FreeMile

User manual

Freemile 60 GHz

VER 1.2

FW 1.12.0

Proprietary notice

The information presented in this guide is the property of SAF Tehnika, JSC. No part of this document may be reproduced or transmitted without proper permission from SAF Tehnika, JSC.

The specifications or information contained in this document are subject to change without notice due to continuing introduction of design improvements. If there is any conflict between this document and compliance statements, the latter will supersede this document.

SAF Tehnika, JSC has no liability for typing errors in this document or damages of any kind that result from the use of this document.

To get up to date information about accessories and their availability, please contact a sales representative.

FODU does not contain serviceable parts. Warranty will not be applicable in the event FODU has been hermetically unsealed.

SAF Tehnika, JSC is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. The operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from the one connected to the receiver.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Innovation, Science and Economic Development Canada license-exempt RSS standard(s). The operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil est conforme aux normes RSS exemptes de licence d'Innovation, Sciences et Développement économique Canada. Le fonctionnement est soumis aux deux conditions suivantes :(1) cet appareil ne doit pas causer d'interférences, et (2) cet appareil doit accepter toute interférence, y compris les interférences pouvant entraîner un fonctionnement indésirable de l'appareil.

Copyright Notice

Copyright © 2024 SAF Tehnika, JSC. All rights reserved.

Contents

Chapter 1: OVERVIEW 4
Labeling 5
Safety Measures 5
Microwave Radiation 5
Freemile 60 FODU interfaces and LED indications 6
Chapter 2: INSTALLATION 8
Package contents 8
Freemile 60 radio installation on a wall 8
Freemile 60 radio installation on a pole 9
Freemile 60 attaching to 100mm antenna kit 10
Powering Freemile 60 FODU 11
Bench-testing of Freemile 60 FODUs 11
Basic configuration of Freemile 60 link 12
Configuration of network settings 12
Configuration of Access Point or Point-to-point master unit 12
Configuration of Station or Point-to-point slave unit 12
Chapter 3: WEB GUI 14
Initial configuration 14
System requirements 14
Ethernet management connection configuration 14
Accessing Web GUI 14
Web GUI description 15
Dashboard 17
Activity 20
Configuration 20
Configuration→Network 21
Configuration→Wireless 24
Configuration→Services 25
Configuration→System 28
Users 29
Tools 29
Tools→Site survey & Aiming 29
Tools→Ping 30
Tools→Traceroute 30
Tools→View log 30
Tools→Device discovery 31
Tools→View bridge table 31
Tools→Sector info 32
Backups and recovery 32
Chapter 5: FUNCTIONAL DESCRIPTION and TOOLS 34
Failover mode 34
Sector info tool 34
MIB files 35
ABBREVIATIONS 36

Chapter 1: OVERVIEW

This document briefly describes the Freemile 60 series IP FODU (Full Outdoor) system covering the built-in management system, configuration functionality, hardware features, etc.

The Freemile 60 is a robust and versatile 60 GHz frequency band TDD (Time Division Duplex) type Full Outdoor unit designed for High Capacity point-to-point and point-to-multipoint microwave networks. In point-to-multipoint mode, Freemile 60 product family can deliver multi-Gigabit speeds to up to 32 customers per sector at a fraction of the cost of deploying fiber.

The Freemile 60 units feature a proprietary TDMA scheduling protocol which is perfect for video surveillance networks requiring high-capacity upload bandwidth.

Key features of Freemile 60 products:

- 2+ Gbps speed can be achieved in distances of up to 4+ km (antenna kit dependent) without trenching, permits, or licenses
- Support of the full 60GHz band, including channels 5 and 6 (57-71 GHz), enabling longer links and increased co-location opportunities
- The Freemile 60 radio features a modular design. The base unit features 90º of beam-forming coverage and can be paired with an antenna kit (sold separately as an accessory) to convert the radio from a wide beam-steering device to a highly directional one
- The low cost of the Freemile 60 product, combined with high subscriber density and quick installation, greatly decreases total cost of ownership for service providers
- The Freemile 60 has 1 x 2.5 Gbps port (active PoE in) and 1 x 1 Gbps port with PoE out
- The 1 Gbps Ethernet port can be used as an "any"-band failover option, or to power accessories such as surveillance cameras

FODUs mechanical features

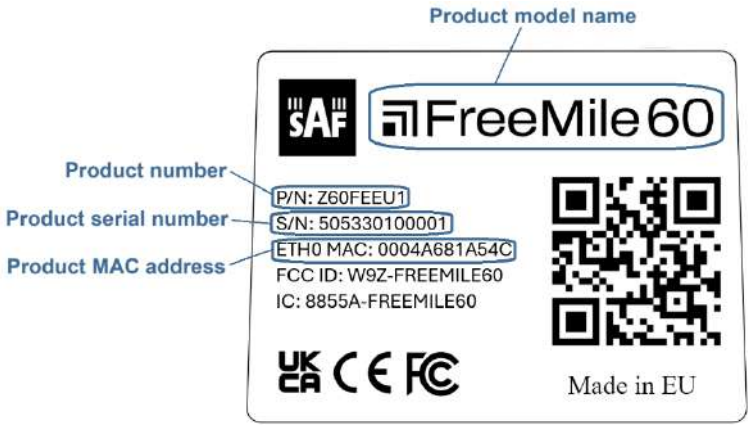
- Compact unit, Height: 130mm/5", Width: 120mm/5", Depth: 55mm/2”; Weight 425g/15 oz
- 1 x 2.5 Gbps Ethernet (PoE input), 1 x 1 Gbps Ethernet (PoE output) interfaces for Ethernet traffic and PoE power supply
- Pole or wall mountable via mounting backplate
- All the connectors downwards
- Power consumption: 17W without PoE output in use; 41W with PoE output in use

Figure 1.1 *Freemile 60 FODU*

Labeling

The label contains the following information (see sample in the picture below):

Product model name (“Freemile 60”): 60 GHz unlicensed band FODU
Product number (Z60FEEU1): product identification number of the unit
Serial Number (505330100001): the serial number uniquely identifies the unit
MAC address (ETH0 MAC: 0004A681A54C): indicates the MAC address of the unit

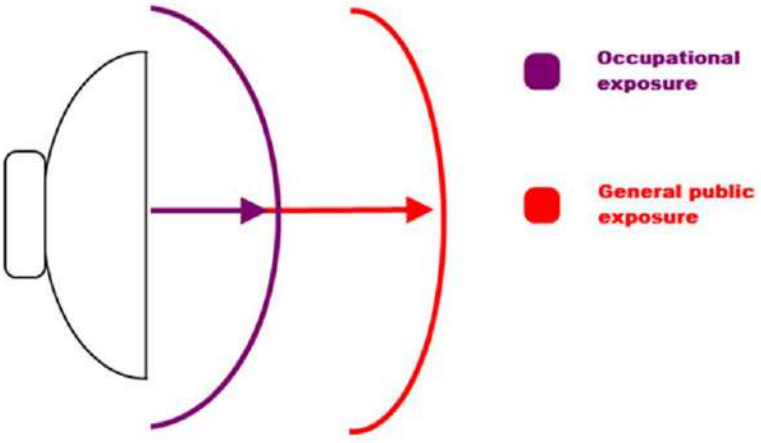


Safety Measures

Following safety measures must be considered when working/using the Freemile 60 equipment:

- This product is not suitable for use in locations where children are likely to be present
- A suitable and easily accessible disconnecting device or switch must be used to interconnect Power Supply Circuits
- Keep the radio unit at least 2.5 cm (1 inch) away from the face. Keeping the radio at the proper distance is important as RF exposure decreases with distance from the antenna. The antenna should be kept away from the face and eyes
- Use of non-approved antennas, batteries, and accessories causes the radio to exceed the FCC/ISEDC RF exposure guidelines
- Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment

Microwave Radiation



Freemile 60 radios conform to both occupational and general public exposure limit guidelines and restrictions to time-varying electric, magnetic and electromagnetic fields which are specified or referred in the documents below:

- 1999/519/EC: Council Recommendation of July 12, 1999, on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz);
- WHO: Environmental Health Criteria 137: ´Electromagnetic Fields (300 Hz to 300 GHz);
- ANSI/IEEE C95.1, 1999: ´IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz;
- BRD, Bundesimmissionsschutzgesetz, 26. BImSchV Verordnung über elektromagnetische Felder;
- Bundesamt für Umwelt, Wald und Landwirtschaft (BUWAL), Bern/Schweiz Schriftenreihe Umwelt Nr. 164, Luft, Mai 1992 ´Messung nichtionisierender elektromagnetischer Strahlung, 1. Teil: Frequenzbereich 100 kHz bis 300 GHz;
- DIN VDE 0848-2, Entwurf, Oktober 1991: ´Sicherheit in elektrischen, magnetischen und elektromagnetischen Feldern, ´Teil 2: Schutz von Personen im Frequenzbereich von 30 kHz bis 300 GHz;
- ENV 50166-2, January 1995 (withdrew in December 1999 by CENELEC) ´Human Exposure to Electromagnetic Fields (10 kHz – 300 GHz)

Freemile 60 FODU interfaces and LED indications

Freemile 60 radio unit has following interfaces:

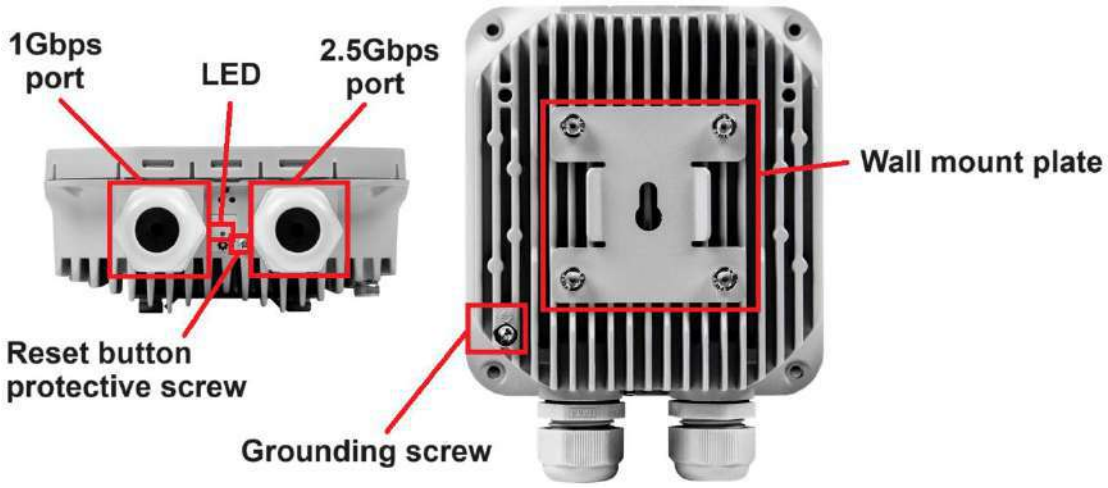


Figure 1.2 *Freemile 60 FODU interfaces*

1 Gbps port

1 Gbps Ethernet traffic port (RJ-45) supporting PoE output. It has implemented LED indication. The LED light will turn on and blink when a link is established, and the PoE out light will turn on when PoE output is enabled in software

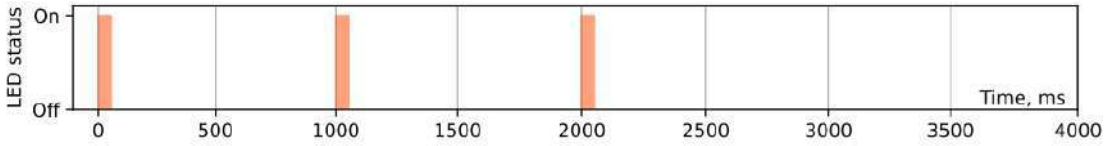
2.5 Gbps port

2.5 Gbps Ethernet traffic port (RJ-45) supporting PoE input. It has implemented LED indication. The LED light will turn on when a link is established, and the power light will turn on once the device is supplied with power

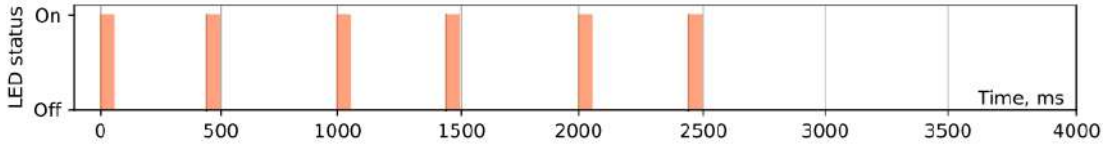
LED

Indicates the status and alarms of the device. Status/alarm LED indications are the following:

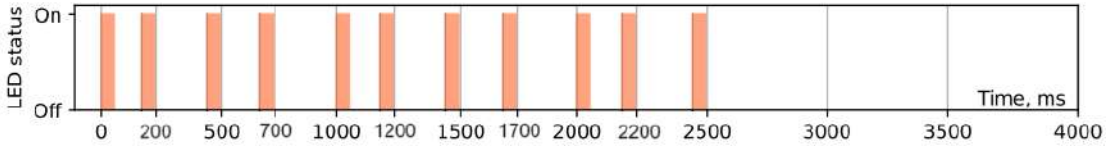
- **OFF** – the device is currently operating in Access Point mode, the device is powered off, or the radio modem is not detected
- **Blinking slowly** – the device is in Station or PTP mode and is currently scanning, blinking intervals is 1000 ms:



- **Blinking with medium speed** – the device is in Station or PTP mode and is connected with a low received signal in the range of -68..-71 dBm, blinking intervals is 400 ms:



- **Blinking with fast blink speed** – Case 1: If the unit is just booting up, the device is flashing the internal modem firmware. Case 2: If the unit is fully booted, then the device is in Station or PTP mode and connected to an Access Point with a medium received signal strength in the range of -65..-67 dBm, blinking intervals is 100-200 ms:



- **Solid ON** – The device is in Station or PTP mode and connected to an Access Point with excellent received signal strength in the range of -13..-64 dBm

Reset button protective screw

By removing the screw, the reset button will become available for resetting the device to factory defaults. To reset the device, use a paperclip, or something similar to press the reset button. Press and hold the reset button for 20 seconds or more. Note that it will not have any effect if the reset button is disabled in the software.

Grounding screw

Grounding screw for equipment grounding. The equipment grounding can be done by connecting it to the grounding point of the tower. The recommended minimum grounding cable wire cross-section must be 2.5 mm2.

Wall mount plate

The plate for mounting the device on a wall – refer to *Freemile 60 radio installation on a wall* section. It can be used also for mounting the device on the pole – refer to *Freemile 60 radio installation on a pole* section. The wall mount plate must be removed to substitute with the pole mount bracket for using with 100mm antenna kit – refer to *Freemile 60 attaching to 100mm antenna kit* section

Chapter 2: INSTALLATION

Package contents

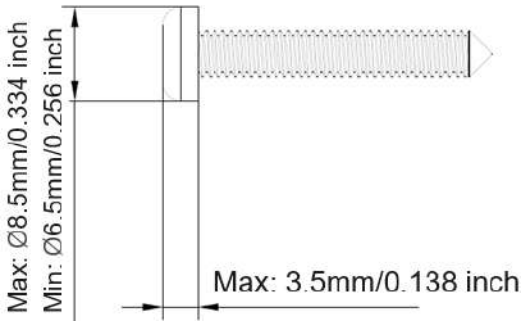
Item	Quantity
Freemile 60 base model	1
48V, 0.5A PoE injector and power cable	1

Antenna kits (and corresponding mounts), if ordered, are shipped separately.

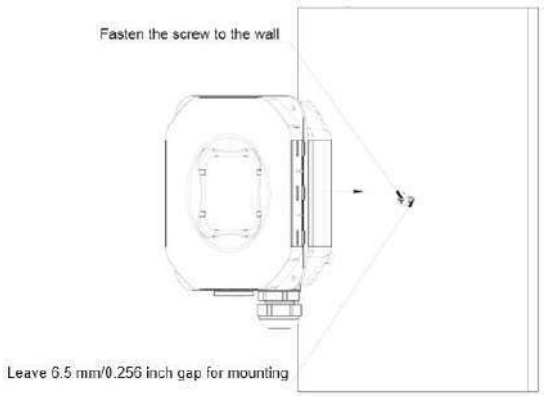
Freemile 60 radio installation on a wall

The Freemile 60 radio can be installed on the wall using single screw (not included in the package). The wall mounting instructions are as follows:

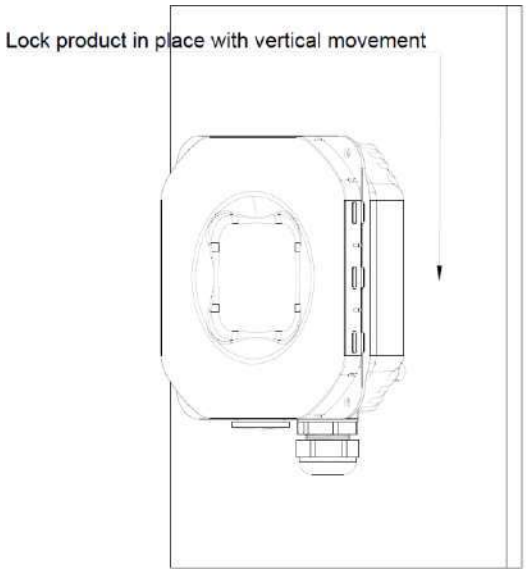
Tools required: screwdriver (depending on a used screw)



1 The dimensions of the screw which can be used to install the Freemile 60 radio on a wall



2 Fasten the screw into the wall leaving about 6.5mm/0.256 inch gap for radio mounting

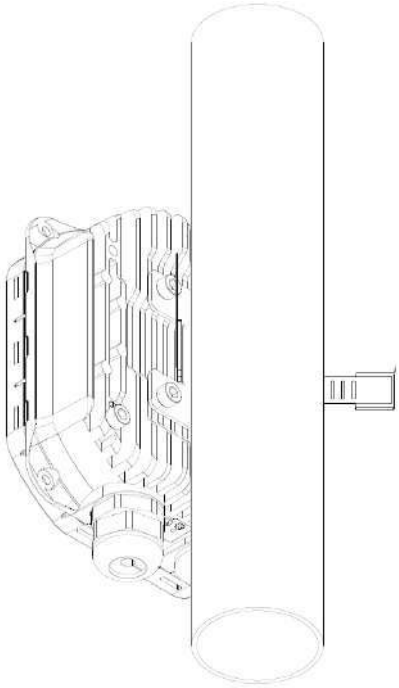


3 With vertical movement mount the radio onto the screw. Adjust the screw gap if the radio is too loose. The ports/interfaces must be faced downwards

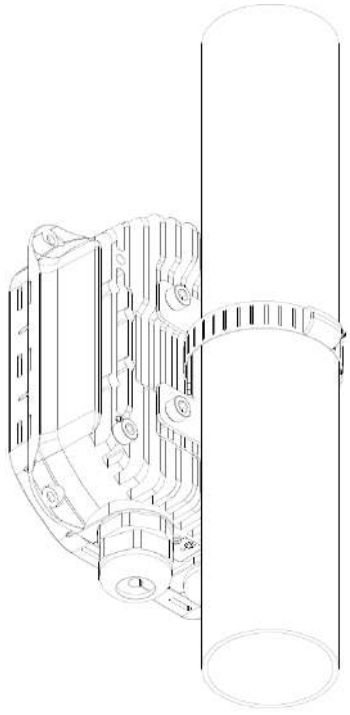
Freemile 60 radio installation on a pole

The Freemile 60 radio can be installed on a pole using steel cable tie (not included in the package). The pole mounting instructions are as follows:

Tools required: Steel cable tie: width: up to 20 mm/0.79 inch; length: depending on the pole diameter



1 Place a steel cable tie into the radio mount and around the pole



2 Tighten the tie around the pole

It is recommended to protect the installed radio from direct sunlight.

Freemile 60 attaching to 100mm antenna kit

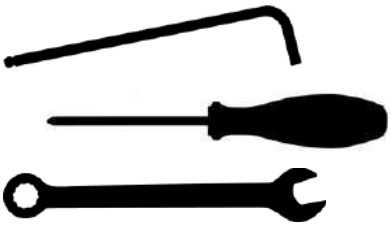
100mm antenna kit contains following parts:

Item	Quantity
Radom	1
Screws for radome connection	4
Mounting bracket	1

Tools required: Size 4 Allen wrench (not supplied)

Size 2 Philips screwdriver (not supplied)

10mm (0.394”) wrench (not supplied)



1. Attach the radom to the radio with 4 screws included in the antenna kit package. Use size 2 Philips screwdriver
2. Remove the existing mounting bracket from the radio with size 4 Allen wrench
3. Using the same screws attach the mounting bracket from the antenna kit package to the radio
4. Use 10 mm (0.394”) wrench to attach and tighten the radio mounting bracket to the pole. The recommended pole diameter size is 40mm..50mm (1.575 inch..1.969 inch)

Powering Freemile 60 FODU

Use the supplied Power over Ethernet (PoE) injector with an appropriate power supply (38…57V DC, at least 30W for a single Freemile 60 unit). The input power to the Freemile 60 should be 48V DC, and a minimum of 0.5A (24W) is recommended. The Freemile 60 FODU does support active PoE (802.3at, etc.).

PoE injector is included in Freemile 60 radio package. The PoE injector has a built-in AC/DC converter supporting 100-240V AC input and 48V DC output. It has a LED indicating about connected AC input (solid green).

The Ethernet cable from the PoE injector "POE" port must be connected to the 2.5 Gbps RJ-45 port on Freemile 60 radio unit (refer to *Freemile 60 FODU interfaces and LED indications* section). The total length of Ethernet cables from CPE to PoE injector (LAN port) and from Freemile 60 to PoE injector (POE port) combined should not exceed 100m. It is recommended to use outdoor-rated STP/FTP Ethernet cable Cat6 or better.

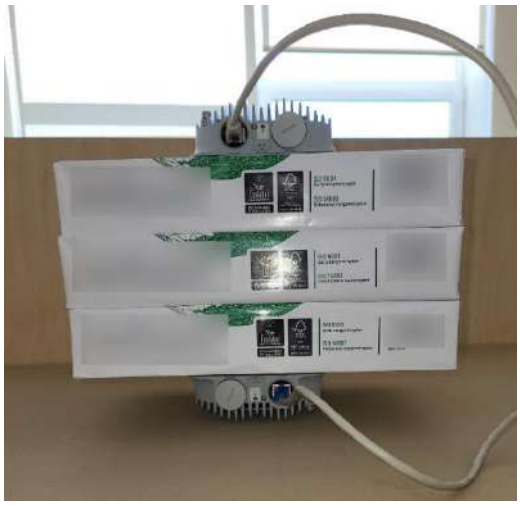
The Freemile 60 unit has the ability to send passive PoE out of the 1 Gbps port to power another device using the input power provided to the Freemile 60 unit. The setting of this option is described in the Web GUI *Configuration →Network* section. The output voltage is the same as the input voltage and supports maximum 0.5A current (24W total).

When using the PoE-out feature on the Freemile 60 unit, make sure that the used power supply unit is rated at > 60W to power both Freemile 60 units. The supplied PoE injector provides only 24W excluding losses that may not be adequate to power both devices and may result in unstable operation.

Passive PoE out on the 1Gbps port can damage non-PoE devices. Do not connect non-PoE devices to the 1Gbps port when PoE out is enabled.

Bench-testing of Freemile 60 FODUs

For Freemile 60 radio link connection on the table 2-3 office paper packs can be used as attenuators between both radios as indicated in the following example:



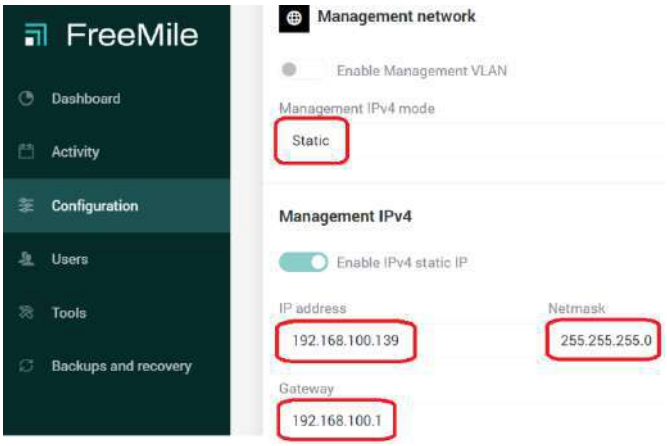
It can take up to 20-30 minutes for the link to stabilize to max MCS12 (or MCS9) capacity mode on both radios. In such testing conditions, the MCS value may differ on each side radio. Refer to *Configuration →Wireless* for MCS parameter description

Basic configuration of Freemile 60 link

This section describes Freemile 60 FODU's basic configuration to establish the link – either for production link before its installation on sites, or for bench-testing. For details of accessing the radios refer to *Initial configuration* section. For configuration details refer to *Web GUI description* section. The steps of the basic configuration of Freemile 60 FODUs are described below.

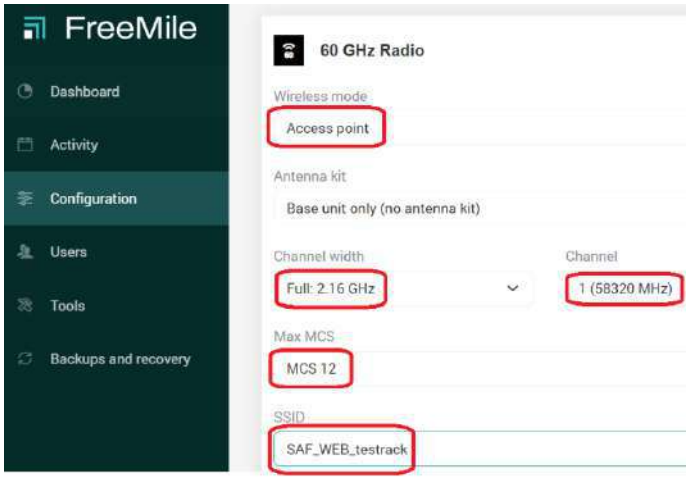
Configuration of network settings

For both Access Point (Point-to-point master) and Station (Point-to-point slave) units set the Management IPv4 mode to 'Static', and specify IP address/netmask/gateway, or to 'DHCP' and obtain parameters automatically from the DHCP server. This can be set in web GUI section *Configuration →Network*:



Configuration of Access Point or Point-to-point master unit

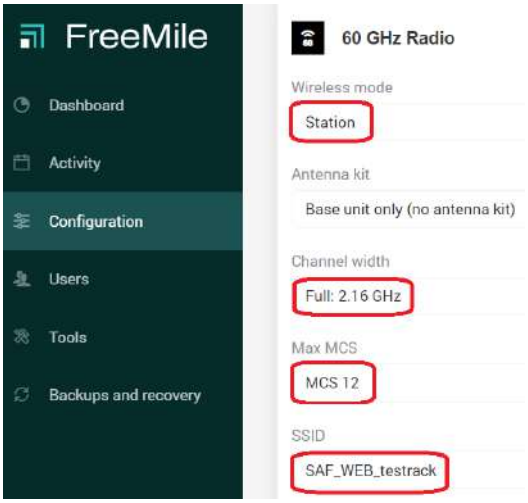
For Access point (point-to-multipoint) or Point-to-point master unit set Wireless mode to 'Access point' or 'Point-to-point master', specify the Channel width, frequency channel, and Max MCS (Modulation Coding Scheme) settings, and make sure the SSID is the same for Access point unit and the Station unit. This all can be set in web GUI section *Configuration →Wireless*:



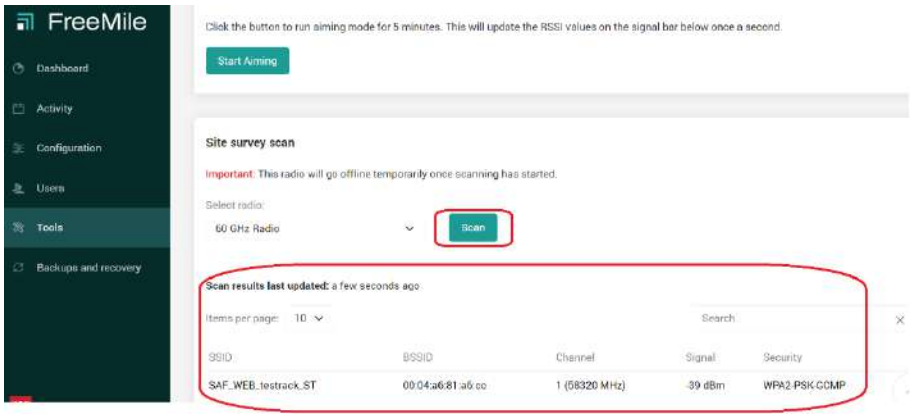
Configuration of Station or Point-to-point slave unit

For Station (point-to-multipoint) or Point-to-point slave unit set Wireless mode to 'Station' or 'Point-to-point slave', specify the Channel width and Max MCS (Modulation Coding Scheme)

settings – the same as on Access point unit, and make sure the SSID is the same for Station unit and the Access point unit. This all can be set in web GUI section *Configuration →Wireless*:



For point-to-multipoint mode, in case there are several Freemile 60 Access point units available in range, and the Station device must be connected to one of them/specific one, use scanning functionality which can be found in web GUI *Tools →Site survey & aiming* section to find all the Freemile 60 Access points and to choose the required one:



Chapter 3: WEB GUI

Initial configuration

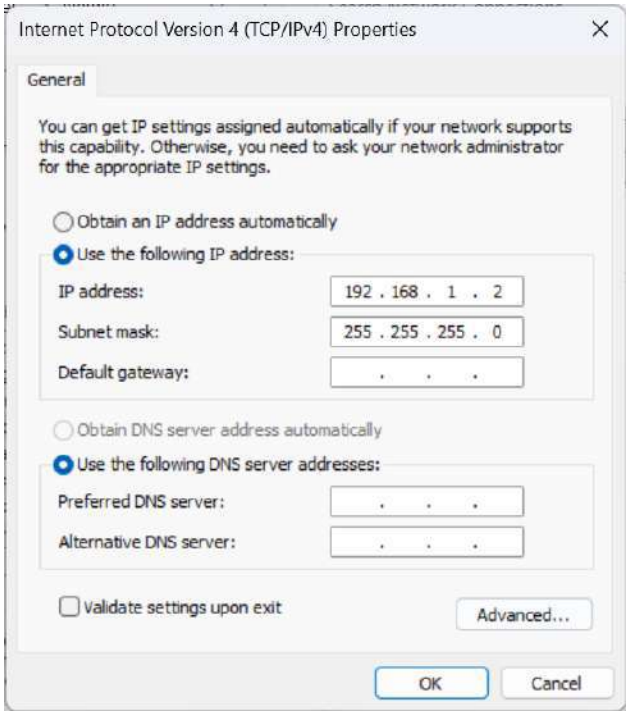
System requirements

To access the Freemile 60 Web GUI a PC with the following Web browser must be used:

- Mozilla Firefox;
- Google Chrome;
- Microsoft Edge.

Ethernet management connection configuration

Before proceeding with the initial link setup in the Web GUI, adjust the IPv4 settings of your LAN adapter to 192.168.1.0 subnet. The IP address should be something other than the default IP addresses (192.168.1.1).



After applying these settings, you are ready to connect to the Web GUI.

DHCP client is enabled on the main management network bridge of the device as well.

Accessing Web GUI

1. Connect your laptop to any of Ethernet ports of the Freemile 60 device
2. Launch your browser and in the address field enter the IP address of a FODU. Default IP address is: 192.168.1.1

The device can be accessible also on the additional "alternative local IP" of 169.254.1.1

3. Press “Enter” key.
4. The login screen will appear.
5. Enter username and password. Default credentials are as follows:
    - Username: **root**
    - Password: **admin**

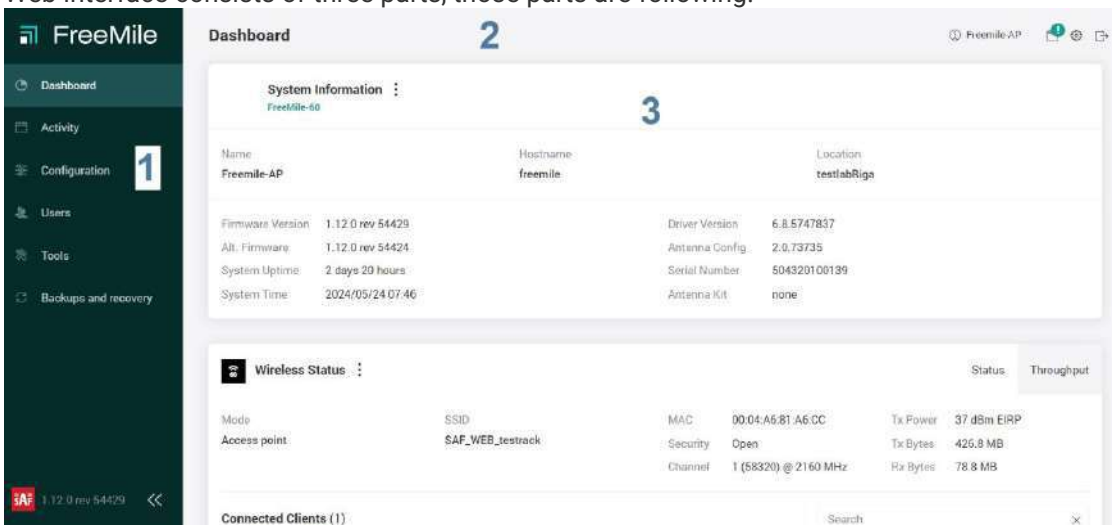
Change the default user credentials after logging in for the first time

6. Press “Log in” button.

User will automatically be logged out of the session in case of inactivity for more than 30 minutes

Web GUI description

Web interface consists of three parts, those parts are following:



1 Main menu tree

Allows navigating between pages and sections of web GUI. It contains following sections:

- **Dashboard** – shows the overall status of your device
- **Activity** – event log indicating recent events happened on the device, like client association/disassociation events, user logins, DHCP events, etc
- **Configuration** – allows configuration of the device
- **Users** – allows configuration of user access for the web GUI and API

- **Tools** – set of various tools for advanced debugging tasks such as Ping, Site survey and aiming, Traceroute, Device discovery and others
- **Backups and recovery** – allows download and upload of configuration files to/from the user's PC

Clicking on the arrow on the bottom of this section

allows hiding or expanding the side panel.

2 Header of the page

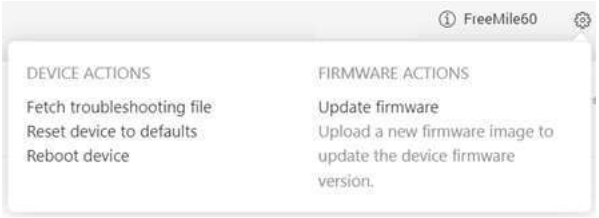
Indicates currently opened section name and system/device information and settings:

-

Freemile 60 radio information, can be viewed by pointing the cursor on it
-

indicates about new event information. When clicking on it, the list of latest events will be opened
-

by clicking on it the device actions/settings will be opened:



The following device actions can be done here:

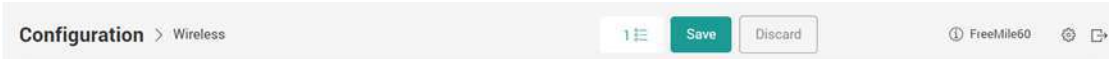
- **Fetch troubleshooting file** – allows downloading troubleshooting file from the device
- **Reset device to defaults** – allows resetting the device to factory default settings
- **Reboot device** – allows rebooting of the device
- **Update firmware** – allows upgrading or downgrading the firmware of the device. The following dialog will be shown when clicking on this option allowing you to choose the firmware file and perform upgrade:

The option "Reset config after device update" must be enabled only in case the firmware has been downgraded.

-

allows logging out from the device's Web GUI

When the 'Configuration' or 'Users' page is opened and settings are changed, the following buttons will appear in the Header:



-

"List" button indicates parameters that were changed and are pending for saving in the configuration file

- Save "Save" button must be used to apply and save the changes in the configuration file
- Discard "Discard" button can be used to discard all made changes

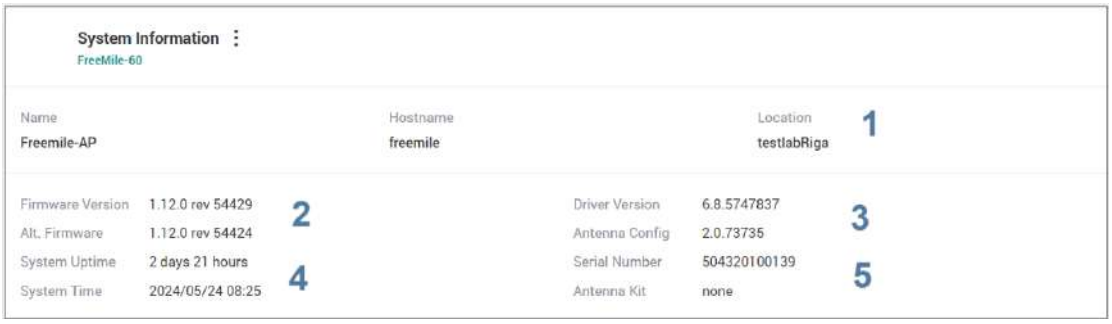
3 Main web GUI window

By default, the Dashboard page ("Dashboard") is shown after logging in. Contents will change according to the menu panel selection

Dashboard

Dashboard page consists of several informational sections:

- **System information** of the device:



1) Device name, location, and hostname: device name is used to populate LLDP discovery fields, and the hostname will be used when sending DHCP requests
2) The firmware versions running on each device boot-bank (active and alternate/backup)
3) Driver and antenna config versions: these fields are mainly used for debug purposes
4) System Uptime since last reboot and current System Time: this is the device's current date and time. Time zone and other time settings are configurable in web GUI section *Configuration →System*
5) Serial number and antenna kit: the device's antenna kit can be configured in web GUI section *Configuration →Wireless* and is used to determine the estimated target RSSI of any connected peers

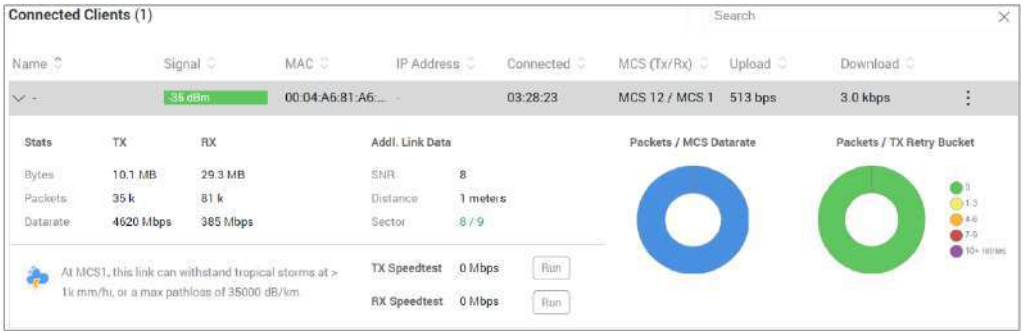
Clicking on the "three dots" button will lead to *Configuration →System* page:

- **Wireless status** of the device. This section differs for Access Point (Point-to-point master) devices and Station (Point-point-slave) devices. The Access Point (Point-to-point master) Wireless status page is following:

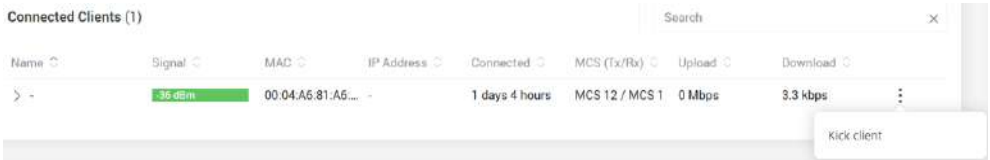
1) Contains Access point (Point-to-point master) wireless information.

2) Indicates the list of Stations found by the Access point unit using built-in Device discovery functionality in *Configuration →Services* page. Clicking on the arrow button

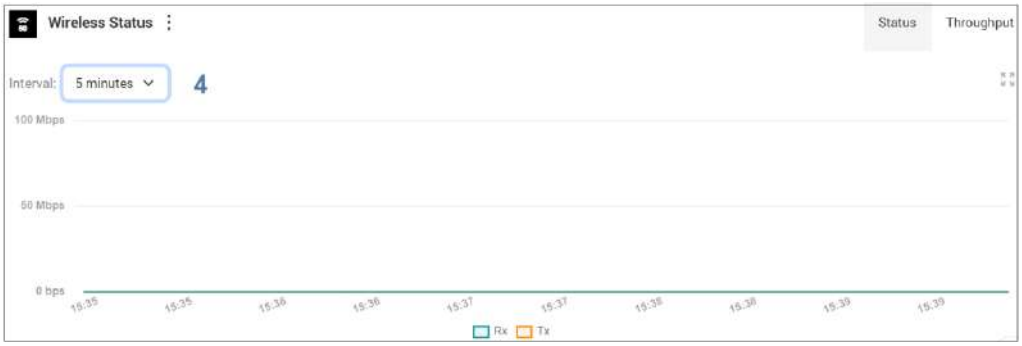
in the connected Stations list will open Station device information page:



Clicking on the “three dots” button on the right side of the Station devices list in Access point device menu will show “Kick client” option which allows disconnecting of particular Station from the Access point device:



3) Clicking on the ”Throughput” tab will open wireless throughput graph:

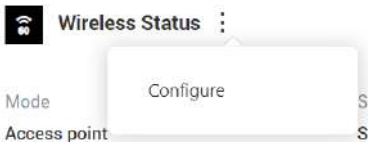


4) Allows choosing graph interval among 5 minutes, 2 hours, 1 day, 1 week and 1 year

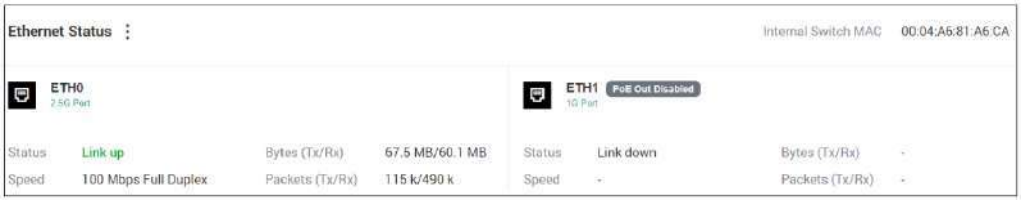
The Station (Point-to-point slave) Wireless status page is following:

5) Connection status information of the Station (Point-to-point slave) device
6) Implemented Speed-test functionality to test throughput between the Access Point and clients, or vice versa. To start the speed test the “Run” button must be pressed. The Speed-test is useful for troubleshooting purposes
7) Connected Access point details and connection information/status

Clicking on the “three dots” button will lead to *Configuration →Wireless* page:

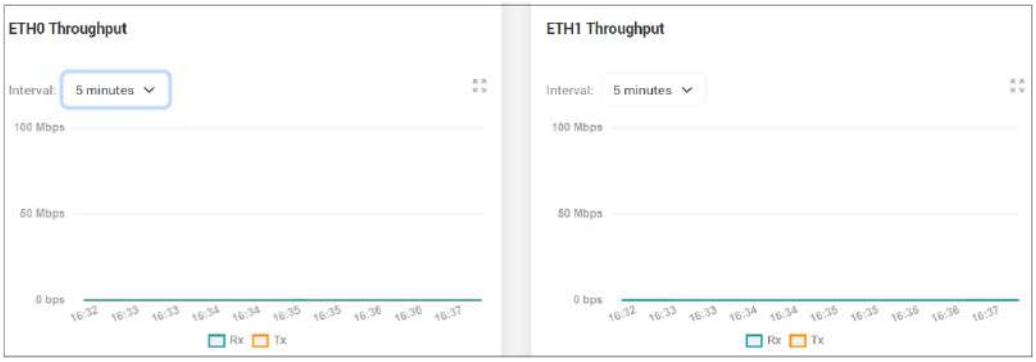


- **Ethernet status** of the device indicates both Ethernet ports statuses, PoE status and MAC address

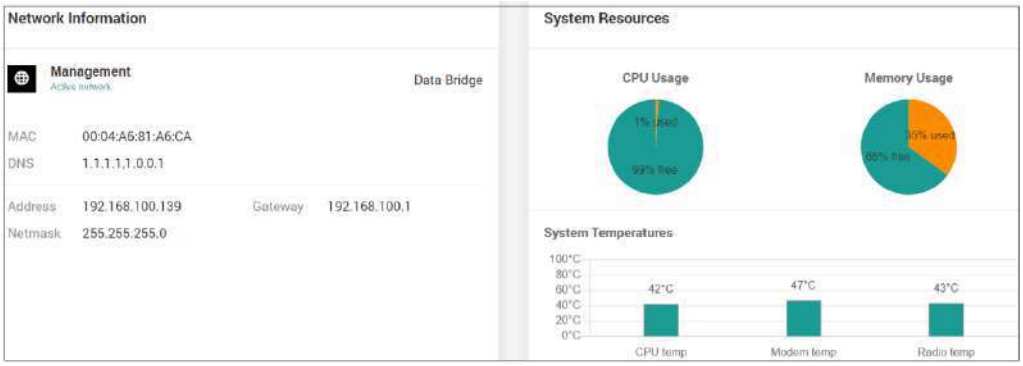


Clicking on the “three dots” button will lead to *Configuration →Network* page:

- **Ethernet throughput** of device’s Ethernet ports with option to choose intervals of 5 minutes, 2 hours, 1 day, 1 week and 1 year:

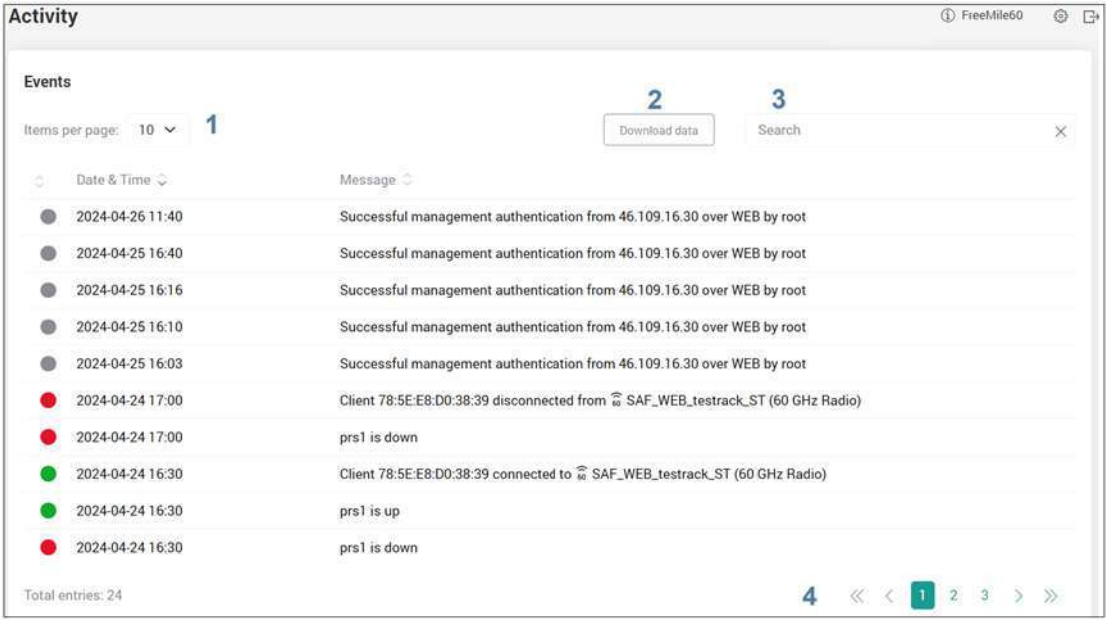


- **Network information** and **System resources** indicate management access information and system information like CPU and memory usage, and system temperature:



Activity

Indicates recent events, such as client association/disassociation, user login, DHCP events, etc.



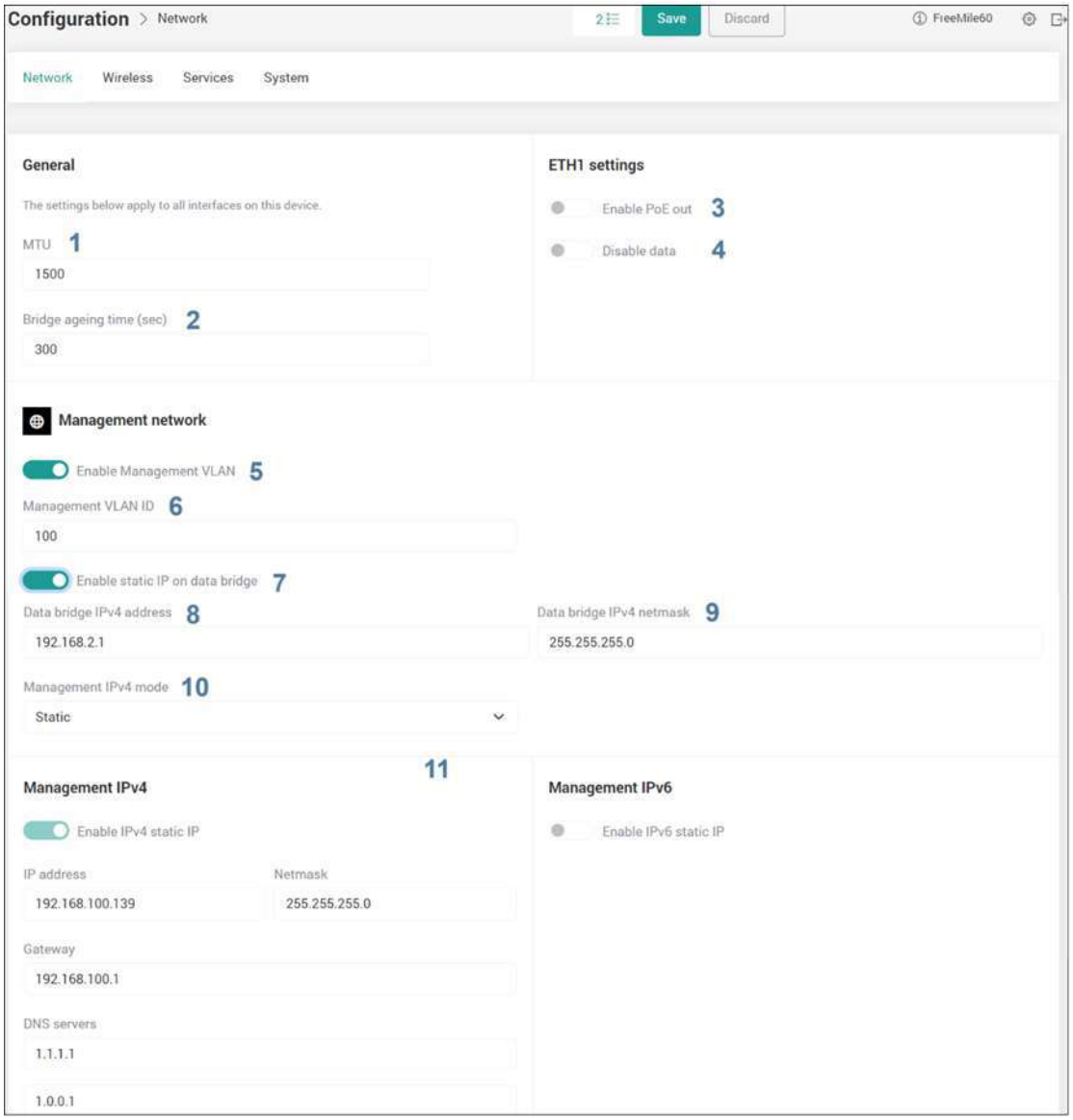
1) Allows choosing how many items per page will be displayed. It is possible to choose between 10, 25, 50, and “All” items
2) Allows downloading the event data to the PC
3) Allows searching any specific event from the list
4) Allows navigating through the event data lists

Configuration

Configuration section allows configuration of Network, Wireless, System parameters and supported Services. When any of the parameters will be changed in the Configuration section the “List”, “Save” and “Discard” buttons will appear in the header of the web page. All new settings will be applied by pressing “Save” button.

Configuration→Network

For the Access Point or Point-to-point master device the Configuration→Network section is following:



1) ***MTU*** – allows setting MTU (maximum transmission unit) for wireless interfaces, ethernet ports, and management/local bridge. The minimum allowed value is 1280 bytes, and the max is 7900 bytes
2) ***Bridge ageing time*** – allows setting aging time. The ageing determines the number of seconds a MAC address is kept in the forwarding database (FDB) after a packet has been received from that address. Setting to 0 will disable the ageing.
3) ***Enable PoE out*** – enables or disables PoE out on the ETH1 1G interface
4) ***Disable data*** – disables data over the ETH1 interface. This is useful if an external device will be powered via PoE out but there is no need for data to pass over the link
5) ***Enable Management VLAN*** – enables or disables management VLAN on the device.
6) ***Management VLAN ID*** – appears when Management VLAN option is enabled. Allows to specify the management VLAN ID

Once the management VLAN is enabled and VLAN ID is specified, reconnect to the unit using the same VLAN ID set on the external device (e.g. switch). In case of wrong VLAN

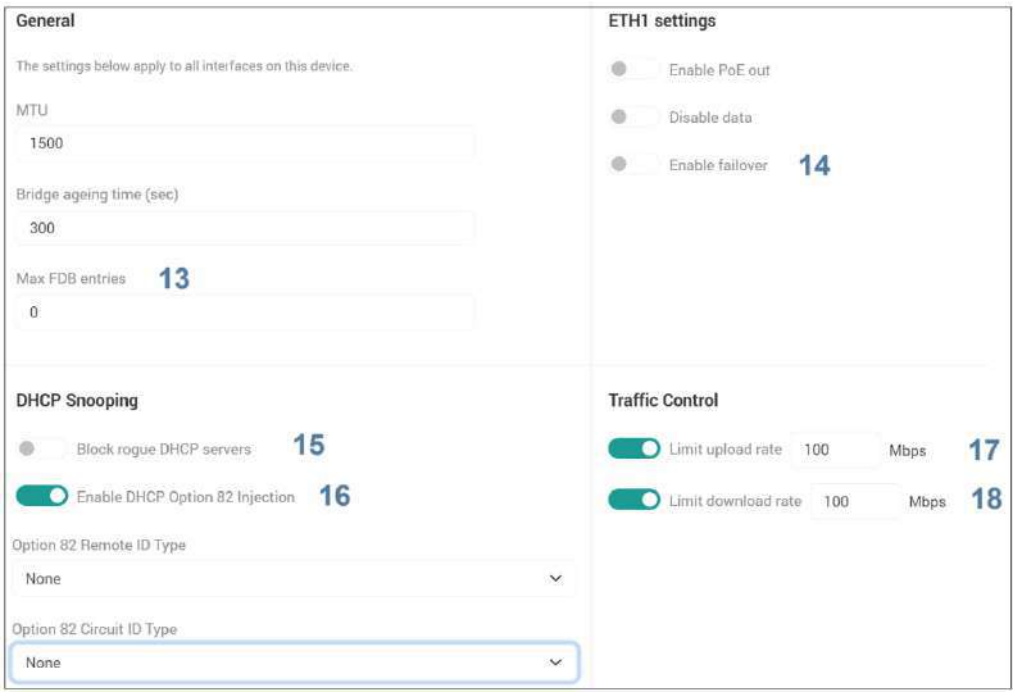
settings, the unit may not be reachable and may require resetting the device to factory settings unless the data bridge static IP is enabled and set (see below point 7)

7) ***Enable static IP on data bridge*** – enables data bridge to the management over the data network instead of the management VLAN network. This can be helpful in cases where access to the device is needed during installation over the non-management VLAN network. Once aiming and installation are complete, this setting can be turned off, only allowing access to the web GUI over the management VLAN network.
8) ***Data bridge IPv4 address*** – appears when the data bridge functionality is enabled. It allows setting IPv4 address for data bridge
9) ***Data bridge IPv4 netmask*** – appears when the data bridge functionality is enabled. It allows setting IPv4 netmask for data bridge
10) ***Management IPv4 mode*** – allows choosing between Static IP address or DHCP client mode
11) ***Management IPv4*** and ***Management IPv6*** – when Static management mode is chosen, allows setting IPv4 or IPv6 settings for management access

In the case of the "DHCP Client" mode, the following options will appear:

12) ***Management fallback IPv4, Management IPv4 netmask, DHCP broadcast*** and ***Custom DNS*** – when DHCP Client management mode is chosen, allows setting mentioned options for management access

For the Station or Point-to-point slave device in the Configuration→Network section following additional settings are available:



13) ***Max FDB entries*** – allows setting the maximum number of allowed FDB (forwarding database) entries. Value 0 is for unlimited number (default setting). Altering the value will effectively limit the number of MAC addresses that can pass traffic via the ETH1 port. This setting is useful for limiting the number of connected customer devices - for example, value 1 will ensure only one customer router connection is allowed.

This setting is not compatible with failover mode

14) ***Enable failover*** – allows enabling/disabling failover/backup over a device connected to the ETH1 port. For more detailed information about the failover mode refer to *Failover mode* description

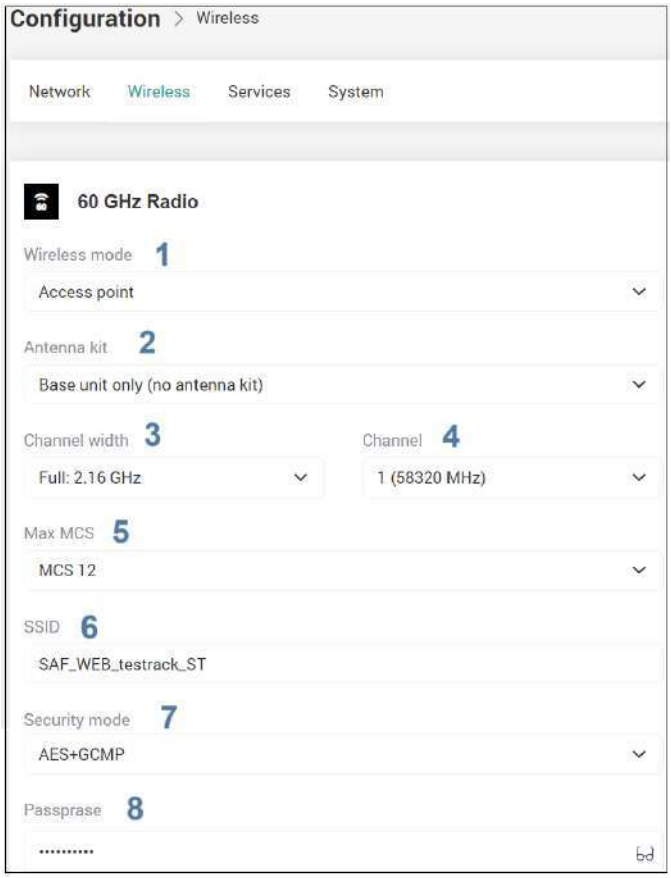
- When data is disabled over ETH1 port, the Failover function will be automatically disabled
- Failover mode is supported only when Data VLAN is disabled
- Failover mode must be enabled BEFORE interconnecting the ETH1 port of the FreeMile 60 unit set in "Station" mode with the failover device in order to prevent network loops

When enabling the failover mode the ***RSSI threshold*** and ***Flap protection time*** settings will be displayed:

15) ***Block rogue DHCP servers*** – when this setting is enabled, DHCP discovery packets will be dropped at the Station before being passed downstream; and DHCP offer packets will be dropped at the Station before being passed upstream. Rogue DHCP servers can occur when a user connects the router backwards, exposing the DHCP server to the upstream WAN network, instead of the local network.
16) ***Enable DHCP Option 82 injection*** – allows enabling injection of DHCP Option 82 fields into upstream DHCP request packets. Users can choose to populate the Remote ID field, the Circuit ID field, or both. These fields can be set to one of the following options:
    - ***Station's wireless MAC address*** – inserts the Station's wireless MAC address into the specified DHCP option 82 field. When the MAC address is inserted, it will be ASCII encoded and will include the colons, and a null terminator character at the end. The station MAC, 00:04:A6:81:A5:4E would show up on the DHCP server as 30:30:3A:30:34:3A:41:36:3A:38:31:3A:41:35:3A:34:45
    - ***Custom field*** – inserts an ASCII string of the user's choice (such as a customer's ID number or phone number) into the specified option 82 field. The string must be between 1 and 64 characters. The string will be hex-encoded and include a null terminator character at the end
    - ***None*** – does not insert anything into the specified option 82 field
17) ***Limit upload rate*** – enables or disables traffic shaping on the upload (wireless) path, and sets upload or download limit in Mbps
18) ***Limit download rate*** – enables or disables traffic shaping on the download (ethernet) path, and sets upload or download limit in Mbps

Configuration→Wireless

For the Access Point or Point-to-point master device the Configuration→Wireless section is following:



1) ***Wireless mode*** – allows choosing wireless operation mode among Access point, Station, Point-to-point master or Point-to-point slave

When the point-to-point modes are enabled, only a single peer connection will be allowed, and the link will be optimized for point-to-point performance

Changing the operating modes will require a reboot of the device to take effect

2) ***Antenna kit*** – allows selecting the additional antenna kit that is attached to the device. If no additional antenna kit is attached to the device, the option "Base unit only (no antenna kit)" must be selected
3) ***Channel width*** – allows choosing between Full (2.16 GHz) or Half (1.08 GHz) options

- The benefit of half channel is more channels available for high-density deployments and an increase in SNR due to increased receiver sensitivity
- The data rate of a half channel is 1/2 of that of a full channel (up to MCS9)
- The channel scanning time is a bit longer for half channels so it will take longer time for stations to connect. Each channel scanned has up to 64 beam forming locations and there are 11 half channels - so the total time to complete a full scan can be up to 1 minute

4) ***Channel*** – indicates the list of available non-overlapping channels. For the full 2.16 GHz channel width, the selectable channels are 1-6, and channels 1-11 for half 1.08 GHz channel width

The "Channel" option is not available in Station or Point-to-point slave units

5) ***Max MCS*** – allows choosing the max MCS (Modulation Coding Scheme). The data rates will be dynamically selected up to the maximum MCS configured by the user

- When half-channel support is enabled, the max MCS allowed is MCS 9
- Setting max MCS only affects the TX MCS rate of the current device. To set MCS for both TX And RX, the user must change the max MCS value on both the Access point and Station sides of the link

6) ***SSID*** – the radio's SSID/network name, configurable by the user
7) ***Security mode*** – select link encryption type – either "Open" or "AES+GCMP"
8) ***Passphrase*** – will appear when the "AES+GCMP" security mode is chosen, and can be changed by the user

For the Station or Point-to-point slave device in the Configuration→Wireless section following additional settings are available:

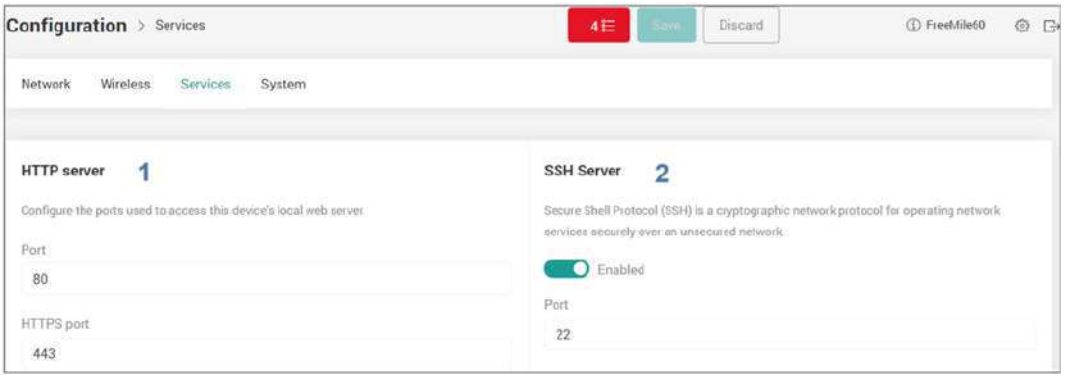
9) ***Failover*** – indicates the status of Failover mode
10) ***Enabling*** of Station profiles – allow to input multiple connection profiles. The client will connect to the SSID/profile with the highest priority first

Once the station profiles are enabled, this radio's main SSID and security settings will no longer be in use, and the station will attempt to connect to the profiles created in the station profiles' table in order of priority.

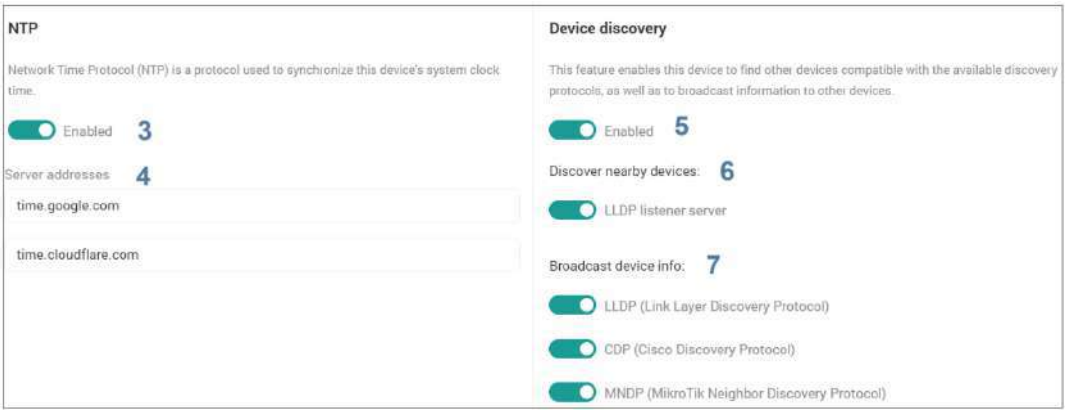
11) ***Priority*** – allows choosing the priority of the profile. Value 1 is the highest priority, and value 10 is the lowest one. When the user defines multiple profiles with the same priority, the device will connect to the SSID that has the better signal strength
12) ***SSID*** – the SSID for the connection profile
13) ***Security Mode*** – the security mode that should be used when connecting to the specified Access point
14) ***Security Passphrase*** – the passphrase that should be used when connecting to the specified AP if the AES-GCMP security mode is chosen
15) ***Enable sorting*** – unchecking this option will disable sorting of the profiles table while adding/entering profiles to keep the entries from jumping around during the changing of profile priorities

Configuration→Services

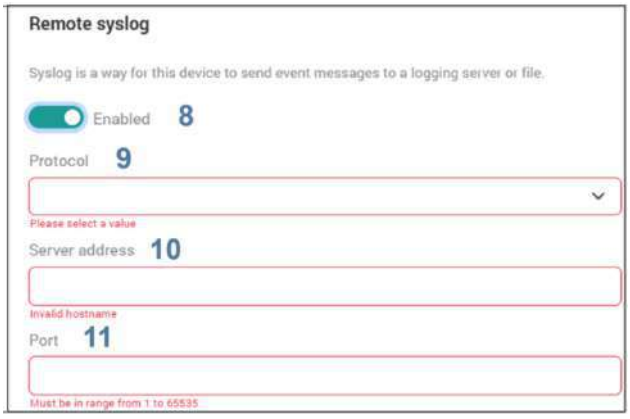
The following Services configuration options are available:



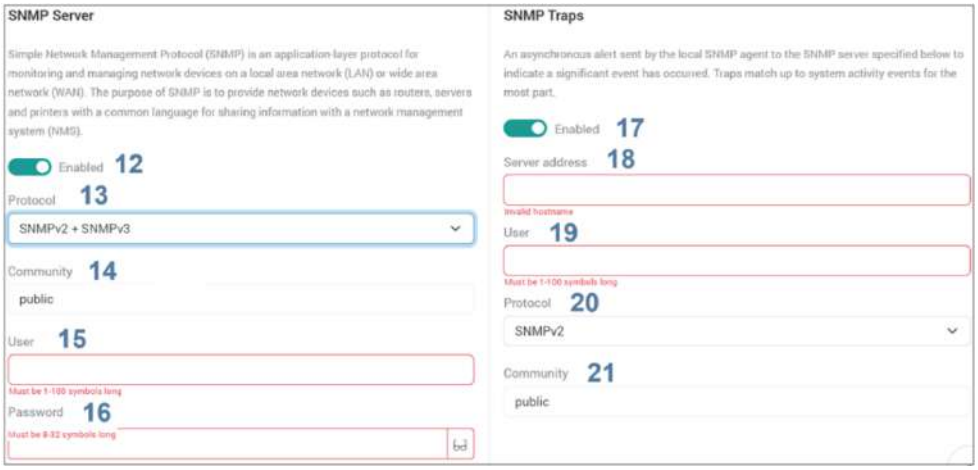
1) ***HTTP server*** – allows configuring HTTP and HTTPS ports used to access the device's local Web server
2) ***SSH server*** – allows enabling/disabling the SSH service, and configuring SSH port for device access



3) ***Enable*** NTP – allows enabling/disabling the NTP (Network Time Protocol) server. This service is enabled by default
4) ***Server addresses*** – a list of NTP peers that the device should use when updating the local time
5) ***Enable*** device discovery – allows enabling/disabling the device discovery service for the device
6) ***Discover nearby devices*** – enables the LLDP (Link Layer Discovery Protocol) server to find nearby devices on the network. Nearby devices can be found by using the Device discovery tool in the *Tools →Device discovery* page
7) ***Broadcast device info*** – allows the device to be discoverable over LLDP (Link Layer Discovery Protocol), CDP (Cisco Discovery Protocol), and MNDP (Mikrotik Neighbor Discovery Protocol)



8) ***Enable*** remote syslog – allows enabling/disabling the remote syslog service
9) ***Protocol*** – allows choosing remote syslog server protocol: TCP or UDP
10) ***Server address*** – allows entering an IP address or hostname of the remote syslog server
11) ***Port*** – allows specifying port at which the remote syslog server is running

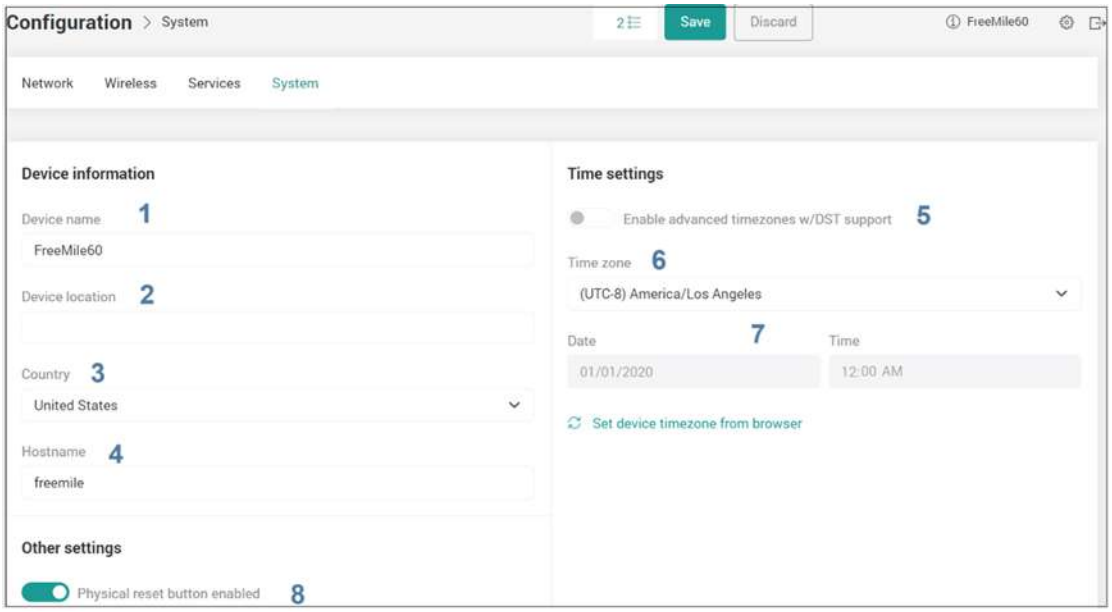


12) ***Enable*** SNMP server – enables the local SNMP server. The SNMP server is disabled by default
13) ***Protocol*** – allows choosing following SNMP versions: SNMPv2, SNMPv3, or dual SNMPv2 + SNMPV3
14) ***Community*** – allows entering the community string for the SNMP server. Available only for SNMPv2. The default value is *public*
15) ***User*** – allows entering SNMPv3 authentication username. Length must be between 1 and 100 characters. Available only for SNMPv3
16) ***Password*** – allows entering SNMPv3 SHA+AES authentication passphrase. Length must be between 1 and 32 characters. Available only for SNMPv3
17) ***Enable*** SNMP traps – allows enabling/disabling SNMP traps to be sent from the device
18) ***Server address*** – allows entering the hostname or IP of the SNMP trap receiver
19) ***User*** – allows entering the username that should be included when connecting to the server. If no username is required, just use a dummy value
20) ***Protocol*** – allows choosing the trap version: SNMPv2 or SNMPv3
21) ***Community*** or ***Password*** – allows entering community string for SNMPv2, or allows specifying password used for SNMPv3

22) ***Enable*** Ping watchdog – enables the ping watchdog service. This service pings the specified IP address at the given interval and reboots the device after receiving a certain number of failures in a row. This service is disabled by default
23) ***Ping interval*** – how long the service should wait, in seconds, between attempts to ping the provided IP address
24) ***Startup delay*** – the length of time in seconds that the service should wait until it attempts the first ping after the device has finished the bootup process
25) ***Failure count*** – the maximum allowed number of failures allowed (in a row) before the device will be rebooted
26) ***IP address(es) to ping*** – the IP address that the service will attempt to ping

Configuration→System

The following System configuration options are available:

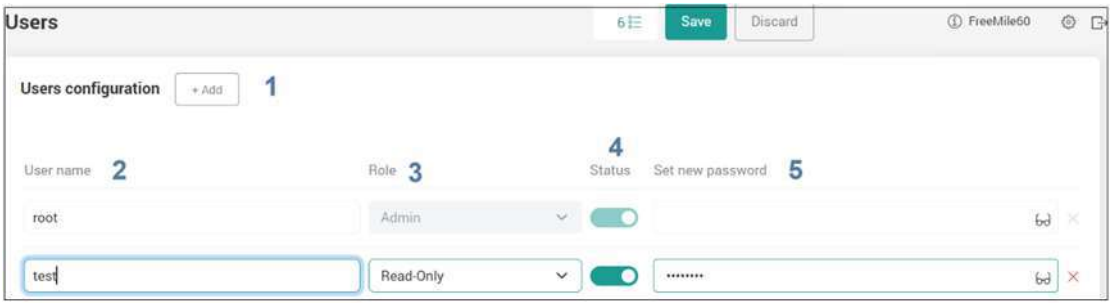


1) ***Device name*** – allows entering the name of this device. This field is used to populate the system name field used in the *Tools→Device discovery* list
2) ***Device location*** – allows entering the physical location of this device. This free-form field is not used internally by the system, it can be set to any customer's chosen name
3) ***Country*** – allows selecting the country where this device will be used. The country field is used to set local regulatory rules
4) ***Hostname*** – allows entering the system hostname of the device. This must be a valid hostname format and only contain alphanumeric characters, periods, and dashes, and must start or end in an alphanumeric character
5) ***Enable advanced time zones w/DST support*** – allows selecting this option to enable time zones that have DST support enabled
6) ***Time zone*** – allows selecting the time zone that should be used for this device's time
7) ***Date, time*** – use the date and time fields to manually set the device's local date and time. Manual date/time configuration is not possible if the NTP is enabled.
8) ***Physical reset button enable*** – allows enabling or disabling the physical reset button

It is not recommended to disable the device's physical reset button, as misconfiguration could make the device become unreachable

Users

Users section allows the configuration of users. When any of the parameters are changed in the Users section the “List”, “Save” and “Discard” buttons will appear in the header of the Web page. All new settings will be applied by pressing “Save” button.



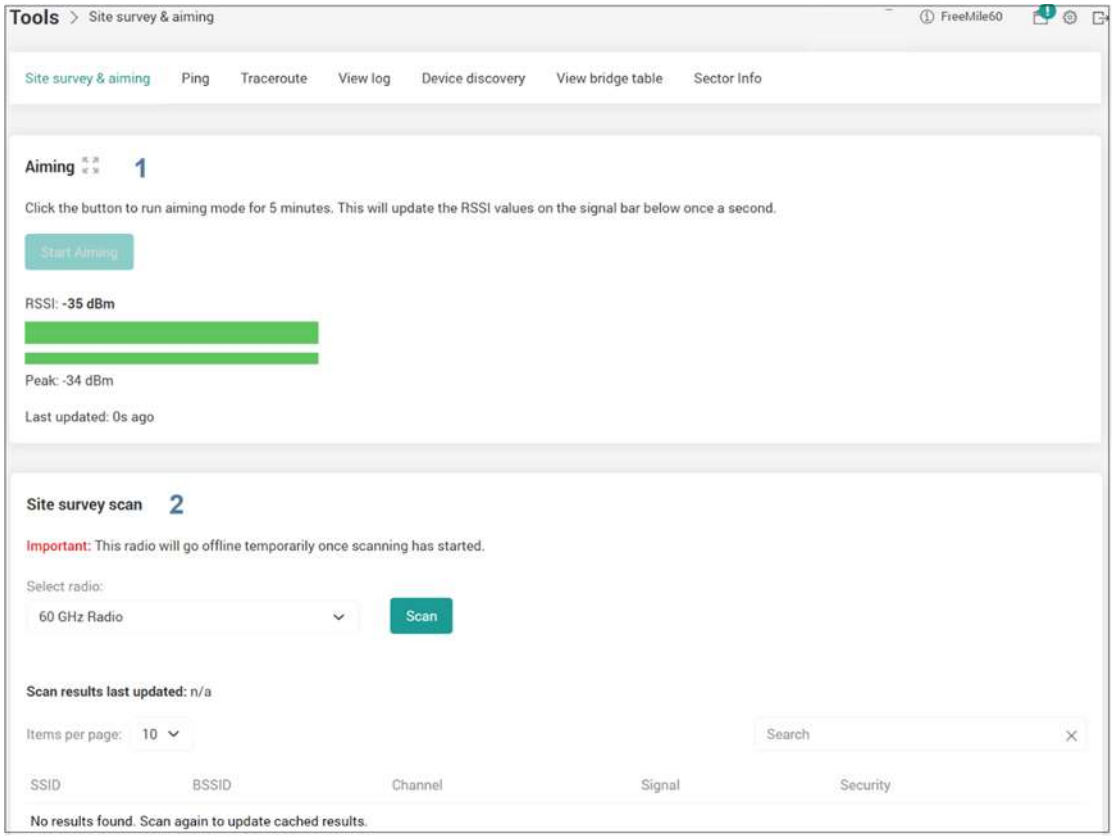
1) ***+Add*** – allows adding new users to the list
2) ***User name*** – allows setting the user name
3) ***Role*** – allows choosing the user role between “Admin” and “Read-Only” options
4) ***Status*** – allows enabling or disabling the user
5) ***Set new password*** – allows setting the password for each user

Tools

Tools section contains several tools for operation with Freemile 60 radios.

Tools→Site survey & Aiming

The following options are available:



1) ***Aiming*** – the Aiming tool can be used during the link alignment to display the RSSI signal strength changes at a faster rate than it is displayed in the device's dashboard. This tool is available only when operating in Station or Point-to-point slave modes. To view the aiming data in full-screen mode, click the "fullscreen" icon next to the Aiming header

When the Aiming is started two lines are displayed – the RSSI line indicating the actual RSSI level, and the Peak line indicating the max reached RSSI level at some point during the Aiming process.

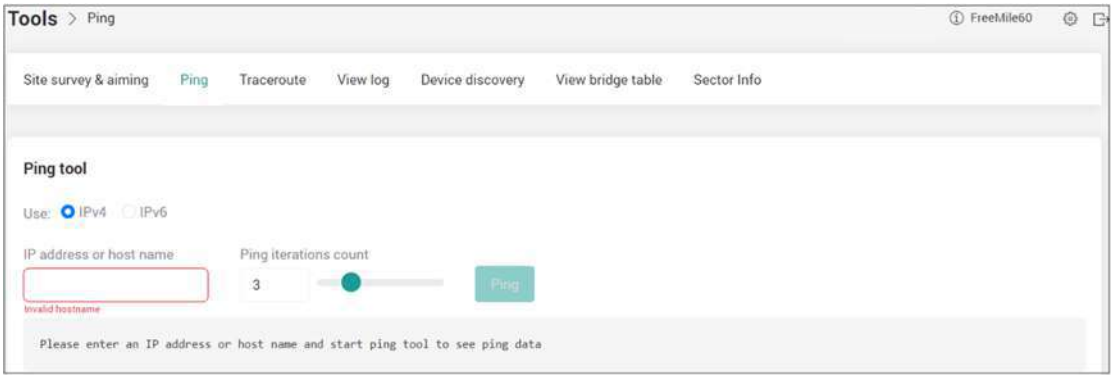
The coloring of both lines will change among green, orange and red depending on the RSSI level, and in accordance with LED blinking pattern. For LED blinking pattern refer to *Freemile 60 FODU interfaces and LED indications* section

2) ***Site survey scan*** – use the site survey tool to view a list of other Freemile 60 Access points broadcasting in the nearby area. This tool is only available when operating in Station or Point-to-point slave modes

Running a site survey scan will temporarily cause the radio to become unreachable. It will come back automatically when scanning is complete

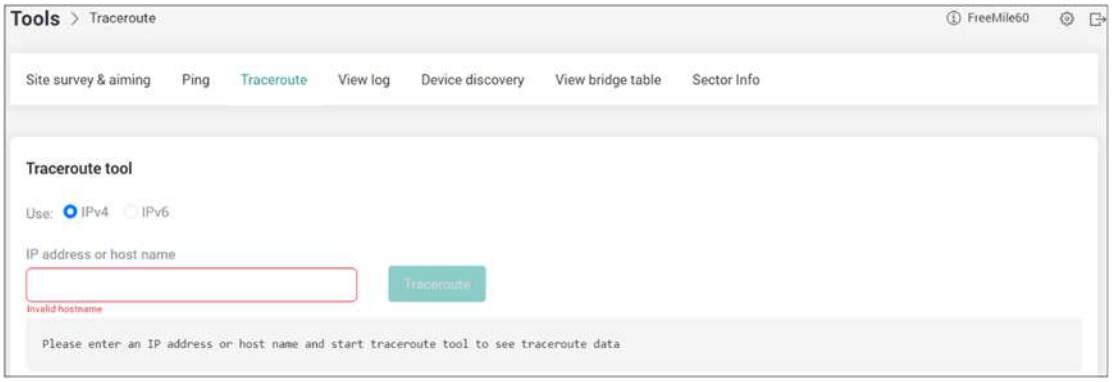
Tools→Ping

Performs basic pinging of IPv4 or IPv6 address from the device:



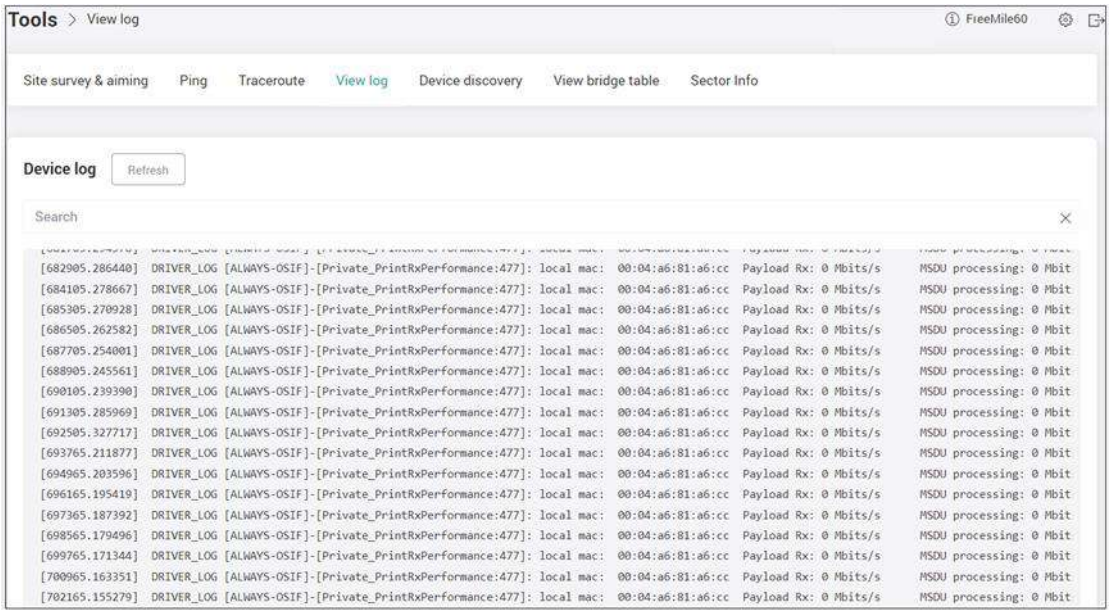
Tools→Traceroute

Performs a basic traceroute operation from the device:



Tools→View log

Search and view the device's log output:



Tools→Device discovery

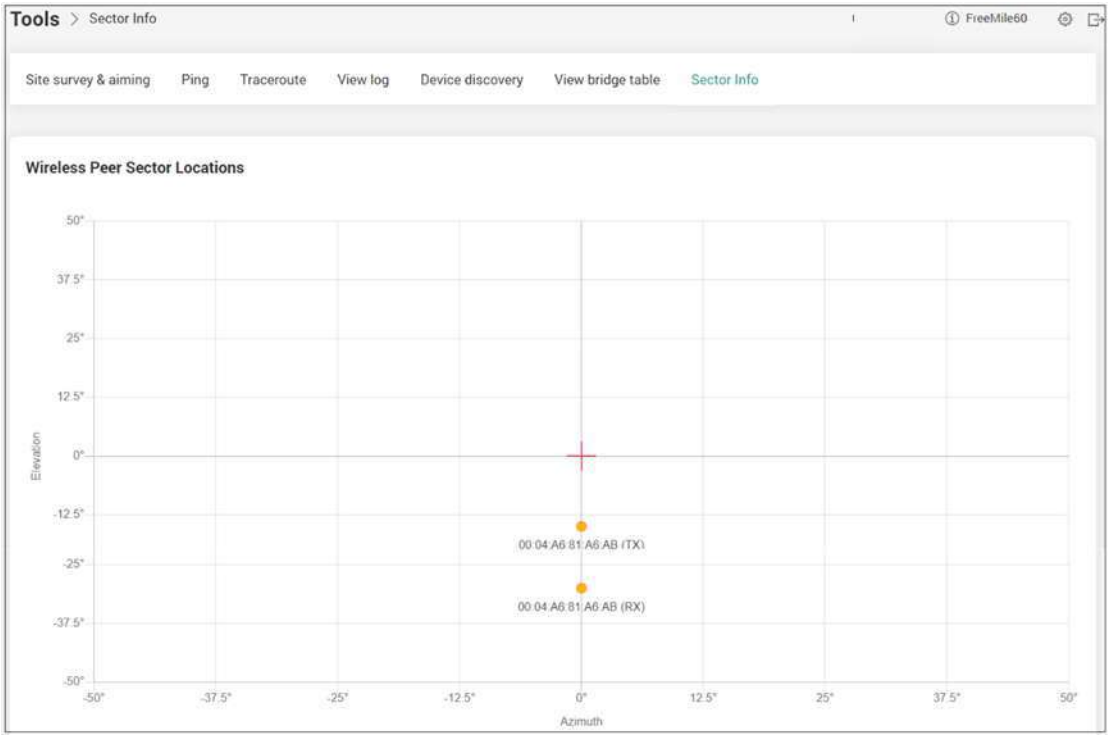
Use the device discovery tool to find other devices in the network. The Device Discovery option must be enabled under the *Configuration →Services* in “Device discovery” section for the device(s) to be discoverable:

Tools→View bridge table

Use the bridge table tool to view the MAC addresses in the device's bridge forwarding table, as well as their associated interface and bridge:

Tools→Sector info

The sector tool will allow visually see how each peer is connected to the current device (the orange dots), which can help to determine how close connected peers are to the boresight (red “X”):



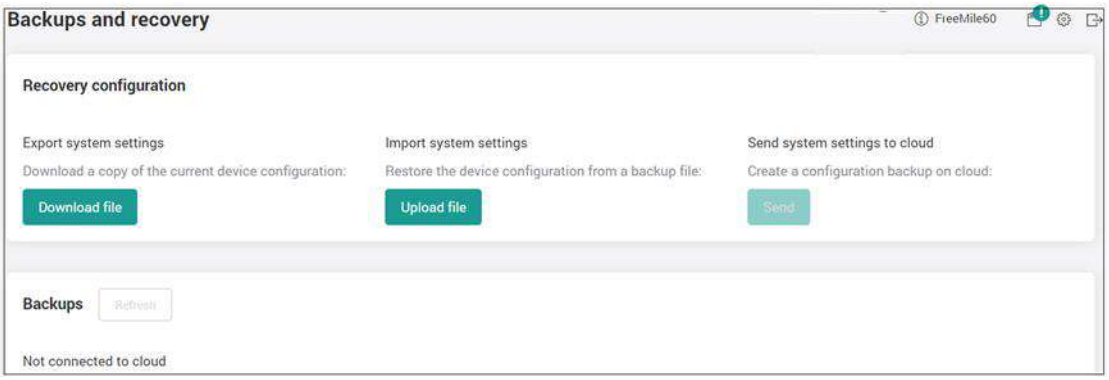
On the Access point side, boresight should be pointed in the center of the area. It is expected that each client will show up on a different sector, based on its physical location (azimuth & elevation), relative to the Access point.

On the Station side, the general goal is to get as close to boresight as possible. However, this is not a strict requirement. As long as there is a signal in the expected range, no need to adjust further the position of the Station. More details of Sector info tool can be found in *Sector info tool description*

- Sector info is not currently available when an antenna kit is selected
- When clicking on a connected peer's sector ID from the Dashboard section, it will be possible only to see that individual sector on the sector tool
- When multiple peers are connected to the same sector, the point will be indicated as larger, and a list of up to the first 3 devices connected on that sector will be indicated
- It is possible for a peer to be connected on different sectors for RX and TX. When this happens, a peer will be represented by two dots, each with a "(RX)" or "(TX)" label following the peer's name
- There are 4 total beams used when a link is made: Access point TX and RX, and Station TX and RX
- TX and RX sectors will be the same in almost all cases on each side of the link

Backups and recovery

Allows downloading/uploading configuration file to the PC for backup and recovery purposes:


Backups and recovery
FreeMile60
Recovery configuration
Export system settings
Download a copy of the current device configuration:
Download file
Import system settings
Restore the device configuration from a backup file:
Upload file
Send system settings to cloud
Create a configuration backup on cloud:
Send
Backups
Refresh
Not connected to cloud

Chapter 5: FUNCTIONAL DESCRIPTION and TOOLS

Failover mode

The Freemile 60 units operating in Station or Point-to-point slave modes can be configured in Failover mode. In this mode, it can use an alternative upstream data path via a device connected to the ETH1 (1Gbps) port if the wireless link has faded or has lost the synchronization. For example, the device connected to ETH1 port can be even a different Station unit pointed to a completely different site.

The alternative data path will be used under the following circumstances:

1. The Station is not currently associated with any Access Point, or
2. The RSSI of the wireless link drops below the pre-configured RSSI threshold (refer to section *Configuration →Network* for Failover mode configuration details)

The device will switch back to the wireless uplink data path once the following two conditions are met:

1. The station is connected to the Access Point at an RSSI level that is above the pre-configured failover threshold, and
2. The RSSI level of the link has been above the failover threshold value for the amount of time defined in the "Flap protection time (sec)" field under the Failover mode settings

The current failover status can be viewed from the Station device Dashboard. It will be updated once the device's wireless signal is back within a normal range, and the flap timer is counting down. More status details are available under the ETH1 settings of the Dashboard. Also, the activity events, log entries, and SNMP traps are all created whenever the device's failover state changes.

Sector info tool

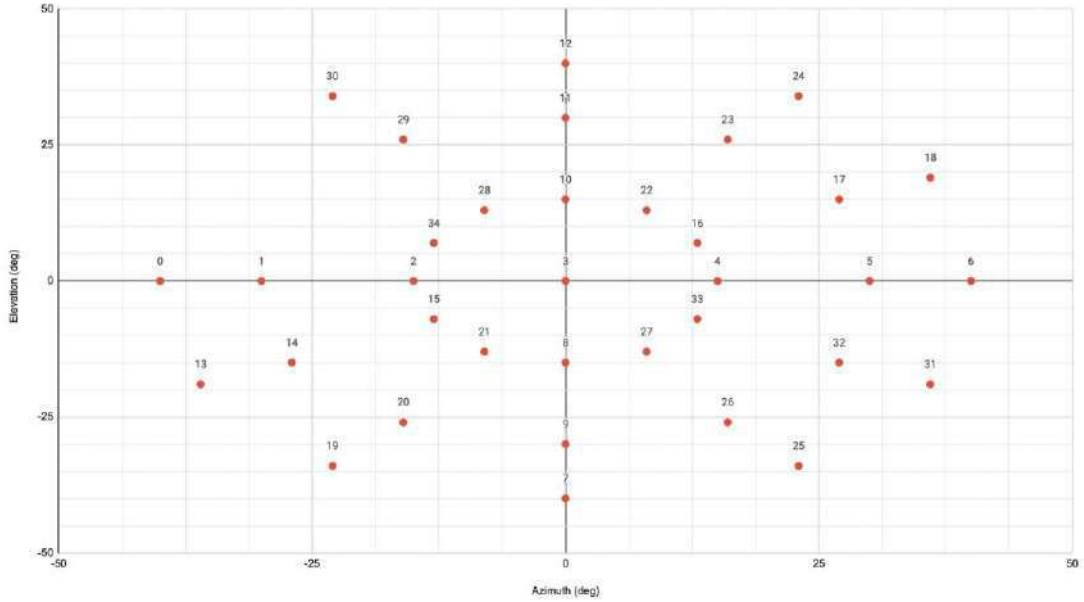
The sector tool will allow visually see how each peer is connected to the current device (the orange dot), which can help to determine how close connected peers are to the boresight. The boresight is the red cross in the graph indicating the device itself.

On the Access Point side, boresight should be pointed in the center of the area. It is expected that each client will show up on a different sector, based on its physical location (azimuth & elevation), relative to the Access Point.

On the Station side, the general goal is get as close to boresight as possible. However, this is not a hard requirement. As long as there is a signal in the expected range there is no need for further adjusting the position of the Station.

There are 4 total beams used when a link is made: Access Point TX and RX, and Station TX and RX. The TX and RX sectors will be the same in almost all cases on each side of the link.

Sector mapping example:



MIB files

Refer to techsupport@saftehnika.com for MIB files

ABBREVIATIONS

AP – Access Point
AC – Alternating Current
AES – Advanced Encryption Standard
ANSI – American National Standards Institute
API – Application Programming Interface
CPU – Central Processing Unit
CDP – Cisco Discovery Protocol
DC – Direct Current
DHCP – Dynamic Host Configuration Protocol
DNS – Domain Name System
DST – Daylight Saving Time
ETH – Ethernet
FCC - The Federal Communications Commission
FDB – Forwarding Database
FODU – Full Outdoor Unit
FTP – Foil Twisted Pairs
FW – Firmware
GUI – Graphical User Interface
GCMP – Galois/Counter Mode Protocol
HTTP – Hypertext Transfer Protocol
HTTPS – Hypertext Transfer Protocol Secure
IEEE - Institute of Electrical and Electronics Engineers
IP – Internet Protocol
ISEDC – Innovation, Science and Economic Development Canada
LED – Light-Emitting Diode
LLDP – Link Layer Discovery Protocol
MAC – Media Access Control
MCS – Modulation Coding Scheme
MIB – Management Information Base
MNDP – Mikrotik Neighbor Doscovery Protocol
MTU – Maximum Transmission Unit
NTP – Network Time Protocol
PC – Personal Computer
PoE – Power over Ethernet
PTP – Point-to-point
RF – Radio frequency
RSSI – Received Signal Strength Indicator
RX – Receive
SHA – Secure Hash Algorithm
SNMP - Simple Network Management Protocol
SSID – Service Set Identifier
SSH - Secure Shell
STP – Shielded twisted pair
TCP – Transmission Control Protocol
TDD – Time Division Duplex
TDMA – Time Division Multiple Access
TV – Television
TX – Transmit
UDP – User Datagram Protocol
URL – Uniform Resource Locator
VLAN – Virtual Local Area Network

SAF Tehnika JSC
24a, Ganibu dambis, Riga, LV-1005, Latvia, EU
techsupport@saftehnika.com
www.saftehnika.com