



RACER

Cisco Ultra-Reliable Wireless Backhaul FM RACER

Configuration Manual

(Formerly Fluidmesh)
Edition 1.2

Firmware V1.2.1 (FM 1000 and FM 10000) V7.6 (1200 VOLO) V8.3 (3200- and 4200-series)
V9.1 (3500- and 4500-series) V10.0 (4800 FIBER))

Copyright © Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word 'partner' does not imply a partnership relationship between Cisco and any other company. (1110R) © 2018–2020 Cisco Systems, Inc. All rights reserved.

Table of Contents

1. HAZARDOUS CONDITION WARNINGS	6
2. Reporting Mistakes And Recommending Improvements	7
3. Introduction	8
3.1. CLI Account Types	8
4. Using The Fluidmesh Partner Portal	10
4.1. Accessing The Partner Portal	10
4.2. Enabling Two-Factor Authentication For Security	11
4.3. Administering Plug-In License Codes	13
4.4. Viewing The Technical Documentation For Your Fluidmesh Device	13
5. Preparing To Use RACER	14
5.1. Compatible Fluidmesh Hardware Devices	14
5.2. Software And Hardware Prerequisites	14
Fluidmesh Device Firmware	14
Computer Workstation	15
Supported Web Browsers	15
Software Plug-Ins	15
5.3. User Permissions	16
Device Configuration Privileges	17
6. Using FM Racer To Configure A Fluidmesh Device	18
6.1. Adding Fluidmesh Devices To Your FM Racer Portfolio	18
6.2. Applying A Configuration Template	19
6.2.1. Creating A New Configuration Template	20
6.2.2. Copying And Modifying A Pre-Defined Configuration Template	24
6.2.3. Sharing One Or More Templates With Another User	27
6.2.4. Deleting Templates From Your Partners Portal Account	29
6.3. Configuring Your Device Using FM Racer	31
6.3.1. Specifying Configuration Parameters Without A Template	31
Method 1: Use The RACER™ Radio Configuration View.	32
Method 2: Use The Update Configuration Parameters View.	34
Available Configuration Parameters	35
MANAGEMENT Tab	36
GENERAL Tab	38
WIRELESS RADIO Tab	38
ADVANCED RADIO SETTINGS Tab	39
ETHERNET SETTINGS Tab	41
MULTICAST Tab	42
SNMP Tab	43
RADIUS Tab	44
NTP Tab	45
FLUIDMESH WI-FI Tab	46
L2TP Tab	49
VLAN Tab	49
FLUIDITY Tab	50
FLUIDITY ADVANCED Tab	52
Degree Of Preference	52
Selection Of 'Best' Infrastructure Unit	52
RSSI Zones Threshold In Correlation With Handoff Hysteresis Thresholds	53
FLUIDITY POLE BAN Tab	57
FLUIDITY FREQUENCY SCAN Tab	59
MISC Tab	61

SPANNING TREE Tab	62
QOS Tab	62
MPLS Tab	63
FAST FAILOVER (TITAN) Tab	64
ARP Tab	65
INTRA-CAR Tab	66
REMOTE ACCESS Tab	67
VIEW MODE SETTINGS Tab	67
PLUG-INS Tab	68
STATIC ROUTES Tab	69
Pass List / Block List Tab	69
6.3.2. Applying A Configuration File To An Internet-Connected Device	70
6.3.3. Applying A Configuration File To A Device That Is Not Connected To The Internet	72
6.3.4. Exporting A Configuration File From A Device To FM Racer	74
6.4. Sharing A Device With Another User	76
6.5. Project Management	78
6.5.1. Creating A Project	78
Creating A New Project Using The Projects View	78
Associating A New Or Existing Project With A Fluidmesh Device	79
Associating A New Or Existing Project With A Device Configuration Template	80
6.5.2. Sharing A Project With Another User	82
6.5.3. Editing The Details Of A Project	83
6.5.4. Deleting A Project	84
6.5.5. Assigning Entities To, And Removing Entities From A Project	85
Removing A Device From A Project Using The Projects View	85
Adding Or Removing A Device From A Project Using The RACER™ Radio Configuration View	86
Removing A Plug-In From A Project Using The Projects View	88
Adding Or Removing A Plug-In From A Project Using The Plug-Ins View	89
Removing A Template From A Project Using The Projects View	90
Add Or Removing A Template From A Project Using The Configuration Templates View	91
6.5.6. Filtering Entities By Project	93
Searching By Choosing A Project Listing From A Drop-Down List	94
Searching Among All Project Listings Simultaneously	94
Searching For Entities That Are Not Associated With A Project	94
Searching By Project Name	95
6.6.	95
7. Troubleshooting	96
7.1. I Cannot Get The Log-In Screen	96
7.2. I Forgot The Administrator Password	96
7.3. The Wireless Link Is Poor Or Non-Existent In Bridge Mode	96
7.4. I Purchased A Fluidmesh Device, But It Is Not Shown In FM Racer	97
7.5. I Cannot Connect My Fluidmesh Device To The FM Racer Interface	97
7.6. I Applied Configuration Settings To The Device Using FM Racer, But I Have Lost Connection To The Device In FM Racer.	97
7.7. How Do I Connect An Existing Pre-FM Racer Device To FM Racer?	98
8. Notices And Copyright	99
9. Fluidmesh End-User License Agreement	101
9.1. Preamble	101
9.2. Notice	101

9.3. Definitions	101
9.4. License Grant	102
9.5. Uses And Restrictions On Use	102
9.6. Open-Source Software	103
9.7. Termination	103
9.8. Feedback	104
9.9. Consent To Use Of Data	104
9.10. Warranty Disclaimer	105
9.11. Limitation Of Liability	105
9.12. Exclusion Of Liability For Emergency Services	106
9.13. Export Control	106
9.14. General	107
10. Contact Us	108

1. HAZARDOUS CONDITION WARNINGS

Like all other global technology vendors, Fluidmesh 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, Fluidmesh 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 Fluidmesh 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 Fluidmesh Networks dealer for assistance.

If you are adjusting and/or controlling a Fluidmesh 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@fluidmesh.com.

3. Introduction

This manual is intended for use by wireless networking professionals who have been tasked with configuring Fluidmesh gateway units and/or radio transceivers, and/or configuring and maintaining the system using Fluidmesh software.

Throughout this manual, configuration and adjustment settings are given for Fluidmesh device parameters. You must have a thorough understanding of each parameter before attempting to configure and/or adjust it. Many configuration parameters are interdependent, and misconfiguration or poor adjustment of parameters could severely degrade the performance of the device, or make it inoperable.



IMPORTANT

All device configuration parameters are explained in detail in the Cisco FM Racer Configuration Manual, and in the user manual for your Fluidmesh gateway device or radio transceiver device. Be sure to read and understand these documents before attempting to configure your device using the command-line interface.

This manual is applicable to the following Fluidmesh device firmware versions:

7.5.1 (FM1200 Volo)

8.2.1 (Cisco 3200-series and Cisco 4200-series radio transceivers)

9.0.1 (Cisco FM3500 Endo and Cisco 4500-series radio transceivers)

10.0 (4800 radio transceiver)

3.1. CLI account types

Users can log onto the CLI using Administrator or View Mode credentials. The differences between credential types are shown in the table below:

If you are logging onto the device as an administrative user, log on using the following command:

```
ssh <admin_user>@<device IP address>;
```

If you are logging onto the device in View Mode, log on using the following command:

```
ssh <view_mode>@<device IP address>;
```

To configure the unit using the command-line interface, refer to the content in this manual.

To configure the unit using FM Racer, refer to the Cisco FM Racer manual.

To configure the unit using the Configurator interface, refer to the Fluidmesh Installation and Configuration manual for the specific device.

4. Using the Fluidmesh Partner Portal

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

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

4.1. Accessing the Partner Portal

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

To access the Fluidmesh 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 1 \(page 10\)](#) below. If needed, upgrade your browser version.
2. Click [this link](#).
 - The Fluidmesh 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 1. 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	-

4.2. Enabling Two-Factor Authentication for security

To enhance cyber-security on the Partner Portal, Fluidmesh 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 [Fluidmesh 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 1 \(page 11\)](#)). Click the **Account** option.

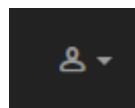


Figure 1. Partner Portal (Profile icon)

- Your portal account page will be shown.
4. Click the **Two Factor Auth.** link on the left-hand side of the web page ([Figure 2 \(page 12\)](#)).

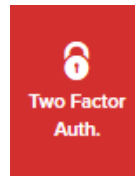


Figure 2. Partner Portal (Two Factor Auth. icon)

- 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 3 \(page 12\)](#) is a typical example of the QR code you will be shown.



Figure 3. 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.

4.3. 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 Fluidmesh device users
- Accept shared License codes from other Fluidmesh device users

To do the tasks above, refer to [Plug-In management](#).

4.4. Viewing the technical documentation for your Fluidmesh device

All documentation relating to your Fluidmesh 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 Fluidmesh device, do the following steps:

1. Log in to the Fluidmesh 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.

5. Preparing to use RACER

5.1. Compatible Fluidmesh hardware devices

FM Racer is compatible with the following Fluidmesh hardware devices:

Gateway devices:

- FM1000 Gateway
- FM10000 Gateway

Radio transceivers:

- FM FM1200 Volo
- All FM 3200 models
- FM Cisco FM3500 Endo
- All FM 4200 models
- All FM 4500 models



IMPORTANT

FM Racer is not compatible with the FM Ponte kit and FM FM1300 Otto radio transceivers.

To configure and maintain these transceiver devices, refer to the Fluidmesh Installation and Configuration manual for the specific device.

5.2. Software and hardware prerequisites

To configure Fluidmesh devices using FM Racer, all hardware devices, software applications and firmware applications must conform to the standards in this section.

Fluidmesh device firmware

To be compatible with FM Racer, the device firmware on your Fluidmesh device must conform to the following version:

- Version 1.2.1 or later (*FM1000 Gateway and FM10000 Gateway*)
- Version 7.5.1 or later (*FM1200 Volo*)
- Version 8.2.1 or later (*All 3200 and 4200 variants*)
- Version 9.0.1 or later (*All 3500 and 4500 variants*)

To upgrade the firmware, refer to the *Overwriting and upgrading the unit firmware* section of the Fluidmesh Installation and Configuration manual for the specific device.

Following a firmware upgrade, the device may retain its previous configuration mode, or switch to a different configuration mode, as follows:

- If the device firmware was upgraded from a version that was not supported by the *Online* (cloud-managed) configuration mode, the configuration mode will automatically be set to *Offline*. Provisioning Mode will not be available, and the FM Racer embedded agent will be disabled. To use *Online* configuration Mode, refer to the *Switching between offline and online modes* section of the Fluidmesh Installation and Configuration manual for the specific device.
- If the device firmware has been upgraded from a version that supported *Online* configuration mode, the previously selected configuration mode will be preserved.

To connect compatible Fluidmesh devices that were purchased before FM Racer came online, refer to [“How do I connect an existing pre-FM Racer device to FM Racer?”](#) (page 98).

Computer workstation

You will need a personal computer with the following minimum specifications:

Table 2. Minimum computer specifications

Operating system	Windows 7 or later	Mac OS X 10.9.x or later	Linux (32-bit or 64-bit): <ul style="list-style-type: none"> • Ubuntu 14.04 or later • Debian 9 or later • OpenSuSE 14.2 or later • Fedora Linux 19 or later
Processor	Intel or AMD	Intel or AMD	Intel or AMD
RAM	2 GB minimum	2 GB minimum	2 GB minimum
Screen resolution	1024x768 minimum	1024x768 minimum	1024x768 minimum

Supported web browsers

A current web browser must be installed on your computer. For a list of compatible web browsers, refer to the *Supported web browsers* table in [“Using the Fluidmesh Partner Portal”](#) (page 10).


Software plug-ins

Various plug-in software upgrades are available for Fluidmesh hardware devices. These plug-ins add functionality and enhance the performance of the unit.

The need for at least some additional software functionality may have been identified at the network design stage, or after initial device installation and configuration. In either case, installation and activation of the correct plug-ins is essential for correct device configuration.

For plug-in management procedures and a complete list of available software plug-ins for your Fluidmesh hardware unit, refer to the *Available plugins* section of the Fluidmesh Installation and Configuration manual for the specific device.

5.3. User permissions



IMPORTANT

FM Racer user permissions are used to grant or deny users the ability to change the device's configuration settings.

These permissions are not related to the permissions needed to configure the device in *Offline* mode using the onboard Configurator.

The permissions required by a user to change device configuration settings differ, depending on the following factors:

- Whether the device is in *Online* (cloud-managed) mode, or *Offline* (on-board Configurator) mode.
- Whether the user has been granted Administrator or View-mode privileges.
- Whether an attempt is being made to configure the device using FM Racer, or using the on-board Configurator interface.

Table 3 (page 16) shows the various user permissions for Online and Offline configuration.

Table 3. User permissions for the RACER™ Cloud Server

Device configuration mode	User type	Command-line interface (CLI) permissions	Offline Configurator permissions
Online (cloud-managed)	Administrator / Viewer	Read-only	<ul style="list-style-type: none"> • Read-only configuration parameters • Reboot device • Upgrade device firmware • Reset to factory defaults • Activate and deactivate plug-ins
Offline (through on-board Configurator UI)	Administrator	Full	All

Device configuration mode	User type	Command-line interface (CLI) permissions	Offline Configurator permissions
Offline (through on-board Configurator UI)	Viewer	Read-only	Configurable permissions (through View Mode settings)

Device Configuration privileges

FM Racer includes a progressive set of configuration privilege levels (*Viewer* and *Administrator*).

These configuration privilege levels apply to the FM Racer user interface only. They do not apply to offline management of a physical device. To change the parameters of a physical device through the on-board Configurator Interface, refer to the *Device configuration using the Configurator interface* section of the Fluidmesh Installation and Configuration manual for the specific device.

Two levels of device configuration privilege are available:

The *Administrator* role is typically assigned to a senior member of the technical support team, or a technician responsible for commissioning the system. This role has privileges to:

- Edit any aspect of a device's configuration.
- Assign hardware devices to other users, using the FM Racer interface.

The *Viewer* role is typically assigned to a member of the technical support team responsible for remote monitoring or local supervision. This role has privileges to:

- View all aspects of a device's configuration, but not edit any configuration parameters.

6. Using FM Racer to configure a Fluidmesh device

To use the FM Racer web-based interface, do the following steps:

1. Click [this link](#).
 - The Fluidmesh Partners Portal Sign In dialog will be shown.
2. Register as a portal user by clicking the **Create Account** link and following the software prompts.
 - When registration is complete, you will be redirected to the Partners Portal homepage.
3. Click the **RACER™** icon on the homepage.
 - The FM Racer portal will be shown.

6.1. Adding Fluidmesh devices to your FM Racer portfolio

To be able to configure a Fluidmesh device, the device must be added to your FM Racer portfolio.

When the purchase order for your Fluidmesh device is finalized and you take delivery of the physical device, the device will be added to your portfolio by Fluidmesh Support.







To check that a device has been added to your Fluidmesh portfolio, do the following steps:

1. Using your login credentials, go to the FM Racer interface on the Fluidmesh Partners Portal.
2. Click the **Configure Devices** link on the left side of the FM Racer interface (below).



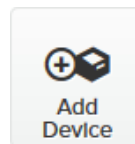
- The **RACER™ Radio Configuration** view will be shown.

- Your device should be listed as part of your device list (below).

<input type="checkbox"/>	Mesh ID - Serial Number ⌵	Model ⌵	Config
<input type="checkbox"/>	  5.0.157.185 - 4501010015	FM4500F	Online C
<input type="checkbox"/>	  5.0.4.18 - 1200101041	FMVOLO	Online C
<input type="checkbox"/>	  5.84.75.86 - 1000997777	FM1000	Online C

If your device has not been added to your Fluidmesh portfolio, add the device manually by doing the steps that follow:

- Click the **Add Device** button (below).



- The **Add Devices** dialog will be shown.
- Click the green **Add +** button on the dialog (below).



- Mesh-ID** and **Serial Number** entry fields will be shown below the **Add +** button.
- Enter the correct **Mesh-ID** and **Serial Number** values in the fields.
 - Click the blue **Add Devices** button on the dialog (below).



- If the **Mesh-ID** and **Serial Number** values are correct, the device will be added to your Fluidmesh portfolio, and you will receive an E-mail confirming that the device has been added.

6.2. Applying a configuration template

FM Racer is designed to save time by speeding and simplifying the configuration of Fluidmesh devices.

Mass configuration works on the principle that if multiple devices of a single type all need configuration, a custom configuration file only needs

to be created once, using the needed parameters. Once created, the configuration file can be applied to all other devices of the same type, and minor configuration adjustments can be made to each device as needed.

A configuration can be applied to any FM Racer-compatible Fluidmesh device using either of the two methods shown in the sections below:

- A new, custom configuration template can be created and saved.
- A configuration template pre-defined by Fluidmesh can be modified and saved.

Pre-defined and custom templates are shown on the **Configuration Templates** page as follows:

- The total number of templates you have access to is shown to the right of the **Configuration Templates** heading (below).

Configuration Templates (6) - All projects

- To quickly filter all saved templates by name or category, enter one or more keywords in the **Search** field (below) and press the *Enter* key. The Search tool will filter and show saved templates accordingly.

🔍

🔍 [Advanced Search](#)

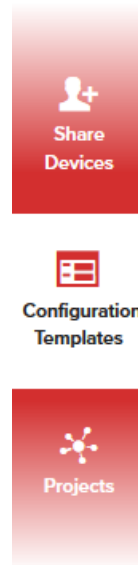
- A list of saved templates, including pre-defined templates, is shown on the **Configuration Templates** page. All management information associated with a template is shown to the right of the template name (below).

<input type="checkbox"/>	Name	Description	Product Line
<input type="checkbox"/>	☰ Fluidity On-Board Fast Failover	Fluidity Layer 2 On-board Fast Fail...	FM3200, FM4200, FM4200F (8.2.1)
<input type="checkbox"/>	☰ Fluidity Mesh-End Fast Failover	Fluidity Layer 2 Mesh-End Fast Fal...	FM3200, FM4200, FM4200F (8.2.1)
<input type="checkbox"/>	☰ Fluidity Vehicle	Layer 2 Fluidity Vehicle configurati...	FM3200, FM4200, FM4200F (8.2.1)
<input type="checkbox"/>	☰ Fluidity Infrastructure	Layer2 Fluidity Infrastructure Mes...	FM3200, FM4200, FM4200F (8.2.1)
<input type="checkbox"/>	☰ Arctic Explorer ROVs V1.21		FMVOLO (7.5.1)
<input type="checkbox"/>	☰ Fluidity Gautrain JNB line	Layer2 Fluidity Infrastructure Mes...	FM3200, FM4200, FM4200F (8.2.1)

6.2.1. Creating a new configuration template

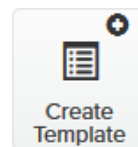
If needed, create and save a new configuration template by doing the steps that follow:

1. Click the **Configuration Templates** link on the left side of the FM Racer interface (below).



- The **RACER™ Configuration Templates** view will be shown.

2. Click the **Create Template** button (below).



- The **Create Configuration Template view** will be shown (below).

Fluidmesh Product Line *	<input type="text" value="Select FMProduct Line"/>
Template name *	<input type="text" value="Configuration Template Name"/>
Template description	<input type="text" value="Description (optional)"/>
Project name	<input type="text" value="Type project"/>

3. Click the **Fluidmesh Product Line** drop-down.
 - The product line options will be shown.
4. Click the correct device model listing.



IMPORTANT

It is important to choose the correct device model listing. The product line options are categorized by firmware version, and include different parameter sets for each model.

- The device model listing will be chosen, and a selection of parameter sets will be shown for the chosen model.
5. Enter a descriptive name for the template in the **Template name** field.
 6. Enter a written description in the **Template description** field.

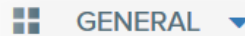


TIP

A detailed description of what the template is intended for will make the future task of choosing and organizing templates much simpler.

If needed, the **Template Name** and **Template description** can be changed at any time.

7. Associate the template with a project using either of the following procedures, as needed:
 - To associate the device with an existing project, do the following steps:
 1. Type one or more characters from the project name in the **Type project** field.
 - All project listings that contain the characters will be shown.
 2. Click the correct project listing to select it.
 - The project listing will be selected.
 - To associate the device with a new project, do the following steps:
 1. Click the **+** button.
 - The **Create Project** dialog will be shown.
 2. Complete the dialog to create the new project.
8. Set the configuration parameters for each of the parameter sets by doing the steps that follow. The **GENERAL** section is shown as an example:
 - a. Click the correct section heading under the **SECTIONS** block.
 - b. If the section you want to edit is collapsed, extend the section by clicking the collapse/extend button to the right of the section heading (below).



- c. By default, all parameters and parameter sets are included in the configuration template. If you want to exclude a parameter set from the template, click the **Included all** switch (below).



- The **Included all** switch will change to an **Excluded all** switch, and all parameters in the parameter set will be greyed out.
- d. If you want to exclude any single parameter that is part of a parameter set, click the **Included** switch (below) for the parameter.



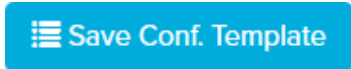
- The **Included** switch will change to an **Excluded** switch, and the parameter will be greyed out.



IMPORTANT

If single parameters and/or parameter sets are excluded from the configuration template, the relevant parameters will not be modified when the template is used to create a radio configuration.

- e. Specify each configuration parameter in the parameter set. For detailed instructions on how to do this, refer to [“Specifying configuration parameters without a template” \(page 31\)](#).
- 9. When you have finished configuring the template, click the blue **Save Conf. Template** button (below).



- FM Racer will check for any errors or conflicts in the configuration.



IMPORTANT

If a configuration parameter cannot be set because a relevant software plug-in has not been installed, FM Racer will prompt you to install the relevant plug-in.







- If no errors are found, the template will be saved.
- If errors are found, FM Racer will prompt you to correct the errors. If you want to review the parameters before proceeding, click the black **No** button on the prompt dialog, and review the configuration parameters. Errors will be marked with warning icons.
- Alternatively, click the blue **Continue** button on the prompt dialog (below) to continue.



TIP

If you save a template that contains configuration errors, the errors can be corrected before the configuration is applied to a Fluidmesh device.

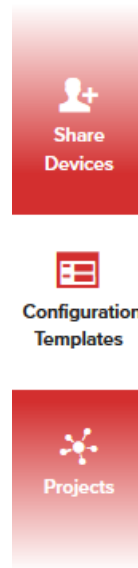
10. Click the blue **Continue** button on the prompt dialog to continue.
 - The template will be saved in the **Configuration Templates** page (below).

<input type="checkbox"/>	Name	Description	Product Line
<input type="checkbox"/>	 Fluidity On-Board Fast Failover	Fluidity Layer 2 On-board Fast Fail...	FM3200, FM4200, FM4200F (8.2.1)
<input type="checkbox"/>	 Fluidity Mesh-End Fast Failover	Fluidity Layer 2 Mesh-End Fast Fal...	FM3200, FM4200, FM4200F (8.2.1)
<input type="checkbox"/>	 Fluidity Vehicle	Layer 2 Fluidity Vehicle configurati...	FM3200, FM4200, FM4200F (8.2.1)
<input type="checkbox"/>	 Fluidity Infrastructure	Layer2 Fluidity Infrastructure Mes...	FM3200, FM4200, FM4200F (8.2.1)
<input type="checkbox"/>	 Arctic Explorer ROVs V1.21		FMVOLO (7.5.1)
<input type="checkbox"/>	 Fluidity Gautrain JNB line	Layer2 Fluidity Infrastructure Mes...	FM3200, FM4200, FM4200F (8.2.1)

6.2.2. Copying and modifying a pre-defined configuration template

If needed, create a modified configuration template from a pre-defined Fluidmesh template by doing the steps that follow:

1. Click the **Configuration Templates** link on the left side of the FM Racer interface (below).



- The **RACER™ Configuration Templates** view will be shown.
2. Four pre-defined templates are available. All are designed for specific purposes, but all can be adapted to any purpose you need:
- **Fluidity Infrastructure:** This template is mostly intended for Fluidity (vehicle-to-ground) trackside infrastructure applications.
 - **Fluidity Vehicle:** This template is mostly intended to be used by vehicle-mounted devices in Fluidity applications.
 - **Fluidity Mesh-End Fast Failover:** This template is mostly intended for applications where a redundant Mesh End unit (in other words, a primary Edge unit connected to a wired backbone) is equipped with Fluidmesh TITAN functionality, allowing it to ‘fail over’ to a backup Edge unit of the same type).
 - **Fluidity On-Board Fast Failover:** This template is mostly intended for applications where a redundant Fluidmesh unit installed in a moving vehicle is equipped with Fluidmesh TITAN functionality.

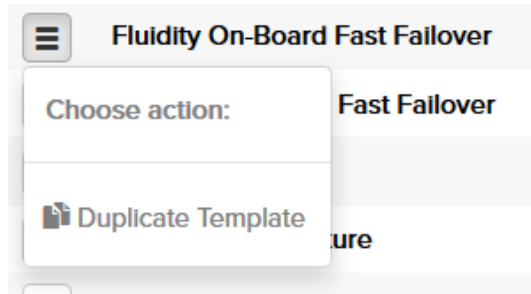


IMPORTANT

The pre-defined templates are not restricted to any particular device type or firmware version. The product line can be changed when the configuration parameters are set.

Note that pre-defined templates cannot be edited, shared with other users, or deleted.

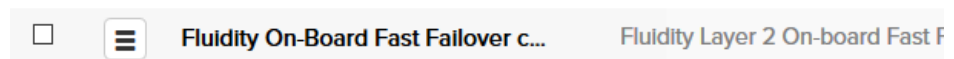
3. Familiarize yourself with the configuration parameters in each template by clicking the template name.
 - The configuration sub-categories in the template will be opened for viewing. To go back to the template list, click the *Back* button on your web browser.
4. Make a copy of the chosen template by clicking the drop-down button to the left of the template name (below) and clicking the **Duplicate Template** option.



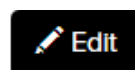
- The **Duplicate Template** dialog will open.
5. Enter a descriptive name for the duplicated template in the entry field, and click the blue **Duplicate** button (below).



- The copied template will be saved in the **Configuration Templates** page of the FM Racer interface (below).



6. To specify the device model listing and configuration parameters, click the template name listing.
 - The **Configuration Templates** view will be shown.
7. Click the black **Edit** button (below) to open the template for editing.



8. Enter the device model listing and configuration parameters as shown in [“Creating a new configuration template” \(page 20\)](#).



TIP

If necessary, the template name can also be changed at this stage.

6.2.3. Sharing one or more templates with another user

If different members within your team or organization have Partners Portal accounts, it is possible to share one or more configuration templates between members in order to modify the templates and/or apply them to Fluidmesh devices.

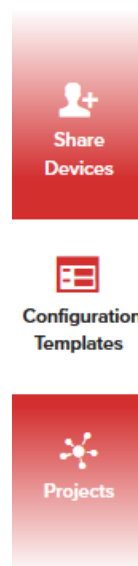


IMPORTANT

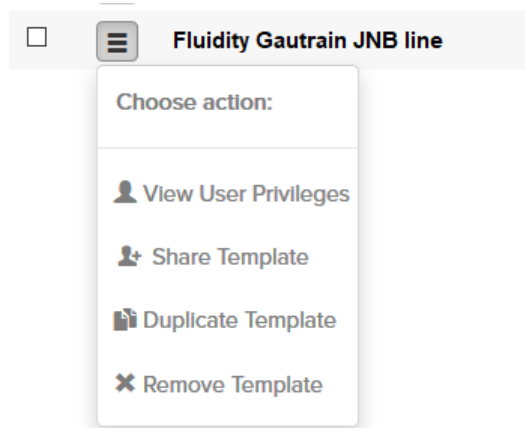
Pre-defined templates cannot be shared with other users. To share a template, modify an existing template or create a new template. Then, share the modified or new template.

If needed, share a single modified or custom template by doing the steps that follow:

1. Click the **Configuration Templates** link on the left side of the FM Racer interface (below).



- The **Configuration Templates** view will be shown.
2. Share the chosen template by clicking the drop-down button next to the template name (below) and clicking the **Share Template** option.



- The **Share Template** dialog will open.
3. Enter the E-mail address of a person with which you want to share the template in the **Invite people** field.
 4. Left-click outside the **Invite people** field.
 - The E-mail address will be saved.
 5. To set the template usage privileges for each user, click the **Privilege** drop-down, then click the chosen privilege level:
 - **Modify and share**: The target user can apply the template to devices, modify configuration settings and share the template with other users.
 - **Read-only**: The target user can share the template with other users only.



TIP

If a different usage privilege level is applied to the template by a target user, the change will affect all other users of the template. To avoid this, copy and save the template with a different name.

6. Repeat the steps above to add as many people as needed and set their user privileges.
7. Click the blue **Share Template** button.
 - The template will be shared with the target users.


If needed, share two or more modified or custom templates simultaneously by doing the steps that follow:

1. Select the target templates by checking the check-box next to each template name (below).



- The **Share Templates** and **Remove Templates** buttons will be shown at the bottom of the interface.
2. Click the blue **Share Templates** button.
 - The **Share Template** dialog will open. Enter the E-mail addresses of target users and set their template usage privileges as shown in this section.
 3. Click the blue **Share Templates** button.
 - The templates will be shared with the target users.

6.2.4. Deleting templates from your Partners Portal account



IMPORTANT

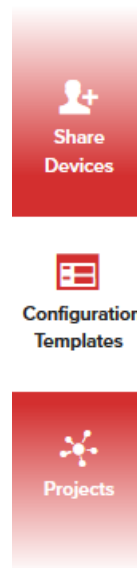
Pre-defined templates cannot be deleted. Only modified and custom templates can be deleted.

The **Remove Template** option is only available if the template privilege is set to *Modify and share*.

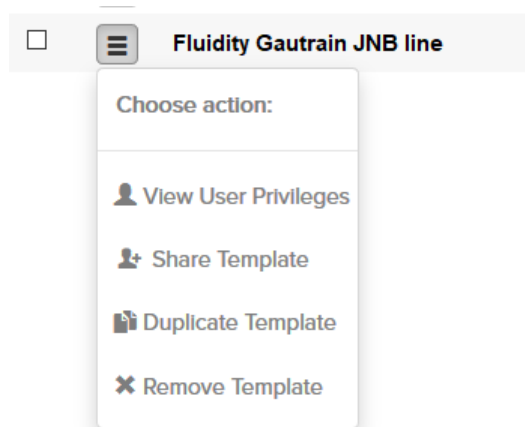
Deleting a shared template will invalidate all references to the template. If the template was forwarded to other users, those users will also lose access to the template.

If needed, delete a modified or custom template by doing the steps that follow:

1. Click the Configuration Templates link on the left side of the FM Racer interface (below).



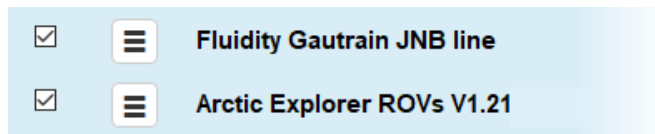
- The **Configuration Templates** view will be shown.
2. Click the drop-down button next to the template name (below) and click the **Remove Template** option.



- The **Remove Template** dialog will open.
3. To delete the chosen template, click the blue **Remove** button. Alternatively, stop the deletion by clicking the black **No** button.
 - If you click the **Remove** button, the template will be permanently deleted from your Partners Portal account.

If needed, delete two or more modified or custom templates simultaneously by doing the steps that follow:

1. Select the target templates by checking the check-box next to each template name (below).



- The **Share Templates** and **Remove Templates** buttons will be shown at the bottom of the interface.
2. Click the black **Remove Templates** button.
 - The **Remove Templates** dialog will be shown.
 3. To delete the chosen templates, click the blue **Remove** button. Alternatively, stop the deletion by clicking the black **No** button.
 - If you click the **Remove** button, the templates will be permanently deleted from your Partners Portal account.

6.3. Configuring your device using FM Racer

You can use the RACER™ Radio Configuration interface to configure your Fluidmesh device using either of the two methods described below. Both methods are shown in this section:

- Configuration settings can be applied directly to the device without the need for a configuration template.
- A configuration template can be modified with the needed parameters, then applied to the device and saved for future use.

FM Racer is a centralized and internet-based configuration platform. To configure your Fluidmesh device using FM Racer, an internet connection must be made between the Fluidmesh device and the FM Racer Cloud Server (an internet-based radio management service).

6.3.1. Specifying configuration parameters without a template



IMPORTANT

This section shows how to adjust a device's configuration settings using the FM Racer interface. It also describes how to apply configuration settings to a device, without the need for a configuration template.

If you want to apply configuration settings to a device using a configuration template, do the following steps:

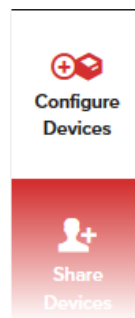
1. Refer to this section for detailed information on how to adjust the configuration settings.
2. Next, refer to [“Applying a configuration file to an internet-connected device” \(page 70\)](#) for instructions on how to apply the needed settings by using a configuration file.

To access a unit's configuration tabs, use either of the following methods:

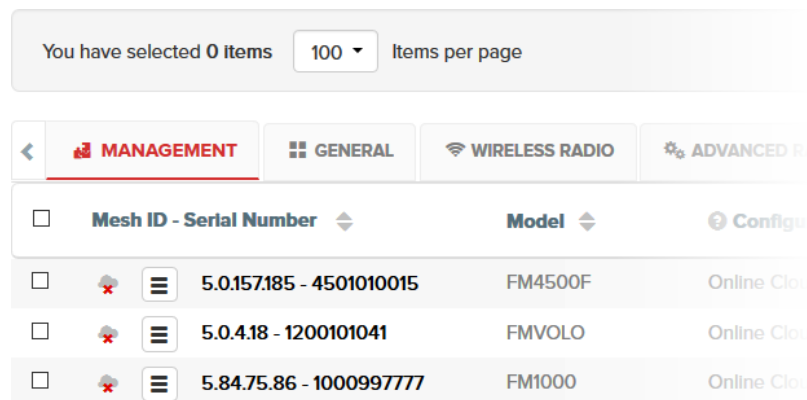
Method 1: Use the RACER™ Radio Configuration view.

If you use this method, you do not need to choose a single device for configuration. FM Racer presents the device listings in a way that allows the same parameter to be configured on more than one of your devices at the same time.

1. Click the **Configure Devices** link on the left side of the FM Racer interface (below).



- The **RACER™ Radio Configuration** view will be shown.
- The lower part of the view includes a list of the devices assigned to your user profile (below).



- The category tabs above the device list contain drop-down menus with a range of configuration options that are relevant to each of your devices.

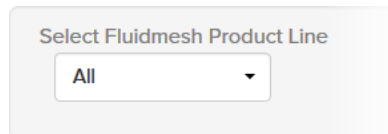


IMPORTANT

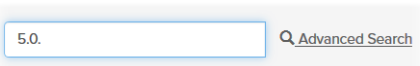
Depending on the device type, some configuration options may not be available for certain devices. If a configuration option is not available for the device being configured, an *Unsupported* notification will be given (below).



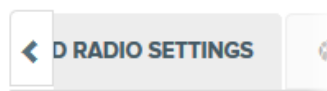
2. If you cannot find the listing for the device that must be configured, do the following steps:
 - To search the list by *product line* (in other words, by firmware version), choose the correct option from the **Select Fluidmesh Product Line** drop-down menu (below).



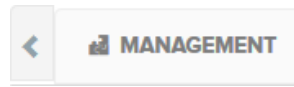
- To search the list by Mesh ID number or serial number, type part or all of the unit Mesh ID number or unit serial number into the search field (below). All devices containing the relevant numbers will appear in the view.



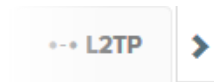
- To do an advanced search, click the **Advanced Search** link (above). FM Racer will display options to search the device list by model, Fluidmesh sales invoice number, unit connection status, project name and device-sharing status. When all criteria have been entered, click the blue search button to execute the search.
 - FM Racer will show a list of all devices matching the specified criteria in the **Radio Configuration** view.
3. The configuration category tabs are shown in a horizontal row above the device listings. When all devices needing configuration are shown in the **Radio Configuration** view, click-and-hold the left arrow button (below).



- The tabs will scroll to the left until the **MANAGEMENT** tab is shown (below).



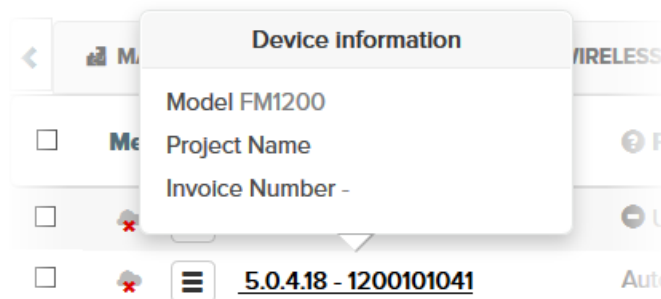
4. To show more configuration category tabs as configuration proceeds, click or click-and-hold the right arrow button (below).



5. When the configuration is complete, confirm that all configuration changes have been done correctly.
6. Click the blue **Save** button on the interface to save the configuration settings.

Method 2: Use the Update configuration parameters view.

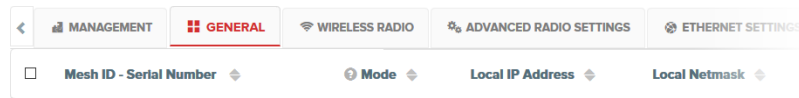
1. Find the listing for the device that must be configured, as shown above.
2. Click the listing for the device that must be configured (a typical device listing is shown below).



- The **Update configuration parameters** view for the device will be shown.
3. By default, the **Update configuration parameters** view is locked for each device. Click the black **Edit** button to open the view for editing.
 - The configuration category tabs are shown in a vertical column on the left side of the interface.
 4. To show more configuration category tabs as configuration proceeds, click-and-drag the vertical scroll bar.

To directly set or adjust a unit's configuration parameters, do the following steps:

1. Click the relevant configuration tab to access the configuration settings. Below, the **GENERAL** tab has been clicked, and a selection of the relevant settings are shown.



2. To set or adjust a configuration parameter, do the following steps as needed:
 - If a drop-down menu is shown, click the drop-down to open it, then click the correct menu option.
 - If a text-entry field is shown, enter the correct information in the entry field.
 - If some fields are clicked, an *On/Off* switch or *Enabled/Disabled* switch will be shown. Click the switch to enable the setting by turning it on, or to disable the setting by turning it off.
 - If configuration parameters must be specified using an entry form, an entry form icon will be shown in the field, in medium grey (below). Click the icon to open the form for editing.



3. Confirm that all configuration changes have been done correctly.
4. Click the blue **Save** button on the interface to save the configuration settings.

Available configuration parameters

All possible configuration parameters that can be applied using FM Racer are listed in the following sub-sections.

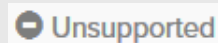


IMPORTANT

If you are using FM Racer to configure your Fluidmesh device, it is assumed that you have prior networking experience, and that you are qualified to install Fluidmesh units and alter their configuration settings. Therefore, detailed explanations of telecommunications concepts are not given in this manual. Detailed information on some of these concepts is given in the Fluidmesh Installation and Configuration manual for the specific device.

A detailed explanation of which configuration options are and are not applicable to a given device, and the reasons why, is beyond the scope of this manual. For detailed information in this regard, consult the latest product data sheet and Fluidmesh Installation and Configuration manual for the specific device.

Depending on the device type, some configuration options may not be available for certain devices, or may depend on other configuration options being activated. If a configuration option is not available for the device being configured, an *Unsupported* notification will be given (below).



If a configuration option is not available for the device because a dependent parameter has not been set, the *Not currently available* icon will be shown (below).



MANAGEMENT tab

The following information and settings options are contained in this tab:

Model: The device's model number. This field cannot be edited.

Configuration Mode: This field shows the unit's current configuration status.

- If the field reads *Online Cloud-Managed*, the device's configuration settings are under control of the FM Racer portal.
- If the field reads *Offline*, the device's configuration must be done locally by connecting a computer to the unit hardware, and using the offline Configurator interface. For instructions on how to change the configuration mode, refer to the *Switching between offline and online modes* section of the Fluidmesh Installation and Configuration manual for the specific device.

Status: This field shows the unit's current internet-connection status.

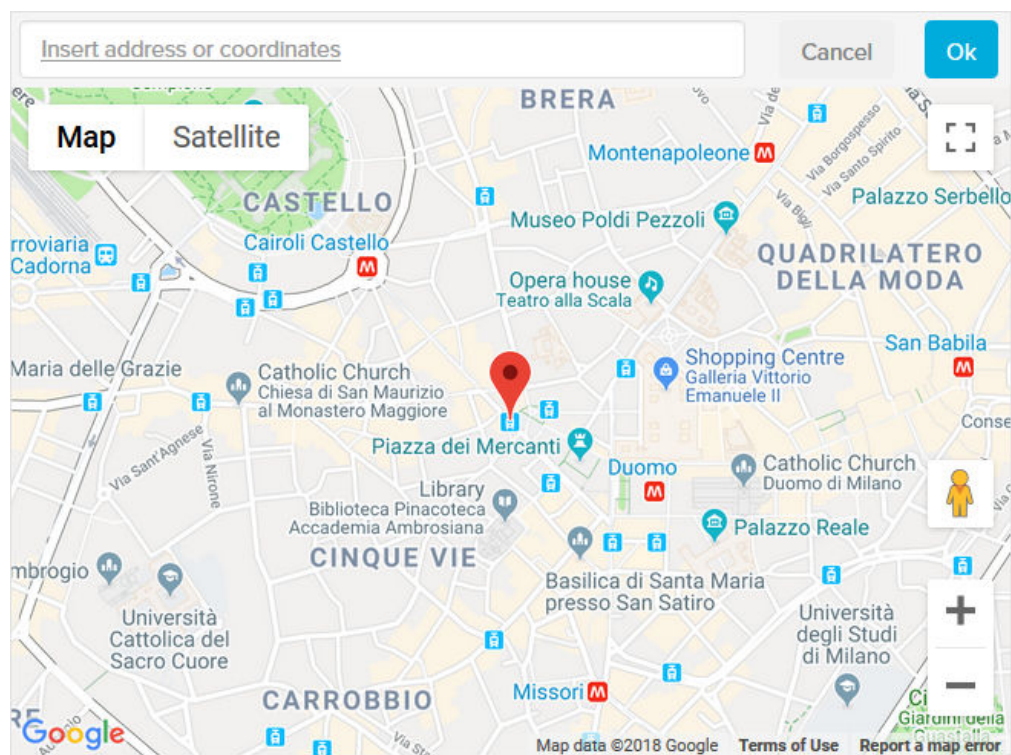
- If the icon reads *Disconnected*, the unit is disconnected from the FM Racer Cloud Server, and is currently relying on configuration settings from its offline Configurator interface.
- If the icon reads *Connected*, the unit is connected to, and currently relying on configuration settings supplied by the FM Racer Cloud Server.

Project Name: The device has been assigned to the Project listed in this field. A Project is a virtual container that encompasses part, or all, of any network installation containing Fluidmesh components, such as hardware devices, software plug-ins and device software configuration templates. For instructions on how to change the Project name, refer to [“Editing the details of a project” \(page 83\)](#).

Position: This field shows the current physical location of the unit.

To change the listed location, do the following steps:

1. Click the **Position** field for the unit listing.
 - A Google Maps view containing an entry field will be shown (a typical view is shown below).



2. If needed, use the built-in map controls to increase or decrease the size of the map view, and to switch between map and satellite aerial views.
3. If needed, click-and-drag the map view to center the map at a different location.

4. The red pin represents the physical location of the unit. To change the unit's location, click-and-drag the pin to a new position. Alternatively, enter a physical address or geographic co-ordinates in the **Insert address or coordinates** field.
5. Click the blue **Ok** button.
 - The physical location of the unit will be saved in the **Position** field as latitude/longitude co-ordinates, expressed in decimal degrees.

Invoice No.: This field shows the Fluidmesh sales invoice number associated with the original purchase of the unit. This field cannot be edited.

Shared With: If responsibility for the unit is shared with other users, the details of the responsible users are shown in this field.

GENERAL tab

The following information and settings options are contained in this tab:

Mode: This field shows the unit's operational mode. Typically, three options are available. If needed, change the unit's operational mode:

- **Mesh End:** This mode allows you to install the unit as the junction point between the wireless network and a wired LAN.
- **Mesh Point:** This mode allows you to use the unit as a relay point in the mesh network and/or attach an IP edge device (for example, a CCTV camera) to the unit.
- **Bridge:** This mode creates a layer 2 connection between the local unit and another Bridge unit.

Local IP Address, Local Netmask, Default Gateway, Local Dns 1, Local Dns 2 and Passphrase: All needed information is self-explanatory. To enter a new parameter, click the entry field and type the parameter.

WIRELESS RADIO tab

The following information and settings options are contained in this tab:

Country / Regulatory: Use this field to specify the country/regulatory domain in which the unit is currently installed.



CAUTION

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

If your unit was purchased in the USA or Canada, the **Country / Regulatory** selection is set to the country of purchase, and the drop-down will be disabled.

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



NOTE

Operation in the 4.9 GHz band must be enabled using a software plug-in (Fluidmesh part number *FM-49*). Contact your Fluidmesh Network representative for details.

Note that the 4.9 GHz band is not available in Brazil and Canada.

Channel width: Choose the required channel bandwidth from the drop-down. Note that radio units on both sides of a wireless link must be set to the same channel width value. A channel width mismatch will result in degraded or broken communication between the units.

Enable RTS Protection (*Cisco FM3500 Endo and Cisco 4500-series transceivers only*): This field shows the unit's current IEEE 802.11 request-to-send (RTS) setting. Click the switch ON to reduce frame collisions caused by 'hidden' radio nodes (in other words, radio nodes that are out of range of your Fluidmesh radio transceiver). Alternatively, click the switch OFF to decrease the system overhead.

Promisc: This field shows the unit's current setting for backwards compatibility with Fluidmesh units that are no longer in production. Click the switch ON for full backwards compatibility, or OFF to maintain compatibility with newer devices only.

Noise floor Calibration: This field shows the unit's current noise floor calibration setting. If the unit is installed in an environment where the radio noise level is very high, click the switch OFF to reduce the amount of radio noise emitted by the unit.

ADVANCED RADIO SETTINGS tab



NOTE

Fluidmax settings are currently only available for FM1200 Volo, Cisco 3200-series and Cisco 4200-series transceivers.

The following information and settings options are contained in the tab:

FluidMAX™ mode: This field shows the unit's current FluidMAX operating mode. Choose the FluidMAX operating mode by selecting the correct option from the drop-down menu:

- **AUTO:** The FluidMAX engine is enabled, and the unit role is set automatically. Depending on various factors, the unit will automatically choose whether to transmit using the time-division

multiple access (TDMA) protocol or the carrier-sense multiple access (CSMA) protocol.

- **principal:** The unit will be set as the center unit within a mesh cluster featuring a 'star' topology. If the unit is set as a principal, it will dictate the operating frequency of the mesh cluster of which it is a principal unit.
- **SUBORDINATE:** The unit will be set as a subordinate unit within a mesh cluster featuring a 'star' topology. If the unit is set as a Subordinate, and its *FluidMAX™ Autoscan* feature is enabled, the unit will scan the spectrum of available frequencies for a principal unit that shares its Cluster ID and use that principal unit's frequency, and its frequency selection feature will be disabled.
- **OFF:** The FluidMAX engine will be disabled.

FluidMAX™ Cluster ID: If the operating mode is set to principal or SUBORDINATE, enter a unique cluster ID tag in the FluidMAX Cluster ID field.

FluidMAX™ Autoscan: If the operating mode is set to SUBORDINATE, enable this option to allow the principal unit of the local mesh cluster to dictate the frequency on which the unit will transmit and receive.

Include 5-10 MHz Channels in Autoscan: If the *FluidMAX™ Autoscan* option is enabled, this option will become available. Enable this option to increase the unit's scan resolution from the default scan value to 5-10 MHz.

MAX Transmission MCS: This setting is used to choose the unit's modulation and coding scheme (MCS). This is the schema by which the unit automatically chooses its maximum data transmission rate using parameters such as channel width, number of spatial streams, coding method, modulation technique and guard interval. The transmission rate can be manually adjusted from 0 Mbps, to the maximum rate seen in the drop-down menu. Alternatively, select the *Auto* option to allow the unit to automatically choose the most efficient transmission rate.

TX Power: This setting controls the effective isotropic radiated power (EIRP) output of the unit. By default, EIRP is automatically regulated using Fluidmesh's Transmission Power Control (TPC) algorithm. The algorithm tries to obtain an optimal link signal strength of approximately -55 dBm on both sides of the radio link while not exceeding the user-defined maximum transmission power threshold. Transmission power can be manually adjusted from -3 dBm to the maximum power level seen in the drop-down menu. Alternatively, select the **AUTO** option to allow the unit to automatically choose the most efficient transmission power level according to prevailing conditions. If this option is chosen, the unit will not exceed the last manually selected TX Power value.



NOTE

If TX Power is set to AUTO, maximum transmission power may vary at any moment depending on the operating frequency of the unit, atmospheric conditions, and other factors.

If the unit's country selection is set to any country within Europe, TPC is automatically enabled.

Enable AES: This setting controls whether Advanced Encryption Standard (AES) encryption is applied to outgoing data packets. Choose the correct encryption activation setting from the list of drop-down options.

Automatic link distance: This setting is used to let the system choose the maximum effective distance between the relevant wireless links. It is also used to set media access control (MAC) layer timeouts for transmitted packets. To set the link distance manually using the following options, select the *Disabled* option. To let the system choose an optimal value, select the *Enabled* option.

Distance: To specify the correct link distance, enter the correct distance value in this field.

Distance measure: Use this setting to choose a unit of distance measurement (Kilometres or Miles).

ETHERNET SETTINGS tab



IMPORTANT

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

The Ethernet settings window contains controls to change the data exchange speeds of the unit's RJ45 Ethernet ports (if fitted). The following information and settings options are contained in the tab:


Ethernet 1 speed / Ethernet 2 speed: Choose the correct data exchange speed for each Ethernet port by clicking one of the following data exchange speeds:

- **Auto** (The data exchange speed for the selected port will be chosen automatically).
- **10 Mbit half duplex**
- **10 Mbit full duplex**
- **100 Mbit half duplex**
- **100 Mbit full duplex**

SFP speed: Choose the correct data exchange speed for the SFP fiber-optic port (if fitted) by clicking one of the following data exchange speeds:

- 100 Mbit full duplex
- 1000 Mbit full duplex

MULTICAST tab



IMPORTANT

Some MULTICAST parameters cannot be set if other dependent parameters have not been set first.

To enable the relevant MULTICAST parameter setting on the left, open the GENERAL tab, and choose the correct operational mode for the unit as listed on the right:

Parameter	Condition
Multicast	Enabled only if operational mode is <i>Mesh End</i> .
Enable Multicast	Enabled only if operational mode is <i>Bridge</i> .

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 Fluidmesh transceiver unit operating in *Mesh Point* mode, and the unit has not been explicitly configured to forward Multicast traffic, the unit will drop the traffic. To enable Multicast forwarding, Multicast settings must be defined.

By default, units 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 to a *Mesh Point* unit, all multicast flow redirection information must be specified using the Multicast settings on the closest *Mesh End* unit.

The following information and settings options are contained in the tab:

Enable Multicast: Click the field to show the On/Off switch. Then click the switch ON to enable Multicast, or OFF to disable Multicast.

Multicast: Change the multicast settings by doing the following steps:

1. Click the entry-form button on the right-hand side of the entry field to open the form.
2. Enter a valid Multicast group designator in the *Multicast Group* field.


TIP

To specify a multicast network mask that includes all subnet addresses, enter `224.1.1.0/24`.

3. If needed, individual or specified destination addresses can be also entered as follows:
 - The destination address consists of one or more Fluidmesh unit ID numbers, in the form **5.a.b.c**. Each of these ID numbers belongs to a physical Fluidmesh device to which multicast traffic must be forwarded.
 - Wildcards can also be used. For example, `5.255.255.255` includes all units within the mesh network.
 - Entering `5.0.0.0` will direct each unit to send multicast traffic to the primary mesh end (this may be particularly useful if the mesh end unit's fast-failover functionality is enabled).
4. If needed, add entry fields for another Multicast route by clicking the green **+** icon.
5. Add the Multicast group by clicking the blue **Update** button.
 - The Multicast details for the unit will be shown in the **Multicast** field.

SNMP tab

The SNMP window can be used to configure an SNMP v2c or SNMP v3 service to run on the device. Both walk-throughs (no agent-to-manager notifications) and traps (agent-to-manager notifications enabled) are supported. If SNMP traps are enabled, you must specify the server address to which monitoring information must be sent.


IMPORTANT

The same SNMP configuration must be set for all Fluidmesh units in the wireless network. For detailed information on Fluidmesh unit SNMP configuration, refer to the Fluidmesh *SNMP FM-MIB OID Table* and *MIB configuration* files. These can be downloaded from the Fluidmesh Partner Portal (**Documentation** section > **User Manuals** > **Advanced Manuals**).

The following information and settings options are contained in the tab:

SNMP Mode: Click this drop-down to choose between **SNMP disabled**, **SNMP v2c**, and **SNMP v3**.

SNMP Community ID: Enter a community identity value in this field. Note that the same value must be used for all Fluidmesh units in the wireless network.

Enable SNMP periodic trap: If needed, configure the unit to send SNMP traps at defined periodic intervals by selecting the **Enable** option.

Enable SNMP event trap: If needed, enable SNMP traps for significant system-related events by selecting the **Enable** option.

NMS hostname: Enter the name of the network management station (NMS) host in this field.

Notification period (minutes): If the *Enable SNMP periodic trap* option was enabled, enter the period at which notifications will be sent in this field.

SNMP username: This parameter is only used if SNMP v3 is specified. Enter a user name in this field. The same user name must be set for all Fluidmesh units in the wireless network.

SNMP password: This parameter is only used if SNMP v3 is specified. To change the current SNMP v3 password, enter a new password in this field. The default password is *fluidmesh*.

SNMP authentication protocol: This parameter is only used if SNMP v3 is specified. Choose the correct authentication protocol from the drop-down. The available options are MD5 and SHA. Note that the same SNMP authentication protocol must be set for all Fluidmesh units in the wireless network.

SNMP encryption: This parameter is only used if SNMP v3 is specified. If needed, choose the correct encryption protocol from the drop-down. The available options are **No Encryption**, **DES** (Data Encryption Standard) and **AES** (Advanced Encryption Standard). Note that the same encryption protocol must be set for all Fluidmesh units in the wireless network.

SNMP encryption passphrase: This parameter is only used if SNMP v3 is specified. To change the current encryption passphrase, enter a new passphrase in this field. The default encryption passphrase is *fluidmesh*.

RADIUS tab

The RADIUS tab contains controls to provide centralized authentication, authorization, and accounting management, using the remote authentication dial-in user service (RADIUS) networking protocol. Note that the RADIUS protocol cannot be used to verify the identity of the user accessing the FM Racer interface. The Partners Portal login controls do this function.

**IMPORTANT**

The RADIUS feature is only available if the unit is set to *Mesh Point* mode or *Mesh End* mode. If the unit is set to *Bridge* mode, Radius configuration options will not be available.

For RADIUS to function correctly, the unit must be receiving accurate time data from one or more network time protocol (NTP) servers. To configure the unit's NTP settings, refer to “NTP tab” (page 45).

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

The following information and settings options are contained in the tab:

IP address / hostname: Enter the IP address or host name of the RADIUS server in this field.

Port: By default, the RADIUS port number is 1812. Do not change the port number unless there is a specific need to do so.

Secret: Enter the RADIUS access password in this field.

Expiration (s): 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.

Authentication Method: Choose the data authentication method by clicking the drop-down and clicking the correct option. Available options are MSCHAPV2, MD5, GTC, TTLS and PEAP.

Inner Authentication Method: Available Inner Authentication Methods are dependent on which Authentication Method (if any) was chosen. If applicable, choose an inner authentication method by clicking the drop-down and clicking the correct option.

Username: Enter the personal username for access to the RADIUS server in this field.

Password: Enter the personal password for access to the RADIUS server in this field.

NTP tab

All Fluidmesh devices 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 Fluidmesh 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.

The following information and settings options are contained in the tab:

Enable NTP: Enable NTP synchronization by selecting the **Enable** option.

NTP server hostname: Enter the host name of a chosen primary NTP server in this field.

Secondary NTP server hostname: Enter the host name of a chosen secondary or backup NTP server in this field.

Timezone: Select the time zone in which the unit is installed by clicking the drop-down menu and clicking the correct time zone option.

FLUIDMESH WI-FI tab

The controls on this tab allow you to set up a second, segregated Wi-Fi interface (known as a wireless access point, or WAP) that allows technicians access to the unit for configuration and maintenance purposes.


**NOTE**

The wireless access point feature is only available for the FM1200 Volo, Cisco 3200-series and Cisco 4200-series transceivers.

The following information and settings options are contained in the tab:

WLAN Mode: Use this control to change the wireless LAN mode of the unit. Available options are:

- **Disabled:** The unit will not relay wireless LAN traffic.
- **AP:** The unit will be configured as an access point (AP), sometimes also called a wireless access point (WAP). The unit will facilitate connection to the wired network for Wi-Fi-enabled devices.
- **STA:** The unit will be configured as an IEEE 802.11 station.



IMPORTANT


If the **WLAN Mode** option is set to **AP** (access point), the following settings will be made available:

- Disable SSID Broadcasting**
- Network Mode**
- WLAN Security**
- Network Protocol**
- WLAN passphrase**
- WLAN SSID**
- WAN IP Address**
- WAN Netmask**
- DHCP first IP address**
- DHCP last IP address**

If the **WLAN Mode** option is set to **STA** (station), the following settings will be made available:

- Network Address Translation**
- WLAN Security**
- Network Protocol**
- WLAN passphrase**
- WLAN SSID**

Network Address Translation: Network address translation (NAT) is a method of remapping one IP address space into another. This is done by modifying network address information in the IP header of packets while they are being transmitted. This setting specifies whether the NAT feature is active or inactive. Available options are *Enable* and *Disable*.



IMPORTANT

Network address translation modifies the IP address information contained in packets. It has the potential to seriously affect quality of connectivity. Do not modify this setting unless there is a specific need to do so.

Disable SSID Broadcasting: If enabled, this setting prevents the unit from broadcasting its service set identifier (SSID).

Network Mode: Use this setting to choose the Wi-Fi network mode. Available options are:

- **Bridged:** The Wi-Fi interface and the wired LAN are bridged together.
- **Routed:** The data traffic carried by the Wi-Fi interface is routed independently of the traffic carried by the wired LAN.

WLAN Security: Use this parameter to configure the unit's standard Wi-Fi access security settings.

WLAN SSID: Enter the SSID of the wireless LAN in this field.

WLAN passphrase: Enter the secure passphrase of the wireless LAN in this field.

WAN IP Address: Enter the IP address of the unit as applicable to the wide-area network (WAN) that contains the wireless LAN.

WAN Netmask: WAN Netmask: Enter the netmask of the unit, as applicable to the wide-area network (WAN) containing the wireless LAN.



IMPORTANT

The **DHCP first IP address** and **DHCP last IP address** settings are available only if the *Network Mode* option is set to **Routed**.

DHCP first IP address: Use this field to specify a primary DHCP server for the Wi-Fi client.

DHCP last IP address: Use this field to specify a secondary DHCP server for the Wi-Fi client.



IMPORTANT

The **Network Protocol**, **WLAN Default Gateway** and **WLAN Name Server** options are available only if the *WLAN Mode* option is set to **STA**.

Network Protocol: Available options are **DHCP** or **Static**.

- If you select the **DHCP** option, the client will accept its IP Address, netmask, default gateway and DNS server settings from the DHCP server.
- If you select the **Static** option, the IP Address, netmask, default gateway and DNS server settings must be manually configured.



IMPORTANT

The **WLAN Default Gateway** and **WLAN Name Server** settings are available only if the *Network Protocol* option is set to **Static**.

WLAN Default Gateway: Enter the name of the default WLAN gateway in this field.

WLAN Name Server: Enter the name of the WLAN name server in this field.

L2TP tab



IMPORTANT

To change the unit's L2TP settings, make sure that the unit is in *Mesh End* mode or *Mesh Point* mode as shown in “GENERAL tab” (page 38). L2TP controls are not available if the unit is set to *Bridge* mode.

Layer 2 Tunneling Protocol (L2TP) functionality allows Fluidmesh radio transceivers to support integration with virtual private networks (VPNs). By default, Fluidmesh hardware devices are shipped from the factory with L2TP functionality disabled.

To enable L2TP functionality for the unit, click the **Enable L2TP** field, then select the **On** option.



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 *Fluidmesh Networks L2TPv3 Configuration Manual*.

VLAN tab

This tab contains controls to connect the unit to one or more virtual local area networks (VLANs) that are part of the local wireless network.

VLAN-capable Fluidmesh transceivers feature smart VLAN management. The transceiver polls the local network switch for a functional VLAN configuration, and adopts the configuration. There is no need to apply a custom VLAN configuration.



IMPORTANT

For detailed information on the predefined rules for VLAN packet management, refer to the *Rules for packet management table* in the Fluidmesh Installation and Configuration manual for the specific device.

To enable VLAN connectivity, do the following steps:

1. Click the **Enable VLAN field** and select the **On** option.
2. Enter the management identification number of the VLAN (used to communicate with the device's operating system) in the **Management VLAN ID** field.
3. Enter the native identification number (the VLAN ID implicitly assigned to untagged packets received on trunk ports) in the **Native VLAN ID** field.

FLUIDITY tab



IMPORTANT

To change the unit's Fluidity settings, make sure that the unit is in *Mesh End* mode or *Mesh Point* mode as shown in "GENERAL tab" (page 38). Fluidity controls are not available if the unit is set to *Bridge* mode.

Some FLUIDITY parameters cannot be set if other dependent parameters have not been set first. To enable the relevant parameter setting in the left column, choose the relevant *Unit Role* setting from the right column:

To enable the relevant FLUIDITY parameter setting...	...Choose the correct <i>Unit Role</i> setting.
Vehicle ID	Vehicle
Automatic Vehicle ID	Vehicle
Network Type	Vehicle Infrastructure Infrastructure(wireless relay)
Handoff Logic	Vehicle

Fluidity is the proprietary track-side and vehicle-to-ground data transfer protocol developed by Fluidmesh. The protocol ensures usable throughput of up to 500 Mbps for high-speed railway trains and other vehicles capable of traveling at up to 225 mph (360 Km/h), under optimal wireless link conditions.

The following basic information and settings options are contained in the tab:

Unit Role: Fluidmesh radio transceivers are shipped from the factory with Fluidity functionality disabled. Enable Fluidity functionality by clicking this drop-down and clicking the correct option from the list below:

- **Infrastructure:** Choose this setting if the unit is connected to a wired LAN and/or a network that includes other Infrastructure nodes, and the unit acts as the network infrastructure entry point for mobile vehicles.
- **Infrastructure (wireless relay):** Only choose this setting if the unit is used as a wireless relay agent to other infrastructure units.



IMPORTANT

If a unit is set to *Infrastructure (wireless relay)* mode, do not connect the unit to the wired LAN.

Vehicle: Choose this setting if the unit is installed on or in a moving vehicle. If the **Unit Role** has been set as **Vehicle**, assign the unit a vehicle identity using either of the methods below:

- **Automatic Vehicle ID:** Allow the unit to automatically generate a unique vehicle identity by clicking this field, then selecting the **On** option.
- **Vehicle ID:** Manually assign a vehicle identity by clicking the **Automatic Vehicle ID** field and selecting the **Off** option, and manually entering an identification string in the **Vehicle ID:** field.



IMPORTANT

If vehicle identities have been manually assigned, the **Vehicle ID** string must be unique for every individual Fluidmesh unit operating on the same network, even if more than one Fluidmesh unit is installed on the same vehicle.

Network Type: Select the correct network type designation for the unit by clicking this 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.



CAUTION

The following settings are intended for use by qualified network engineers. Do not change these settings unless there is a specific need to do so. For detailed information on how to set Handoff logic and Rate adaptation, refer to the *Fluidmesh Networks Fluidity Configuration Manual*.

Handoff Logic: Select the correct handoff logic setting for the unit by clicking the drop-down and clicking the correct option from the list below:

- **Standard:** The unit connects to the transceiver providing the strongest signal.
- **Load Balancing:** The unit connects to the transceiver that provides the most suitable balance between signal strength and the amount of traffic presently being carried.
- **Allow V2V:** in cases where a vehicle-mounted unit is not able to communicate directly with an infrastructure point, this setting allows data traffic to be routed from the source vehicle through a second vehicle, to an infrastructure point.



IMPORTANT

If the **Allow V2V** setting is chosen, note the following points:

- Communication between vehicle radio units that bypasses infrastructure radio units is not supported.
- A maximum of two hops are allowed (for example, vehicle-to-vehicle-to-infrastructure).

Rate Adaptation: Select the correct rate adaptation setting for the unit by clicking the drop-down and clicking the correct option from the list below:

- **Standard:** This option applies a standard reactive rate selection, as used by WiFi access points.
- **Advanced:** This option applies Fluidmesh's proprietary predictive AI-powered algorithm.

FLUIDITY ADVANCED tab

This tab contains controls to adjust the load-balancing, handoff and network optimization characteristics of a radio transceiver unit. These characteristics are calculated according to the following functions:

Degree of Preference

Degree of Preference (DoP) is a metric that represents a transceiver unit's current level of utilization (referred to as 'load'). DoP is updated every five seconds, as well as when handoffs, topology changes and similar events occur within the network.

Higher DoP values correspond to increased load levels. DoP is expressed as a ratio of utilization in inverse proportion to preference for establishing a connection. In other words, the higher its current load, the less suitable a unit is considered for the purpose of carrying a greater load.

Each unit continuously advertises its DoP value. Mobile units use the DoP values of infrastructure units to determine the 'best' AP with which to connect (referred to as 'load-balancing handoff'). Infrastructure units use the DoP values of mobile units to perform admission control when handoff requests are received.

Selection of 'best' Infrastructure unit

An infrastructure unit is considered eligible for handoff by a mobile unit if:

- The two units are already connected.
- The RSSI of the infrastructure unit is above the critical RSSI threshold.
- The infrastructure unit's advertised DoP is lower than the configured DoP limit.
- The infrastructure unit is not blocked (in other words, it has not rejected a handoff request in the last 15 seconds).

- The infrastructure unit is not currently banned by the pole-ban algorithm.
- The number of clients already connected to the infrastructure unit is lower than the configured limit.

Mobile units constantly evaluate and choose the best possible infrastructure unit operating on the current frequency on the basis of the infrastructure unit's RSSI and DoP values. The optimal unit is chosen as the one providing:

- The highest RSSI (within the `rssi-delta` dBm value, from the strongest value received).
- The lowest DoP.

In case of multiple Infrastructure units operating on the same frequency and whose RSSI values differ for more than the `rssi-delta` dBm value, the RSSI value always takes priority over the DoP value.

RSSI zones threshold in correlation with Handoff hysteresis thresholds

These settings are safeguards against handoffs happening too late (in other words, against an unreasonably long period of time between received signal strength from the connected unit falling too low, and a handoff request from a relief unit). The relationship between these three settings governs whether handoff will take place from one unit to another, based on a difference in comparative signal amplitude values over a period of time.

For example, if mobile unit A simultaneously approaches static unit B (which is closer) and static unit C (which is farther away), and the RSSI (received signal strength) from unit B is currently stronger than the RSSI from unit C, it is assumed that if the movement of the mobile unit is predictably linear, then the RSSI from unit B is likely to peak, and then decrease, in proportion to relative distance. At the same time this happens, the RSSI from unit C will still be increasing.

At some point in this progression, the mobile unit must decide:

- *Whether* to accept a handoff request from unit B, and break contact with unit A.
- *When* the handoff will happen.

Handoff hysteresis is defined as the likelihood of a handoff from one unit to another, based on relative averages of RSSI strengths in the recent past. In this context, it can be called an 'ideal handoff zone' whose boundaries are the *Handoff hysteresis high threshold* and *Handoff hysteresis low threshold*. Within this zone, handoff will happen from static unit C to mobile unit A if the average RSSI detected by mobile unit A from static unit C is higher than the average RSSI from static unit B.

If mobile unit A is currently connected to static unit B and initiates a handoff request to static unit C, the handoff will be accepted or denied based on the outcome of the following scenarios:

Scenario 1: The handoff will be accepted if the current RSSI between units A and B is:

- Greater than the *RSSI low/high zones threshold*.
- Less than the combined values of the current RSSI between units A and C, and the *Handoff hysteresis high threshold*.

Scenario 2: The handoff will also be accepted if the current RSSI between units A and B is:

- Less than the *RSSI low/high zones threshold*.
- Less than the combined values of the current RSSI between units A and C, and the *Handoff hysteresis low threshold*.

Scenario 3: If neither set of conditions above are met, the handoff will not be initiated.



IMPORTANT

Some FLUIDITY ADVANCED parameters cannot be set if other dependent parameters have not been set first.

To enable the relevant FLUIDITY ADVANCED parameter setting in the left column, open the FLUIDITY tab and choose the relevant *Unit Role* setting from the right column:

To enable the relevant FLUIDITY ADVANCED parameter setting...	...Choose the correct Unit Role setting.
Large Network Optimization	Vehicle Infrastructure Infrastructure(wireless relay)
Routes	Vehicle Infrastructure Infrastructure(wireless relay)
Degree of Preference Limit	Vehicle Infrastructure Infrastructure(wireless relay)
Degree of Preference Bias	Vehicle Infrastructure Infrastructure(wireless relay)
Per-Client DoP overhead	Vehicle Infrastructure Infrastructure(wireless relay)
Warm Up Time	Vehicle Infrastructure Infrastructure(wireless relay)
Infra. Timeout	Vehicle Infrastructure Infrastructure(wireless relay)
Handoff hysteresis high threshold	Vehicle
Handoff hysteresis low threshold	Vehicle
RSSI low/high zones threshold	Vehicle
Max Clients Number	Infrastructure Infrastructure(wireless relay)
Backhaul Check	Infrastructure
Mesh End Backhaul Check	Infrastructure

The following advanced information and settings options for Fluidity are contained in this tab:

Large Network Optimization: It is recommended that you enable this option for larger Layer-2 Fluidity networks with star topology. Enabling this option activates a data transmission schema that is better optimized for large wireless networks, enables Mesh-end-only pseudo-wire creation, and disables Spanning Tree Protocol (STP) forwarding. Disabling this option disables Mesh-end-only pseudo-wire creation, and sets the STP forwarding parameter to *Auto*.

Max Clients Number: If the unit is set in *Infrastructure* mode, use this setting to limit the maximum number of mobile units that are allowed to connect to the unit at the same time. Enter 0 to specify an unlimited number of mobile units.

Backhaul Check: Use this setting to allow the unit to choose its handoff status if its wired Ethernet connection is compromised in any way. Options are as follows:

- **Handoff-inhibition** (If the unit is an *Infrastructure* unit, it will not be eligible for handoff if its Ethernet ports are not connected to the backhaul.)
- **Relay-switch** (If its Ethernet connection is compromised, the unit will switch to *Wireless Relay* mode until the Ethernet connection is restored.)
- **Disabled** (The unit will be eligible for handoff regardless of its Ethernet status.)

Mesh End Backhaul Check: Use this setting to allow the unit to choose its handoff status if the connection to the closest *Mesh End* unit is compromised in any way. Options are as follows:

- **Handoff-inhibition** (If the unit is an *Infrastructure* unit, it will not be eligible for handoff if the closest *Mesh End* unit cannot be contacted.)
- **Relay-switch** (If the closest *Mesh End* unit cannot be contacted, the unit will switch to *Wireless Relay* mode until the *Mesh End* unit is online.)
- **Disabled** (The unit will be eligible for handoff regardless of the status of the closest *Mesh End* unit.)

Routes: If needed, use this setting to restrict the radio unit types to which the local unit can hand off transmissions. Options are as follows:

- **Backhaul** (the unit will hand off transmissions to units that are set in *Infrastructure mode* only).
- **All** (the unit will hand off transmissions to units of any type. It is recommended that you select this option if the unit is set in *vehicle-to-vehicle* (V2V) mode.)

Degree of Preference Limit: Use this parameter to set the DoP upper limit. The unit will not attempt or accept handoff requests if the current

DoP value exceeds this threshold. To disable the DoP limit, set the value to zero.

Degree of Preference Bias: Use this parameter to set the fixed bias value that is applied to the computed DoP value to give greater (positive) or less (negative) importance to a Fluidity access point for load-balancing purposes. This value can be negative.

Per-Client DoP overhead: Use this parameter to set the overhead value that is applied to each DoP advertised by connected clients. The value dictates the limit for overhead that is introduced by connected devices.

Warm Up Time: If the unit is set in *Infrastructure* mode or *Vehicle* mode, use this setting to adjust the warm-up time (in milliseconds) after the unit is powered ON. During the warm-up time, the unit will not accept handoff requests if it is in *Infrastructure* mode, and will not attempt to connect to the network if it is in *Vehicle* mode.

Infra. Timeout: If the unit is set in *Vehicle* mode, use this setting to adjust the time period for which the unit's infrastructure records are saved. If the unit does not receive a signaling packet from the closest *Infrastructure* unit within this period of time, it will discard all information associated with that Infrastructure unit.

Handoff hysteresis high threshold: Use this parameter to specify the optimal upper handoff hysteresis threshold.

Handoff hysteresis low threshold: Use this parameter to specify the optimal lower handoff hysteresis threshold.

RSSI low/high zones threshold: Use this parameter to specify the optimal RSSI low/high zone threshold value.

FLUIDITY POLE BAN tab

The Pole Ban function can greatly reduce sudden degradations in bandwidth that happen when a unit moving at speed approaches, then leaves behind, a second unit (for example, when a unit mounted in a railway carriage approaches, then leaves behind, a unit mounted at trackside).



IMPORTANT

Certain FLUIDITY POLE BAN parameters cannot be set if other dependent parameters have not been set first.

To enable the relevant FLUIDITY POLE BAN parameter setting in the left column, choose one of the *Pole Ban Mode* parameters on the right:

To enable the relevant FLUIDITY POLE BAN parameter setting...	...Choose the correct Pole Ban Mode parameter.
Pole Ban RSSI Threshold (dB)	Slow
	Fast
Pole Ban Interval (ms)	Slow
	Fast
Pole Ban Pause (ms)	Slow
	Fast
Pole Ban Min Rssi (dB)	Slow
	Fast

The following information and settings options are contained in the tab:

Pole Ban Mode: Use this setting to switch the Pole Ban function on or off. Options are as follows:

- **Disable** (Switches the Pole Ban function off.)
- **Slow** (Switches the Pole Ban function on, and optimizes the function for slow-moving vehicles. Use this setting if mobile units are expected to move at between 0 and 25 MPH (0 and 40 Km/h).)
- **Fast** (Switches the Pole Ban function on, and optimizes the function for fast-moving vehicles. Use this setting if mobile units are expected to move at more than 25 MPH (40 Km/h).)

Pole Ban RSSI Threshold (dB): Use this setting to adjust the lower signal-strength threshold (in Decibels) at which the signal from the affected static unit will be ignored by the mobile unit.

Pole Ban Interval (ms): Use this setting to adjust the time (in ms) for which the signal from the affected static unit will be ignored by the mobile unit.

Pole Ban Pause (ms): Use this setting to adjust the time (in ms) for which signal termination between the affected static unit and the mobile unit will be delayed after signal strength falls to the level of the *Pole Ban RSSI Threshold*.

Pole Ban Min Rssi (dB): Use this setting to adjust the lower signal-strength threshold (in Decibels) at which the mobile unit will attempt to connect to a secondary infrastructure unit.

FLUIDITY FREQUENCY SCAN tab



IMPORTANT

Some FLUIDITY FREQUENCY SCAN parameters cannot be set if other dependent parameters have not been set first.

To enable the relevant FLUIDITY FREQUENCY SCAN parameter setting in the left column, enable the option shown in the right column:

To enable the relevant FLUIDITY FREQUENCY SCAN parameter setting...	...Enable the relevant option.
Scan Isolation (ms)	Enabled if <i>Frequency Autoscan</i> enabled.
Scan List	Enabled if <i>Frequency Autoscan</i> enabled.
Frequency Scan Periodic Enable	Enabled if <i>Frequency Autoscan</i> enabled.
Scan RSSI Threshold Enabled	Enabled if <i>Frequency Autoscan</i> enabled.
Frequency Scan Periodic (s)	Enabled if <i>Frequency Scan Periodic Enable</i> enabled.
Scan RSSI Threshold (dB)	Enabled if <i>Scan RSSI Threshold Enabled</i> enabled.

These controls are used where mobile Fluidity units are configured with different frequencies. When Fluidity is enabled as part of a mobile infrastructure (for example, on a rail train where each rail car is connected to a following rail car), each unit must be configured with a set of frequency / channel-width values.

If the mobile unit is disconnected from the infrastructure for a specified period of time, or the radio signal strength indication (RSSI) is below a specified threshold, the mobile unit will scan the specified list of frequencies. If it finds another Fluidity-enabled unit that is set to one of the specified frequency / channel-width values, it will connect to that unit.

The following information and settings options are contained in the tab:

Frequency Autoscan: Use this switch to enable or disable automatic scanning for other *Infrastructure* units or *Vehicle* units on the same network.

Scan Isolation (ms): Use this field to enter the time (in ms) after which the unit will automatically scan for an alternative *Infrastructure* unit if it loses its connection to the network Infrastructure.

Scan List: This control is used to create and save a list of frequency channels. The unit will scan this list for the presence of other Fluidity-enabled units on the same network. Use the Scan List by doing the following steps:

1. Click the *Scan List* field for the unit.
 - The *Frequency Autoscan List* dialog will be shown.
2. Click the *frequency-value* drop-down, and click the correct frequency to scan.
3. Click the *channel-width* drop-down, and click the correct channel width.



IMPORTANT

The chosen frequency and channel width must exactly match the values of the unit to which the local unit is expected to connect. A frequency and/or channel width mismatch will result in degraded or non-existent communication between the units.

4. To add another frequency/channel-width listing, choose a different frequency and, if needed, a different channel width, then click the green **+** **Add** button.
 - The chosen frequency and channel width values will be listed on the *Frequency Autoscan List* dialog.
5. Save the Scan List settings by clicking the blue **Update** button.
 - The chosen frequency and channel width values will be listed in the *Scan List* field for the unit.

Frequency Scan Periodic Enable: Use this switch to enable or disable periodic scanning for other *Infrastructure* units or *Vehicle* units on the same network.

Frequency Scan Periodic (s): Use this field to enter the time period (in seconds) at which the unit will scan for *Infrastructure* units if its connection to the network Infrastructure is lost.

Scan RSSI Threshold Enabled: Use this switch to enable or disable scanning for other *Infrastructure* units or *Vehicle* units if network signal strength falls below a specified threshold.

Scan RSSI Threshold (dB): Use this field to enter the lower network signal strength threshold (in Decibels) at which the unit will scan for alternative Infrastructure units.

MISC tab



IMPORTANT

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

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

- FIPS: *FM-FIPS*
- PROFINET: *FM-PROFINET*
- QNET: *FM-QNET*

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

Contact your Fluidmesh Networks representative for details.

The following information and settings options are contained in the tab:

Name: The device name, as used to identify the unit in context of other Fluidmesh devices and utilities. Enter a unique reference name for the unit by clicking the field, and entering the text of the name.



NOTE

When entering the device name, the following characters are not allowed: ‘ “ ` \$ = and spaces created by using the keyboard's *Space* key.

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.

Profinet: To enable PROFINET support for the unit, make sure the *FM-PROFINET* plug-in is installed, then click the field and click the switch to ON.

Fips: To enforce FIPS 140-2 compliance for data transmitted by the unit, make sure the *FM-FIPS* plug-in is installed, then click the field and click the switch to ON.

QNET: To enable QNET support for the unit, make sure the *FM-QNET* plug-in is installed, then click the field and click the switch to ON.

Reset Button Function: Set the functionality of the unit's hardware Reset button by clicking the drop-down and clicking the needed option as described below:

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



NOTE

If the *Disabled* option is chosen, you can still reboot or do a hard reset of the unit using the unit's offline Configurator GUI. For instructions, refer to the *Resetting the unit to factory defaults* section of the Fluidmesh Installation and Configuration manual for the specific device.

SPANNING TREE tab

Spanning Tree Protocol (STP) is a network protocol that builds a logical topology for Ethernet networks. STP includes backup links to provide fault tolerance if an active link fails, and renders the network topology free of bridge loops. (These are undesirable because of excessive broadcast radiation, and the network interference that can result from it.)

STP creates a tree-like link structure within a network of connected layer-2 bridges. If any loops (multiple possible paths between switches) are found in the network topology, the network switches will co-operate to disable ports, ensuring that only one active path can be taken from one device to any other device in the layer 2 network.

The tab also contains controls for Bridge Protocol Data Unit (BPDU) snooping and forwarding. BPDUs are frames that contain information about the spanning tree protocol.

The following information and settings options are contained in the tab:

BPDU Snooping: This setting controls the unit's ability to include or exclude itself from the current spanning tree configuration, based on the contents of the BPDUs it intercepts. Available options are On and Off.

BPDU Forwarding: This setting controls the unit's ability to forward or block data transmissions through itself, based on the contents of the BPDUs it intercepts. Available options are:

- **Pass** (This is an override setting. Use this setting if the unit must pass all data traffic regardless of BPDU content.)
- **Auto** (Use this setting if the unit must pass or prohibit data traffic based on the relevant BPDU content.)
- **Stop** (This is an override setting. Use this setting if the unit must prohibit data traffic regardless of BPDU content.)

Link Guard: This setting contains the Link guard time (in seconds). This time interval is used by the unit to check that the wireless network has reached a stable condition before co-ordinating data traffic exchange.

QOS tab

This tab also contains controls for Quality of Service (QoS) and Class of Service (CoS).

Quality of Service refers to measurement of traffic prioritization and resource reservation control mechanisms. It is defined as the ability to

effectively assign different priorities to different applications, users, or data flows, or to guarantee a certain level of performance for a data flow.

Class of Service is a parameter used in data and voice protocols to differentiate the types of payloads contained in the packet being transmitted. The objective of this differentiation is to assign priorities to a data payload, or access levels to a telephone call. CoS is a three-bit field, present in an Ethernet frame header when 802.1Q VLAN tagging is used. The field specifies a priority value between 0 and 7 that can be used by quality of service (QoS) disciplines to differentiate, shape or police network traffic.

The following information and settings options are contained in the tab:

QoS Enable: Use this switch to enable or disable QoS processing.

CoS Map: Use this parameter to specify the CoS re-mapping vector. This is always expressed as a string of eight values. For example, *0 1 2 3 4 5 6 7* can be used for transparent 1:1 mapping. As another example, *7 6 5 4 3 2 1 0* will invert the priorities.

CoS Shaping: Use this parameter to activate per-CoS shaping. Available options are *Enabled* and *Disabled*.

CoS Shaping Rates: Use this parameter to specify the CoS shaping rates. These are always expressed as a string of eight values containing the shaping bitrate (in Kbps) for each class-of-service.



IMPORTANT

The sum of the CoS shaping rates (expressed in Mbps) cannot exceed the total bandwidth value of the bandwidth license currently installed on the unit.

It may be possible to upgrade the unit's bandwidth-handling capability by using a higher-specification bandwidth plug-in. For a complete list of available software plug-ins for your Fluidmesh hardware unit, refer to the *Available plugins* section of the Fluidmesh Installation and Configuration manual for the specific device.

QoS 802.1P: If *Enabled*, this parameter forces Type of Service (ToS) reading from VLAN tags. If *Disabled*, ToS data will be read from the TOS/DSCP field in layer-3 packets.

MPLS tab

This tab contains controls for adjustment of the unit's multiprotocol label switching (MPLS) settings. MPLS is a data-carrying technique that directs data from one network node to the next, based on short path labels. This avoids the need for complex look-ups from a routing table.

The following information and settings options are contained in the tab:

Unicast flooding: This setting controls the unit's restrictions on unicast flooding (in other words, unicast frames being sent to all forwarding ports within the respective VLAN). Available options are:

- **Enable** (Unicast flooding is permitted to private IP addresses only.)
- **Disable** (Unicast flooding is disabled.)
- **Unrestricted** (Unicast flooding is unconditionally permitted, with forwarding of packets carrying non-private IP addresses allowed.)



IMPORTANT

Wherever possible, unicast flooding should be avoided, as it may negatively impact the available capacity of the wireless network.

Arp Unicast: Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address associated with a given internet layer address. This setting specifies whether the unit is allowed to treat unicast ARP packets as broadcast packets. Available options are *Enable* and *Disable*.

Pseudo-wires set: A pseudo-wire is an emulated point-to-point connection over the wireless network. This setting specifies the unit types with which the local unit is allowed to establish pseudo-wires. Available options are:

- **Mesh-ends only:** The unit is permitted to establish label-switched paths (LSPs) with *Mesh End* units only.
- **All:** The unit is permitted to establish LSPs with units of any type.

Cluster ID: Enter the MPLS layer-2 mode cluster identity number in this field.

FAST FAILOVER (TITAN) tab

This tab contains controls to enable fast fail-over capability on networks where redundant (backup) units are installed. If a primary unit and secondary unit are installed at the same location, and the primary unit fails, TITAN enables seamless switch-over to the secondary unit, allowing uninterrupted network performance.



IMPORTANT

Fast fail-over capability must be enabled using a software plug-in (Fluidmesh part number *FM-TITAN*). Contact your Fluidmesh Networks representative for details.

The following information and settings options are contained in the tab:

Fast Failover Status: This setting specifies whether the fast fail-over feature is active or inactive. Available options are *Enable* and *Disable*.

Fast Failover Timeout (ms): If the unit has been set as the primary unit, and fails, this setting specifies the time period (in ms) after failure in which the secondary unit will take over as the network link.

The Fast Failover WAN Delay controls are used in Layer-3 Fluidity applications only. These parameters facilitate an additional delay on the WAN interface of the local *Mesh End* unit's L2TP tunnel, allowing the network to establish a stable pre-failover condition. The settings are as follows:

- **Fast Failover WAN Delay Enabled:** This setting specifies whether the fast fail-over WAN delay feature is active or inactive. Available options are *Enable* and *Disable*.
- **Fast Failover WAN Delay (ms):** Use this field to specify the delay (in ms) before the WAN IP address information used by the L2TP tunnels is updated.

Virtual (hot-standby) IP address: Use this field to enter the IP address of the secondary (redundant) unit if the local unit is part of a layer-3 scenario. Note that this parameter only needs to be set if the unit being configured is a global gateway, or a transceiver unit aboard a moving vehicle.

Fast Failover Preempt Delay (ms): If the local unit is a primary unit that has failed and recovered, this setting specifies the time period (in ms) after failure in which the local unit will take over from the secondary unit as the network link.

ARP tab

Address Resolution Protocol (ARP) is a protocol used for discovering MAC addresses that are associated with IP addresses. To get this information, Fluidmesh hardware devices may transmit gratuitous ARP packets.

In context of ARP, *Gratuitous* refers to a request and/or reply that is sent outside of the conventional ARP specification.

Within an address resolution protocol (ARP) scenario, transmission of gratuitous ARP packets may improve the time taken by Ethernet switches to react to changes in network topology.

The following information and settings options are contained in the tab:

Gratuitous arp: This setting specifies whether the gratuitous ARP feature is active or inactive. Available options are *Enable* and *Disable*.

Gratuitous arp Delay (ms): This field specifies the delay (in ms) before gratuitous ARP packets are forwarded by the unit.

INTRA-CAR tab



IMPORTANT

To enable the Intra-car parameter settings, navigate to the *General* tab, and switch the **Mode** setting to *Bridge*.

This tab contains controls to create and maintain a wireless backbone network throughout a physically large, compartmentalized vehicle (for example, a railway train), in which each compartment (for example, a rail car) has its own wireless relay link to another compartment. This allows an in-car, end-to-end backbone infrastructure to be created for train-to-ground data transfer.

A typical example of the scenario described above could be a locomotive, connected to multiple rail cars. For this intra-car scenario, the design assumptions are as follows:

- Each rail car has its own internal, wired switched network (for example, through on-board switches).
- Any rail car can be randomly exchanged with any other rail car.
- The relevant antennas are installed in such a way that if two cars are connected to one another, the signal amplitude between the antennas bridging the two cars is higher than between either of the two cars and any other car. (In other words, if cars C, D, E and F are connected in series, the signal amplitude between cars D and E is higher than, say, between car D and cars C or E, or between car E and cars D or F.)
- Existing wireless links that fall below a set amplitude threshold are not considered for association (for example, adjacent trains currently idle in a train depot).

The following information and settings options are contained in the tab:

Intra-car Mode: This setting specifies whether Intra-car Mode is active or inactive. Available options are *Enable* and *Disable*.

RSSI Threshold (delta): This field specifies the average signal strength value (in Decibels) that is needed to maintain a wireless link between the unit and its connected unit. If average signal strength consistently falls below this value, the wireless connection between the unit and its connected unit will be terminated.

RSSI Threshold (min): This field specifies the minimum instantaneous signal strength value (in Decibels) that is needed to maintain a wireless link between the unit and its connected unit. If instantaneous signal strength falls below this value, the wireless connection between the unit and its connected unit will be terminated.

Car ID: If the unit is being used in an intra-car role, enter a unique identity number for the unit in this field.

REMOTE ACCESS tab

This tab contains controls to change the Administrator's user name and password for the Fluidmesh unit, and to enable remote access to the unit using Telnet.



IMPORTANT

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

The Telnet protocol suffers from serious security weaknesses that limit its usefulness in environments where the network cannot be fully trusted. Telnet is used at your own risk.

The following information and settings options are contained in the tab:

Username: The default administrator user name is *admin*. To change the user name, click the entry field, then enter the new user name.

Password: The default administrator password is *admin*. To change the password, click the entry field, then enter the new password.



IMPORTANT

Only alphanumeric characters and the `_` - and `.` characters are allowed. The password must contain a minimum of eight characters, including at least one uppercase letter and at least one number.

Telnet: Click the entry field, then click the switch ON to enable Telnet access, or OFF to disable access.

VIEW MODE SETTINGS tab

This tab contains controls that allow the system administrator to grant or deny lower-level users access to device configuration settings by category.

To gain editing privileges for the View Mode settings window, you must have the correct administrator user name and password.

The following information and settings options are contained in the tab:

View Mode Username: To change the administrator user name for the current user, click the entry field, then enter the new administrator user name.

View Mode Password: To change the administrator password for the current user, click the entry field, then enter the new password.



IMPORTANT

Only alphanumeric characters and the _ - and . characters are allowed. The password must contain a minimum of eight characters, and at least one uppercase letter and one number.

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

1. Click the relevant setting field.
2. Click the switch ON to enable access to the setting for lower-level users, or OFF to disable access.

PLUG-INS tab

This tab shows which software plug-ins are currently active on the unit. It also contains controls that allow you to activate uploaded software plug-ins for use with the unit, and deactivate uploaded software plug-ins so they can be used on other Fluidmesh units.



IMPORTANT

For a complete list of software plug-ins that are currently available for, and compatible with the unit, refer to the *Available plug-ins* section of the Fluidmesh Installation and Configuration manual for the specific device.

If a plug-in is firmware-embedded, or has already been installed for the unit, a green **active** icon will be shown (below).



NOTE

To uninstall an active plug-in so it can be used on another unit, refer to the *Deactivating an active plug-in* section of the Fluidmesh Installation and Configuration manual for the specific device.

To view current plug-in status and activate or deactivate software plug-ins, do the following steps:

1. If you have purchased a license code to activate a plug-in, click the relevant plug-in field, then click the switch ON to activate the plug-in.
 - If you click the switch ON to activate the plug-in and FM Racer informs you that the plug-in is not installed, contact support@fluidmesh.com for assistance.

2. If you have purchased a license code to activate a *Bandwidth* plug-in, a *Fluidity-Bandwidth Mobile* plug-in or a *Fluidity-Bandwidth Trackside* plug-in, click the relevant plug-in field, then click the relevant plug-in listing to activate the plug-in.

STATIC ROUTES tab

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 Fluidmesh 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 Fluidmesh 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 for a unit, do the following steps:

1. Click the blue **View / Edit** button under the **STATIC ROUTES** heading to open the entry form.
2. Click the blue **Edit** button on the entry form.
 - The **Static Routes** entry form will be shown.
3. Enter **Subnet**, **Netmask** and **Gateway** designators in the relevant fields.
4. Click the blue **Update** button.
 - If the new static route is valid, it will be added to the *Active static routes* list.
5. If needed, add entry fields for another static route by clicking the green **Add Routes +** button, and completing the form as shown above.

Pass list / Block list tab



IMPORTANT

To change the unit's Pass list or Block list settings, make sure that the unit is in *Mesh End* mode or *Mesh Point* mode as shown in "[GENERAL tab](#)" (page 38). Pass list / Block list controls are not available if the unit is set to *Bridge* mode.

The Pass list / 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 Fluidmesh 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 Fluidmesh 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

For detailed instructions on how to create Pass lists and Block lists, refer to the *Pass lists and Block lists* section of the Fluidmesh Installation and Configuration manual for the specific device.


To upload a *.CSV-format Pass list or Block list to a unit, do the following steps:

1. Click the blue **View / Edit** button under the **Pass lists / Block lists** heading.
2. Click the blue **Upload File** button.
 - The Pass list / Block list entry form will be shown.
3. Specify whether a Pass list or Block list is being uploaded by clicking the correct **Select Type** radio button.
4. Drag-and-drop the Pass list or Blocklist *.CSV file to the **Drop a file here** section of the form.
 - If the link rules contained in the *.CSV file are valid, the rules will be listed in the Pass list / Block list entry form.
5. Set the routing priority for each link rule by clicking the relevant **Priority** drop-down and clicking a priority option.
6. If needed, discard a link rule by clicking the discard button to the right of the rule.
7. Click the blue **Update** button.
 - The Pass list / Block list confirmation dialog will be shown.
 - The Pass list / Block list file will be uploaded to the device.
8. If needed, add more Pass list and/or Block list rules by clicking the blue **Upload File** button and proceeding as shown in this section.

6.3.2. Applying a configuration file to an internet-connected device

Using configuration templates to configure a Fluidmesh device has several advantages over manual configuration of each separate device. Once they are created, configuration templates exist as a baseline that

can be readily and quickly re-used, copied, and modified for different applications, even among devices of the same type.




IMPORTANT

This section shows how to apply configuration settings to a device using a configuration template. If you want to apply configuration settings to a device without using a configuration template, refer to [“Specifying configuration parameters without a template” \(page 31\)](#) for instructions.

To apply configuration settings to your Fluidmesh device using a saved configuration template, do the following steps:

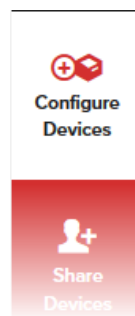
1. Create a new configuration template as shown in [“Creating a new configuration template” \(page 20\)](#), or copy and modify a pre-defined configuration template as shown in [“Copying and modifying a pre-defined configuration template” \(page 24\)](#).



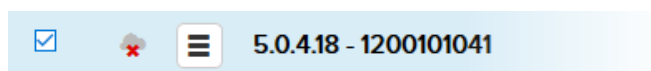
IMPORTANT

Configuration templates are always created for specific product lines (in other words, for specific firmware versions). Note that a template created for a product line cannot be used on any other product line.

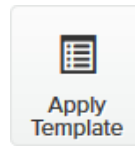
2. Click the **Configure Devices** link on the left side of the FM Racer interface (below).



- The **RACER™ Radio Configuration** view will be shown.
3. Identify the device that must receive the configuration template.
 4. Check the check-box to the left of the device listing (below).



5. Click the **Apply Template** button (below).



- The **Select Configuration Template** dialog will be shown.
6. Click the **Select template** drop-down.
 - A list of currently available templates that can be applied to the device will be shown.
 7. Click the needed template to select it, and click the blue **Apply Template** button.
 - The configuration template will be applied to the device.
 8. Click the blue **Save** button to save the device configuration.
 - If there are any configuration errors that must be corrected, an **ERROR** dialog will be shown. Correct the errors, then save the device configuration.

6.3.3. Applying a configuration file to a device that is not connected to the internet

If needed, a FM Racer configuration file can be applied to a single device or multiple devices that are not connected to the Internet. The devices can be of the same product line, or different product lines.

An exported configuration file in *.FMCONF format can contain configuration settings for one device or multiple devices, no matter whether the devices are of the same type or different types. Every Fluidmesh device is capable of parsing, recognizing and acquiring only the relevant settings for its own configuration.




IMPORTANT

Configuration templates must be downloaded from the **RACER™ Radio Configuration** view. Templates cannot be downloaded from the **Configuration Templates** view.

To apply a configuration file to a non-connected device, do the following steps:

1. Configure a Fluidmesh device of the same type or types as the devices that must be configured, using either of the following methods:
 - Create a new configuration template as shown in [“Creating a new configuration template” \(page 20\)](#).

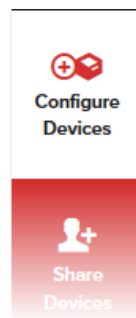
- Copy and modify a pre-defined configuration template as shown in “[Copying and modifying a pre-defined configuration template](#)” (page 24).



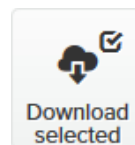
IMPORTANT

Configuration templates are always created for specific product lines (in other words, for specific firmware versions). Note that a template created for a product line cannot be used on any other product line.

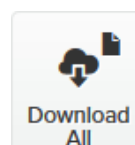
2. Click the **Configure Devices** link on the left side of the FM Racer interface (below).



- The **RACER™ Radio Configuration** view will be shown.
3. Identify the device or devices for which configuration templates were created in [Step 1](#) above.
 4. Download the needed template or templates, using either of the following methods:
 - To download only selected templates, check the check-box to the left of each relevant device listing, then click the **Download selected** button (below).



- To download all templates from all currently listed devices, click the **Download All** button (below).



- The template or templates will be downloaded to the chosen download location on your computer as an *.FMCONF file.
5. Upload the *.FMCONF file to your device as shown in the *Uploading a device configuration file from FM Racer* section of the Fluidmesh Installation and Configuration manual for the specific device.



NOTE

Configuration settings for more than one Fluidmesh product line can be added to a single *.FMCONF configuration file. When the configuration file is uploaded to each device, the device automatically parses and loads the correct configuration settings for its device type.

6.3.4. Exporting a configuration file from a device to FM Racer

If needed, offline configuration settings can be exported from a device as a *.CONF configuration file and uploaded to FM Racer for use on devices of the same type.



IMPORTANT

*.CONF configuration files are always created for specific product lines (in other words, for specific firmware versions). A configuration file created for a specific product line cannot be used on any other product line.

To export a configuration file from a device and upload the file to FM Racer, do the following steps:

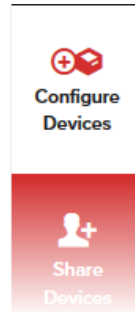
1. Complete the device configuration using FM Racer as shown in [“Configuring your device using FM Racer” \(page 31\)](#). Alternatively, do an offline configuration as shown in the *Device configuration using the Configurator interface* section of the Fluidmesh Installation and Configuration manual for the specific device.
2. Download the unit's configuration (*.CONF) file to your computer as shown in the *Saving and restoring the unit settings* section of the Fluidmesh Installation and Configuration manual for the specific device.



TIP

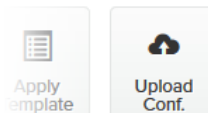
Save the file to a place on your computer where you can find it easily.

3. If needed, repeat step [Step 2](#) above for other Fluidmesh devices.
4. Click the **Configure Devices** link on the left side of the FM Racer interface (below).



- The **RACER™ Radio Configuration** view will be shown.

5. Click the **Upload Conf.** button (below).



- The **Upload Configuration File** dialog will be shown.

6. Upload the *.CONF file saved in step [Step 2](#) to the FM Racer portal. You can do this in any of two ways:
 - Drag-and-drop the *.CONF file to the center of the **Upload Configuration File** dialog.
 - Click the center of the **Upload Configuration File** dialog. Your computer's file explorer dialog will be shown. Use the file explorer dialog to find and upload the correct *.CONF file.
7. The uploaded configuration will be saved as the unit's current FM Racer configuration. If needed, this configuration can be saved as an *.FMCONF (FM Racer format) configuration file by using the FM Racer interface.



NOTE

If a *.CONF file contains errors, or the device from which the *.CONF file was downloaded is not part of your FM Racer portfolio, the **Upload Configuration File** dialog will warn you that the file cannot be uploaded.

8. If a file contains an error, correct the error. If the relevant device is not currently part of your FM Racer portfolio, add the device to your portfolio as shown in [“Adding Fluidmesh devices to your FM Racer portfolio”](#) (page 18).

9. When all errors have been corrected, repeat the configuration upload from step [Step 5](#) above.
 - The **Upload Configuration File** dialog will ask you to confirm the upload. To confirm, click the blue **Save Conf.** button.
 - The unit configuration files will be uploaded to FM Racer.
 - If more than one configuration file has been uploaded for any device, the name of the new configuration template will automatically be incremented from the name of the last template saved for the device.
 - If the saved configuration contains any errors, the **Upload Configuration File** dialog will warn you of the errors after the blue **Save Conf.** button has been clicked. Correct the errors using the FM Racer interface.

To edit a *.CONF file that has been uploaded to FM Racer, refer to [“Copying and modifying a pre-defined configuration template” \(page 24\)](#).

To apply an uploaded *.CONF file to a Fluidmesh device, refer to [“Applying a configuration file to an internet-connected device” \(page 70\)](#).



NOTE

If applying a saved configuration to a device, note the following user-privilege rules:

- Users with *Administrator* privileges can apply uploaded unit configurations to all Online-mode units that are being managed within FM Racer.
- Users with *Viewer* privileges can apply uploaded unit configurations to units that have been assigned to them by users with Administrative privileges.
- Users with *Viewer* privileges cannot apply apply uploaded unit configurations to units that have not been assigned to them.

6.4. Sharing a device with another user

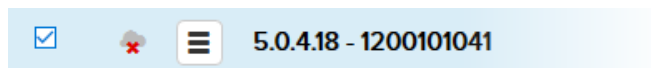
If a Fluidmesh device appears in your *Share Devices* list, responsibility for configuring and maintaining the device can be jointly shared with another Partners Portal user or users. In Fluidmesh terminology, this is known as *Sharing a device*.

To share a device with another user, do the following steps:

1. Click the **Share Devices** link on the left side of the FM Racer interface (below).



- The **Share Devices** view will be shown.
2. Identify the device that must be shared with another user.
 3. Check the check-box to the left of the device listing (below).



4. Click the blue **Share Devices** button.
 - The **Share devices with other users dialog** will be shown.
5. Enter the E-mail address of the chosen user in the **User Email** field.
6. Click the **Privilege** drop-down to show the available privilege options. Click either of the following privilege options:
 - **Admin:** An Admin user can view and change the unit configuration settings, and can assign the unit to other users.
 - **Viewer:** A Viewer can only view the unit configuration settings.



IMPORTANT

The privilege level you are able to assign to other users depends on your personal privilege level. If you are an Admin user, you can assign *Admin* or *Viewer* privileges. If you are a Viewer, you can assign *Viewer* privileges only. If a device is already assigned to a user whose E-mail address you have entered, and you assign a privilege level to that user that is different from their previous privilege level, the old privilege level settings for that user will be overwritten.

7. Click the blue **Share** button.
 - The device will be shared with the specified user.
 - The user will receive a notification E-mail.
 - The device will be listed in the device list of the user's **RACER™ Radio Configuration** view.



TIP

You can assign devices to users who are not yet registered on the Fluidmesh Partners Portal. When the user completes their Partners Portal registration, they will see all devices associated with their account.

6.5. Project management

The FM Racer Projects Management function addresses the need to categorize and organize Fluidmesh-branded elements that form part of a large network installation. It can do this by grouping some or all of the separate elements of a Fluidmesh-oriented telecommunications installation, such as hardware devices, software plug-ins and device software configuration templates, into an easily searchable virtual container called a *Project*.

A project allows the responsible party to more easily categorize and compartmentalize installations, or parts of installations, in relation to other installations.

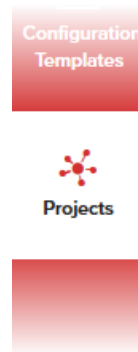
6.5.1. Creating a project

To create a project, or associate a Fluidmesh device or configuration template with a new or existing project, use the appropriate method for your circumstances as shown in this section.

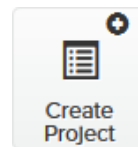
Creating a new project using the Projects view

To create a new project using the Projects view, do the following steps:

1. Click the **Projects** link on the left side of the FM Racer interface (below).



- The **Projects** view will be shown.
2. Click the **Create Project** button (below).

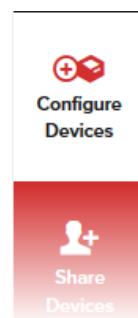


- The **Create Project** dialog will be shown.
3. Enter the name of the project in the **Name** field.
 4. Click the **Type** drop-down and click the chosen project type.
 5. If needed, enter a short description of the project in the **Description** field.
 6. Click the blue **Create** button.
 - The project container will be opened in the *Project* view.

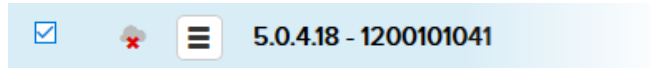
Associating a new or existing project with a Fluidmesh device

To associate a new or existing project with a Fluidmesh device, do the following steps:

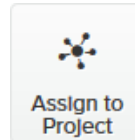
1. Click the **Configure Devices** link on the left side of the FM Racer interface (below).



- The **RACER™ Radio Configuration** view will be shown.
2. Identify the device that must be made part of the new project.
 3. Check the check-box to the left of the device listing (below).



4. Click the **Assign to Project** button (below).

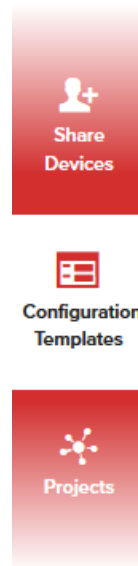


- The **Assign devices to project** dialog will be shown.
5. Associate the device with a project using either of the following methods:
 - To associate the device with an existing project, do the following steps:
 1. Type one or more characters from the project name in the **Type project** field.
 - All project listings that contain the characters will be shown.
 2. Click the correct project listing to select it.
 - The project listing will be selected.
 - To associate the device with a new project, do the following steps:
 1. Click the **+** button.
 - The **Create Project** dialog will be shown.
 2. Complete the dialog as shown in the sub-section above, and click the blue **Create** button.
 - The **Assign devices to project** dialog will be shown.
 6. Click the blue **Assign** button.
 - The device will be associated with the chosen project.

Associating a new or existing project with a device configuration template

To associate a new or existing project with a device configuration template, do the following steps:

1. Click the **Configuration Templates** link on the left side of the FM Racer interface (below).

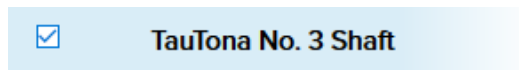


- The **Configuration Templates** view will be shown.
2. Identify the template that must be made part of the new project.

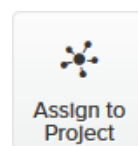


IMPORTANT
Pre-defined templates cannot be associated with projects. Only modified and custom templates can be associated.

3. Check the check-box to the left of the template listing (below).



4. Click the **Assign to Project** button (below).



- The **Assign templates to project** dialog will be shown.
5. Associate the template with a project by doing the following steps:
 - To associate the template with an existing project, do the following steps:
 1. Type one or more characters from the project name in the **Type project** field.
 - All project listings that contain the characters will be shown.

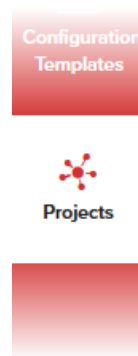
2. Click the correct project listing to select it.
 - The project listing will be selected.
- To associate the template with a new project, do the following steps:
 1. Click the **+** button.
 - The **Create Project** dialog will be shown.
 2. Complete the dialog as shown in the first sub-section above, and click the blue **Create** button.
 - The **Assign templates to project** dialog will be shown.
6. Click the blue **Assign** button.
 - The template will be associated with the chosen project.

6.5.2. Sharing a project with another user

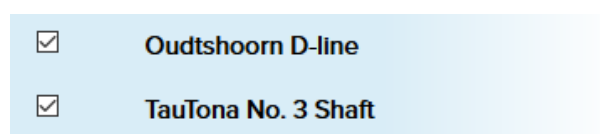
If a project listing appears in your Projects view, responsibility for modifying and maintaining the project can be jointly shared with another Partners Portal user or users.

To share one or more projects with another user, do the following steps:

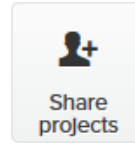
1. Click the **Projects** link on the left side of the FM Racer interface (below).



- The **Projects** view will be shown.
2. Identify the project or projects that must be shared with another user.
 3. Check the check-boxes to the left of the relevant project listings (typical examples are shown below).



- The **Share Projects** button will appear (below).



4. Click the **Share projects** button.
 - The **Share Project** dialog will open.
5. Enter the E-mail address of a person with which you want to share the template in the **Enter valid email addresses** field. If you want to add more than one E-mail address, separate the E-mail addresses with spaces.
6. Click the blue **Share** button.
 - The project details will be distributed to the E-mail addresses you have specified.



NOTE

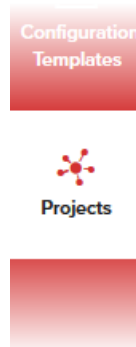
Empty projects (in other words, projects that do not contain devices, software plug-ins or configuration templates) cannot be shared with other users.

6.5.3. Editing the details of a project

The basic details of a project can be edited at any time, as shown in this section.


To edit the basic details of a project, do the following steps:

1. Click the **Projects** link on the left side of the FM Racer interface (below).



- The **Projects** view will be shown.
2. Identify the project that must be edited.
 3. Click the project listing to open the project.

- The project will be shown as a descending series of four sections: **Project** (including the basic details of the project), **Devices**, **Plug-ins**, and **Templates**.
- 4. If needed, view each of the four sections by scrolling down the page.
- 5. Click the black **Edit** button on the upper right-hand corner of the view.
 - The basic details section will be unlocked for editing.
 - Edit the **Name**, **Project Type** and **Description** fields as needed.




IMPORTANT
The **Creation Date** and **Created By** fields cannot be edited.

6. Click the blue **Update** button.
 - The changes will be saved.

The devices, software plug-ins and configuration templates associated with a project can also be changed. To edit the contents of a project, refer to [“Assigning entities to, and removing entities from a project”](#) (page 85).

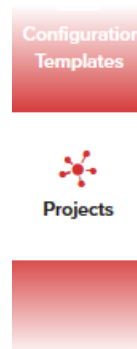
6.5.4. Deleting a project



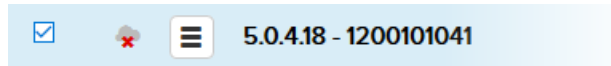
IMPORTANT
If a project is shared with other Partners Portal users, deleting the project from your project list will not remove the project from the project lists of other users.

To delete one or more projects from your project list, do the following steps:

1. Click the **Projects** link on the left side of the FM Racer interface (below).



- The **Projects** view will be shown.
2. Identify the project or projects that must be deleted.
 3. Check the check-box to the left of each relevant project listing (below).



- The **Remove Projects** button will appear.
4. Click the **Remove Projects** button.
 - The **Remove Project** dialog will appear.
 5. Confirm the deletion by clicking the blue **Remove** button.
 - The projects will be removed from your project list.

6.5.5. Assigning entities to, and removing entities from a project

Hardware devices, software plug-ins and configuration templates can be associated with, or removed from, a project. Add an entity to, or remove an entity from a project using any of the appropriate procedures shown below.

Removing a device from a project using the Projects view


To remove a device from a project using the Projects view, do the following steps:

1. Click the **Projects** link on the left side of the FM Racer interface (below).



- The **Projects** view will be shown.
2. Identify the project from which a device must be removed.
 3. Click the project listing to open the project.
 - The project will be shown as a descending series of four sections: **Project** (including the basic details of the project), **Devices**, **Plug-ins**, and **Templates**.

4. Scroll down to the **Devices** section.
 - All devices currently associated with the project will be listed.
5. Identify the device or devices that must be removed from the project.
6. Check the check-boxes to the left of the relevant device listings.
7. Click the **Remove** button.
 - The **Remove Assignment** dialog will appear.
8. Confirm the deletion by clicking the blue **Remove** button.
 - The devices will be removed from the project's **Devices** list.



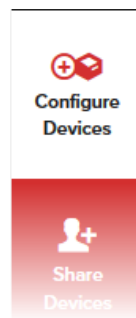
IMPORTANT

If a device is removed from a project, all software plug-ins associated with the device will also be removed from the project.

Adding or removing a device from a project using the RACER™ Radio Configuration view

To add or remove a device from a project using the RACER™ Radio Configuration view, do the following steps:

1. Click the **Configure Devices** link on the left side of the FM Racer interface (below).




- The **RACER™ Radio Configuration** view will be shown.
2. Identify the device that must be added to, or removed from the project.
 3. Check the check-box to the left of the relevant device listing.

Add the device to a project by doing the following steps:

1. Click the **Assign to Project** button.

- The **Assign devices to project** dialog will be shown.
2. Associate the device with a project by using either of the following procedures as needed:
 - To associate the device with an existing project, do the following steps:
 1. Type one or more characters from the project name in the **Type project** field.
 - All project listings that contain the characters will be shown.
 2. Click the correct project listing to select it.
 - The project listing will be selected.
 - To associate the device with a new project, do the following steps:
 1. Click the **+** button.
 - The **Create Project** dialog will be shown.
 2. Complete the dialog as shown above, and click the blue **Create** button.
 - The **Assign devices to project** dialog will be shown.
 3. Click the blue **Assign** button.
 - The device will be associated with the chosen project.

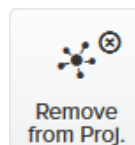


IMPORTANT

If a device is associated with a project different to a project with which it was previously associated, it will be associated with the newly selected project instead. All plug-ins active on the device will also be associated with the new project.

Alternatively, remove the device from a project by doing the following steps:

1. Click the **Remove from Proj.** button (below).



- The **Remove Assignment** dialog will be shown.
2. Click the blue **Remove** button.
 - The device will be deleted from the chosen project.



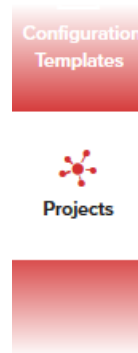
IMPORTANT

If a device is removed from a project, all plug-ins active on the device will also be removed from the project.

Removing a plug-in from a project using the Projects view

To remove a software plug-in from a project using the Projects view, do the following steps:

1. Click the **Projects** link on the left side of the FM Racer interface (below).

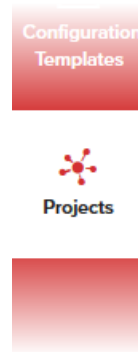


- The **Projects** view will be shown.
2. Identify the project from which a plug-in must be removed.
 3. Click the project listing to open the project.
 - The project will be shown as a descending series of four sections: **Project** (including the basic details of the project), **Devices**, **Plug-ins**, and **Templates**.
 4. Scroll down to the **Plug-ins** section.
 - All plug-ins currently associated with devices that are part of the project will be listed.
 5. Identify the plug-in or plug-ins that must be deleted.
 6. Check the check-boxes to the left of the relevant plug-in listings.
 7. Click the **Remove** button.
 - The **Remove Assignment** dialog will appear.
 8. Confirm the deletion by clicking the blue **Remove** button.
 - The plug-ins will be removed from the project's Plug-ins list.

Adding or removing a plug-in from a project using the Plug-ins view

To add or remove a plug-in from a project using the Plug-ins view, do the following steps:

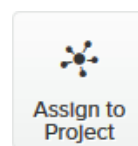
1. Click the **Projects** link on the left side of the FM Racer interface (below).



- The **Projects** view will be shown.
2. Click any of the project listings.
 - The **Plug-ins** view will be shown.
 3. Identify the plug-in or plug-ins that must be added to, or removed from the project.
 4. Check the check-boxes to the left of the relevant plug-in listings.


Add the plug-in to a project by doing the following steps:

1. Click the **Assign to Project** button (below).



- The **Assign plug-ins to project** dialog will be shown.
2. Associate the plug-in with a project by doing the following steps:
 - To associate the plug-in with an existing project, do the following steps:
 1. Type one or more characters from the project name in the **Type project** field.
 - All project listings that contain the characters will be shown.
 2. Click the correct project listing to select it.
 - The project listing will be selected.

- To associate the plug-in with a new project, do the following steps:
 1. Click the **+** button.
 - The **Create Project** dialog will be shown.
 2. Complete the dialog as shown above, and click the blue **Create** button.
 - The **Assign plug-ins to project** dialog will be shown.
 3. Click the blue **Assign** button.
 - The plug-in will be associated with the chosen project.

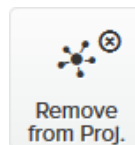


IMPORTANT

If a plug-in is associated with a project different to a project with which it was previously associated, it will be associated with the newly selected project instead.

Alternatively, remove the plug-in from a project by doing the following steps:

1. Deactivate the plug-in as shown in the *Deactivating an active plug-in* section of the Fluidmesh Installation and Configuration manual for the specific device.
2. Check the check-box to the left of the relevant plug-in listing.
3. Click the **Remove from Proj.** button (below).

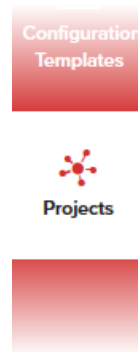


- The **Remove Assignment** dialog will be shown.
4. Click the blue **Remove** button.
 - The plug-in will be deleted from the chosen project.

Removing a template from a project using the Projects view

To remove a configuration template from a project using the Projects view, do the following steps:

1. Click the **Projects** link on the left side of the FM Racer interface (below).

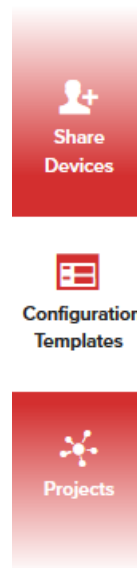


- The **Projects** view will be shown.
2. Identify the project from which a configuration template must be removed.
 3. Click the project listing to open the project.
 - The project will be shown as a descending series of four sections: **Project** (including the basic details of the project), **Devices**, **Plug-ins**, and **Templates**.
 4. Scroll down to the **Templates** section.
 - All templates currently associated with devices that are part of the project will be listed.
 5. Identify the template or templates that must be deleted.
 6. Check the check-boxes to the left of the relevant template listings.
 7. Click the **Remove** button.
 - The **Remove Assignment** dialog will appear.
 8. Confirm the deletion by clicking the blue **Remove** button.
 - The templates will be removed from the project's **Devices** list.

Add or removing a template from a project using the Configuration Templates view

To add or remove a configuration template from a project using the Configuration Templates view, do the following steps:

1. Click the **Configuration Templates** link on the left side of the FM Racer interface (below).



- The **Configuration Templates** view will be shown.
2. Identify the templates that must be added to, or removed from the project.
 3. Check the check-boxes to the left of the relevant template listings.

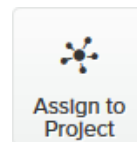


IMPORTANT

Pre-defined templates cannot be associated with or removed from projects. Only modified and custom templates can be associated and removed.

Add the templates to a project by doing the following steps:

1. Click the **Assign to Project** button (below).

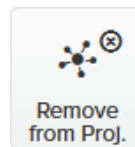


- The **Assign templates to project** dialog will be shown.
2. Associate the template with a project by doing the following steps:
 - To associate the template with an existing project, do the following steps:
 1. Type one or more characters from the project name in the **Type project** field.

- All project listings that contain the characters will be shown.
2. Click the correct project listing to select it.
 - The project listing will be selected.
 - To associate the template with a new project, do the following steps:
 1. Click the **+** button.
 - The **Create Project** dialog will be shown.
 2. Complete the dialog as shown above, and click the blue **Create** button.
 - The **Assign templates to project** dialog will be shown.
 3. Click the blue **Assign** button.
 - The template will be associated with the chosen project.

Alternatively, remove the template from a project by doing the following steps:

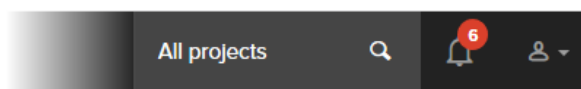
1. Click the **Remove from Proj.** button (below).



- The **Remove Assignment** dialog will be shown.
2. Click the blue **Remove** button.
 - The template will be deleted from the chosen project.

6.5.6. Filtering entities by project

The project search selector (below) is located in the upper right-hand corner of the FM Racer interface.



The selector allows you to search for hardware devices and configuration templates according to project listing. Four different search methods are available:

- You can choose any product listing from a drop-down list.
- You can search among all project listings simultaneously.

- You can search for devices and templates that are not currently assigned to a project.
- If your project list is very large, you can narrow the search by specifying part or all of the project name.

Searching by choosing a project listing from a drop-down list

To search by choosing a project listing from a drop-down list, do the following steps:

1. Click the project search selector's search field.
 - A list of all projects currently linked to your user name will be shown under the search field.
2. Click the correct project listing.
 - The Partners Portal will return the needed search results.
3. Search for the needed hardware device listing by clicking the **Configure Devices** link or **Share Devices** link, or search for the needed configuration templates by clicking the **Configuration Templates** link.
 - All devices and templates associated with the selected project will be shown.

Searching among all project listings simultaneously

To search among all project listings simultaneously, do the following steps:

1. Click the project search selector's search field.
2. Click the **All projects** option.
 - The Partners Portal will return the needed search results.
3. Search for the needed hardware device listing by clicking the **Configure Devices** link or **Share Devices** link, or search for the needed configuration templates by clicking the **Configuration Templates** link.
 - All devices and templates that are part of your Partners Portal account will be shown.

Searching for entities that are not associated with a project

To search for devices and templates that are not currently assigned to a project, do the following steps:

1. Click the project search selector's search field.
2. Click the **No projects** option.
 - The Partners Portal will return the needed search results.
3. Search for the needed hardware device listing by clicking the **Configure Devices** link or **Share Devices** link, or search for the

needed configuration templates by clicking the **Configuration Templates** link.

- All devices and templates that are not currently linked to any project will be shown.

Searching by project name

To search by specifying part or all of the project name, do the following steps:

1. Click the project search selector's search field.
2. Type part or all of the relevant project name in the field.
 - If the entered text matches a project name that is linked to your user name, the project listing will be shown under the entry field.
3. Click the project listing that is shown under the entry field.
 - The Partners Portal will return the needed search results.
4. Search for the needed hardware device listing by clicking the **Configure Devices** link or **Share Devices** link, or search for the needed configuration templates by clicking the **Configuration Templates** link.
 - All devices and templates that are linked to the selected project will be shown.

7. Troubleshooting

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

7.1. I cannot get the Log-in screen

If you have directly connected a Windows computer to your Fluidmesh 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 Fluidmesh 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 Fluidmesh device through a proxy server. To stop the computer from trying to access the unit through a proxy connection, refer to [Accessing the Cisco FM RACER for device configuration](#).

7.2. I forgot the Administrator password

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

1. Physically access the unit.
2. Use the hardware **Reset** button to reset the unit to its factory default settings. Refer to [Resetting the unit to factory defaults](#) for more information.

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

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

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

Check the following points to improve the wireless link strength:

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

7.4. I purchased a Fluidmesh device, but it is not shown in FM Racer

The Fluidmesh device you have purchased may not yet be added to your Fluidmesh Partners account. Try manually adding the device using the unit serial number and mesh identity (ID) number as shown in [“Adding Fluidmesh devices to your FM Racer portfolio”](#) (page 18).

7.5. I cannot connect my Fluidmesh device to the FM Racer interface

If your Fluidmesh 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.fluidmesh.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.

7.6. 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 can connect to the internet from the local subnet?

7.7. 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 *Fluidmesh Installation and Configuration manual* for the specific device.

To connect compatible Fluidmesh 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 Fluidmesh 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 Fluidmesh Partners Portal.

8. Notices and copyright



WARNING

Installation of Fluidmesh 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.

Fluidmesh hardware installations must comply with all applicable local legislation.



WARNING

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

On some Fluidmesh 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 © 2020 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.

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

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.

9. Fluidmesh end-user license agreement

9.1. Preamble

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

The Fluidmesh 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.

9.2. Notice

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

You must read and agree to the terms of this firmware license agreement (hereafter known as the 'agreement') before any Fluidmesh firmware can be downloaded, installed or used. By clicking the 'Accept' button on any Fluidmesh firmware download webpage, or by downloading, installing or using Fluidmesh firmware and/or by using any Fluidmesh device running Fluidmesh 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 Fluidmesh firmware, and you agree to forego any implied or stated rights to download, install or use Fluidmesh firmware.

9.3. 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;

'Fluidmesh Device' means a Fluidmesh networking device that you purchase or otherwise rightfully acquire;

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

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

9.4. License grant

Fluidmesh grants you a non-exclusive, non-transferable license to use a copy of the Fluidmesh Firmware and accompanying documentation and any updates or upgrades thereto provided by Fluidmesh according to the terms set forth below. You are authorized by this license to use the Fluidmesh Firmware in object code form only, and solely in conjunction with applicable and permitted Fluidmesh-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 sublicense) to use the software solely for the Fluidmesh Devices that you own and control, and solely for use in conjunction with the Fluidmesh Firmware.

9.5. Uses and restrictions on use

You may:

(a) download and use Fluidmesh Firmware for use in Fluidmesh Devices, and make copies of the Fluidmesh 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 Fluidmesh Firmware on any devices or products that are not owned by you or your business organization;

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

(c) copy the Fluidmesh 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 Fluidmesh Firmware, including without limitation any such mechanism used to restrict or control the functionality of the Fluidmesh Firmware, or (ii) to derive the source code or the underlying ideas, algorithms, structure or organization from the Fluidmesh 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 Fluidmesh Firmware or modifications thereof or accompanying documentation in any form to any person without the prior written consent of Fluidmesh.

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

Fluidmesh Devices must be properly installed and they are sold for installation by a professional installer only. Fluidmesh Devices must be installed by a professional installer of wireless networking products certified by Fluidmesh, 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 Fluidmesh Firmware contains technological protection or other security features designed to prevent unauthorized use of the Fluidmesh Firmware, including features to protect against use of the Fluidmesh 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 Fluidmesh Firmware, and any copy made by you, remain with Fluidmesh and its suppliers. Unauthorized copying of the Fluidmesh 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 Fluidmesh.

9.6. Open-source software

You hereby acknowledge that the Fluidmesh Firmware may contain Open Source Software. You agree to review any documentation that accompanies the Fluidmesh Firmware or is identified in the documentation for the Fluidmesh Firmware, in order to determine which portions of the Fluidmesh Firmware are Open Source Software and are licensed under an Open Source Software license. To the extent that any such license requires that Fluidmesh 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.fluidmesh.com.

9.7. Termination

This license will continue until terminated. Unauthorized copying of the Fluidmesh 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 Fluidmesh. 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, Fluidmesh may immediately terminate this Agreement if (i) you fail to cure a breach of this Agreement (other than a breach pursuant to Fluidmesh intellectual property rights) within thirty (30) calendar days after its receipt of written notice regarding such breach, or (ii) you breach any Fluidmesh intellectual property right. Upon termination of this license for any reason, you agree to destroy all copies of the Fluidmesh Firmware. Any use of the Fluidmesh Firmware after termination is unlawful.

9.8. Feedback

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

9.9. Consent to use of data

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

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

Fluidmesh shall have the right to collect and analyze data and other information relating to the provision, use and performance of various aspects of the Fluidmesh Firmware and Fluidmesh Devices and related systems and technologies ('Data'), and you give Fluidmesh the right to use and disclose such Data (during and after the term of this Agreement) in accordance with Fluidmesh's Privacy Policy. If you choose to allow diagnostic and usage collection, you agree that Fluidmesh 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 Fluidmesh's products and services, facilitate the provision of software updates, product support and other services to you (if any) related to Fluidmesh products, and to verify compliance with the terms of this license. Fluidmesh 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 Fluidmesh's partners and third-party developers to improve their software, hardware and services designed for use with Fluidmesh products, Fluidmesh 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.

9.10. Warranty disclaimer

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

Fluidmesh does not warrant that the operation of the Fluidmesh Firmware will be uninterrupted or error-free or that the Fluidmesh Firmware will meet your specific requirements. You acknowledge that Fluidmesh has no support or maintenance obligations for the Fluidmesh Firmware.

9.11. Limitation of liability

Except to the extent that liability may not by law be limited or excluded, in no event will Fluidmesh 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 Fluidmesh Firmware, howsoever caused and on any theory of liability (including without limitation negligence).

This limitation will apply even if Fluidmesh 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 Fluidmesh'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.

9.12. Exclusion of liability for emergency services

Fluidmesh 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.

Fluidmesh 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.

Fluidmesh 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 Fluidmesh 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 Fluidmesh and the end user and form a basis of the bargain between the parties.

9.13. Export control

You acknowledge that the Fluidmesh Devices, Fluidmesh 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 Fluidmesh Devices and Fluidmesh Firmware, to, or make the Fluidmesh Devices and Fluidmesh 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 Fluidmesh Devices and Fluidmesh 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 Fluidmesh Devices and Fluidmesh 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 Fluidmesh Devices and

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

9.14. 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 Fluidmesh, and supersedes any other communications or advertising with respect to the Fluidmesh 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 Fluidmesh Firmware on behalf of any part of the U.S. Government, the following provisions apply: The Fluidmesh 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 Fluidmesh 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).

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

10. Contact us

Worldwide Headquarters:

Fluidmesh Networks LLC

81 Prospect Street

Brooklyn, New York 11201

United States of America

Tel. +1 (617) 209 -6080

Fax. +1 (866) 458-1522

info@fluidmesh.com

Technical Support desk: support@fluidmesh.com

www.fluidmesh.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