical level, each network cluster becomes part of the private LAN (which the local control room is usually part of). Therefore, the Cisco gateway units and all other edge devices must be provided with a private LAN IP address, and will be accessed through that IP address.

In [Figure 4 \(page 14\)](#), the private LAN IP address classes are 10.140.65.0 / 255.255.255.224, 10.140.66.0 / 255.255.255.224 and 10.140.67.0 / 255.255.255.224. Each Cisco gateway device possesses an IP address that belongs to the relative class. Note that each IP address must be univocal within the entire network, in order to avoid address conflicts.

**NOTE**

Every Cisco hardware device has a factory-set IP address of 192.168.0.10, and a Netmask of 255.255.255.0.

In terms of IP addressing, the onboard subnets can be completely independent of the cluster subnets. In the figure above, the onboard subnet is 10.140.254.0 / 255.255.255.224. The Fluidity protocol ensures that the local IP addresses of the mobile subnets will not change while the network is roaming from one cluster to another, and that inter-cluster roaming is completely seamless.

Configuring the local gateway units

As a general rule, the core network routers and gateway units should be configured to provide full IP reachability to each network segment. This can be done by properly configuring the routing protocols that run on the core network. This task is not covered in this manual, and will be the responsibility of the person tasked with network management.

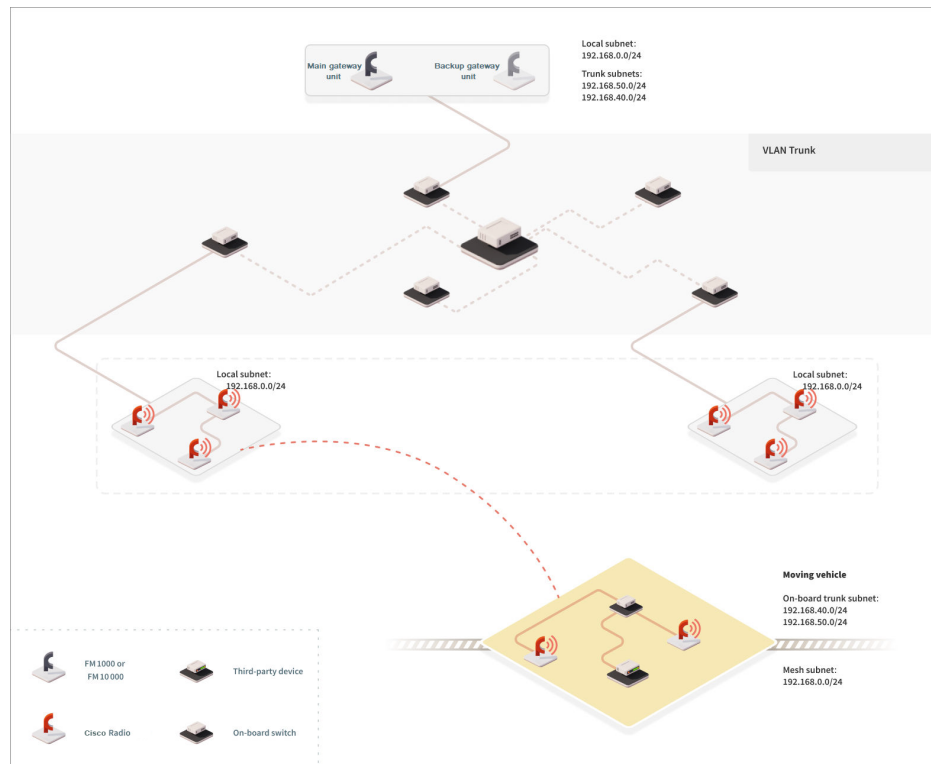


Figure 5. Gateway configuration (hierarchical network architecture with relative IP addressing)

Figure 5 (page 16) illustrates how the local subnet gateways can be configured at each network segment:

- *Network clusters (subnet gateways 10.140.65.0/27, 10.140.66.0/27 and 10.140.67.0/27):* The gateway for each Cisco device, including the FM1000 Gateway, should be the standard one for the local subnet used to reach other remote sub nets belonging to any or all of the remaining network clusters. To allow local devices to reach mobile sub nets, the local gateway should be provided with routes toward the FM1000 Gateway in the same subnet, as in the following typical example:
For subnet gateway 10.140.65.0/27, add route 10.140.254.0/27, gateway 10.140.65.10 (the IP address of the FM1000 Gateway in the subnet should be 10.140.65.10).
- *On-board layer/mobile subnet (subnet gateway 10.140.254.0/27):* For each mobile network, the local gateway should be the Cisco mobile wireless radio transceiver. The transceiver must not be provided with a default gateway, because the local gateway will change dynamically while roaming from one cluster to another.
- *Data-center network (subnet gateway 148.165.15.0/27):* It is assumed that this gateway is granted reachability to all network cluster subnets. The local gateway must also be provided with all

routes to reach the mobile subnets through the FM1000 Gateway or FM10000 Gateway Gateway, as in the following example:

For subnet gateway 148.165.15.0/27, add route 10.140.254.0/27, gateway 148.165.15.10 (this being the IP address of the FM10000 Gateway in the subnet).

VLAN tagging

Virtual LAN (VLAN) tagging is a part of the IEEE 802.1q networking standard that allows multiple switched networks to transparently share the same physical hardware whilst protecting the privacy of the data transmitted within each network.

For example, consider a company with several departments. With VLAN tagging, each department is able to run its own private logical network, but all private networks run on the same physical corporate network. Each VLAN is identified by a specific number called VLAN ID (VID). The VID is also used for tagging packets belonging to specific VLANs. Because VLANs are based on logical and not physical connections, several types of VLANs exist, based on the criteria used to logically separate networks.

Cisco Gateway devices support port-based and MAC-based VLAN tagging. The traditional VLAN scheme is port-based, where each physical Ethernet port is configured to specify membership of a particular VLAN. However, if there are requirements that individuals or devices must be segregated regardless of their physical location, MAC-based VLANs can be used, with the network is configured with an access list that maps individual MAC addresses to VLAN membership.

The Cisco VLAN implementation is compatible with the specification of the IEEE 802.1q standard, meaning that a Cisco network can interoperate with other VLAN-aware network devices. VLAN trunking between the Cisco network and the Ethernet switches is also supported, enabling carriage of VLAN membership information throughout the wireless and wired network segments.

Connecting and configuring an Ethernet edge device

Ethernet edge devices such as IP cameras and Wi-Fi access points can be connected to the Ethernet ports of the Cisco FM10000 Gateway. Such edge devices must be configured using the IP subnet scheme defined for the broadcast domain.

The default *IP subnet mask* for all Cisco devices is *192.168.0.0 / 255.255.255.0*.

The default *IP address* for all Cisco devices is *192.168.0.10 / 255.255.255.0*.

You can configure any Ethernet device manually or automatically, using a DHCP server that resides on the LAN network. The Cisco network is totally transparent to DHCP, therefore, DHCP requests and responses can be forwarded transparently across the network.



IMPORTANT

If an Ethernet-based system using multiple peripheral components is connected to the wireless network, assign each peripheral component a fixed IP address. If dynamic IP addressing is used, the components may not be accessible to third-party software that relies on the components for data input.

A typical example is a video surveillance system equipped with multiple CCTV cameras. Each camera must be assigned a fixed IP address to be accessible to the video-recording software.

Cisco gateway devices

The first-generation Cisco FM10000 Gateway features eight Ethernet ports located on the front panel of the unit. Seven ports can be used to connect the unit to different network trunks. The *Console* port can be used for configuration and maintenance purposes.

4. HARDWARE INSTALLATION

4.1. Cisco hardware installation

4.1.1. The role of the Gateway in a Cisco network architecture

The role of the FM1000 Gateway and FM10000 Gateway Gateways is to connect defined clusters of Fluidity-capable networks where each network resides in a different broadcast domain. The unit does this while allowing enhanced data-transfer speeds.

A typical Fluidity-capable network is shown in [Figure 6 \(page 20\)](#). Within this structure, an FM1000 Gateway or FM10000 Gateway Gateway acts as the aggregation point for all tunnels, connecting all portions of the infrastructure across layer-3 networks or wide-area networks.

The Gateway unit allows easy management of complex system architectures. If your network is scaled up, the unit is capable of offering the additional processing capabilities needed to enable complex data traffic management. In [Figure 6 \(page 20\)](#), each broadcast domain is considered to be a separate network with its own IP addressing schema.

The broadcast domains could be connected to the data center using any type of network medium, including fiber-optic lines and wireless backhaul. In the layout below, the Gateway unit functions as:

1. A bandwidth aggregator for the traffic flows coming from each broadcast domain. The maximum aggregated bandwidth that the FM1000 Gateway can support is 1 Gb/sec. In cases where higher levels of bandwidth must be processed, a combination of FM1000 Gateway and FM10000 Gateway Gateways can be used within the hierarchical network topology.
2. Since the trackside broadcast domains and the mobile networks on board each vehicle can be configured as different IP subnets, the Gateway unit serves as an IP reachability gateway, guaranteeing the reachability of each IP address across the entire network.

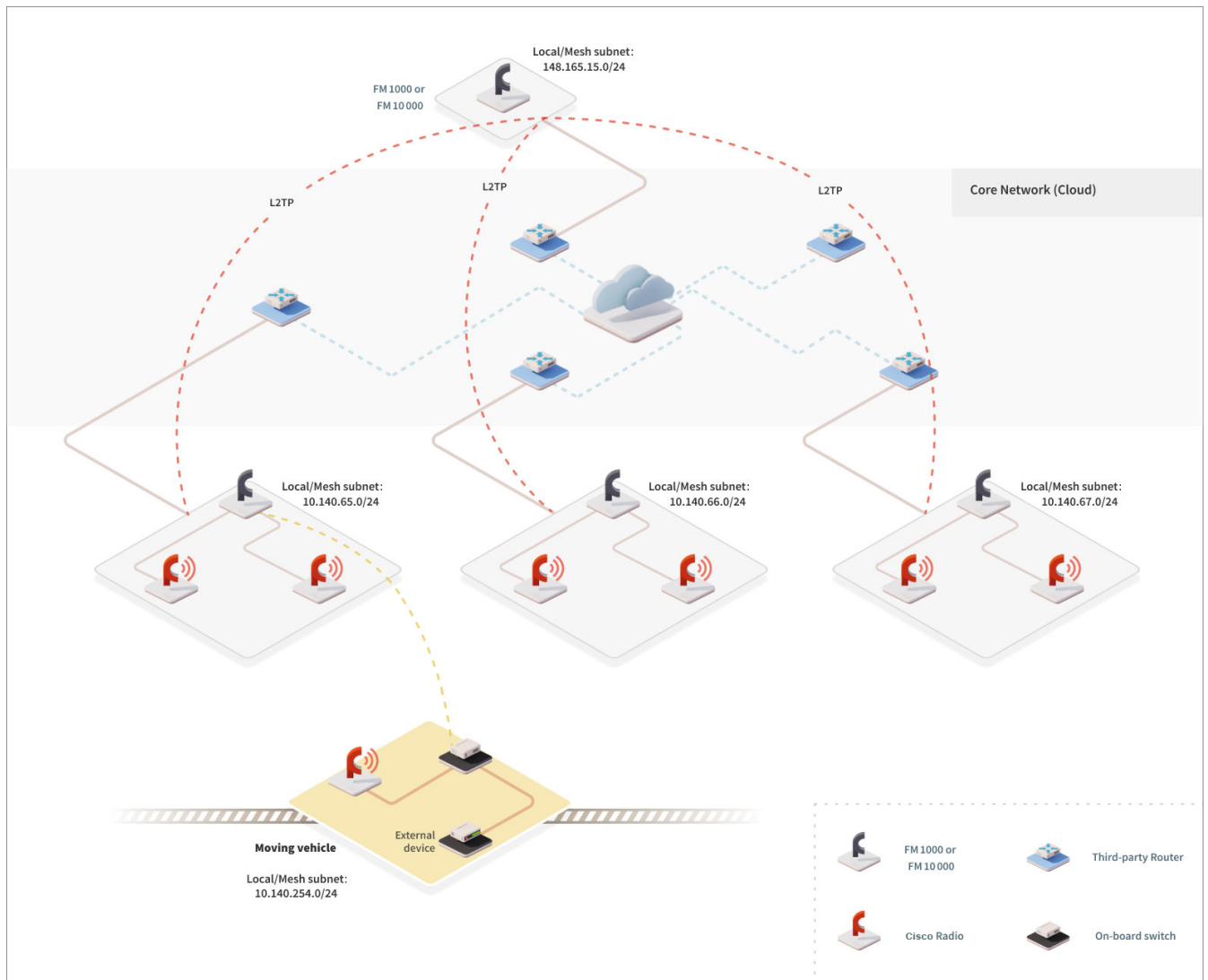


Figure 6. Typical Fluidity network architecture (FM1000 Gateway or FM10000 Gateway as aggregator)

4.1.2. Installing the Cisco FM10000 Gateway

Connecting to the unit hardware (first-generation devices)

The front panel of the unit contains controls and hardware interfaces. The panel is described in the figure below. The table that follows the figure explains the function of each relevant control and hardware interface.

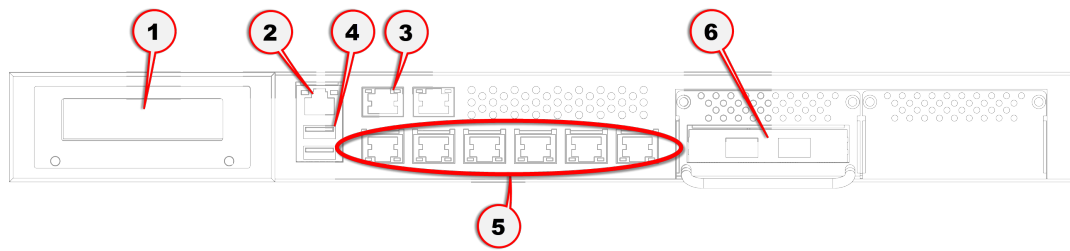


Table 3. Controls and interfaces (front panel)

Control/ interface name	Control/ interface type	Function
LCD Module (1)	LCD display	The LCD Module is reserved for future use.
Console (2)	RJ45 Ethernet port	If needed, use this port to reset the unit to its factory default configuration. For the hardware reset procedure, refer to “Rebooting the firmware and resetting the unit to factory defaults” (page 24).
MGMT (3)	RJ45 Ethernet port	Use this port to connect a computer to the unit for configuration and maintenance For instructions on how to configure the unit using the Configurator interface, refer to “Device configuration using the configurator interface” (page 30). For instructions on how to configure the unit using the FM Racer interface, refer to the Cisco Networks FM Racer user manual.
USB (4)	2x USB 1.1 / USB 2.0-compatible USB ports	If needed, use these ports to connect USB 1.1 or USB 2.0 devices to the unit.
1000M LAN ports (5)	8x RJ45 Ethernet ports	Use these ports to connect network connections to the unit. Multiple ports can be used to connect to multiple network trunks.
SFP (6, optional)	Small form-factor pluggable fiber-optic ports	The unit is equipped with two 10GbE SFP cages. Each cage is capable of accepting a 10 Gb/sec fiber-optic module for connection to a duplex fiber-optic data link. Note that the unit is not shipped with fiber-optic modules installed unless the modules have been specified as part of the purchase order. An extensive range of fiber-optic modules is available separately.

Figure 7. Cisco FM10000 Gateway (front panel)

4.1.3. 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.

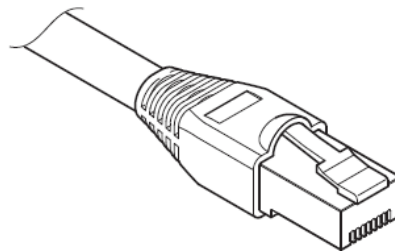


Figure 8. Shielded CAT5/6 connector

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 FM10000 Gateway, 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.

4.1.4. Supplying power to the Cisco FM10000 Gateway



CAUTION

When connecting the Cisco FM10000 Gateway 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 FM10000 Gateway, refer to **“Electrical power requirements”** (page 115).

The Cisco FM10000 Gateway can be provided with power using the following methods:

- First-generation units: AC input at 100 Vac to 240 Vac, 50 to 60 Hz (AC power supply units only).

When providing the power source for the Cisco FM10000 Gateway, remember the following important points:

Connecting power to the Cisco FM10000 Gateway

**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 the device power ports

Depending on specification, first-generation devices are equipped with a single 250W non-redundant AC power supply unit (PSU), or with multiple 275W redundant AC power supply units.

The FM10000 Gateway accepts power through one or more three-terminal power ports at the rear of the unit (**Figure 9** (page 24)).

**IMPORTANT**

The unit must be supplied with AC power (100 Vac to 240 Vac, 50 Hz to 60 Hz) only.

If more than one three-terminal power port is seen at the rear of the unit, each port must be connected to a separate source of power. If only one power port is connected to the mains electrical supply:

- The unit will function, but will be unable to switch to a backup power source if the connected PSU and/or mains electrical supply fails.
- A high-frequency, high-volume sound will be heard. This sound is not an indication of danger, but may be a source of annoyance.

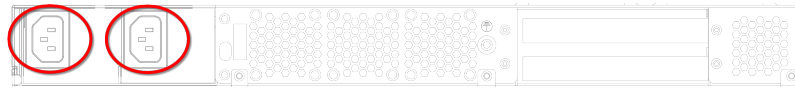


Figure 9. First-generation FM10000 Gateway (AC power connectors)

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

The Cisco FM10000 Gateway 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" \(page 99\)](#).

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

Device firmware reboot

1. Connect one end of an RJ45 Console-over-Ethernet cable to the *Console* Ethernet port on the unit (below).

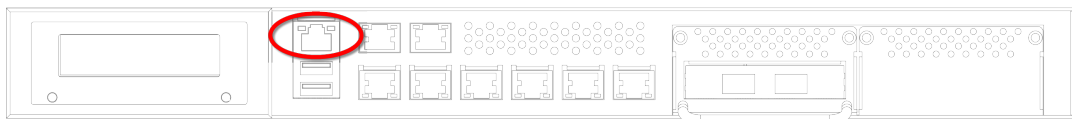


Figure 10. Console port (first-generation FM10000 Gateway devices)

2. Connect the other end of the RJ45 cable to the computer that you will use to configure the unit.
3. Set the serial port speed of the computer to 115 200 baud. For detailed instructions on how to do this, refer to the Help content supplied by your computer's manufacturer.
4. Log in to the Cisco command line interface (CLI). For detailed instructions on how to use the CLI, refer to the *Cisco Networks CLI User Manual*. The factory-set login details are as follows:
 - Username: *admin*
 - Password: *admin*
5. Enter the command *factory*, and press the Enter key.

- You will be asked if you want to reset the unit to factory defaults.
6. To proceed with the firmware reboot, type *yes*, and press the Enter key.

5. USING THE CISCO PARTNER PORTAL

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

1. Participating in Cisco E-learning
2. Using and sharing plug-in license codes for Cisco devices
3. Using the RACER™ radio configuration interface
4. Viewing the technical documentation for your Cisco devices

5.1. 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 4 \(page 26\)](#) 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 4. 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	-

5.2. 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 11 (page 27)**). Click the **Account** option.

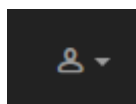


Figure 11. Partner Portal (Profile icon)

- Your portal account page will be shown.
4. Click the **Two Factor Auth.** link on the left-hand side of the web page (**Figure 12 (page 27)**).

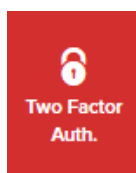


Figure 12. Partner Portal (Two Factor Auth. icon)

- 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 13 (page 28)** is a typical example of the QR code you will be shown.



Figure 13. 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.

5.3. 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 92).

5.4. Using the RACER™ radio configuration interface

RACER™ is Cisco's web-based configuration portal. It is the primary interface with which to configure Cisco radio devices.

You can operate FM Racer using any internet-connected computer with a web browser.

To access the FM Racer portal, do the following steps:

1. Log in to the Cisco Partners Portal using your login credentials.
2. Click [this link](#).

For detailed instructions on how to use the FM Racer interface, refer to the *Cisco Networks RACER™ User Manual*.



IMPORTANT

For a detailed description of the differences between FM Racer and the local Configurator interface, refer to “[Device configuration using the configurator interface](#)” (page 30).

5.5. 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.

6. 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 FM10000 Gateway can be configured by using:

- The RACER™ Radio Configuration interface, or
- 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 subsections.



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 floor calibration 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*.

6.1. Software and hardware prerequisites

To access the Configurator graphical user interface (GUI) and use the Configurator to program the Cisco FM10000 Gateway, 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 26).
 - 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.

6.2. Accessing the Cisco FM10000 Gateway 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 device in 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)

6.2.1. 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 FM10000 Gateway 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 FM10000 Gateway.
4. Connect the other end of the Ethernet cable to the *Console* LAN port on the Cisco FM10000 Gateway.
5. Manually set the computer's IP address and Netmask to be recognizable by the Cisco FM10000 Gateway. The correct settings are as follows:
 - **IP address:** Default class 'C' IP address (for example: 192.168.0.30)
 - **Netmask:** 255.255.255.0
6. Launch the computer's web browser.
7. Enter the IP address of the Cisco FM10000 Gateway 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:

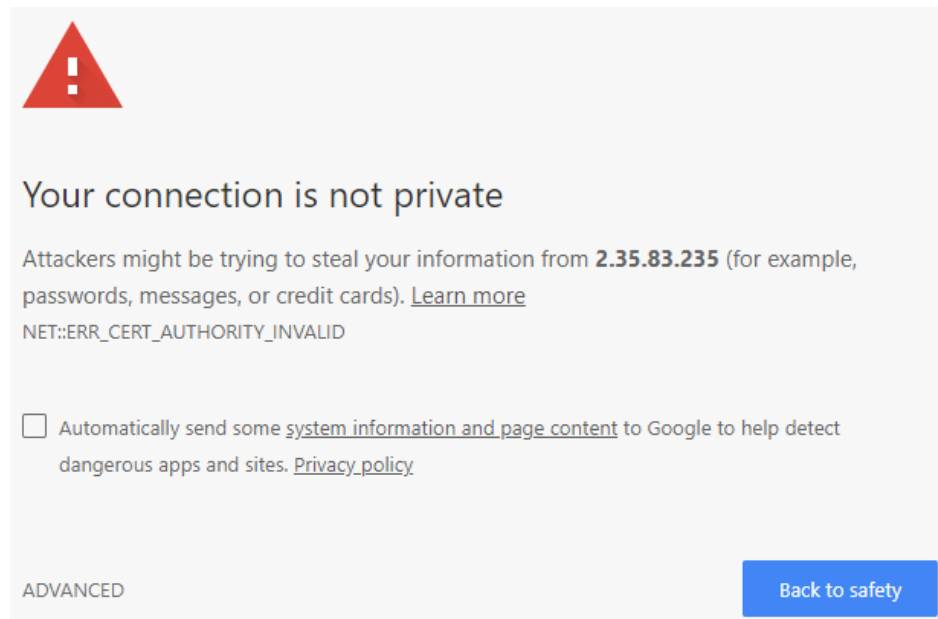



Figure 14. 'Connection Not Private' warning (Google Chrome)



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 FM10000 Gateway 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:

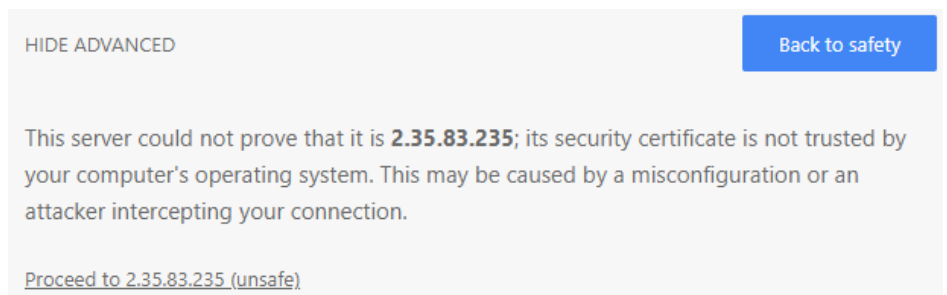


Figure 15. Security certificate warning (Google Chrome)

- b. Click **Proceed to [the URL] (unsafe)**.
 - The device login window will be shown:

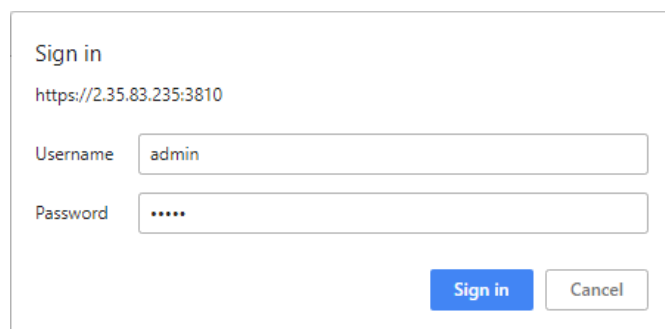
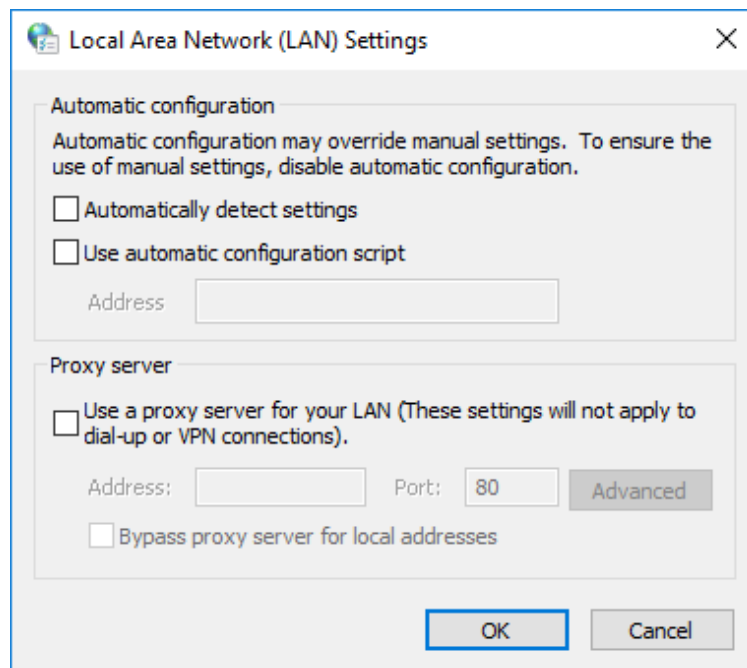


Figure 16. Cisco device login window

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 through a proxy server. To resolve the issue, do the following steps:

 1. Go to **Control Panel > Internet Options > Connections > LAN Settings**.



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 88).

6.2.2. Initial configuration with the unit in Provisioning Mode

The Cisco FM10000 Gateway cannot be operated without entering some basic configuration settings. These settings allow the unit to connect to a local network and communicate with the network hardware.

If a new unit is being configured for use for the first time, or has been reset to factory default configuration for any reason, the unit will enter *Provisioning Mode*. This mode allows you to program the unit's initial configuration settings.

If the unit is in Provisioning Mode, it will try to connect to the internet using Dynamic Host Configuration Protocol (DHCP):

- If the unit successfully connects to the internet, you can do a centralized configuration of the unit using the FM Racer interface, or do a local configuration using the Configurator interface.
- If the unit fails to connect to the internet, you must do a local configuration using the Configurator interface.



NOTE

By default, the local IP address of the unit is set as *192.168.0.10*, and the subnet mask is set as *255.255.255.0* (as shown in the **Current IP Configuration** section).

In Provisioning Mode, the unit connects to the cloud server through a WebSocket connection with 4 096-bit asymmetric encryption and verified security certificates, protecting the communication from cyber-security threats.

- Check that the unit is in Provisioning Mode by looking at the colored icon to the right of the **RACER™** tag in the upper left-hand corner of the screen ([Figure 17 \(page 37\)](#)).

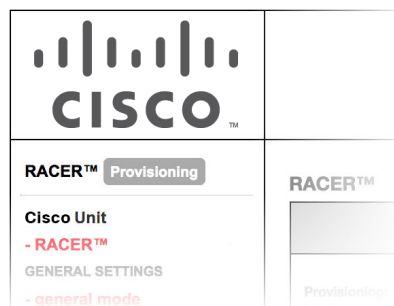


Figure 17. Racer status icon (Provisioning Mode)

- If the icon reads **Provisioning**, the unit is in Provisioning Mode. Configure the unit by doing the steps shown in this section.
- If the icon reads **Online** or **Offline**, the unit has been configured before. In this case, you must choose between two further options:
 - If you want to do a new configuration by reverting the unit to Provisioning Mode, reset the unit as shown in [“Resetting the unit to factory defaults” \(page 99\)](#).
 - If you want to change the connection settings, but keep the current configuration, change the settings as shown in [“General settings” \(page 45\)](#).

If the Cisco FM10000 Gateway is in Provisioning Mode:

- The **RACER™** dialog will be shown ([Figure 18 \(page 38\)](#)).

RACER™ Cloud connection info	
Status:	Disconnected
Current IP Configuration	
Current IP:	192.168.0.10 (fallback)
Current Netmask:	255.255.255.0

Configure DHCP to connect to RACER™	
Use this section to connect the radio to the Internet via DHCP to use RACER™ Cloud Management. Set fall-back IP settings if DHCP is not available.	
DHCP fall-back configuration	
Local IP:	<input type="text" value="192.168.0.11"/>
Local Netmask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text"/>
Local Dns 1:	<input type="text"/>
Local Dns 2:	<input type="text"/>
<input type="button" value="Save fallback IP"/>	

Figure 18. FM Racer dialog

- The unit's **Local IP** address will be set to **169.254.a.b**, where **a** and **b** are the last two parts of the unit's unique unit identification (ID) number. For example, if the unit ID number is **5.12.34.56**, the unit's IP address will be set as **169.254.34.56**.
- The unit can also be reached using the DHCP fallback IP address (*192.168.0.10/24*).
- The unit will attempt to connect to the internet using DHCP.



NOTE

DHCP is disabled when the unit leaves *Provisioning Mode*.

Make sure that the Cisco FM10000 Gateway is connected to a local network that supports DHCP. If the unit connects successfully to the internet *and* to the Partners Portal, the **RACER™ Cloud connection info** Status will be shown as **Connected** (Figure 19 (page 39)).

RACER™ Cloud connection info	
Status:	Connected
Current IP Configuration	
Current IP:	10.11.1.152 (dhcp)
Current Netmask:	255.255.0.0

Figure 19. RACER™ Cloud connection info status (Connected)

Configure the unit using either of the following methods:

- To do a centralized (online) configuration of the unit using the FM Racer interface, refer to the *Cisco Networks FM Racer User Manual*.
- To do a local (offline) configuration using the Configurator interface, refer to [“Device configuration using the configurator interface” \(page 30\)](#).

If the unit is not able to connect to the internet:

- The unit will revert to a *Fallback* state.
- The unit’s IP address will automatically be set to **192.168.0.10/24**.

If the unit connects to the internet in Provisioning Mode, but cannot connect to the Partners Portal, the unit’s IP address will automatically be set to 192.168.0.10/24. If the unit cannot connect to the Partners Portal, verify that the Partners Portal can be reached by doing the following steps:

1. Check that the Ethernet cable leading to the unit is properly connected.
2. Check that the local DNS server can resolve [this address](#).
3. Check that the local DNS server can resolve the IP address of the FM Racer Cloud server, and that the address can be reached.
4. Check the network firewall settings. Port 443 must be enabled.
5. Click [this link](#).
 - The Cisco Partners Portal page should open in your browser.
6. If the Partners Portal cannot be accessed, contact the Cisco support desk by sending an E-mail to support@cisco.com.
7. If the Partners Portal does not come back online, do a local (offline) configuration using the Configurator interface. For further information, refer to [“Device configuration using the configurator interface” \(page 30\)](#).

If the unit cannot connect to the internet in Provisioning Mode, try to connect to the internet by doing the following steps:

1. Enter alternative **Local IP**, **Local Netmask**, **Default Gateway**, **Local Dns 1** and **Local Dns 2** values as needed, using the **RACER™** dialog.
2. Click the **Save fallback IP** button (Figure 18 (page 38)).
 - The web browser will show the unit reboot dialog (Figure 20 (page 40)).

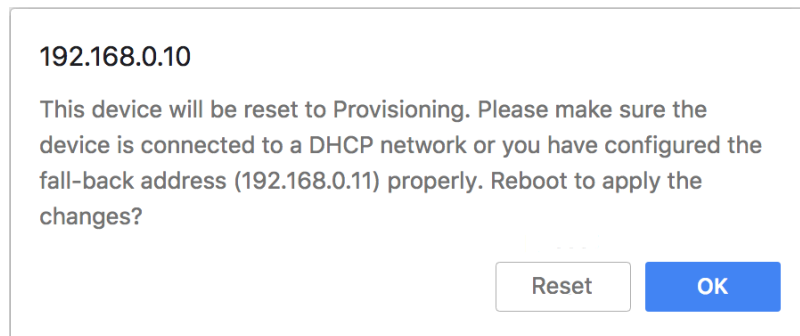


Figure 20. Unit reboot dialog (typical)

3. Click the **OK** button to proceed, or click the **Reset** button to go back to the **RACER™** dialog and adjust the settings.
 - If you click the **OK** button, the unit will reboot, but will remain in Provisioning Mode.
 - The unit will attempt to connect to the internet using the new connection values.

If the unit cannot connect to the internet using the **DHCP fall-back configuration** settings, the **RACER™ Cloud connection** info Status will be shown as **Disconnected** (Figure 21 (page 40)).



RACER™ Cloud connection info	
Status:	Disconnected 
Current IP Configuration	
Current IP:	10.11.1.152 (dhcp)
Current Netmask:	255.255.0.0

Figure 21. RACER™ Cloud connection info status (Disconnected)

Configure the unit by doing the following steps:

1. Click the **Reset to Provisioning** button at the bottom of the **DHCP fall-back configuration** section.
2. Do a local (offline) configuration using the Configurator interface. For further information, refer to **“Device configuration using the configurator interface”** (page 30).

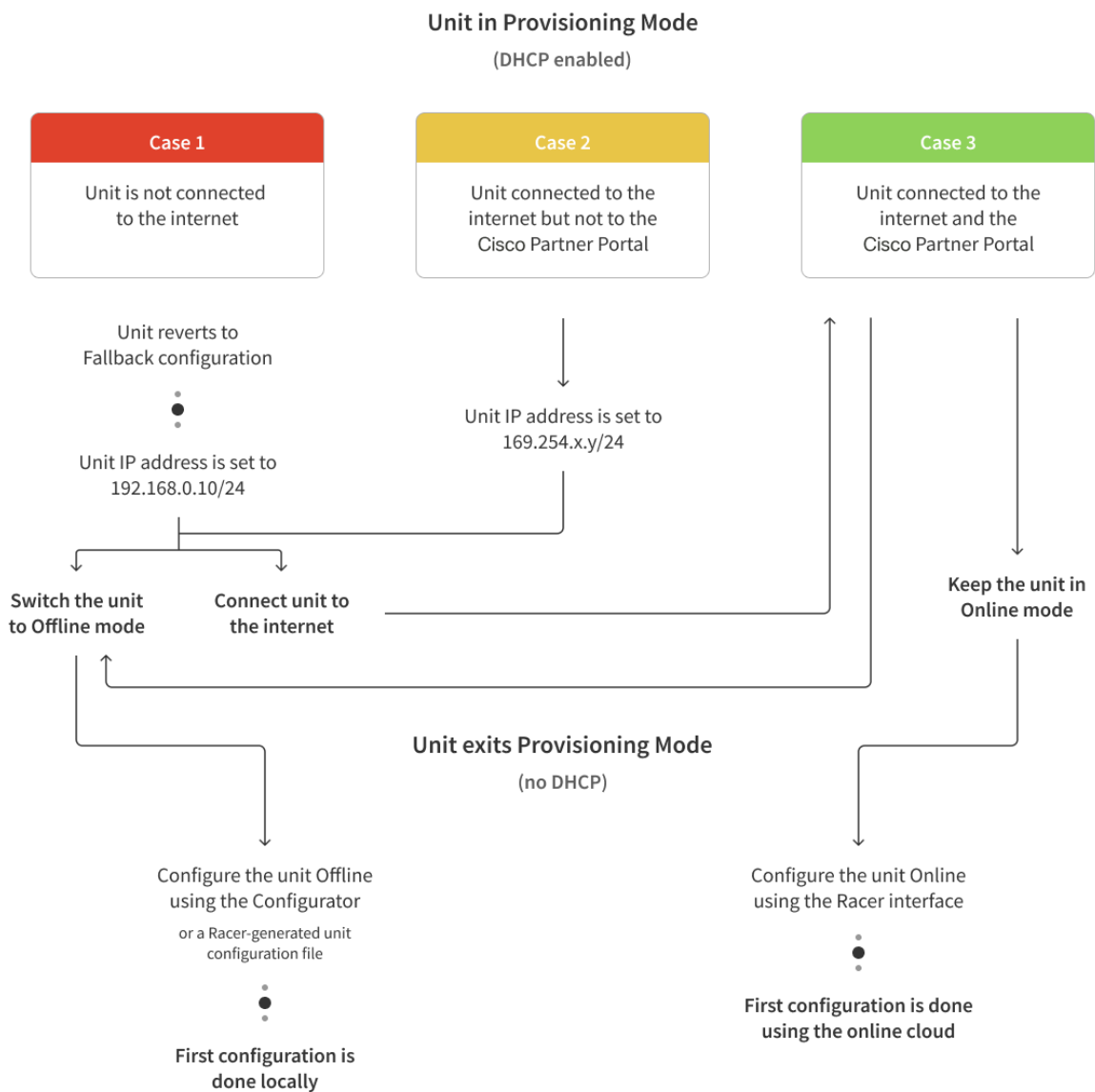
For a quick overview of the initial configuration process, refer to the flowchart below.



NOTE

Each individual Cisco radio transceiver unit has a factory-set mesh identification number that takes the form **5.w.x.y**.

If the unit's IP address is set to **169.254.x.y/24** as in Case 2 below, the values **x** and **y** represent parts **x** and **y** of the unit's mesh identification number.



6.3. Switching between offline and online modes

The Configurator interface may not be in the needed mode when you log in. To switch between *Offline* and *Online* modes, do the steps that follow:

1. Log in to the Configurator interface as shown in “[Accessing the Cisco FM10000 Gateway for device configuration](#)” (page 32).
 - The Configurator landing page will be shown ([Figure 22](#) (page 42)).

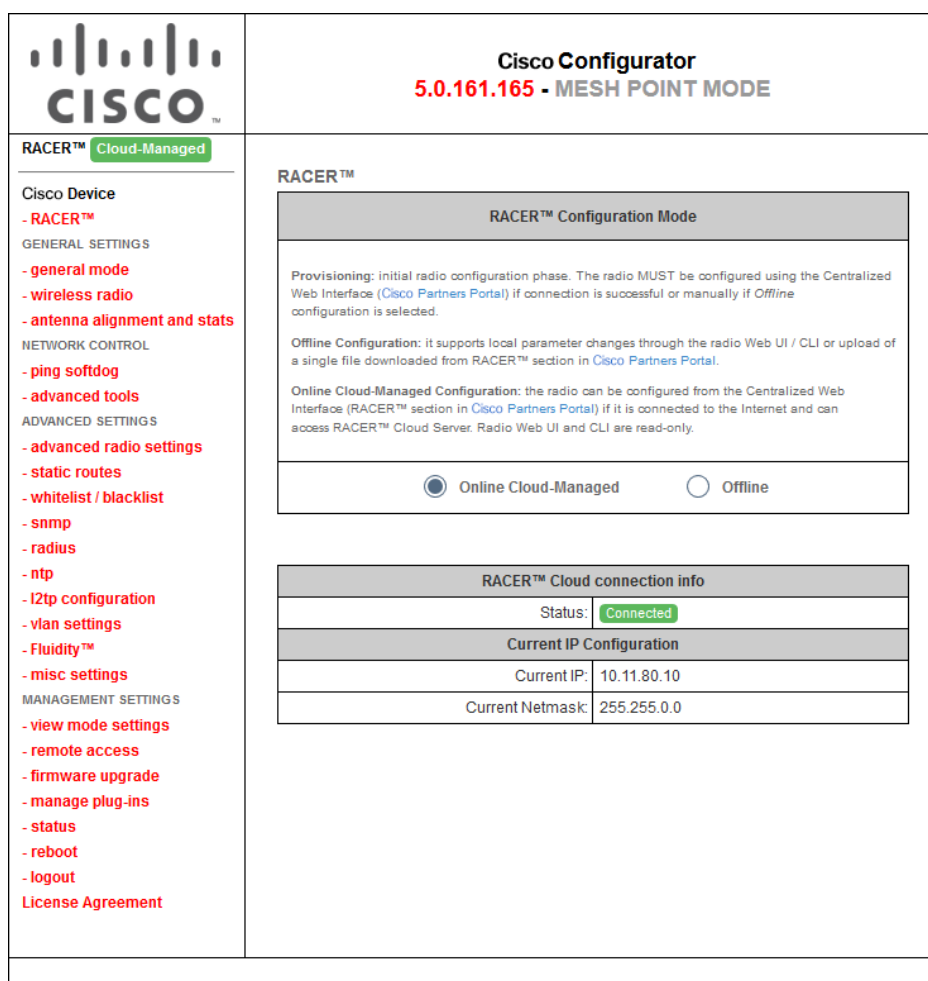


Figure 22. Cisco Configurator (landing page)

2. The lower section of the **RACER™ Configuration Mode** box has two radio buttons that show whether the unit is in **Online (Cloud-Managed)** mode, or **Offline** mode.
3. If the unit is not in the correct mode, click the **Online (Cloud-Managed)** or **Offline** radio button as needed.
 - A confirmation dialog will be shown, asking if you want to switch the unit to the chosen mode.
4. To switch the radio to the chosen mode, click the **Confirm** button.

- A ten-second countdown will be shown.
- The Configurator interface web page will reload.
- The unit will be switched to the chosen configuration mode.

Uploading a device configuration file from FM Racer

A FM Racer device configuration template contains a set of pre-configured parameters that can be customized and applied to a single Cisco device, or to a group of devices.

FM Racer configuration files use the *.FMCONF file extension.

If the unit is not connected to the Internet, you can still use the FM Racer configuration interface to define a configuration file, then upload it to the unit. This can be done in either of two different ways:

- A range of ready-made configuration templates are available from the FM Racer interface. Each template caters to a particular configuration scenario, and can be copied and modified to your needs.
- Alternatively, you can create a new, custom configuration template.

For instructions on how to copy, modify or create a configuration template using the FM Racer interface, refer to the *Cisco Networks FM Racer User Manual*.

A configuration file that has been created using the FM Racer interface must be uploaded to the unit. To upload a FM Racer configuration file, do the following steps:

1. Switch the unit to Offline mode as shown in “Switching between offline and online modes” (page 42).
2. Click the **-RACER™** link in the left-hand settings menu.
 - The Configurator landing page will be shown.
3. Click the **Choose File** button in the **Upload Configuration File** section (Figure 23 (page 43)).

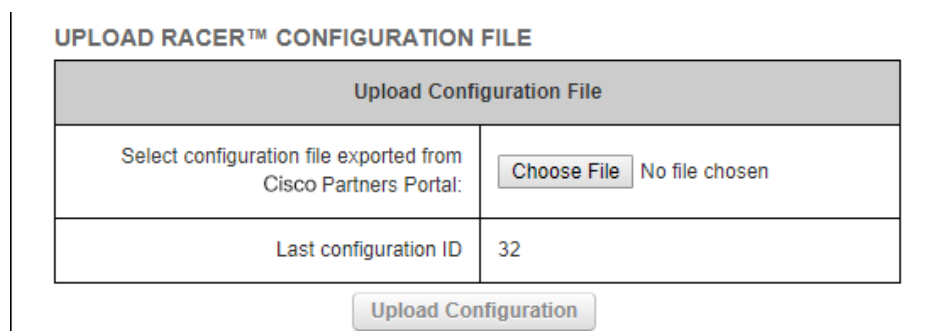


Figure 23. Configurator interface (FM Racer configuration file upload dialog)

- Find and choose the correct configuration file by following the software prompts.
4. Click the **Upload Configuration** button.
 - The configuration file will be uploaded and applied to the unit.

6.4. Viewing and accessing the FM Monitor settings

FM Monitor is Cisco's diagnostic and analysis interface. FM

Monitor is used to:

- Monitor the real-time condition of Cisco-based networks.
- Generate statistics from network history.
- Verify that device configuration settings are optimal for current network conditions.
- Detect network-related events for diagnostic and repair purposes, and generate alerts if network-related faults arise.
- Analyse network data with the goal of increasing system uptime and maintaining optimum network performance.
- Generate and back up network statistics databases for future reference.



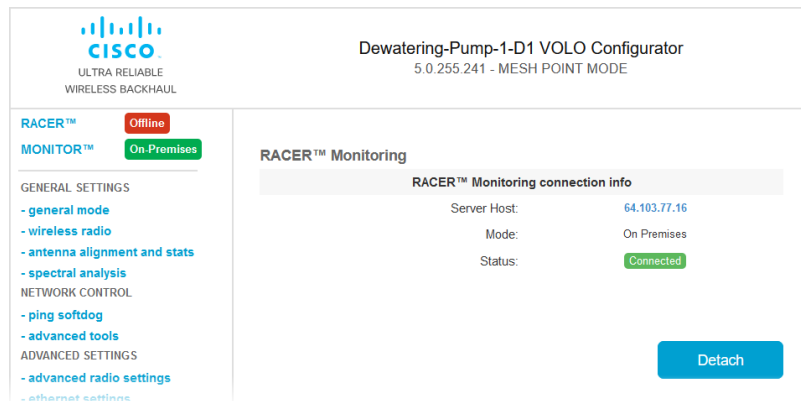
IMPORTANT

FM Monitor cannot be used to configure Cisco gateway and radio transceiver devices. Cisco devices can be configured using any of the following methods:

- You can apply a pre-created Cloud-based configuration, or do manual configuration of a device, using the FM Racer interface. For instructions on how to use the FM Racer interface, refer to the *Cisco FM Racer Configuration Manual*.
- You can manually configure a device by using the device's built-in Configurator interface. For instructions on how to use the Configurator interface, refer to the relevant section of this manual.
- You can do command-line-based manual configuration of a device by using the device's built-in CLI interface. For instructions on how to use the CLI interface, refer to the *Cisco Command-line interface user manual*.

To view and access the FM Monitor settings, do the steps that follow:

1. Log in to the Configurator interface as shown in [“Accessing the Cisco FM10000 Gateway for device configuration”](#) (page 32).
2. Click the **MONITOR™** link in the left-hand settings menu.
 - The **MONITOR™** landing page will be shown (below).



- A colored icon will be shown to the right of the red MONITOR™ link. The icon shows a summary of the current mode and status parameters:
 - If the icon is red and reads *Disabled*, the FM Monitor application has been disabled.
 - If the icon is gray and reads *On-Premises*, the FM Monitor application is enabled, but the device is not currently connected to the FM Monitor server. A possibility is that the FM Monitor server cannot be reached.
 - If the icon is green and reads *On-Premises*, the FM Monitor application is enabled and the device is connected to the FM Monitor server.
- For more information on how to use the controls and configure FM Monitor, refer to the *Cisco Radio Monitoring Dashboard Configuration Manual*.

6.5. General settings

6.5.1. The General Mode window

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

- The unit's LAN parameters.
- The shared network passphrase.

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

Mesh Settings	
"Shared Passphrase" is an alphanumeric string (e.g. "mysecurecamnet") that identifies your network. It MUST be the same for all the FMunits belonging to the same network.	
Shared Passphrase:	<input type="text" value="cisco"/>
LAN Parameters	
Local IP:	<input type="text" value="10.11.80.1"/>
Local Netmask:	<input type="text" value="255.255.0.0"/>
Default Gateway:	<input type="text" value="10.11.0.1"/>
Local Dns 1:	<input type="text" value="8.8.8.8"/>
Local Dns 2:	<input type="text"/>

Figure 24. Configurator GUI (General Mode)

Changing the operational mode

Operational mode settings on a Gateway unit

Since the Cisco FM10000 Gateway is always connected to a wired LAN backbone, it is capable of operating in *Mesh End* mode only.

A Cisco hardware device that is a junction point between the wireless network and any IP-based wired network is always set in *Mesh End* mode.

Changing the LAN parameters

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

LAN Parameters	
Local IP:	<input type="text" value="10.11.80.10"/>
Local Netmask:	<input type="text" value="255.255.0.0"/>
Default Gateway:	<input type="text" value="10.11.0.1"/>
Local Dns 1:	<input type="text" value="8.8.8.8"/>
Local Dns 2:	<input type="text"/>

**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.

6.6. Network control

6.6.1. FM-QUADRO

FM-QUADRO for mesh network-capable devices

The **FMQuadro** window contains controls to do the following functions:

- Plot all stationary wireless devices within a network, or plot all stationary wireless devices in a Fluidity network in relation to the mobile wireless-equipped vehicles from which they receive relayed traffic.
- Plot all wireless links within a network.
- Show important information about each static device, mobile device and wireless link.
- Diagnose problems with wireless links.
- Show user-configured physical positions of all Cisco Ultra-Reliable Wireless Backhaul components in a wireless network, against the background of an aerial map.

**IMPORTANT**

For detailed information on the operational concepts that govern Fluidity, refer to the *Cisco Ultra-Reliable Wireless Backhaul Fluidity Specifications* document.

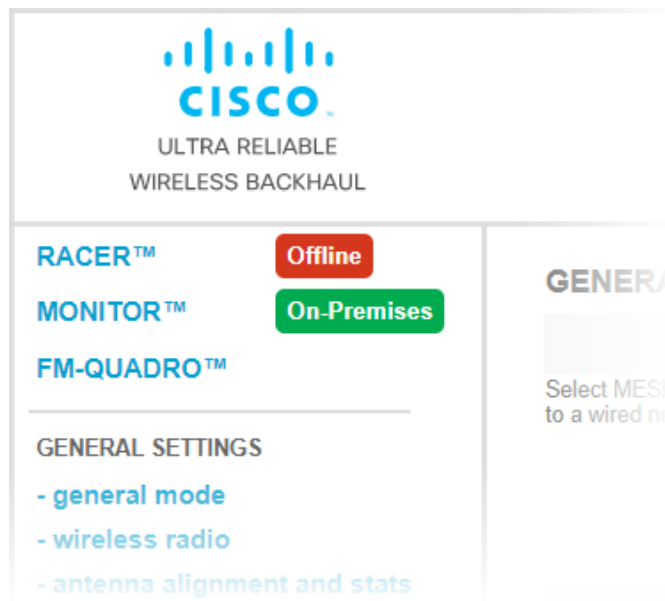
Plotting and interpreting the wireless links

**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).



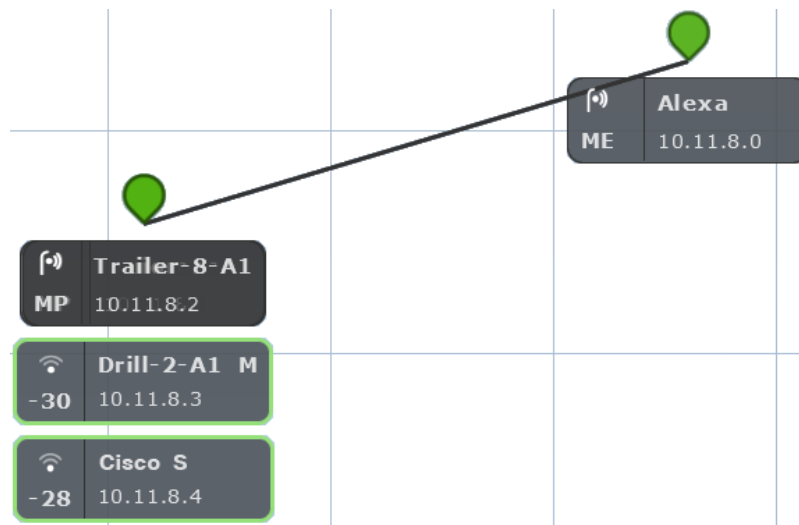
IMPORTANT

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.

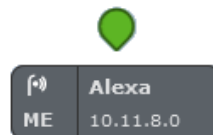
- A graphical view of the current network topology will be shown. A typical example is shown below.



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



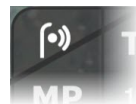
- Stationary radio transceiver icons are colored according to the performance of their data links relative to preset KPI thresholds:
 - If an icon is white, KPI checking is not currently enabled for the FM Quadro view.
 - If an icon is red, the performance of at least one link is below standard (red 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.

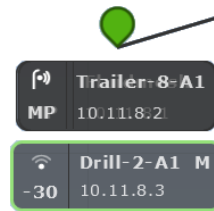


- The icon below will be shown if the device is an Ultra-reliable Wireless Backhaul Gateway device.




- The device label, corresponding to the device's name configuration parameter (*A/lexa* in the image above).
- If the device is a mobile radio transceiver, the device's Principal/Subordinate setting will be shown. A Principal device is marked M (for *Master*), and a Subordinate device is marked S (for *Slave*).
- 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 will be 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

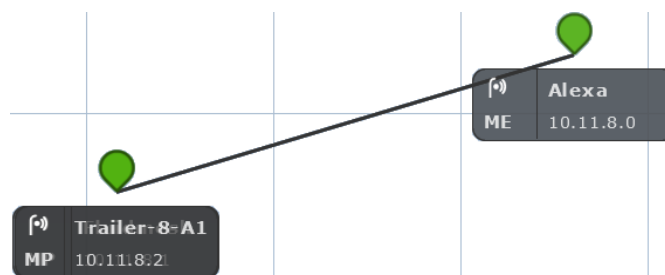
The KPI thresholds that govern tooltip border color cannot be changed.

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

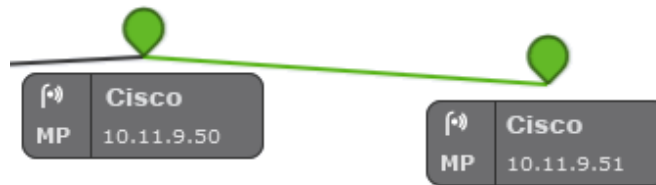
If a mobile radio connected to a stationary radio hands off to another stationary radio, the tooltip representing the mobile radio will move to a position underneath the tooltip of the connected stationary radio. If a stationary or mobile radio is disconnected from the network or cannot be reached, it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

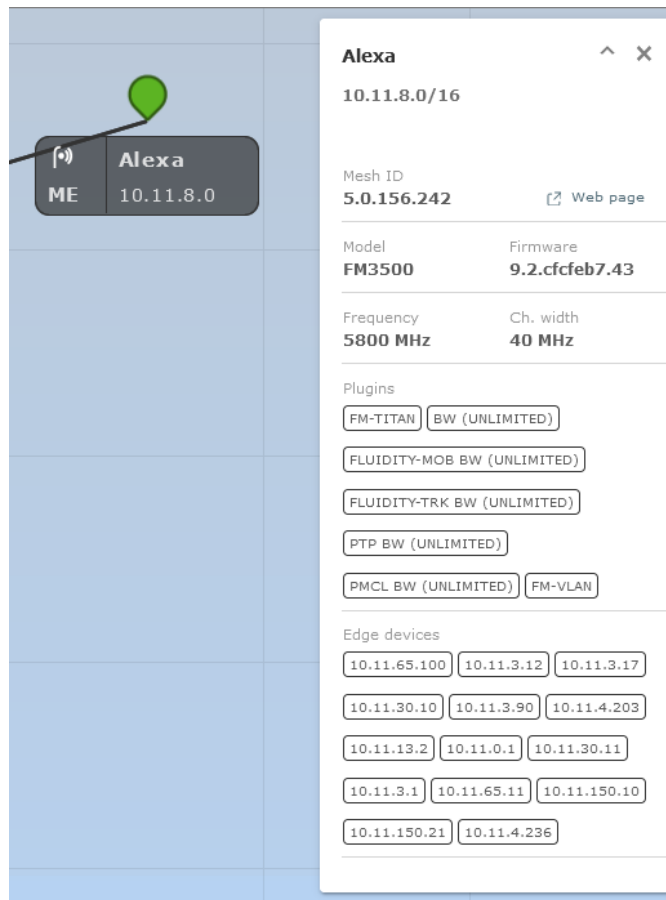
The KPI thresholds that govern wireless link line color cannot be changed.

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).

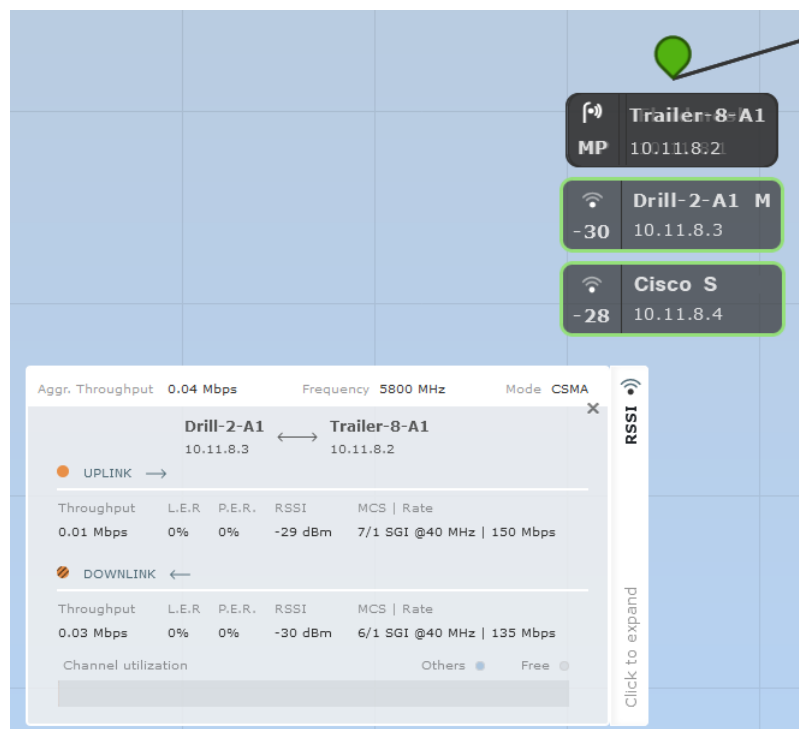


- When an information sidebar is shown for a stationary radio, the sidebar shows the following information:
 - The device name label.
 - The device's IP address and netmask (a typical example might be 10.11.8.0/16).
 - The device's Mesh ID number.
 - A **Web page** link. Clicking this link will open 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:

**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.

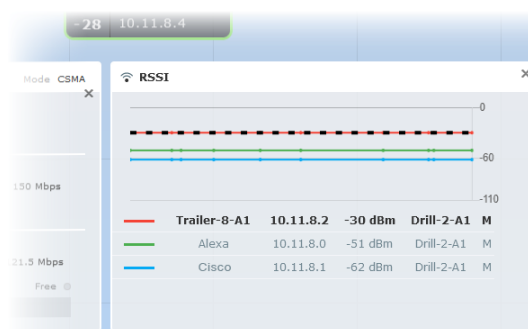
A channel-utilization bar shows uplink and downlink utilization for the selected pair of devices, as well as link utilization by other links.

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:



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” \(page 59\)](#).

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.

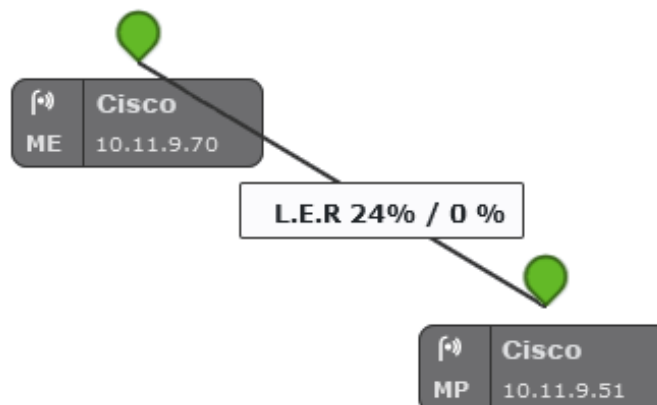
Showing KPI values for wireless links

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 $\leq 15\%$, 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 $\geq 30\%$, 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” \(page 56\)](#).

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.

6.6.2. 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 the IP address of the other unit.
2. Enter the IP address of the other unit in the **Ping (10 packets only)** field ([Figure 25 \(page 63\)](#)).

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):	<input type="text" value="2.35.83.235"/>	<input type="button" value="Run"/>
Bandwidth test (4Mbit/s UDP):	<input type="text"/>	<input type="button" value="Run"/>
Path MTU discovery:	<input type="text"/>	<input type="button" value="Run"/>
<pre> 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 </pre>		
<input type="button" value="Cancel"/>		

Figure 25. 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 the IP address of the other unit.
2. Enter the IP address of the other unit in the **Bandwidth test (4Mbit/s UDP):** field (Figure 26 (page 64)).

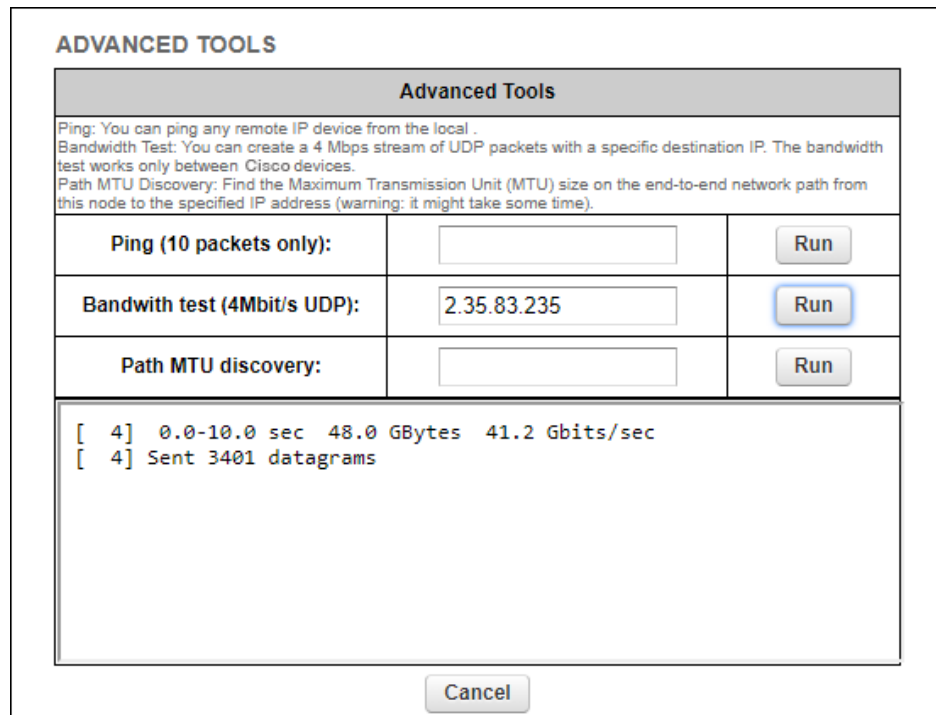


Figure 26. Advanced Tools window (Bandwidth test tool)

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 the IP address of the other unit.
2. Enter the IP address of the second unit in the **Path MTU discovery** field (Figure 27 (page 65)).

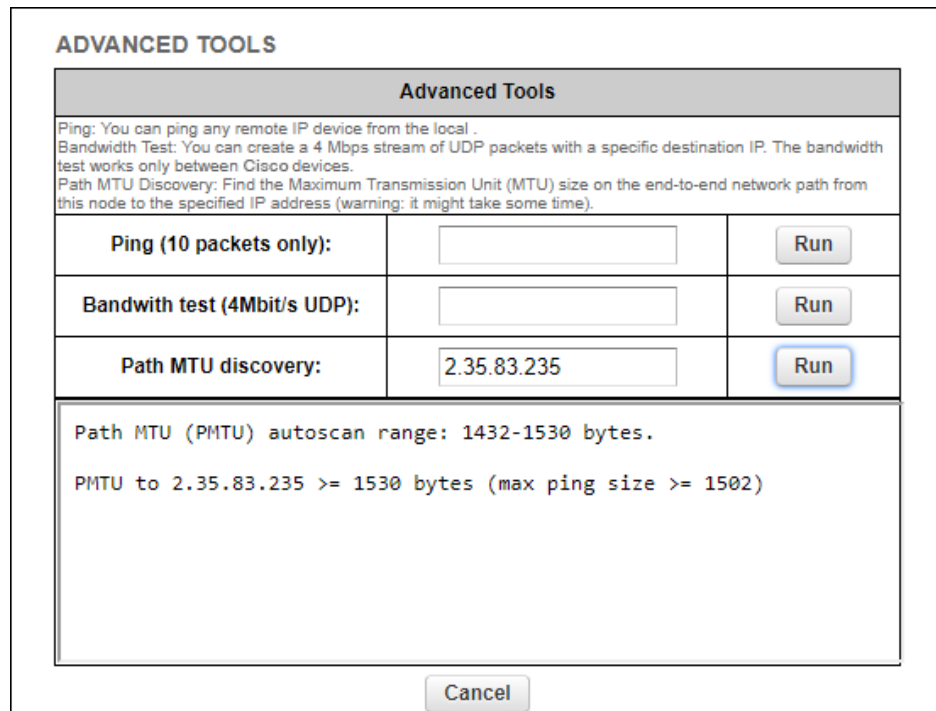


Figure 27. Advanced Tools window (Path MTU test tool)

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.

6.7. Advanced settings

6.7.1. 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 66)).

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	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="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.

6.7.2. Pass lists and Block lists

The Pass list or Block list function is a security feature that prevents fake IP addresses from intercepting or intruding on the network.

A Pass list is a group of Cisco transceivers, described as a list of linked pairs. Within the list, each transceiver unit is considered a valid hop in the routing table. If a Pass list is created, all transceiver units that are not on the Pass list are excluded from packet routing.

Conversely, a Block list is a group of Cisco transceivers that are excluded by the routing table computation, and to which data packets must not be routed. If a Block list is created, all transceiver units that are on the Block list are excluded from packet routing.



IMPORTANT

The same Pass list or Block list must be applied to all transceiver units that are part of a defined network.

Failure to use the same Pass list or Block list may cause units to incorrectly receive, or be incorrectly excluded from, network traffic.

If a Pass list or Block list is applied to a network, the list must be created as a *.CSV file before being uploaded to each unit in the network. This procedure is described below.

To create a Pass list or Block list, do the following steps:

1. Create a *.CSV file. Open the file for editing.
2. Enter the Pass list or Block list into the *.CSV file. Use the following syntax rules to create the list:

- A Pass list and Block list are mutually exclusive. Pass lists and Block lists are always separate lists, and are never combined.
- A Pass list is always expressed in the form of `<source>,<destination>,<routing priority>`, where `<source>` is the unique unit ID number of the sending unit, `<destination>` is the unique unit ID number of the receiving unit, and `<routing priority>` is a natural number with a minimum value of 0 and a maximum value of 3.



IMPORTANT

Source and *destination* values are always unit ID numbers. Do not enter a unit's IP address as a source or destination value.

The unit ID number is printed on the identification label of each unit. This number always takes the following form: **5.a.b.c**

- The *smaller* the routing priority value, the *greater* the routing priority.
 - Block list syntax is the same as shown above, except for one additional rule: Block lists do *not* include routing priority numbers.
 - Unit ID numbers and routing priority values are always separated with commas (,) and never with spaces.
 - To make sure that the packet flow is allowed or blocked in *both* directions, the unit ID numbers for each link in a Pass list or Block list must be listed in forward order *and* in reverse order.
 - If a wireless link is not specified in a Pass list, it will be assigned the lowest routing priority, but will not be completely excluded from routing.
3. **Example 1:** If you want to create a simple Pass list that includes the link between unit ID numbers 5.2.22.136 and 5.29.252.213 ([Figure 29 \(page 68\)](#)), and give the link routing priority 0 (the highest possible priority):
 - Cell A1 of the *.CSV file would contain the parameter `5.2.22.136,5.29.252.213,0`
 - Cell A2 of the *.CSV file would contain the parameter `5.29.252.213, 5.2.22.136,0`

	A	B
1	5.2.22.136,5.29.252.213,0	
2	5.29.252.213, 5.2.22.136,0	
3		

Figure 29. Sample Pass list (Example 1)

4. **Example 2:** If you want to create a Pass list that includes the links between unit ID numbers 5.2.22.136 and 5.29.252.213 (with routing priority 0), and between unit ID numbers 5.29.252.213 and 5.155.105.128 (with routing priority 1) (Figure 30 (page 68)):
 - Cell A1 of the *.CSV file would contain the parameter 5.2.22.136,5.29.252.213,0
 - Cell A2 of the *.CSV file would contain the parameter 5.29.252.213, 5.2.22.136,0
 - Cell A3 of the *.CSV file would contain the parameter 5.29.252.213,5.155.105.128,1
 - Cell A4 of the *.CSV file would contain the parameter 5.155.105.128,5.29.252.213,1

	A	B
1	5.2.22.136,5.29.252.213,0	
2	5.29.252.213, 5.2.22.136,0	
3	5.29.252.213,5.155.105.128,1	
4	5.155.105.128,5.29.252.213,1	
5		

Figure 30. Sample Pass list (Example 2)

5. **Example 3:** If you want to create a simple Block list that includes the links between unit ID numbers 5.2.22.136 and 5.29.252.213 (Figure 31 (page 68)):
 - Cell A1 of the *.CSV file would contain the parameter 5.2.22.136,5.29.252.213
 - Cell A2 of the *.CSV file would contain the parameter 5.29.252.213, 5.2.22.136

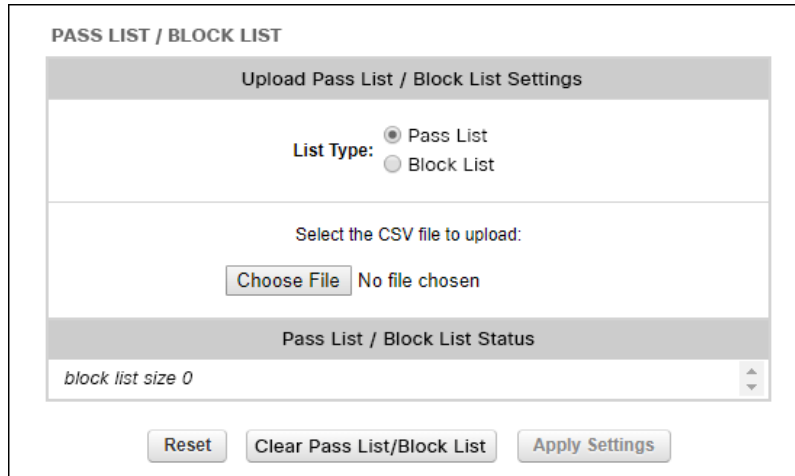
	A	B
1	5.2.22.136,5.29.252.213	
2	5.29.252.213, 5.2.22.136	
3		

Figure 31. Sample Block list (Example 3)

6. Save and close the *.CSV file.

To upload a Pass list or Block list using the Configurator interface, do the following steps:

1. Click the **Pass list / Block list** link under **ADVANCED SETTINGS** in the left-hand settings menu.



The screenshot shows a web interface titled "PASS LIST / BLOCK LIST". It features a section for "Upload Pass List / Block List Settings" with two radio buttons for "List Type": "Pass List" (selected) and "Block List". Below this is a file selection area with the text "Select the CSV file to upload:" and a "Choose File" button next to "No file chosen". A "Pass List / Block List Status" section shows "block list size 0". At the bottom are three buttons: "Reset", "Clear Pass List/Block List", and "Apply Settings".

Figure 32. Configurator (Pass list / Block list dialog)

- The **Pass list / Block list** dialog will be shown (Figure 32 (page 69)).
2. Choose the type of list to be uploaded by clicking the correct **List Type:** radio button.
 3. Click the **Choose File** button. Upload the saved *.CSV file using the upload dialog.
 - The contents of the uploaded *.CSV file will be shown in the **Pass list / Block list Status** section.

To apply the list settings contained in the *.CSV file, click the **Apply Settings** button.

To clear the Pass list or Block list settings without deleting the *.CSV file, click the **Clear Pass list or Block list** button.

To delete the Pass list or Block list *.CSV file, click the **Reset** button.

6.7.3. Multicast

Multicast management for gateway devices

Multicast is a group-communication method in which data transmissions are addressed simultaneously to more than one destination computer. Multicast transmissions can be point-to-multipoint, or multipoint-to-multipoint.

By default, if CCTV cameras and devices that operate in a similar fashion are linked to a Cisco transceiver unit operating in *Mesh Point* mode,

the unit forwards all multicast traffic generated by the cameras to the closest *Mesh End* unit in the wireless network.

Note that the Cisco FM10000 Gateway operates in *Mesh End* mode only. By default, Cisco devices operating in *Mesh End* mode do not forward multicast traffic to a wireless network. The only exceptions to this rule are universal plug and play (UPnP) and Internet Group Management Protocol (IGMP) traffic.

To redirect traffic flow from the Cisco FM10000 Gateway to a *Mesh Point* unit, all multicast flow redirection information must be specified using the Multicast settings.

To set multicast rules on the 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 33 (page 70)).

MULTICAST

Multicast routes		
List of multicast routes already present. You can manually add multicast routes. Multicast network masks and wildcard addresses are ignored in Prodigy 1.0 mode.		
Multicast Group	Destination Address	

Add a new multicast route		
Use these forms to add new static multicast routes. In the Multicast Group field it is possible to specify multicast network masks such as 224.1.1.0/24. The Destination Address field accepts the following special values: - 5.255.255.255 is a wildcard address that indicates all units of the mesh network. - 5.0.0.0 is special address that forces each unit to send multicast traffic to the primary mesh end. This is particularly useful when the mesh ends fast-failover is enabled.		
Multicast Group <input style="width: 90%;" type="text"/>	Destination Address <input style="width: 90%;" type="text"/>	<input type="button" value="add"/>

Figure 33. Multicast dialog

2. Compile the needed multicast rule. Use the following syntax rules to create the rule:
 - A multicast rule consists of two parts: a multicast group designator and a destination address.
 - The destination address consists of one or more Cisco unit mesh ID numbers, in the form **5.a.b.c**. A mesh ID number always belongs to a physical Cisco device to which the multicast traffic must be forwarded.
 - Destination-address wildcards can also be used. For example, the destination address **5.255.255.255** represents all Cisco units in the wireless network.
3. Enter the multicast group designator in the *Multicast Group* field.

4. Enter the destination address in the *Destination Address* field.
5. Click the **add** button.
 - The new multicast route will be shown in the *Multicast routes* section.

Configuring Multicast within a Layer-3 network

Within a typical Layer-3 network, consider a scenario in which Multicast traffic must be routed in both directions between Fluidity-enabled, vehicle-mounted radio transceivers, and the global gateway unit that governs data traffic through the core network.

In the case above, since different multicast groups must be used for upstream and downstream traffic, consider that group designator 224.5.5.5 is being used to route traffic from the vehicle radios to the global gateway, and that group designator 224.5.5.6 is being used to route traffic from the global gateway to the vehicle radios.

Apply the needed multicast rules by doing the steps that follow:

1. Identify all Mesh End units belonging to each subnet cluster in the Layer-3 network.
2. Enable upstream (vehicle to infrastructure) Multicast traffic by adding multicast route 224.5.5.5 / 5.a.b.c to the Mesh End unit in each subnet cluster, where 5.a.b.c is the actual Mesh ID number of the global gateway unit.



IMPORTANT

If TITAN is enabled at core network level and dual-redundant global gateway units are installed, do not enter the global gateway's actual Mesh ID number as the Destination Address. Instead, use Destination Address 5.0.0.0

3. Enable downstream (infrastructure to vehicle) Multicast traffic by adding multicast route 224.5.5.6 / 5.255.255.255 to the global gateway unit, *and* to the Mesh End unit in each subnet cluster.



NOTE

5.255.255.255 is the wildcard address for all Mesh ID destinations within the network.

6.7.4. SNMP configuration

The SNMP window can be used to configure an SNMP v2c or SNMP v3 service to run on the Cisco FM10000 Gateway.

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.



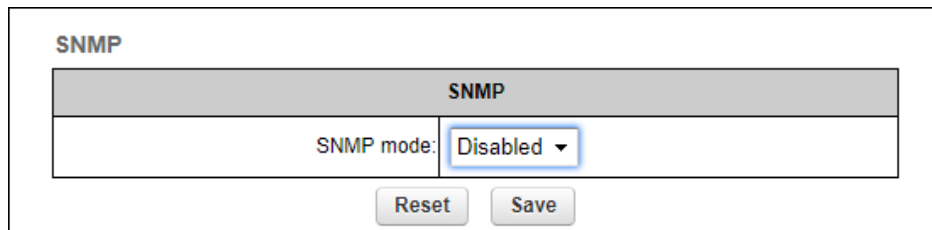
IMPORTANT

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 34 \(page 72\)](#)).



The screenshot shows the SNMP configuration dialog. At the top, the title 'SNMP' is displayed. Below the title is a table with a header row labeled 'SNMP'. The table contains one row with the label 'SNMP mode:' and a dropdown menu currently set to 'Disabled'. Below the table are two buttons: 'Reset' and 'Save'.

Figure 34. 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 35 \(page 73\)](#)).

SNMP	
SNMP mode:	v2c
Community ID:	cisco
Enable SNMP periodic trap:	<input checked="" type="checkbox"/>
Enable SNMP event trap:	<input type="checkbox"/>
NMS hostname:	
Notification period (minutes):	

Figure 35. 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 36 \(page 74\)](#)).

SNMP	
SNMP mode:	v3
SNMP v3 username:	cisco
SNMP v3 password:	*****
Show SNMP v3 password:	<input type="checkbox"/>
SNMP v3 authentication proto:	MD5
SNMP v3 encryption:	No Encryption
SNMP v3 encryption passphrase:	*****
Show SNMP v3 encryption passphrase:	<input type="checkbox"/>
Enable SNMP periodic trap:	<input type="checkbox"/>
Enable SNMP event trap:	<input type="checkbox"/>
Engine ID:	0x80001f88804879aadd5b313a99
NMS hostname:	
Notification period (minutes):	

Figure 36. 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, check the **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.

6.7.5. RADIUS configuration

The **RADIUS** window contains the controls to provide centralized authentication, authorization, and accounting management using the remote authentication dial-in user service (RADIUS) networking protocol.



IMPORTANT

Use of this window requires extensive familiarity with the RADIUS networking protocol. Do not change these settings unless there is a specific need to do so.

To change the RADIUS settings for the Cisco unit, do the following steps:

1. Enable and configure network time protocol (NTP) as shown in [“NTP Configuration” \(page 78\)](#).
2. Click the **-radius** link under **ADVANCED SETTINGS** in the left-hand settings menu.

- The **RADIUS** dialog will be shown (Figure 37 (page 76)).

RADIUS	
RADIUS Mode:	Enabled ▾
IP address / hostname:	<input type="text"/>
Port:	1812 ▾
Secondary IP address / hostname:	<input type="text"/>
Secondary Port:	1812 ▾
Secret:	<input type="text"/> <input type="checkbox"/> show
Expiration (s):	28800 ▾
Authentication	
Authentication Method:	MSCHAPV2 ▾
Username:	<input type="text"/>
Password:	<input type="text"/> <input type="checkbox"/> show
Inner Authentication Method:	none ▾
<input type="button" value="Reset"/> <input type="button" value="Save"/>	

Figure 37. Configurator GUI (RADIUS dialog)

3. Choose the RADIUS mode for the device by clicking the **RADIUS Mode** drop-down and selecting one of the following options:
 - **Disabled:** RADIUS functionality will be disabled.
 - **Enabled:** RADIUS functionality will be enabled, and the configuration options will be shown.
 - **Passthrough:** If the device is a trackside-mounted Fluidity device, this parameter can be used to simultaneously activate RADIUS device authentication, and enable RADIUS passthrough (communication between RADIUS-authenticated vehicle-mounted devices and non-authenticated trackside-mounted devices).
4. Enter the IP address or host name of the RADIUS server in the **IP address / hostname** field.
5. By default, the RADIUS port number is **1812**. Do not change the port number unless there is a specific need to do so.
6. Enter the RADIUS access password in the **Secret** field. To read the password as it is typed, check the **show** check-box.

7. By default, the RADIUS inactivity **Expiration (s)** period is 28 800 seconds (8 hours). Do not change the expiration period unless there is a specific need to do so.
8. Choose the data authentication method by clicking the **Authentication Method** drop-down and clicking the correct option. Available options are:
 - **MSCHAPV2** (Microsoft Challenge-Handshake Authentication Protocol V2)
 - **MD5** (Hash function producing a 128-bit hash value)
 - **GTC** (Generic Token Card)
 - **TTLS** (Tunneled Transport Layer Security)
 - **PEAP** (Protected Extensible Authentication Protocol)
9. Enter the personal username for access to the RADIUS server in the **Username** field.
10. Enter the personal password for access to the RADIUS server in the **Password** field. To read the password as it is typed, check the **show** check-box.
11. Available *Inner Authentication Methods* depend on which *Authentication Method* has been chosen. If applicable, choose an inner authentication method by clicking the **Inner Authentication Method** drop-down and clicking the correct option. Available options are shown in the following table:

Table 5. Available inner authentication methods (per authentication methods)

Authentication Method	Available Inner Authentication Methods
MSCHAPV2	None
MD5	None
GTC	None
TTLS	<ul style="list-style-type: none"> • PAP (Password Authentication Protocol) • CHAP (Challenge-Handshake Authentication Protocol) • MSCHAP (Microsoft Challenge-Handshake Authentication Protocol) • MSCHAPV2 • MD5 • GTC
PEAP	<ul style="list-style-type: none"> • MSCHAPV2 • MD5 • GTC

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

6.7.6. NTP Configuration

All Cisco radio transceiver units have a built-in clock.

No manual time-setting controls are provided. Instead, the unit has network time protocol (NTP) functionality that allows it to synchronize its time settings with a chosen internet time server. If the unit cannot synchronize with its primary time server, and the host name of a backup time server is entered, the unit defaults to synchronizing with the backup server.

CAUTION

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

If the same NTP settings are not applied to all units, the network may encounter timestamp conflicts and/or equipment malfunctions.

To change the NTP settings, do the following steps:

1. Click the **-ntp** link under **ADVANCED SETTINGS** in the left-hand settings menu.
 - The **NTP** dialog will be shown ([Figure 38 \(page 78\)](#)).

NTP - Network Time Protocol

NTP	
Enable NTP:	<input checked="" type="checkbox"/>
NTP server hostname:	<input type="text" value="time.windows.com"/>
Secondary NTP server (optional):	<input type="text" value="time.nist.gov"/>
Select Timezone:	<input type="text" value="Europe/Paris"/>

Figure 38. Configurator GUI (NTP dialog)

2. Enable NTP synchronization by checking the **Enable NTP** checkbox.
3. Enter the host name of a chosen primary NTP server in the **NTP server hostname:** field.

IMPORTANT

The NTP server host names shown in [Figure 38 \(page 78\)](#) are for reference purposes only. Your company policy may dictate that you use one or more specific time servers.

4. If needed, enter the host name of a chosen secondary NTP server in the **Secondary NTP server (optional):** field.
5. Select the time zone in which the unit is installed by clicking the **Select Timezone:** drop-down menu and clicking the correct time zone option.
6. Save the NTP settings by clicking the **Save** button. Alternatively, clear the settings by clicking the **Reset** button.

6.7.7. L2TP configuration

Layer 2 Tunneling Protocol (L2TP) functionality allows Cisco radio transceivers to support integration with virtual private networks (VPNs).

Cisco hardware devices are shipped from the factory with L2TP functionality disabled. To change the unit's L2TP settings, do the following steps:

1. Click the **-l2tp configuration** link under **ADVANCED SETTINGS** in the left-hand settings menu.

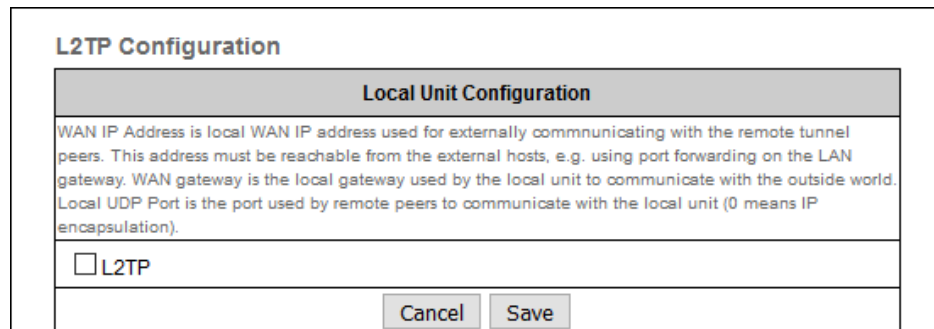


Figure 39. Configurator GUI (L2TP Configuration dialog)

- The **L2TP Configuration** dialog will be shown ([Figure 39 \(page 79\)](#)).
2. To enable L2TP functionality for the unit, check the **L2TP** checkbox.
 - The L2TP configuration settings window will be shown.
3. When the L2TP configuration has been set, save the settings by clicking the **Save** button. Alternatively, clear the settings by clicking the **Reset** button.




IMPORTANT

A detailed description of L2TP configuration methods is beyond the scope of this manual. For detailed instructions on how to set the L2TP configuration, refer to the *Cisco Networks L2TPv3 Configuration Manual*.

6.7.8. VLAN settings

VLAN configuration


The **VLAN SETTINGS** window contains controls to connect the Cisco FM10000 Gateway 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 FM10000 Gateway 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 smart VLAN packet management, refer to the **“Rules for packet management”** (page 81) 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 40 (page 80)).

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:	<input type="checkbox"/>
Management VLAN ID:	<input type="text" value="1"/>
Native VLAN ID:	<input type="text" value="1"/>

Figure 40. 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. Check the **Enable VLANs** check-box.
4. 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 must be used on all Cisco devices that are part of the same mesh network.

5. Enter the native identification number (the VLAN ID implicitly assigned to untagged packets received on trunk ports) in the **Native VLAN ID:** field.
6. 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

Parameter	Default value
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)	
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 <i>Management VLAN</i> 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

6.7.9. Fluidity settings

Fluidity™ is Cisco's proprietary trackside and vehicle-to-ground data transfer protocol for video, voice and data communication.

The **FLUIDITY** window contains controls to change the unit's Fluidity settings. To change the settings, do the following steps:

1. Click the **-Fluidity™** link under **ADVANCED SETTINGS** in the left-hand settings menu.
 - The **FLUIDITY** dialog will be shown (Figure 41 (page 83)).

FLUIDITY

Fluidity Settings	
<p>The unit can operate in 3 modes: Infrastructure, Infrastructure (wireless relay), Vehicle. The unit must be set as Infrastructure when it acts as the entry point of the infrastructure for the mobile vehicles and it is connected to a wired network (backbone) which possibly includes other Infrastructure nodes. The unit must be set as Infrastructure (wireless relay) ONLY when it is used as a wireless relay agent to other Infrastructure units. In this operating mode, the unit MUST NOT be connected to the wired network backbone as it will use the wireless connection to relay the data coming from the mobile units. The unit must be set as Vehicle when it is mobile. Vehicle ID must be set ONLY when the unit is configured as Vehicle. Specifically, Vehicle ID must be a unique among all the mobile units installed on the same vehicle. Unit installed on different vehicles must use different Vehicle IDs. The Network Type field must be set according to the general network architecture. Choose Flat if the mesh and the infrastructure networks belong to a single layer-2 broadcast domain. Use Multiple Subnets if they are organized as different layer-3 routing domains.</p>	
Fluidity	<input checked="" type="checkbox"/> Enable
Unit Role:	Infrastructure ▼
Network Type:	Flat ▼

Figure 41. Configurator GUI (FLUIDITY dialog for gateway devices)

2. Cisco radio transceivers are shipped from the factory with Fluidity functionality disabled. Enable Fluidity functionality by checking the **Fluidity** check-box.



IMPORTANT

The **Unit Role:** drop-down is set to **Infrastructure** mode, and cannot be changed.

3. The network type must be set in accordance with the general network architecture. Select the correct network type designation for the unit by clicking the **Network Type:** drop-down and clicking the correct option from the list below:
 - **Flat:** Choose this setting if the wireless mesh network and the infrastructure network both belong to a single layer-2 broadcast domain.

- **Multiple Subnets:** Choose this setting if the wireless mesh network and the infrastructure network are organized as separate layer-3 routing domains.
4. Save the Fluidity settings by clicking the **Save** button. Alternatively, clear the settings by clicking the **Reset** button.

6.7.10. Miscellaneous settings



IMPORTANT

Support for FIPS, CANBUS, PROFINET and QNET are only available if the corresponding plug-ins are installed. If the corresponding plug-in is not installed, the check-box for the relevant option will not be available.

The following plug-ins are needed to activate these features:

- CANBUS: *FM-CANBUS*
- PROFINET: *FM-PROFINET*
- QNET: *FM-QNET*

Note that FIPS support is not available for the FM1000 Gateway and FM10000 Gateway.

Contact your Cisco Networks representative for details.

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

- The device name, as used to identify the Cisco FM10000 Gateway within the FMQuadro network map and to other Cisco utilities.
- The unit's controller area network (CANBUS) support settings (if applicable).
- The unit's process field net (PROFINET) support settings (if applicable).
- The unit's Neutrino Qnet (QNET) support settings (if applicable).

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 42 (page 85)).

MISC SETTINGS	
Device	
Name:	<input type="text" value="Cisco"/>
PROFINET Settings	
Enable PROFINET:	<input type="checkbox"/>
QNET Settings	
Enable QNET:	<input type="checkbox"/>

Figure 42. 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. To enable CANBUS support for the unit, make sure the FM-CANBUS plug-in is installed, then check the **Enable CANBUS:** check-box.
4. To enable PROFINET support for the unit, make sure the FM-PROFINET plug-in is installed, then check the **Enable PROFINET:** check-box.
5. To enable QNET support for the unit, make sure the FM-QNET plug-in is installed, then check the **Enable QNET:** check-box.
6. Save the miscellaneous settings by clicking the **Save** button. Alternatively, clear the settings by clicking the **Reset** button.

6.8. Management settings

6.8.1. 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 43 (page 86)).

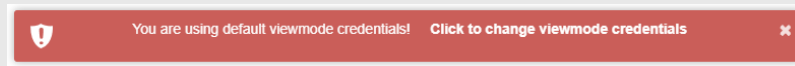


Figure 43. Default credentials notification banner

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 44 (page 86)).

Viewmode Credentials	
View Mode Username:	<input type="text" value="user"/>
View Mode User Password:	<input type="password" value="••••••••"/>
Show Password:	<input type="checkbox"/>

Figure 44. 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 FM10000 Gateway for device configuration](#)” (page 32) for more information.
2. Click the **-view mode settings** link under **MANAGEMENT SETTINGS** in the left-hand settings menu ([Figure 45 \(page 87\)](#)).

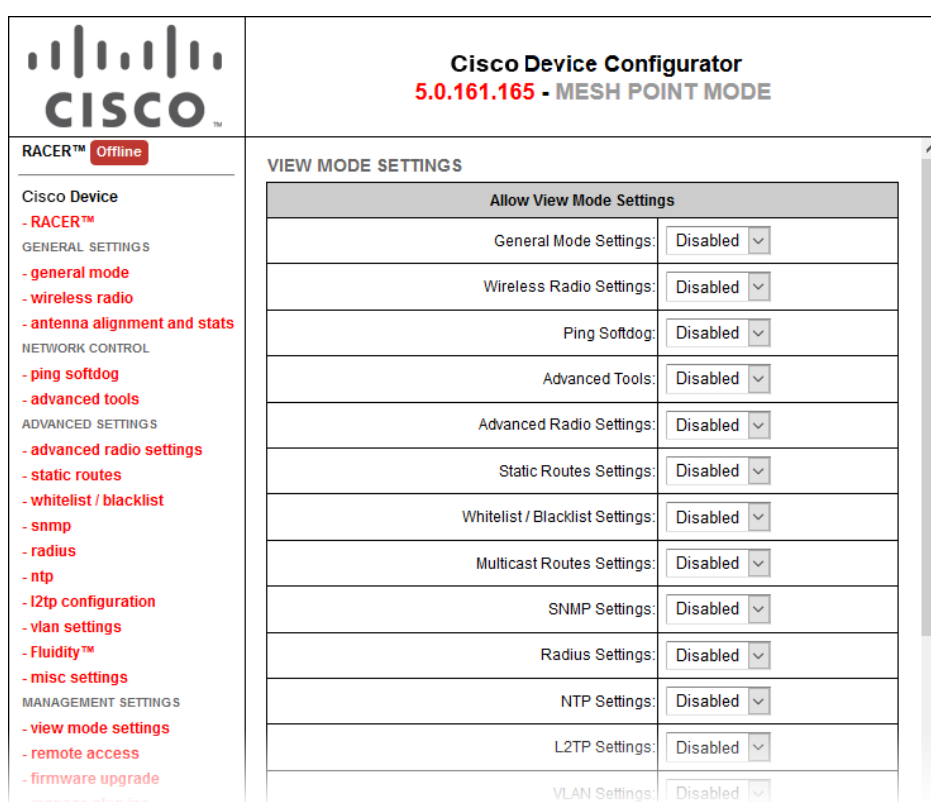


Figure 45. Configurator GUI (VIEW MODE SETTINGS dialog)

- 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.

6.8.2. 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 46 \(page 88\)](#)).

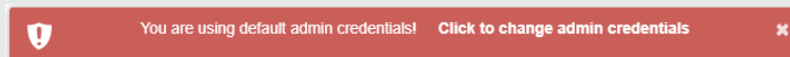


Figure 46. Default admin credentials notification banner

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 47 \(page 89\)](#)).

CHANGE USERNAME AND PASSWORD

Change Username and Password

Username:	<input type="text" value="admin"/>
Old password:	<input type="password"/>
New password:	<input type="password"/>
Confirm new password:	<input type="password"/>
Show password:	<input type="checkbox"/>

Figure 47. 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” \(page 99\)](#) for more information.

6.8.3. Overwriting and upgrading the unit firmware



IMPORTANT

The instructions in this section apply to first-generation FM1000 gateways only.

For instructions on how to overwrite and upgrade the unit firmware on second-generation FM1000 gateways, refer to ???.

The **FIRMWARE UPGRADE** window contains controls to overwrite the device firmware of the Cisco FM10000 Gateway, 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 needs to 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 network is 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 FM10000 Gateway for device configuration](#)” (page 32).
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 97).
6. Click the **-firmware upgrade** link under **MANAGEMENT SETTINGS** in the left-hand settings menu.
 - The **FIRMWARE UPGRADE** dialog will be shown ([Figure 48 \(page 91\)](#)).

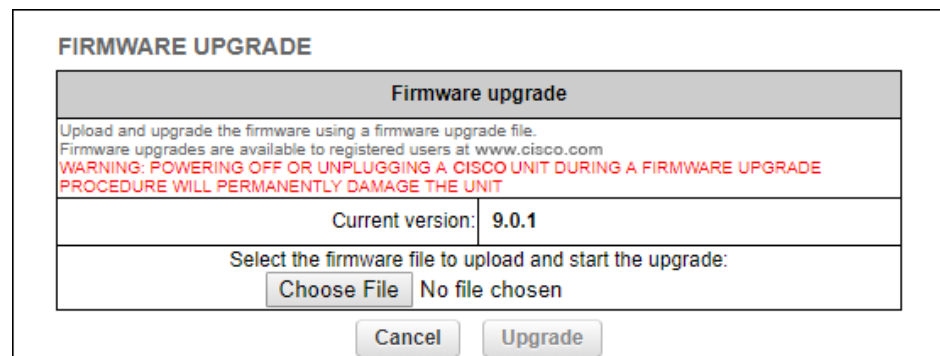


Figure 48. Configurator GUI (typical FIRMWARE UPGRADE dialog)

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.

6.8.4. Plug-In management



IMPORTANT

For a complete list of software plug-ins that are currently available for the Cisco FM10000 Gateway, refer to “[Available plug-ins](#)” (page 102).

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.
- 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 49](#) (page 93)).

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 49. 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 50 \(page 94\)](#)). A countdown timer shows how much Demo time remains.

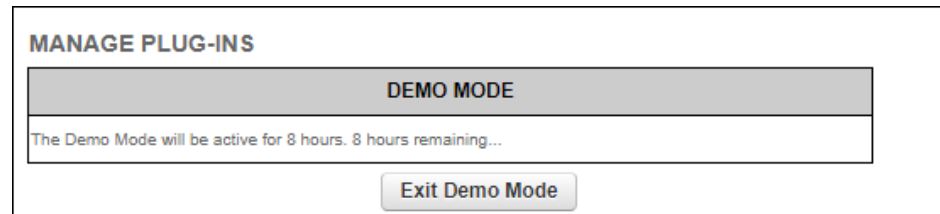


Figure 50. MANAGE PLUG-INS dialog (Demo Mode activated)

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” \(page 106\)](#).

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” \(page 106\)](#).

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.

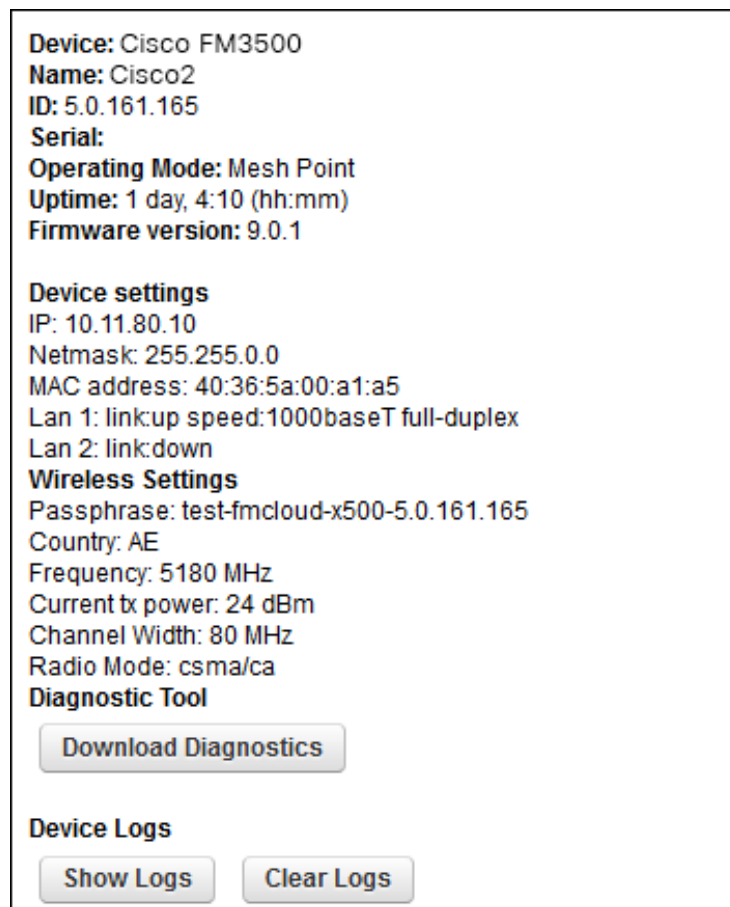
6.8.5. The device status view

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).



The screenshot shows a status dialog box with the following information:

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

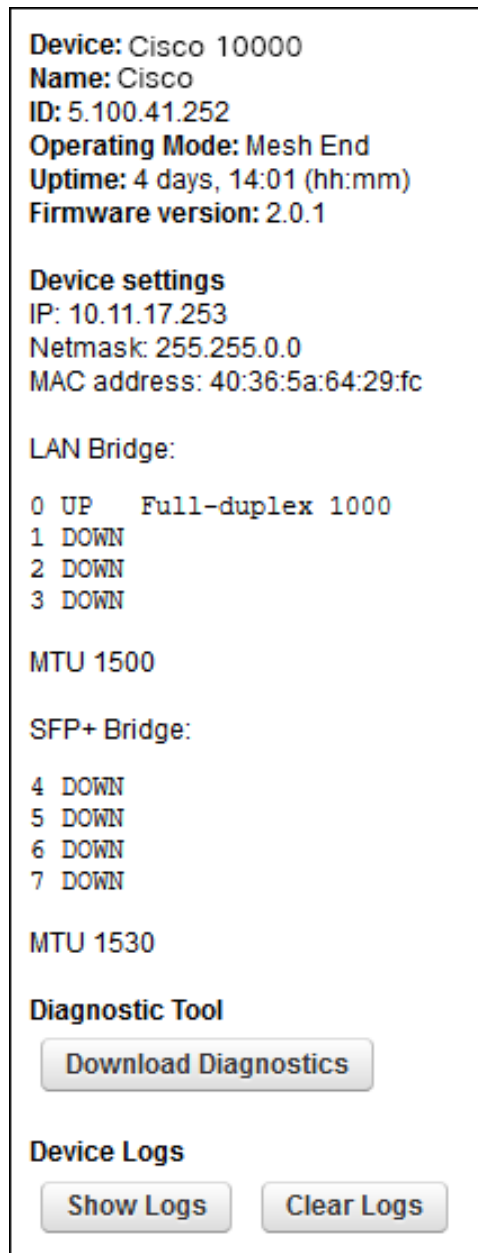
Device settings
IP: 10.11.80.10
Netmask: 255.255.0.0
MAC address: 40:36:5a:00:a1:a5
Lan 1: link:up speed:1000baseT full-duplex
Lan 2: link:down

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 51. 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

[Download Diagnostics](#)

Device Logs

[Show Logs](#) [Clear Logs](#)

Figure 52. 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 <timestamp>*: Possible duplicate IP address 'A' has migrated from MAC address 'X' to MAC address 'Y', at the time shown.

6.8.6. 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 53 \(page 98\)](#)).

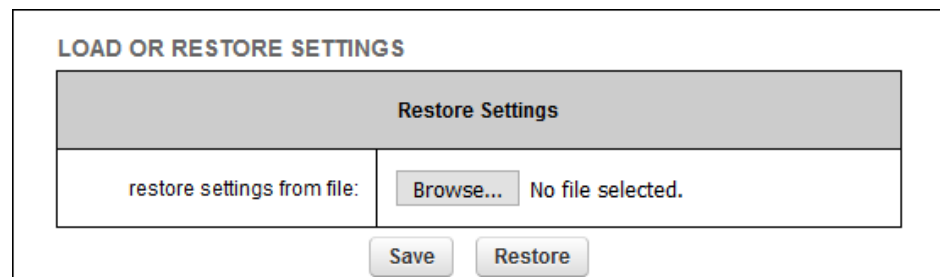


Figure 53. Configurator GUI (LOAD OR RESTORE SETTINGS dialog)

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.

6.8.7. Resetting the unit to factory defaults

The **reset factory default** window contains controls that allow you to restore the Cisco FM10000 Gateway 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” \(page 99\)](#) 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 54 \(page 99\)](#)).

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 54. 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” \(page 97\)](#).

Rebooting the unit

The **reboot** window contains controls that allow you to reboot the Cisco FM10000 Gateway (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 55 (page 100)).

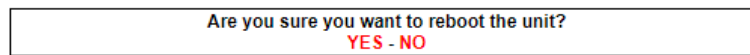


Figure 55. Configurator GUI (unit reboot dialog)

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.

6.8.8. 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 56 (page 100)). If needed, use the dialog to log in again.

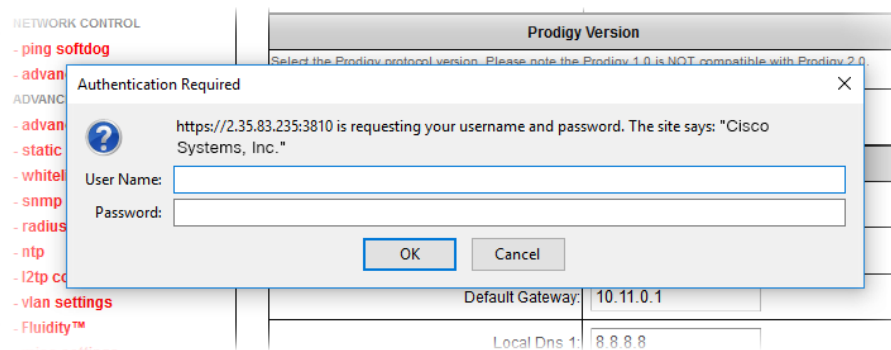


Figure 56. Web browser (Authentication Required dialog)

6.8.9. Viewing the end-user license agreement

The **License Agreement** window contains the Cisco end-user license agreement for the Cisco FM10000 Gateway, 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 57 (page 101)).

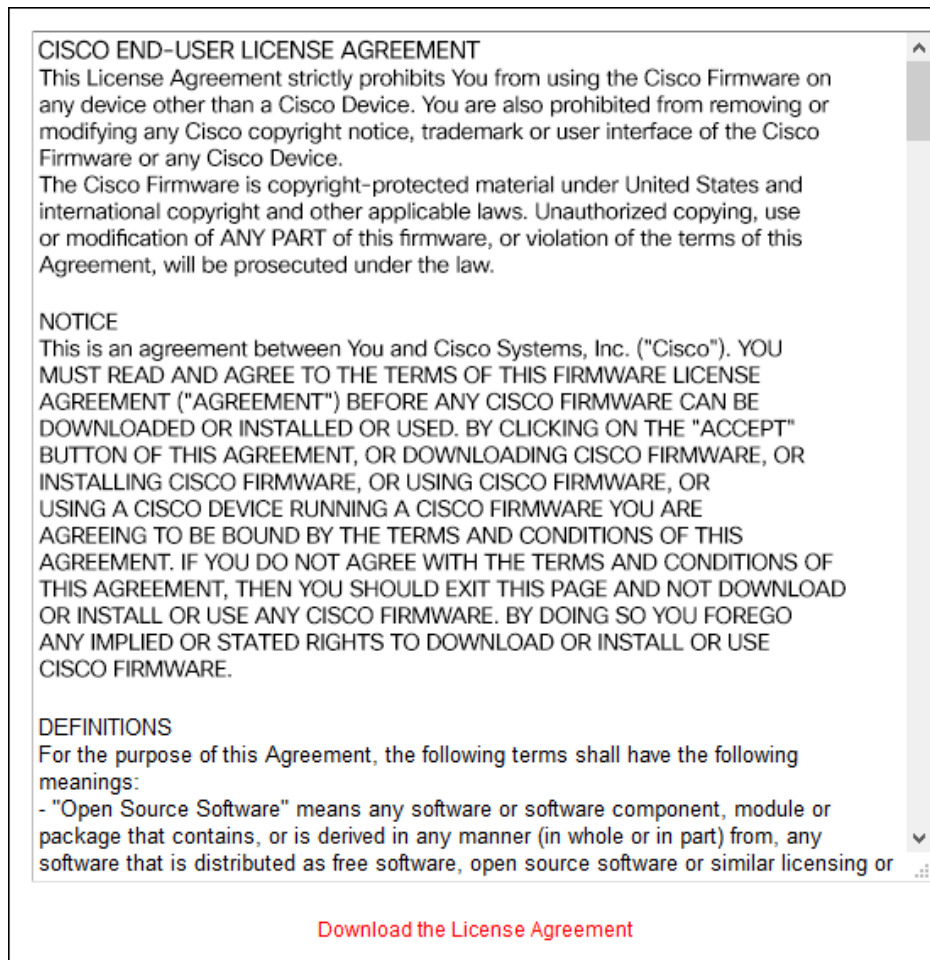


Figure 57. Configurator GUI (End-user license agreement)

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.

7. SOFTWARE PLUG-INS

7.1. Available plug-ins

Like other Cisco radio transceivers, the Cisco FM10000 Gateway is able to take 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 6. 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	<p>If an existing bandwidth plug-in is installed, this plug-in allows bandwidth to be upgraded to a higher, specified value.</p> <p>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.</p>	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 7. 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	<i>Firmware embedded</i>	Available	Available	Not available
Virtual Gigabit	Not available	Not available	Available	Not available
L2TP	<i>Firmware embedded</i>	Not available	Available	Not available
PROFINET	<i>Firmware embedded</i>	Not available	Available	Not available
QNET	<i>Firmware embedded</i>	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 8. 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.

7.2. Plug-in management procedures

7.2.1. 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 58 \(page 107\)](#)).

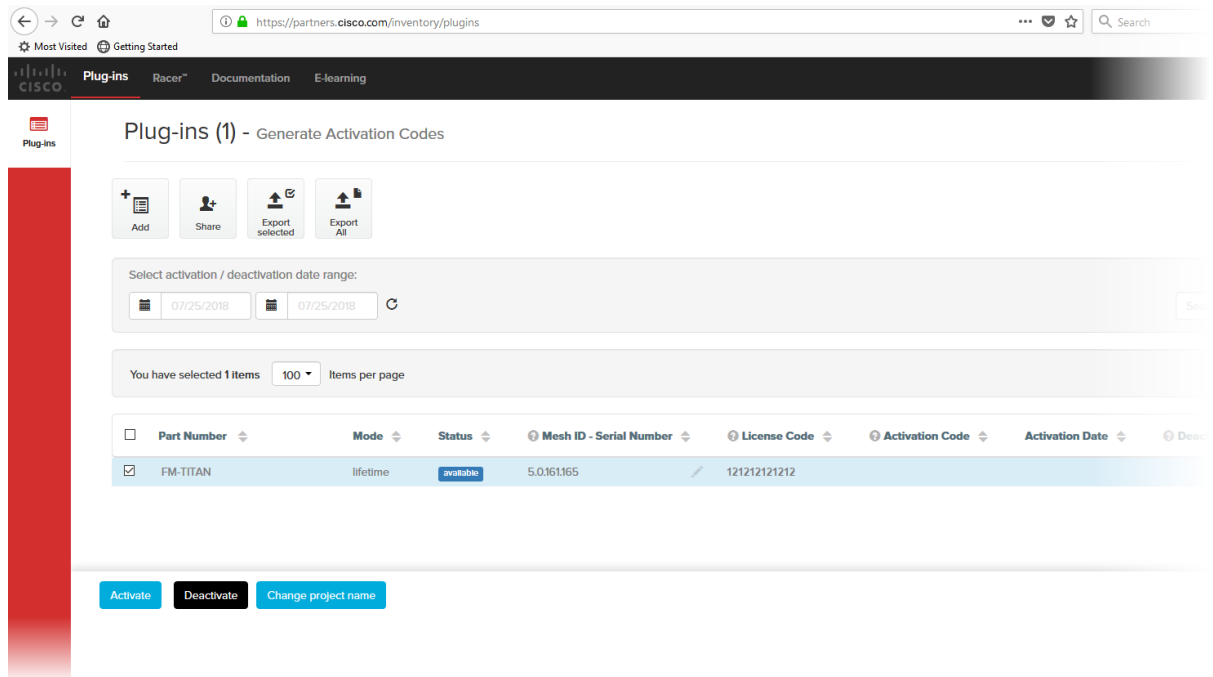


Figure 58. Partner Portal Plug-ins page (License code plug-in)

- 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 92) for details.
 - The plug-in will be activated, and the relevant functionality can be used.

7.2.2. 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 59 (page 109)).

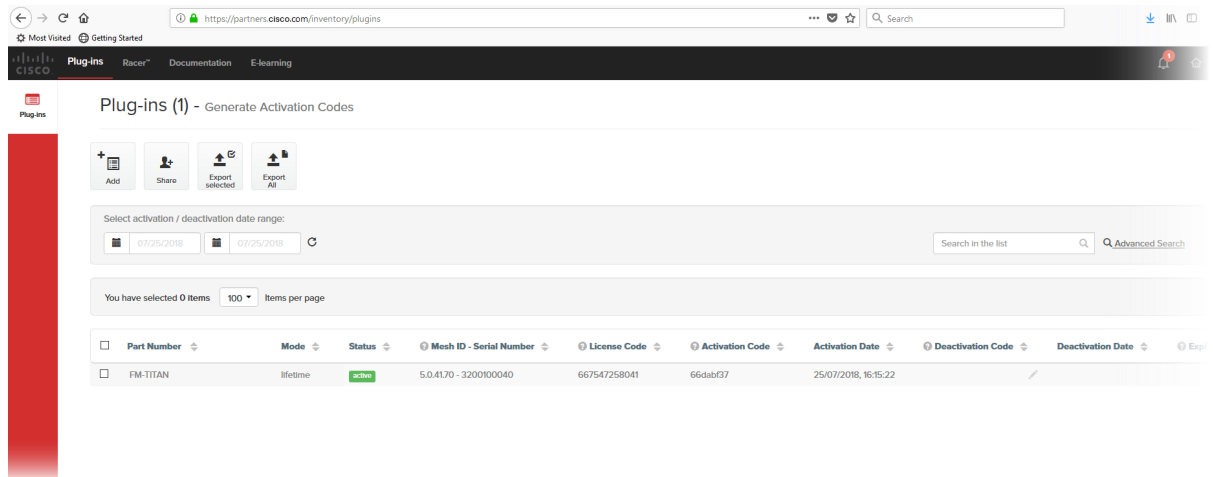


Figure 59. Partner Portal Plug-ins page (License code deactivation)

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 60 (page 109)).

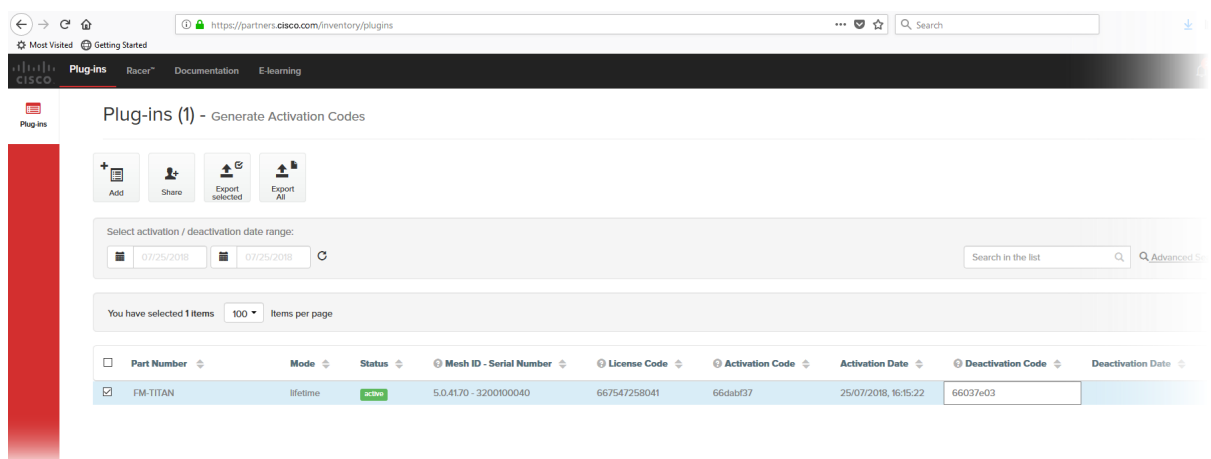


Figure 60. Partner Portal Plug-ins page (deactivation code entry)

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.

7.2.3. 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 61 \(page 110\)](#)).

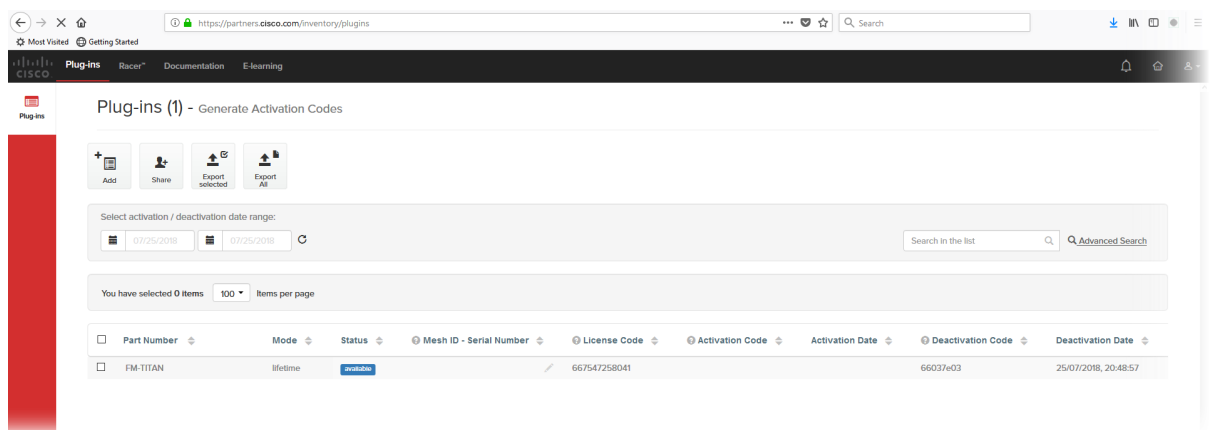


Figure 61. Partner Portal (Plug-ins web page)

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 106).

7.2.4. 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 62 (page 111)**).

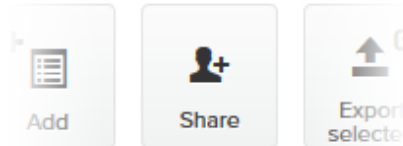


Figure 62. Plug-ins web page (Share button)

- 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.

8. TROUBLESHOOTING

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

8.1. 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 stop the computer from trying to access the unit through a proxy connection, refer to ["Accessing the Cisco FM10000 Gateway for device configuration"](#) (page 32).

8.2. I cannot log in to the FM Racer interface



IMPORTANT

For a detailed description of the differences between the FM Racer configuration interface and the local Configurator interface, refer to ["Device configuration using the configurator interface"](#) (page 30).

If you are not able to log in to the FM Racer web-based configuration interface, check that you have entered the correct user name and password.

The factory-set user name for the FM Racer configuration interface is **admin**. The factory-set password is **admin**.

To change the factory-set user name and password, refer to the *Cisco Networks FM Racer User Manual*.

8.3. 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 99) for more information.

8.4. I purchased a Cisco device, but it is not shown in FM Racer

The Cisco device you have purchased may not yet be added to your Cisco Partners account. Try manually adding the device using the unit serial number and mesh identity (ID) number, as shown in the *Cisco FM Racer user's manual* (section: *Adding Cisco devices to your FM Racer portfolio*).

8.5. I cannot connect my Cisco device to the FM Racer interface

If your Cisco device refuses to connect to FM Racer, or you cannot switch the device to *Online* mode using the onboard Configurator interface, check the following points:

- Was the Ethernet cable disconnected from the computer or the device after the device acquired the IP address leased by the DHCP server? If it was, repeat the connection, making sure the cable remains connected to the computer and the device.
- Is the local DNS server able to resolve the address *partners.cisco.com*, and the address of the RACER™ Cloud Server? If not, check for possible DNS server misconfiguration.
- Is port 443 open in the network firewall? If not, make sure the port is open.

8.6. I applied configuration settings to the device using FM Racer, but I have lost connection to the device in FM Racer.

When configuration settings are successfully applied to a device in Provisioning Mode:

- The device exits Provisioning Mode.
- DHCP is disabled for the device.
- The device is restarted using the configuration that has just been set.

Is the device expected to be connected to the internet? If so, check the following points:

- Do the configuration settings include the correct default gateway address and DNS server address?
- Can the device connect to the internet from the local subnet?

8.7. How do I connect an existing pre-FM Racer device to FM Racer?



IMPORTANT

Please note that Cisco FM Ponte kit and FM1300 Otto transceivers are not compatible with FM Racer.

To configure and maintain these transceivers, refer to the *Cisco Installation and Configuration manual* for the specific device.

To connect compatible Cisco devices that were purchased before FM Racer came online, do the following steps:

1. Upgrade your device firmware to a version that supports FM Racer.



NOTE

As of October 2018, the most current firmware versions are as follows:

- 1.2.1 (FM1000 Gateway and FM10000 Gateway gateways)
- 7.5.1 (FM FM1200 Volo)
- 8.2.1 (All FM x200 variants)
- 9.0.1 (All FM x500 variants)

2. Connect a computer to the Cisco device.
3. Launch the offline Configurator interface.
4. Switch to *Online Cloud-Managed* mode as shown in the *Switching between offline and online modes* section of your device's Installation and Configuration manual.
5. Adjust the device configuration as needed using the Cisco Partners Portal.

9. 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 9. 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	
AC IN	First-generation FM10000 Gateway: unit may be equipped with multiple 275W redundant AC power supply units (input power: 100 Vac to 240 Vac at 50 Hz to 60 Hz).		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 10. 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 11. 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

10. HEAT RADIATION DATA

When in use, all Cisco gateway units and radio transceivers generate heat 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

11. FCC AND CE COMPLIANCE CERTIFICATES



Figure 63. CE certificate of compliance (first-generation FM10000)

Gateway)



Figure 64. FCC certificate of compliance (first-generation FM10000 Gateway)

12. 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.

13. CISCO END-USER LICENSE AGREEMENT

13.1. 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.

13.2. 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 can be 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 stated rights to download, install or use Cisco firmware.

13.3. 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 you purchase 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.

13.4. 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.

13.5. 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 Firmware or 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 Cisco branding 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 Firmware 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.

13.6. 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.

13.7. 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 pursuant to Cisco intellectual property rights) within thirty (30) calendar days after its receipt of written notice regarding such breach, or (ii) you breach any Cisco intellectual property right. Upon termination of this license for any reason, you agree to destroy all copies of the Cisco Any use of the Cisco Firmware after termination is unlawful.

13.8. 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 free to 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.

13.9. 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 of the 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 related systems and technologies ('Data'), and you give Cisco the right to use 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 of this license. Cisco may use this information, as long as it is collected in a form that does not personally identify you, for the purposes described above.

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

13.10. 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, statutory 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-infringement and 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 no support or maintenance obligations for the Cisco Firmware.

13.11. 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.

13.12. 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, and you, 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.

13.13. 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, but without limitation, the Cisco Devices and Cisco Firmware may not 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 further responsibility 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.

13.14. 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.

14. 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