CONFIGURATION GUIDE FOR THE WEB UI

RADWIN 5000

Release 5.1.45

Doc.Rev 1

RADWIN

Table of Contents

Chapter 1: Introduction

1.1. Scope of This Document

This document shows how to use the Web UI to configure RADWIN 5000 radios and sectors.

- For a list of which products are configured by the Web UI, and which are configured by the RADWIN Manager, see Which Management Tool to Use.
- For a detailed description of how to use the RADWIN Manager to configure RADWIN 5000, see the RADWIN 5000 *Configuration Guide for the RADWIN Manager*.
- For a detailed description of how to physically install RADWIN 5000 radios, see the RADWIN 5000 Installation Guide.

1.2. RADWIN 5000 Overview

1.2.1. Sector

The RADWIN 5000 system consists of a “sector” that includes a base station, and at least one subscriber unit. The subscriber units are installed and work opposite the base stations.

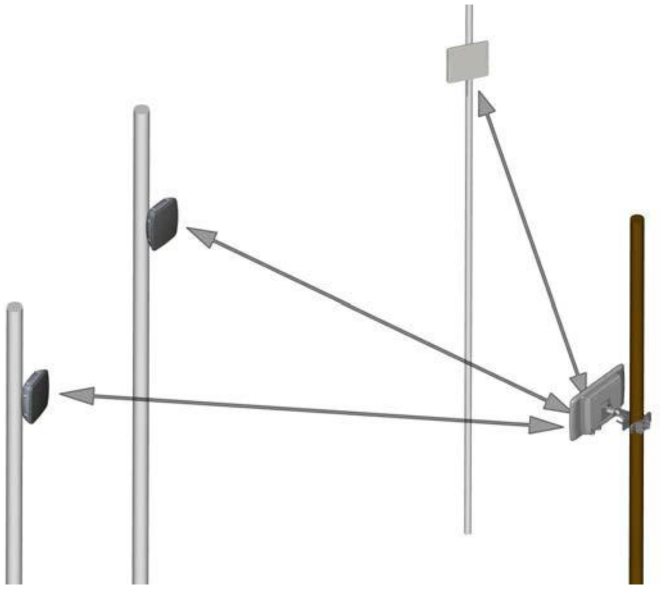


Figure 1-1: A RADWIN 5000 Sector

1.2.2. Base Station

There are several types of base stations, all of which are High Capacity Base Stations (HBS):

- Large Form Factor (LFF) - With an integrated or external antenna
- RADWIN 5000L - With an integrated or external antenna
- Beamforming (JET and NEO units) - With an integrated antenna
- Beamforming (DUO and NEO DUO) - With an integrated antenna and can work with two carrier frequencies
- MultiSector Base Station - Integrated
- MultiSector Base Station - Connectorized

1.2.3. Subscriber Unit

There are four categories of RADWIN 5000 subscriber units:
(SU) series:

- **SU PRO/AIR Embedded series**
- **SU PRO/AIR Integrated series**
- **SU PRO/AIR Connectorized series**
- **LFF HSU – not covered by this guide**

An SU can have one of the following resource allocations:

- CIR - Committed Information Rate: receives a guaranteed percentage of resources
- BE - Best Effort: receives resources according to availability

In addition, an SU can have one of the following form factors:

- Large Form Factor (LFF) - Its external appearance is similar to a Large Form Factor HBS, and can have an integrated or external antenna.
- Small Form Factor (SFF) - As its name implies, this unit is smaller than an LFF unit, but can also have an integrated or external antenna.

SU PRO/AIR Embedded series

- SU ***PRO*** EMB - Can operate using the CIR or BE resource type.
- SU ***AIR*** EMB - Can operate using the BE resource type only.

SU PRO/AIR Integrated series

- SU Integrated and SU ***PRO*** INT 3.x - Can operate using the CIR or BE resource type.
- SU Integrated - Can operate using the BE resource type only.

SU PRO/AIR Connectorized series

- Requires an external antenna.

Note

With the exception of the frequency band, the SU Integrated and SU ***PRO*** INT 3.x unit are identical in form factor and function. We will use the term SU Integrated to refer to both models.

1.2.4. External Antennas

The following units can work with an external antenna:

- Large Form Factor (LFF) - Connectorized only
- Small Form Factor (SFF) - Connectorized only
- SU Connectorized - Can ***only*** work with an external antenna
- SU ***PRO/AIR*** EMB - Can work with standard external antennas or with the Turbo Gain antenna
- MultiSector Base Station Integrated - Can work with standard external antennas or with the MultiSector antenna
- MultiSector Base Station Connectorized - Can work with standard external antennas

RADWIN offers many kinds of external antennas; some are shown here. They vary according to their azimuth beam width, size, polarization and approved frequency. For specific antennas and their characteristics, contact your customer representative. For a more theoretical account of antennas, see Appendix B, *About Antennas*.

All external antennas, with the exception of the Turbo Gain and the MultiSector antenna, can be used with all units. The Turbo Gain can only be used with the SU ***PRO/AIR*** EMB, and the MultiSector antenna can only be used with the MultiSector Base Station.

Although omni antennas can work with any radio, they are more suited to nomadic units.

Table 1-1: Antenna Summary (Sheet 1 of 3)

Type	Figure	Azimuth beam width (degrees)	Typical Use
Flat		<60 to 120, depending on model	General purpose
Rectangular		60-120 (depending on model)	Sector

Table 1-1: Antenna Summary (Sheet 2 of 3)

Type	Figure	Azimuth beam width (degrees)	Typical Use
Dish Mesh	 	<60	Point to Point, Long Distance
Omni		360	Nomadic

Table 1-1: Antenna Summary (Sheet 3 of 3)

Type	Figure	Azimuth beam width (degrees)	Typical Use
Turbo Gain		10	SU ***PRO/AIR*** EMB only
MultiSector		90 per wing (180 total)	MultiSector Base Station integrated only

1.2.5. Method of Work

- Both the base stations and the subscriber units communicate respectively, with the service provider and users. The communication protocol for both the service provider and the users is Ethernet.

Warning

These models shall be located in a Restricted Access Location and be accessible only to a skilled person familiar with the unit construction and possible hazards. Check the voltage on the antenna connector before access. Possibility of hazardous voltage 56VDC appearance exists on accessible antenna connections. Use Personal Protection Equipment (e.g. insulating gloves) when working with the units or antennas.

Connect the shield of antenna coaxial cable to protective earth when a coaxial cable is used.

1.2.6. Worldwide single PN products

RADWIN products released before 2023 have specific part numbers for each regulation domain. New worldwide RADWIN products such as JET AIR and JET AIR DUO automatically enforce regulation based on GPS location, therefore there is no need for a specific part number per each regulation domain.

Enforcing Regulation Restrictions

Worldwide products include a built-in GPS/GNSS receiver. The radio's identify their location from GNSS, and determine the country in which they are located and the regulation and bands available for that country. Subsequently, a single PN is available for each HW version of the radio, without needing to create multiple PNs (dedicated PN for each regulation). The same radio device can be transferred from one regulation zone to another.

In cases where the operator is permitted by his local regulatory authority to operate in additional bands not specified by the regulation in his country, a licensing mechanism is available to enable opening additional bands for use in the radio device.

Outdoors (GPS-based) operation mode

When the radio detects a GNSS signal, it will determine the country it is located in and the applicable regulation.

User will only be able to select a frequency band that is allowed by the regulation of the detected country.

Indoors (No GPS) operation mode

In cases in which the user wishes to test the device indoors - e.g., inside a warehouse / lab, the device would not detect a GNSS signal. In this case, the device would be in "No GPS" mode, in which the user will be allowed to select the country manually. Once the country is selected, the device would detect the allowed regulation for this country, and the user will be able to select a frequency band allowed by this regulation.

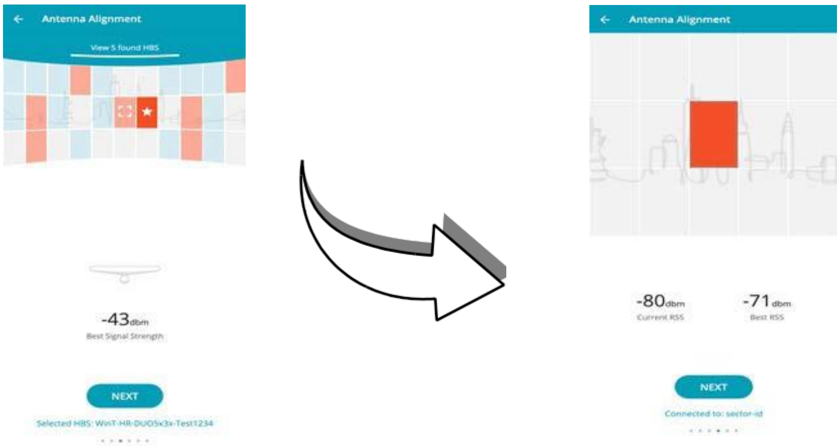
The selected country will be remembered by the device as long as the device doesn't detect a GNSS signal. Once GNSS signal is detected, the device would update the country to the country detected by GNSS, and would check for regulation mismatch between its previously selected band and the current allowed regulation. This functionality is intended to prevent the device from transmitting in a band forbidden by the local regulation.

The transmission would not be affected in case there is no mismatch between the regulation of the previously selected band and the current detected regulation.

1.3. Management Tools

1.3.1. WINTouch

WINTouch is a mobile application that guides you in installing and aligning SU ***PRO/AIR*** EMB, SU Integrated, and SU Connectorized subscriber units.



1.3.2. Web Interface

A Web Interface is available for SU ***PRO/AIR*** EMB, SU Integrated, DUO, NEO DUO, JET-AIR/ JET-PRO, SU Connectorized, and MultiSector units. The Web Interface is integrated with the radio unit, and, unlike the RADWIN Manager, requires no external application. You merely enter the unit’s IP address, username and password, and log in.

Note

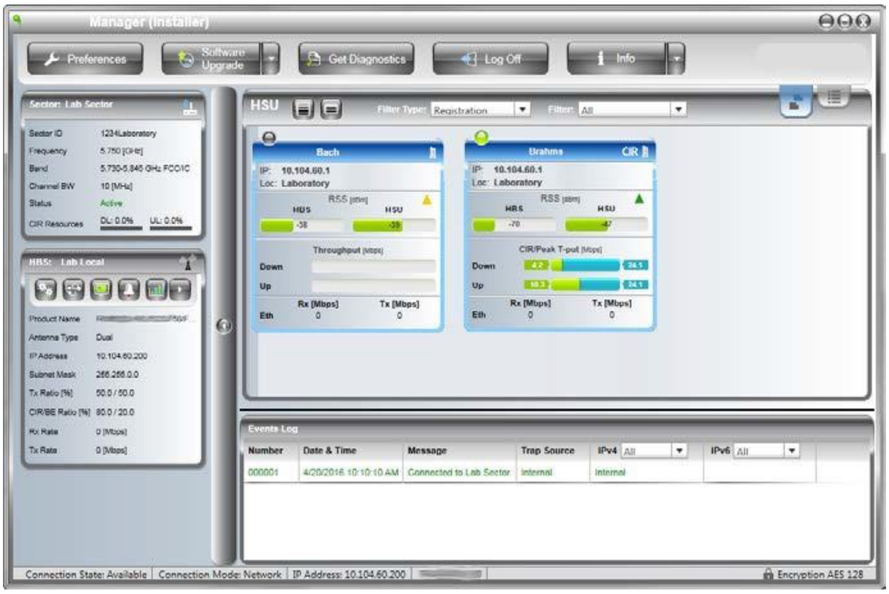
If the hardware version of the base station is of the format x.y, where x and y are numerals, the base station is managed via the RADWIN Manager, see Chapters 2 through 11.

If the hardware version of the base station is of the format xxxJ, where x is a numeral, the base station is managed via the WebUI. See Chapter 2.

1.3.3. RADWIN Manager

The RADWIN Manager is an SNMP-based management application, operating on your local computer, which manages a complete sector over a single IP address. Install the RADWIN Manager from http:/www.radwin.com/download.

A sample user interface is shown below:



Sector: Lab Sector

Sector ID 1234Laboratory
Frequency 5.750 [GHz]
Band 5.730-5.845 GHz FCC/IC
Channel BW 10 [MHz]
Status Active
CIR Resources DL: 0.0% UL: 0.0%

HBS: Lab Local

Product Name [redacted]
Antenna Type Dual
IP Address 10.104.60.200
Subnet Mask 255.255.0.0
Tx Ratio [%] 50.0 / 50.0
CIR/BE Ratio [%] 80.0 / 20.0
Rx Rate 0 [Mbps]
Tx Rate 0 [Mbps]

HSU Filter Type: Registration Filter: All

Bach
IP: 10.104.60.1
Loc: Laboratory
RSS [dBm] HBS -38 HSU -39
Throughput [Mbps] Down Up
Eth Rx [Mbps] 0 Tx [Mbps] 0

Brahms CIR
IP: 10.104.60.1
Loc: Laboratory
RSS [dBm] HBS -70 HSU -47
CIR/Peak T-put [Mbps] Down 4.2 24.1 Up 10.3 24.1
Eth Rx [Mbps] 0 Tx [Mbps] 0

Events Log

Number	Date & Time	Message	Trap Source	IPv4 All	IPv6 All
000001	4/20/2016 10:10:10 AM	Connected to Lab Sector	Internal	Internal	

Connection State: Available | Connection Mode: Network | IP Address: 10.104.60.200 | [redacted] | Encryption AES 128

Figure 1-2: RADWIN Manager

1.3.4. Which Management Tool to Use

Depending on the product you are using, use the Management Tool indicated below.

Table 1-2: Which Management Tool to Use

Product	Primary Management Tool (full functionality)	Secondary Management Tool (limited functionality)
LFF, SFF, JET base stations	RADWIN Manager	None (use only the RADWIN Manager)
DUO, JET-AIR/JET-PRO[a], NEO, NEO DUO, RADWIN 5000 L, MultiSector base stations	Web User Interface[b]	None (use only its Web Interface)
LFF, SFF, subscriber units	RADWIN Manager	None (use only the RADWIN Manager)
SU ***PRO/AIR*** EMB SU Integrated SU Connectorized subscriber units	Web User Interface	WINTouch+ for initial antenna alignment

[a] *New HW versions only*

[b] *Rel. 4.9.34 and above. For earlier Releases, use the RADWIN Manager*

1.4. Key Features of RADWIN 5000

1.4.1. General

- Ethernet connectivity
- Transparent to L2 protocols
- AAA RADIUS support
- Advanced OFDM & MIMO 2x2 for nLOS and NLOS performance
- Enhanced interference mitigation capability
- Inter & intra site sync to reduce self interference
- Multiband radios: different frequencies in the same radio unit
- Dedicated Bandwidth ensuring SLA & latency
- Regulations supported - FCC/IC/ETSI/WPC/MII/Universal
- Up to 128 Subscriber Units per base station (depending on model)
- Fully integrated with RADWIN legacy solutions
- Nomadic support

1.4.2. Beamforming Solutions

Smart beamforming integrated antenna, on-the-fly beamforming reduces interference, increases efficiency. Exceptional interference immunity through 2nd gen antenna

RADWIN 5000 JET, JET-AIR/JET-PRO, and NEO

- Single carrier platform
- 750Mbps
- Up to QAM 64 (old h/w) / up to QAM 256 (newer HW versions)[1], 1 x 80Mhz
- Integrated GPS synchronization capability, ethernet-based synchronization (old h/w)
- JET AIR/PRO (older HW) configured via RADWIN Manager, (new h/w)[1] Web UI only
- Support 64 SUs
- Interfaces: GbE and Fiber (SFP) (JET AIR/PRO older HW support GBE only)

JET-DUO 3/5 GHz, and NEO DUO (Web UI only)

- Multi-carrier platform for 3.x and 5.x GHz bands: JET-DUO 3/5 GHz
- Multi-carrier platform for two separate 5.x GHz bands in one radio: JET-DUO 5 GHz
- 2 x 750Mbps when operated as a dual-band solution
- Up to QAM 256, 2 x 80MHz
- Integrated GPS synchronization capability
- Support 128 customers (64 SUs per carrier)
- Interfaces: GbE and Fiber (SFP) (new h/w) [1]

[1] *Some models offer a Fiber (SFP) interface*

1.4.3. MultiSector

- Multi-carrier platform for 5.x GHz bands
- 2 x 750Mbps
- Up to QAM 256
- Supports up to 128 (2x64) subscriber units
- Can cover 360^o with a single radio unit
- Interfaces: Fiber (SFP) and GbE

1.4.4. RADWIN 5000L

- Single Carrier
- Up to 250 Mbps net aggregated throughput
- Supports up to 16 HS Subscriber Units
- Guaranteed Service Level Agreement (SLA) per Subscriber Unit
- Single radio supporting multiple bands
- Models: Integrated 90deg antenna or connectorized
- Integrated GPS synchronization capability
- Interfaces: PoE - GbE

1.5. What's New in Release 5.1.45

- Introducing the new Jet Air with a new antenna and a sing world-wide PN

Note

For complete and comprehensive characteristics of the specific model you are working with, refer to its Data Sheet.

1.6. Release Versions

Although this document is for Release 5.1.45, certain products and regulatory environments may use other versions. For more information, contact customer support.

1.7. Notifications

Notifications consist of Notes, Cautions, and Warnings:

Note

Note: Draws your attention to something that may not be obvious.

Caution	Caution: Risk of damage to equipment or of service degradation.

Warning	Warning: Risk of danger to persons operating near the equipment.

1.8. Miscellaneous Cautions and Warnings

Warning	All units shall be located in a Restricted Access Location and be accessible only to a skilled person familiar with the unit construction and possible hazards.

Warning	When working with the SU Connectorized unit - Possibility of hazardous voltage 56VDC appearance exists on accessible antenna connections. Use Personal Protection Equipment (e.g. insulating gloves) when working with the unit or the antenna. Connect the shield of antenna coaxial cable to protective earth when coaxial cable is used.

Chapter 2: Managing a Web-Configured HBS

2.1. Scope of this Chapter

This chapter covers both HBS configurations and SU configurations from the HBS.

- The following products are HBS units that are managed from the WebUI only[1]. Availability depends on your regulatory environment:
    - JET-DUO 5 GHz (5.x GHz & 5.x GHz)
    - JET-DUO 3/5 GHz (5.x GHz & 3.xGHz)
    - NEO, NEO DUO
    - JET-AIR (5.x GHz single-carrier unit)
    - JET-PRO (3.5 GHz or 5.x GHz single-carrier units)
    - MultiSector Base Station
- With dual-carrier units, the frequencies operate independently, but since they are from the same unit, the Sector ID for all carriers are the same, and if the HBS is reset, the action affects all carriers.

The MultiSector Base Station has two carrier frequencies in one unit which can be connected to up to two antennas, each with a different gain. The two carrier frequencies operate independently (they can be activated and de-activated independently, for example).

Caution

When starting manager release 11.0.x, a web management unit (SU-Air/Pro/DUO/NEO/Multisector) manager may indicate it is an unsupported version and will redirect the user to the web browser.
If you are working with an LFF, SFF, or JET base station , use the RADWIN Manager as the management application.

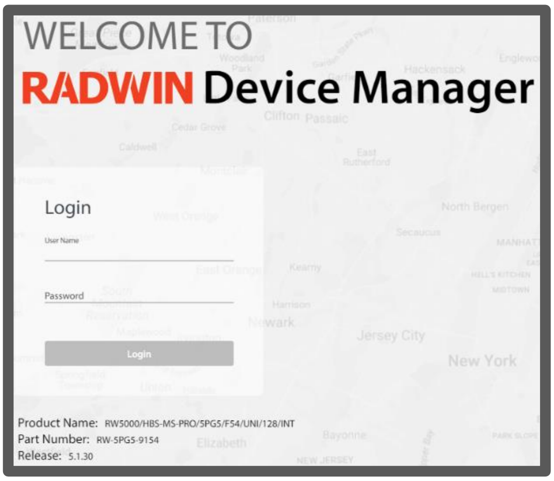
[1] *Other HBS units are managed via the RADWIN Manager. If the hardware version of the base station is of the format xxxJ, where x is a numeral, the base station is managed via the WebUI.*

2.2. Login

Supported browsers for the web interface are:

- Chrome (Windows)
- Safari (Macintosh)
- Edge (Windows - basic functionality only)
- Firefox (Windows - basic functionality only)

Access the web interface by connecting to the unit, either directly via RJ45 cable, or via the internet. We recommend using a PC or laptop. Enter the unit's IP address in a web browser (default value: 10.0.0.120). A welcome message will appear.



WELCOME TO

RADWIN Device Manager

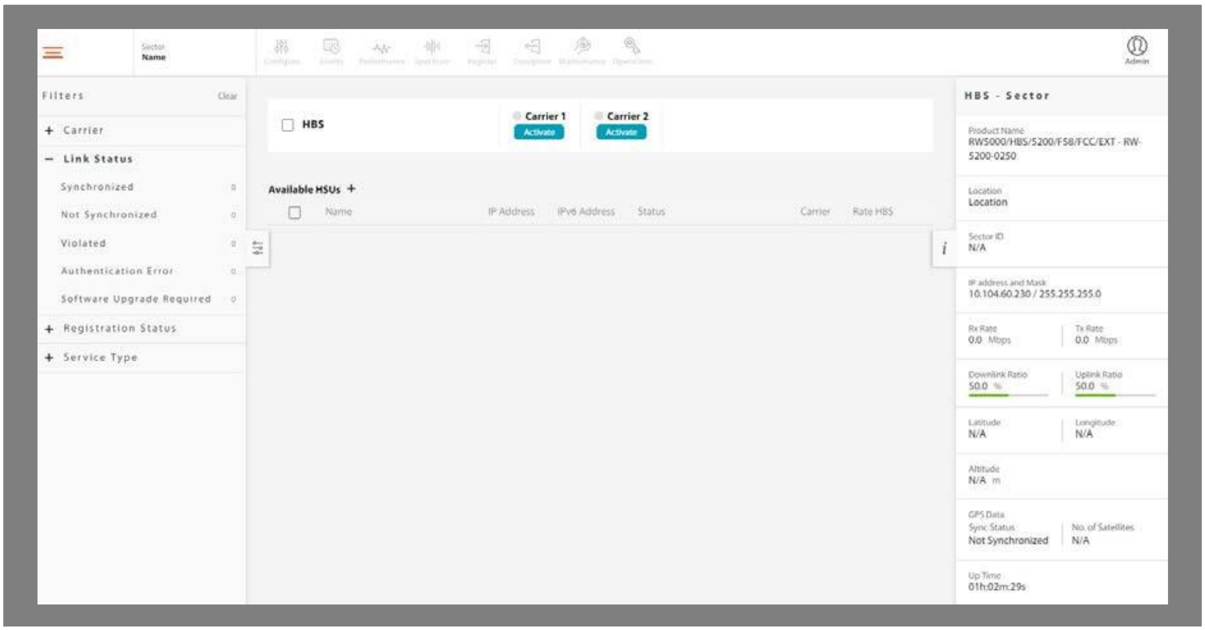
Product Name: RW5000/HBS-MS-PRO/5PG5/F54/UNI/128/INT
Part Number: RW-5PG5-9154
Release: 5.1.30

Enter the username and password, then click **Login.**

User name: **admin**

Password: **netwireless**

The main window will appear.



□ HBS

□	Name	IP Address	IPv6 Address	Status	Carrier	Rate HBS

HBS - Sector

Product Name
RW5000/HBS/5200/F58/FCC/EXT - RW-5200-0250

Location
Location

Sector ID
N/A

IP address and Mask
10.104.60.230 / 255.255.255.0

Rx Rate
0.0 Mbps

Tx Rate
0.0 Mbps

Downlink Ratio
50.0 %

Uplink Ratio
50.0 %

Latitude
N/A

Longitude
N/A

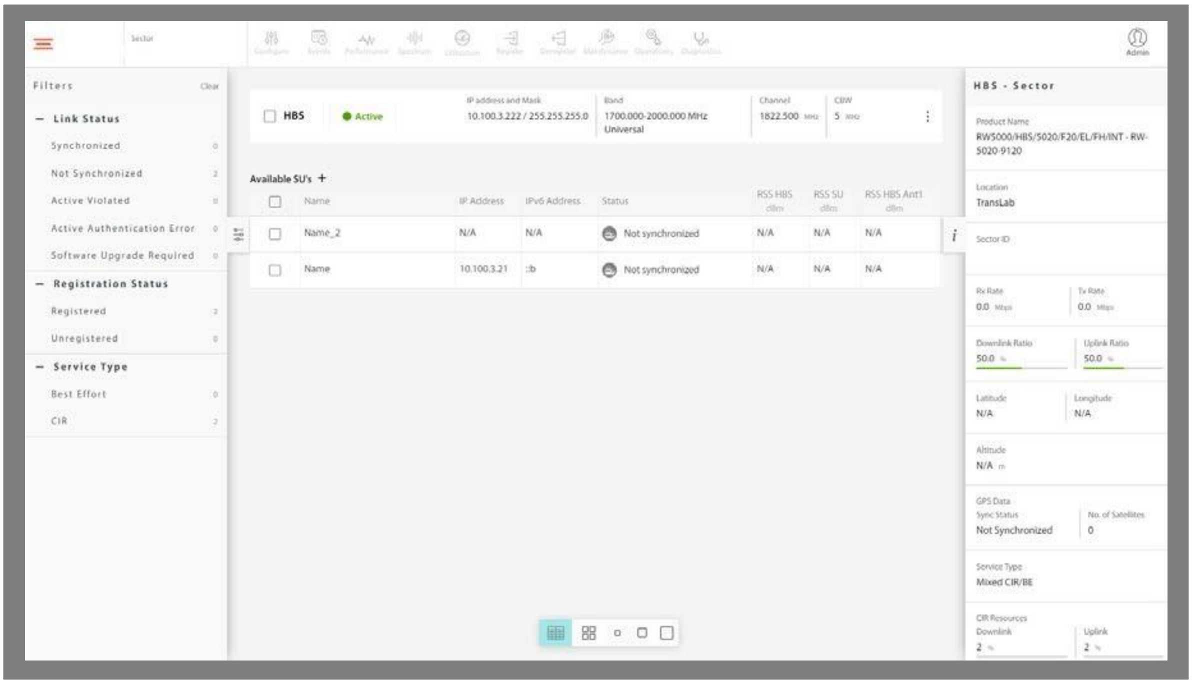
Altitude
N/A m

GPS Data
Sync Status
Not Synchronized

No. of Satellites
N/A

Up Time
01h:02m:29s

Figure 2-1: Main window for dual-carrier and multi-sector units



□ HBS	● Active	IP address and Mask 10.100.3.222 / 255.255.255.0	Band 1700.000-2000.000 MHz Universal	Channel 1822.500 MHz	CBW 5 MHz

□	Name	IP Address	IPv6 Address	Status	RSS HBS dBm	RSS SU dBm	RSS HBS Ant1 dBm
□	Name_2	N/A	N/A	Not synchronized	N/A	N/A	N/A
□	Name	10.100.3.21	::b	Not synchronized	N/A	N/A	N/A

HBS - Sector

Product Name
RW5000/HBS/5020/F20/EL/FH/INT - RW-5020-9120

Location
TransLab

Sector ID

Rx Rate
0.0 Mbps

Tx Rate
0.0 Mbps

Downlink Ratio
50.0 %

Uplink Ratio
50.0 %

Latitude
N/A

Longitude
N/A

Altitude
N/A m

GPS Data
Sync Status
Not Synchronized

No. of Satellites
0

Service Type
Mixed CIR/BE

CIR Resources
Downlink
2 %

Uplink
2 %

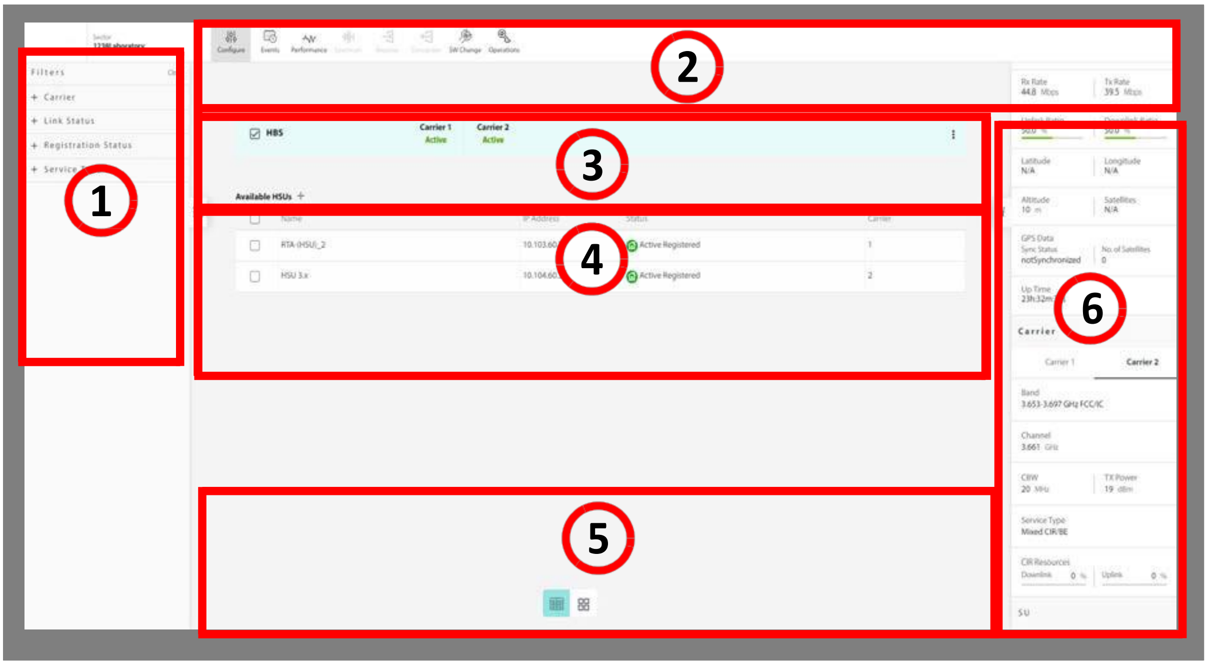
Figure 2-2: Main window for single carrier units

For an explanation of the Web User Interface, see *WebUI Overview*.

For instructions on first-time use of a base station, see *First-Time Use*.

2.3. WebUI Overview

The WebUI shows the base station and any subscriber units it has detected.



In dual-carrier units, you can see all carriers at the same time, with all subscriber units.

You can filter what you see, and display the subscriber units in various manners.

Click on the section of the WebUI of which you want more information:

1	*Filters*	2	*Main icons*
3	*HBS List*	4	*SU List*
5	*Sector Display views*	6	*Info Panel*

2.3.1. Filters

Here you can use certain criteria to filter what is displayed:

- **Carrier:** Select Carrier 1 or Carrier 2 (in multi-carrier systems) to show only devices using the selected carrier.
- **Link Status:** Select the status of the SUs you want displayed. Possible SU statuses are:

Icon	SU status Description	
⌂	Active Registered & Synchronized	Registered, in sync
⌂	Active Unregistered	Unregistered

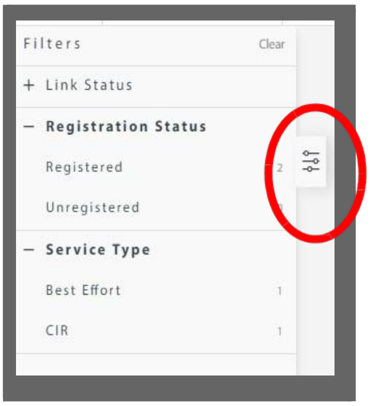
Icon	SU status Description	
🔴	Not Synchronized	Registered, no sync
🔵	Active Violated	Belongs to another sector
🟤	Software Upgrade Required	Software Upgrade required / Freq band mismatch
🟣	Active Authentication Error	Authentication error
⚪	Nomadic Unregistered	Unregistered, no sync, placeholder
🟢	Nomadic Registered	Registered, in sync
🔴	No Available Channel	No permitted TV channel is available for the SU

To show all devices using all statuses, select the Link Status title.

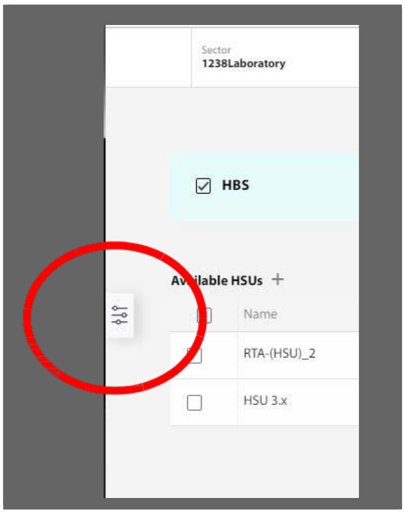
- **Registration Status:** Select Registered or Unregistered to show only devices in the indicated state.

  To show all devices, whether registered or not, select the Registration Status title.
- **Service Type:** Select Best Effort or CIR to show only devices with the indicated service type.

  To show all devices, no matter what the service type, select the Service Type title.
- To minimize the Filters list, click on the minimize symbol:



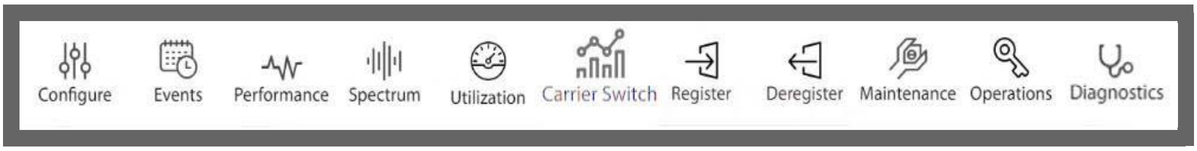
- To restore the Filters list, click on the minimize symbol again:



2.3.2. Main icons

Along the top edge of the WebUI, there are icons that allow you to carry out certain tasks for the radio units.

The applicable icons become enabled when you select the radio unit relevant for the task. For example, if you select an un-registered SU, the Register icon will become enabled, but the Deregister icon will not.



If you are configuring an SU directly, the Events, Performance, Utilization, Register and Deregister icons will not appear.

Configure	***Configure***	Set various parameters for the selected unit, including, but not limited to: • IP address • Frequency and bandwidth or channels • Transmission power • Passwords • NTP settings • VLAN • QoS, and more
Events	***Events***	Shows system failures, loss of synchronization, loss of signal, compatibility problems and other fault conditions and events for the selected unit or units. You can also search and filter the events by severity, source, and time.

Performance	***Performance***	The Performance Monitoring feature constantly monitors traffic and collects statistics data, whether or not the WebUI is open. Use this to see performance monitoring for the selected unit or units.
Spectrum	***Spectrum***	The Spectrum view feature provides spectral measurements, and is useful in assisting with diagnosing interference related problems prior to full sector activation. It is operated per carrier.
Utilization	***Utilization***	The Utilization shows how much of the available sector-wide resources of the air interface is actually being used.
Carrier Switch	***Carrier Switch***	Shows Carrier Switch events, including on which unit the carrier switch was done and its cause. This icon only appears for the JET-DUO 5 GHz.
Register	***Register***	Registers an SU: Enables service traffic between the SU and the HBS.
Deregister	***Deregister***	Deregisters an SU.
Maintenance	***Maintenance***	Back up, upgrade or restore the software in the selected unit or units.
Operations	***Operations***	Resets, restores to factory default configuration, and allows license-dependent upgrades on the selected unit or units.
Diagnostics	***Diagnostics***	Creates diagnostics files, for use by RADWIN professional services and supports personnel to expedite assistance.
Admin	***User Profile Icon***	Click this icon to log out of the HBS.

	Start monitor	Creates a monitoring file every 5 min, which contains all the parameters that are presented in the SU list. Select the required SU to be monitored and recorded in the file. Click on the + icon (next to the “Available SU’s” to add / remove parameters from the SUs list

2.3.3. Configure

These are the configuration categories:

System	*Services (HBS only)*	*Services (SU via HBS only)*
Tx & Antenna	*Air Interface (HBS or SU directly)*	*Management*
Hub Site Sync (HBS only)	*Inventory*	*Nomadic (HBS)*
Security	*Date & Time*	*Ethernet*
General (HBS only)	*IGMP*	*Networking (HBS only)*
WiFi (SU only)		

Most categories are relevant for both HBSs and SUs, but some are applicable only under certain criteria, as shown in the title of the category, and summarized below:

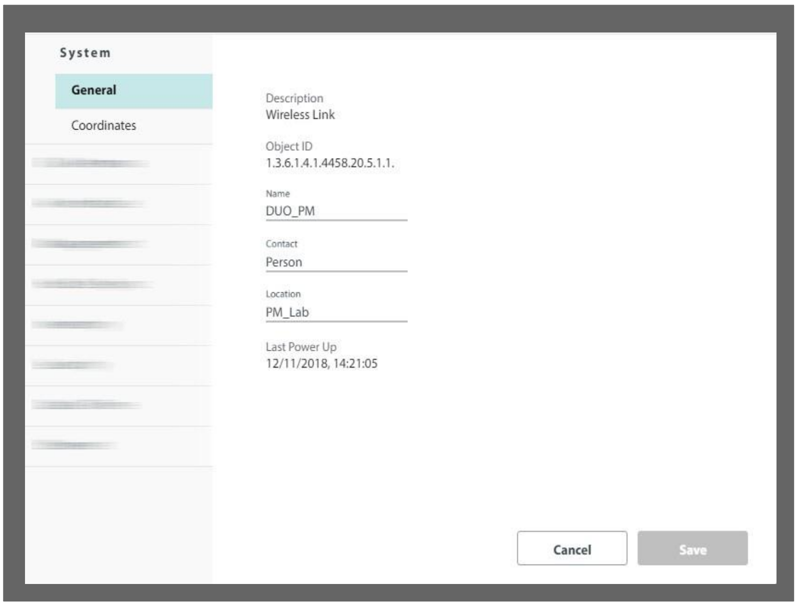
- HBS only: Only relevant for the HBS
- SU only: Only relevant for the SU
- SU directly: Can only be carried out if configuring the SU from a direct connection, not via the HBS. A full description of configuring an SU directly is found in Chapter 3: *Managing SU PRO/AIR Units Directly*.
- SU via HBS only: Can only be carried out if you are configuring the SU via the HBS.

In addition, some options in the categories can also be different according to what type of unit is accessed and how it is accessed.

2.3.4. System

General

These items are convenience fields: **Description, Object ID, Name, Contact, Location,** and **Last Power Up**. Name and Location are typically entered during HBS activation. If you make any changes, click **Save** to have them take effect.



Description
Wireless Link

Object ID
1.3.6.1.4.1.4458.20.5.1.1.

Name
DUO_PM

Contact
Person

Location
PM_Lab

Last Power Up
12/11/2018, 14:21:05

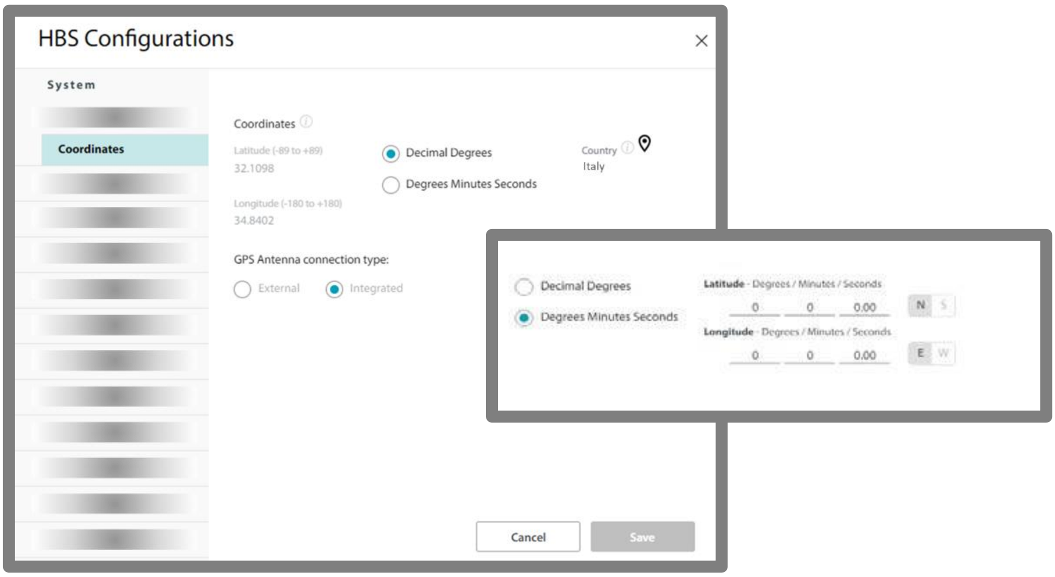
Coordinates

The coordinates (latitude and longitude) use either decimal degrees or degrees, minutes, and seconds. These coordinates can be changed manually for an SU only, and only if the radio does not have a GPS.

If the radio has an external GPS connection, you will be able to choose the connection type (external or integrated), height, and height uncertainty of the GPS antenna.

In Jet Air / Jet Air DUO, the current HBS country is displayed (either according to the GPS fix or according to user’s manual selection when there is no GPS fix). You can change the country only if there is not GPS fix, in the Change Band screen.

If you make any changes, click **Save** to have them take effect.



HBS Configurations

Coordinates

Latitude (-89 to +89)
32.1098

Longitude (-180 to +180)
34.8402

● Decimal Degrees
○ Degrees Minutes Seconds

Country
Italy

GPS Antenna connection type:
○ External ● Integrated

○ Decimal Degrees
● Degrees Minutes Seconds

Latitude - Degrees / Minutes / Seconds
0 0 0.00 N S

Longitude - Degrees / Minutes / Seconds
0 0 0.00 E W

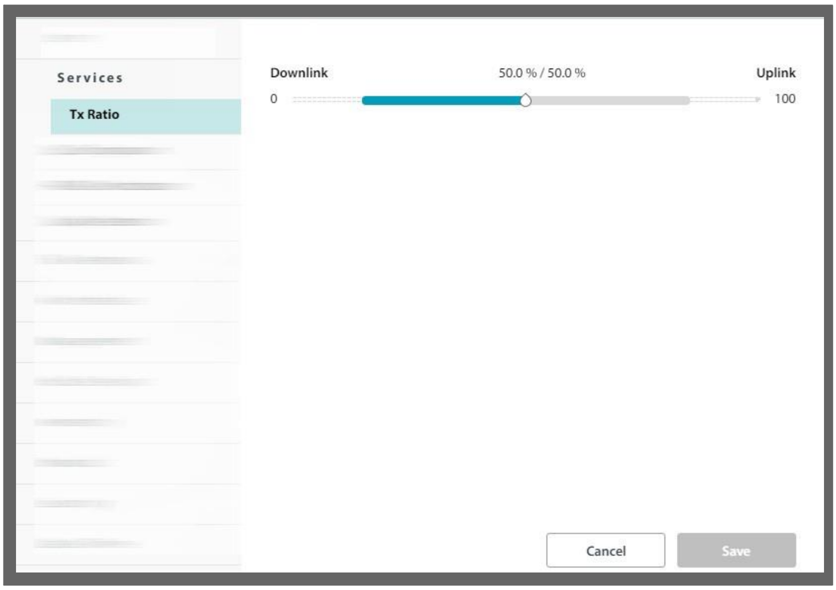
2.3.5. Services (HBS only)

Here you can configure the Tx Ratio, the QoS, RADIUS Service Authorization, and the Quality Detection.

Tx Ratio

The **Tx Ratio** (Transmission Ratio, Asymmetric Allocation) shows the allocation of throughput between downlink and uplink traffic at the HBS. The Transmission Ratio is not only sector-wide: If you use Hub Site Synchronization to collocate several HBSs (to cover adjacent sectors), they must all use the same Transmission Ratio.

1. Move the slider to the right or left to determine the Tx Ratio.
2. Click **Save** to have your changes take effect.



Caution

The allowable range is from 50/50 % to 85/15 %. Setting values beyond this range will cause unpredictable results. If the channel bandwidth is 10MHz, the range is up to 75/25% .

If you are configuring GPS Hub Site Synchronization and choose the “Shifted” option, the Tx Ratio must be exactly 50/50 %

You must ensure that the range remains within allowable values. There is no fail-safe.

The effective available range for symmetric allocation is determined by channel bandwidth (as shown) as well as link distance. In this context, “link” is any collocated RADWIN HBS.

QoS Configuration (HBS side)

QoS (Quality of Service) is a technique for prioritization of network traffic packets during congestion.

The RADWIN 5000 sectors support two classification criteria: 802.1p priority (referred to as "VLAN" for simplicity) or Diffserv based. You may choose which of them to use. To work with them properly, you must be familiar with the use of VLAN (802.1p) or Diffserv.

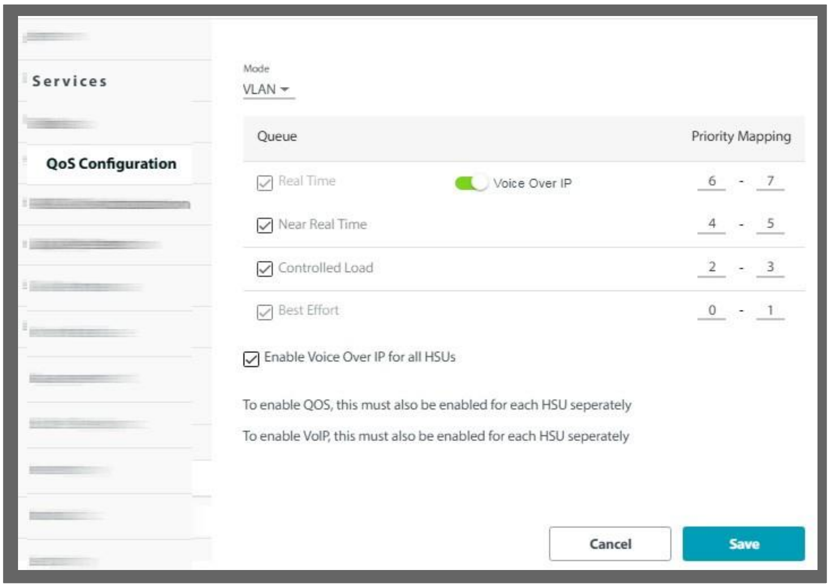
This section describes how to configure QoS for the HBS for the whole sector. However, to fully configure QoS properly, you must also configure it for each SU in turn.

Based upon the classification criterion chosen, received packets will be mapped into one of four quality groups: real time, near real time, controlled load or best effort. You may partition the total link capacity across the four quality queues. The default weights as percentages are shown in the table below:

Quality queue	Priority	
	Diffserv	VLAN
Real time	48-63	6-7
Near real time (responsive applications)	32-47	4-5
Controlled load	16-31	2-3
Best effort	0-15	0-1

You can also define part of the link capacity as carrying Voice-over-IP traffic. This is similar to defining part of it as real time.

1. From the Mode pull-down menu, choose either the VLAN or Diffserv method.
2. For the method you selected, type the Priority Mapping for each queue. This determines the translation of the priority mapping of the traffic to what is used by the HBS. Default settings for Diffserv and VLAN are as shown in the next two figures:



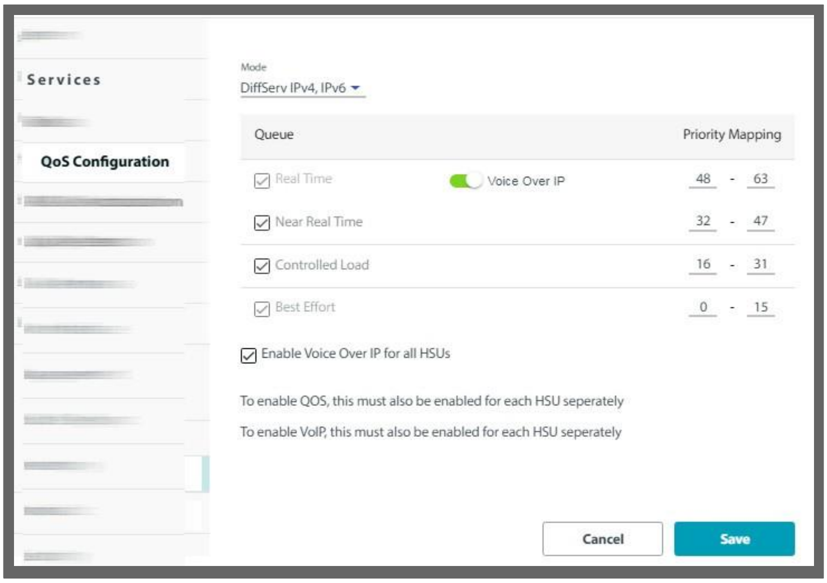
Mode: VLAN

Queue		Priority Mapping
☑ Real Time	Voice Over IP	6 - 7
☑ Near Real Time		4 - 5
☑ Controlled Load		2 - 3
☑ Best Effort		0 - 1

☑ Enable Voice Over IP for all HSUs

To enable QOS, this must also be enabled for each HSU seperately

To enable VoIP, this must also be enabled for each HSU seperately



Mode
DiffServ IPv4, IPv6

Queue		Priority Mapping
☑ Real Time	Voice Over IP	48 - 63
☑ Near Real Time		32 - 47
☑ Controlled Load		16 - 31
☑ Best Effort		0 - 15

☑ Enable Voice Over IP for all HSUs

To enable QOS, this must also be enabled for each HSU seperately

To enable VoIP, this must also be enabled for each HSU seperately

3. If you un-check a queue, the queue will be ignored for the sector. It will not prevent the HSU from configuring traffic labeled with this priority level as “live”; it will merely ignore its priority level, as if the traffic was not assigned with any priority level whatsoever. You cannot un-check the Best Effort queue.

Note the following:

- You can enable QoS from either the HBS or the SU. If enabled from the SU, it is done for that SU only, and its HBS. If done from the HBS, it is done sector-wide.
- If QoS is enabled from the HBS, it is applied to all SUs presently connected to the sector. For SUs connected to the sector after QoS was defined, do one of the following:
  - Enable QoS on those individual SUs (this is the intention of the note “To enable QoS, this must also be enabled for each HSU separately”), or
  - Re-enable it for the whole sector from the HBS.

<u>Enabling a VoiP Queue (HBS side)</u>

Note the following:

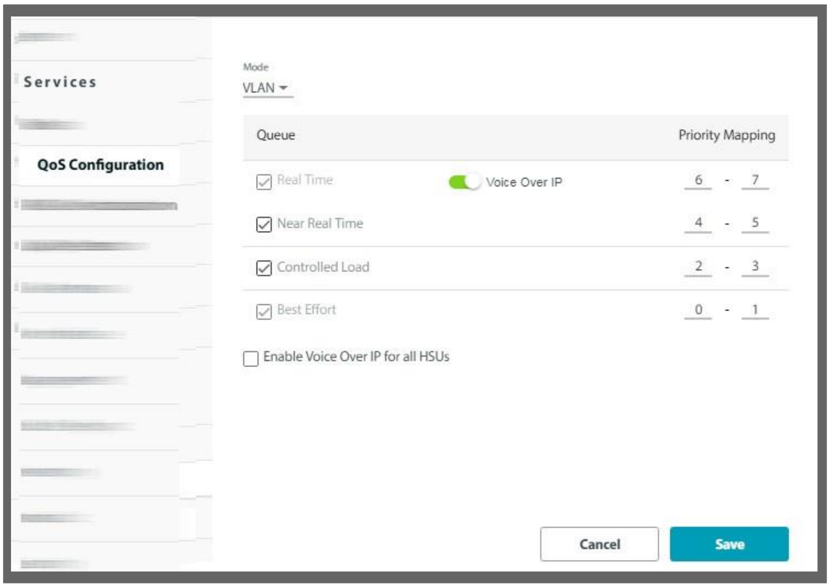
- You can enable a VoIP queue from either the HBS or the SU. If enabled from the SU, it is done for that SU only and its HBS. If done from the HBS, it can be done sector-wide. To enable a VoIP queue from the HBS, select **Enable Voice Over IP for all HSUs** .
- If a VoIP queue is enabled from the HBS, it is applied to all SUs presently connected to the sector. For SUs connected to the sector after the VoIP queue was defined, do one of the following:
  - Enable VoIP on those individual SUs (this is the intention of the note “To enable VoIP, this must also be enabled for each HSU separately”), or
  - Re-enable it for the whole sector from the HBS.
- The VoIP feature - as implemented here - assumes that your end-user has a gateway or other network device that defines the traffic to be VoIP with the correct QoS defined (VLAN or DiffServ, in accordance with your configuration done here). The definition must be done at both ends of the data stream.

- Enabling a VoIP queue may decrease the sector’s peak throughput in some scenarios. Therefore, make sure that you absolutely need to enable a VoIP queue before doing so.

1. Click Voice Over IP. The Real Time queue will become disabled. This means that VoIP traffic is treated in a similar fashion to Real Time traffic. VoIP works whether you are using VLAN or DiffServ.
2. Optionally, apply VoIP to all of the SUs in the sector by clicking on Enable Voice Over IP for all HSUs.
   - If you do not choose this, you must go to each SU for which you want to enable a VoIP queue and enable it there.
3. Click **Save** to have your changes take effect.

Note

Make sure the “Mode” selected is the proper one, is consistent throughout your configuration, and that your end-user has equipment that also defines its VoIP traffic with the Mode you defined here.



Mode: VLAN

Queue		Priority Mapping
☑ Real Time	● Voice Over IP	6 - 7
☑ Near Real Time		4 - 5
☑ Controlled Load		2 - 3
☑ Best Effort		0 - 1

□ Enable Voice Over IP for all HSUs

RADIUS Authorization

This option enables the HBS to validate and authorize SU service based on information in a RADIUS server. You can also set a RADIUS server for accounting. You define service categories based on parameters set here.

Operation

This option works as follows:

- SU definition and assignment information is saved in the authorization RADIUS server.
- 32 Service categories are defined in the HBS.
- The HBS queries the authorization RADIUS server on each synchronization of a new SU and periodically for active SUs. Server replay if the SU is authorized and provides the SU’s definition, service category and assignment information
- The HBS then applies this information to each SU.
- The results of this assignment process are then sent to the accounting RADIUS server.

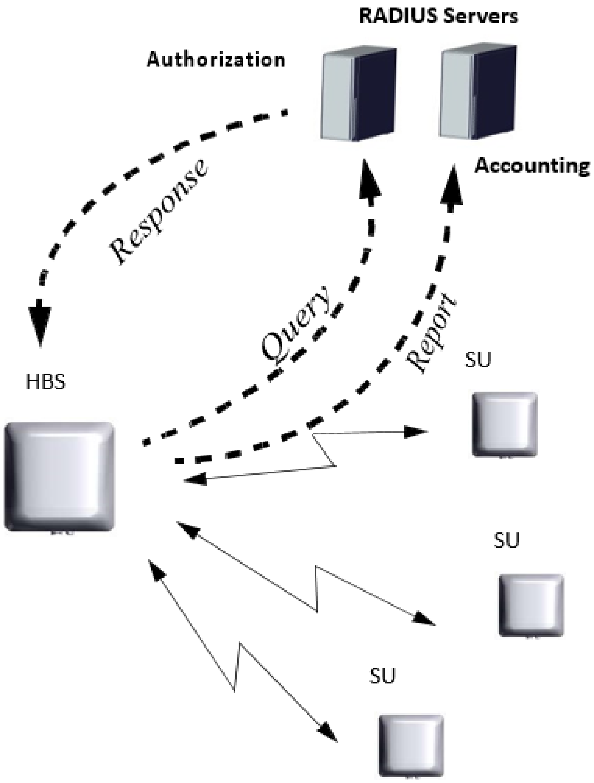


Figure 2-3: Service Validation and Authorization via a RADIUS Server

To change SU definitions and assignments, update the information in the authorization RADIUS server. You do not need to access the HBS at all to make this change, as the HBS automatically queries the authorization RADIUS server periodically for status updates.

Customer Preparations

1. You must supply servers that operate the RADIUS protocol. Both authorization and accounting RADIUS servers can be the same device.

2. The HBS functions as a radius client. Prepare the following parameters for both RADIUS servers:

- The IP address of the RADIUS server.
- The port of the RADIUS server to which the HBS must connect.
- The Secret of the RADIUS server.
- A username and password. The HBS uses the username and password in the access request query that it sends to the radius server for each SU.

3. Prepare the following configuration information for each SU in your sector. This information will be saved in the users list of the authorization RADIUS server:

- Serial number (acquired from your vendor)
- Name
- Location
- VLAN identifier (If relevant - if the HBS and SU are 5.1.30 or above, set the value to zero as the VLAN configuration is part of the VLAN Traffic attributes in release 5.1.30 and above)
- Register Availability (whether or not to register this specific SU)
- Desired service category

In version 5.1.30 and above, in addition to the above parameters, more parameters were supported, including:

- Management IP (3 parameters)
- Traffic VLAN
  - Traffic VLAN: VLAN mode
  - Provider parameters: VLAN ID, VLAN priority, TPID
  - Tag parameters: Ingress mode, VLAN ID, priority, Egress mode, Allowed VLAN IDs (X4), Un-tag VLAN ID(X4)
- NTP server (IP and offset)
- Syslog
- Contact info
- Trap destination addresses (support 3 addresses)

Users can fill just part of the parameters above. The mandatory parameters shall be the key parameter used for identifying the user.

4. In version 5.1.30 and above, an optional SU identification key parameter has been added. SUs can be identified by one of the following keys:

- S/N
- MAC Address
- Customer/Work Order ID (a string, limited to 32 characters)

Select one of the below identification keys on the HBS. This identification key shall be included as the first parameter on each SU configuration in the radius server's users file.

5. Prepare the service category definitions that you will set for use in the authorization RADIUS server. Up to 32 categories can be defined; each category sets the following parameters:

- Uplink Resources
- Downlink Resources
- Resource Type (CIR or Best Effort)
- Maximum Information Rate (MIR) Up (sector-wide)
- Maximum Information Rate (MIR) Down (sector-wide)
- Protocol filtering
  Select the protocol filtering desired, if any. However, be careful to make sure there are no contradictions in the definitions of the protocol filtering versus the definitions of DHCP 82 enablement. Protocol filtering cannot be implemented at all with 802.1x authentication.
- QoS Configuration queues (for uplink and again for downlink):
  - Real Time (and its Strict Weight percentage, MIR and TTL (Time-to-Live)
  - Near Real-Time
  - Controlled Load
  - Best Effort
- VoIP queue, if applicable

Prepare Files for the RADIUS Servers

Prepare 3 files for the authorization RADIUS server: Data Dictionary supplement, Clients and Users definitions. The accounting RADIUS server only needs the Data Dictionary supplement. The examples below refer to freeradius.net server.

- **Data Dictionary supplement:**

  This is a supplement to the standard RADIUS Data Dictionary. This file defines the attributes that are used by the RADIUS server as configuration parameters for the SUs. Add this text to the end of the standard RADIUS Data Dictionary. An example supplement looks as follows:

```
#  dictionary.radwin
#
#vendor id
VENDOR             Radwin                     4458

BEGIN-VENDOR Radwin
#Service category for translate between the number and its name
ATTRIBUTE   RADWIN_ServiceCategory                   1             integer
VALUE       RADWIN_ServiceCategory                   Residential1         1
VALUE       RADWIN_ServiceCategory                   Residential2         2
VALUE       RADWIN_ServiceCategory                   Residential3         3
VALUE       RADWIN_ServiceCategory                   Residential4         4
VALUE       RADWIN_ServiceCategory                   Business1                  5
VALUE       RADWIN_ServiceCategory                   Business2                  6
VALUE       RADWIN_ServiceCategory                   Business3                  7
VALUE       RADWIN_ServiceCategory                   Business4                  8

#for cpe's serial number to check
ATTRIBUTE   RADWIN_SerialNumber        2      string

#cpe name return from Radius server
ATTRIBUTE   RADWIN_Name                       3      string

#cpe location return from Radius server
ATTRIBUTE   RADWIN_Location                   4      string

#cpe vlan id return from Radius server
ATTRIBUTE   RADWIN_Vlan                       5      integer

#is the cpe enable or disabled , if enable register or update id necessary otherwise
deregister if necessary
ATTRIBUTE   RADWIN_RegisterAvailability                     6      integer

ATTRIBUTE   RADWIN_AccountingConnectivityCheck                            21    string

VALUE RADWIN_RegisterAvailability             Disable              0
VALUE RADWIN_RegisterAvailability             Enable       1

#####################################################################
#New provisioning for Radius Authorization from release 5.1.30 ######
#####################################################################

#Mac Address:
ATTRIBUTE RADWIN_MacAddress 22 string

#Identification Key:
ATTRIBUTE RADWIN_IdentificationKeyId 23 string

#Management IP:
ATTRIBUTE RADWIN_ManagementIP 24 string
ATTRIBUTE RADWIN_ManagementSubnetMask 25 string
ATTRIBUTE RADWIN_ManagementDefaultGateway 26 string

#NTP server:
ATTRIBUTE RADWIN_NTPServer 27 string
ATTRIBUTE RADWIN_NTPOffset 28 integer

#Syslog:
ATTRIBUTE RADWIN_SyslogServerIP 29 string
```

```
#Trap destination addresses:

#First address:
ATTRIBUTE RADWIN_TrapIP_1 30 string
ATTRIBUTE RADWIN_TrapPort_1 31 integer
ATTRIBUTE RADWIN_TrapSecurityMode_1 32 integer
VALUE RADWIN_TrapSecurityMode_1 SNMP_V1 1
VALUE RADWIN_TrapSecurityMode_1 SNMP_V3 3
ATTRIBUTE RADWIN_TrapV3_userName_1 33 string
ATTRIBUTE RADWIN_TrapV3_userPassword_1 34 string

#Second address:
ATTRIBUTE RADWIN_TrapIP_2 35 string
ATTRIBUTE RADWIN_TrapPort_2 36 integer
ATTRIBUTE RADWIN_TrapSecurityMode_2 37 integer
VALUE RADWIN_TrapSecurityMode_2 SNMP_V1 1
VALUE RADWIN_TrapSecurityMode_2 SNMP_V3 3
ATTRIBUTE RADWIN_TrapV3_userName_2 38 string
ATTRIBUTE RADWIN_TrapV3_userPassword_2 39 string

#Third address:
ATTRIBUTE RADWIN_TrapIP_3 40 string
ATTRIBUTE RADWIN_TrapPort_3 41 integer
ATTRIBUTE RADWIN_TrapSecurityMode_3 42 integer
VALUE RADWIN_TrapSecurityMode_3 SNMP_V1 1
VALUE RADWIN_TrapSecurityMode_3 SNMP_V3 3
ATTRIBUTE RADWIN_TrapV3_userName_3 43 string
ATTRIBUTE RADWIN_TrapV3_userPassword_3 44 string

#Contact info:
ATTRIBUTE RADWIN_ContactInfo 45 string

#Traffic VLAN:
#on\off:
ATTRIBUTE RADWIN_TrafficVlan 46 integer
VALUE RADWIN_TrafficVlan Off 0
VALUE RADWIN_TrafficVlan On 1

#provider\tag:
ATTRIBUTE RADWIN_TrafficVlanType 47 integer
VALUE RADWIN_TrafficVlanType Provider 0
VALUE RADWIN_TrafficVlanType Tag 1

#provider:
ATTRIBUTE RADWIN_TrafficVlanProviderID 48 integer
ATTRIBUTE RADWIN_TrafficVlanProviderPriority 49 integer
ATTRIBUTE RADWIN_TrafficVlanProviderTPID 50 integer


ATTRIBUTE RADWIN_TVPPriority 49 integer
ATTRIBUTE RADWIN_TVPTPID 50 integer

VALUE RADWIN_TVPTPID 9100 0
VALUE RADWIN_TVPTPID 8100 1
VALUE RADWIN_TVPTPID 88A8 2

#tag:
#SU ingress Traffic:
#TVTI = Traffic Vlan Tag Ingress
ATTRIBUTE RADWIN_TVTITraffic 51 integer

#SU ingress Traffic:
#Transparent:
VALUE RADWIN_TVTITraffic Transparent 0
#Tag:
VALUE RADWIN_TVTITraffic Tag 1
```

```
#TVTI = Traffic Vlan Tag Ingress
ATTRIBUTE   RADWIN_TVTITraffic                  51 integer
ATTRIBUTE   RADWIN_TVTITrafficTagId      52 integer
ATTRIBUTE   RADWIN_TVTITrafficTagPriority 53 integer

#SU Egress Traffic:
#TVTET = Traffic Vlan Tag Egress Traffic
ATTRIBUTE RADWIN_TVTET 54 integer
VALUE RADWIN_TVTET Transparent 0
VALUE RADWIN_TVTET UntagAll 1
VALUE RADWIN_TVTET Filter 2
VALUE RADWIN_TVTET UntagFiltered 3

#SU Egress Traffic:
#Filter:
#TVTETF = Traffic Vlan Tag Egress Traffic Filter
ATTRIBUTE RADWIN_TVTETF_allowedVlanId_1 55 integer
ATTRIBUTE RADWIN_TVTETF_allowedVlanId_2 56 integer
ATTRIBUTE RADWIN_TVTETF_allowedVlanId_3 57 integer
ATTRIBUTE RADWIN_TVTETF_allowedVlanId_4 58 integer

#SU Egress Traffic:
#Untag Filtered:
#option 1:
#TVTETUF = Traffic Vlan Tag Egress Traffic Untag Filtered
#ATTRIBUTE RADWIN_TVTETUF_allowedVlanId_1 59 integer
#ATTRIBUTE RADWIN_TVTETUF_allowedVlanId_Untag_1 60 integer
#VALUE RADWIN_TVTETUF_allowedVlanId_Untag_1 Disabled 0
#VALUE RADWIN_TVTETUF_allowedVlanId_Untag_1 Enabled 1

#SU Egress Traffic:
#Untag Filtered:
#option 2:
#ATTRIBUTE RADWIN_TVTETUF_allowedVlanId_2 61 integer
#ATTRIBUTE RADWIN_TVTETUF_allowedVlanId_Untag_2 62 integer
#VALUE RADWIN_TVTETUF_allowedVlanId_Untag_2 Disabled 0
#VALUE RADWIN_TVTETUF_allowedVlanId_Untag_2 Enabled 1

#SU Egress Traffic:
#Untag Filtered:
#option 3:
#ATTRIBUTE RADWIN_TVTETUF_allowedVlanId_3 63 integer
#ATTRIBUTE RADWIN_TVTETUF_allowedVlanId_Untag_3 64 integer
#VALUE RADWIN_TVTETUF_allowedVlanId_Untag_3 Disabled 0
#VALUE RADWIN_TVTETUF_allowedVlanId_Untag_3 Enabled 1

#SU Egress Traffic:
#Untag Filtered:
#option 4:
#ATTRIBUTE RADWIN_TVTETUF_allowedVlanId_4 65 integer
#ATTRIBUTE RADWIN_TVTETUF_allowedVlanId_Untag_4 66 integer
#VALUE RADWIN_TVTETUF_allowedVlanId_Untag_4 Disabled 0
#VALUE RADWIN_TVTETUF_allowedVlanId_Untag_4 Enabled 1


# TVTETUF = Traffic Vlan Tag Egress Traffic Untag Filtered
# U = Untag
ATTRIBUTE   RADWIN_TVTETUF_allowedVlanId1     59 integer
ATTRIBUTE   RADWIN_TVTETUF_allowedVlanId_U1   60 integer
ATTRIBUTE   RADWIN_TVTETUF_allowedVlanId2     61 integer
ATTRIBUTE   RADWIN_TVTETUF_allowedVlanId_U2   62 integer
ATTRIBUTE   RADWIN_TVTETUF_allowedVlanId3     63 integer
ATTRIBUTE   RADWIN_TVTETUF_allowedVlanId_U3   64 integer
ATTRIBUTE   RADWIN_TVTETUF_allowedVlanId4     65 integer
ATTRIBUTE   RADWIN_TVTETUF_allowedVlanId_U4   66 integer
```

```
 # TVTETUF = Traffic Vlan Tag Egress Traffic Untag Filtered
 # U = Untag
 VALUE       RADWIN_TVTETUF_allowedVlanId_U1   Disabled            0
 VALUE       RADWIN_TVTETUF_allowedVlanId_U1   Enabled             1
 VALUE       RADWIN_TVTETUF_allowedVlanId_U2   Disabled            0
 VALUE       RADWIN_TVTETUF_allowedVlanId_U2   Enabled             1
 VALUE       RADWIN_TVTETUF_allowedVlanId_U3   Disabled            0
 VALUE       RADWIN_TVTETUF_allowedVlanId_U3   Enabled             1
 VALUE       RADWIN_TVTETUF_allowedVlanId_U4   Disabled            0
 VALUE       RADWIN_TVTETUF_allowedVlanId_U4   Enabled             1

 #######################################################################


 # User Permissions Profile, the attribute starts with “number”=10 in order not to
 # collide with previous RADWIN RADIUS definitions for HSU Authorization
 ATTRIBUTE RADWIN_UserProfile 10 integer

 # Old profiles for Authentication in Telnet in GEN3 Release 4.2.84:
 VALUE       RADWIN_UserProfile ReadOnlyHbsReadOnlyHsu    1
 VALUE       RADWIN_UserProfile ReadWriteHbsReadWriteHsu  2
 VALUE       RADWIN_UserProfile ReadOnlyHbsReadWriteHsu   3


 # New profiles for Authentication in SNMPv3 from Release 4.9.75:
 VALUE RADWIN_UserProfile ObserverHbsObserverHsu 1
 VALUE RADWIN_UserProfile AdminHbsAdminHsu 4
 VALUE RADWIN_UserProfile InstallerHbsInstallerHsu 5
 VALUE RADWIN_UserProfile OperatorHbsOperatorHsu 6
 VALUE RADWIN_UserProfile OperatorHbsInstallerHsu 7
 VALUE RADWIN_UserProfile ObserverHbsOperatorHsu 8

 #ObserverHbsObserverHsu is identical to ReadOnlyHbsReadOnlyHsu

 ATTRIBUTE RADWIN_SessionTimeout 11 integer

END-VENDOR    Radwin
```

The above example shows that the first attribute is in the Service Category. Following that definition is a list of the Service Categories. In this case, ServiceCategory 1 is called “Residential1”, ServiceCategory 2 is called “Residential2”, etc. These terms must be used precisely - as shown here - when you set the service categories. In the dictionary above, 8 service categories are listed, however, there are 32 service categories.

A line with the # character above the attributes provides a short description about the attributes or a group of attributes.

» **Users definitions (for authorization RADIUS server only)**

The Users file (users.conf) defines the list of SUs for this sector. Each SU serial number is listed. Save this file in the same location as the Data Dictionary file.

Note

Although the Users file has the definitions of the SUs, it does not determine which SU belongs to which HBS. The HBS tried to connect with any available SUs.

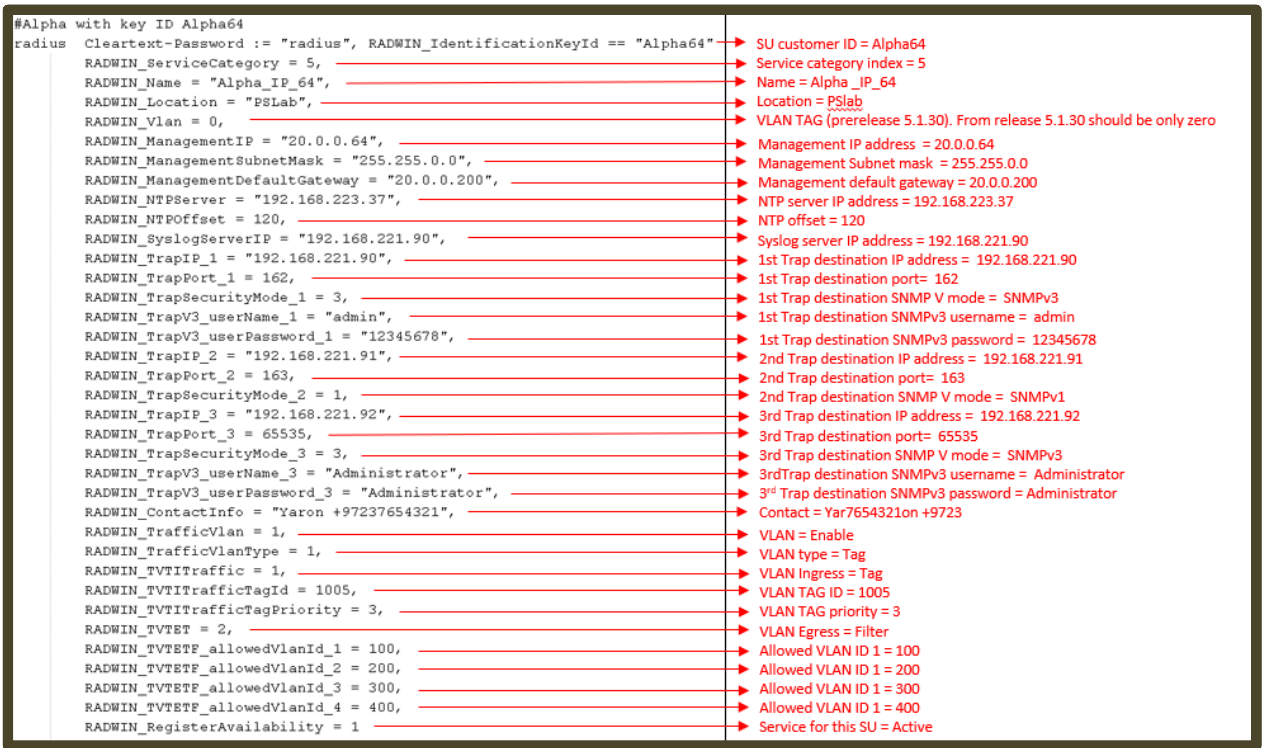
An example of a Users file appears as follows.

```
#### SETUP 10.112.5.200 - Jig4x ####

radiusCleartext-Password  := "radius", RADWIN_SerialNumber  == "VERIFI2X5KLXY444"
          RADWIN_ServiceCategory = 1,
          RADWIN_Name = "Name4.4",
          RADWIN_Location = "Loc4.4",
          RADWIN_Vlan = 44,
          RADWIN_RegisterAvailability  = 1

radiusCleartext-Password  := "radius", RADWIN_SerialNumber  == "VERIF2X5KLXY2221"
          RADWIN_ServiceCategory = 2,
          RADWIN_Name = "Name4.3",
          RADWIN_Location = "Loc4.3",
          RADWIN_Vlan = 33,
          RADWIN_RegisterAvailability  = 1
```

The above example refers to release < 5.1.30:

The first SU has a serial number of VERIFI2X5KLXY444. This is a unique S/N number for this specific SU. In release <5.1.30, the S/N is the only identification key option. This unit has a ServiceCategory of “1”, which translates into “Residential1” according to the Data Dictionary above. Its name is “Name4.4”, and Location is “Loc4.4” and will appear as such in the WebUI. It has a date VLAN ID 44 , and the registration and service for this SU is approved and active.

The second SU has a serial number of VERIFI2X5KLXY2221, a ServiceCategory of “2”, which translates into “Residential2”, its name is “Name4.3”, and Location is “Loc4.3”, it has a data VLAN ID 33 and the registration and service for this SU is approved and active.



```
#Alpha with key ID Alpha64
radius  Cleartext-Password := "radius", RADWIN_IdentificationKeyId == "Alpha64"
        RADWIN_ServiceCategory = 5,
        RADWIN_Name = "Alpha_IP_64",
        RADWIN_Location = "PSLab",
        RADWIN_Vlan = 0,
        RADWIN_ManagementIP = "20.0.0.64",
        RADWIN_ManagementSubnetMask = "255.255.0.0",
        RADWIN_ManagementDefaultGateway = "20.0.0.200",
        RADWIN_NTPServer = "192.168.223.37",
        RADWIN_NTPOffset = 120,
        RADWIN_SyslogServerIP = "192.168.221.90",
        RADWIN_TrapIP_1 = "192.168.221.90",
        RADWIN_TrapPort_1 = 162,
        RADWIN_TrapSecurityMode_1 = 3,
        RADWIN_TrapV3_userName_1 = "admin",
        RADWIN_TrapV3_userPassword_1 = "12345678",
        RADWIN_TrapIP_2 = "192.168.221.91",
        RADWIN_TrapPort_2 = 163,
        RADWIN_TrapSecurityMode_2 = 1,
        RADWIN_TrapIP_3 = "192.168.221.92",
        RADWIN_TrapPort_3 = 65535,
        RADWIN_TrapSecurityMode_3 = 3,
        RADWIN_TrapV3_userName_3 = "Administrator",
        RADWIN_TrapV3_userPassword_3 = "Administrator",
        RADWIN_ContactInfo = "Yaron +97237654321",
        RADWIN_TrafficVlan = 1,
        RADWIN_TrafficVlanType = 1,
        RADWIN_TVTITraffic = 1,
        RADWIN_TVTITrafficTagId = 1005,
        RADWIN_TVTITrafficTagPriority = 3,
        RADWIN_TVTET = 2,
        RADWIN_TVTETF_allowedVlanId_1 = 100,
        RADWIN_TVTETF_allowedVlanId_2 = 200,
        RADWIN_TVTETF_allowedVlanId_3 = 300,
        RADWIN_TVTETF_allowedVlanId_4 = 400,
        RADWIN_RegisterAvailability = 1
```

SU customer ID = Alpha64
Service category index = 5
Name = Alpha _IP_64
Location = PSlab
VLAN TAG (prerelease 5.1.30). From release 5.1.30 should be only zero
Management IP address = 20.0.0.64
Management Subnet mask = 255.255.0.0
Management default gateway = 20.0.0.200
NTP server IP address = 192.168.223.37
NTP offset = 120
Syslog server IP address = 192.168.221.90
1st Trap destination IP address = 192.168.221.90
1st Trap destination port= 162
1st Trap destination SNMP V mode = SNMPv3
1st Trap destination SNMPv3 username = admin
1st Trap destination SNMPv3 password = 12345678
2nd Trap destination IP address = 192.168.221.91
2nd Trap destination port= 163
2nd Trap destination SNMP V mode = SNMPv1
3rd Trap destination IP address = 192.168.221.92
3rd Trap destination port= 65535
3rd Trap destination SNMP V mode = SNMPv3
3rdTrap destination SNMPv3 username = Administrator
3rd Trap destination SNMPv3 password = Administrator
Contact = Yar7654321on +9723
VLAN = Enable
VLAN type = Tag
VLAN Ingress = Tag
VLAN TAG ID = 1005
VLAN TAG priority = 3
VLAN Egress = Filter
Allowed VLAN ID 1 = 100
Allowed VLAN ID 1 = 200
Allowed VLAN ID 1 = 300
Allowed VLAN ID 1 = 400
Service for this SU = Active

The above example refers to release 5.1.30 and above.

The explanation for each attribute is written in red.
In this example, the SU identification key type is Customer ID. The username **radius** and password **radius** as configured in the HBS (server access setting).

SU identification key can be also by its MAC address or S/N.
Example 1 – SU identification key is the SU’s Mac Address

```
#radius Cleartext-Password := "radius", RADWIN_MacAddress == "00:15:67:f6:a6:b1"
```

Example 2 – SU identification key is the SU’s S/N

```
#radius  Cleartext-Password := "radius", RADWIN_SerialNumber == "P14930I200300168"
```

Note

If you add SUs to the sector, make sure you update the Users file on the RADIUS server, otherwise the HBS will not register them, and you will see an error message.

» Clients definitions (RADIUS server)

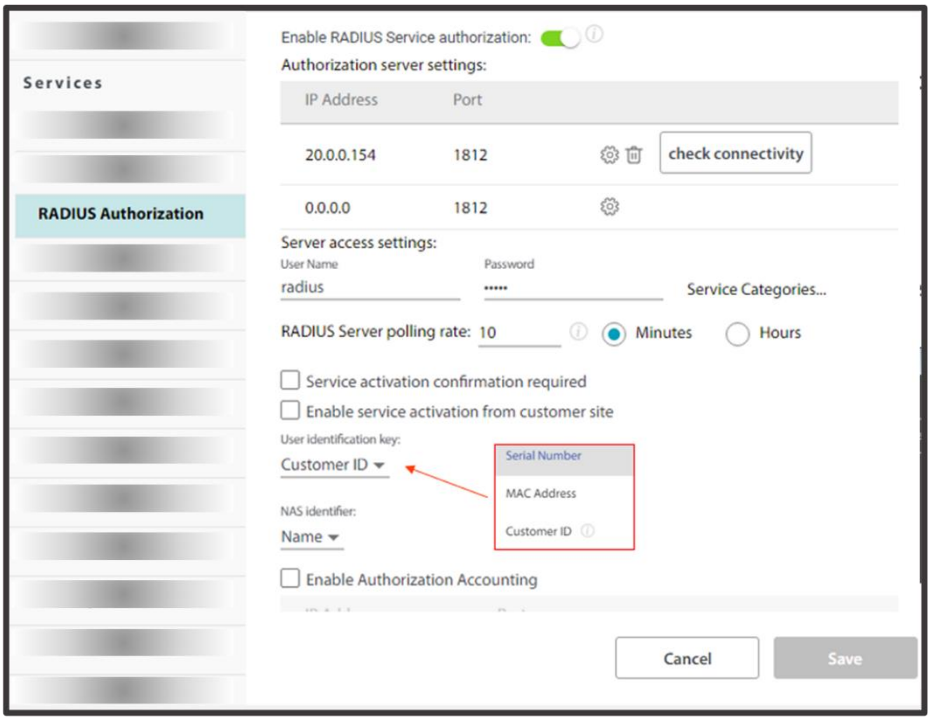
Each HBS is a radius client and should be defined as a client in the radius server. Set the IP address and secret key for each HBS in the radius client file (clients.conf).

```
client 20.0.0.130/24 {
 secret              = radius
 shortname       = Radwin-MSector
}
```

In the example above, the IP address of the HBS is 20.0.0.130, the secret password is radius. The short name is a description of the HBS just for information. /24 defines a list of HBS clients in the subnet 20.0.0.130/24.

Configuring the RADIUS Authorization option

Select the HBS, click the Configure icon (Configure), then from the **Services** option, select **RADIUS Authorization**.



Services
RADIUS Authorization

Enable RADIUS Service authorization: ●
Authorization server settings:

IP Address	Port
20.0.0.154	1812
0.0.0.0	1812

Server access settings:
User Name: radius
Password: •••••

RADIUS Server polling rate: 10 ● Minutes ○ Hours

□ Service activation confirmation required
□ Enable service activation from customer site

User identification key: Customer ID

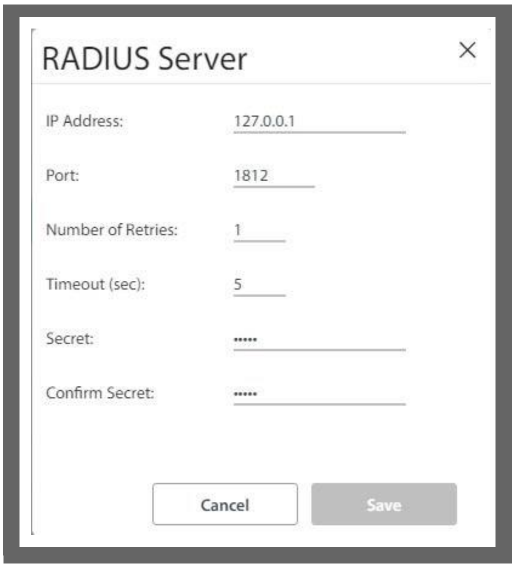
NAS identifier: Name

□ Enable Authorization Accounting

To enable the RADIUS authorization mode, check **Enable RADIUS Service authorization**.

Authorization server settings: This shows a list of the available RADIUS servers, their IP addresses, their connection Ports (this is usually 1812), and their Statuses (Check Connectivity, Testing, or Connected), in addition to a configuration button and trash button.

Click the configuration button (⚙) to open the RADIUS server parameters dialog box.



RADIUS Server

IP Address: 127.0.0.1

Port: 1812

Number of Retries: 1

Timeout (sec): 5

Secret: •••••

Confirm Secret: •••••

IP Address: Enter the IP Address of the RADIUS server here

Port: Enter the communication port to which the HBS connects (usually 1812)

Note

Although you can use the same IP for the different functions of the RADIUS server, you must still use a different port for each function.

Number of Retries: If the first attempt at establishing a connection with the RADIUS server was unsuccessful, carry out this number of retries before moving on to the next available RADIUS server.

Timeout: If there is no response from the RADIUS server after this many seconds, disconnect. A message will appear indicating this situation.

Secret: Secret password of the RADIUS server.

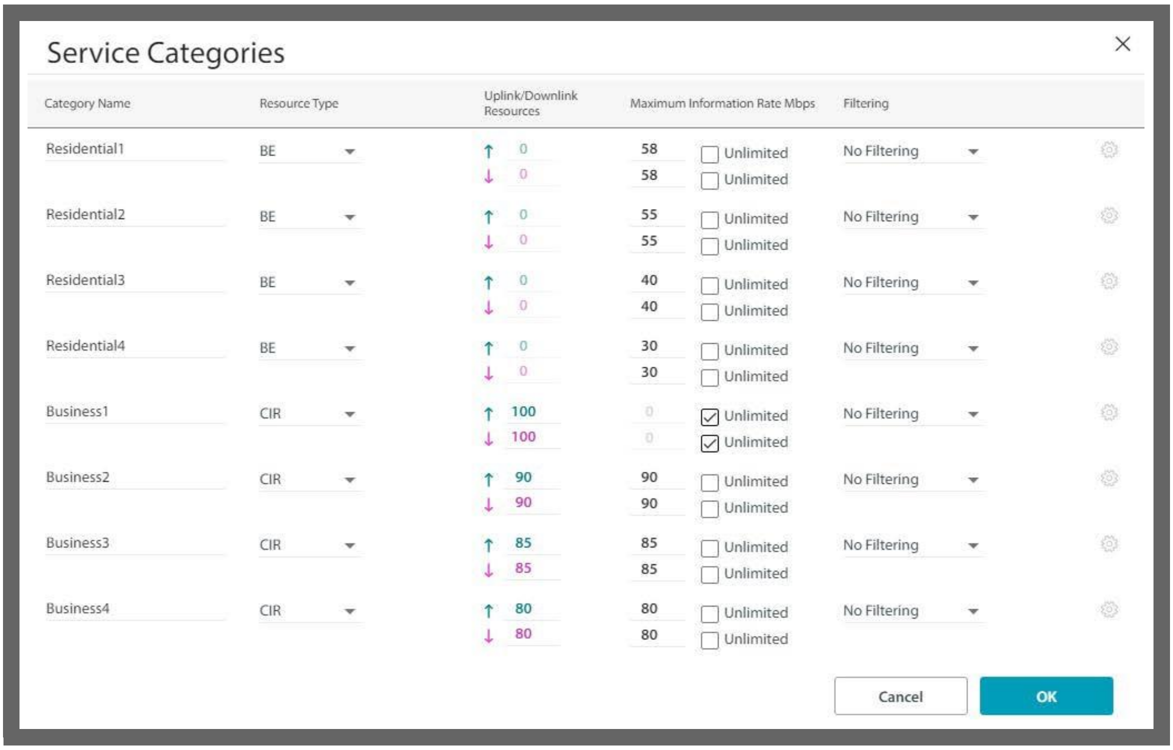
Click **Save** to have your changes take effect.

Check Connectivity: This button will appear once you enter the connectivity parameters of the RADIUS server. Click this button to test the connectivity of the specific RADIUS server. Its status will change to Testing, and if the connection is successful, a “Connectivity test success” message will appear. The connectivity test must be successful for this RADIUS feature to work.

Server Access Settings: Enter the username and password that the RADIUS servers use to identify and verify the SU (user) credential. These are the users (SU) credential that the HBS sends in the access request query to the radius server for each SU.

Service Categories:

Click this button to open the dialog box where you define the Service Categories.



Service Categories

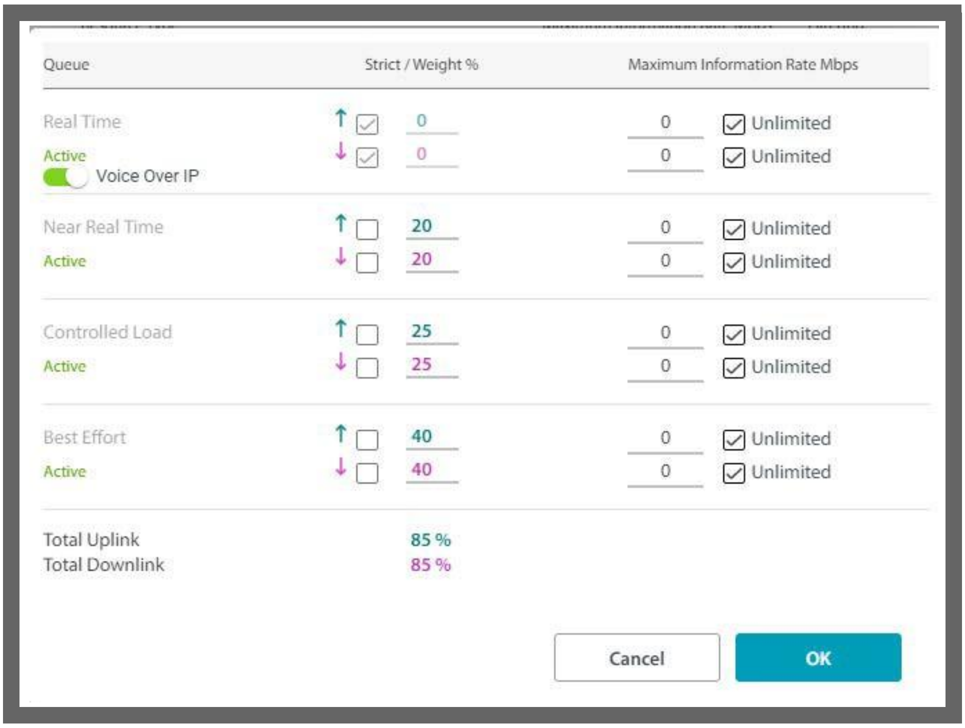
Category Name	Resource Type	Uplink/Downlink Resources	Maximum Information Rate Mbps		Filtering
Residential1	BE	↑ 0 ↓ 0	58 58	□ Unlimited □ Unlimited	No Filtering
Residential2	BE	↑ 0 ↓ 0	55 55	□ Unlimited □ Unlimited	No Filtering
Residential3	BE	↑ 0 ↓ 0	40 40	□ Unlimited □ Unlimited	No Filtering
Residential4	BE	↑ 0 ↓ 0	30 30	□ Unlimited □ Unlimited	No Filtering
Business1	CIR	↑ 100 ↓ 100	0 0	☑ Unlimited ☑ Unlimited	No Filtering
Business2	CIR	↑ 90 ↓ 90	90 90	□ Unlimited □ Unlimited	No Filtering
Business3	CIR	↑ 85 ↓ 85	85 85	□ Unlimited □ Unlimited	No Filtering
Business4	CIR	↑ 80 ↓ 80	80 80	□ Unlimited □ Unlimited	No Filtering

Figure 2-4: Service Categories

Category Name: The names of the categories here should be the same names as those in the Data Dictionary supplement.

Define the other parameters according to the values that are required for this service category and click OK.

The QoS Configuration queues are accessed by clicking the configuration button (⚙) from the Service Categories dialog box. The following screen appears:



Queue		Strict / Weight %		Maximum Information Rate Mbps	
Real Time	↑	☑	0	0	☑ Unlimited
Active	↓	☑	0	0	☑ Unlimited
Voice Over IP					
Near Real Time	↑	□	20	0	☑ Unlimited
Active	↓	□	20	0	☑ Unlimited
Controlled Load	↑	□	25	0	☑ Unlimited
Active	↓	□	25	0	☑ Unlimited
Best Effort	↑	□	40	0	☑ Unlimited
Active	↓	□	40	0	☑ Unlimited
Total Uplink			85 %		
Total Downlink			85 %		

Set the various Quality of Service parameters (including VoIP, if needed), and click OK.

Caution

The SUs receive their service characteristics in accordance with the definition of the Service Category (here) and the Service Category to which they were assigned based on the files in the authorization RADIUS server. In the radius server, only the service category index number (1–32) is set for the SU. The HBS is assigned to service category parameters according to the service category index it gets from the server.
However, if you manually change any of these parameters (via Services -> QoS Configuration or Service -> QoS Configuration from the SU's menu), the new values you have set will remain, even though they do not correspond to those in any defined Service Category in the RADIUS server.

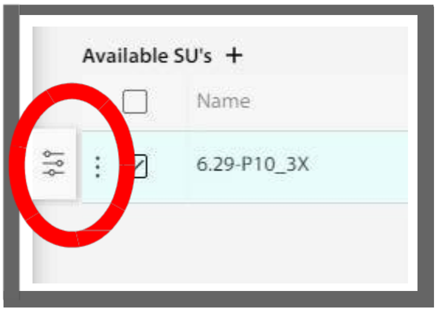
If you change the assigned Service Category of such an SU using the files in the authorization RADIUS server, then the next time the HBS receives updated information from the authorization RADIUS server, it will change these parameters to correspond to those of the new Service Category as set in the RADIUS server.
Name and Location parameter values also do not change even if they changed in the radius server. It only deregister the SU and resync update them.

Radius server polling rate: The time in minutes or hours that the HBS periodically sends an access request query to the radius server to check the status and the information for each SU. If there is any change in the status or the configuration, the HBS updates the SU accordingly. To disable the periodical query to the radius server, set the value to zero.

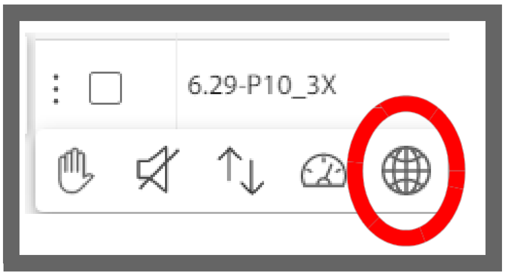
Service Activation Confirmation Required: When this feature is enabled, then the HBS send access requests to each SU manually. If this is not enabled, the HBS can register the SUs in its sector via the radius server without further action.
Note - When using WINTouch+ for the SU alignment, this feature must be enabled. Otherwise, the SU will immediately register to the HBS before the alignment is completed.

This option is useful if, for instance, a technician is installing an SU, and it is not quite ready to be activated.
To confirm the installation from the SU side, do the following:

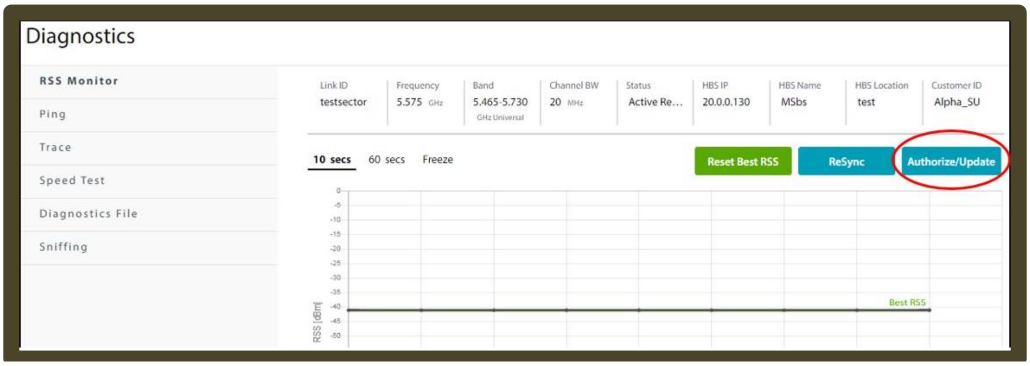
From the main window of the WebUI, click on the three vertical dots next to the SU for which you want to confirm the service activation.



Then click on the Authorize / Update icon (looks like a globe):



Enable service activation from customer site: When this feature is enabled, then the user can locally access the web interface of the SU and remotely ask the HBS to send access request to server. When this feature is enabled, an "Authorize / Update" button appears under the Diagnostic-> RSS monitor menu in the SU web interface. When using WINTouch+ for SU alignment, it also enables the user to send access requests to the server.



Link ID	Frequency	Band	Channel BW	Status	HBS IP	HBS Name	HBS Location	Customer ID
testsector	5.575 GHz	5.465-5.730 GHz Universal	20 MHz	Active Re...	20.0.0.130	MSbs	test	Alpha_SU

NAS Identifier: If the authorization accounting was enabled, then each time the HBS authorizes an SU in its sector, it reports this fact to the accounting RADIUS server. The report is based on either the Device Name of the SU or the Device Location, according to your selection in here.

Note

The NAS Identifier Convention chosen here will also change the NAS Identifier Convention for the 802.1x Authentication option, even though the RADIUS server used here and in the 802.1x Authentication option are not necessarily the same server.

Enable Authorization Accounting: If this is enabled, then each time the HBS authorizes an SU in its sector, it reports this fact to an accounting RADIUS server. Define at least one accounting server here by clicking the configuration button (⚙), opening the RADIUS server parameters dialog box, and entering the parameters.

The authorization RADIUS server and the accounting RADIUS server can be either the same or two different servers.

Click **Save** to have your changes take effect.

Quality Detection

This option allows you to configure the HBS to send an indication when link quality degrades. There are three parameters, evaluated per link (HBS-SU pair):

BLQ Baseline Link Quality: Value that the throughput [Mbps] of the link should have. Configured at the SU for the uplink and downlink separately.

Th Detection Threshold[1]: A percentage of the Baseline Link Quality below which the link quality is considered to be degraded. Configured at the HBS. (If BLQ is 100Mbps, and TH is 25%, the alarm will be issued when the throughput is below 75Mbps)

tF Detection Seconds[2]: Time that the degradation must persist (Th) before an indication is issued. Setting this parameter to an appropriate value can prevent the system from reacting to brief peaks (or valleys) of link quality value (throughput) changes that do not disturb link functionality. Configured at the HBS.

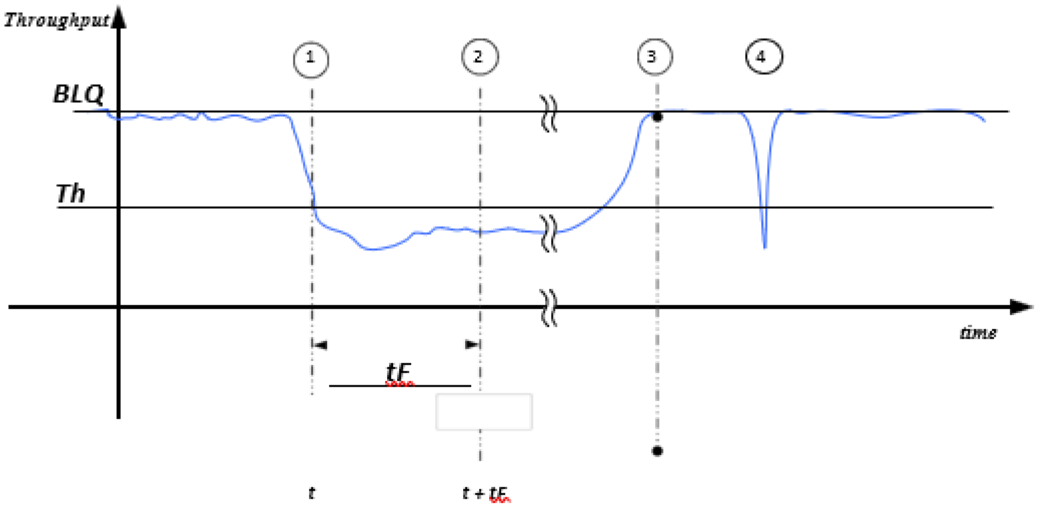


Figure 2-5: Quality Detection parameters

In Figure 2-5, *Quality Detection parameters*, the blue line represents the real-time throughput value of the link.

① The user has set the baseline link quality (**BLQ**) and the indication threshold value (Th). At time *t*, the signal throughput of the link decreases below this threshold. This causes the system to start a clock to measure the persistence of the low throughput condition.

② From the time *t* to the time *t* + tF (Detection Seconds), the low throughput condition persisted. An indication of link degradation is then issued.

③ The user has taken whatever measures necessary to rectify the link degradation, and the signal recovers. At that point, an indication is issued that the link quality degradation condition no longer exists.

④ For a link quality degradation that lasts for a shorter period of time than tF (Detection Seconds), no indication is issued.

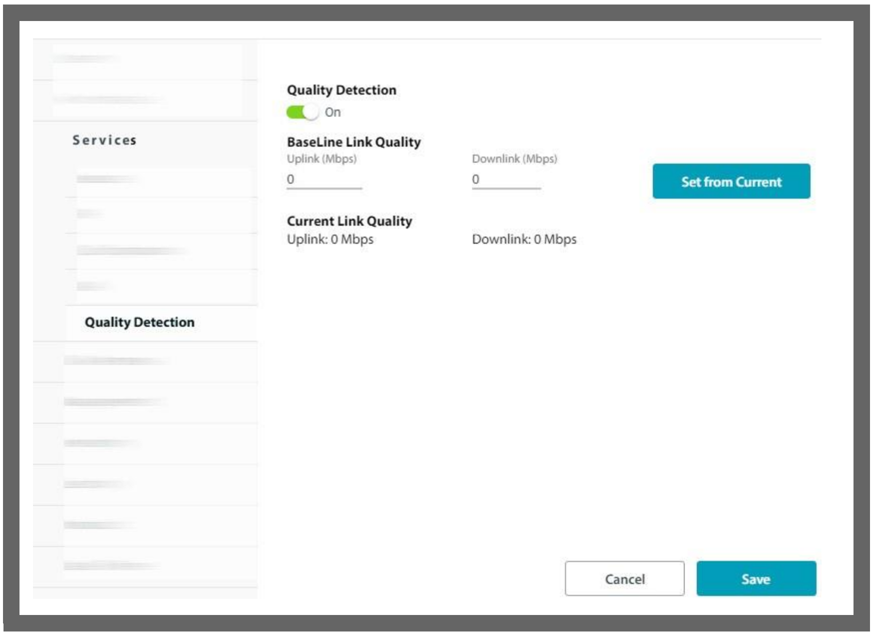
Configure Quality Detection as follows:

[1] *This is called "Indication Threshold" (Th) in the RADWIN Manager*

2. This is called "Indication Time" (tF) in the RADWIN Manager

SU side

1. Select the SU.
2. Click the Configuration icon (Configure).
3. Click Services -> Quality Detection.
4. Enable Quality Detection by clicking its switch to On.



Services

Quality Detection

Quality Detection

On

BaseLine Link Quality

Uplink (Mbps): 0

Downlink (Mbps): 0

Current Link Quality

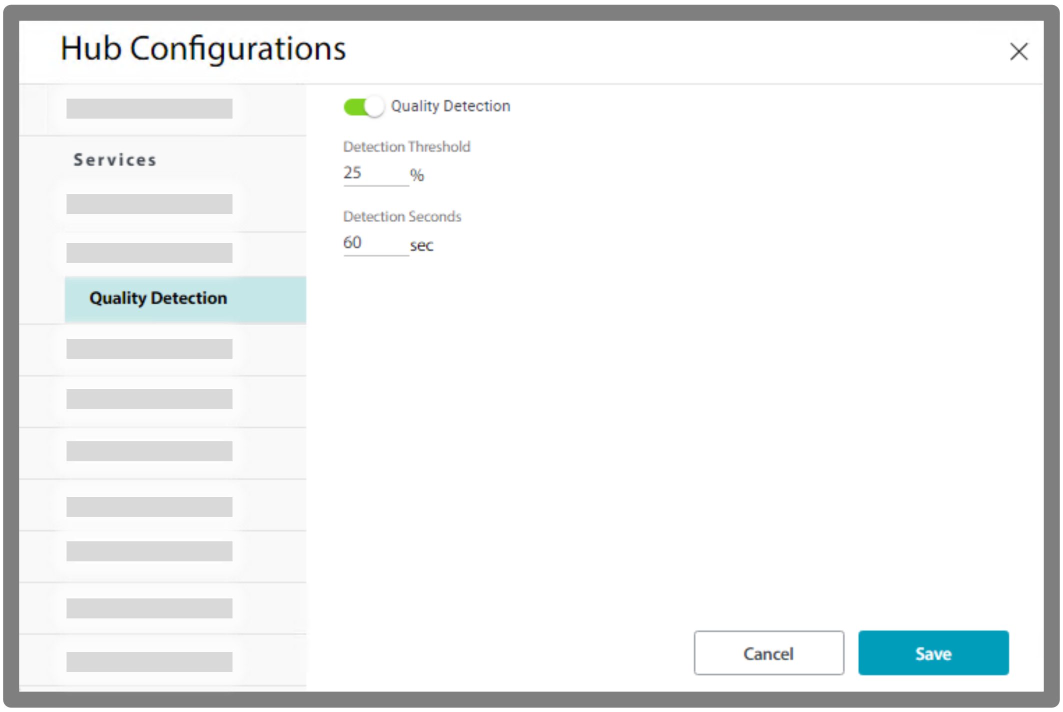
Uplink: 0 Mbps

Downlink: 0 Mbps

5. Select the **Baseline Link Quality** for the uplink and for the downlink in mega-bits per second (Mbps). They do not have to be the same.
6. You can set this value from the current throughput value (shown as Current Link Quality) by clicking **Set from Current**.
7. Click **Save**.

HBS side

1. Select the HBS.
2. Click the Configuration icon (Configure).
3. Click **Services -> Quality Detection**.
4. Enable Quality Detection by clicking its switch to **On**.
5. Select the Detection Threshold (Th) in percent value, relative to the baseline link quality value.
6. Select the Detection Seconds time (tF).
7. Click **Save**.



Hub Configurations

Quality Detection: on

Detection Threshold: 25 %

Detection Seconds: 60 sec

Self Registered SU

The user can set the HBS to accept SUs to be self-registered. This option is very useful when the user wants to be able to register an SU by themselves from the installation site, without the need to ask another person to connect to the BS to register the SU.

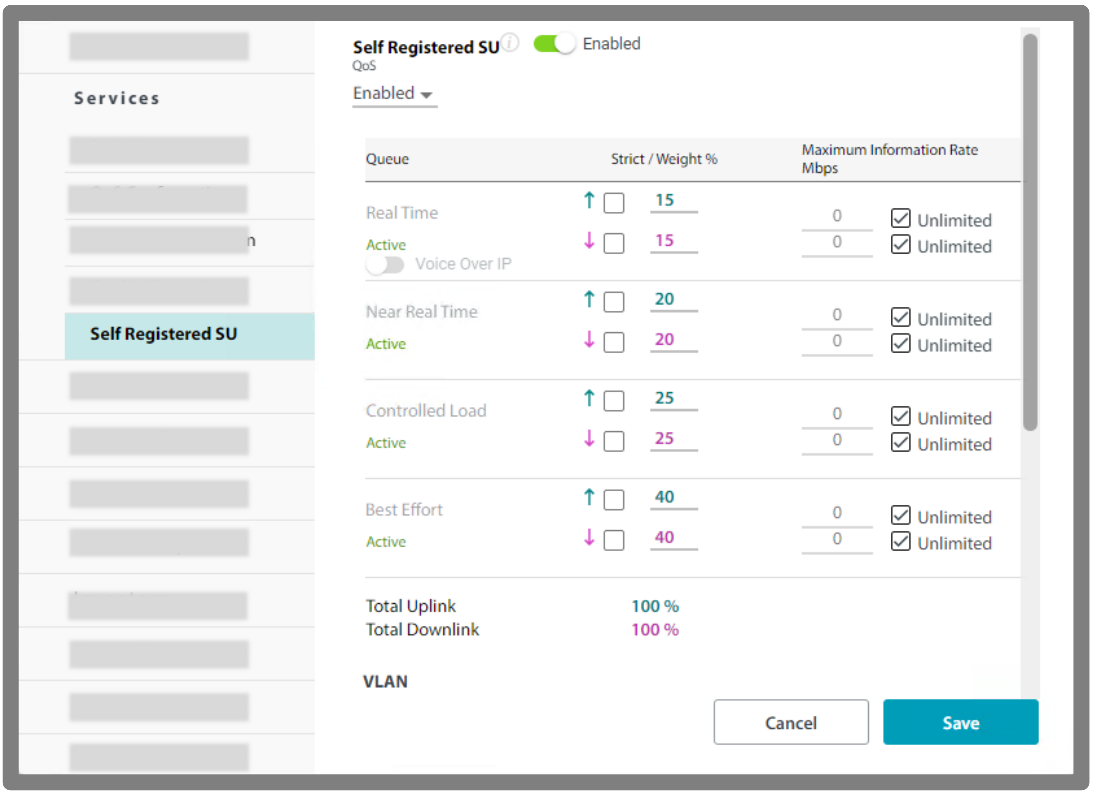
The user can set default settings for a self-registered SU. Any SU that will be self-registered, will receive the default settings when it registers.

The default settings include:

- QOS settings
- VLAN settings

After the self-registration is successful and service is established, the user can enter the SU configuration via the BS web-ui, and further customize the settings of the SU.

The following figures show the Self-registration settings screen in the BS Web-UI:



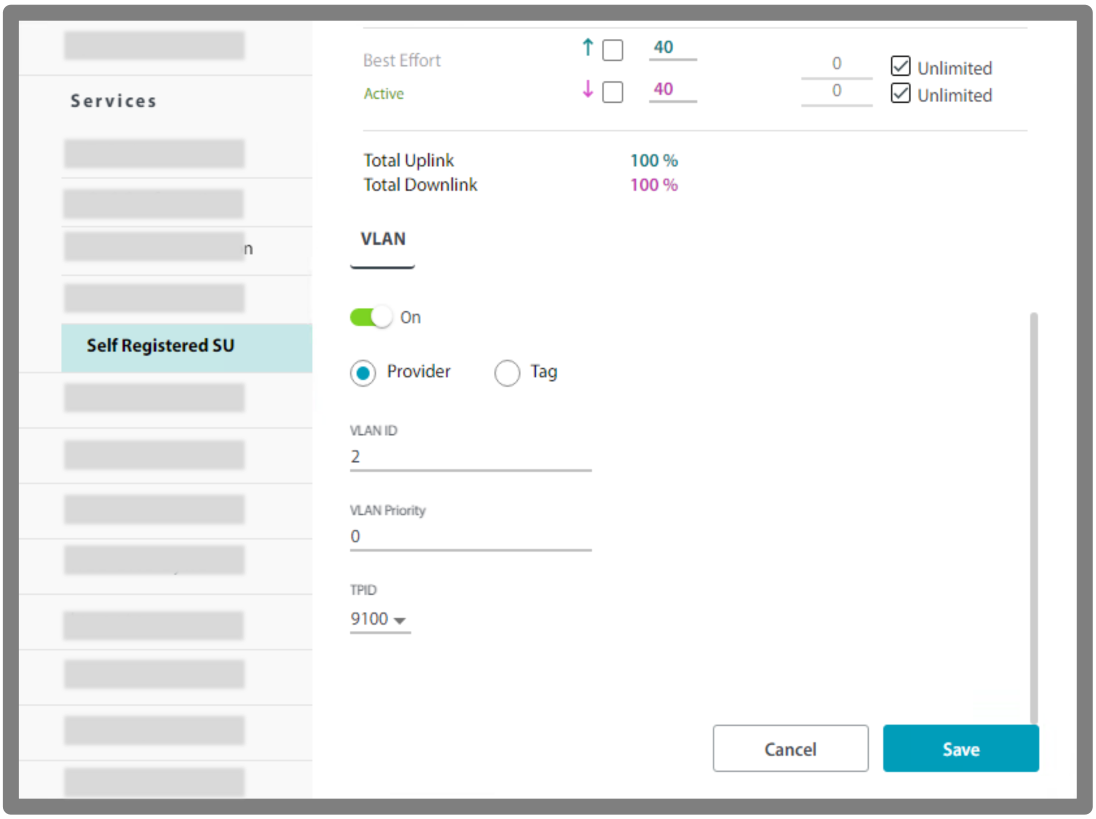
Self Registered SU ⓘ Enabled

QoS
Enabled

Queue		Strict / Weight %	Maximum Information Rate Mbps	
Real Time Active Voice Over IP	↑ □	15	0	☑ Unlimited
	↓ □	15	0	☑ Unlimited
Near Real Time Active	↑ □	20	0	☑ Unlimited
	↓ □	20	0	☑ Unlimited
Controlled Load Active	↑ □	25	0	☑ Unlimited
	↓ □	25	0	☑ Unlimited
Best Effort Active	↑ □	40	0	☑ Unlimited
	↓ □	40	0	☑ Unlimited

Total Uplink 100 %
Total Downlink 100 %

VLAN



Best Effort Active	↑ □	40	0	☑ Unlimited
	↓ □	40	0	☑ Unlimited

Total Uplink 100 %
Total Downlink 100 %

VLAN

On

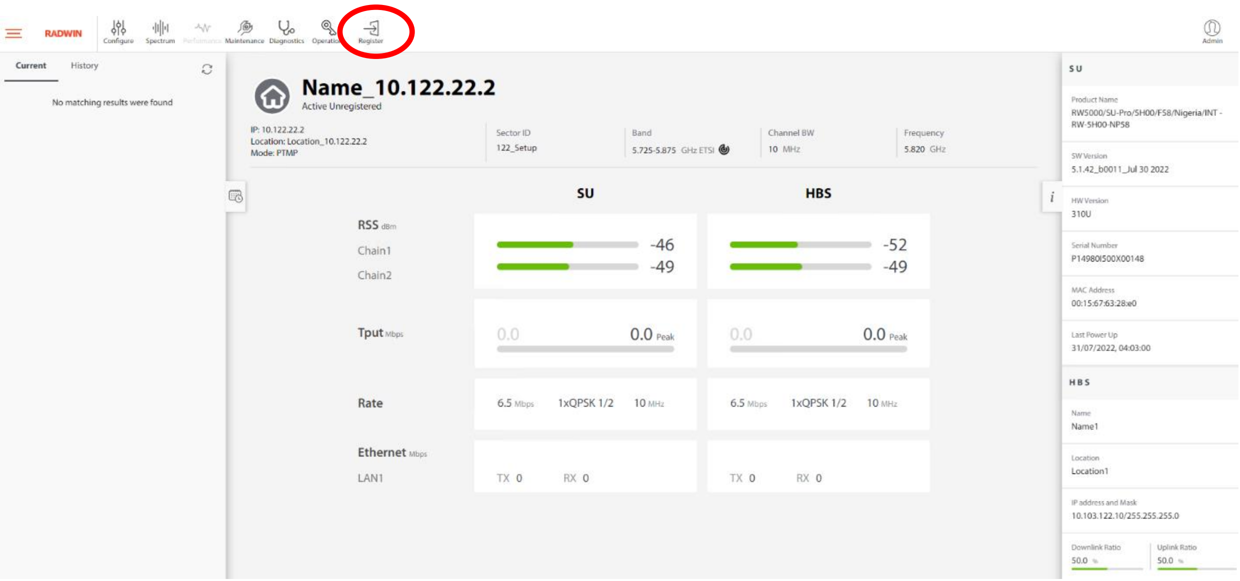
● Provider ○ Tag

VLAN ID
2

VLAN Priority
0

TPID
9100

Once the self-registration is enabled in the BS and the SU is synchronized to the BS, to perform the self-registration from the SU device, user needs to connect locally the SU web-UI (IP address of the SU) and press the button “Register” (as shown in the figure below)



No matching results were found

Name_10.122.22.2
Active Unregistered

IP: 10.122.22.2
Location: Location_10.122.22.2
Mode: PTMP

Sector ID	Band	Channel BW	Frequency
122_Setup	5.725-5.875 GHz ETSI	10 MHz	5.820 GHz

	SU	HBS
RSS dBm		
Chain1	-46	-52
Chain2	-49	-49
Tput Mbps	0.0 0.0 Peak	0.0 0.0 Peak
Rate	6.5 Mbps 1xQPSK 1/2 10 MHz	6.5 Mbps 1xQPSK 1/2 10 MHz
Ethernet Mbps		
LAN1	TX 0 RX 0	TX 0 RX 0

SU

Product Name
RW5000/SU-Pro/5H00/F58/Nigeria/INT - RW-5H00-NP58

SW Version
5.1.42_b0011_Jul 30 2022

HW Version
310U

Serial Number
P14980I500X00148

MAC Address
00:15:67:63:28:e0

Last Power Up
31/07/2022, 04:03:00

HBS

Name
Name1

Location
Location1

IP address and Mask
10.103.122.10/255.255.255.0

Downlink Ratio
50.0 %

Uplink Ratio
50.0 %

Note

Self-registered SU mode supported by SUs in Best Effort mode. In order to configure CIR, user must configure it after the SU is registered

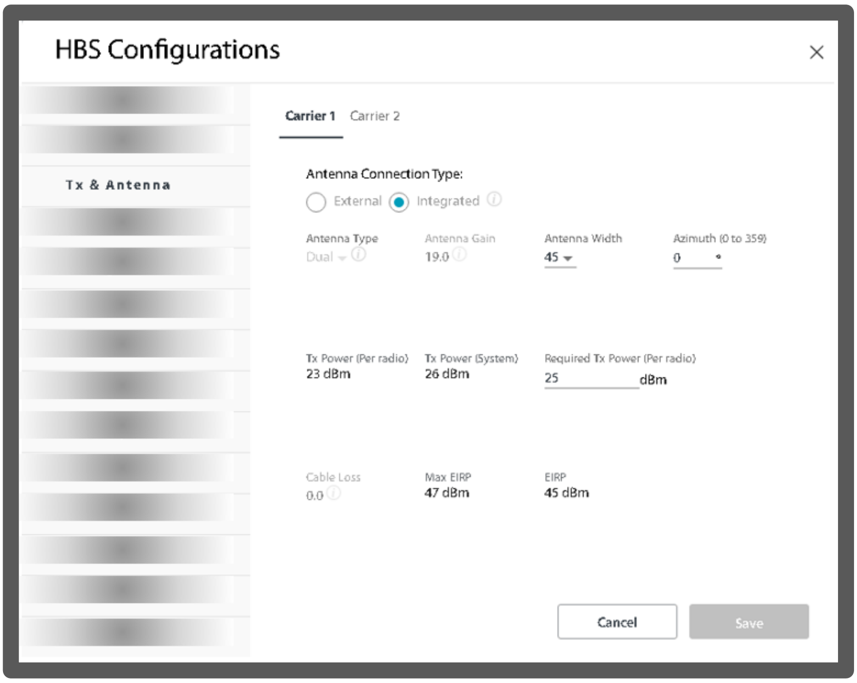
Note

Self-registered SU mode and Radius authentication mode can’t work together. If Self-registered mode is enabled, the Radius authentication will be disabled.

2.3.6. Tx & Antenna

- Changes made here may affect link quality and, in the case of antenna type, cause a re-sync.
- Changing the antenna type for an SU will cause a re-sync to that site only.
- For dual-carrier units, you can make changes for each carrier independently of each other, and if a re-sync occurs, it occurs for only the selected carrier.
- If you make any changes, click **Save** to have them take effect.

HBS (except MultiSector)



Antenna Connection Type: ○ External ● Integrated

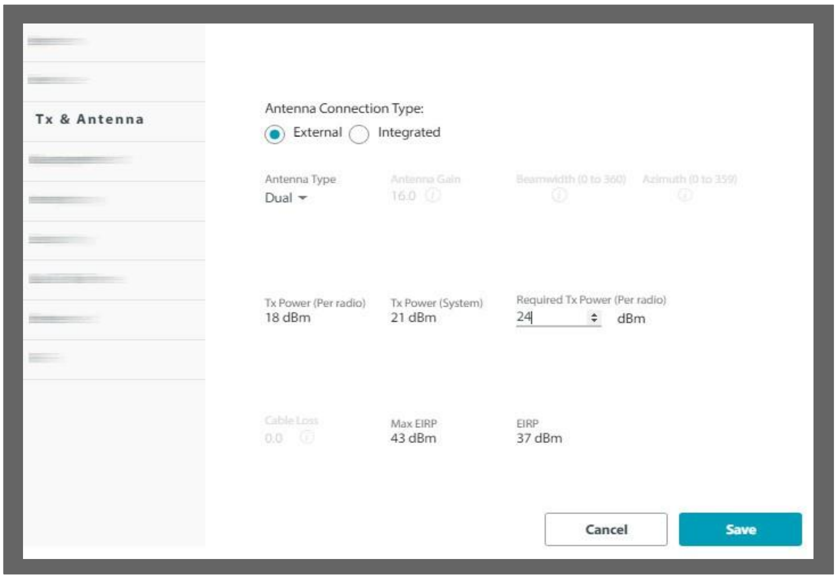
Antenna Type: Dual
Antenna Gain: 19.0
Antenna Width: 45
Azimuth (0 to 359): 0

Tx Power (Per radio): 23 dBm
Tx Power (System): 26 dBm
Required Tx Power (Per radio): 25 dBm

Cable Loss: 0.0
Max EIRP: 47 dBm
EIRP: 45 dBm

(Dual-carrier shown: Single carrier units do not show the carriers in the heading)

SU:



Antenna Connection Type: ● External ○ Integrated

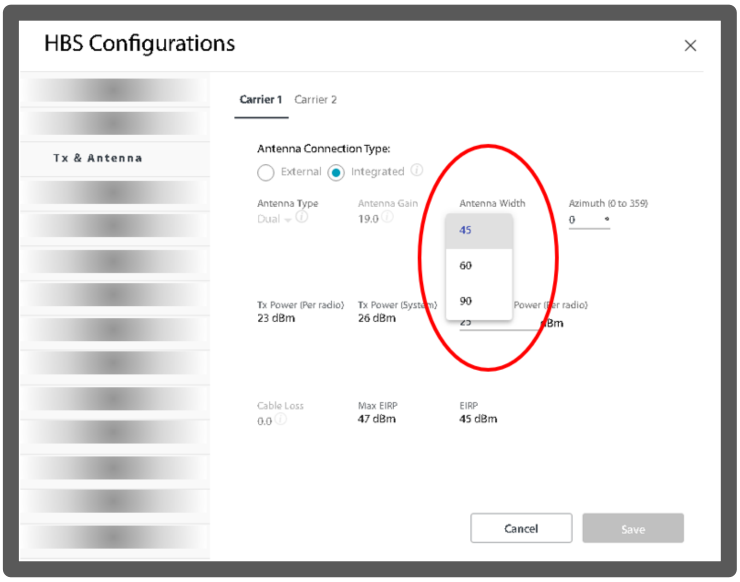
Antenna Type: Dual
Antenna Gain: 16.0
Beamwidth (0 to 360)
Azimuth (0 to 359)

Tx Power (Per radio): 18 dBm
Tx Power (System): 21 dBm
Required Tx Power (Per radio): 24 dBm

Cable Loss: 0.0
Max EIRP: 43 dBm
EIRP: 37 dBm

SDS – Software Defined Sector (Jet DUO only)

- In Jet DUO you can set the sector beamwidth from the UI
- You can select between the following beamwidth values:
  - 90 degrees (default)
  - 60 degrees
  - 45 degrees
- The selected beamwidth will apply to both carriers



HBS Configurations

Antenna Connection Type: ○ External ● Integrated

Antenna Type: Dual

Antenna Gain: 19.0

Antenna Width: 45

Azimuth (0 to 359): 0 °

Tx Power (Per radio): 23 dBm

Tx Power (System): 26 dBm

Power (Per radio): 25 dBm

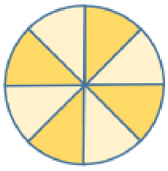
Cable Loss: 0.0

Max EIRP: 47 dBm

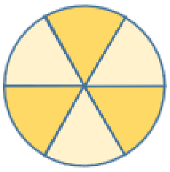
EIRP: 45 dBm

- The SDS feature allows to have up to 8 sectors at one site, with frequency reuse 2 (for each carrier) for exceptionally efficient spectrum use for very dense deployment environments. This capability increases the site capacity by up to double, without increasing the used frequency.

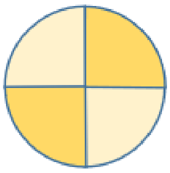
360 degree site with eight 45 degree sectors, with frequency reuse 2



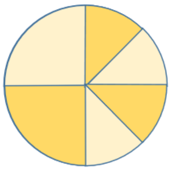
360 degree site with six 60 degree sectors, with frequency reuse 2



360 degree site with four 90 degree sectors, with frequency reuse 2



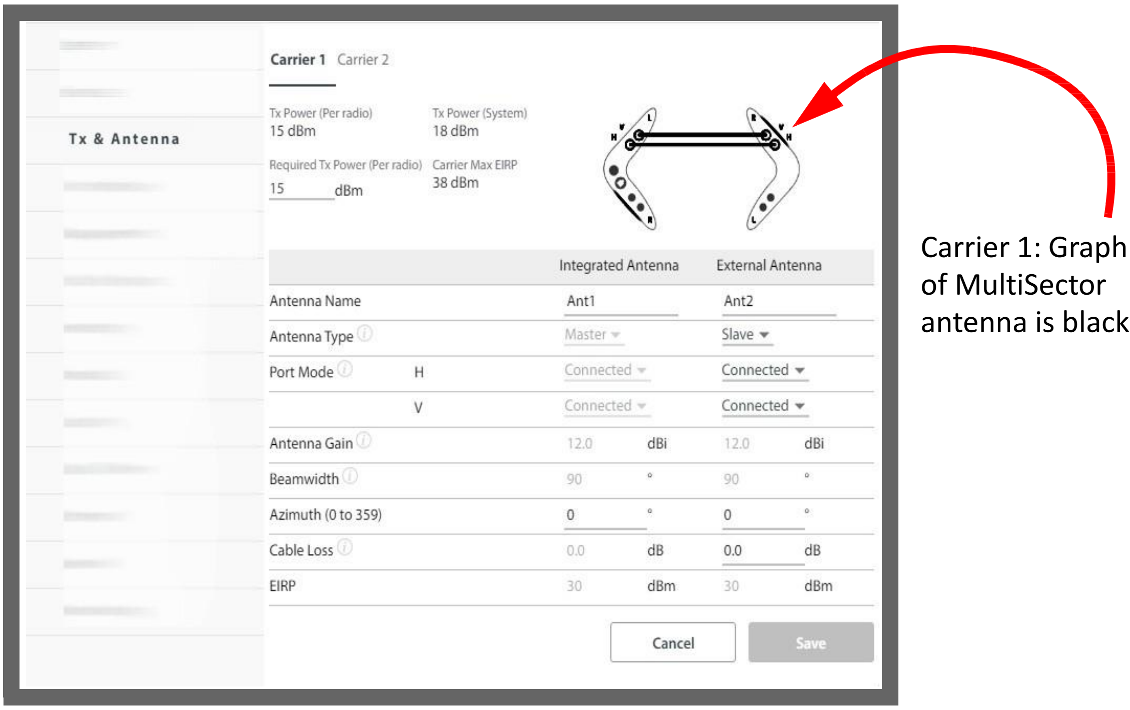
Partial deployment of SDS sectors with frequency reuse 2, is also an option as long as the number of sectors is even



HBS MultiSector Integrated

- You can make changes for each carrier independently of each other. Changes made here may affect link quality and, in the case of antenna type, cause a re-sync for the selected carrier.

- Changing the antenna type for an SU will cause a re-sync to that site only.
- If you make any changes, click **Save** to have them take effect.



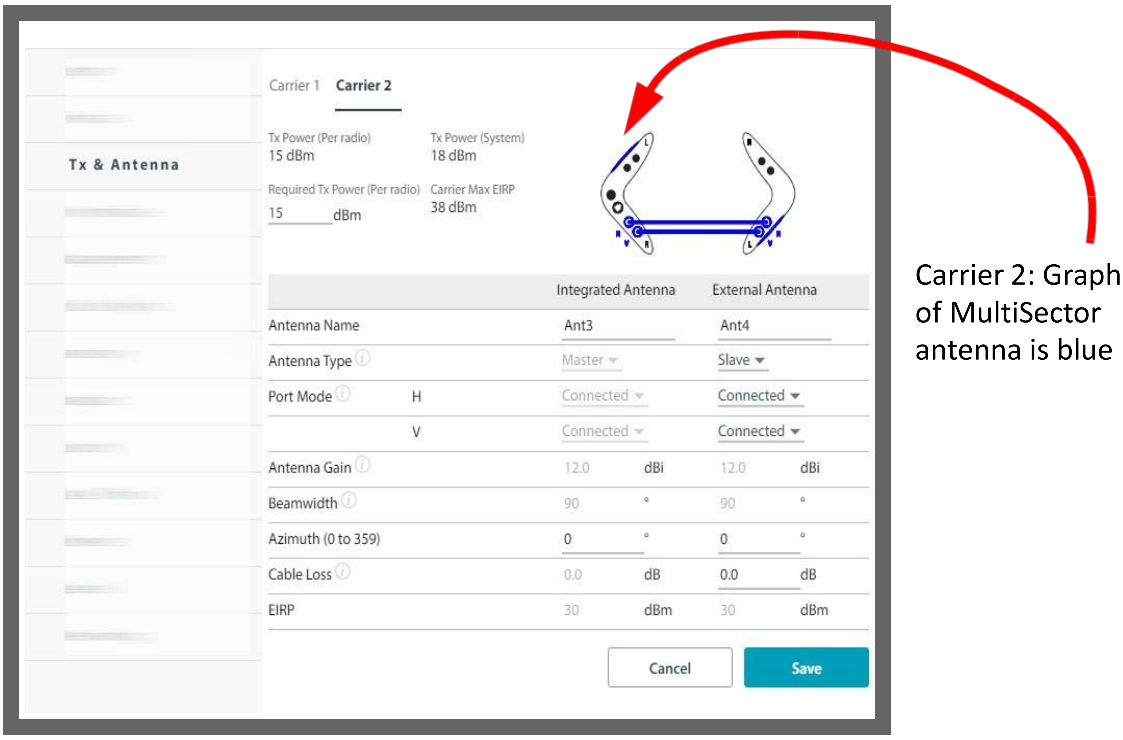
Tx & Antenna

Carrier 1 | Carrier 2

Tx Power (Per radio): 15 dBm
Tx Power (System): 18 dBm
Required Tx Power (Per radio): 15 dBm
Carrier Max EIRP: 38 dBm

		Integrated Antenna		External Antenna	
Antenna Name		Ant1		Ant2	
Antenna Type		Master		Slave	
Port Mode	H	Connected		Connected	
	V	Connected		Connected	
Antenna Gain		12.0	dBi	12.0	dBi
Beamwidth		90	°	90	°
Azimuth (0 to 359)		0	°	0	°
Cable Loss		0.0	dB	0.0	dB
EIRP		30	dBm	30	dBm

Carrier 1: Graphic of MultiSector antenna is black



Tx & Antenna

Carrier 1 | Carrier 2

Tx Power (Per radio): 15 dBm
Tx Power (System): 18 dBm
Required Tx Power (Per radio): 15 dBm
Carrier Max EIRP: 38 dBm

		Integrated Antenna		External Antenna	
Antenna Name		Ant3		Ant4	
Antenna Type		Master		Slave	
Port Mode	H	Connected		Connected	
	V	Connected		Connected	
Antenna Gain		12.0	dBi	12.0	dBi
Beamwidth		90	°	90	°
Azimuth (0 to 359)		0	°	0	°
Cable Loss		0.0	dB	0.0	dB
EIRP		30	dBm	30	dBm

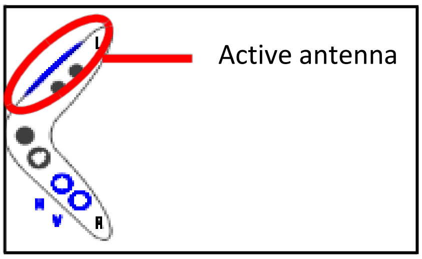
Carrier 2: Graphic of MultiSector antenna is blue

- Select Carrier 1 or Carrier 2 to see the parameters for the specific carrier.
- You can change the required Tx Power, which will be applied for the whole unit.
- For each carrier, there are two antennas, each with its unique name. Carrier 1 has Ant1

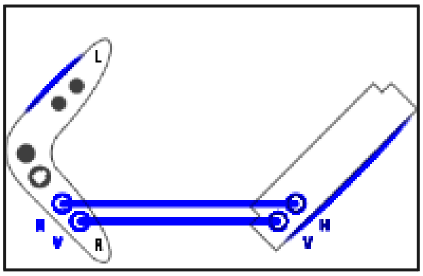
and Ant2, and Carrier 2 has Ant3 and Ant4.

- Antenna Type should appear as Master for the integrated antenna.
- For the external antenna, it can appear as None, External, or Slave. The graphic shows the status of the antenna(s). The colors show which side of the MultiSector the antenna resides at and the selected carrier. For more details about this connection scheme, see the RADWIN 5000 Installation Guide.

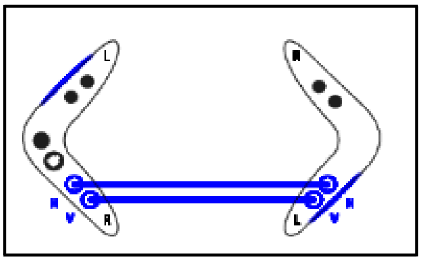
  - None: No external or supplemental antenna is used whatsoever. The MultiSector base station only is shown from above.



  - External: An external, 3rd party antenna is used. The MultiSector base station is shown from above as well as a graphic of an external antenna.



  - Slave: The MultiSector base station and the MultiSector antenna are shown from above.



- Port Mode appears for each polarization: Horizontal (H) and Vertical (V):

  Connected: A DC-grounded antenna is connected properly to the indicated port.

  Termination: A proper termination plug is connected to the indicated port.

  Not connected: Nothing is connected to the port, a plug, or an antenna without a DC-ground connection attached to the port.

Note

Port Mode is an indication field. That is, it does not change the actual port mode.

Even if an antenna without a DC-ground is connected, traffic may still be flowing.

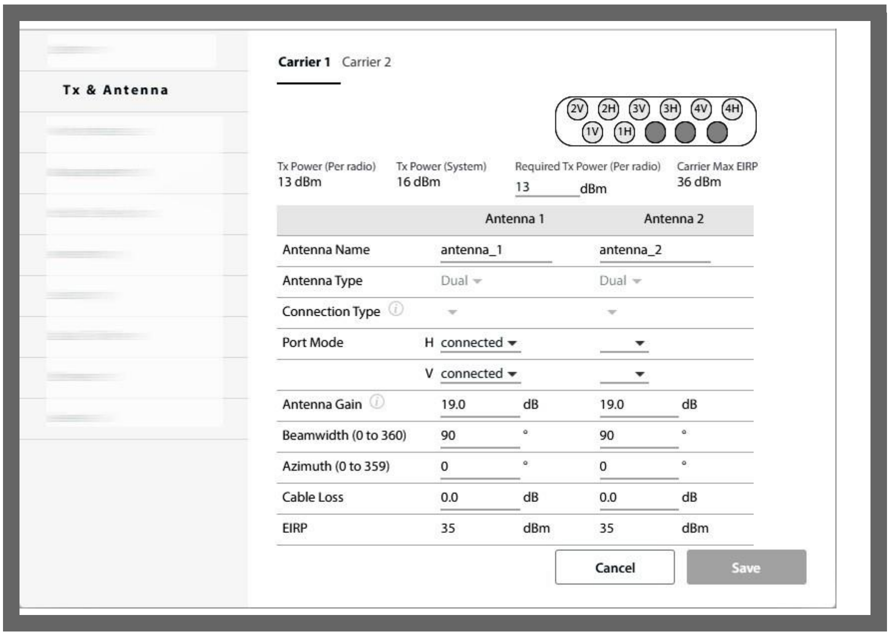
- Antenna gain: Make sure this is appropriate for the specific antenna being used.
- Beamwidth: Enter the beamwidth of the antenna being used.
- Azimuth: Enter the azimuth of the antenna being used.
- Cable Loss: Make sure you enter the correct cable loss.
- EIRP: Shows the final calculated antenna Tx power, taking all the parameter's values into consideration.

Note

Beamwidth, Azimuth, and Cable Loss are for information purposes only, and do not change the actual parameter value.

HBS MultiSector Connectorized

- You can make changes for each carrier independently of each other. Changes made here may affect link quality and in the case of antenna type, cause a re-sync for the selected carrier.
- If you make any changes, click **Save** to have them take effect.



Tx Power (Per radio) 13 dBm

Tx Power (System) 16 dBm

Required Tx Power (Per radio) 13 dBm

Carrier Max EIRP 36 dBm

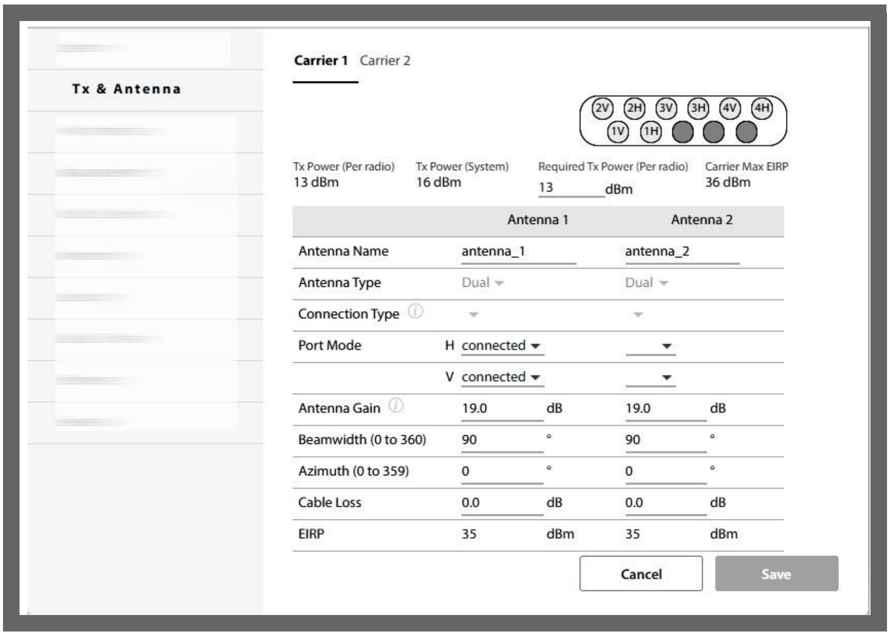
		Antenna 1		Antenna 2	
Antenna Name		antenna_1		antenna_2	
Antenna Type		Dual		Dual	
Connection Type					
Port Mode	H	connected			
	V	connected			
Antenna Gain		19.0	dB	19.0	dB
Beamwidth (0 to 360)		90	°	90	°
Azimuth (0 to 359)		0	°	0	°
Cable Loss		0.0	dB	0.0	dB
EIRP		35	dBm	35	dBm

- Select Carrier 1 or Carrier 2 to see the parameters for the specific carrier.
- You can change the required Tx Power, which will be applied for the whole unit.
- For each carrier, there are two antennas, each with its unique name. Carrier 1 has Antenna 1 and Antenna 2, and Carrier 2 has Antenna 3 and Antenna 4. Note that the indications on the graphic are the same as those on the unit itself.
- Antenna Type should appear as Dual.
- Connection Type should appear as External.
- Port Mode appears for each polarization: Horizontal (H) and Vertical (V):

  Connected: A DC-grounded antenna is connected properly to the indicated port.

  Termination: A proper termination plug is connected to the indicated port.

Not connected: Nothing is connected to the port, a plug, or an antenna without a DC-ground connection attached to the port.



Tx Power (Per radio) 13 dBm

Tx Power (System) 16 dBm

Required Tx Power (Per radio) 13 dBm

Carrier Max EIRP 36 dBm

		Antenna 1	Antenna 2
Antenna Name		antenna_1	antenna_2
Antenna Type		Dual ▾	Dual ▾
Connection Type ⓘ		▾	▾
Port Mode	H	connected ▾	▾
	V	connected ▾	▾
Antenna Gain ⓘ		19.0 dB	19.0 dB
Beamwidth (0 to 360)		90 °	90 °
Azimuth (0 to 359)		0 °	0 °
Cable Loss		0.0 dB	0.0 dB
EIRP		35 dBm	35 dBm

- Select Carrier 1 or Carrier 2 to see the parameters for the specific carrier.
- You can change the required Tx Power, which will be applied for the whole unit.
- For each carrier, there are two antennas, each with its unique name. Carrier 1 has Ant1 and Ant2, and Carrier 2 has Ant3 and Ant4.
- Antenna Type should appear as Dual.

- Connection Type should appear as External.
- Port Mode appears for each polarization: Horizontal (H) and Vertical (V):

  Connected: A DC-grounded antenna is connected properly to the indicated port.

  Termination: A proper termination plug is connected to the indicated port.

  Not connected: Nothing is connected to the port, a plug, or an antenna without a DC-ground connection attached to the port.

Note

Port Mode is an indication field. That is, it does not change the actual port mode.
Even if an antenna with a DC-ground is connected, traffic may still be flowing.

- Antenna gain: Make sure this is appropriate for the specific antenna being used.
- Beamwidth: Enter the beamwidth of the antenna being used.
- Azimuth: Enter the azimuth of the antenna being used.
- Cable Loss: Make sure you enter the correct cable loss.

- EIRP: Shows the final calculated antenna Tx power, taking all the parameter’s values into consideration.

Note

Beamwidth, Azimuth, and Cable Loss are for information purposes only, and do not change the actual parameter value.

Note

If you change the Tx Power, it will be applied to the whole unit (both carriers).

- Antenna gain: Make sure this is appropriate for the specific antenna being used.
- Beamwidth: Enter the beamwidth of the antenna being used.
- Azimuth: Enter the azimuth of the antenna being used.
- Cable Loss: Make sure you enter the correct cable loss.
- EIRP: Shows the final calculated antenna Tx power, taking all the parameter’s values into consideration.

Note

Port Mode is an indication field. That is, it does not change the actual port mode. Even if an antenna with a DC-ground is connected, traffic may still be flowing.

Beamwidth, Azimuth, and Cable Loss are for information purposes only, and do not change the actual parameter value.

2.3.7. Air Interface (HBS or SU directly)

In dual-carrier units, configure these parameters per carrier.

In single-carrier units, these parameters are configured for the whole sector.

If you are accessing an SU directly, only the Radio option is available, and it is more limited than the option for the HBS. See *Air Interface* for a description.

If you are accessing an SU directly, options here are very different. See *Air Interface*.

Radio (HBS option)

Sector ID: Set the Sector ID here. The value will “percolate” to all registered SUs. It will be “picked up” by newly installed and registered SUs.

To see the results of the most recent Spectrum scan (see Spectrum), click the Spectrum icon (Spectrum).

Automatic Channel Selection: We recommend you do this only at configuration time.

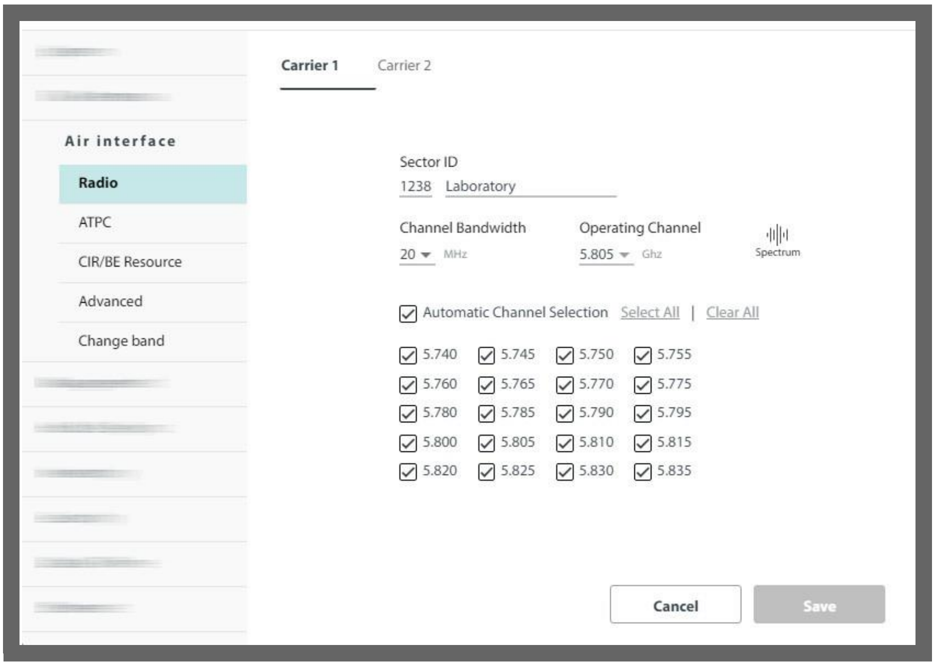
Once you are finished with any changes, click **Save**.

Channel selection options differ depending on the specific product you are working with (JET-DUO 3/5 GHz:, JET-DUO 5GHz , NEO, NEO DUO, and MultiSector:, JET AIR/

PRO (5GHz), JET PRO (3.5 GHz)):

JET-DUO 3/5 GHz:

- The initial operating channel for the 3.x and for the 5.x carrier are shown.
- Select the channel bandwidth for each carrier in turn, independently.
- To change the operating channel, select a new frequency from the list below. The larger the channel bandwidth you have chosen, the fewer frequencies are available.
- You can choose "Automatic Channel Selection" (ACS), which allows the unit to dynamically select the best frequency to work with. You can allow the unit to choose between two or more frequencies (you must choose at least two frequencies when working with ACS).



Sector ID
1238 Laboratory

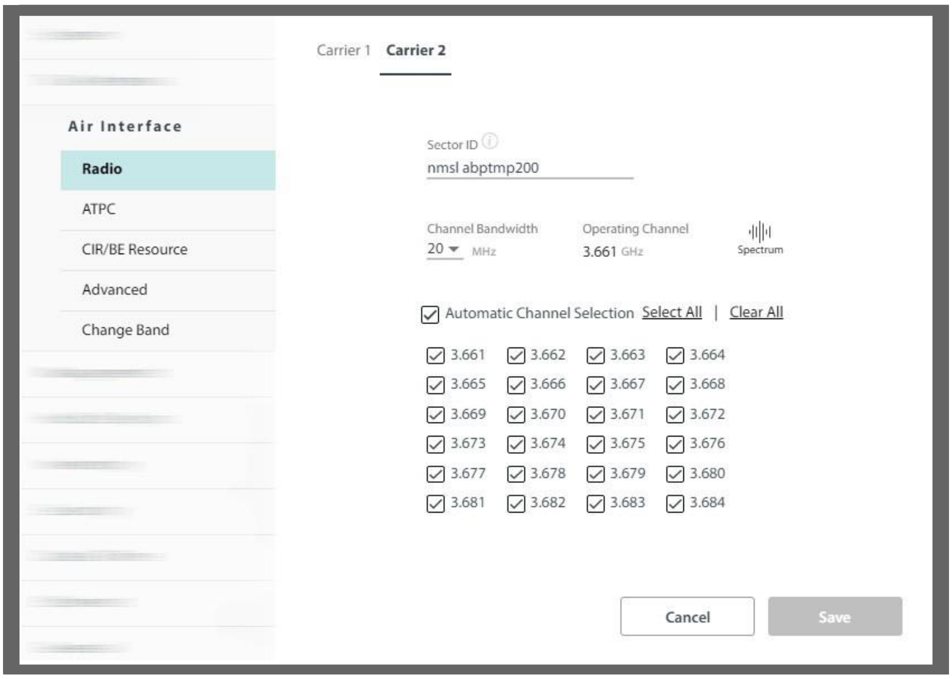
Channel Bandwidth 20 MHz

Operating Channel 5.805 Ghz

☑ Automatic Channel Selection Select All | Clear All

☑ 5.740 ☑ 5.745 ☑ 5.750 ☑ 5.755
☑ 5.760 ☑ 5.765 ☑ 5.770 ☑ 5.775
☑ 5.780 ☑ 5.785 ☑ 5.790 ☑ 5.795
☑ 5.800 ☑ 5.805 ☑ 5.810 ☑ 5.815
☑ 5.820 ☑ 5.825 ☑ 5.830 ☑ 5.835

Figure 2-6: JET-DUO 3/5 GHz: Carrier 1 (5.x band)



Sector ID
nmsl abptmp200

Channel Bandwidth 20 MHz

Operating Channel 3.661 GHz

☑ Automatic Channel Selection Select All | Clear All

☑ 3.661 ☑ 3.662 ☑ 3.663 ☑ 3.664
☑ 3.665 ☑ 3.666 ☑ 3.667 ☑ 3.668
☑ 3.669 ☑ 3.670 ☑ 3.671 ☑ 3.672
☑ 3.673 ☑ 3.674 ☑ 3.675 ☑ 3.676
☑ 3.677 ☑ 3.678 ☑ 3.679 ☑ 3.680
☑ 3.681 ☑ 3.682 ☑ 3.683 ☑ 3.684

Figure 2-7: JET-DUO 3/5 GHz: Carrier 2 (3.x band)

JET-DUO 5GHz , NEO, NEO DUO, and MultiSector:

- The initial operating channel for both carriers are shown.
- Select the channel bandwidth for each carrier in turn, independently.
- To change the operating channel, select a new frequency from the list. The larger the channel bandwidth you have chosen, the fewer frequencies are available.
- You can choose “Automatic Channel Selection” (ACS), which allows the unit to dynamically select the best frequency to work with. You can allow the unit to choose between two or more frequencies (you must choose at least two frequencies when working with ACS).
- The system ensures that there are no conflicts between carriers. You are limited in choosing the same (or very nearby) frequencies for both carriers. This works as follows:
  - The operating channel you have chosen on Carrier X is noted.
  - The channel bandwidth you have chosen on Carrier X is noted.
  - Channels that are “too close” (See *Proximity Table*) to the operating channel of Carrier X are tagged on the other carrier (Carrier Y), accordingly:
    > If a channel on Carrier Y is tagged blue, then if you choose that channel on Carrier Y, this indicates that the corresponding channel on Carrier X can be changed to allow this channel to be chosen on Carrier Y. This is because there are other channels available on Carrier X. You can choose any of the blue tagged channels on Carrier Y (to become the new operating channel on Carrier Y), but note that once you click Save, the operating channel on Carrier X might change.

    > If a channel on Carrier Y is tagged red, the system will not use that channel, even if you placed a checkmark there. This is because it would conflict with the operating channel on Channel X.

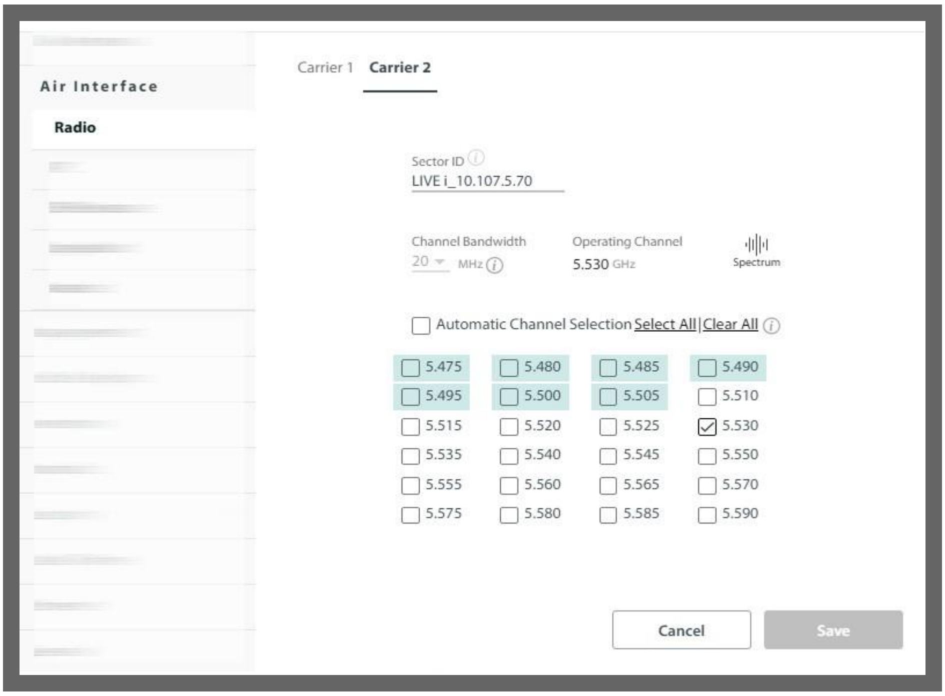
For example:

- The operating channel of Carrier 2 is 5.530 GHz, and its Channel Bandwidth is also 20MHz.
- The operating channel of Carrier 1 is 5.480 GHz, and the Channel Bandwidth is 20 MHz.

According to the proximity table (See *Proximity Table*), the channels of the two carriers must have a separation of 30MHz.

- **Carrier 2**:
  > As a result of the conditions above, channels of Carrier 2 from 5.475 GHz to 5.505 GHz are tagged (ie, 5.480 GHz +/- 30MHz).

  > In Carrier 1 several channels are chosen, so it is possible for the operating channel to be moved to one of these, therefore, the channels that are tagged in Carrier 2 are tagged blue. This indicates that if you choose one or more channels of these blue channels in Carrier 2, it is possible that the operating channel of Carrier 1 will be pushed aside.



Sector ID
LIVE i_10.107.5.70

Channel Bandwidth 20 MHz

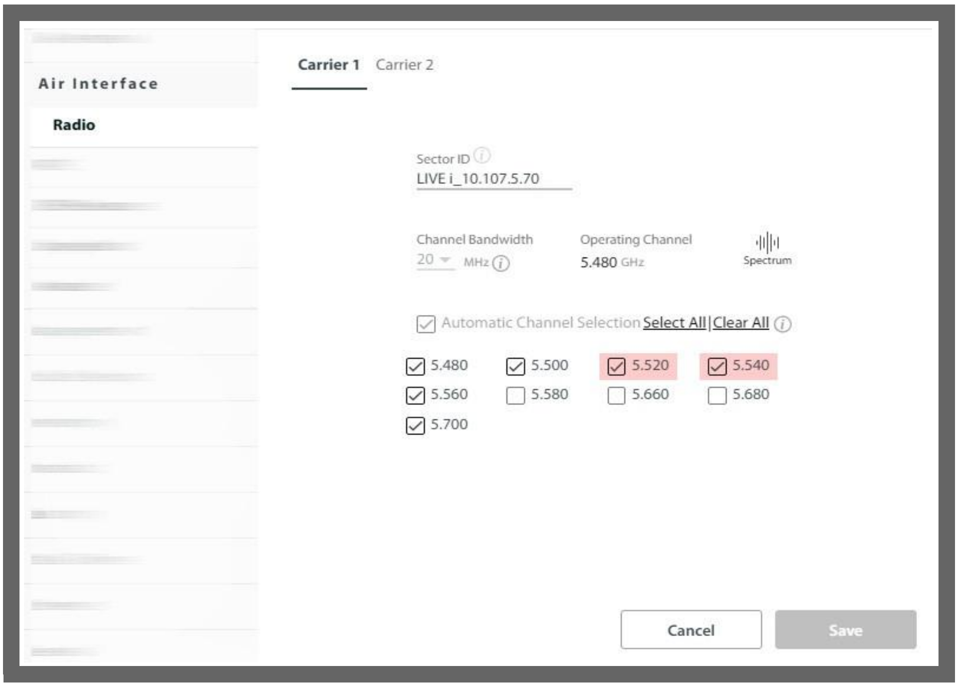
Operating Channel 5.530 GHz

□ Automatic Channel Selection Select All | Clear All

□ 5.475	□ 5.480	□ 5.485	□ 5.490
□ 5.495	□ 5.500	□ 5.505	□ 5.510
□ 5.515	□ 5.520	□ 5.525	☑ 5.530
□ 5.535	□ 5.540	□ 5.545	□ 5.550
□ 5.555	□ 5.560	□ 5.565	□ 5.570
□ 5.575	□ 5.580	□ 5.585	□ 5.590

Figure 2-8: JET-DUO 3/5 GHz 5GHz and MultiSector: Carrier 2

- **Carrier 1**:
  - > Similarly, channels of Carrier 1 from 5.520 GHz to 5.540 GHz are tagged (ie, 5.530 GHz +/- 30MHz).
  - > In Carrier 2, only one channel is chosen (5.530 GHz), so it is not possible to switch to 5.520GHz or 5.540GHz on Carrier 1, because these would interfere with 5.530GHz on Carrier 2. Therefore, these channels are tagged red, indicating that even if you choose one or more, it is they will not be selected as the operation channel of Carrier 1.



Sector ID
LIVE i_10.107.5.70

Channel Bandwidth 20 MHz

Operating Channel 5.480 GHz

☑ Automatic Channel Selection Select All | Clear All

☑ 5.480	☑ 5.500	☑ 5.520	☑ 5.540
☑ 5.560	□ 5.580	□ 5.660	□ 5.680
☑ 5.700			

Figure 2-9: JET-DUO 3/5 GHz 5GHz and MultiSector: Carrier 1

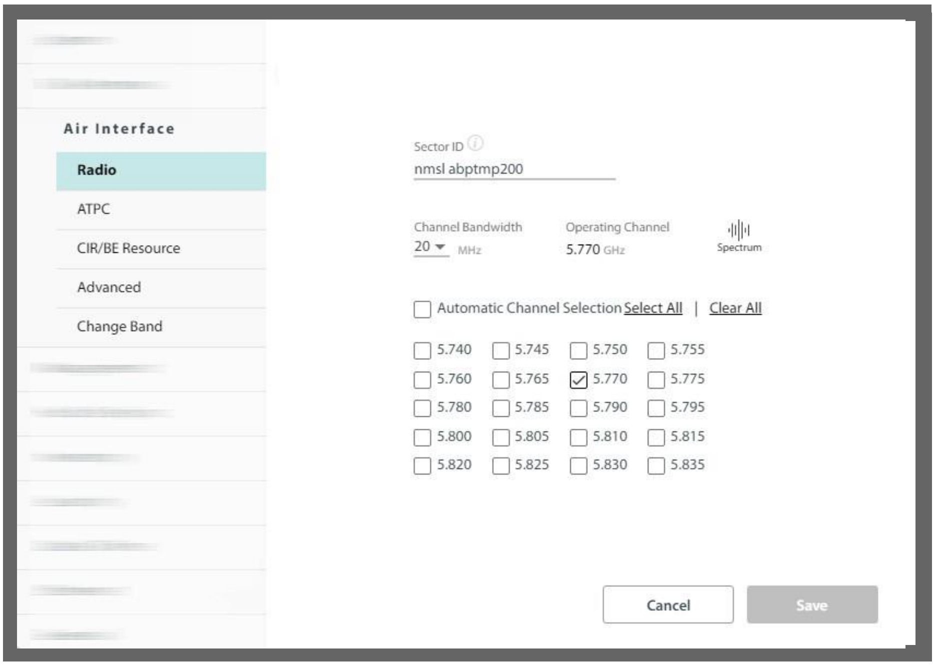
Table 2-1: Proximity Table

		Interferer BW				
		5	10	20	40	80
Victim BW	5	10	10	15	25	45
	10	10	15	20	30	50
	20	15	20	30	40	90
	40	25	30	40	60	90
	80	45	50	90	90	120

The table above shows the temporal separation required between operating channels of the two carriers, according to the bandwidth of the carriers. For example, if one carrier (the “Interferer”) has a bandwidth of 40MHz, and the other (the “Victim”) has a bandwidth of 80MHz, the separation between the two operating channels must be at least 90MHz (eg. 5.480GHz and 5.390GHz).

JET AIR/PRO (5GHz)

- The initial operating channel is shown.
- To change the operating channel, select a new frequency from the list below. The larger the channel bandwidth you have chosen, the fewer frequencies are available.
- You can choose “Automatic Channel Selection” (ACS), which allows the unit to dynamically select the best frequency to work with. You can allow the unit to choose between two or more frequencies (you must choose at least two frequencies when working with ACS).



Sector ID: nmsl abptmp200

Channel Bandwidth: 20 MHz

Operating Channel: 5.770 GHz

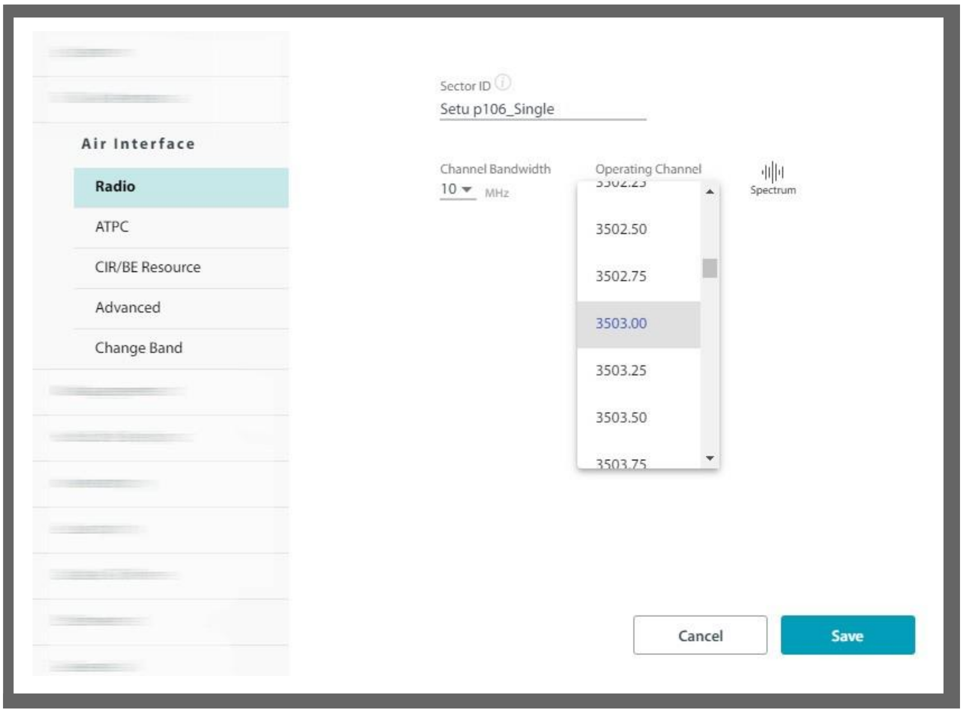
□ Automatic Channel Selection Select All | Clear All

□ 5.740	□ 5.745	□ 5.750	□ 5.755
□ 5.760	□ 5.765	☑ 5.770	□ 5.775
□ 5.780	□ 5.785	□ 5.790	□ 5.795
□ 5.800	□ 5.805	□ 5.810	□ 5.815
□ 5.820	□ 5.825	□ 5.830	□ 5.835

Figure 2-10: JET AIR/PRO (5 GHz)

JET PRO (3.5 GHz)

- Select the channel bandwidth.
- The initial operating channel is shown.
- To change the operating channel, select a new frequency from the pull-down menu below “Operating Channel”.
- Since this is a “high resolution” product, the distance between each channel is 250 kHz, no matter what channel bandwidth was chosen.
- “Automatic Channel Selection” (ACS) is not available for this product.



Sector ID: Setu p106_Single

Channel Bandwidth: 10 MHz

Operating Channel: 3503.00

Figure 2-11: JET PRO (3.5 GHz)

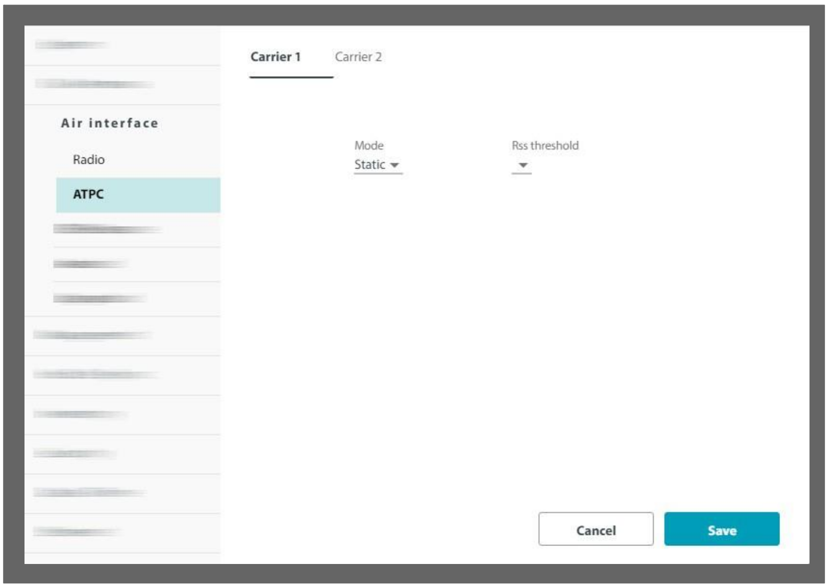
- If you make any changes, click **Save** for them to take effect.

ATPC

The Automatic HSU Transmit Power Control enables the HBS to optimize the transmit power of all SUs in the sector for the selected carrier. This is done by configuring the desired RSS (radio signal strength) threshold level. The HBS then tunes the transmission power of the SUs to give this RSS value.

- Mode: Select Disabled, Static, or Dynamic from the pull-down menu.
    - Disabled: Disables the ATPC option
    - Static: Instructs the HBS to find an optimal transmit RSS value for the SUs. The HBS then locks on to this power value and does not change it until this configuration option is changed.
    - Dynamic: Instructs the HBS to find an optimal transmit RSS value for the SUs. The HBS will change this power value from time to time when needed.

- RSS Threshold: The desired RSS level, which the HBS refers to in order to tune the transmission power of the SUs. The best power level depends on the radio plan, but is also influenced by your choice of Channel Bandwidth.



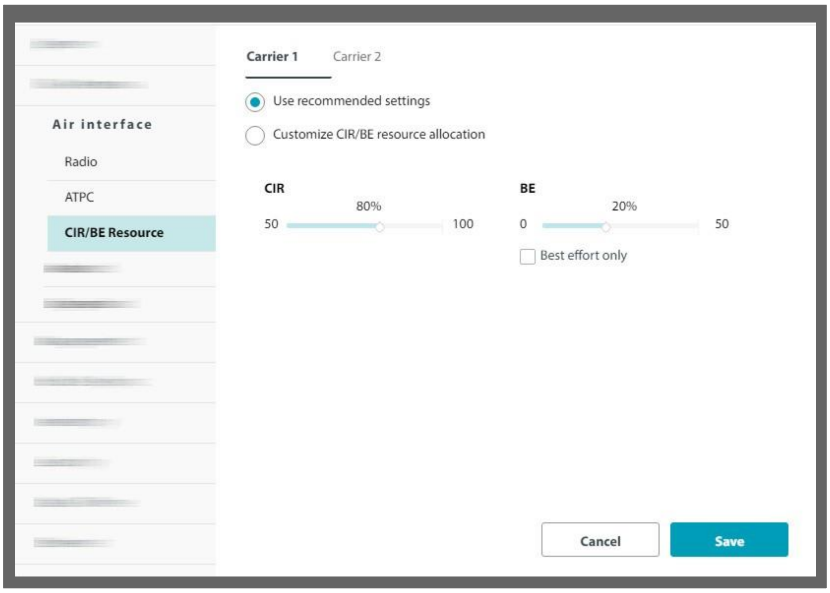
Mode: Static ▾

Rss threshold: ▾

CIR/BE Resource

If the sector you are working with, has a combination of CIR (Committed Information Rate) and Best Effort SUs, this option allows you to set what percentage of the sector resources are allocated to CIR units and what percentage are allocated to BE units.

Click the **Use recommended settings** radio button to set the CIR/Best Effort to 80%-20%.



● Use recommended settings

○ Customize CIR/BE resource allocation

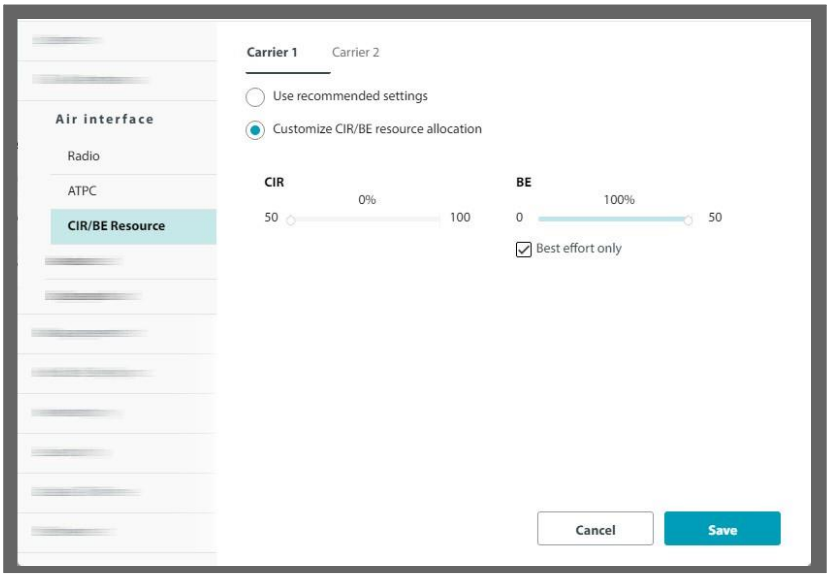
CIR: 50 — 80% — 100

BE: 0 — 20% — 50

□ Best effort only

If you wish to **customize** the settings, do the following:

- If you have only BE units, check the Best Effort only box. This is like setting the CIR/Best Effort Ratio to 0.0%/100.0%. If you have at least one CIR unit, this box is disabled.



○ Use recommended settings

● Customize CIR/BE resource allocation

CIR 0% (50 – 100)

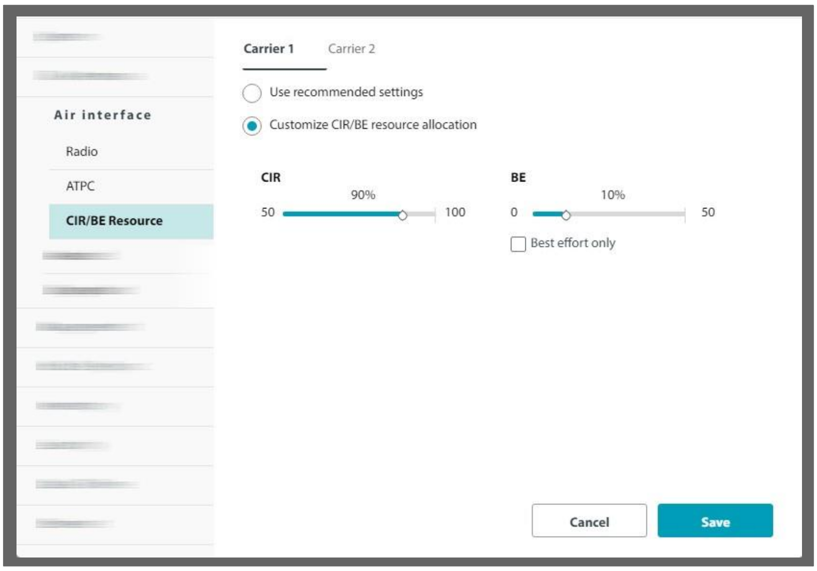
BE 100% (0 – 50)

☑ Best effort only

- If you have only CIR units, move the slider to the far right, and get 100% for CIR. This is the most efficient use of resources for a sector with only CIR units.

You can set this before any fixed SUs are registered, and if you choose 100% of one kind or another, you will be limited when registering the SUs to that resource type.

When you register a specific SU, you choose what percentage of the specific resource type (CIR or BE) to allocate to this SU.



○ Use recommended settings

● Customize CIR/BE resource allocation

CIR 90% (50 – 100)

BE 10% (0 – 50)

□ Best effort only

Click **Save** to have your changes take effect.

Change Band

Changing the band in use is always carried out at the sector level, each carrier by itself.

1. Make sure you are logged in to the base station as Installer.
2. For single world-wide PN products (Jet Air, Jet Air DUO), please see Change country and band for world-wide products.
3. From the "**Select a band from the list**" pull-down menu, select the new band. The specific list depends on your regulatory environment.
4. Choose the working channel bandwidth and operating channel.

5. Click **Save**. A message will appear cautioning you that all the devices will be reset. Note that this applies to both carriers even if you are only changing the band for one of the carriers.

Caution

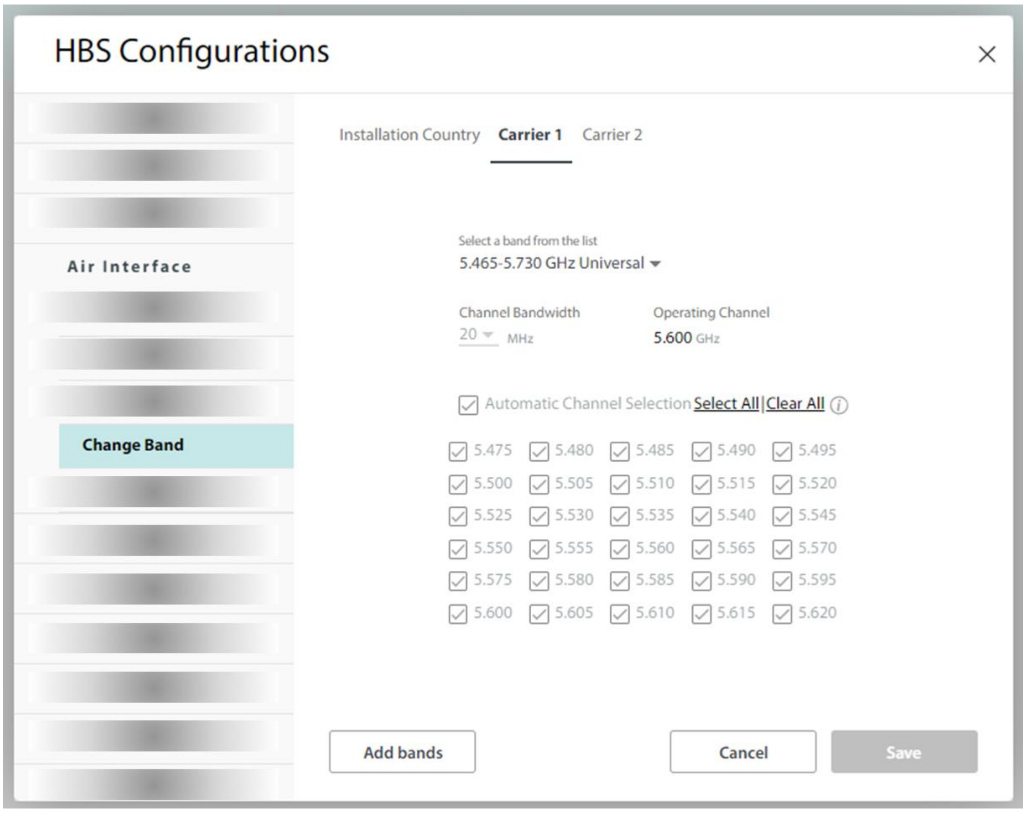
When changing a frequency band for one carrier, both carriers will be reset.

Note

Note: the DFS icon indicates which products have DFS enabled.

6. Click **Yes** to continue.

7. Click **OK**. A sector reset follows.



Select a band from the list
5.465-5.730 GHz Universal

Channel Bandwidth: 20 MHz

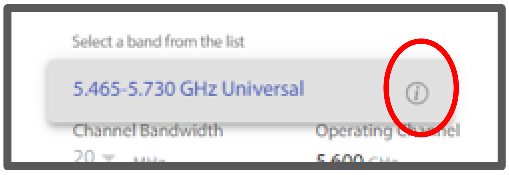
Operating Channel: 5.600 GHz

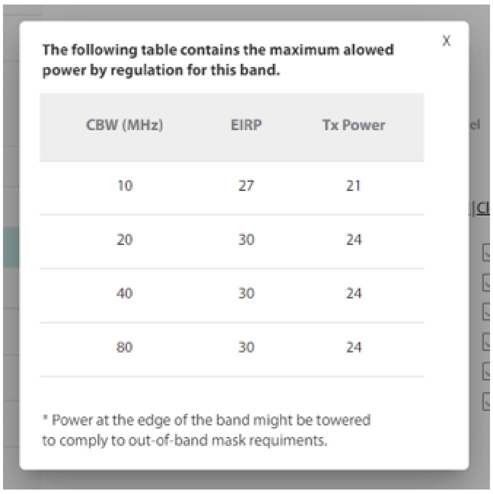
☑ Automatic Channel Selection Select All|Clear All

☑ 5.475 ☑ 5.480 ☑ 5.485 ☑ 5.490 ☑ 5.495
☑ 5.500 ☑ 5.505 ☑ 5.510 ☑ 5.515 ☑ 5.520
☑ 5.525 ☑ 5.530 ☑ 5.535 ☑ 5.540 ☑ 5.545
☑ 5.550 ☑ 5.555 ☑ 5.560 ☑ 5.565 ☑ 5.570
☑ 5.575 ☑ 5.580 ☑ 5.585 ☑ 5.590 ☑ 5.595
☑ 5.600 ☑ 5.605 ☑ 5.610 ☑ 5.615 ☑ 5.620

Note

You can see the regulation limitation of the band by pressing the info button near the channel in the band selection box





The following table contains the maximum alowed power by regulation for this band.

CBW (MHz)	EIRP	Tx Power
10	27	21
20	30	24
40	30	24
80	30	24

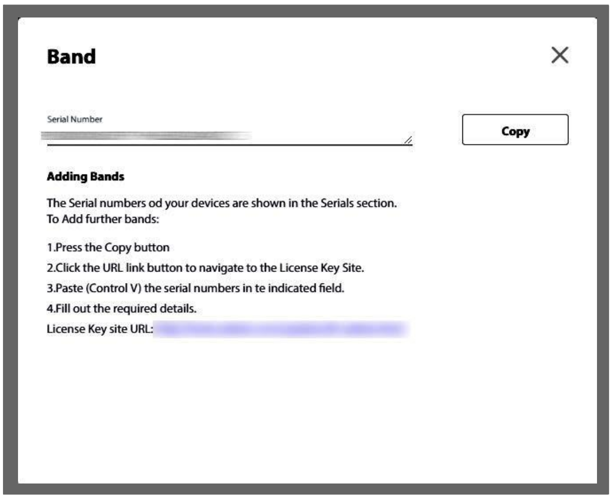
* Power at the edge of the band might be towered to comply to out-of-band mask requiments.

You may also add new Bands by clicking Add Bands. There are several provisos to this:

- Additional Bands must be available for your hardware
- Such additional Bands must be available within the framework of your local regulations

To obtain and install additional bands:

1. Make a list of ODU serial numbers for all HBSs and all SUs to receive additional bands. The list should be a simple text file with one serial number per line. (The serial numbers are located on the stickers on the ODUs.)
2. Click **Add Bands**. An instruction panel is displayed.



Band

Serial Number [redacted]

Adding Bands

The Serial numbers od your devices are shown in the Serials section.
To Add further bands:

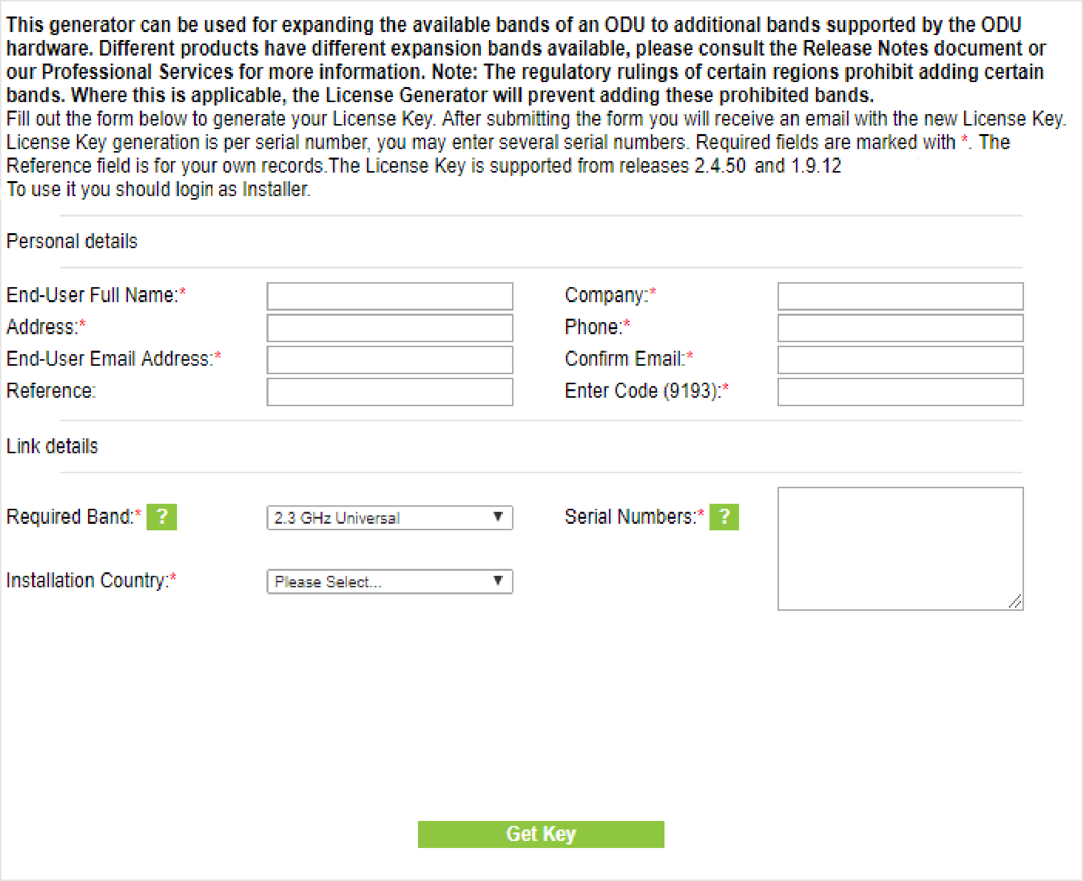
1.Press the Copy button
2.Click the URL link button to navigate to the License Key Site.
3.Paste (Control V) the serial numbers in te indicated field.
4.Fill out the required details.
License Key site URL: [redacted]

The serial numbers displayed relate to the radios in the sector. Click Copy to copy the numbers to the clipboard.

3. This step applies only if you have additional un-installed units:

Before proceeding to Step 2 in the instruction panel, make your own list of the serial numbers of the units you have in a plain text editor. If the serial numbers are in the list, select your list and copy it all to the clipboard. Otherwise, append the clipboard contents to your list. Select the whole list and save it to the clipboard.

4. Now carry out steps 2 to 4 in the instruction panel. Step 2 will take you to a Web page.



This generator can be used for expanding the available bands of an ODU to additional bands supported by the ODU hardware. Different products have different expansion bands available, please consult the Release Notes document or our Professional Services for more information. Note: The regulatory rulings of certain regions prohibit adding certain bands. Where this is applicable, the License Generator will prevent adding these prohibited bands.

Fill out the form below to generate your License Key. After submitting the form you will receive an email with the new License Key. License Key generation is per serial number, you may enter several serial numbers. Required fields are marked with *. The Reference field is for your own records.The License Key is supported from releases 2.4.50 and 1.9.12

To use it you should login as Installer.

Personal details

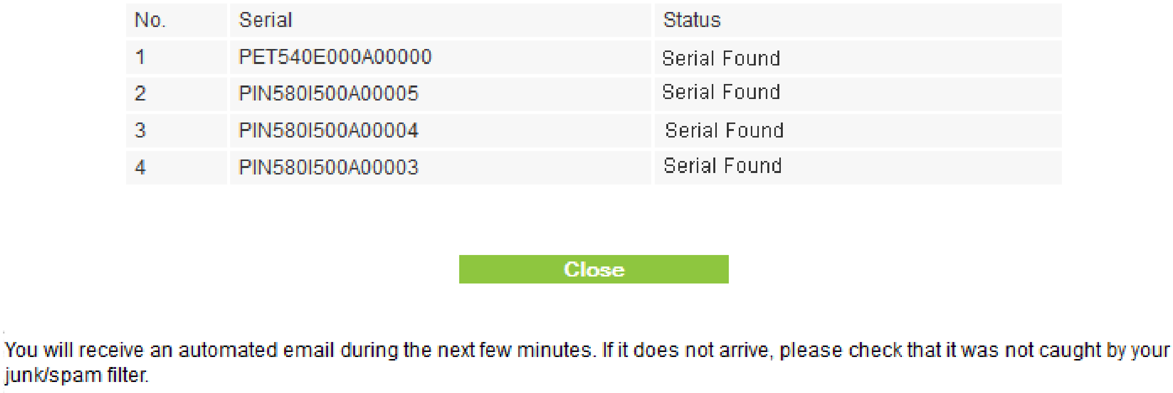
End-User Full Name:*		Company:*	
Address:*		Phone:*	
End-User Email Address:*		Confirm Email:*	
Reference:		Enter Code (9193):*	

Link details

Required Band:* ?	2.3 GHz Universal ▼	Serial Numbers:* ?	
Installation Country:*	Please Select... ▼		

5. Fill out the requested details in the Web page. Click **Get Key** to terminate the dialog box.

6. The results of your request will be displayed with further instructions.



No.	Serial	Status
1	PET540E000A00000	Serial Found
2	PIN580I500A00005	Serial Found
3	PIN580I500A00004	Serial Found
4	PIN580I500A00003	Serial Found

You will receive an automated email during the next few minutes. If it does not arrive, please check that it was not caught by your junk/spam filter.

A few minutes later, you should receive an email containing a list of license keys.

7. Copy and Paste the license keys into a plain text file and save it to a safe known place.

Note

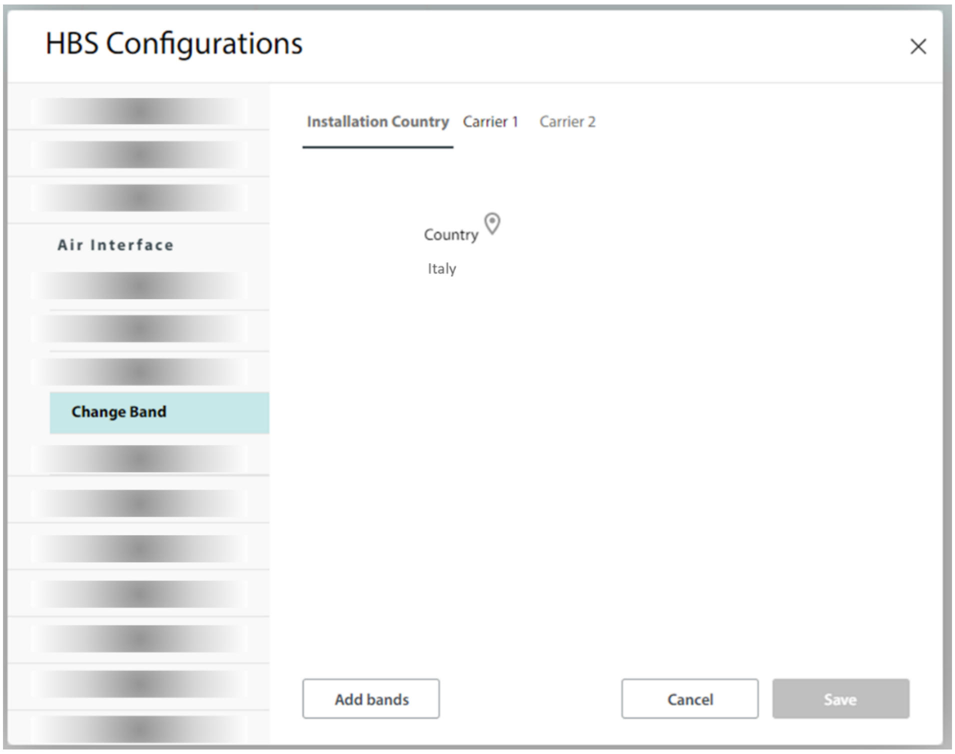
You may see error messages in the Status Column, such as Band not supported or Serial not found. Supported bands typically reflect your local regulations. Check missing serial numbers with the RADWIN Customer Service.

8. Open the Operations -> Licenses window. Check the **License File** button and navigate to the file you saved in the last step.
9. Click Activate. The next time you enter the Change Bands tab, the new bands will be available.

Change country and band for world-wide products

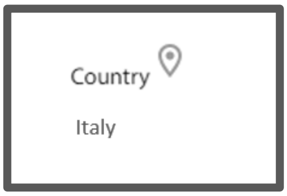
For world-wide products (Jet Air, Jet Air DUO), the allowed frequency bands and transmission restrictions are derived from the regulation that applies to the installation country. The SU receives the operating band and channel from the HBS, and doesn't require its own country setting. See Worldwide single PN products for additional explanation regarding country and regulation detection.

- The country setting is provided in the "**Installation country**" tab under "**Configuration** -> **Air interface** -> **change band**" screen.


HBS Configurations

Country
Italy

- When the HBS detects a GNSS signal, it determines the country and derives the applicable regulation from that country.
    - In this case, the GPS icon near the country displays normal GPS reception, and the county selection is disabled for the user. Example:

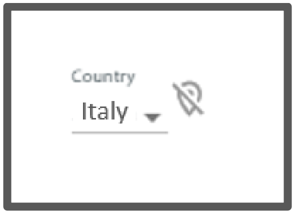


Country

Italy

  - Once the country has been detected once, it is remembered by the HBS regardless of losing GNSS signal afterwards, or of any reboots.

- If a GNSS signal is not detected during HBS boot, the GPS icon near the country displays in “no GPS” state, and manual country selection is possible. Example:



Country

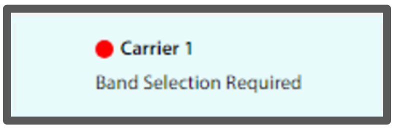
Italy

  - If HBS has been activated already, the previously detected / set country will continue to be applied, and service will resume after the device boot with no need for user intervention.

Note

In order to manually change the country when there is no GPS reception after boot, you must first deactivate the carriers.

  - If the carriers haven’t yet been activated, user must first select a country and then a frequency band in the **Change Band** screen, to allow entering the band activation wizard. The UI will show a notification “Band selection required” under the carrier indication in the main screen.



● Carrier 1

Band Selection Required

Note

After manual country selection, when GNSS signal is detected again, the HBS will automatically update the country to the one detected from GNSS. If you configured a country / band that now becomes not supported in the updated country, the HBS will cease transmission until you select a permitted band. The UI will show a notification “Band selection required” under the carrier indication in the main screen, and issue an active alare “Regulation mismatch” until you select a valid band in the **Change Band** screen.

Therefore, always make sure you select the correct country in order to avoid working in non-permitted bands and to avoid having the service interrupted due to contradiction between the manually selected band and the automatically-detected regulation.

Advanced

This option allows you to configure the Throughput Mode and enable Automatic Carrier Switching.

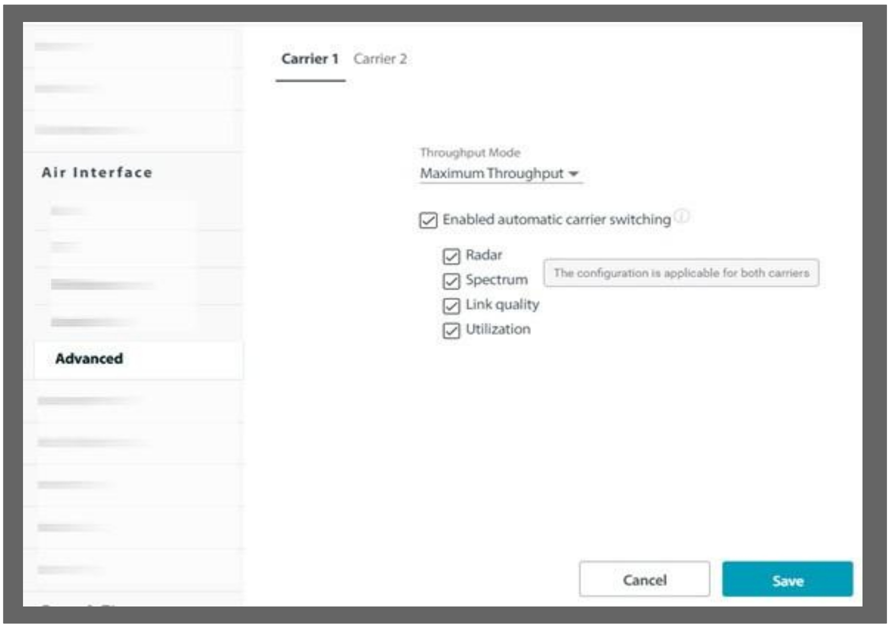
Throughput Mode: This determines how the Adaptive Modulation mechanism works.

- Maximum Throughput (default) should be chosen if throughput is more important than higher delay.
- Optimized Latency minimizes delay at the expense of lower throughput.

Enable Automatic Carrier Switching: Place a checkmark here to enable automatic carrier switching. It is enough to enable this on one of the carriers.

A Carrier Switch occurs according to some or all of these criteria: Radar, Spectrum, Line Quality, or Utilization (See *Carrier Switch* for detailed descriptions of these criteria). You can enable this feature to take into account on any one, some, or all of these criteria by placing a checkmark next to the specific criterion. Note that this feature is only relevant for systems with two carriers of similar bands, and not for the MultiSector Base Station.

(See *Carrier Switch* for more information).



Throughput Mode
Maximum Throughput

☑ Enabled automatic carrier switching

☑ Radar
☑ Spectrum
☑ Link quality
☑ Utilization

The configuration is applicable for both carriers

Click **Save** to have your changes take effect.

2.3.8. Management

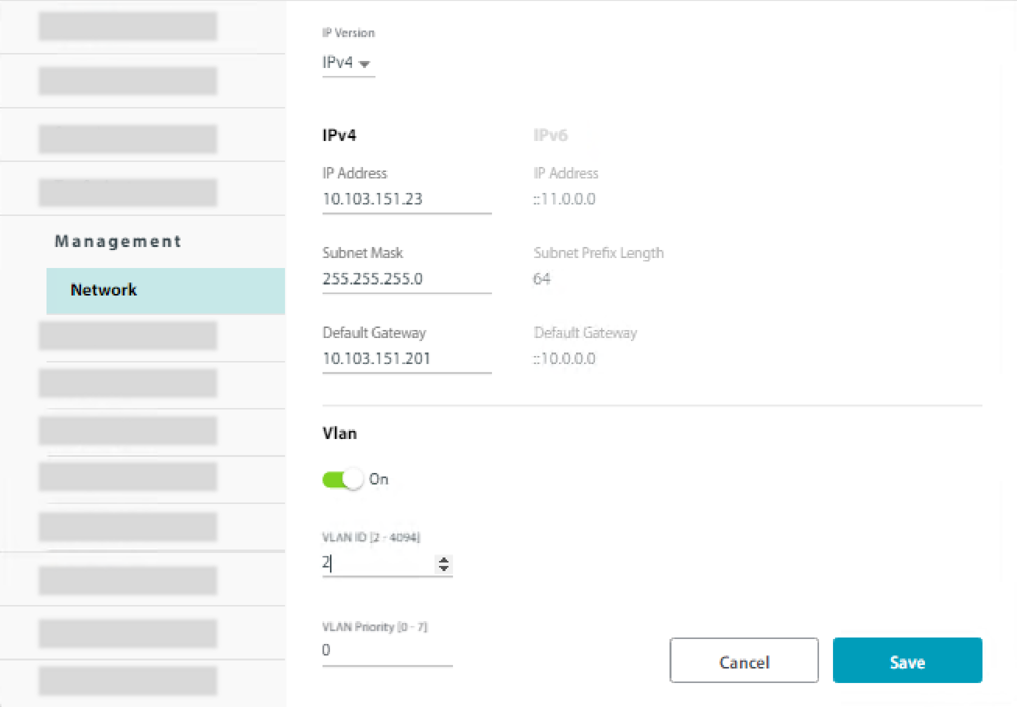
This category enables you to change the IP address, subnet, mask and gateway of the selected device, set its DNS server, configure the management VLAN, set trap destinations, change the management protocol and its authentication mode, add a Syslog server, add or remove user definitions, and configure a RADIUS user authentication server.

Network

Configure management IP address

You may configure a link for IPv4, IPv6, or both. Using both IP versions is useful in conjunction with applications that do not fully support IPv6.

1. Choose what type of IP address to enter (IPv4, IPv6, or both).



IP Version
IPv4

IPv4

IP Address
10.103.151.23

Subnet Mask
255.255.255.0

Default Gateway
10.103.151.201

IPv6

IP Address
::11.0.0.0

Subnet Prefix Length
64

Default Gateway
::10.0.0.0

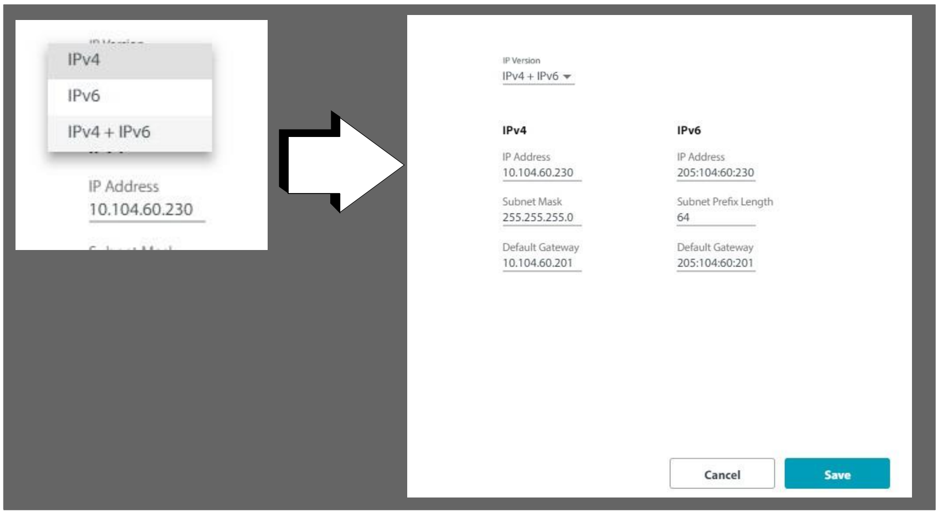
Vlan

On

VLAN ID [2 - 4094]
2

VLAN Priority [0 - 7]
0

Here, we choose both, and enter the IPv6 addresses:



IP Version
IPv4 + IPv6

IPv4

IP Address
10.104.60.230

Subnet Mask
255.255.255.0

Default Gateway
10.104.60.201

IPv6

IP Address
205:104:60:230

Subnet Prefix Length
64

Default Gateway
205:104:60:201

2. Enter the appropriate IP address or addresses, including the Subnet Mask and Default Gateway (for IPv4), and/or the Subnet Prefix Length and Default Gateway (for IPv6).
3. Click **Save**.
4. If you changed any values, you will see a warning message that a device reset will be done. To confirm, click **OK**.

Configure management VLAN

Configure the management VLAN here. To configure a VLAN for traffic, See VLAN.

The management VLAN enables the separation of user traffic from management traffic whenever such separation is required.

To enable VLAN for management:

1. Check ON in the VLAN checkbox.
2. Enter a VLAN ID. Its value should be between 2 and 4094.

   After entering the VLAN ID, only packets with the specified VLAN ID are processed for management purposes by the HBS/SU. This includes all the protocols supported by the radio (ICMP, SNMP, Telnet and NTP). Using VLAN for management traffic affects all types of management connections (local, network and over the air).
3. Enter a Priority number between 0 and 7.

   The VLAN priority is used for the traffic sent from the radio to the managing computer.
4. Change the VLAN ID and Priority of the managing computer NIC to be the same as those of steps 2 and 3 respectively.
5. Click **Save**.

Lost or forgotten VLAN ID or IP Address (Base Station)

If the VLAN ID or IP address of the unit is forgotten, you can carry out the steps shown below to restore the values.

- Set the NIC of the managing computer to a static IP address, using an appropriate Subnet value. Record this subnet value (for eg. 192.168.3.100)
- Open a command line interface, and type

```
ARP -s xxx.yyy.zzz.www 00-15-67-8D-5F-FF
```

Where **xxx.yyy.zzz.www** is an IP address appropriate for the NIC's subnet value.

00-15-67-8D-5F-FF is a unique RADWIN MAC address, and must be entered as-is.

Note that as soon as you enter this command, you have 3 minutes to change whatever needs to be changed on the unit, so do the next few steps quickly:

- Enter the command:

```
ping xxx.yyy.zzz.www
```

You will see several timeout messages. Wait until you see about 3 or 4 of them.

- Enter the command:

```
ARP -d xxx.yyy.zzz.www
```

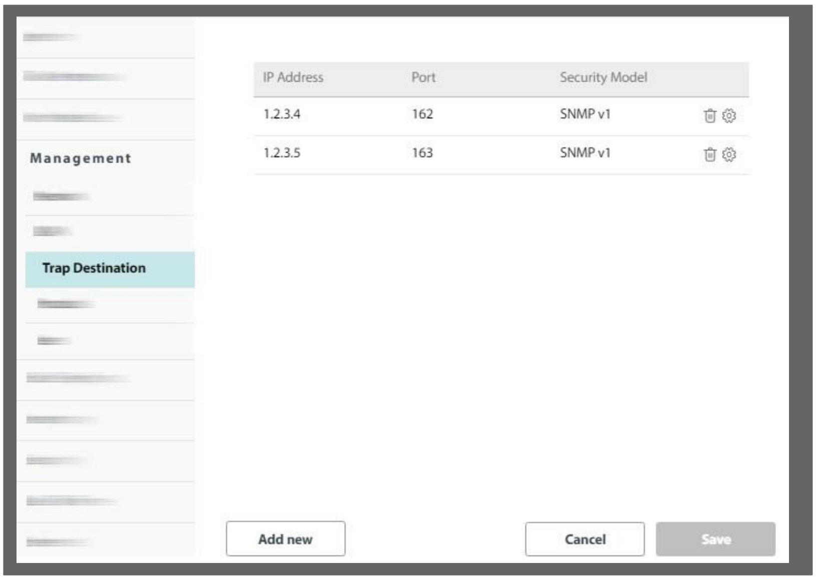
- Open a web browser, and enter **xxx.yyy.zzz.www**

  You will see the welcome message of RADWIN 5000.
- Enter the username and password and click **Login**.
- From the main window, follow the instructions as shown in this document to either change the IP address or record the IP address. Do the same with the VLAN ID, if relevant.

  Note that during this 3-minute window, there is no VLAN tagging for management packets.

Trap Destinations

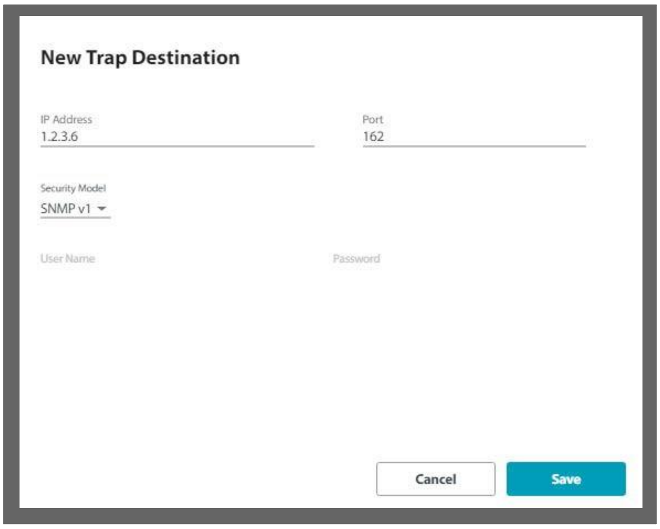
All traps are saved at each location you define.



IP Address	Port	Security Model
1.2.3.4	162	SNMP v1
1.2.3.5	163	SNMP v1

To set a new trap destination:

1. Click **Add new.**
2. In the window that appears, enter the Trap Destination IP Address, Port, and Security Model (SNMP v1 or v3). If choosing SNMP v3, enter the Username and password. The IP address can be the same as the managing computer. The events log will be stored at the address(es) chosen.



New Trap Destination

IP Address: 1.2.3.6

Port: 162

Security Model: SNMP v1

User Name

Password

3. Once you are finished, click **Save** to have your changes take effect.

To change (edit or delete) a trap destination:

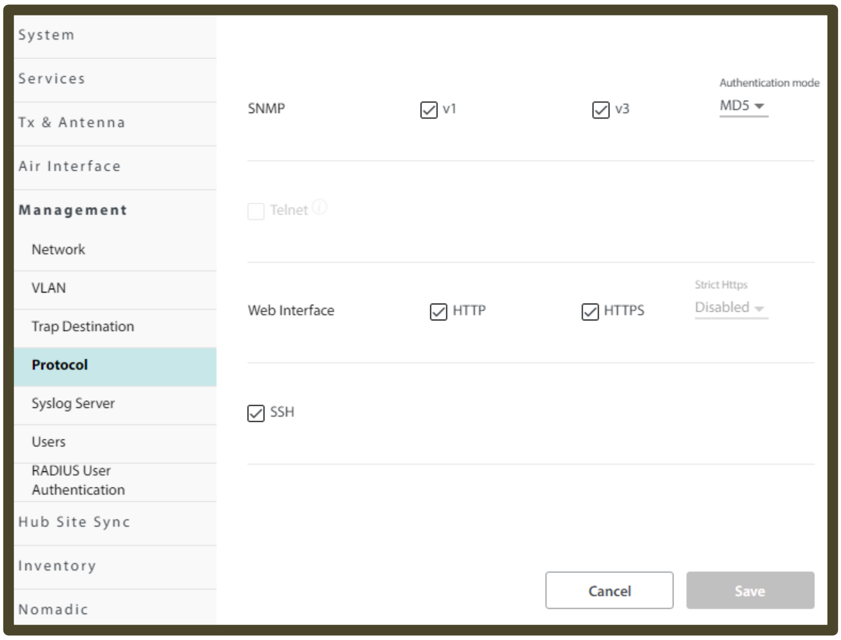
1. To delete a trap destination, click the trash icon (🗑) on the same line as the IP address.
2. To edit a destination, click the configuration icon (⚙) on the same line as the IP address.
3. In the window that appears, update the parameters you wish to change (Trap

Destination IP Address, Port, and/or Security Model). If choosing SNMP v3, enter the username and password. The IP address can be the same as the managing computer. The events log will be stored at the address(es) chosen.

4. Once you are finished, click **Save** to have your changes take effect.

Protocol

You can set the management protocol as well as the authentication mode.



SNMP ☑ v1 ☑ v3 Authentication mode MD5

□ Telnet

Web Interface ☑ HTTP ☑ HTTPS Strict Https Disabled

☑ SSH

SNMP

SNMP support is permanently enabled. You may choose between SNMPv1, SNMPv3 or both.

You can leave the default authentication mode for SNMPv3 as MD5 (message digest algorithm), or change it to SHA1 (secure hash algorithm).

Caution

If you wish to use the RADIUS User Authentication, your SNMP protocol must be v3 only.

Web Interface

- The unit can be configured for HTTP, HTTPS, or both. To do this, place a checkmark in the box next to the protocol you want from the **Web Interface** line.
- The next time you log on to the unit's Web Interface, use the protocol you chose here.
- An admin user must be logged in with HTTPS to make changes in users.

Caution

If you wish to use the RADIUS User Authentication, the Web Interface can only be HTTPS.

Once you are finished, click **Save** to have any changes take effect.

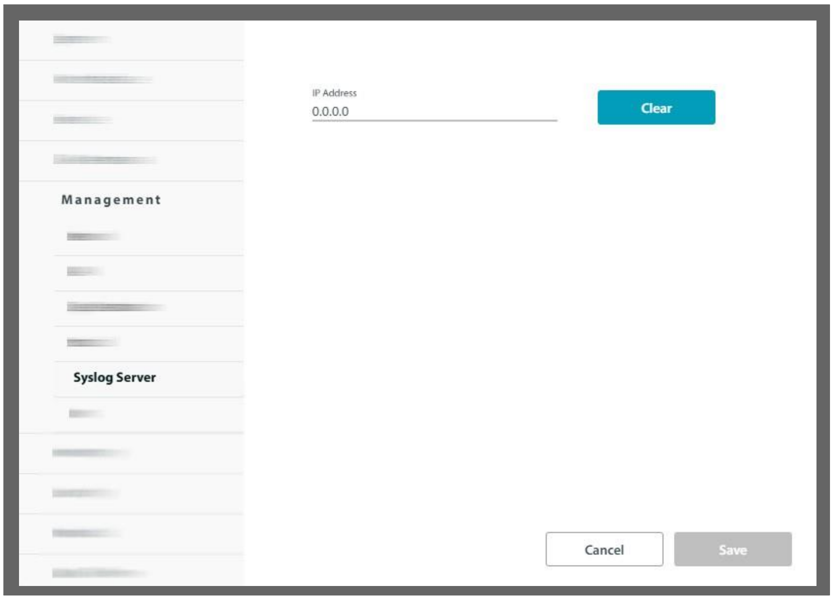
SSH

Turn SSH CLI on or off

For a list of supported CLI commands, See appendix

Syslog Server

This allows you to enter the IP address of a Syslog server to which the specific radio unit sends Syslog messages. This is configured per individual unit.



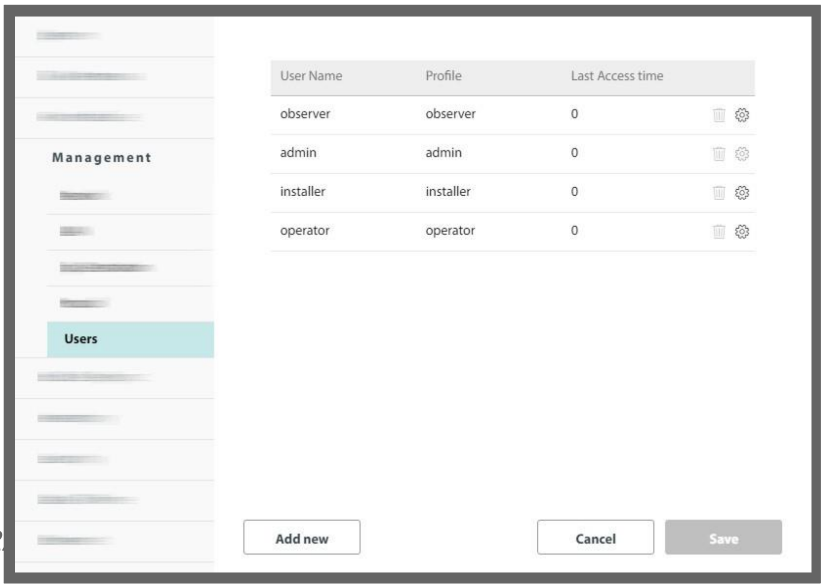
IP Address
0.0.0.0

- Enter the IP Address of the Syslog server. If you wish to change it, click Clear and re-enter the text. It could be the IP address of the managing computer. The Syslog events will be stored at the address chosen.

Once you are finished, click **Save** to have your changes take effect.

Users

Here, an admin user can define users and assign them to a pre-defined category. The admin user must be logged in using HTTPS. Once you define a user, that person can use the username and password to log in.



User Name	Profile	Last Access time
observer	observer	0
admin	admin	0
installer	installer	0
operator	operator	0

Possible user profiles are as follows:

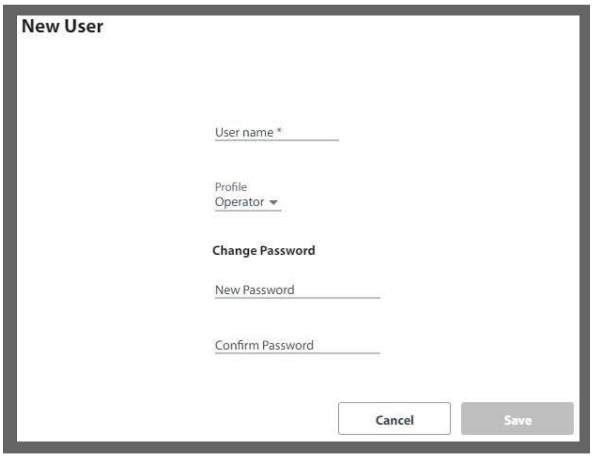
Profile	Default Password	Function
observer	netobserver	Read Only
operator	netpublic	Can install and configure the sector but cannot change the frequency band/regulation.
Installer	netinstaller	Functions as Operator in addition to being able to change the operating frequency and frequency band /regulation, antenna gain and cable loss. Only an Installer can change the antenna gain and cable loss.
Admin	netwireless	Functions as Operator in addition to being able to change new users. Pre-defined users cannot be changed. Can change the operating frequency and frequency band/regulation, and enhance the security mode.

Caution

To add or edit a user, you must be logged in via secure HTTP.
Do this by making sure that HTTPS is selected (from a selected HBS, click the Configure icon, then from Management -> Protocols, select the HTTPS box).
Then, log in using the same IP address as before, but add https:// before its address.

New user:

Click **Add new**, and the New User window will open.

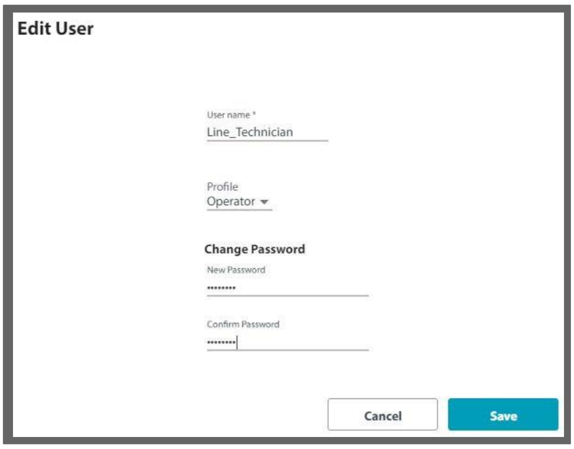


Profile: Operator

1. Enter a convenient name for the new user.
2. Choose the profile for this user. The profile determines what the user can and cannot do.
3. Set the password for this user, and confirm it.
4. Click **Save** to have your changes take effect.
5. You will see the new user in the Users list.

Edit user:

Click the configuration icon (⚙), and the Edit User window will open.



Edit User

User name *
Line_Technician

Profile
Operator

Change Password

New Password
••••••••

Confirm Password
••••••••

1. Change the name, if needed.
2. Change the profile, if needed. This determines what the user can and cannot do.
3. Set the password for this user and confirm it. This must be done no matter what action you take here.
4. Click **Save** to have your changes take effect.
5. You will see the edited user in the Users list.

Remove user:

You cannot remove the pre-defined users.

1. Click on the trash icon (🗑) to remove the user.
2. The user will be removed from the Users list.

RADIUS User Authentication (HBS only)

Caution

You must be logged in using SNMPv3 and via HTTPS for this option to be available (See SNMP).

This option enables you to set lists of individuals and IP addresses that are permitted to manage radio units. The lists consist of a user/permissions list (which uses a RADIUS server), an access control list for IP addresses, or your own “white list”, which does not use a RADIUS server.

Note

This RADIUS option is used to authenticate management access to the radios in the sector. It is **not** used to authorize the various SU radios in the sector. That RADIUS option is described elsewhere (See RADIUS Authorization).

RADIUS User Authentication – Operation

This option uses parameters stored on both the HBS and the RADIUS server as follows:

HBS- based parameters:

» A list of IP addresses from which management access is permitted is stored on the HBS. There are two lists:

- A RADIUS-based Authentication Control List (ACL)
- A non-RADIUS-based “White List”

» SNMP community definition is defined and stored in the HBS[1].

» The HBS then applies this information to each SU in turn.

RADIUS Server-based parameters:

» Username, password and a permissions list are stored in a RADIUS server. This list is in addition to - and independent of - the IP address lists stored in the HBS.

» When logging on, the HBS queries the RADIUS server for this information.

[1] *The SNMP community may be different for the SUs, depending on your system configuration*

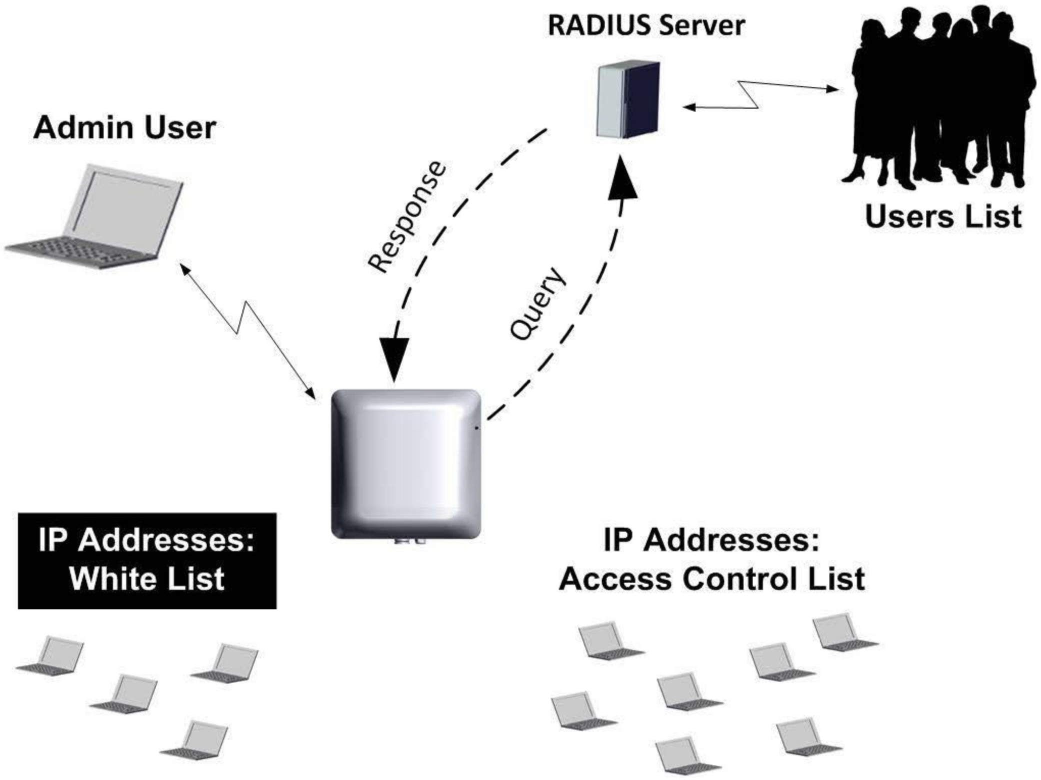


Figure 2-12: RADIUS Authentication set up

Customer Preparations

1. You must supply a server that operates the RADIUS protocol. Make sure you have:
   - The IP address of the RADIUS server.
   - The port of the RADIUS server to which the HBS must connect.
   - The Secret of the RADIUS server.
2. Prepare the following parameters for the RADIUS server:
   a. User profile definitions. These are usually, but not always, confined to the following definitions:
      - HBS Read-Only, SU Read-Only
      - HBS Read-Write, SU Read-Write
      - HBS Read-Only, SU Read-Write

   b. Permitted users. Each one must have:
      - Username
      - Password
      - Timeout value (in seconds)
      - User profile choice
3. Prepare a list of IP addresses for the Access Control List (ACL). This will be a list of IP addresses from which management access to the HBS is permitted. This list is

stored on the HBS, but works only when a RADIUS server is connected, and when the RADIUS authentication mode is enabled.

4. Prepare a “whitelist” of IP addresses. This will be a list of IP addresses from which management access to the HBS is permitted. This list is stored on the HBS, and is independent of a RADIUS server, although it works only when RADIUS authentication mode is enabled.

Prepare Files for the RADIUS Server

Prepare two files for the RADIUS server: Data Dictionary supplement and Users definitions.

Data Dictionary supplement:

This is a supplement to the standard RADIUS Data Dictionary. This file defines the user profiles. Add this text to the end of the standard RADIUS Data Dictionary. An example supplement looks as follows:

```
#vendor id
VENDOR    RADWIN         4458

BEGIN-VENDOR  RADWIN

# User Permissions Profile, the attribute starts with “number”=10 in
# order not to collide with previous RADWIN RADIUS definitions for HSU
# Authorization
ATTRIBUTE RADWIN_UserProfile 10 integer


VALUE RADWIN_UserProfile ObserverHbsObserverHsu  1
VALUE RADWIN_UserProfile AdminHbsAdminHsu   4
VALUE RADWIN_UserProfile InstallerHbsInstallerHsu   5
VALUE RADWIN_UserProfile OperatorHbsOperatorHsu  6
VALUE RADWIN_UserProfile OperatorHbsInstallerHsu   7
VALUE RADWIN_UserProfile ObserverHbsOperatorHsu   8

#ObserverHbsObserverHsu  is identical to ReadOnlyHbsReadOnlyHsu

ATTRIBUTE RADWIN_SessionTimeout 11 integer

END-VENDOR RADWIN
```

The above example shows that the UserProfile is defined as attribute “10”, to differentiate it from other attributes defined in this file.

- The first profile definition is called “1”, the second profile definition is called “4”, the third is “5”, and so on.

Users definitions

The Users file (users.conf) defines the list of users who are allowed to access this sector (HBS), what user profile each one has, and a timeout value (in seconds) after which access is denied. An example appears as follows:

```
# User Name = SectionHead, Password = SunBoss_365, Read-Write
# permissions HBS and HSU, Timeout 24h
SectionHead     Cleartext-Password :=”SunBoss_365”
RADWIN_UserProfile = 4
RADWIN_SessionTimeout = 86400

# User Name = LocalTech, Password = Moon_Crater, Read-Only permissions
# HBS, Read-Write permissions HSU, Timeout 1h
LocalTech     Cleartext-Password := “Moon_Crater”
RADWIN_UserProfile = 1
RADWIN_SessionTimeout = 3600
```

The above example shows that there are two users with the following user names: SectionHead, and LocalTech.

SectionHead has a password = SunBoss_365

His user profile is “4”, meaning he has read and write access to all radios (according to the definition of user profile 4 in the dictionary example shown above).

His timeout value is 86,400 seconds, meaning that he has 24-hour access from the time of his log on. Note that the user will be automatically re-authenticated before this timeout expires.

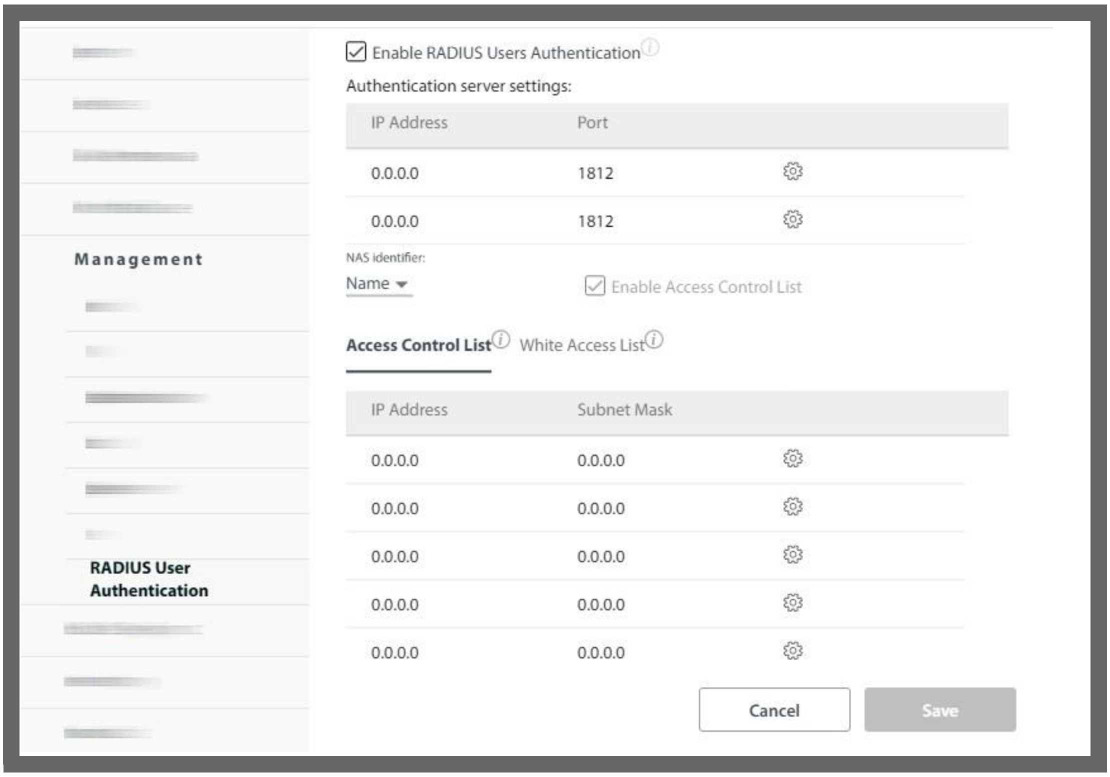
LocalTech has a password = Moon_Crater

His user profile is “1”, meaning he has read-only access to all radios (according to the definition of user profile 1 in the dictionary example shown above).

His timeout value is 3600 seconds, meaning that he has 1-hour access from the time of his log on.

Radius user authentication Configuration

Select the HBS, then from the **Management** option, select **RADIUS User Authentication**.



☑ Enable RADIUS Users Authentication

Authentication server settings:

IP Address	Port	
0.0.0.0	1812	⚙
0.0.0.0	1812	⚙

NAS identifier: Name

☑ Enable Access Control List

IP Address	Subnet Mask	
0.0.0.0	0.0.0.0	⚙
0.0.0.0	0.0.0.0	⚙
0.0.0.0	0.0.0.0	⚙
0.0.0.0	0.0.0.0	⚙
0.0.0.0	0.0.0.0	⚙

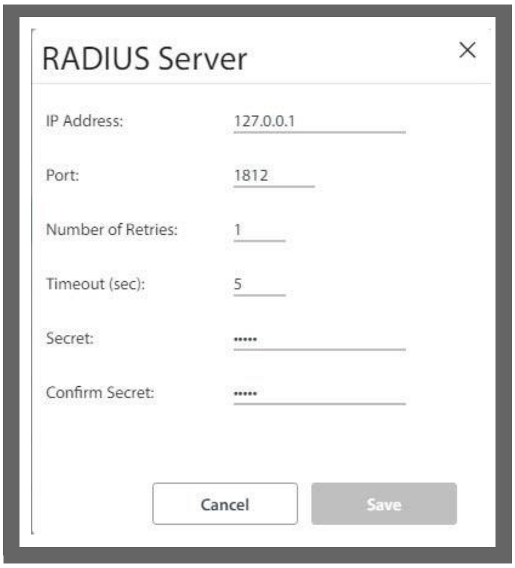
To enable the RADIUS authentication mode, check **Enable RADIUS Users Authentication**.

Note

Any time you enter this configuration page, or when you enable one of the options, you will be reminded that you must run the connectivity check to enable the RADIUS User Authentication option. The connectivity check button appears only after you have entered the connectivity information for the RADIUS server.

Authorization server settings: This shows a list of the available RADIUS servers, their IP addresses, their connection Ports (this is usually 1812), and their Statuses (Check Connectivity, Testing, or Connected), in addition to a configuration button and trash button.

Click the configuration button (⚙) to open the RADIUS server parameters dialog box.


RADIUS Server

IP Address: 127.0.0.1

Port: 1812

Number of Retries: 1

Timeout (sec): 5

Secret: •••••

Confirm Secret: •••••

IP Address: Enter the IP Address of the RADIUS server here.

Port: Enter the communication port to which the HBS connects (usually 1812).

Although you can use the same IP for the different functions of the RADIUS server, you must still use a different port for each function.

Number of Retries: If the first attempt at establishing a connection with the RADIUS server was unsuccessful, carry out this number of retries before moving on to the next available RADIUS server.

Timeout: If there is no response from the RADIUS server after this many seconds, disconnect. A message will appear indicating this situation.

Secret: Secret of the RADIUS server.

Click **Save** to have your changes take effect.

NAS Identifier: If the Access Control List was enabled, then each time the HBS authenticates a user, it reports this fact to the authorization RADIUS server. The report is based on either the Device Name of the HBS or the Device Location, according to your selection in here.

Note

The NAS Identifier Convention chosen here will also change the NAS Identifier Convention for the *802.1x* Authentication option, even though the RADIUS server here and that was used in the *802.1x* Authentication option are not necessarily the same server.

Enable Access Control List: If this is enabled, then only users accessing the system from the IP addresses in the list can access the HBS.

Access Control List

This is a list of IP addresses from which access to the HBS is permitted.

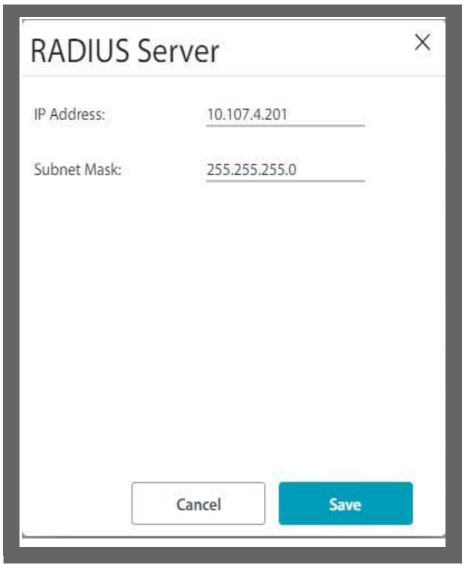
This list is applicable only if both the Enable RADIUS Users Authentication and the Enable Access Control List box have checkmarks in them.

White Access List

This is a list of IP addresses from which access to the HBS is permitted.

Although the HBS does not query the RADIUS server for authentication for this list, this list is nevertheless applicable only if the Enable RADIUS Users Authentication box has a checkmark in it.

- Each item in each of these lists shows an IP address and subnet mask.
- To change or add an item to each of these lists, click the configuration button (⚙) to open the RADIUS server parameters dialog box. In this box, you can only change the IP address and the Subnet Mask of the Access Control List item or the White Access List item:



RADIUS Server

IP Address: 10.107.4.201

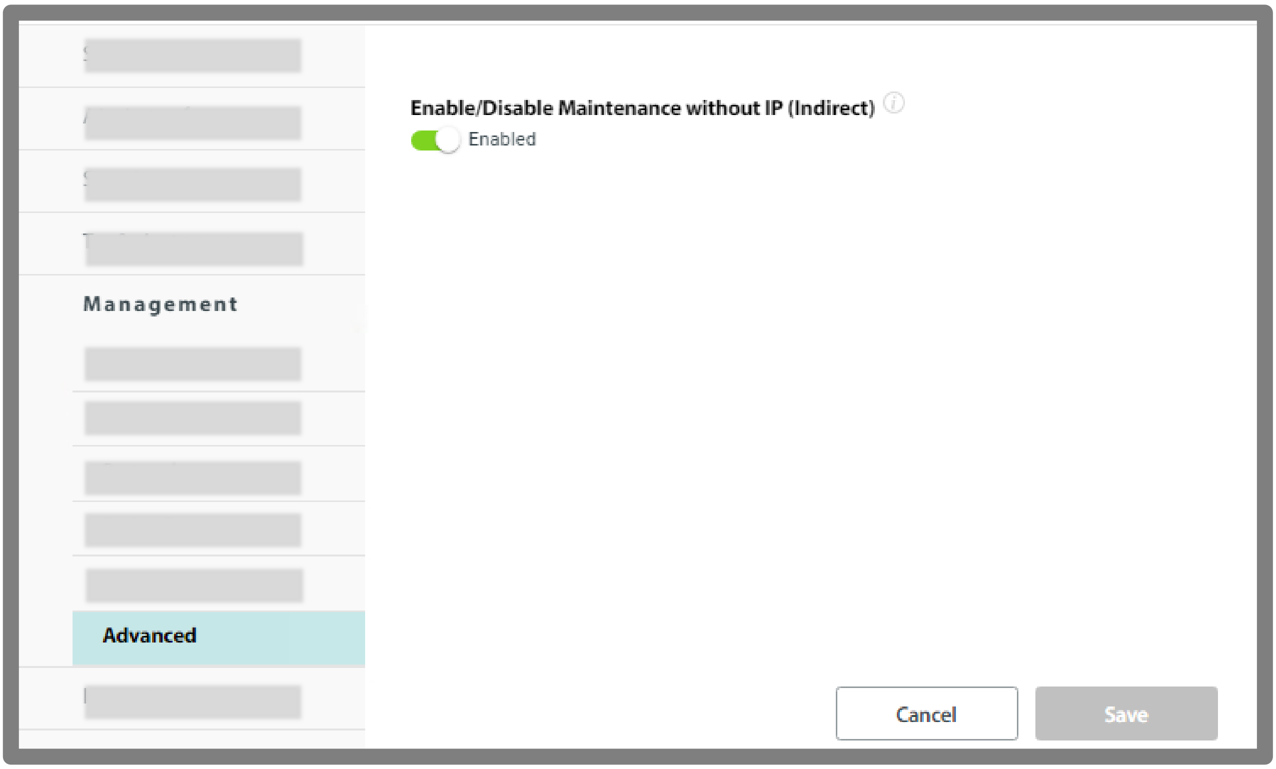
Subnet Mask: 255.255.255.0

- The authorization RADIUS server and the authentication RADIUS server can be either the same or two different servers.
- Click **Save** to have your changes take effect.

Advanced

Enable / Disable maintenance without IP (indirect)

This option enables to perform SW upgrade or backup to SU devices via the BS without using the IP address of the SUs, meaning without having IP connection to the local IP address of the SU. If you don’t use SW upgrade or backup without IP, or wish to disable IP forwarding, disable this option.



Enable/Disable Maintenance without IP (Indirect)

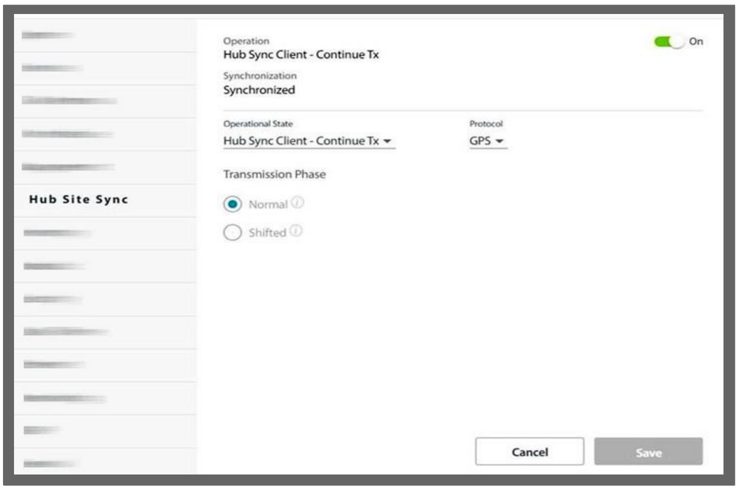
Enabled

2.3.9. Hub Site Sync (HBS only)

If there are co-located radio units with your HBS, they can interfere with each other. The Hub Site Synchronization (HSS) feature prevents this.

To enable Hub Site Synchronization, click **On**.

See the *Hub Site Synchronization Application Note* for more details.



Operation: Hub Sync Client - Continue Tx

Synchronization: Synchronized

Operational State: Hub Sync Client - Continue Tx

Protocol: GPS

Transmission Phase

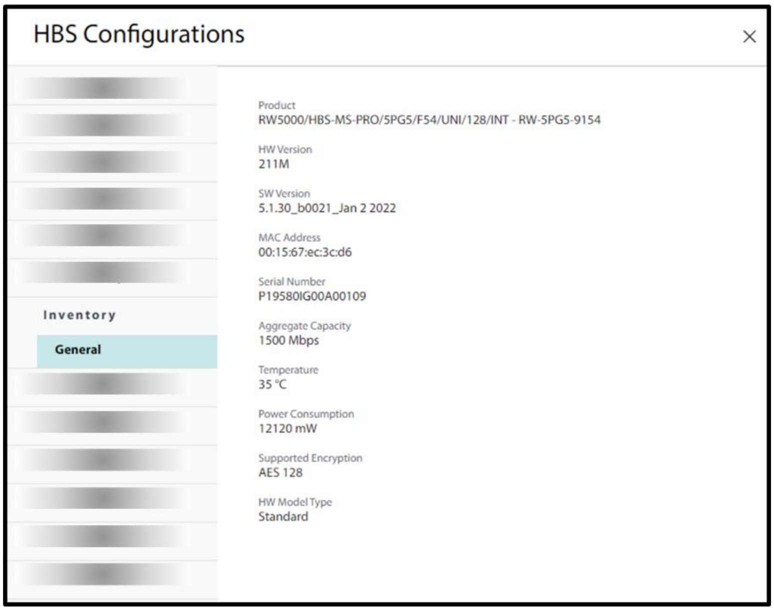
● Normal

○ Shifted

2.3.10. Inventory

This shows the identification information for the selected unit: product version, hardware version and software version, MAC address, serial number, aggregate capacity, the present temperature inside the unit, the unit's power consumption, supported encryption, and hardware motel type and if the Dying Gasp feature is active.

Note you cannot see the IP address here. Go to **Configure -> Management -> Network** to see the IP address of the selected unit.



HBS Configurations

Product
RW5000/HBS-MS-PRO/5PG5/F54/UNI/128/INT - RW-5PG5-9154

HW Version
211M

SW Version
5.1.30_b0021_Jan 2 2022

MAC Address
00:15:67:ec:3c:d6

Serial Number
P19580IG00A00109

Aggregate Capacity
1500 Mbps

Temperature
35 °C

Power Consumption
12120 mW

Supported Encryption
AES 128

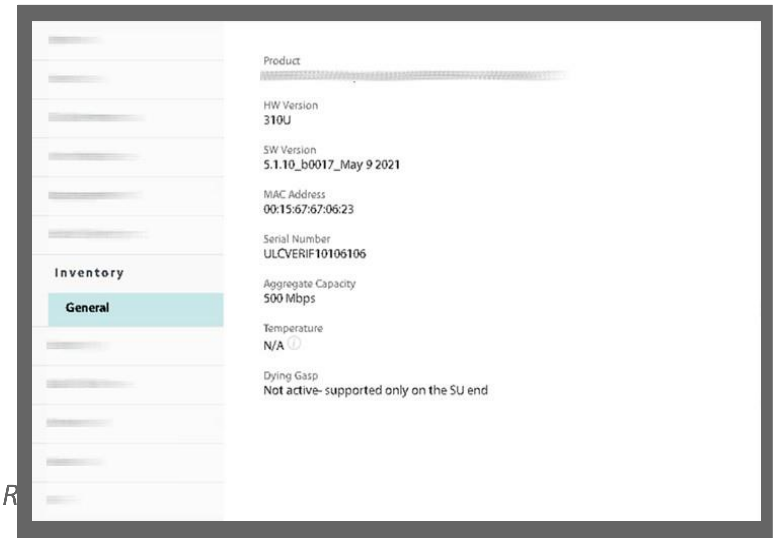
HW Model Type
Standard

Dying Gasp

Dying Gasp feature (supported in SU-Pro only): If the unit was shut down due to a power outage, a signal is sent indicating that the reason for the sync loss is a power outage at the RT-B(HSU) that lost the power. Note the following:

> The Dying Gasp signal is sent from RT-B(HSU) (Slave ODU or Client site) units only.
The signal is not sent from RT-A(HBS) (Master ODU or HUB site) units and is indicated as being not active.

> You must use an appropriate PoE for the RT-B(HSU) unit for the Dying Gasp feature to work. The PoE voltage must be >= 55 V. If the PoE voltage entered to the unit is lower than 50V (such as 24V POE units or voltage degraded over the cable), Dying Gasp will be inactive .



Product
[redacted]

HW Version
310U

SW Version
5.1.10_b0017_May 9 2021

MAC Address
00:15:67:67:06:23

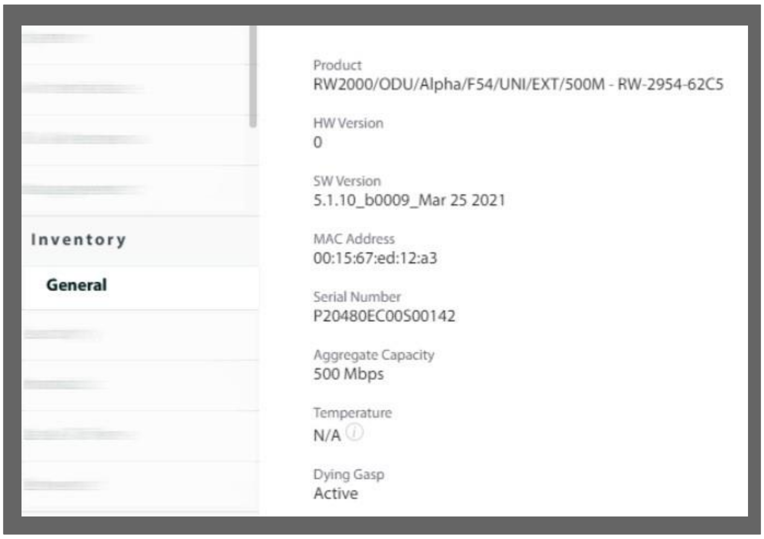
Serial Number
ULCVERIF10106106

Aggregate Capacity
500 Mbps

Temperature
N/A

Dying Gasp
Not active- supported only on the SU end

Dying Gasp on RT-A(HBS): not relevant



Product
RW2000/ODU/Alpha/F54/UNI/EXT/500M - RW-2954-62C5

HW Version
0

SW Version
5.1.10_b0009_Mar 25 2021

MAC Address
00:15:67:ed:12:a3

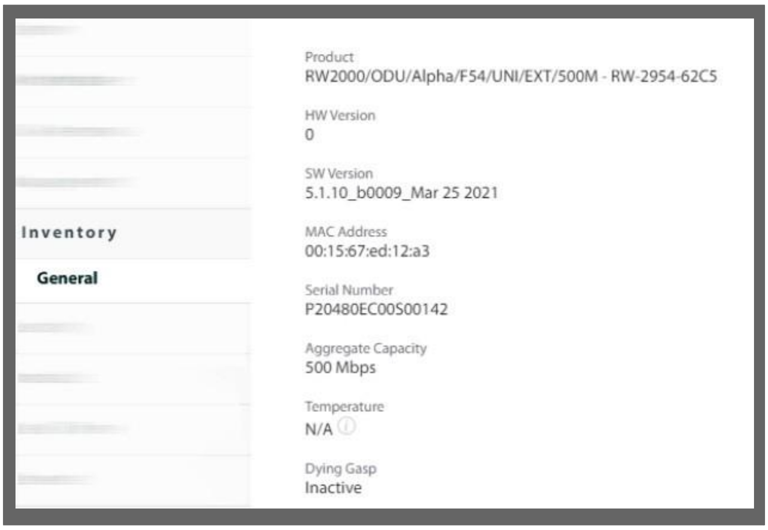
Serial Number
P20480EC00S00142

Aggregate Capacity
500 Mbps

Temperature
N/A

Dying Gasp
Active

Dying Gasp on RT-B(HSU): active



Product
RW2000/ODU/Alpha/F54/UNI/EXT/500M - RW-2954-62C5

HW Version
0

SW Version
5.1.10_b0009_Mar 25 2021

MAC Address
00:15:67:ed:12:a3

Serial Number
P20480EC00S00142

Aggregate Capacity
500 Mbps

Temperature
N/A

Dying Gasp
Inactive

Dying Gasp on RT-B(HSU): Inactive: Low PoE voltage

> Feature supported only when AC (of AC PoE) or DC (on DC PoE) input disconnected since it based also on internal capacitance of PoEs

> Feature supported on PtP and PtMtP (up to 16 CPEs)

2.3.11. Nomadic (HBS)

Each nomadic SU is allocated to one of four HBS levels labelled A, B, C and D. Some operating parameters for each level (such as VLAN, MIR, QoS, resources, fixed rate, Spatial Multiplexing/Diversity antenna mode) can be different for each level allowing for broad prioritization of service between different types of nomadic units. This requires that each nomadic SU be assigned a level to join a sector.

A nomadic SU may only send and receive service traffic while stationary. A nomadic SU detects that it is time to seek another HBS upon sync loss. Upon entering and stopping in a new sector, it may take several seconds to establish sync with the sector HBS.

Note

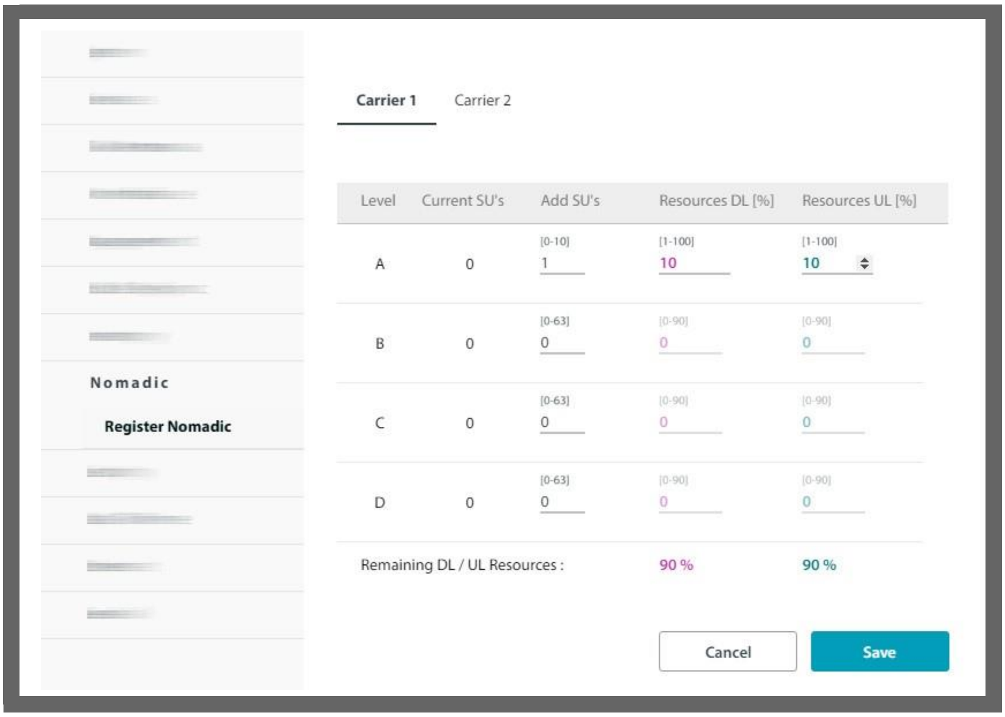
Changing the VLAN, MIR, QoS, fixed rate, or Spatial Multiplexing/Diversity antenna mode for one configured SU at a given level changes all other SUs at that level.

If you add a new SU to a sector (by direct connection) at a given level, at sync time, it will acquire the existing parameters for that level.

To configure nomadic HSUs, you must set up a virtual or "placeholder" SU as nomadic from the HBS. This process is effectively "registering" the placeholder SU. Then access a real SU (either directly or via the HBS), and define it as nomadic. This is done per carrier.

To configure a placeholder nomadic SU:

1. Select the HBS.
2. Click the Configuration icon ().
3. Select **Register Nomadic** from **Nomadic.**
4. Click the Carrier for which you want to add placeholder nomadic SUs.

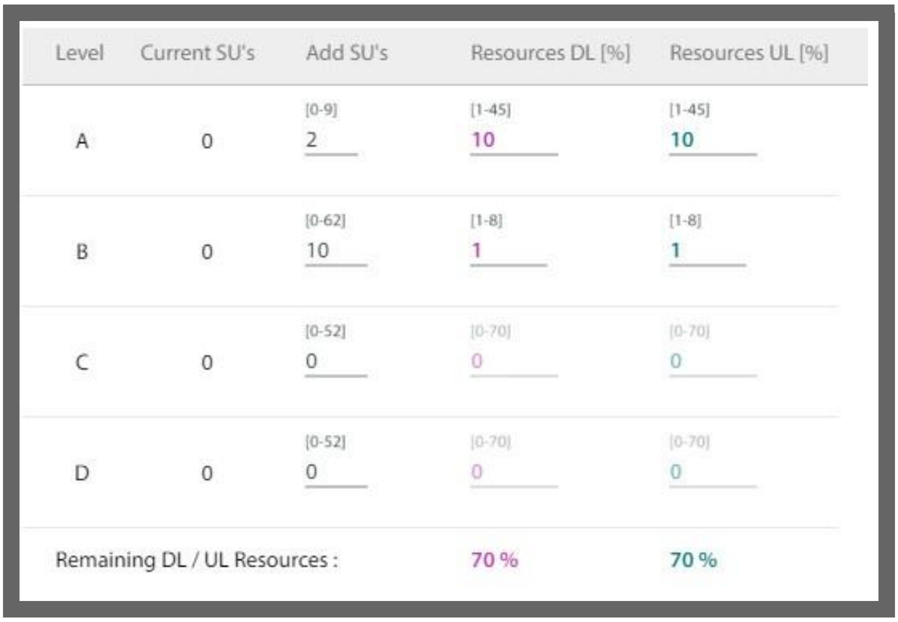


Level	Current SU's	Add SU's	Resources DL [%]	Resources UL [%]
A	0	[0-10] 1	[1-100] 10	[1-100] 10
B	0	[0-63] 0	[0-90] 0	[0-90] 0
C	0	[0-63] 0	[0-90] 0	[0-90] 0
D	0	[0-63] 0	[0-90] 0	[0-90] 0
Remaining DL / UL Resources :			90 %	90 %

5. Choose the level at which to add the placeholder nomadic SU. On that line, set the number of placeholder units to be created under **Add SUs**. Note you can only have up to 10 A level units, but you can have up to 64 B, C, and D level units.
6. Set the **Resources** to be used per unit, in the Downlink (DL) and Uplink (UL) directions, in percentage units. A level units must have at least 10% of the resources in each direction.

   Note the remaining DL/UL resources. When it reaches 0, you cannot add any more placeholder units. Note – as Nomadic requires DL & UL resource allocation, Nomadic doesn't supported by SU-Air or SU in BE mode.

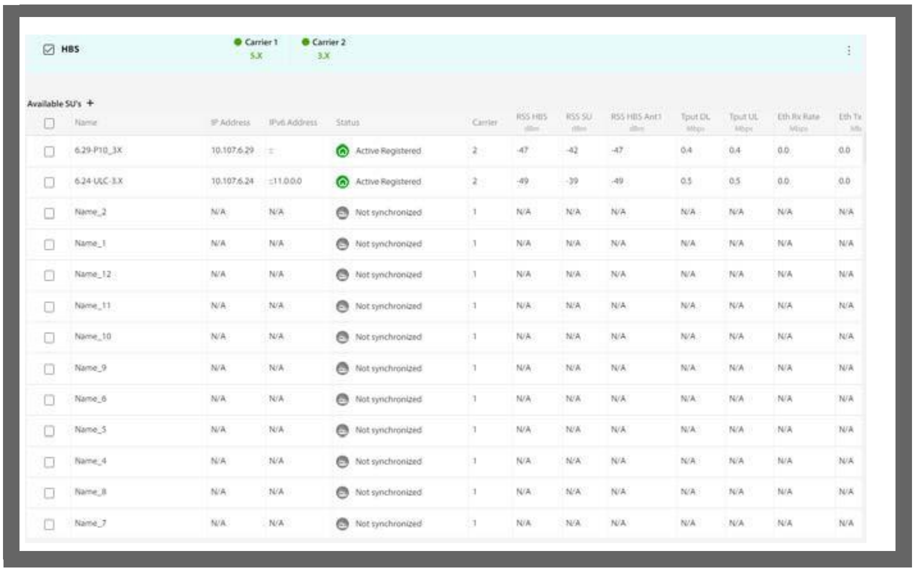
   Example: In the figure below, we are adding 2 level A units, each of which takes up



Level	Current SU's	Add SU's	Resources DL [%]	Resources UL [%]
A	0	[0-9] 2	[1-45] 10	[1-45] 10
B	0	[0-62] 10	[1-8] 1	[1-8] 1
C	0	[0-52] 0	[0-70] 0	[0-70] 0
D	0	[0-52] 0	[0-70] 0	[0-70] 0
Remaining DL / UL Resources :			70 %	70 %

10% of the resources (total 20%), and 10 Level B units, each of which takes up 1% of the resources (total 10%). The total resources taken up is therefore 30%, and the Remaining DL/UL Resources are 70%.

We click **Save**, then look at the main window of the GUI, where we can see many placeholder nomadic SUs have been added:



☑ HBS

● Carrier 1 5.X ● Carrier 2 3.X

Available SU's +

□	Name	IP Address	IPv6 Address	Status	Carrier	RSS HBS dBm	RSS SU dBm	RSS HBS Ant1 dBm	Tput DL Mbps	Tput UL Mbps	Eth Rx Rate Mbps	Eth Tx
□	6.29-P10_3X	10.107.6.29	::	Active Registered	2	-47	-42	-47	0.4	0.4	0.0	0.0
□	6.24-ULC-3.X	10.107.6.24	::11.0.0.0	Active Registered	2	-49	-39	-49	0.5	0.5	0.0	0.0
□	Name_2	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A
□	Name_1	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A
□	Name_12	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A
□	Name_11	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A
□	Name_10	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A
□	Name_9	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A
□	Name_6	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A
□	Name_5	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A
□	Name_4	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A
□	Name_8	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A
□	Name_7	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A

At this point, we can now define existing SUs as nomadic, from the SU itself, either via the HBS or directly.

7. Click **Save** to have your changes take effect.

2.3.12. Nomadic (SU)

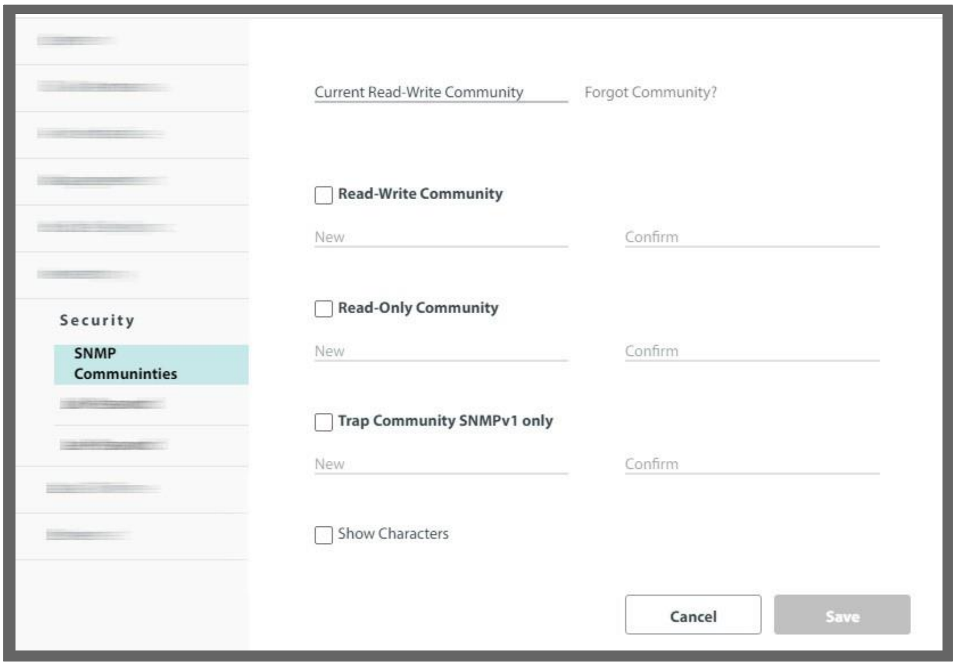
For a full description of configuring an SU as Nomadic, See *Nomadic*.

2.3.13. Security

The Security dialog enables you to change the SNMP Community strings, Link and User passwords (function for the HBS only), Security Mode (function for the SU only, See Security Mode), Secured Sync, and 802.1x authentication option.

SNMP Communities

If the selected unit is an HBS, you can also create an encrypted SNMP Community string value file.



Security

SNMP Communinties

Current Read-Write Community

Forgot Community?

□ Read-Write Community

New

Confirm

□ Read-Only Community

New

Confirm

□ Trap Community SNMPv1 only

New

Confirm

□ Show Characters

Each radio unit communicates with the managing computer using the SNMPv1 or SNMPv3 protocol. The SNMPv1 protocol defines three types of communities:

- Read-only for retrieving information from the radio unit.
- Read-write to configure and control the radio unit.
- Trap used by the radio unit to issue traps.

The read-write community strings and read-only community strings have a minimum of five alphanumeric characters. Changing the trap community is optional.

Editing SNMPv1 Community Strings

When editing these strings, both read-write and read-only communities must be defined.

To change a community string:

1. Type the current read-write community in the **Current Read-Write Community** field (default is *netman*).
2. Click the check box next to the community whose string you wish to change.
3. Type the new community string and re-type to confirm. A community string must contain at least five and no more than 32 characters excluding SPACE, TAB, and any of “>#@|*?;."
4. Click **Save** to have your changes take effect.

Link Password (HBS only)

The link Password enables enhanced security for the link. It is not the same as the user password.

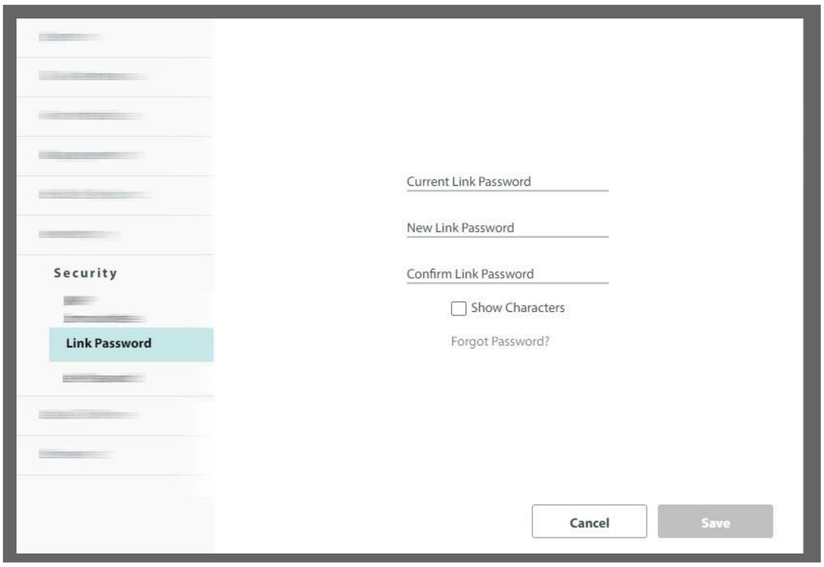
This item is available as follows:

- At an isolated HBS (No active SUs).
- At an isolated SU.
- Never for an active SU.

The default password is *wireless-p2mp*.

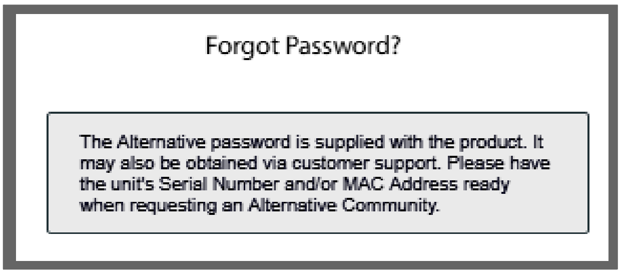
To change the link password:

1. Select **Security -> link Password**. The link Password dialog box opens.



2. Enter the current link password (The default link password for a new unit is *wireless-p2mp*).

   If you have forgotten the link Password, place the cursor over **Forgot Password?, and following the instructions in the tool tip that appears:**



Forgot Password?

The Alternative password is supplied with the product. It may also be obtained via customer support. Please have the unit's Serial Number and/or MAC Address ready when requesting an Alternative Community.

3. Enter a new password.
4. Retype the new password in the Confirm field.
5. Click Save.
6. Click Yes when asked if you want to change the link password.
7. Click OK at the *Password changed* success message.

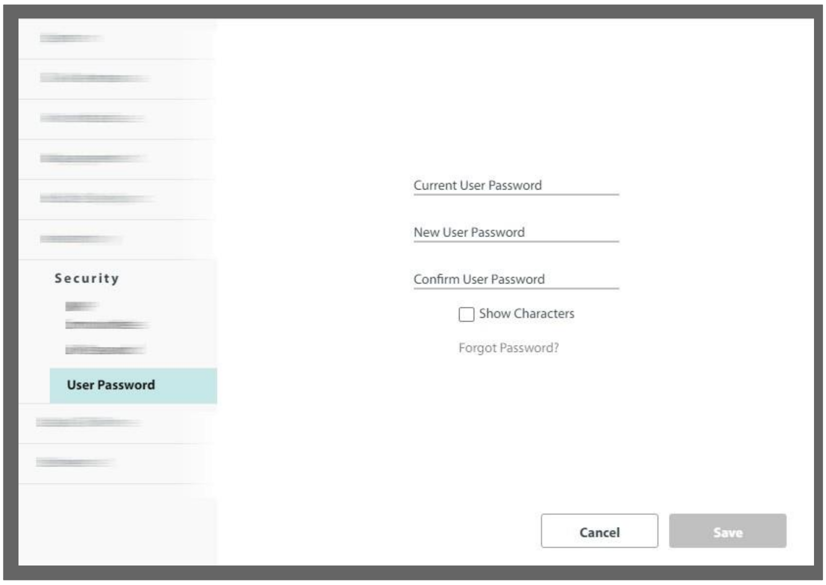
Note

- A link password must contain at least eight but no more than 16 characters, excluding SPACE, TAB, and any of “>#@|*?;.”.
- Restoring Factory Defaults returns the link Password to *wireless-p2mp*.

User Password (HBS or SU directly)

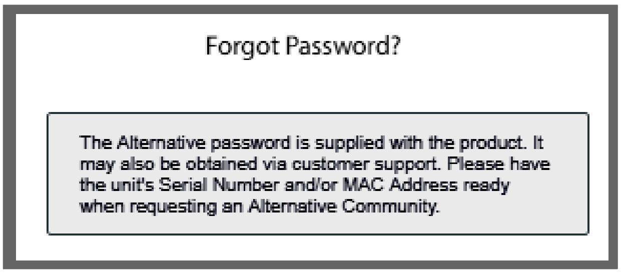
To change the user password of the present user:

1. Select **Security -> User Password**. The User Password dialog box opens.



2. Enter the current password.

   If you have forgotten the password, click **Forgot Password? and following the instructions in the tool tip that appears:**



Forgot Password?

The Alternative password is supplied with the product. It may also be obtained via customer support. Please have the unit's Serial Number and/or MAC Address ready when requesting an Alternative Community.

3. Enter a new password.
4. Retype the new password in the Confirm field.
5. Click Save.
6. Click Yes when asked if you want to change the password.
7. Click OK at the *Password changed* success message.

Note

- A user password must contain at least eight but no more than 16 characters excluding SPACE, TAB, and any of “>#@|*?;.”.

Security Mode (SU only)

This is an enhanced version of the usual secured method of working, which offers extra protection against unauthorized access of the system.

It is performed on a unit-by-unit basis, and is independent of sector structure or hierarchy[1].

Implement this mode as follows:

1. Change the SNMP management interface to SNMPv3:

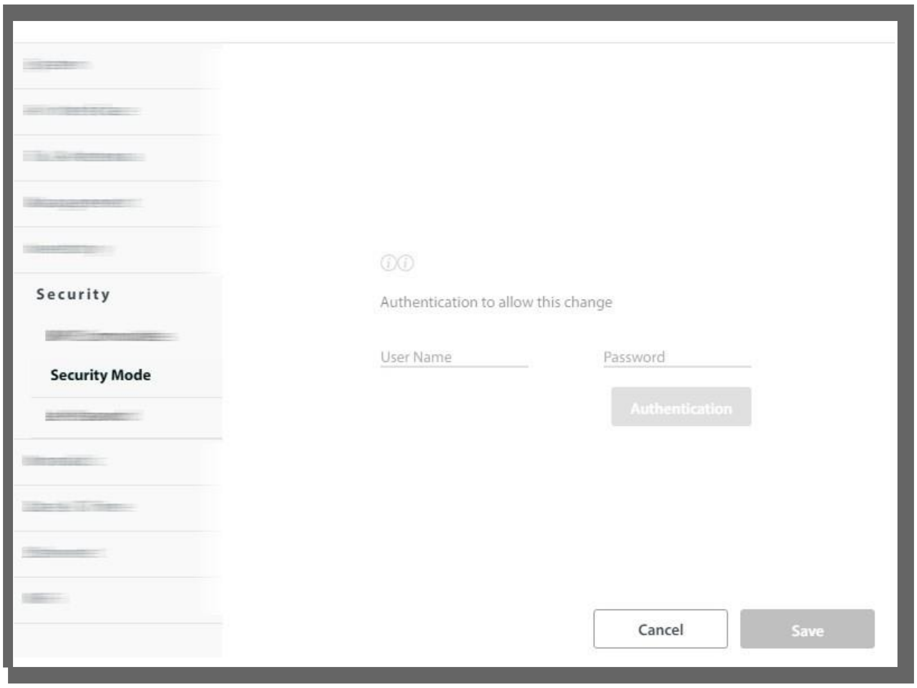
   Select **Configuration -> Management -> Protocol.**

   a. Choose the SNMPv3 radio button. Choose SNMPv3 only, not “V1 and V3”.

   b. You can use either the MD5 or SHA1 authentication mode

   c. Click Save. You will be asked to log in again. Make sure you have the proper SNMPv3 user name and password.

2. Select Configuration -> Security -> Security Mode.



3. Enter the SNMPv3 username and password, and click Authentication.

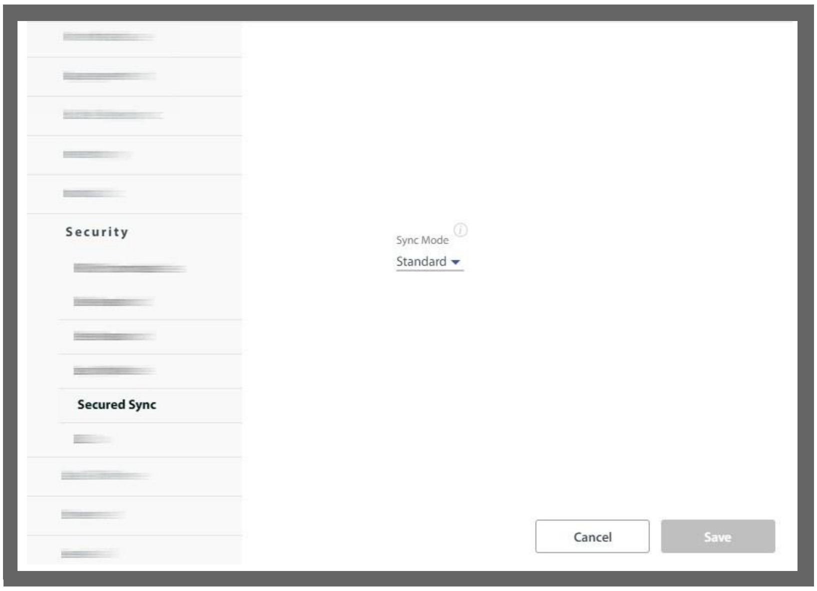
4. Click **Save**.

[1] *When configuring one unit for SNMPv3 and Enhanced Security, its counterpart must also be configured for SNMPv3, but it doesn’t need to be configured with Enhanced Security.*

Secured Sync

This determines whether the SU must have the same Network ID as the HBS to establish a link. The Network ID is the first 4 digits of the Sector ID (See Radio (HBS option) for instructions on configuring the SU’s Network ID).

1. From **Security -> Secured Sync**, choose the sync mode from the pull-down menu.



Sync Mode
Standard

2. Click **Save**.

Caution

If the Secured Sync Type is Secured Network ID, and the wrong Network ID was entered in the SU, the unit will not establish a link and will be prevented from doing so for 10 minutes. Correct the Network ID, and at the end of this 10-minute period, the SU will be able to synchronize with the HBS.

802.1x

This is a port-based Network Access Control (PNAC) authentication mechanism based on the IEEE 802.1x standard. This mechanism involves three parties: a supplicant, an authenticator, and an authentication RADIUS server.

In the RADWIN implementation, the supplicant is the customer site equipment (CSE) the authenticator is the SU ***PRO/AIR*** EMB or SU Integrated & HBS[1], and the authentication server is a customer-supplied RADIUS server. This works as follows:

1. The authenticator requests credentials from the supplicant (CSE). Usually a username and password.
2. The supplicant (CSE) supplies these credentials to the authenticator.
3. The authenticator forwards these credentials to the authentication RADIUS server.
4. The authentication RADIUS server provides a response to the authenticator - approved or not approved.

[1] *This feature works with the SU **PRO/AIR** EMB or SU Integrated as the subscriber unit only.*

5. The authenticator then either enables the supplicant (CSE) to connect or disables it from connecting.

Note

You must configure your authentication RADIUS server to recognize the credentials of the CSE.

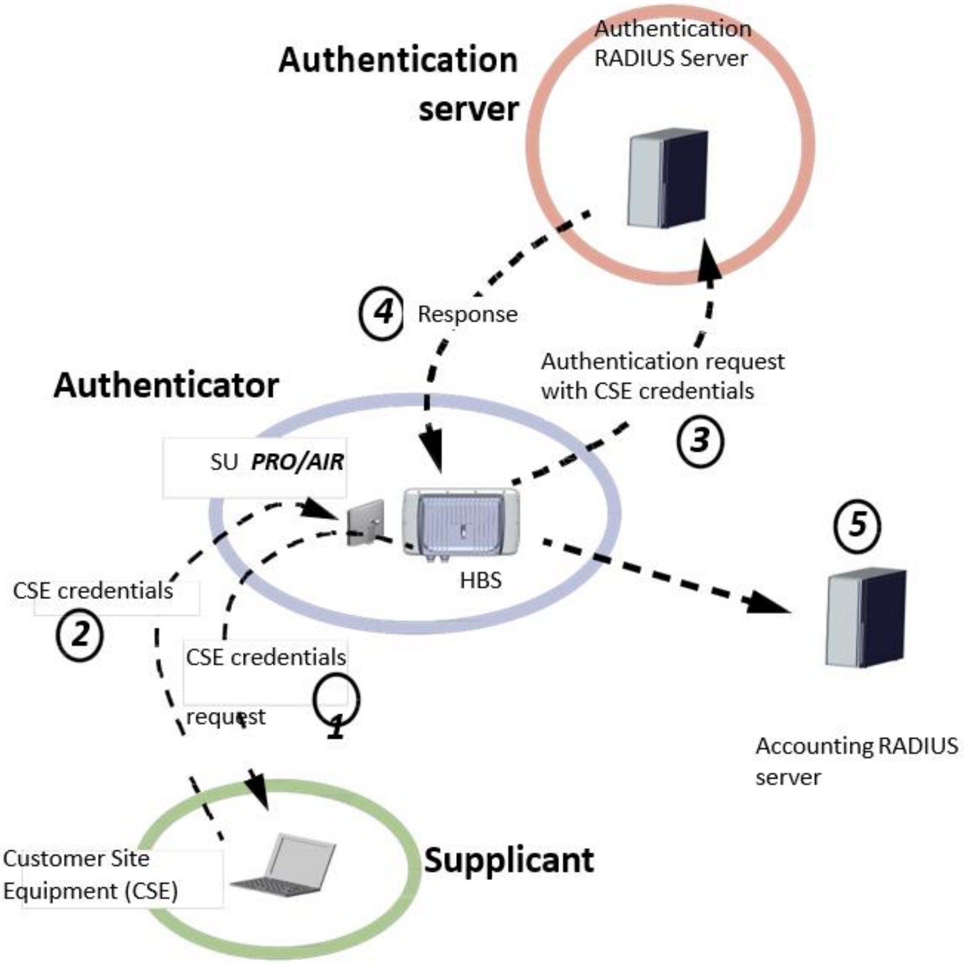
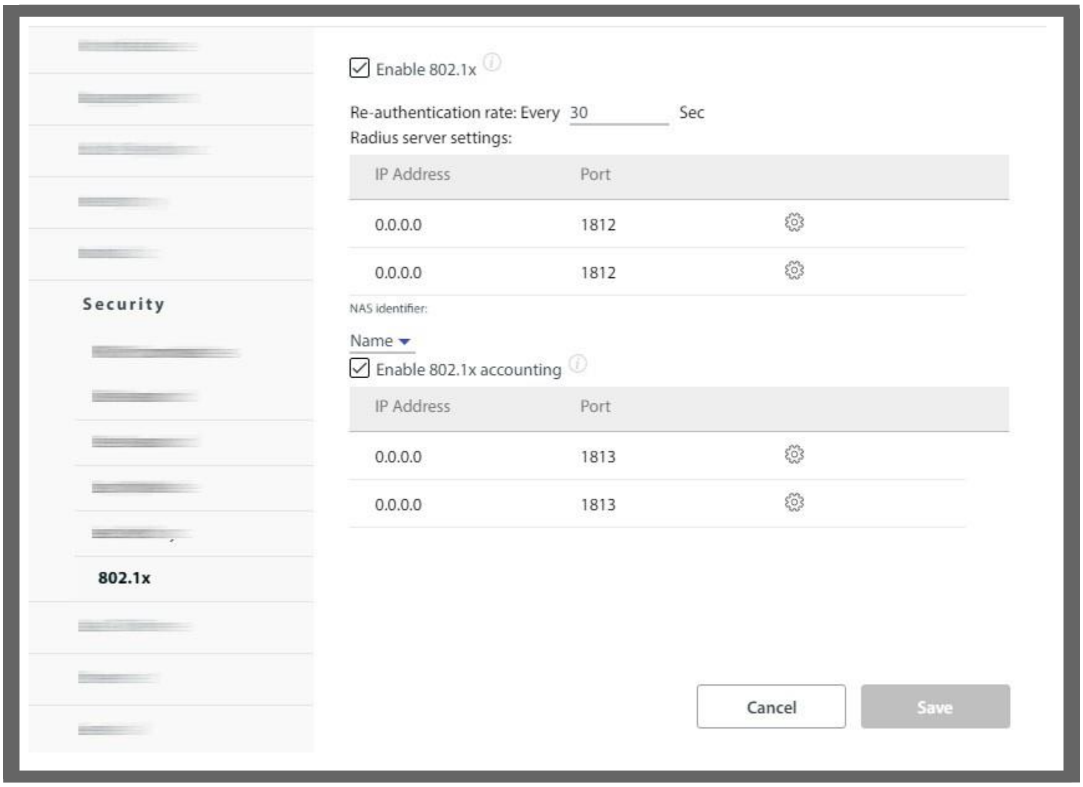


Figure 2-13: 802.1x Authentication & Accounting Scheme

Configure this feature as follows:

1. Select the HBS, then from the **Security** option, select **802.1x**.



Security

802.1x

☑ Enable 802.1x

Re-authentication rate: Every 30 Sec

Radius server settings:

IP Address	Port	
0.0.0.0	1812	⚙
0.0.0.0	1812	⚙

NAS identifier:

Name ▾

☑ Enable 802.1x accounting

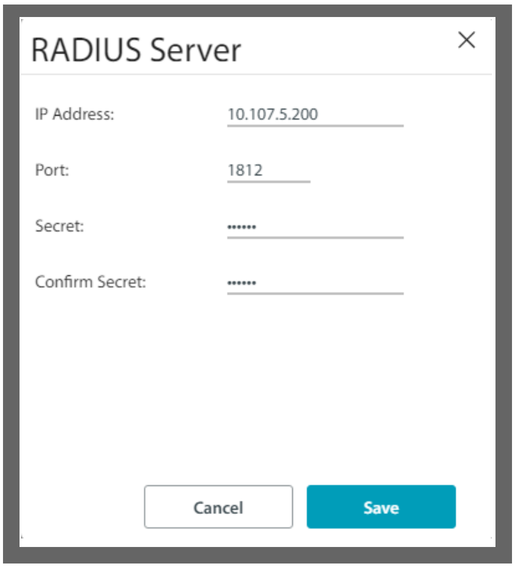
IP Address	Port	
0.0.0.0	1813	⚙
0.0.0.0	1813	⚙

2. To enable the 802.1x authentication mode, check **Enable 802.1x**.
3. Next to **Re-authentication rate**, choose how often the authentication process is done (in seconds). The more often you choose to undertake this process, the better the security, but it requires more resources.
4. **RADIUS server settings:** This shows a list of the available RADIUS servers, their IP addresses, their connection Ports (this is usually 1812), and their Statuses (Check Connectivity, Testing, or Connected), in addition to a configuration button and trash button.

Note

Any time you enter this configuration page, or when you enable one of the options, you will be reminded that you must run the connectivity check to enable the 802.1x option. The connectivity check button will only appear once you have entered all connectivity parameters for the RADIUS server.

5. Click the configuration button (⚙) to open the RADIUS server parameters dialog box.



RADIUS Server

IP Address: 10.107.5.200

Port: 1812

Secret: ••••••

Confirm Secret: ••••••

IP Address: Enter the IP Address of the RADIUS server here.

Port: Enter the communication port to which the HBS connects (usually 1812).

Although you can use the same IP for the different functions of the RADIUS server, you must still use a different port for each function.

Secret: Secret of the RADIUS server.

Click **Save** to have your changes take effect.

6. **NAS Identifier**: If Enable 802.1x accounting is enabled, this determines what basis the report of the identity of the supplicants is made: by the Device Name of the supplicant or the Device Location.

Note

The NAS Identifier Convention chosen here will also change the NAS Identifier Convention for the *RADIUS User Authentication* option, even though the RADIUS server here and that was used in the *RADIUS User Authentication* option are not necessarily the same server.

7. **Enable 802.1x accounting**: If this is enabled, then the system will forward the identity of the supplicants who have supplied credentials to the accounting RADIUS server. This can be the same RADIUS server as the authentication server.
8. Click the configuration button (⚙) to open the RADIUS server parameters dialog box to define the parameters of the 802.1x RADIUS accounting server.
9. Click **Save** to have your changes take effect.

2.3.14. Date & Time

Here you can set the date and time of the selected unit manually based on local time or on an NTP Server.

The radio unit maintains a date and time. The date and time should be synchronized with any Network Time Protocol (NTP) version 3 compatible server.

During power-up the radio attempts to configure the initial date and time using an NTP Server. If the server IP address is not configured or is not reachable, a default time is set.

When configuring the NTP Server IP address, also configure the offset from the Universal

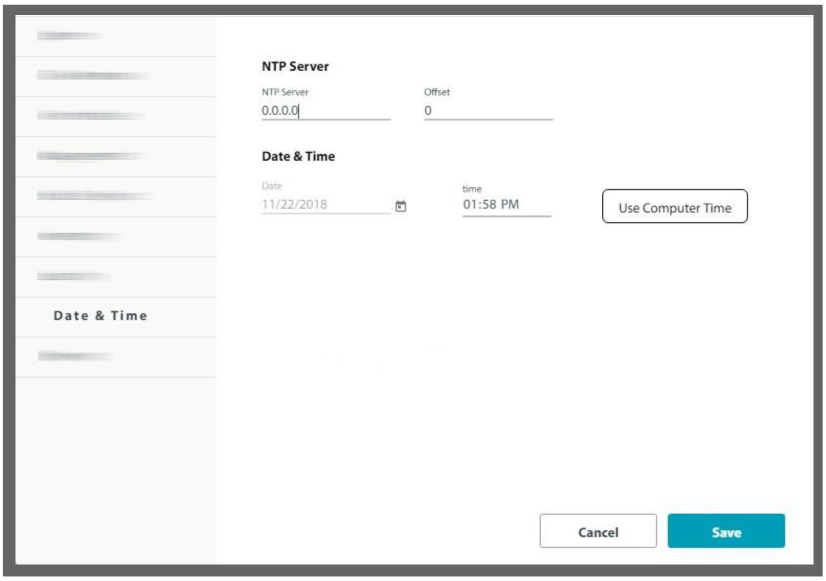
Coordinated Time (UTC). If there is no server available, you can either set the date and time, or you can set it to use the date and time from the managing computer. Note that manual setting is not recommended since it will be overridden by a reset, power up, or synchronization with an NTP Server.

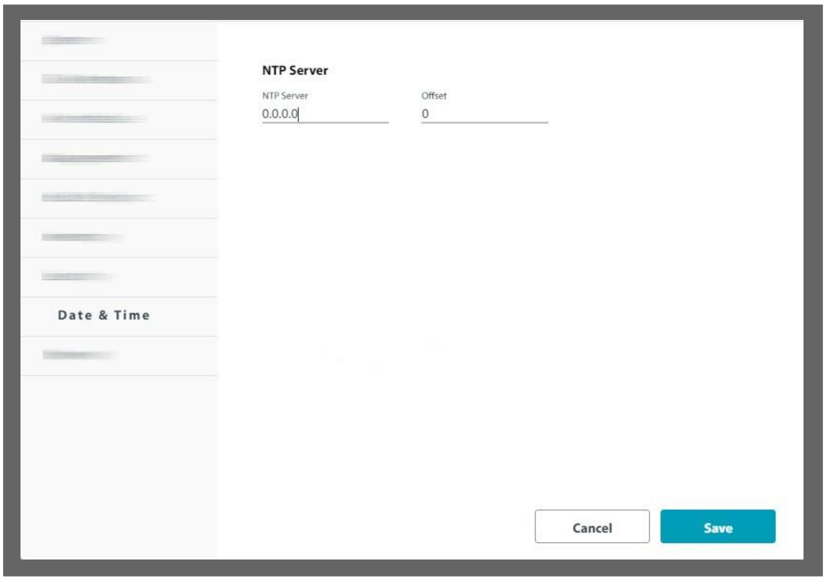
Note

The NTP uses UDP port 123. If a firewall is configured between the radio and the NTP Server, this port must be opened.
It can take up to 8 minutes for the NTP to synchronize the radio date and time.

To set the date and time:

1. Determine the IP address of the NTP server to be used.
2. Test it for connectivity using the command (Windows XP and 7), for example: w32tm /stripchart /computer:216.218.192.202


NTP Server
NTP Server: 0.0.0.0
Offset: 0
Date & Time
Date: 11/22/2018
time: 01:58 PM


NTP Server
NTP Server: 0.0.0.0
Offset: 0

3. If entering an IP address for the NTP Server, enter the new address.
4. Set your site Offset value in minutes ahead or behind GMT[1].
5. To manually set the date and time, click the calendar icon and choose the new date, then click the spinner next to Time to choose the time.

6. To set the time based on the time of the managing computer, click Use Computer Time.
7. Click **Save** to have your changes take effect.

2.3.15. Ethernet

In this category, you can configure the input ports on the unit, the Bridge Table, broadcast and multicast flooding protection, and the DHCP option.

LAN Ports

- LAN1 refers to the input port on the radio unit. This port can be labeled “PoE IN”, “PoE”, or not labeled at all (depending on your product), and can carry data as well as power.
- SFP refers to the port on the radio unit labeled “LAN” or “SFP” or not labeled at all (depending on your product) and functions as an SFP port which can carry data only.

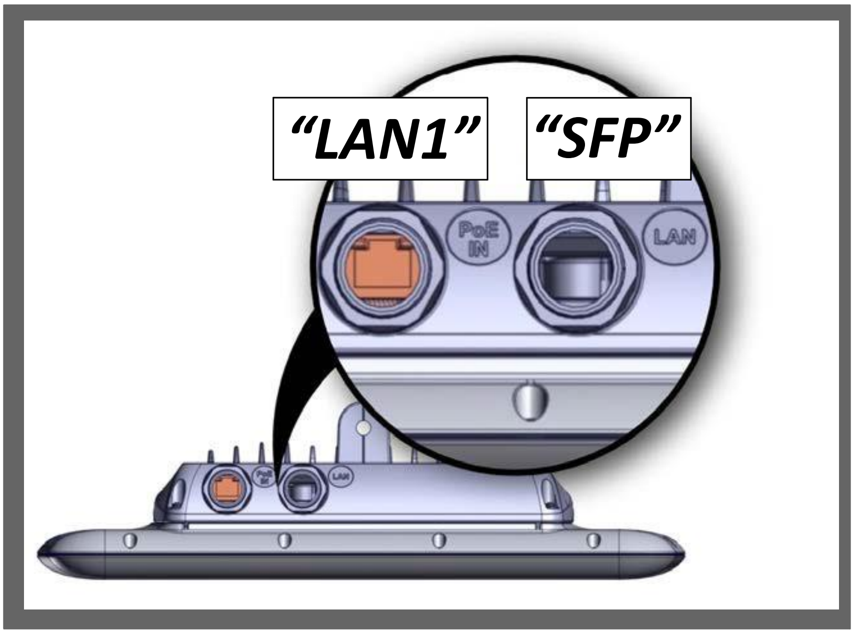


Figure 2-14: Port labeling on JET, NEO, and JET-DUO 3/5 GHz units

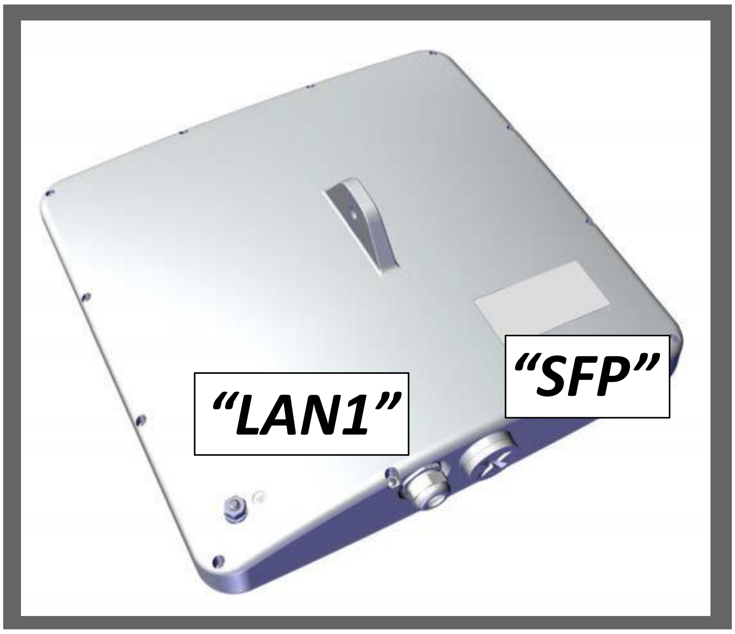


Figure 2-15: Ports are not labeled on NEO DUO units

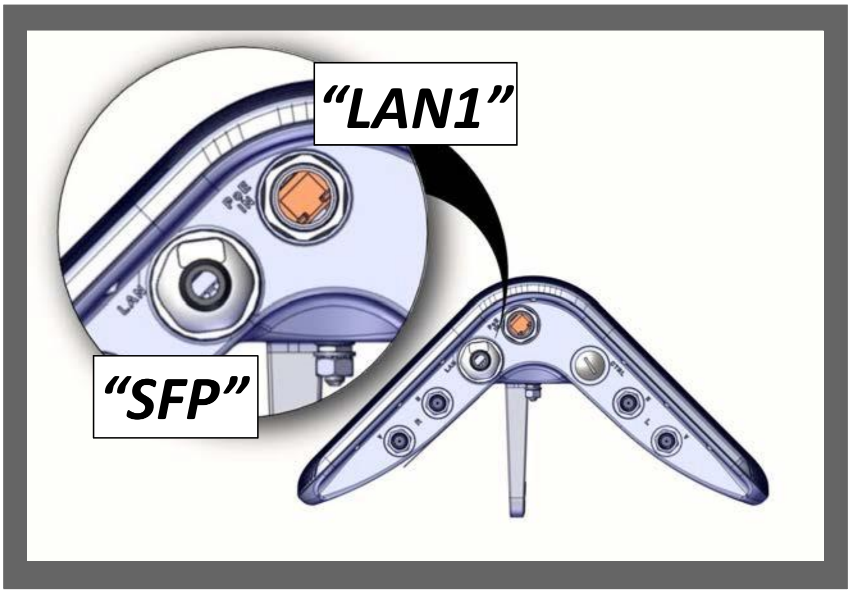


Figure 2-16: Port labeling on MultiSector Integrated units

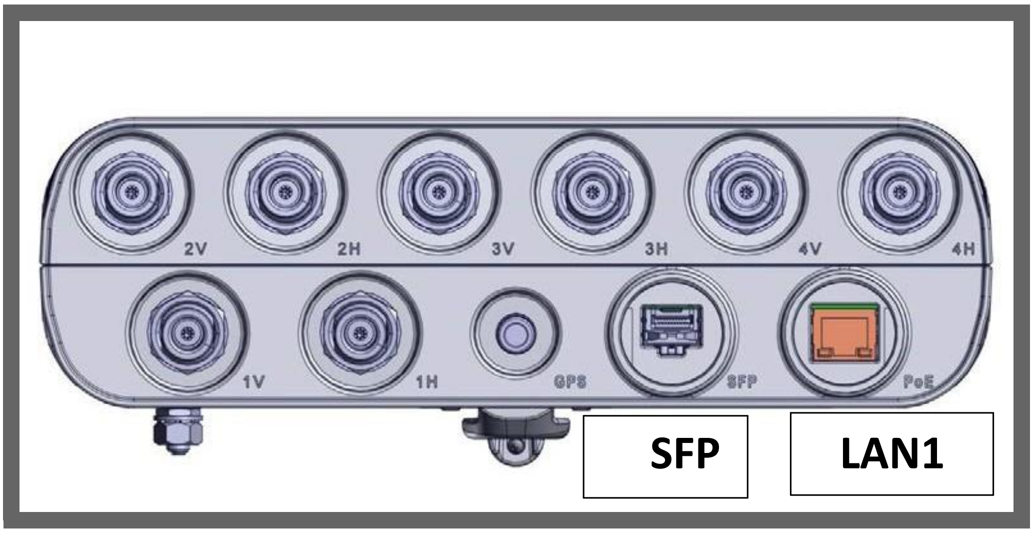
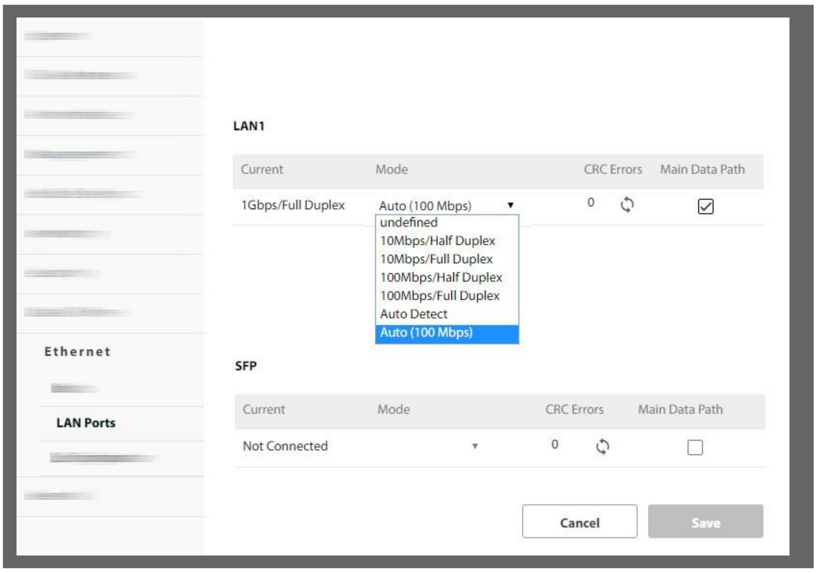


Figure 2-17: Port labeling on MultiSector Connectorized units

- The LAN1 input port is configurable for line speed and duplex mode (half or full duplex).
- Line speed 1000BaseT is only available if the HBS is connected to a GbE PoE device.
- An Auto Detect feature is provided, whereby the line speed and duplex mode are detected automatically using auto-negotiation. Use manual configuration when attached external equipment does not support auto-negotiation. The default setting is Auto Detect.
- The SFP input port can only be set as Auto Detect or Disable.
- CRC Errors shows how many Cyclic Redundancy Check errors occurred since the last rest.
- Main Data Path: Check this to indicate on which port the traffic will flow.

  A few comments:

  - Even if you choose to have the traffic on the SFP port, the LAN1 port must still be connected for input power.
  - Traffic, management, and all other data will be routed via the main data path, including data to and from the subscriber units.
  - The secondary data path can still be used to access the base station itself.



Ethernet

LAN Ports

LAN1

Current	Mode	CRC Errors	Main Data Path
1Gbps/Full Duplex	Auto (100 Mbps) ▾	0	☑

SFP

Current	Mode	CRC Errors	Main Data Path
Not Connected	▾	0	□

Caution

Although you can use the SFP port for traffic and/or management, you still must connect voltage to the LAN1 port.

8. Click **Save** to have your changes take effect.

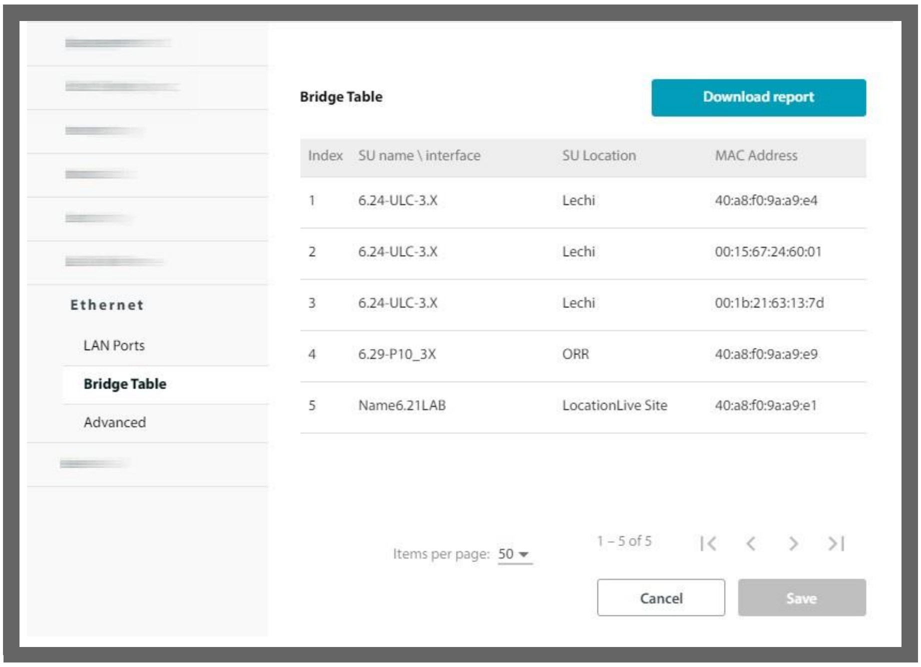
Bridge Table

The Bridge Table provides a list of MAC addresses of the subscriber units in the sector and devices connected to them. This table can be saved in an external *.csv file.

The name of the subscriber units, their locations, and MAC addresses are shown.

If the specific device is not a subscriber unit (customer site equipment connected to a subscriber unit for example), the name and location of the subscriber unit to which the device is connected is shown, but the MAC address shown is that of the device.

- To limit the number of items shown on the page, select the number from the **Items per page** pull-down menu.
- To scroll amongst the items, click the right or left arrows on the bottom right.
- To download the Bridge Table report to an external *.csv file, click **Download report**.



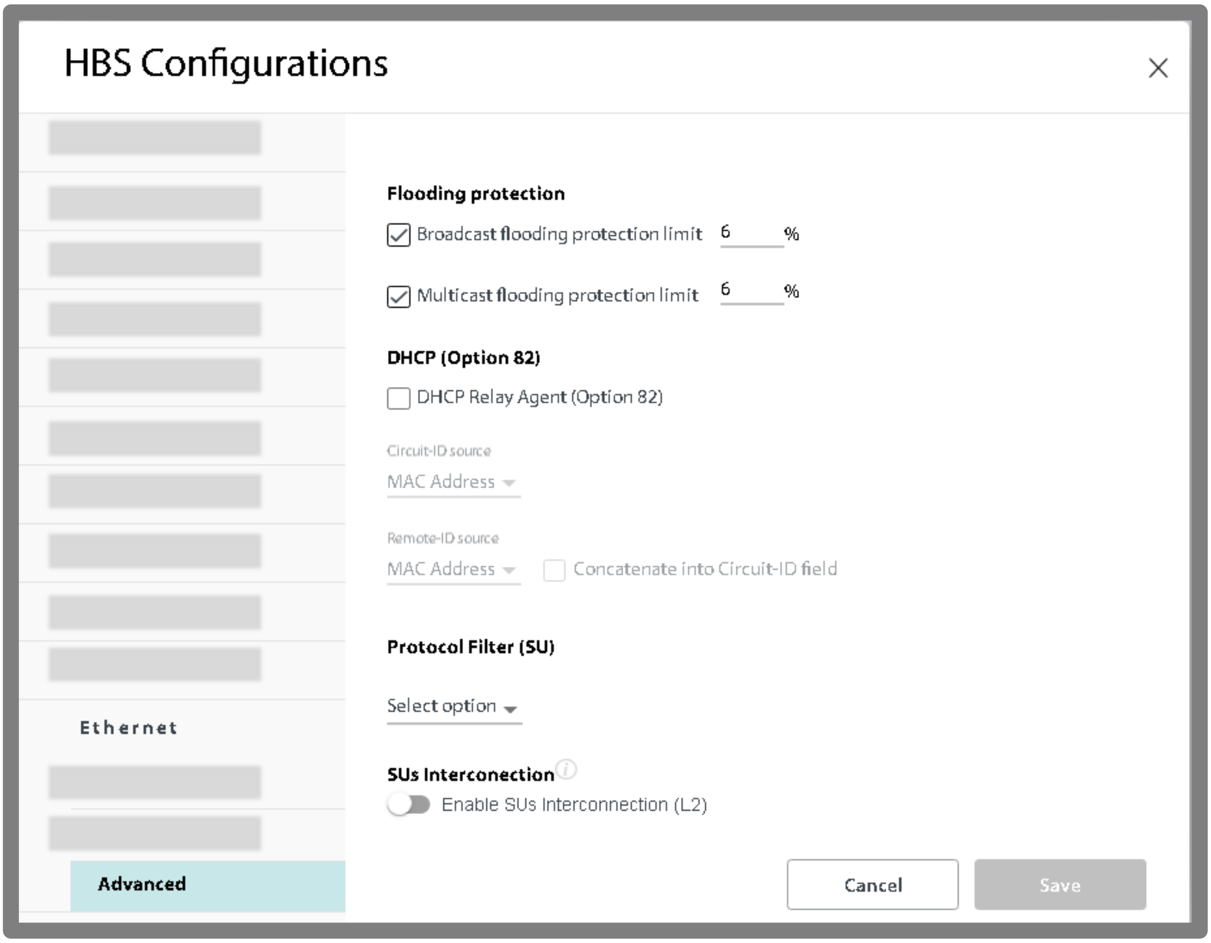
Bridge Table

Index	SU name \ interface	SU Location	MAC Address
1	6.24-ULC-3.X	Lechi	40:a8:f0:9a:a9:e4
2	6.24-ULC-3.X	Lechi	00:15:67:24:60:01
3	6.24-ULC-3.X	Lechi	00:1b:21:63:13:7d
4	6.29-P10_3X	ORR	40:a8:f0:9a:a9:e9
5	Name6.21LAB	LocationLive Site	40:a8:f0:9a:a9:e1

Items per page: 50 1 – 5 of 5

- **Save** is not used here.

Advanced (HBS only)



Flooding protection

☑ Broadcast flooding protection limit 6 %

☑ Multicast flooding protection limit 6 %

DHCP (Option 82)

□ DHCP Relay Agent (Option 82)

Circuit-ID source: MAC Address

Remote-ID source: MAC Address □ Concatenate into Circuit-ID field

Protocol Filter (SU)

Select option

SUs Interconnection

○ Enable SUs Interconnection (L2)

This section has various features: Broadcast and Multicast flooding protection, DHCP (Option 82), protocol filtering (PPPoE, DHCP Client, DHCP Server) and SU interconnection.

Broadcast Flooding Protection

Broadcast Flooding Protection provides a measure of protection by limiting broadcast packets. This feature works in the downlink direction only.

You may wish to disable this feature if your application is based on broadcast packets.

Multicast Flooding Protection

Multicast Flooding Protection provides a measure of protection by limiting multicast packets.

DHCP (Option 82)

Allows a Dynamic Host Configuration Protocol (DHCP) relay agent (in this case the HBS) to insert specific information to a DHCP request it received from a client, and forward the information together with the request to a DHCP server.

This capability allows the residential operator (which has the DHCP server) to distinguish which DHCP IP request came from which SU. With that information, the residential operator can set rules regarding IP address and resource allocation. For example, if there are too many IP requests coming from one SU, it is possible to limit the IP addresses allocated to that equipment.

In the framework of the RADWIN 5000, this works as follows:

- The SU receives DHCP requests from equipment connected to it.
- The SU forwards these requests to the HBS.
- The HBS appends the parameters that were configured (either Serial Number, MAC address or Name of the SU and that of the HBS) to the message, and forwards the request message with the appended data to the DHCP server. This is therefore a DHCP client request.

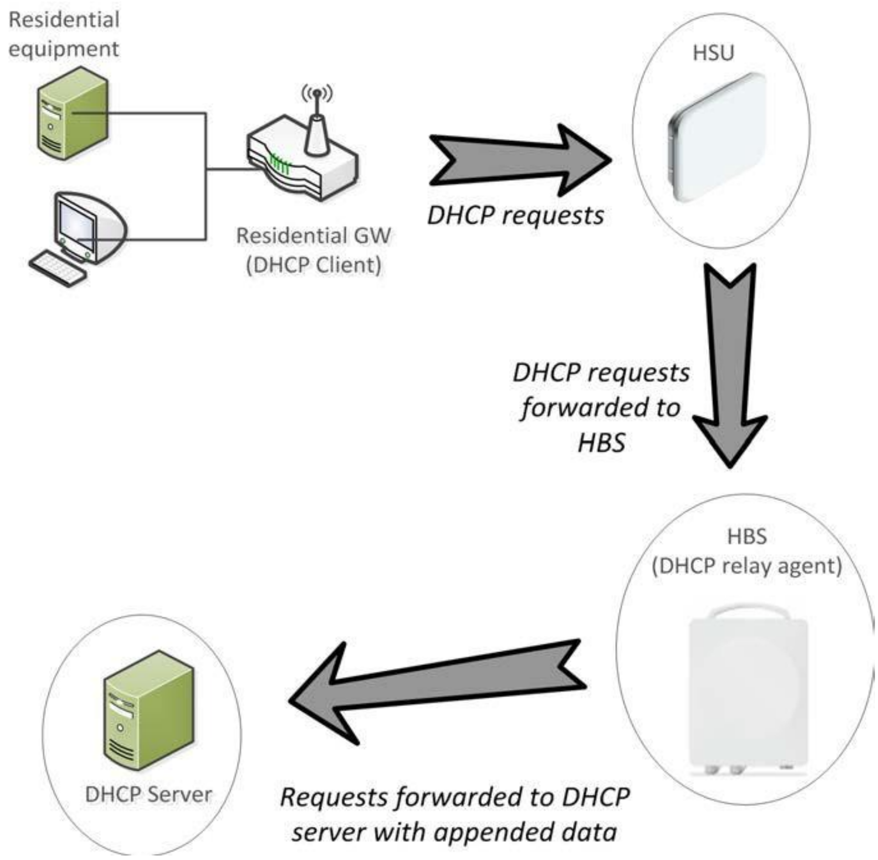

Residential equipment
HSU
Residential GW (DHCP Client)
DHCP requests
DHCP requests forwarded to HBS
HBS (DHCP relay agent)
DHCP Server
Requests forwarded to DHCP server with appended data

Figure 2-18: DHCP Relay Agent (Option 82): Method of operation

To configure the DHCP Relay Agent feature:

- From **Ethernet -> Advanced**, place a checkmark next to DHCP Relay Agent (Option 82) to enable this feature.
- From the pull-down menu labeled Circuit-ID source, choose which parameter of the HBS will be sent to the DHCP server - its MAC address, Serial Number, or Name.
- From the pull-down menu labeled Remote-ID source, choose which parameter of the SU will be sent to the DHCP server - its MAC address, Serial Number, or Name. To simplify the message, it is possible to add the Remote-ID source data directly onto the end of the Circuit-ID data, that is, to concatenate it onto the Circuit-ID field. If you wish to do this, place a checkmark in the **Concatenate into Circuit-ID** field box.
- Make sure to configure your DHCP Server to accept these values of the parameters.
- Click **Save** to have your changes take effect.

Note

It is also possible to filter *all* DHCP client responses from the SU side, per SU. This is possible only using the SU ***PRO/AIR*** EMB or SU Integrated, and if done, the DHCP Relay Agent (Option 82) cannot be implemented.

Protocol Filter (SU)

This option allows you to prevent non-PPPoE or DHCP traffic that is being sent from the customer equipment to the SU from being forwarded to the HBS.

There are 5 options in the Protocol Filtering pull-down menu:

No Filtering: Do not block any non-PPPoE (Point-to-Point over Ethernet) or DHCP traffic that comes from customer equipment connected to the subscriber unit.

PPPoE Only: Prevents non-PPPoE packets coming from customer equipment connected to the subscriber unit from being forwarded to the HBS.

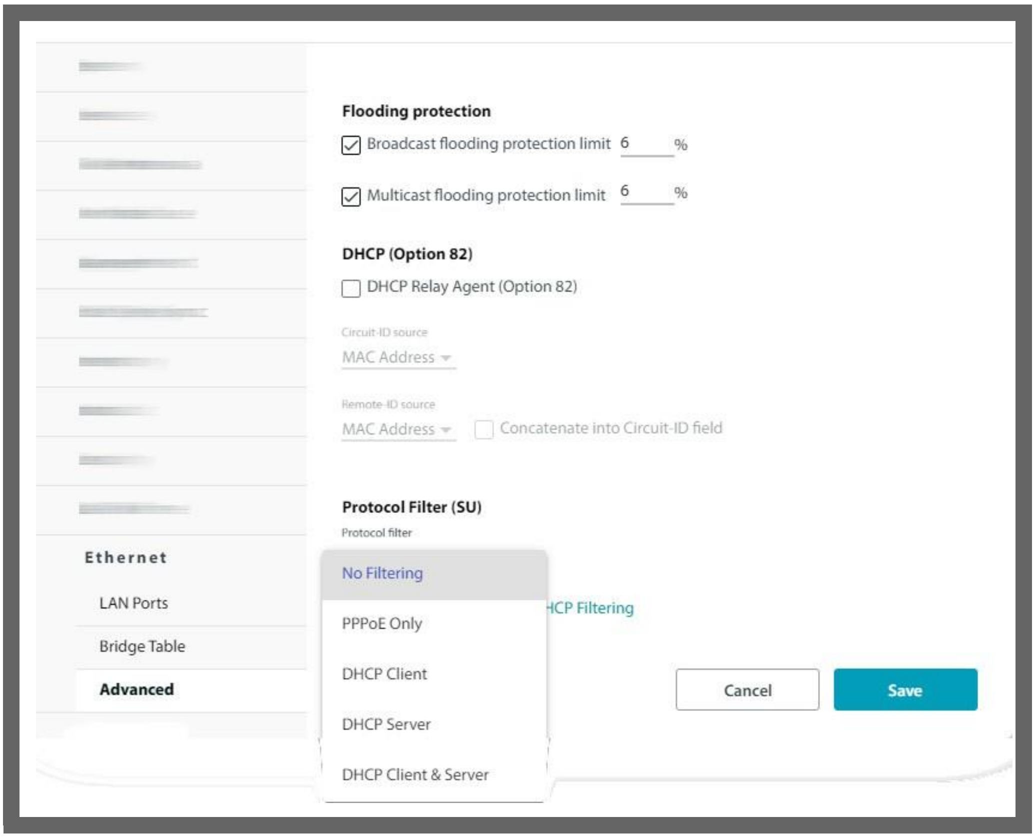
The “No Filtering” or “PPPoE Only” option must be chosen if you are planning to use the DHCP Relay Agent (Option 82).

DHCP Server: Prevent DHCP Server responses from customer equipment from being forwarded to the HBS. DHCP Client responses can be forwarded.

DHCP Client: Prevent DHCP Client requests from customer equipment from being forwarded to the HBS. DHCP Server responses can be forwarded.

DHCP Client & Server:

Prevent DHCP Client and DHCP Server requests from customer equipment from being forwarded to the HBS.



Ethernet

LAN Ports

Bridge Table

Advanced

Flooding protection

☑ Broadcast flooding protection limit 6 %

☑ Multicast flooding protection limit 6 %

DHCP (Option 82)

□ DHCP Relay Agent (Option 82)

Circuit-ID source

MAC Address

Remote-ID source

MAC Address □ Concatenate into Circuit-ID field

Protocol Filter (SU)

Protocol filter

No Filtering

PPPoE Only

DHCP Client

DHCP Server

DHCP Client & Server

HCP Filtering

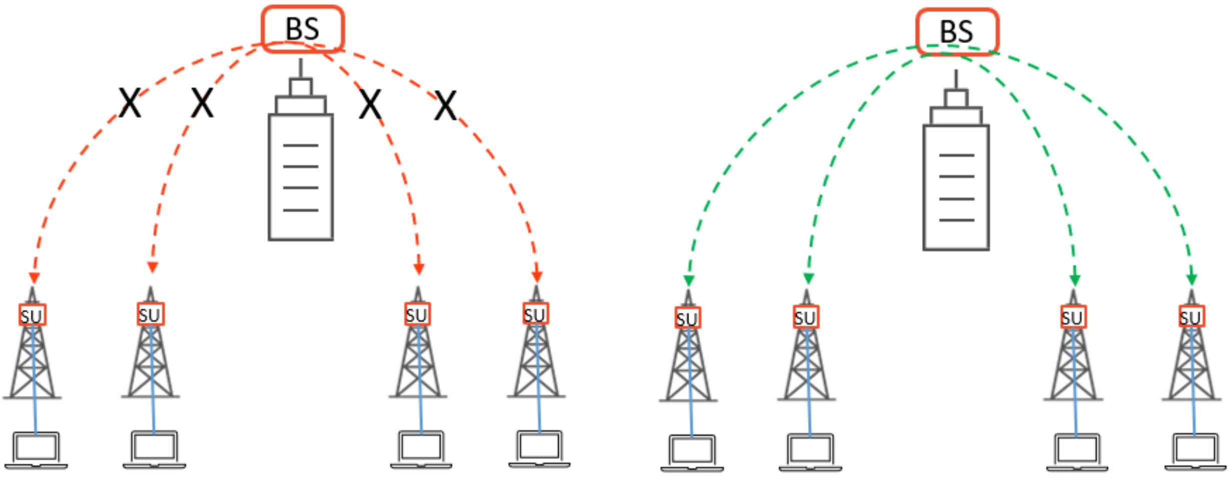
Cancel Save

- Click **Save** to have your changes take effect.

SU interconnection

Enable the BS to function as a wireless bridge between devices connected to SUs that are registered to the BS. This can be used when the devices behind SUs need to communicate with each other, which reduce traffic from the BS to the network. If this option is disabled, the SUs will only be able to communicate through a network element located behind the BS.

However, if this option is enabled, multicast and broadcast traffic of devices on the LAN side of the SUs, would also be transferred over the air to all other SUs, taking up some part of the BS air capacity **and impacting performance.**



2.3.16. IGMP

The IGMP (Internet Group Management Protocol) snooping option allows conversion of multicast IPTV traffic that arrives at the HBS to be unicast towards an SU, according to the IGMP request from the customer site equipment connected to the given SU.

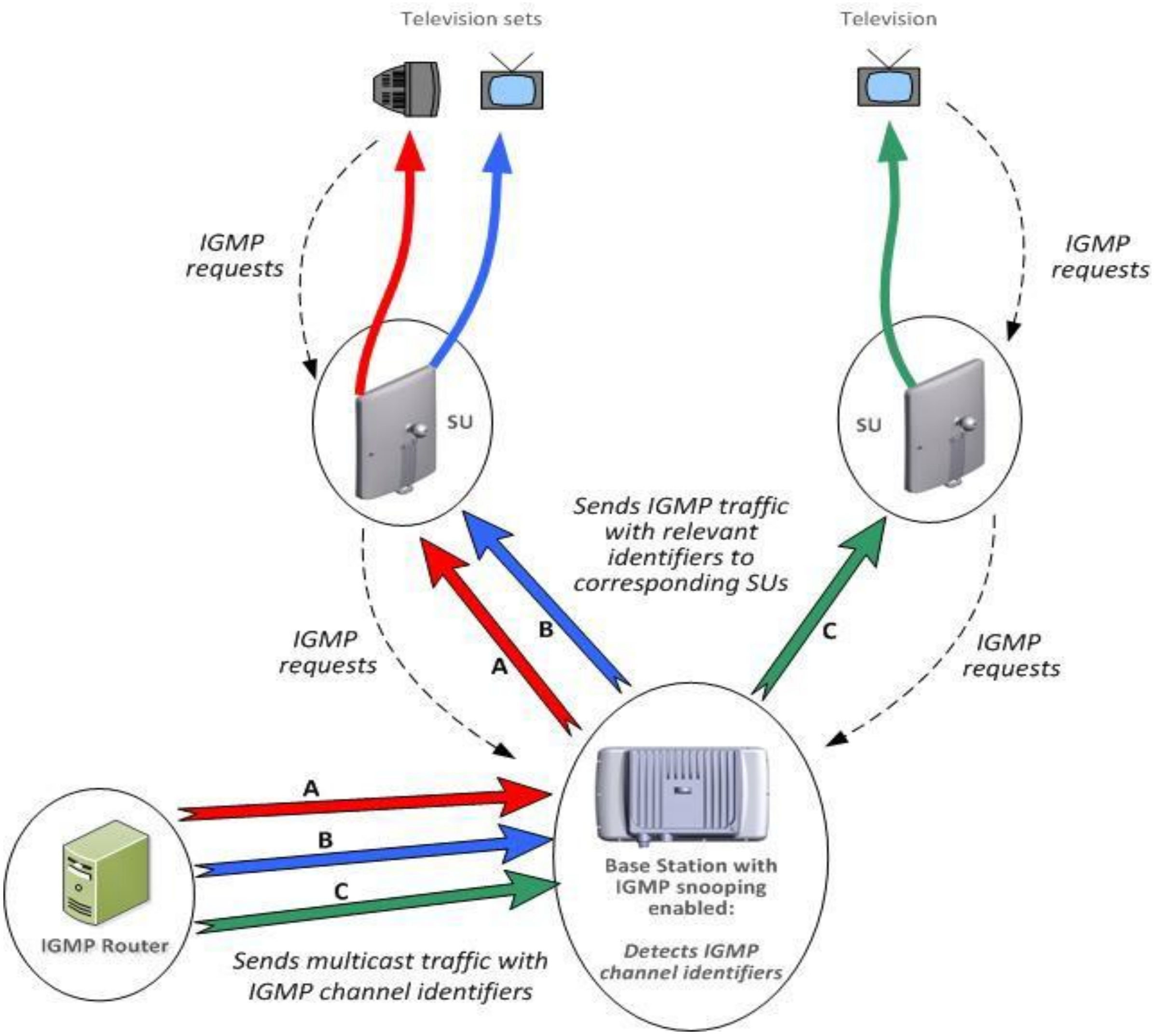

Television sets
Television
IGMP requests
IGMP requests
SU
SU
Sends IGMP traffic with relevant identifiers to corresponding SUs
IGMP requests
IGMP requests
A
B
C
A
B
C
IGMP Router
Sends multicast traffic with IGMP channel identifiers
Base Station with IGMP snooping enabled:
Detects IGMP channel identifiers

Figure 2-19: IGMP operation with the RADWIN 5000

- The customer's television (or setup box) sends IGMP requests.
- The SU forwards this request in the uplink direction.
- The HBS detects ("snoops") the IGMP tag, and sends the corresponding multicast traffic in the downlink direction to those SUs whose customer equipment sent an IGMP request with the same multicast group. Messages from other multicast groups are blocked.

Snooping Enable

To enable IGMP snooping for the sector, click Snooping Enable.

Robustness

The Robustness determines how many non-responses the HBS must "not receive" from a CSE (Customer Site Equipment) in response to an IGMP query before removing it from the

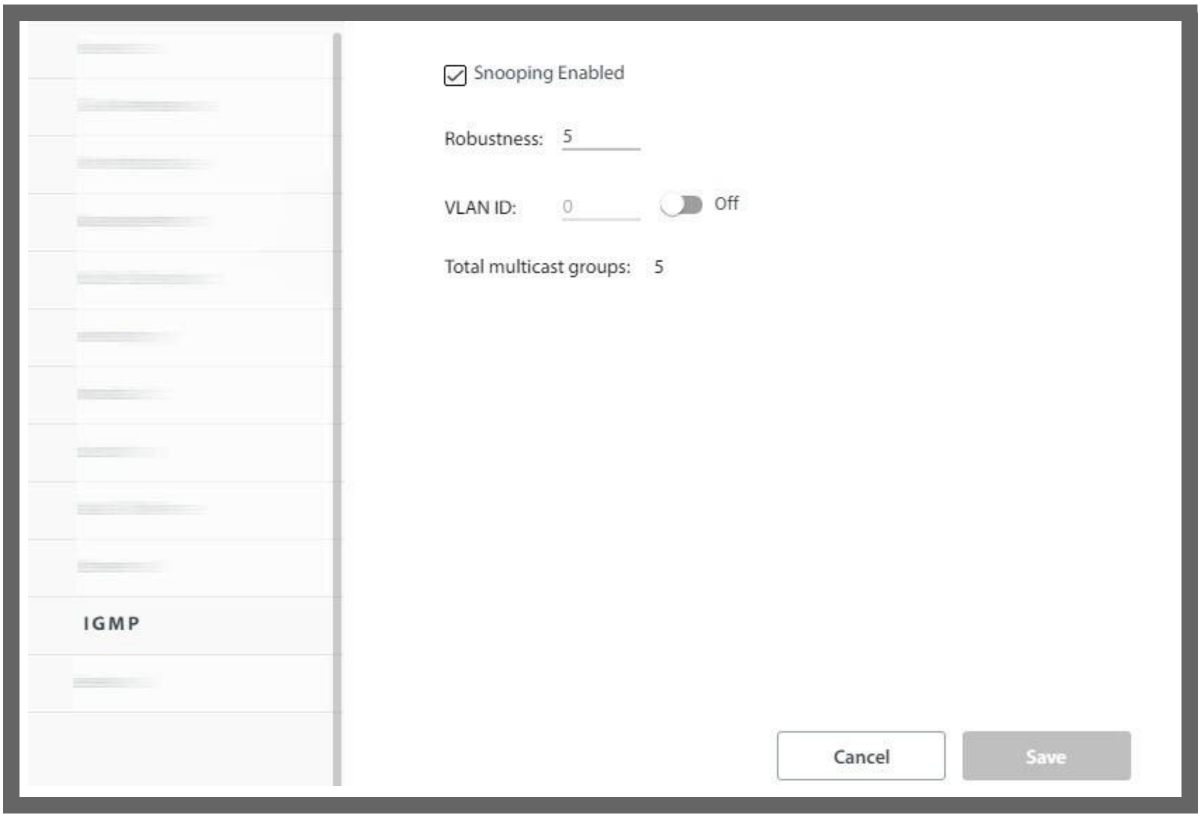
IGMP multicast group. The higher this value is, the more reliable the IGMP operation.

VLAN ID

The IGMP option can be limited to a specified VLAN. This can help to avoid confusion in complicated networks. Configure the **Off** button to **On** to enable limiting the IGMP option to a specific VLAN, then set the VLAN ID. If an IGMP request comes from a VLAN whose ID does not correspond to this VLAN ID, the request will be ignored. If this option is set to Off, VLAN IDs in this context will be ignored.

Total multicast groups

This shows the total multicast groups in the system.



☑ Snooping Enabled

Robustness: 5

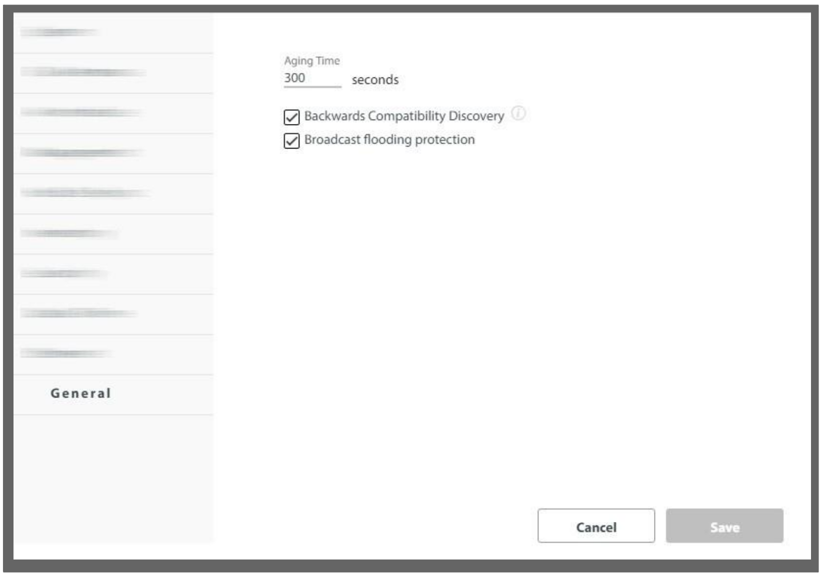
VLAN ID: 0 Off

Total multicast groups: 5

- Click **Save** to have any changes take effect.

2.3.17. General (HBS only)

In this category, you can configure the Aging Time, and enable/disable Backwards Compatibility Discovery.



Aging Time
300 seconds

☑ Backwards Compatibility Discovery

☑ Broadcast flooding protection

Aging Time

The HBS works in Bridge Mode. In Bridge mode, it performs both learning and aging, forwarding only relevant packets over the sector. The aging time of the HBS is by default 300 seconds, although you can change this value here.

Backwards Compatibility Discovery

This allows HSUs with firmware older than Release 4.6 (those without the percentage-based DBA mechanism) to discover HBSs with Release 4.6 or above. To work properly, the firmware of the HSU must be upgraded to firmware that is compatible with that of the HBS.

- Click **Save** to have any changes take effect.

2.3.18. Networking (HBS only)

Sector Self backhaul

When working with a MultiSector Base Station, a subscriber unit in one of the sectors can be used as a backhaul link. Note the following:

» The backhaul link is for both carriers.

» Only a SU PRO or Alpha (in PtMP mode) can be used for this feature.

» This feature does not support jumbo frames.

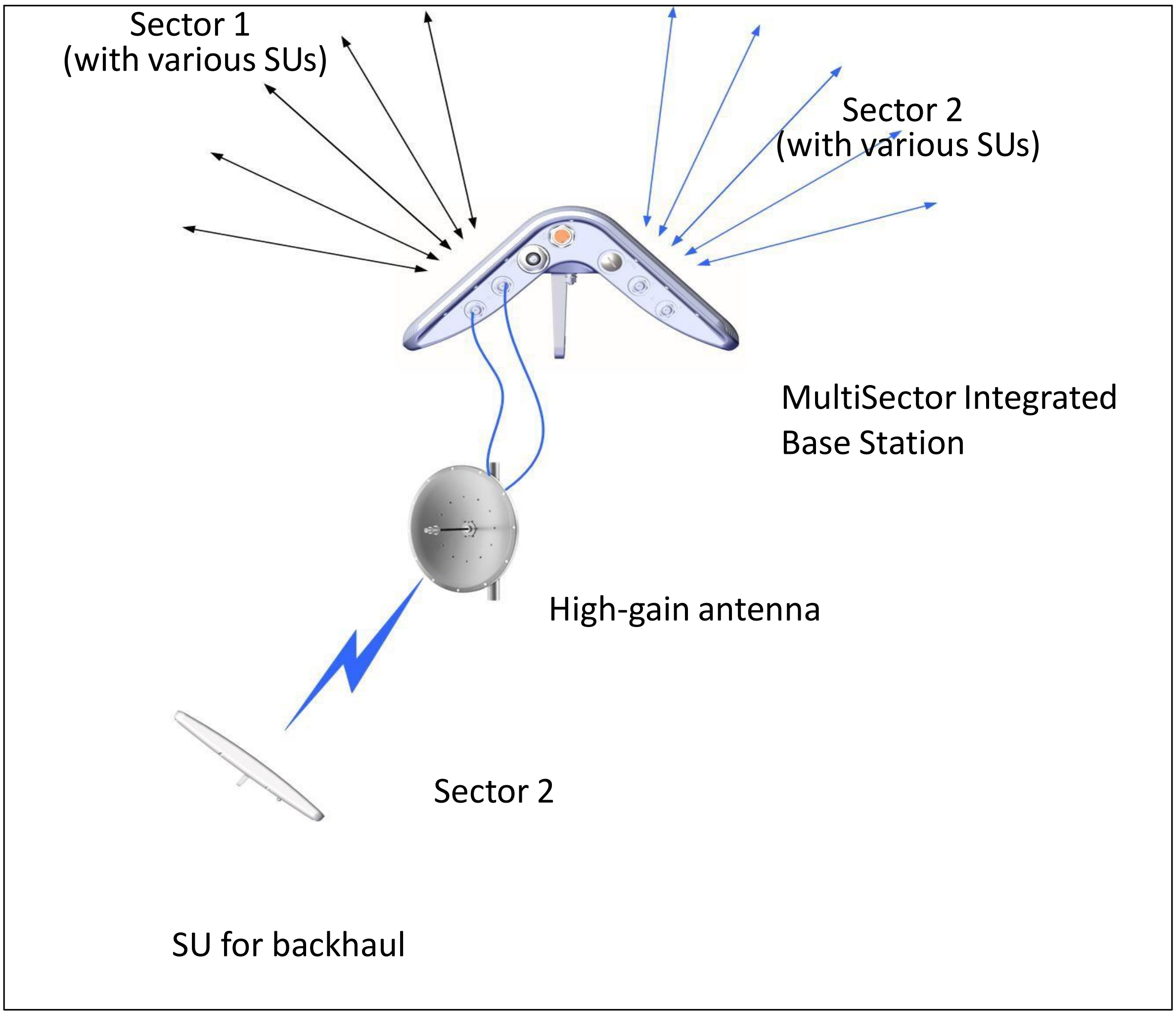


Figure 2-20: Sector Self-Backhaul: MultiSector Integrated

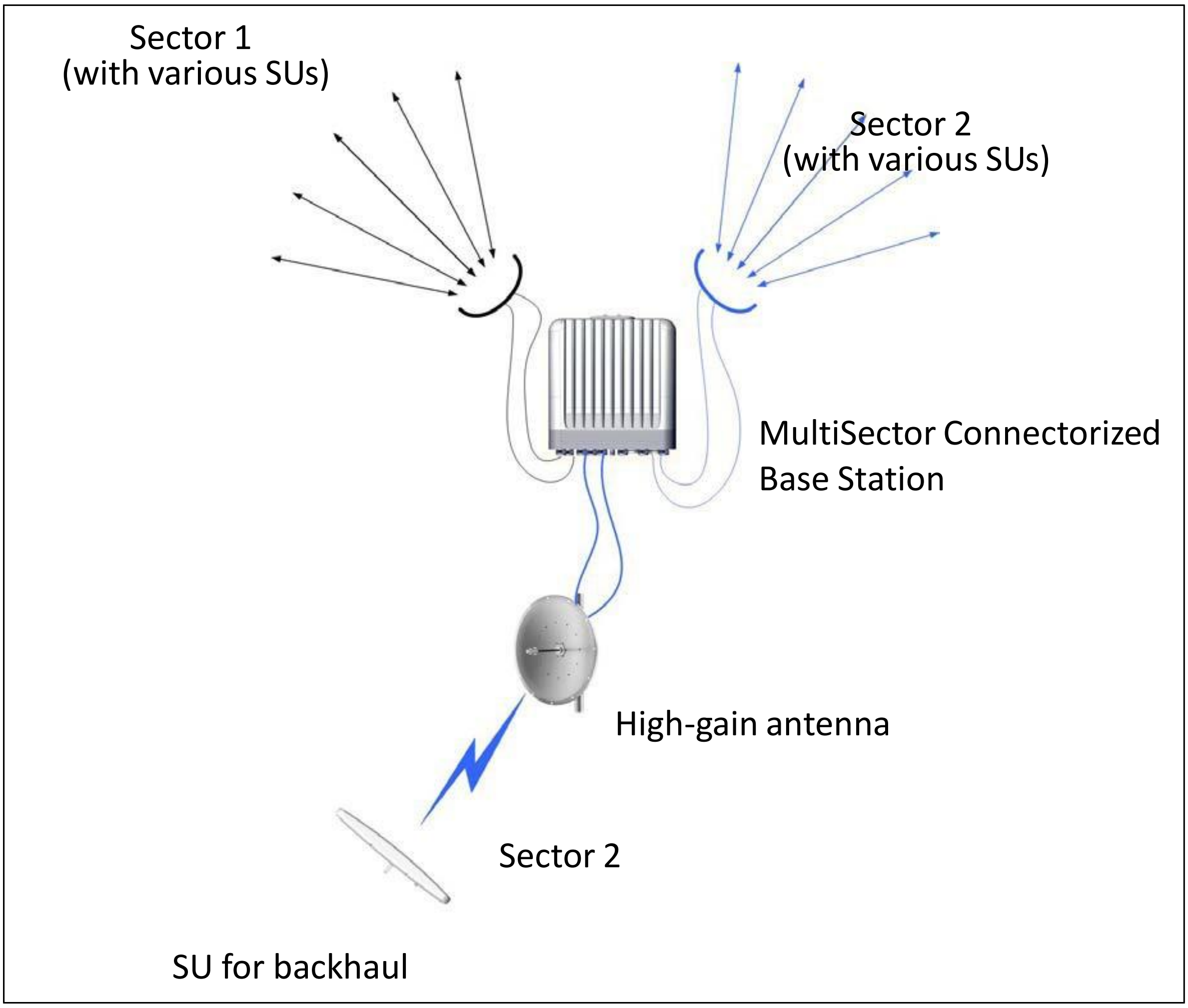
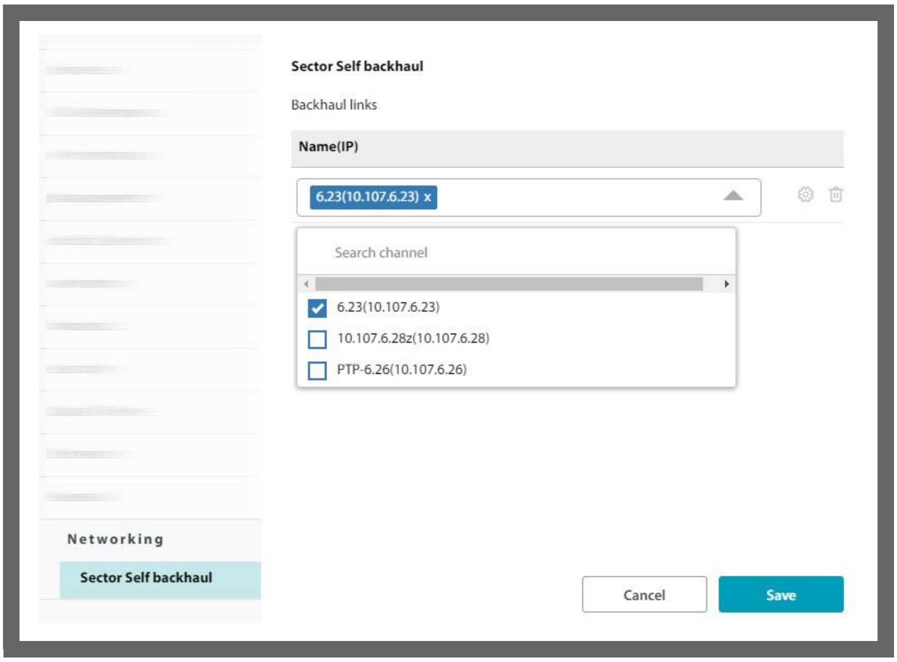


Figure 2-21: Sector Self-Backhaul: MultiSector Connectorized

1. Mount and connect the subscriber unit to be used, then perform antenna alignment opposite the high gain antenna of the base station (as is done for any subscriber unit). The backhaul link can be in any direction. Instructions for this can be found in the RADWIN 5000 Installation Guide.
2. Register the subscriber unit.



3. Click **Add** next to Backhaul links.

   If there is already an SU providing a backhaul connection, its name and IP address will appear instead of the Add button.

4. From the pull-down menu that appears, select the subscriber unit that will carry the backhaul traffic.

   You can only have one subscriber unit on the carrier that is to carry the backhaul traffic.

5. To remove the SU, click the garbage icon. To change the SU, click the configuration icon and select the new SU.

6. Click **Save** to have your changes take effect.

2.3.19. Services (SU via HBS only)

Do not confuse this with the "*Services (HBS only)*" category, which has different sub-categories, and is HBS only.

This category has five sub-categories:

Resources - set the resource type (CIR or BE)

Mir (Maximum Information Rate)

QoS Configuration (SU side)

VLAN

Quality Detection

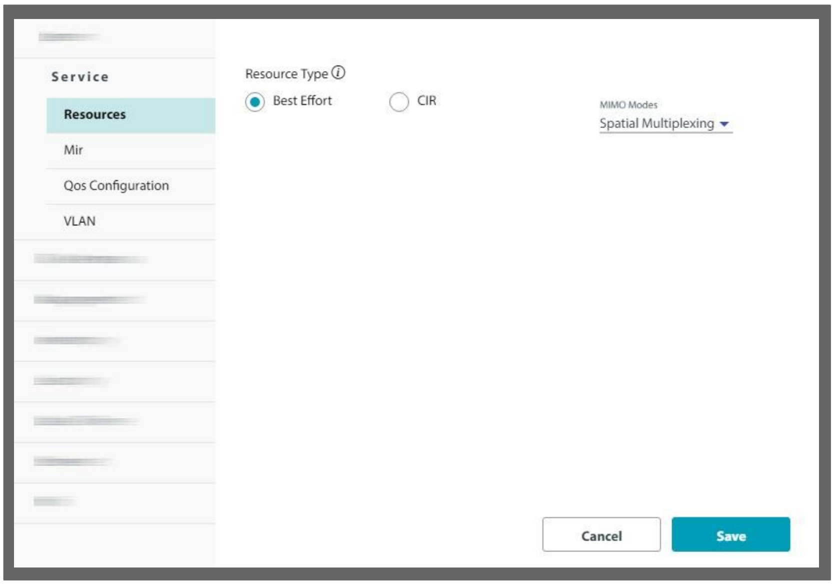
Resources

Even after an SU is registered, you can change these settings here: Resource type and MIMO mode.

- Select the **Resource Type** for the selected HSU. This can be CIR (Committed Information Rate), or BE (Best Effort):
  - BE (Best Effort) grants the SU resources as they become available in the sector.
  - CIR (Committed Information Rate) grants the SU with a certain guaranteed

percentage of resources already allocated to CIR traffic in the sector. That percentage is set in the MIR window.

- Select a MIMO Mode for the selected SU:
  - Spatial Multiplexing (default) splits the data into two streams on transmission and recombines it on reception, providing maximum throughput.
  - **Diversity** transmits the same data on both streams. This mode helps to ensure more reliable data transmission in a noisy environment, although throughput will be lower.
  - Auto Selection instructs the system to choose whichever mode is most efficient.

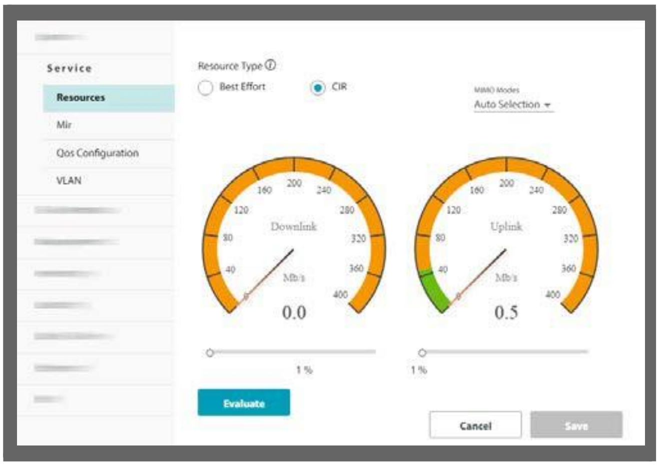


Resource Type ⓘ
● Best Effort ○ CIR

MIMO Modes
Spatial Multiplexing ▾

- Click **Save** to have your changes take effect.

If you chose the CIR resource type, the CIR evaluate window will appear.



Resource Type ⓘ
○ Best Effort ● CIR

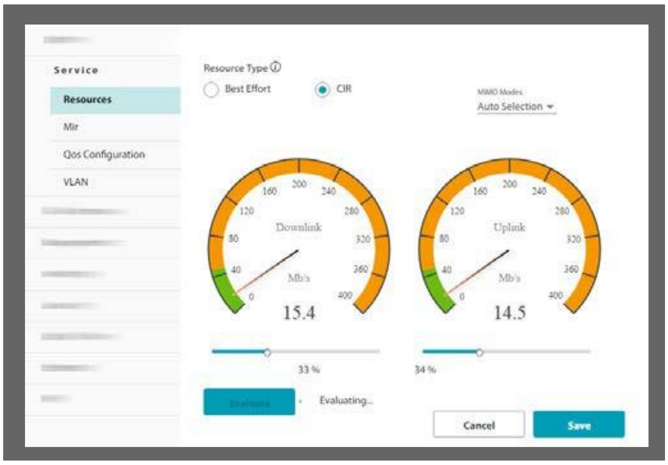
MIMO Modes
Auto Selection ▾

Downlink 0.0 Mb/s, 1 %

Uplink 0.5 Mb/s, 1 %

- Click the **Evaluate** button.

  Service evaluation takes a few seconds during which an “Evaluating ...” message is displayed.



Resource Type ⓘ

○ Best Effort ● CIR

MIMO Modes: Auto Selection

Downlink 15.4 — 33 %

Uplink 14.5 — 34 %

Evaluating...

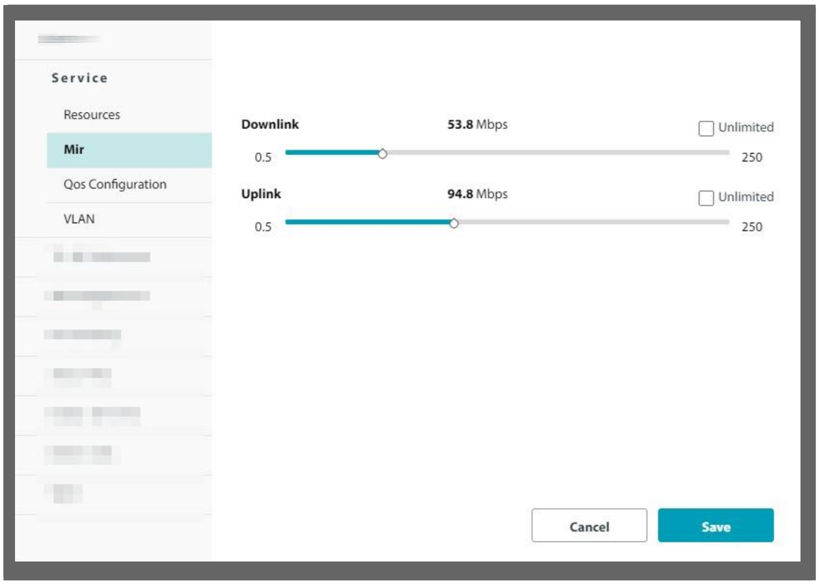
After the initial evaluation, dynamic monitoring of the sector is maintained. This allows you to add SUs in the sector, and the available resources are adjusted automatically.

- Use the sliders to choose the percentage of resources (uplink and downlink) already allocated to CIR traffic in the sector to be allocated to the selected SU.
- Click **Save** to have your changes take effect.

Mir (Maximum Information Rate)

Although this is set during registration, you can change it here.

Use the sliders to set the maximum throughput rate you want for the specific SU in each direction: down link and up link. You can choose a value or click the Unlimited checkbox.



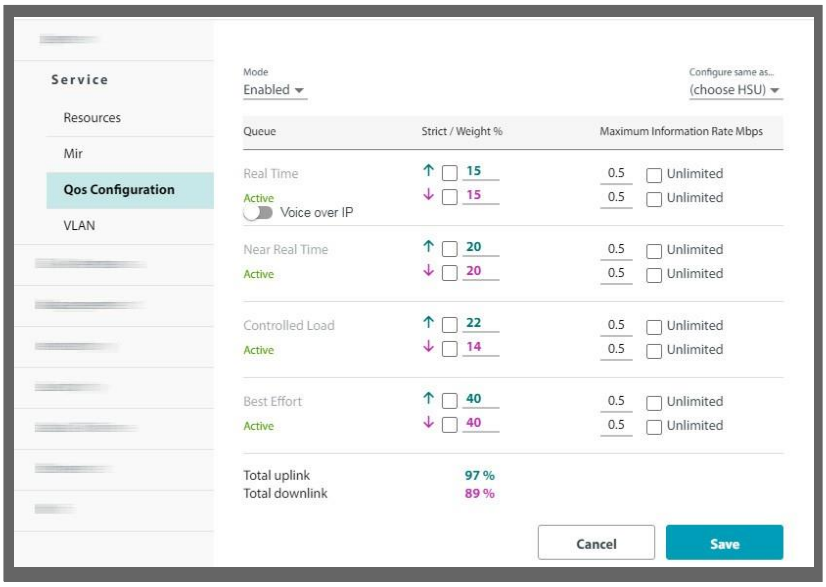
Downlink 53.8 Mbps □ Unlimited
0.5 – 250

Uplink 94.8 Mbps □ Unlimited
0.5 – 250

Click **Save** to have your changes take effect.

QoS Configuration (SU side)

This section describes how to configure QoS for an individual SU. (To see how to configure QoS for the whole sector, that is, from the HBS, see QoS Configuration (HBS side)).



Mode
Enabled ▾

Configure same as...
(choose HSU) ▾

Queue	Strict / Weight %		Maximum Information Rate Mbps	
Real Time Active Voice over IP	↑ □	15	0.5	□ Unlimited
	↓ □	15	0.5	□ Unlimited
Near Real Time Active	↑ □	20	0.5	□ Unlimited
	↓ □	20	0.5	□ Unlimited
Controlled Load Active	↑ □	22	0.5	□ Unlimited
	↓ □	14	0.5	□ Unlimited
Best Effort Active	↑ □	40	0.5	□ Unlimited
	↓ □	40	0.5	□ Unlimited

Total uplink 97 %
Total downlink 89 %

1. Enable the **Mode** field. (*Enabling a VoiP Queue (SU side)* for VoIP).
2. Set the **weight percentage** for each queue by moving the spinners up or down.

   Light blue for uplink, pink for downlink.

   The weight percentage determines what percentage of the throughput will be dedicated for the indicated queue.

   The total weight is shown in the lower part of the window. If you exceed 100% total weight, you will receive an error message.

   If you are under-booked, for example, by setting a queue to zero, the unused weight will be distributed to the remaining queues. The effect of doing this will only become apparent under congestion. In particular, a queue set to zero weight will become nearly blocked under congestion with packets passing through on a best effort basis.
3. **Strict:** If you place a checkmark in the Strict box, *all traffic* of the specific queue will be passed through. The Weight percentage will become disabled. Placing a checkmark here can only be done in order: First Real Time, then finally Best Effort. That is, you cannot place a checkmark in Near Real Time without one in Real Time as well. Like the weight percentage, uplink and downlink are configured separately.
4. **Maximum Information Rate:** Although the weight percentage affects how much relative traffic will be allowed through, you can set here the absolute maximum to allow through. Place a checkmark to make this value as unlimited.
5. **Configure same as ....**: This allows you to copy the VoIP configuration of a different SU. From the pull-down menu, choose the SU whose configuration you want to copy. The settings will appear.

Enabling a VoiP Queue (SU side)

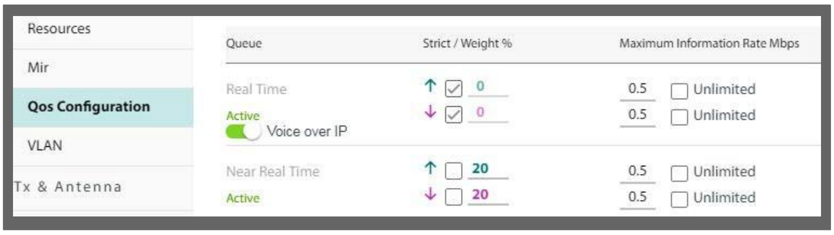
Note the following:

- You can enable a VoIP queue from either the HBS or the SU. If enabled from the SU, it is done for that SU only, and its HBS. If done from the HBS, it can be done sector-wide.

- To configure VoiP from the HBS side, See Enabling a VoiP Queue (HBS side).

- The VoIP feature as implemented here assumes that your end-user has a gateway or other network device that defines the traffic to be VoIP with the correct QoS defined (VLAN or DiffServ, in accordance with your configuration done here). The definition must be done at both ends of the data stream.
- Enabling a VoIP queue may decrease the unit's peak throughput in some scenarios. Therefore, make sure that you absolutely need to enable a VoIP queue before doing so.

1. Click **Voice over IP**. The Voice over IP indicator will turn green.



Queue		Strict / Weight %		Maximum Information Rate Mbps	
Real Time	↑	☑	0	0.5	□ Unlimited
Active	↓	☑	0	0.5	□ Unlimited
● Voice over IP					
Near Real Time	↑	□	20	0.5	□ Unlimited
Active	↓	□	20	0.5	□ Unlimited

The weight percentages of the Real-Time queue will become zero in both the uplink and downlink directions. This means that VoIP traffic is treated in a similar fashion to Real Time traffic.

VoIP works whether you are using VLAN or DiffServ, but you must be consistent with this QoS mode throughout the data stream.

2. Click **Save** to have your changes take effect.

VLAN

Configure a VLAN for traffic here. To configure the management VLAN, See Network.

The VLAN configuration is carried out per SU. It is up to you to ensure consistency between the SUs.

If the VLAN is not enabled, ethernet frames pass transparently over the radio links.

VLAN Background Information

The standards defining VLAN Tagging are IEEE_802.1Q and extensions.

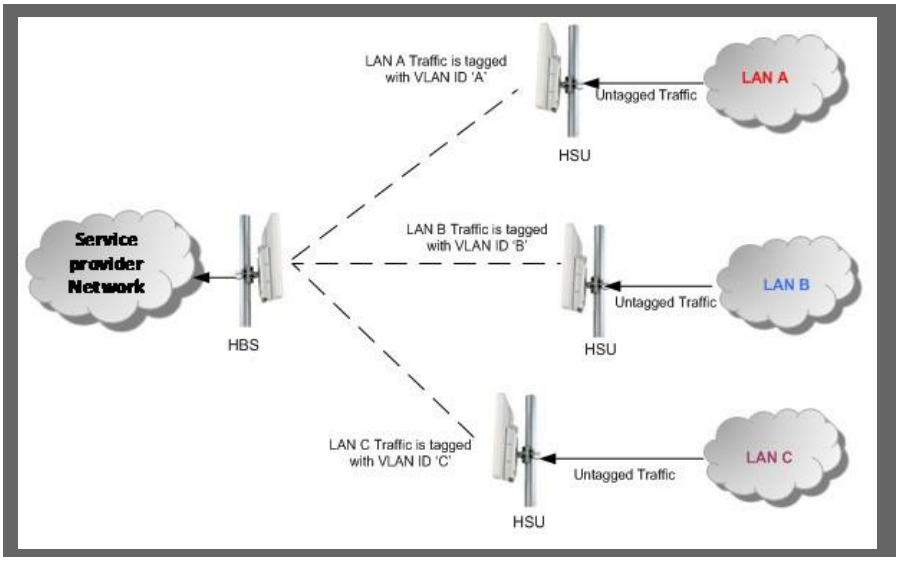
For general background information about VLAN see http://en.wikipedia.org/wiki/Virtual_LAN

Background information about Double Tagging also known as QinQ may be found here:

http://en.wikipedia.org/wiki/802.1QinQ

VLAN Tagging

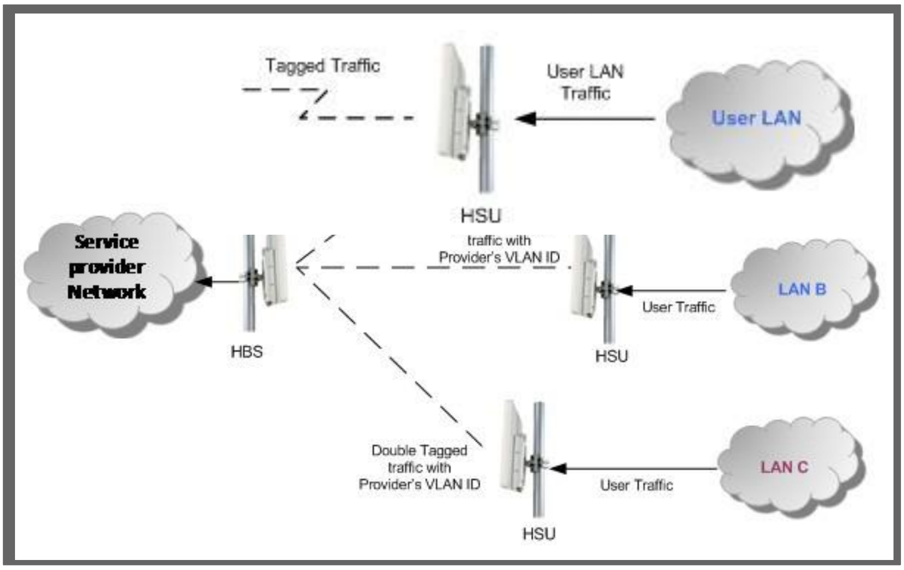
VLAN tagging enables multiple bridged networks to transparently share the same physical network link without leakage of information between networks.


LAN A Traffic is tagged with VLAN ID 'A'
Untagged Traffic
LAN A
HSU
Service provider Network
LAN B Traffic is tagged with VLAN ID 'B'
Untagged Traffic
LAN B
HBS
HSU
LAN C Traffic is tagged with VLAN ID 'C'
Untagged Traffic
LAN C
HSU

IEEE 802.1Q is used as the encapsulation protocol to implement this mechanism over Ethernet networks.

QinQ (Double Tagging) for Service Providers

QinQ is useful for service providers, allowing them to use VLANs internally in their "transport network" while mixing Ethernet traffic from clients that are already VLAN-tagged.



The outer tag (representing the Provider VLAN) comes first, followed by the inner tag. In QinQ, the EtherType = 0x9100. VLAN tags may be stacked three or more deep.

When using this type of "Provider Tagging", you should keep the following in mind:

- Under Provider Tagging, the system double-tags egress frames towards the Provider's network. The system also adds a tag with a VLAN ID and EtherType = 0x9100 to all frames, as configured by the service provider (Provider VLAN ID).
- The system always adds tags with a VLAN ID and EtherType = 0x9100 for each frame. Therefore,
  - For a frame without a tag – the system will add a tag with VLAN ID and EtherType = 0x9100 so the frame will have one tag.

- For a frame with a VLAN tag – the system will add a tag with VLAN ID and EtherType = 0x9100 so the frame will be double-tagged.

For a frame with a VLAN tag and a provider tag – the system will add a tag with VLAN ID and EtherType = 0x9100 so the frame will be triple-tagged and so on.

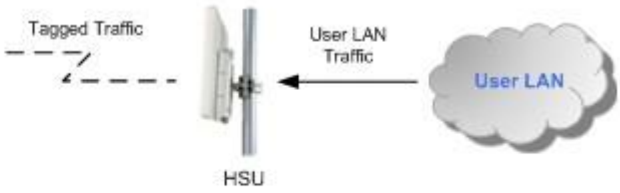
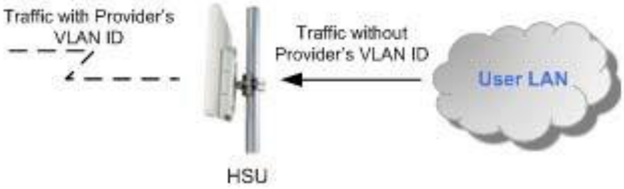
At the egress side, the SU removes the QinQ tag with EtherType = 0x9100 no matter what the value of its VLAN ID is.

Port Setting

In a RADWIN 5000 sector, all VLAN activity is configured and supported from the SUs.

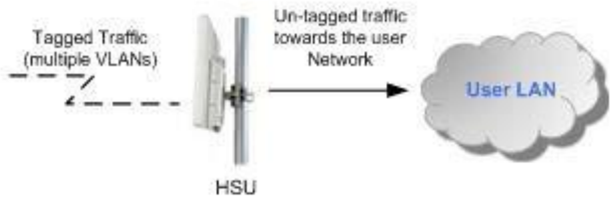
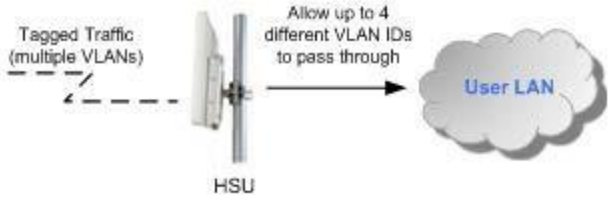
The SU management port can be configured to handle Ethernet frames at the ingress direction (where frames enter the SU) and at the egress direction (where frames exit the SU).

Ingress Direction

Transparent	The port ‘does nothing’ with regard to VLANs - inbound frames are left untouched.
Tag	Frames entering the SU port without a VLAN or QinQ tagging are tagged with VLAN ID and Priority[1], which are preconfigured by the user. Frames which are already tagged at ingress are not modified and pass through. 
Provider tag	Frames entering the SU port are tagged with the provider’s VLAN ID and Priority, which are preconfigured by the user. Frames, which are already tagged with Provider tagging at the ingress, are not modified and passed through  Traffic with Provider's VLAN ID Traffic without Provider's VLAN ID User LAN HSU

[1] Priority Code Point (PCP), which refers to the IEEE 802.1p priority. It indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc.).

Egress Direction

Transparent	The port 'does nothing' with regard to VLANs - outbound frames are left untouched.
Untag all	Port configured to untag user VLAD tags for all frames.  Tagged Traffic (multiple VLANs) Un-tagged traffic towards the user Network User LAN HSU
Filter	 Tagged Traffic (multiple VLANs) Allow up to 4 different VLAN IDs to pass through User LAN HSU

Before proceeding, note the following:

Caution

If you are not a VLAN expert, please be aware that incorrect VLAN configurations may cause havoc on your network. The facilities described below are offered as a service to enable you to get the best value from your RADWIN links and are provided "as is". Under no circumstances does RADWIN accept responsibility for network system or financial damages arising from incorrect use of these VLAN facilities.

Management Traffic and Ethernet Service Separation

You can define a VLAN ID for management traffic separation. You should configure the system to prevent conflicts:

When configured for the default operational mode, a "Provider port" will handle ingress traffic as follows:

- Filters frames that are not tagged with the Provider VLAN ID.
- Removes the Provider double tag.

Therefore, if a port is configured for management traffic separation by the VLAN and as 'Provider port', then the received management frames must be double tagged as follows:

- The outer tag has to be the Provider's tag (so the frame is not filtered).
- The internal tag has to be management VLAN

ID. To avoid mix-ups, best practice is to:

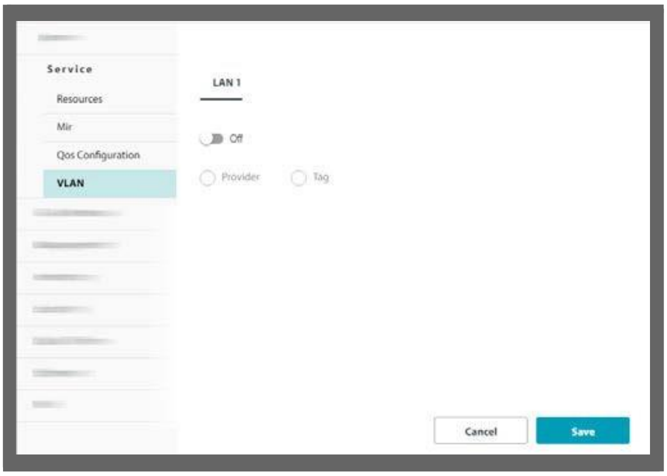
- Separate the management and data ports (if relevant for your product).
- Define only a data port with Provider function.

Note

If traffic VLAN tagging is in force for the SU ingress direction and management VLAN is in use at the HBS (See VLAN), then the VLAN ID at the SU ingress direction must be the same as the VLAN ID for management at the HBS.

VLAN Configuration

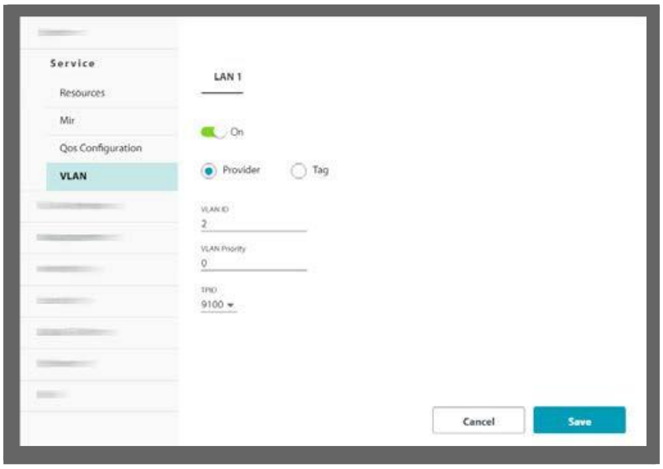
1. Select the SU to be configured, open the Configuration icon, click Service -> VLAN.



Off

○ Provider ○ Tag

2. Click **Off** to enable the VLAN window. It will turn to **On**.



On

● Provider ○ Tag

VLAN ID
2

VLAN Priority
0

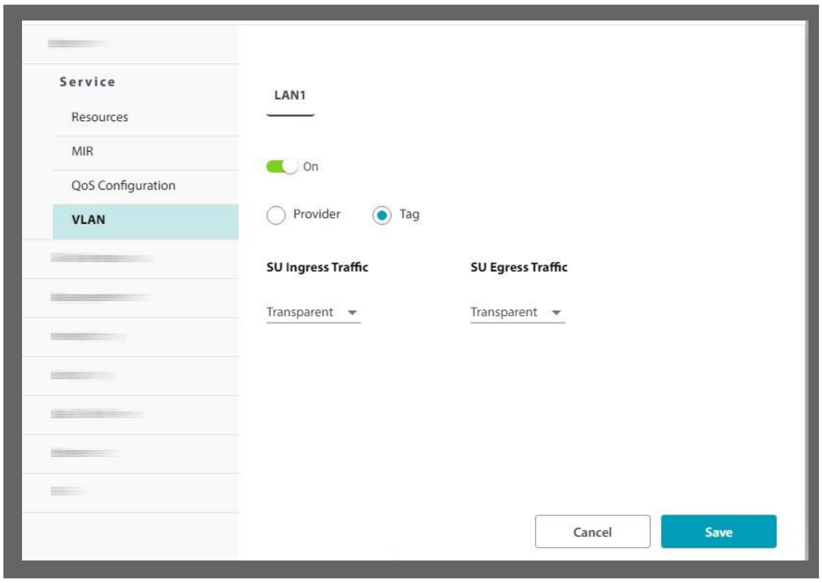
TPID
9100

3. If you are using Provider tagging, click the Provider Radio button.
4. In Provider mode, Ethernet frames are tagged with the provider's VLAN ID before they enter into the provider's network/backbone.
5. Enter a Provider VLAN ID and Priority. The VLAN ID must be in the range of 2 to 4094. The VLAN Priority must be in the range of 0 to 7. You may also change the TPID from the default as shown.
6. Click **Save** to have your changes take effect.
7. If you are using VLAN tagging, click the **Tag** radio button.

Note

This facility is provided to enable a connection through legacy switches requiring it. Otherwise, there is no need to change the TPID.

8. In Tag mode, Ethernet frames are tagged or untagged to distinguish between different networks.



LAN1

On

○ Provider ● Tag

SU Ingress Traffic	SU Egress Traffic
Transparent	Transparent

9. For completely transparent passages of tagged frames, there is nothing further to do. Click **Save** to have your changes take effect.

10. However, if you wish to not have transparent passages of frames, the following table shows the possible settings for each combination of Ingress and Egress modes:

Ingress	**Transparent**	Frames are not modified and are forwarded transparently.
	Tag	Enter a VLAN ID (1-4094) and Priority (0-7).

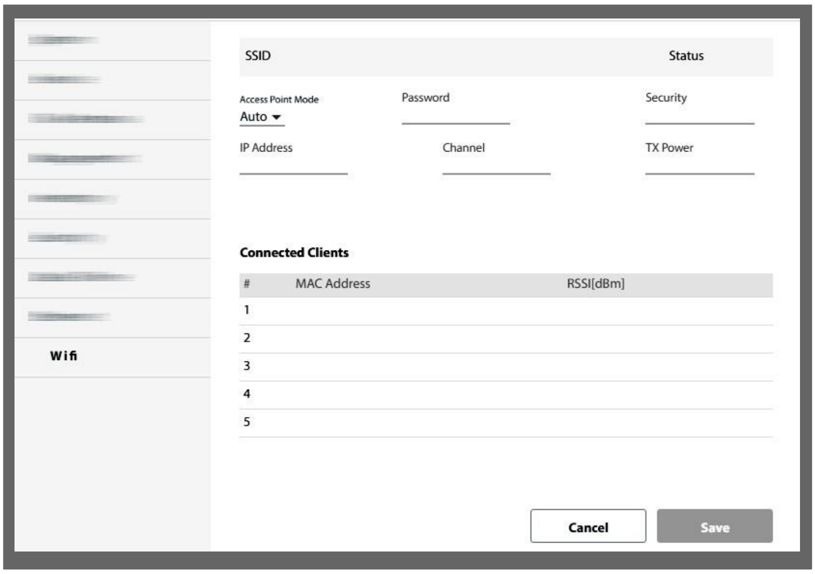
Egress	**Transparent**	Frames are not modified and are forwarded transparently.
	Untag All	All frames with a VLAN tag are untagged.
	Filter	Allow up to 4 VLAN IDs to be passed through.
	Untag Filtered	Allow VLAN IDs: • Allow up to 4 VIDs to be passed through. Untag: • Untag the VLAN tag of the selected VLAN IDs.

11. Click **Save** to have your changes take effect.

Quality Detection

Quality Detection allows you to configure the HBS to send an indication when link quality degrades. You must configure some parameters from the SU. See SU side.

2.3.20. WiFi (SU only)



SSID Status

Access Point Mode: Auto

Password

Security

IP Address

Channel

TX Power

Connected Clients

#	MAC Address	RSSI[dBm]
1		
2		
3		
4		
5		

The SSID status, Security method, and On status of the WiFi unit are displayed.

Access Point Mode: Turn On or Off the WiFi for the device. Auto allows the system to determine if the WiFi needs to be used.

You can set the following WiFi parameters:

- WiFi password
- WiFi IP address
- WiFi channel
- WiFi Tx power

Connected Clients: This area shows up to 5 clients that are connected to this unit, including their MAC addresses and signal strength (RSSI).

Note

The SSID of the WiFi is R- [serial number of unit].

Click **Save** to have your changes take effect.

2.3.21. Events

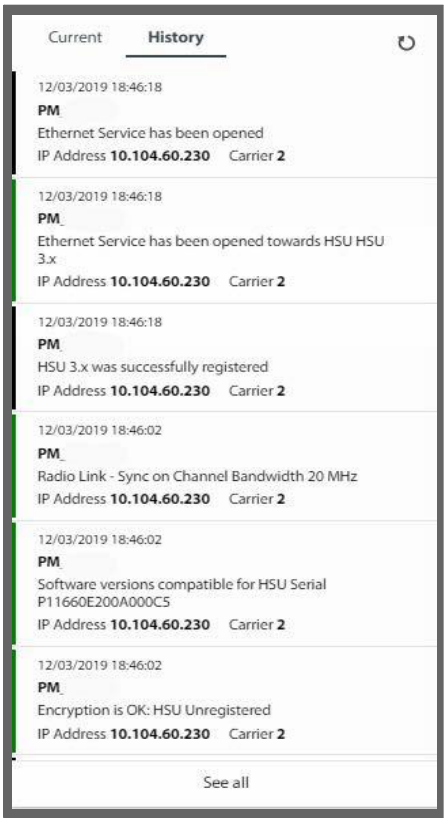
Events

This feature allows you to see events for any or all units.

1. To display the Events Log, first select the unit or units for which you want to display events. You can select any combination of units.

2. Click on the Events icon in the upper panel of the Web page Events ; The events are displayed in the partial Events Log. This is a small version of the complete Events Log, and shows a list of events according to the date and time they occurred, its source, a description of the event, IP address of the source, and on which Carrier the event was recorded.

3. Click **Current** to see all alarms since the last login (these are cleared once the alarm condition is removed) or click **History** to see all events recorded.



12/03/2019 18:46:18
PM
Ethernet Service has been opened
IP Address 10.104.60.230 Carrier 2

12/03/2019 18:46:18
PM
Ethernet Service has been opened towards HSU HSU 3.x
IP Address 10.104.60.230 Carrier 2

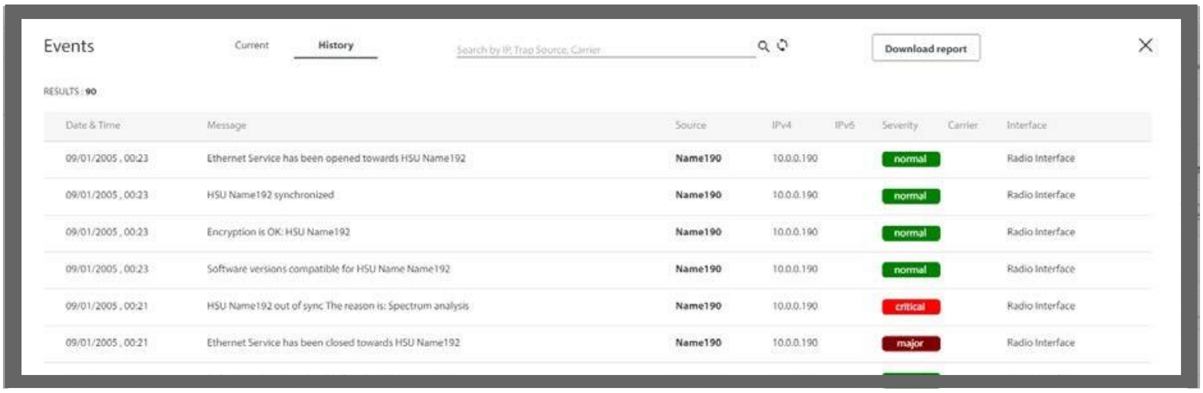
12/03/2019 18:46:18
PM
HSU 3.x was successfully registered
IP Address 10.104.60.230 Carrier 2

12/03/2019 18:46:02
PM
Radio Link - Sync on Channel Bandwidth 20 MHz
IP Address 10.104.60.230 Carrier 2

12/03/2019 18:46:02
PM
Software versions compatible for HSU Serial P11660E200A000C5
IP Address 10.104.60.230 Carrier 2

12/03/2019 18:46:02
PM
Encryption is OK: HSU Unregistered
IP Address 10.104.60.230 Carrier 2

4. Click **See all** to see the full Events Log.



RESULTS : 90

Date & Time	Message	Source	IPv4	IPv6	Severity	Carrier	Interface
09/01/2005 , 00:23	Ethernet Service has been opened towards HSU Name192	Name190	10.0.0.190		normal		Radio Interface
09/01/2005 , 00:23	HSU Name192 synchronized	Name190	10.0.0.190		normal		Radio Interface
09/01/2005 , 00:23	Encryption is OK: HSU Name192	Name190	10.0.0.190		normal		Radio Interface
09/01/2005 , 00:23	Software versions compatible for HSU Name Name192	Name190	10.0.0.190		normal		Radio Interface
09/01/2005 , 00:21	HSU Name192 out of sync The reason is: Spectrum analysis	Name190	10.0.0.190		critical		Radio Interface
09/01/2005 , 00:21	Ethernet Service has been closed towards HSU Name192	Name190	10.0.0.190		major		Radio Interface

The Events Log records system failures, loss of synchronization, loss of signal, compatibility problems, and other fault conditions and events.

5. The Events Log may be saved as an Excel or PDF file. Click **Download report** to do so.

   The Events Log includes the following fields:

   » Date and time stamp

   » Message

   » Trap source (if the source is a radio unit, this is its name)

   » IP address of the unit that initiated the alarm - IPv4 or IPv6. Use the pull-down menu here to filter the list according to the indicated criteria.

   » Severity of the trap (color-coded):

Critical	🟥
Major	🟫
Minor	🟪
Warning	🟦
Normal	🟩
Info	⬛

   » Carrier on which the trap was found (Carrier 1 or Carrier 2).

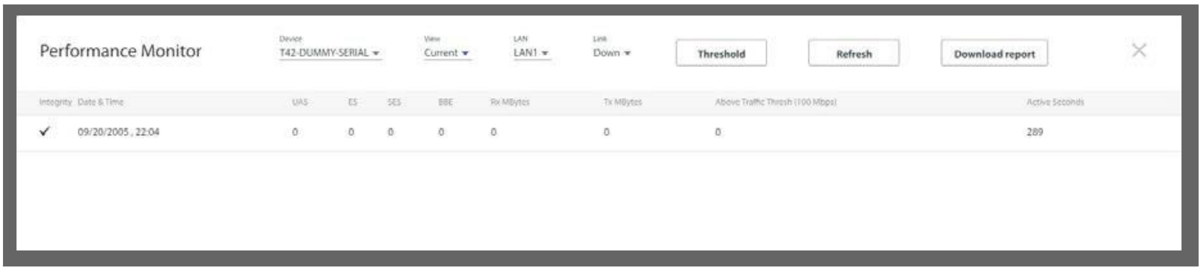
   » Interface of the trap.

6. Click **Current** to see all alarms since the last login (these are cleared once the alarm condition is removed) or click **History** to see all events recorded.

7. You can filter the list of messages by IP or trap source by entering the desired item in the field at the top center of the window and clicking the spyglass icon.

2.3.22. Performance

The Performance Monitoring feature constantly monitors traffic over the radio link and collects statistics data for the air interface and Ethernet ports.



Performance Monitor

Device: T42-DUMMY-SERIAL ▾ View: Current ▾ LAN: LAN1 ▾ Link: Down ▾

Integrity	Date & Time	UAS	ES	SES	BBE	Rx MBytes	Tx MBytes	Above Traffic Thresh (100 Mbps)	Active Seconds
✓	09/20/2005 , 22:04	0	0	0	0	0	0	0	289

When you click on this icon, the Performance Monitor window opens. It differs slightly if you are accessing an HBS or an SU.

You have the following options:

Device Click this pull-down menu and select a radio to display its results

View This pull-down menu has the following options:

- Current - gives you the latest entry.

- 15 Minutes - provides date in a scroll down list in 15 minute intervals.

- Daily (24 hours) - shows result for the last 30 days at midnight.

LAN This pull-down menu allows you to view results from LAN1 or LAN2 (See LAN Ports for an explanation of the input ports).

Link This pull-down menu allows you to select between the downlink and the uplink directions.

Threshold Click on this button to set the upper traffic threshold for reporting. The units used depends on the specific parameter. Traffic conditions above the threshold indicate congestion and probably lost frames.

Refresh Click on this button to refresh the view to include more recent data.

Download report Click on this button to save the report as an Excel file or PDF.

The meaning of the column headings is shown in the following table:

Column Heading	Description
Integrity	Valid data flag: Green tick for current and valid; Red cross for invalidated data. Note that the Performance Monitoring data is not valid if not all the values were stored (e.g., due to clock changes within the interval or power up reset).
Date & Time	Time stamp: Data is recorded every 15 minutes; the last 30 days of recordings are maintained. Roll-over is at midnight.
UAS	Unavailable Seconds: Seconds in which the interface was out of service.
ES	Errored seconds: The number of seconds in which there was at least one error block.
SES	Severe Errored Seconds: The number of seconds in which the service quality was low, as determined by the BBER threshold.
BBE	Background Block Error: The number of errored blocks in an interval.
Rx MBytes	Received Mbytes: The number of Megabytes received at the specified port within the interval.
Tx MBytes	Transmitted Mbytes: The number of Megabytes transmitted at the specified port within the interval.

Column Heading	Description
Above Traffic Thresh	Threshold set in the previous step: Seconds count when actual traffic exceeded the threshold.
Active Seconds	The number of seconds that the configured Ethernet service was active for (available for HBS only).

If you have selected an SU, you will see the following additional parameters:

Column Heading	Description
Min RSL (dBm)	Minimum Receive Signal Level: The minimum of the receive signal level (measured in dBm).
Max RSL (dBm)	Maximum Receive Signal Level: The maximum of the receive signal level (measured in dBm).
RSL Thresh 1 (-88dBm)	Receive Signal Level Threshold: The number of seconds in which the Receive Signal Level (RSL) was below the specified threshold.
RSL Thresh 2 (-88dBm)	Receive Signal Level Threshold: The number of seconds in which the RSL was below the specified threshold.
Min TSL (dBm)	Minimum Transmit Signal Level: The minimum of the transmit signal level (measured in dBm).
Max TSL (dBm)	Maximum Transmit Signal Level: The maximum of the transmit signal level (measured in dBm).
TSL Thresh (25 dBm)	Transmit Signal Level Threshold: The number of seconds in which the Transmit Signal Level (TSL) was above the specified threshold.
BBER Thresh (1.0%)	Background Block Error Ratio Threshold: The number of seconds in which the Background Block Error Ratio (BBER) exceeded the specified threshold.
Rx MBytes	Received Mbytes: The number of Megabytes received at the specified port within the interval.
Tx MBytes	Transmitted Mbytes: The number of Megabytes transmitted at the specified port within the interval.
Below Capacity Thresh	Seconds count when throughput fell below the predefined threshold value.
Above Traffic Thresh	Threshold set in the previous step: Seconds count when actual traffic exceeded the threshold.

2.3.23. Spectrum

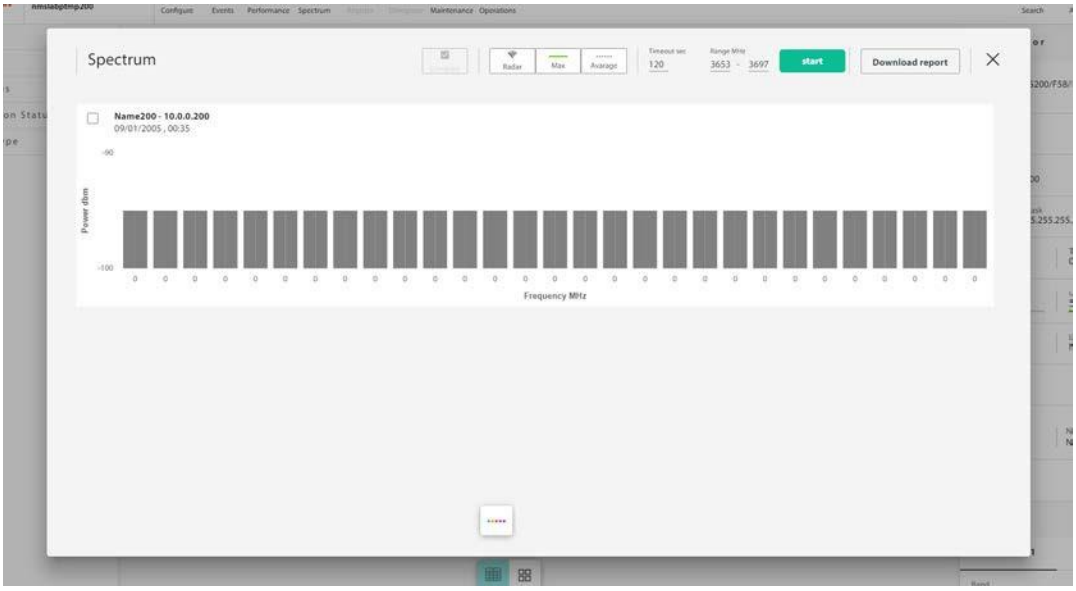
The Spectrum feature is an RF survey tool that provides spectral measurement information: power vs. frequency. You can view real-time spectrum information, save results, and view historic spectrum scans. Separate information is generated for the HBS and SUs - all by selection. The data is stored in the radio unit itself.

The results of the Spectrum View utility are intended for use by RADWIN Customer Service to assist with diagnosing interference related problems.

Spectrum View can be opened from the HBS, or from an SU, or any combination thereof.

We assume the reader knows about RF Spectrum Analysis so detailed theoretical explanations are not needed.

1. Select the device or devices for which you want to see the Spectrum View. No more than 8 fixed SUs can be selected.
2. Click on the Spectrum View icon Spectrum.
3. If you are working with a dual-carrier unit, choose the carrier for which you want to see the Spectrum View. You can only see it for one carrier at a time.
4. The Spectrum View window will appear.



Timeout sec 120

Range MHz 3653 - 3697

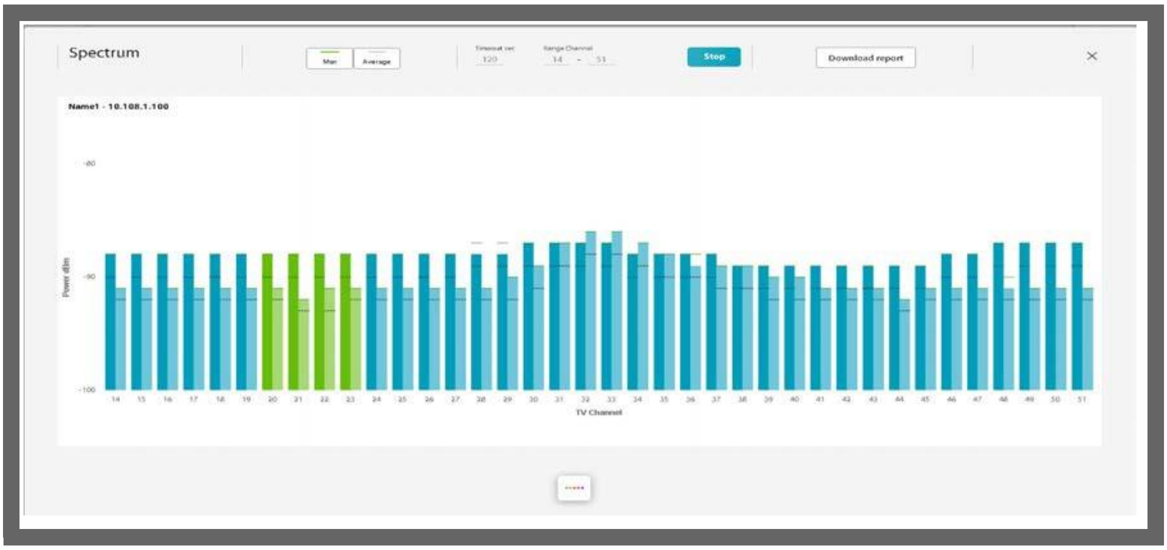
□ Name200 - 10.0.0.200
09/01/2005 , 00:35

A blank Spectrum View result display will appear, where all the bars are grey.

The name(s) of the selected unit(s) appear, together with their IP address(es), date and time.

5. To start a scan, first choose its **Timeout sec** time (top of window), which is the maximum analysis time per scan.

6. Select the frequency range (**Range MHz**, top of window) and channel range (Range Channel, top of window). You can only select allowed frequencies channels.
7. Once you are ready, click **Start** to start the scan and see the results on screen. You will be warned that this is traffic-affecting. If this is acceptable, then click **Ye**s.



Timeout sec 120

Range Channel 14 - 51

- Green bars relate to those frequencies channels as listed when you activated the HBS (See Activate the Base Station). Dark green is Antenna A, and light green is Antenna B.
- If there are frequencies channels you did not choose when you activated the HBS, their bars appear blue.
- The frequency channels the unit is working with has text that appears in blue.
- Green lines show the maximum power found for the indicated frequency channel range.
- Dotted lines show the average power found for the indicated frequency channel range.
- Radar shows/hides DFS information.
- Compare allows you to compare the results from selected units, side-by-side.

8. If you want to save the report, click **Download Report**, and select a location where to save the report file.

2.3.24. Utilization

Utilization

This feature shows how much of the available sector-wide resources of the air interface are actually being used (utilized). The information is available per carrier (for dual carrier systems), for the downlink and uplink separately, and for recent activity or for historical activity.

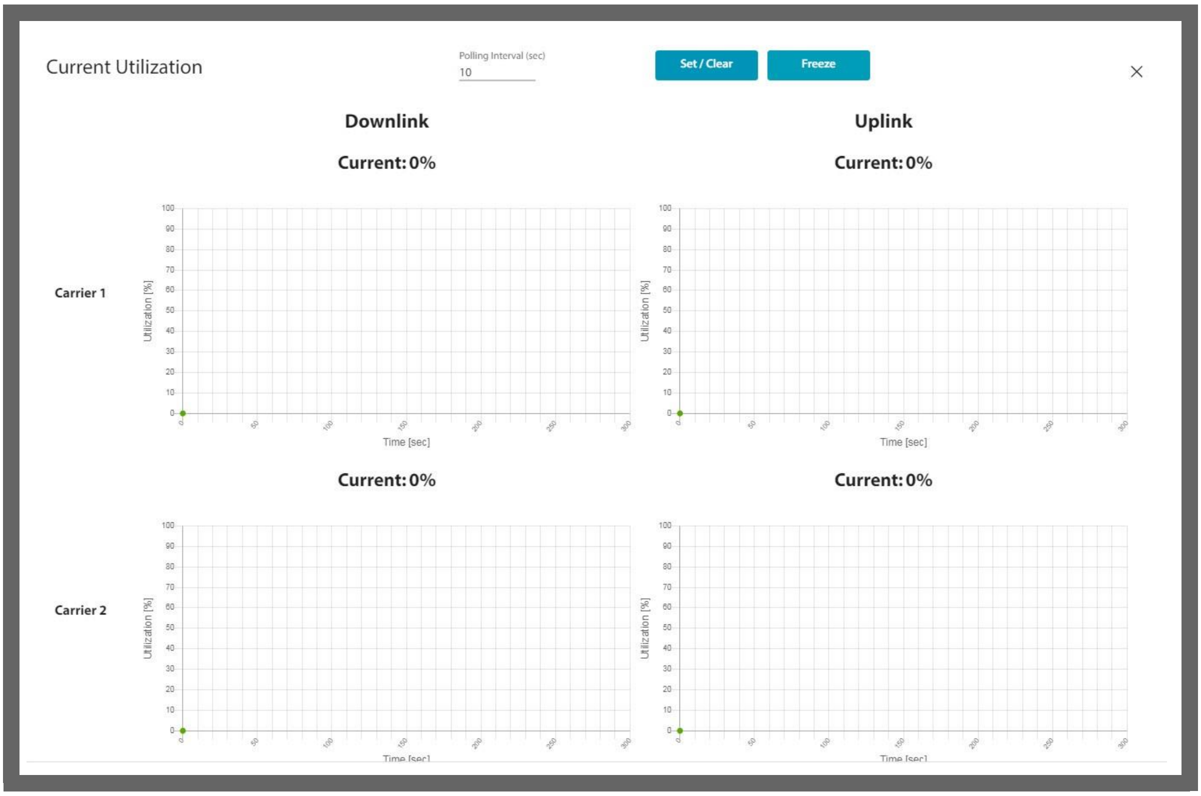
To check the utilization for the whole sector, do the following:

1. Select the HBS.

2. Click the Utilization icon (Utilization). From the pull-down menu, you have two options: *Current*, and *History*.

Current

This allows you to see the present utilization in time intervals that you can set.



Current Utilization

Polling Interval (sec)
10

Current utilization is calculated as follows:

- Set a polling interval, in seconds, the click **Set/Clear**.
- The HBS at that point takes a measurement of two parameters:

CSU: Current Symbols Used. The number of symbols (can be looked at as “bytes”) actually being transmitted in the direction indicated (UL or DL) at this point in time.

CSP: Current Symbols Possible: The number of symbols that could potentially be transmitted in the direction indicated at this point in time if 100% of the air interface was utilized.

- When the measurements are first taken, the parameters will be the “old” parameters.
- The HBS then waits the period of time you have set as the polling interval, and takes the measurements again giving “new” values. The Utilization is then defined as:

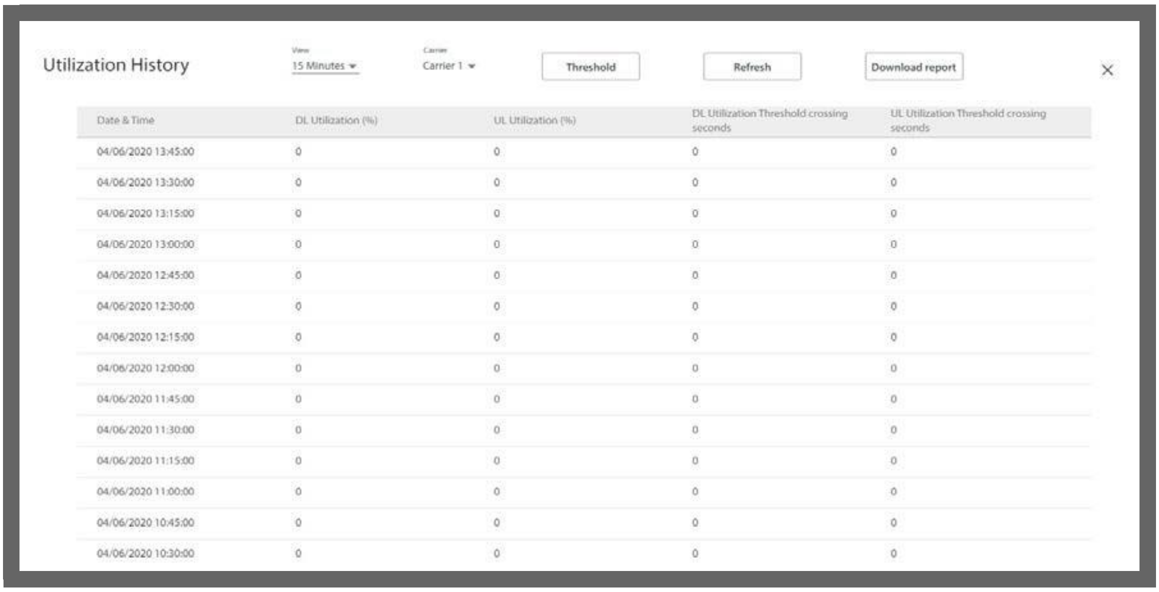
$$Utilizatoin = \frac{\boldsymbol{CSU_{new} - CSU_{old}}}{\boldsymbol{CSP_{new} - CSP_{old}}}$$

- This value is presented as a percentage in the graph, for each carrier separately, and for each direction (UL and DL) separately.
- Measurements for the next polling interval are then taken, and the process is repeated.
- To clear the graphs of data, click **Set/Clear**. The process will start over.
- To stop the displaying of new data, click **Freeze**.

History

This allows you to see the historic utilization.

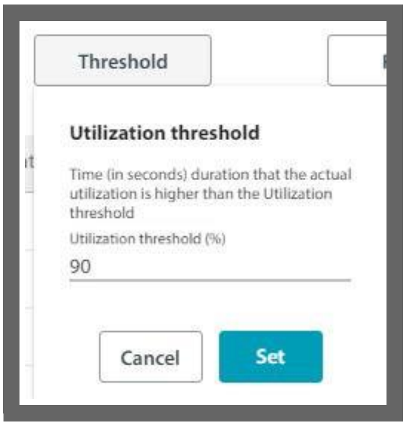
Each second, the HBS records the CSU (current symbols used) and the CSP (current symbols possible) values. The Utilization is given as a percentage: Utilization = CSU/CSP.



Date & Time	DL Utilization (%)	UL Utilization (%)	DL Utilization Threshold crossing seconds	UL Utilization Threshold crossing seconds
04/06/2020 13:45:00	0	0	0	0
04/06/2020 13:30:00	0	0	0	0
04/06/2020 13:15:00	0	0	0	0
04/06/2020 13:00:00	0	0	0	0
04/06/2020 12:45:00	0	0	0	0
04/06/2020 12:30:00	0	0	0	0
04/06/2020 12:15:00	0	0	0	0
04/06/2020 12:00:00	0	0	0	0
04/06/2020 11:45:00	0	0	0	0
04/06/2020 11:30:00	0	0	0	0
04/06/2020 11:15:00	0	0	0	0
04/06/2020 11:00:00	0	0	0	0
04/06/2020 10:45:00	0	0	0	0
04/06/2020 10:30:00	0	0	0	0

The Utilization History table works as follows:

- Set the **View** - the interval for which you want to show the average utilization. This can be the last 15 minutes or the last 24 hours, shown under **Date & Time**.
- Set the **Carrier** for which you want to see the utilization.
- **DL Utilization** - the average Downlink utilization during the course of the interval you chose. The utilization for each second is taken and an average value is made.
- **UL Utilization** - the average Downlink utilization during the course of the interval you chose. The utilization for each second is taken and an average value is made.
- **DL / UL Utilization Threshold crossing seconds** - how many seconds the utilization percentage was higher than a threshold value during the interval. For example, say there was high utilization during a holiday weekend or during a cultural event.
- **Threshold** - set the threshold percent value here. This is used to show how many seconds the utilization percentage was higher than this value. Click and set the value (default 90%), then click **Set.**



Utilization threshold

Time (in seconds) duration that the actual utilization is higher than the Utilization threshold

Utilization threshold (%)

90

- **Refresh** - Click to refresh the report view.
- **Download report** - Click to download the report in CSV or PDF format. The report will include all the utilization lines shown in the Utilization History window.

2.3.25. Carrier Switch

This feature shows “Carrier Switch” events (this feature is also called *PrimeCarrier*). The Carrier Switch feature allows non-stop transmission performance of the dual carriers, dynamically selecting the best carrier for each SU. This maximizes the SU’s capacity, link reliability and service uptime.

Note

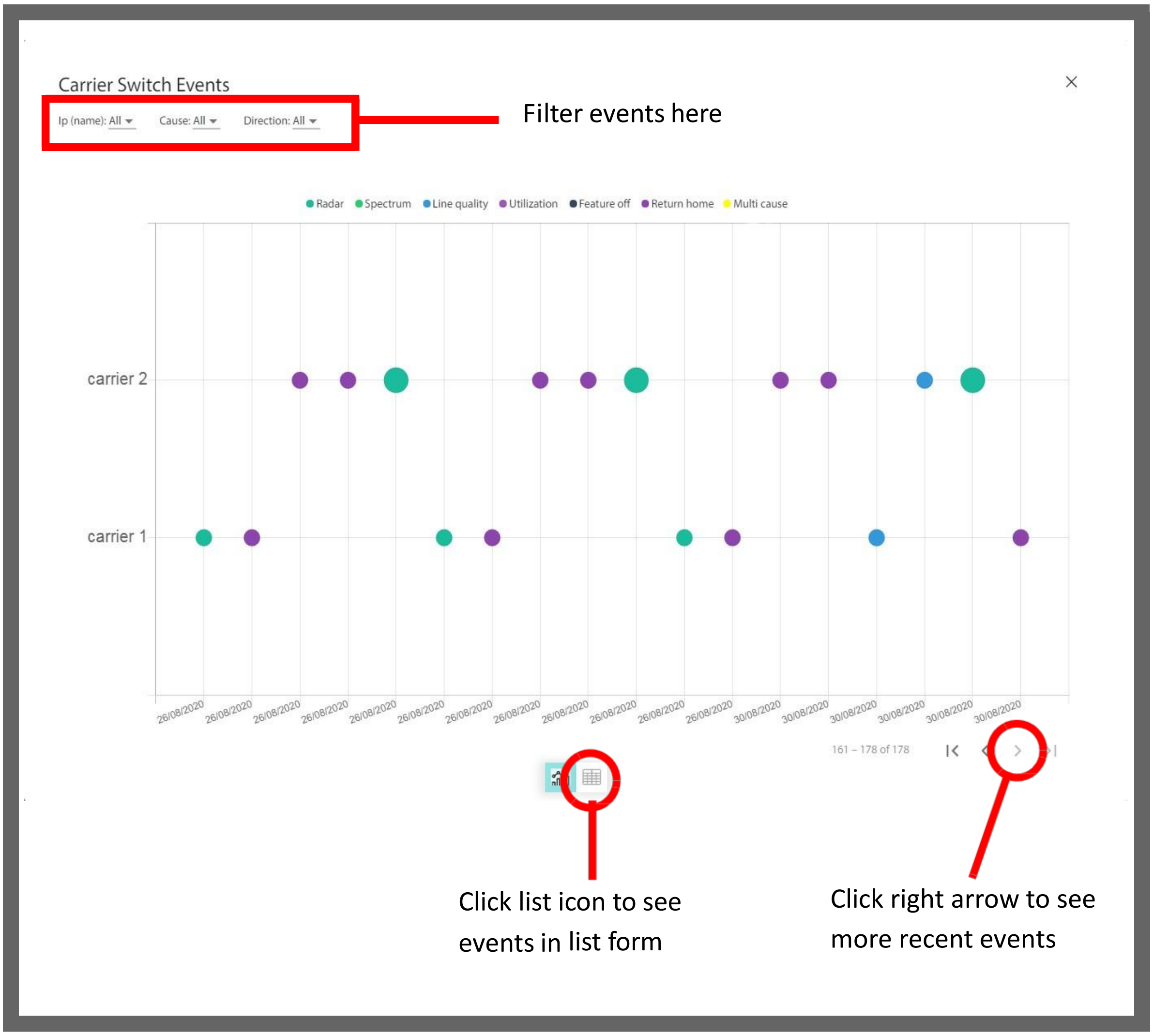
The Carrier Switch only works with SU ***PRO/AIR*** subscriber units, and only with the NEO DUO and JET-DUO 5 GHz base stations.

A Carrier Switch event occurs when a subscriber unit’s carrier is switched from the carrier on which it was originally registered (“home carrier”) to the other carrier (“alternative carrier”), or back to its home carrier.

For this feature to work, Automatic Carrier Switching must be enabled. See *Air Interface (HBS or SU directly)* -> *Advanced* for more details. Note that you can enable or disable each of the criteria.

A Carrier Switch can occur according to one or more of the following criteria: Radar, Spectrum, Line quality, or Utilization.

Click the Carrier Switch icon (Carrier Switch) in the main window to open the Carrier Switch Events display:



Carrier Switch Events

Ip (name): All ▾ Cause: All ▾ Direction: All ▾

161 – 178 of 178

● Radar ● Spectrum ● Line quality ● Utilization ● Feature off ● Return home ● Multi cause
carrier 2
carrier 1
26/08/2020
30/08/2020
×

Filter events here

Click list icon to see events in list form

Click right arrow to see more recent events

The two carriers are shown: Carrier 2 and Carrier 1.

- Each circle indicates a carrier switch event, according to the date and time it occurred.
- Large circles indicate more than one subscriber switching at that time, and smaller circles indicate only one subscriber unit switching at that time.
- Each circle is color-coded to indicate the reason for the event:

Radar - If a radar signal is detected on the carrier. If the SU detected the radar, only that SU is switched. If the base station detected the radar, all SUs on this carrier are switched. Some may lose service[1].

Spectrum - A Spectrum Carrier scan is undertaken on the carrier. Since the carrier is not available for traffic while undergoing the scan, all SUs are switched[1].

Line quality - A certain level of PER (packet error rate) is detected on the carrier (applicable only for SUs whose resource type is defined as Best-Effort).

[1] *Since each carrier supports up to 64 SUs, the number of SUs that can be switched depends on the space available in the second carrier. That is, the number of SUs that can be switched is 64 minus the number of SUs already on the second carrier.*

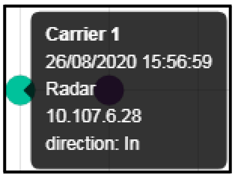
Utilization - If the utilization of the carrier rises above 80% while the utilization of the other carrier is less than 60%. A switch, in this case, balances the load between the carriers.

Feature off - The Carrier Switch feature was disabled at this point in time. All subscriber units go back to the home carrier.

Return home - The previous conditions causing the carrier switch for a specific SU no longer apply, and the SU was returned to its home carrier.

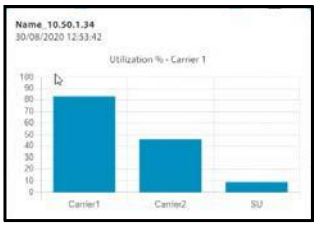
Multi cause - More than one reason caused the carrier switch.

- The date of the event is shown along the x-axis.
- You can move the dates to more recent events by clicking the right arrow at the bottom of the window.
- Mouse-over a circle to show the date and time of the switch, the reason for the switch, the IP address of the SU or SUs switched, and whether the switch is "In" (entered the specific carrier) or "Out" (exited the specific carrier).



Carrier 1
26/08/2020 15:56:59
Radar
10.107.6.28
direction: In

- Click on a small circle to show more details about the cause of the specific switch. The situation for each carrier can be shown in addition to that of the subscriber unit that underwent the switch.

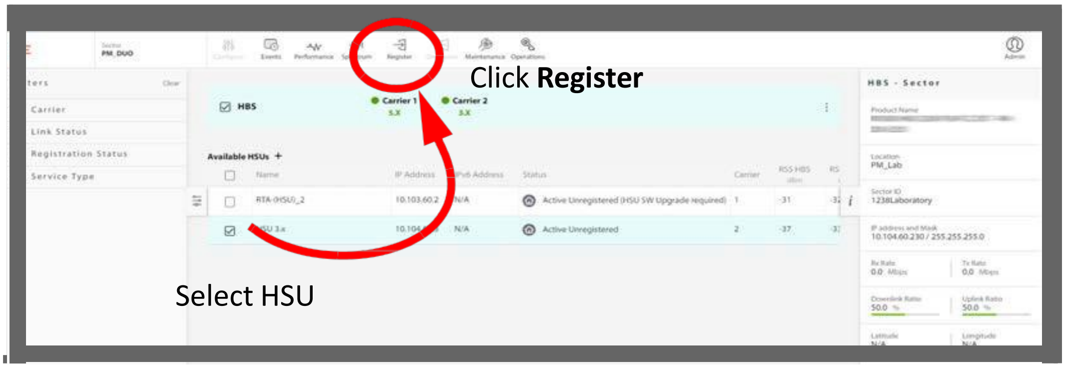


- You can show the events in list form by clicking the list icon on the bottom of the window: (▦). The list also shows the MAC address of the subscriber unit and allows you to down the report in CSV or PDF format.
- You can filter the events shown by the IP of the SU, the cause of the event, and the direction of the event ("In" or "Out").

2.3.26. Register

To enable the SU to communicate with the HBS, you must *register* it.

1. Select the SU you want to register by placing a checkmark next to it.



□	Name	IP Address	IPv6 Address	Status	Carrier	RSS HBS dBm	RS
□	RTA-(HSU)_2	10.103.60.2	N/A	Active Unregistered (HSU SW Upgrade required)	1	-31	-3
☑	HSU 3.x	10.104	N/A	Active Unregistered	2	-37	-3

Product Name

Location
PM_Lab

Sector ID
1238Laboratory

IP address and Mask
10.104.60.230 / 255.255.255.0

Rx Rate 0.0 Mbps | Tx Rate 0.0 Mbps

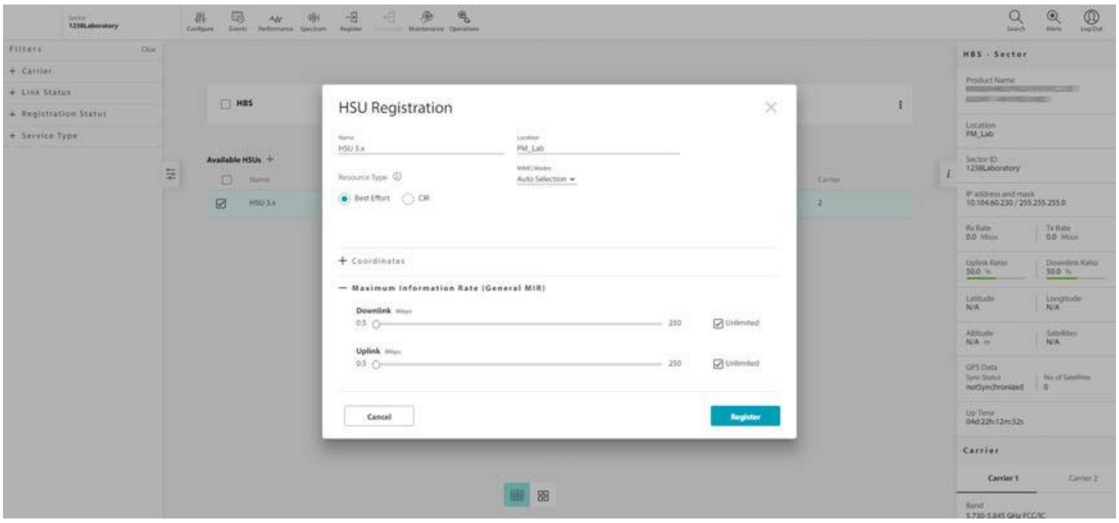
Downlink Ratio 50.0 % | Uplink Ratio 50.0 %

Latitude N/A | Longitude N/A

Click **Register**

Select HSU

2. Click **Register**. The SU Registration window will open.



HSU Registration

Name: HSU 3.x

Location: PM_Lab

Resource Type: ● Best Effort ○ CIR

MIMO Mode: Auto Selection

+ Coordinates

— Maximum Information Rate (General MIR)

Downlink Mbps: 0.5 – 250 ☑ Unlimited

Uplink Mbps: 0.5 – 250 ☑ Unlimited

3. You may edit or add the site's name, location and coordinates.

4. Select the Resource Type for the SU. This can be CIR (Committed Information Rate), or BE (Best Effort):

    - BE grants the SU resources as they become available in the sector.
    - CIR grants the SU with a certain guaranteed percentage of resources. You set this percentage in the General MIR window.

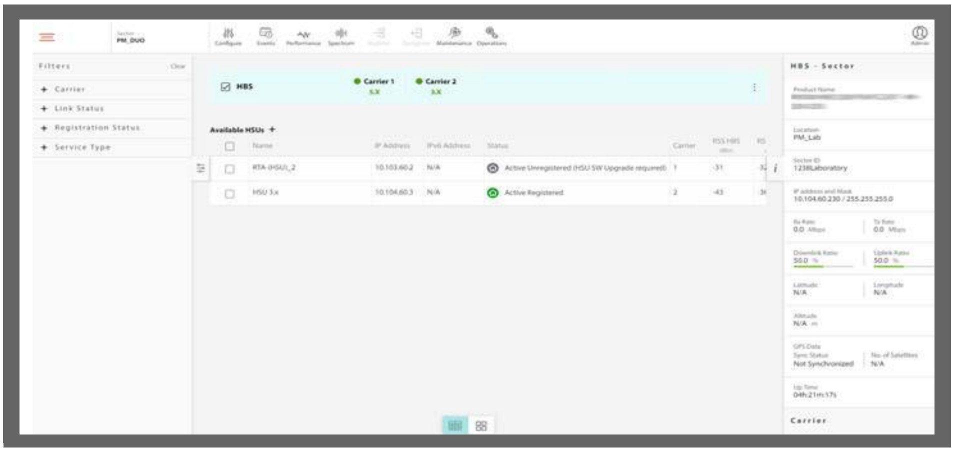
5. Check a MIMO Mode for this SU:

    - Spatial Multiplexing (default) splits the data in to two streams on transmission and recombines it on reception, providing maximum throughput.
    - Diversity transmits the same data from both antennas and checks for correctness on reception. This mode helps to ensure more reliable data transmission in a noisy environment, although throughput will be lower.
    - Auto Selection instructs the system to choose whichever mode is most efficient.

6. Optionally, you can choose the **Maximum Information Rate**. Use the sliders to set the maximum throughput rate you want for the specific SU in each direction: down link and up link. You can choose a value, or click the Unlimited checkbox.

    - *If you chose the BE resource type in Step 4. above, continue to Step 7.*
    - *If you chose the CIR resource type in Step 4. above, continue to Step 8.*

7. If you chose the BE resource type in Step 4. above, click the Register button. In a few moments, the SU will be registered.



Filters Clear

- Carrier
- Link Status
- Registration Status
- Service Type

☑ HBS ● Carrier 1 5.X ● Carrier 2 5.X

Available HSUs +

□	Name	IP Address	IPv6 Address	Status	Carrier	RSS HBS dBm	RS
□	RTA (HSU)_2	10.103.60.2	N/A	Active Unregistered (HSU SW Upgrade required)	1	-31	32
□	HSU 5.x	10.104.60.3	N/A	Active Registered	2	-43	36

HBS - Sector

Product Name
[redacted]

Location
PM_Lab

Sector ID
1238Laboratory

IP address and Mask
10.104.60.230 / 255.255.255.0

Rx Rate 0.0 Mbps | Tx Rate 0.0 Mbps

Downlink Ratio 50.0 % | Uplink Ratio 50.0 %

Latitude N/A | Longitude N/A

Altitude
N/A m

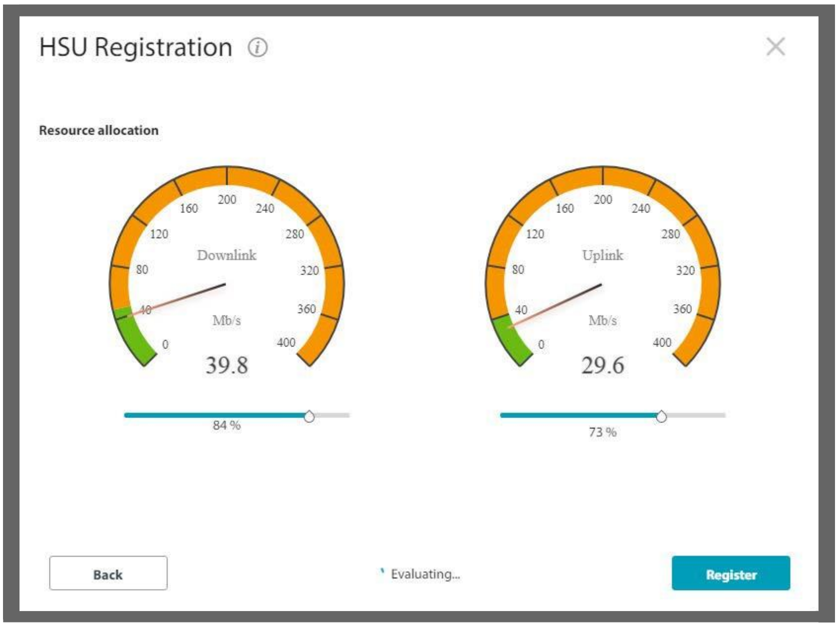
GPS Data
Sync Status Not Synchronized | No. of Satellites N/A

Up Time
04h:21m:17s

Carrier

8. If you chose the CIR resource type in Step 4 above, choose the resource allocation (**General MIR**). Use the sliders to choose the percentage of resources to be allocated to the SU. This is the percentage of available resources in the sector. Obviously, you must make sure that the resource percentages of all the SUs in the sector do not add up to more than 100%. Once you have set the values, click **Evaluate.**

Evaluation dials will appear.

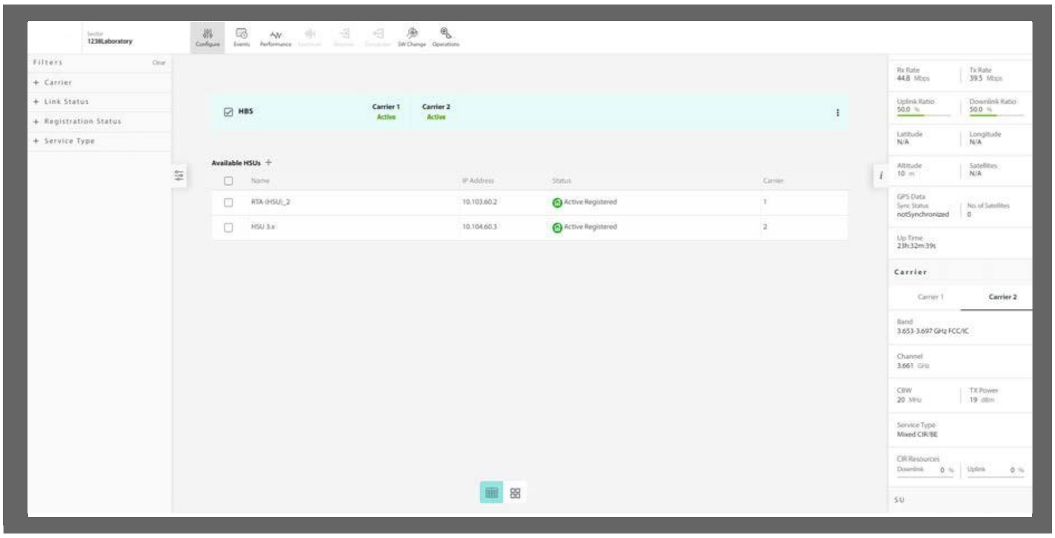


HSU Registration ⓘ

Resource allocation

9. When a stable value is reached, the **Register** button will become enabled.

10.Click **Register**.



☑ HBS | Carrier 1 Active | Carrier 2 Active

Available HSUs +

☐	Name	IP Address	Status	Carrier
☐	RTA-(HSU)_2	10.103.60.2	Active Registered	1
☐	HSU 3.x	10.104.60.3	Active Registered	2

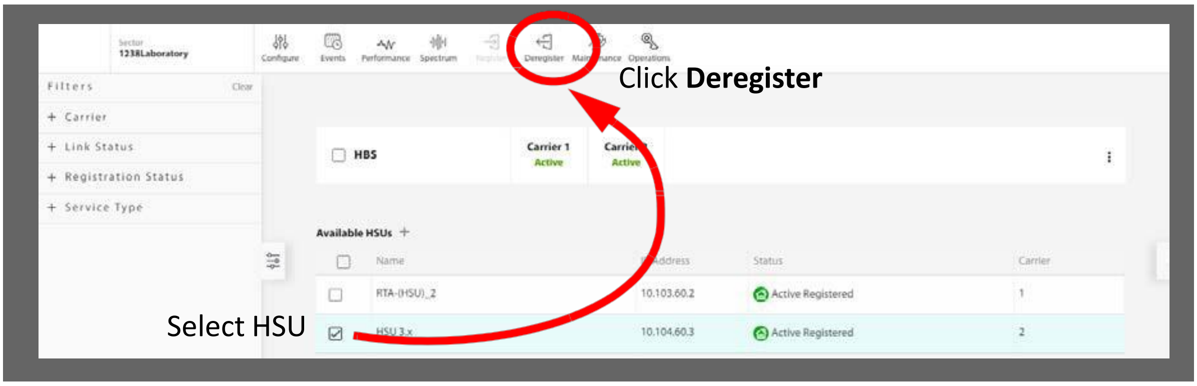
Rx Rate 44.8 Mbps | Tx Rate 39.5 Mbps
Uplink Ratio 50.0 % | Downlink Ratio 50.0 %
Latitude N/A | Longitude N/A
Altitude 10 m | Satellites N/A
GPS Data Sync Status notSynchronized | No. of Satellites 0
Up Time 23h:32m:39s

Carrier: Carrier 1 | Carrier 2
Band 3.653-3.697 GHz FCC/IC
Channel 3.661 GHz
CBW 20 MHz | TX Power 19 dBm
Service Type Mixed CIR/BE
CIR Resources Downlink 0 % | Uplink 0 %
SU

2.3.27. Deregister

Deregister

1. Select the SU you want to de-register by placing a checkmark next to it.



Click **Deregister**

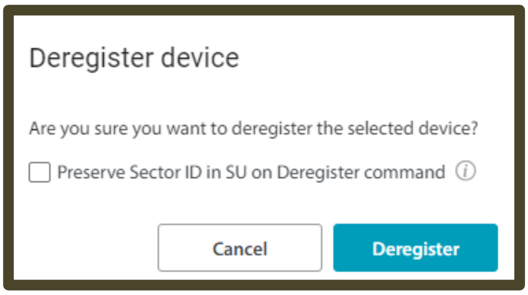
☐ HBS | Carrier 1 Active | Carrier 2 Active

Available HSUs +

☐	Name	IP Address	Status	Carrier
☐	RTA-(HSU)_2	10.103.60.2	Active Registered	1
☑	HSU 3.x	10.104.60.3	Active Registered	2

Select HSU

2. Click **Deregister**. You will be asked to confirm that you want to deregister the radio.



Deregister device

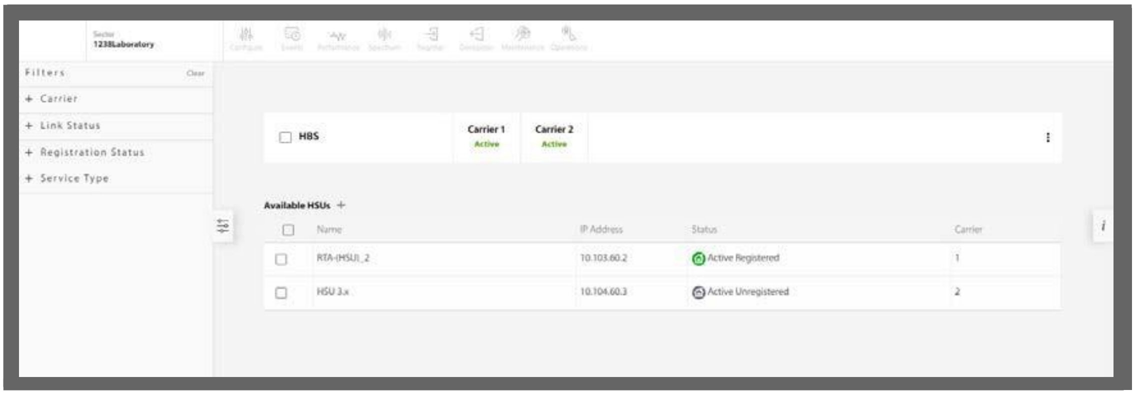
Are you sure you want to deregister the selected device?

☐ Preserve Sector ID in SU on Deregister command ⓘ

Cancel | Deregister

3. if you are sure, click **Deregister**. The device will no longer be registered.

In release 5.1.30, there is an option to preserve the Sector ID on the de-registered SU, for being used when establishing the link with this unit. Select the “Preserved Sector ID” to preserve the sector ID in the SU after the SU will be deregistered.



Sector 1238Laboratory

Filters Clear

- Carrier
- Link Status
- Registration Status
- Service Type

□ HBS	Carrier 1	Carrier 2
	Active	Active

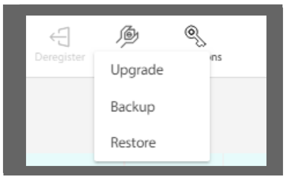
Available HSUs +

□	Name	IP Address	Status	Carrier
□	RTA-(HSU)_2	10.103.60.2	Active Registered	1
□	HSU 3.x	10.104.60.3	Active Unregistered	2

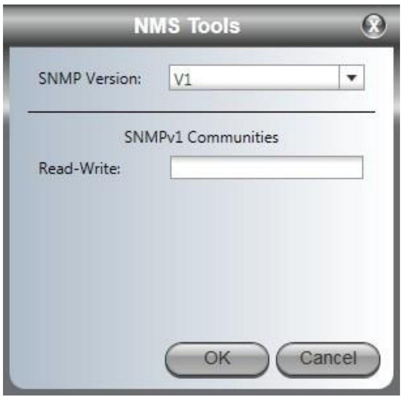
2.3.28. Maintenance

This allows you to upgrade, backup, or restore the target software.

Choose the action you want from the pull-down menu.



- Any of these actions requires the NMSTools.exe application. This is the RADWIN Manager, which must be installed on your computer[1]. When you choose any of these options, you will be asked if you want to open this application. Click **Open NMSTools.exe** to open the application.



SNMP Version: V1

SNMPv1 Communities

Read-Write:

- Enter the password netwireless, and click OK. The RADWIN Manager will open to the Software Upgrade Tool. Continue according to instructions found in the RADWIN 5000 *Configuration Guide*.

[1] *See the Configuration Guide for the RADWIN Manager for more details.*

2.3.29. Operations

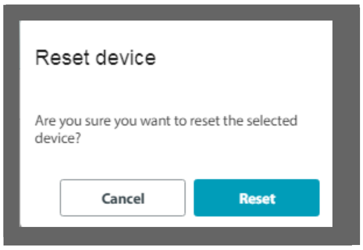
This icon allows you to perform a reset, restore the factory default settings, or to perform a license-dependent upgrade on the selected device.

Caution

If you reset a multi-carrier HBS, this affects traffic on both carriers.

Reset

When you choose Reset, you are asked to confirm. Reset is traffic-affecting, and if it is done on an HBS, it stops the traffic throughout the sector. If you are sure, click **Reset**.

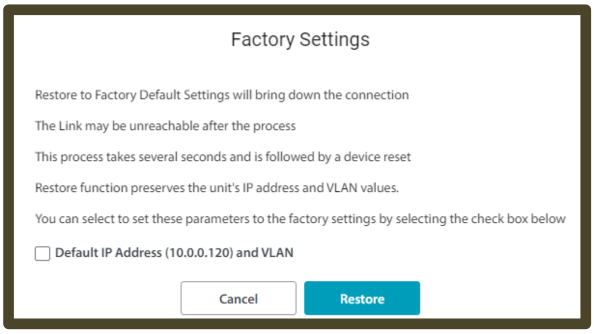


Reset device

Are you sure you want to reset the selected device?

Factory Default

When you choose Factory Default, you are asked to confirm. Since Factory Default involves a reset, it is traffic-affecting, and if it is done on an HBS, it stops the traffic throughout the sector. You have an option to restore the default IP address (10.0.0.120) and management by clicking the box next to the Default IP address. If you do not click this box, the device will retain its previous IP address and management VLAN. Once you are sure, click **Restore Defaults**, otherwise, click **Cancel.**



Factory Settings

Restore to Factory Default Settings will bring down the connection

The Link may be unreachable after the process

This process takes several seconds and is followed by a device reset

Restore function preserves the unit's IP address and VLAN values.

You can select to set these parameters to the factory settings by selecting the check box below

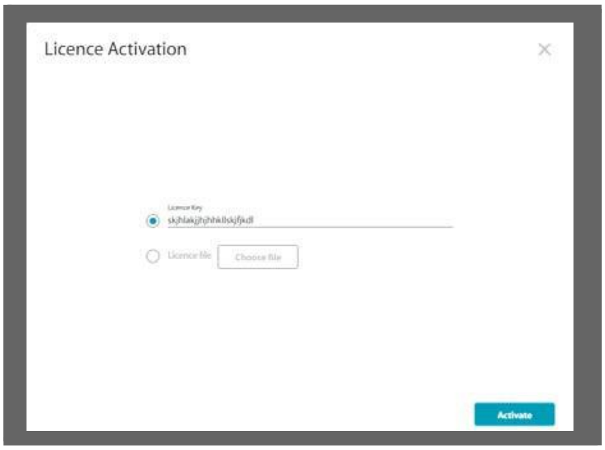
☐ Default IP Address (10.0.0.120) and VLAN

Licenses

To carry out a license-dependent upgrade, you must first acquire a license key. Do this as follows:

1. Catalogue number: Contact your RADWIN representative and get a catalogue number of the upgrade you want. Purchase as many of these upgrades as you deem necessary.

2. PAKs: You will receive a list of Product Activation Keys (PAK) for each upgrade instance. A PAK number can be used on any compatible RADWIN product; they are not specific to any one given item of equipment.
3. Activate PAKs: Associate each PAK to a specific item of equipment: Access the License Key Application website (available from Professional Services), and follow the instructions there to activate each PAK for the specific item of equipment you need to upgrade.
4. Get License Keys: The License Key Application will then give you a list of license keys. These numbers *are* unique for the specific upgrade and specific item of equipment. We recommend saving this list as a text file in a convenient location.
5. Select the device for which you want to apply a license-dependent upgrade.
6. Choose Operations -> License. The License Activation window will open.



Licence Activation

● Licence Key: skjhlakjjhjhhkllskjfjkdl

○ Licence file

7. Enter the license code in the field, or click **License file**, then **Choose file** to where you have saved the license file.
8. Once you are ready, click **Activate**.
9. The unit will be reset, after which it will be upgraded using the new license.

2.3.30. Diagnostics Diagnostics

This creates diagnostic files to be used by RADWIN professional services and support personnel to expedite assistance.

1. Select the items for which you want information (HBS and/or SUs). If an item is not selected, the diagnostic files will not contain information for that item.
2. Click the icon above to open the **Get Diagnostics** window.
3. You will be warned that this could take a few minutes, depending on how many devices have been selected. If this is acceptable, click **Get Diagnostics**.
    - The main window will darken, and the **Getting monitor diagnostics** message will appear.

- After a few seconds or minutes, a comma-delimited (*.csv) file will be created and stored in the default downloads section of the managing computer. The **Getting monitor diagnostics** message will disappear.
- The format of this file name will be: **monitor-DATE TIME.csv.**
- The Diagnostics icon will then be shown with a percentage indicator below it, showing the status of the creation of the second diagnostics file: a JSON file. In addition, a small blue **diagnostics in progress** message will appear next to the Diagnostics icon.
- After a further few seconds or minutes, the JSON file will be created. This file is also stored in the default downloads section of the managing computer.
- The format of this file name will be: **diagnostics-DATE TIME.json,** accurate to the second.

4. Send these files to RADWIN professional services.

2.3.31. User Profile Icon Admin

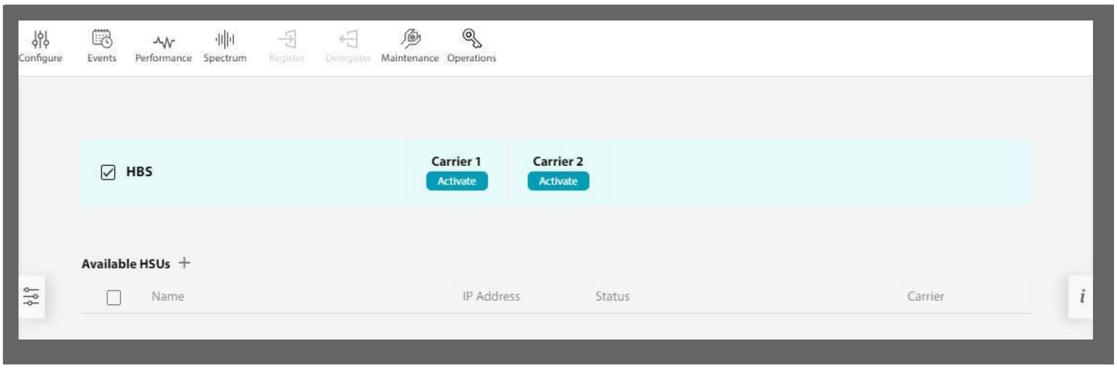
Admin, Observer, Operator, Installer

The name of the user profile will appear on the icon. Click this icon to log out of the HBS.

2.3.32. HBS List

The HBS list appears with dual-carrier products only.

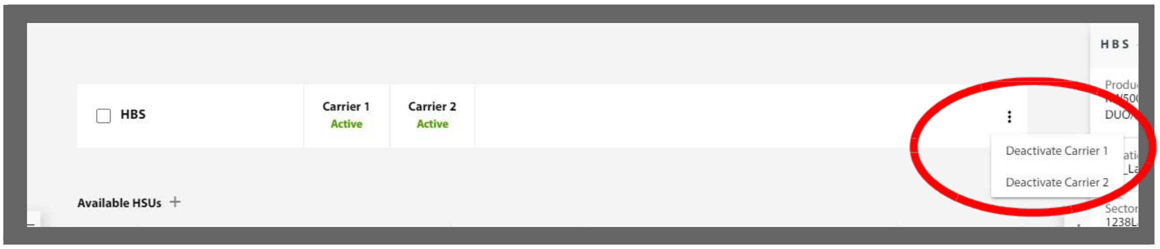
Near the top of the user interface, the status of the connected HBS is shown, together with the activation status of each Carrier.



Toactivate a carrier, click **Activate**. For further instructions, see Activate the Base Station.

Once a Carrier is activated, you can de-activate it.

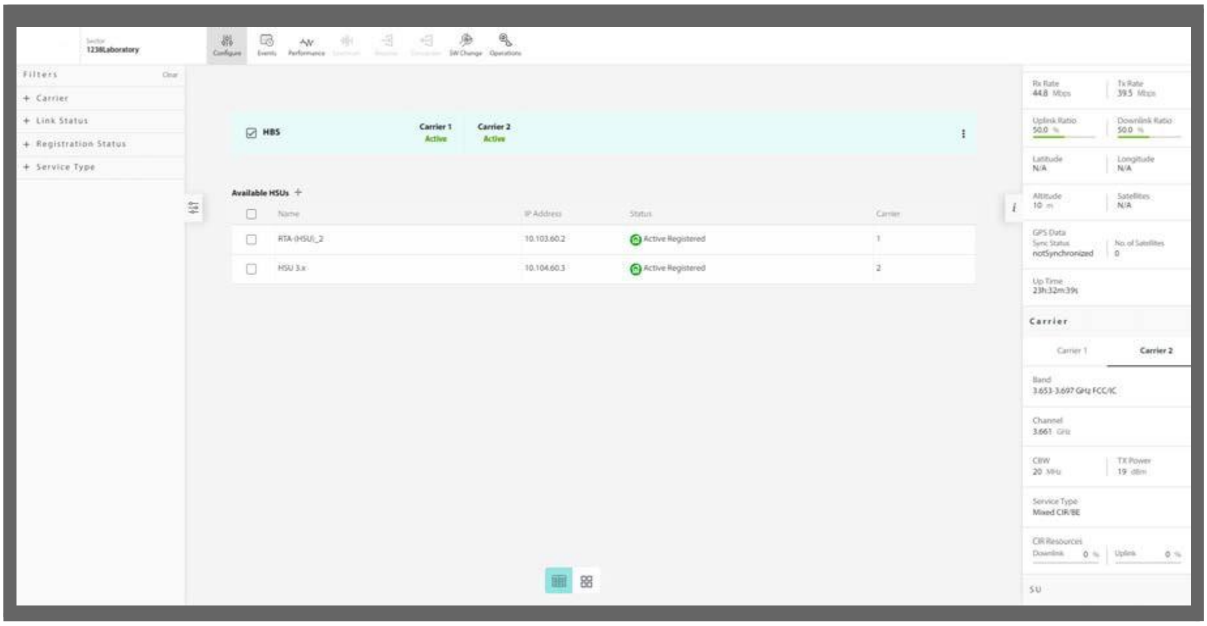
Click the vertical elipsis next to the Right Pane, then choose which Carrier you want to de-activate.



2.3.33. SU List

The central part of the user interface shows a list of the SUs that the HBS has detected. The HBS can only detect SUs if the carrier is activated (for instructions on activating a Carrier, see Activate the Base Station).

The name and IP address of the SUs (as configured) are listed, as well as their statuses and which carrier they are using (see *SU status Description* for the possible SU statuses).

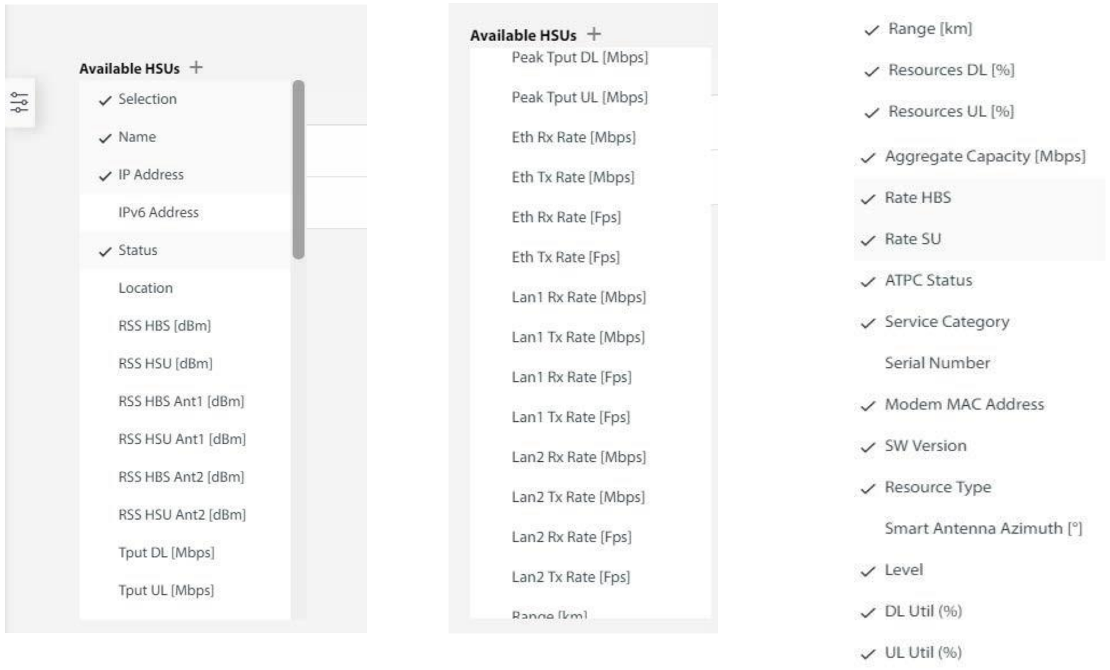


☐	Name	IP Address	Status	Carrier
☐	RTA-(HSU)_2	10.103.60.2	Active Registered	1
☐	HSU 3.x	10.104.60.3	Active Registered	2

Rx Rate 44.8 Mbps
Tx Rate 39.5 Mbps
Uplink Ratio 50.0 %
Downlink Ratio 50.0 %
Latitude N/A
Longitude N/A
Altitude 10 m
Satellites N/A
GPS Data
Sync Status notSynchronized
No. of Satellites 0
Up Time 23h:32m:39s
Band 3.653-3.697 GHz FCC/IC
Channel 3.661 GHz
CBW 20 MHz
TX Power 19 dBm
Service Type Mixed CIR/BE
CIR Resources
Downlink 0 %
Uplink 0 %

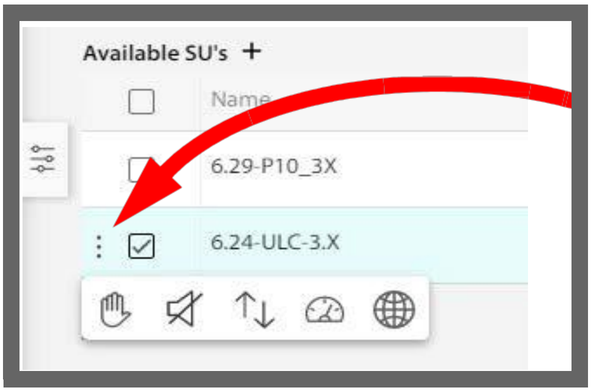
You can add other parameters as well by clicking the plus (+) sign next to the Available SUs label, and selecting the desired parameters.

Additional SU parameters, scrolling down on the list:



SU Mini Menu

At the far left of the SU line is a mini menu that provides various options. Click on the three dots at the end of the line to display this menu.



This menu allows you to carry out the actions below, but only if it is relevant for the selected unit:

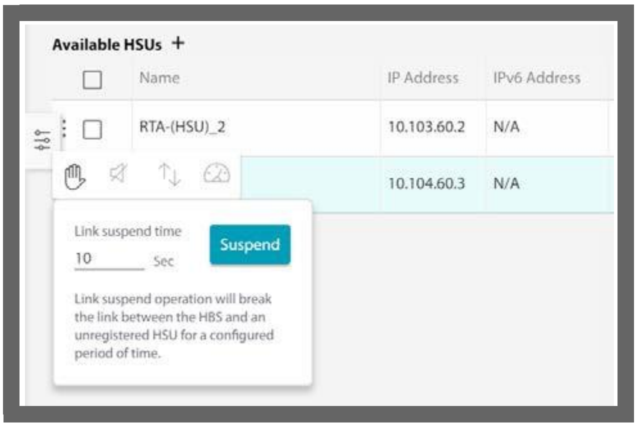
- Suspend an SU,
- Control the SU's Buzzer (if relevant for the specific model).
- Replace a defective SU with an operative SU, and transfer all configurations.
- Carry out a Speed Test.
- Confirm service activation, if required by the RADIUS Authorization Server.

Suspend

Remove the selected subscriber unit from the list for a specified period of time that you determine. You can only suspend an un-registered subscriber unit.

1. Click on the SU mini menu, then click on the Suspend icon: ✋

2. From the window that appears, select the amount of time for which you want to suspend the SU, then click **Suspend.**



Available HSUs +

□	Name	IP Address	IPv6 Address
□	RTA-(HSU)_2	10.103.60.2	N/A
		10.104.60.3	N/A

Link suspend time

10 Sec

Suspend

Link suspend operation will break the link between the HBS and an unregistered HSU for a configured period of time.

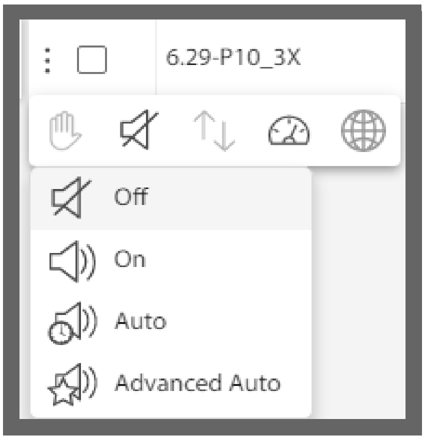
The suspended SU will disappear from the HBS's list. After the time has elapsed, the SU will re-appear only if it re-syncs to the HBS.

Buzzer

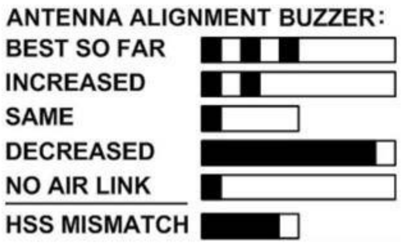
This option is only enabled if the selected SU has a buzzer.

Click on the SU mini menu, then click on the Buzzer icon: 🔇

The Buzzer button turns the buzzer On or Off.



- The Auto position means that the Buzzer will beep, as shown in the figure below, during installation or upon sync loss. The main use of the buzzer tone is for SU antenna alignment.
- The Advanced Auto position means that the buzzer will beep continuously at different rates upon sync loss, antenna misalignment, and other events for up to two minutes following restoration of sync.



Replace

A defective SU may be replaced by another SU belonging to the sector provided that the replacement is not registered.

When doing so, the new SU receives the configuration parameter values of the replaced SU.

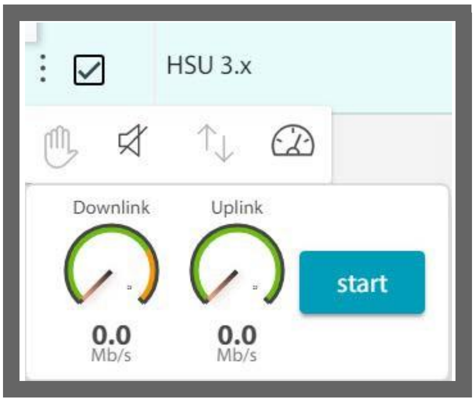
1. Click on the SU mini menu, then click on the Replace icon: ⇅
2. You are offered a list of SUs available as replacements.
3. Select the required unit by clicking on it.
4. You are asked to confirm before proceeding, do so.
5. Once the unit was replaced successfully, a confirmation message will appear. Note that all of the configuration parameters from the replaced unit will appear in the new unit.

Speed Test

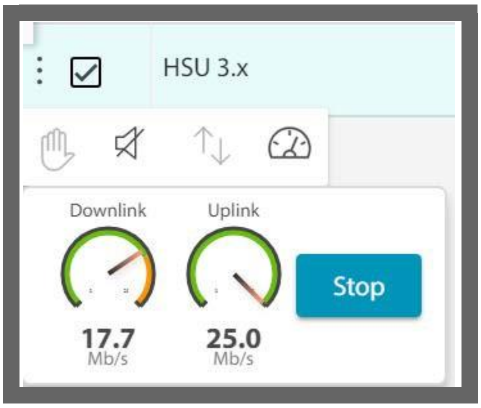
This graphically shows the real-time throughput in the downlink and uplink direction of the selected SU.

You can only carry out a speed test on a registered SU.

1. Click on the SU mini menu, then click on the Speed Test icon:
2. Click **Start** to start the test.



The Downlink and Uplink dials will show the speed in each direction.



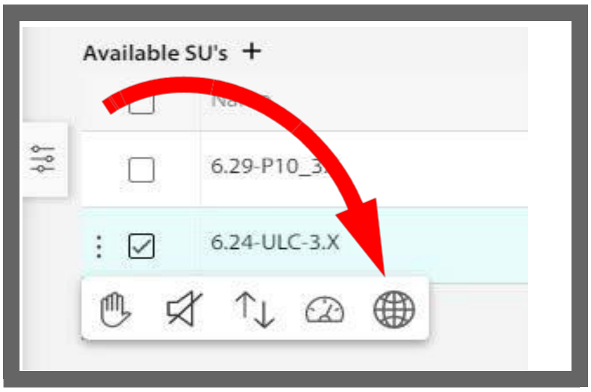
3. Click **Stop** to stop the test.

Note

Running the Speed Test does not affect the utilization measurement because the Speed Test is not data traffic.

Confirm service activation

- **If Service Activation Confirmation Required** was enabled when configuring the RADIUS Authorization Server, select this to confirm the service activation.

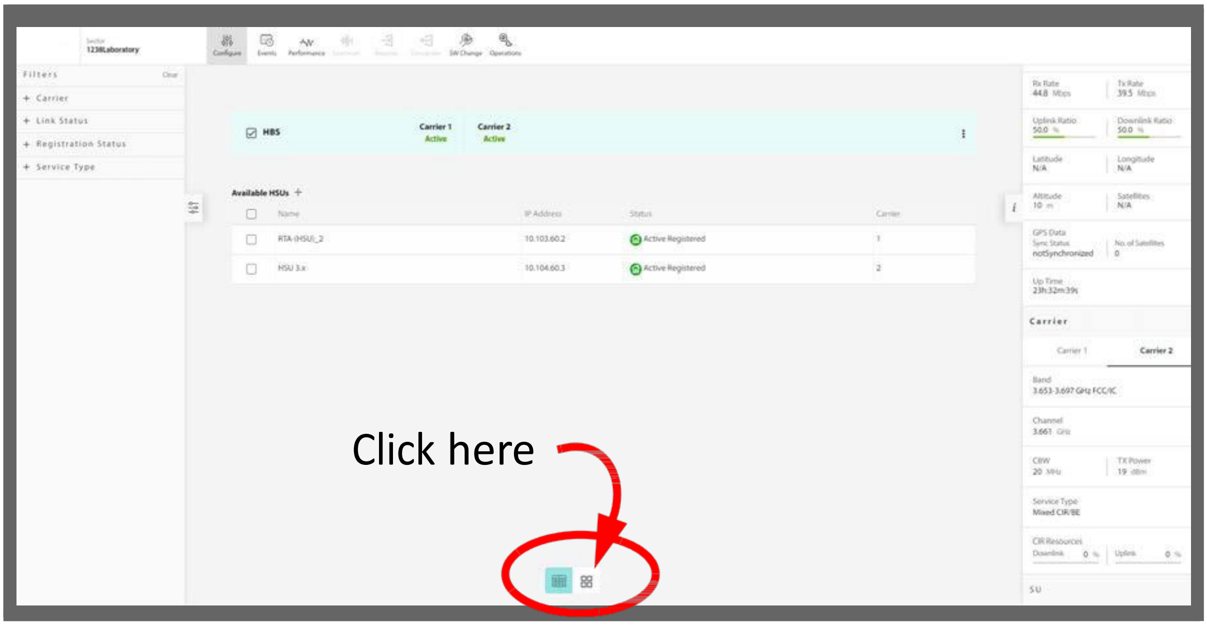


2.3.34. Sector Display views

The default view of the sector (list of SUs) is in a table format.

However, you can display information about the SUs in a card-like format as well.

Click the four-square symbol on the bottom of the user interface.



☑ HBS | Carrier 1 Active | Carrier 2 Active

Available HSUs +

□	Name	IP Address	Status	Carrier
□	RTA-(HSU)_2	10.103.60.2	Active Registered	1
□	HSU 3.x	10.104.60.3	Active Registered	2

Rx Rate 44.8 Mbps | Tx Rate 39.5 Mbps

Uplink Ratio 50.0 % | Downlink Ratio 50.0 %

Latitude N/A | Longitude N/A

Altitude 10 m | Satellites N/A

GPS Data Sync Status notSynchronized | No. of Satellites 0

Up Time 23h:32m:39s

Carrier

Carrier 1 | Carrier 2

Band 3.653-3.697 GHz FCC/IC

Channel 3.661 GHz

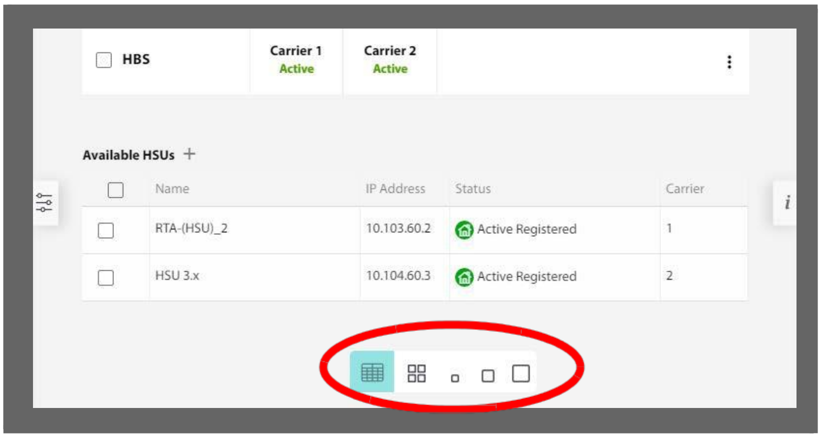
CBW 20 MHz | TX Power 19 dBm

Service Type Mixed CIR/BE

CIR Resources Downlink 0 % | Uplink 0 %

SU

Various card size options will appear.



□ HBS | Carrier 1 Active | Carrier 2 Active

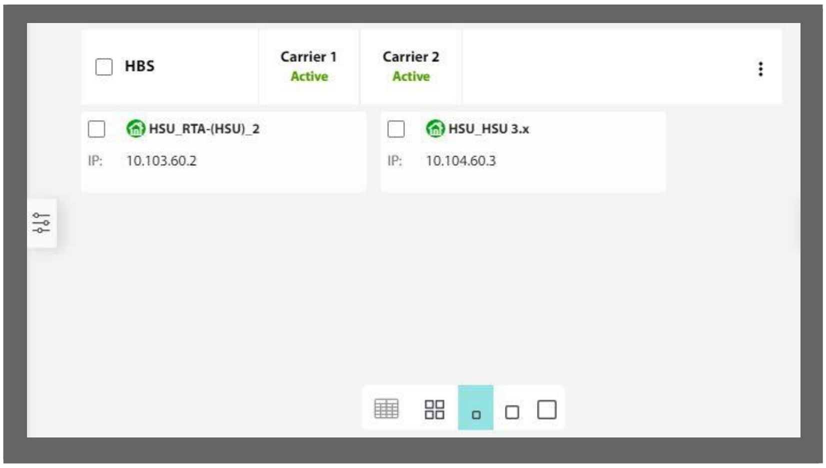
Available HSUs +

□	Name	IP Address	Status	Carrier
□	RTA-(HSU)_2	10.103.60.2	Active Registered	1
□	HSU 3.x	10.104.60.3	Active Registered	2

The size options are small, medium, and large.

Click on the small card option, and the information for the SUs will be displayed in small cards with minimal information:

- Unit name, status
- IP address



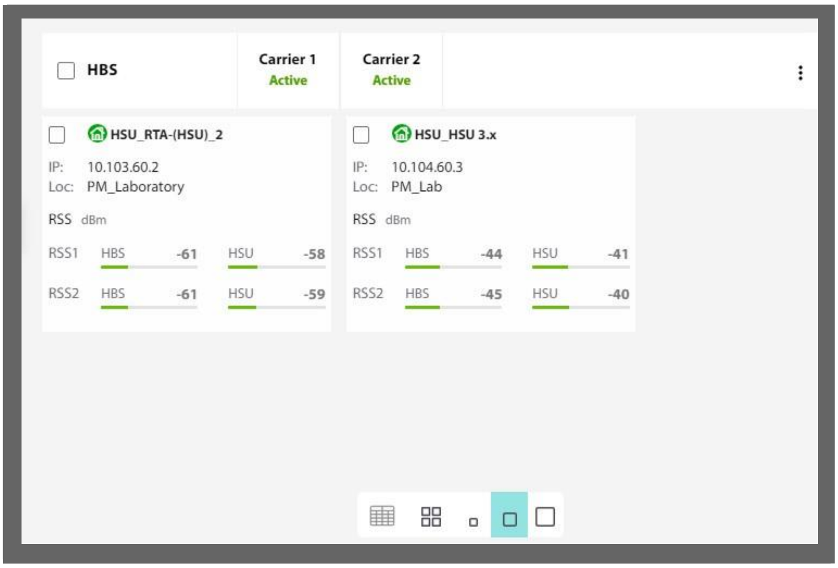
□ HBS | Carrier 1 Active | Carrier 2 Active

□ HSU_RTA-(HSU)_2
IP: 10.103.60.2

□ HSU_HSU 3.x
IP: 10.104.60.3

Click on the medium card option, and the information for the SUs will be displayed in medium-sized cards with more information:

- Unit name, status
- IP address
- Location
- RSS for each stream (RSS1 and RSS2), on both the HBS side and the SU side.



□ HBS

Carrier 1 Active

Carrier 2 Active

□ HSU_RTA-(HSU)_2

IP: 10.103.60.2

Loc: PM_Laboratory

RSS dBm

RSS1 HBS -61 HSU -58

RSS2 HBS -61 HSU -59

□ HSU_HSU 3.x

IP: 10.104.60.3

Loc: PM_Lab

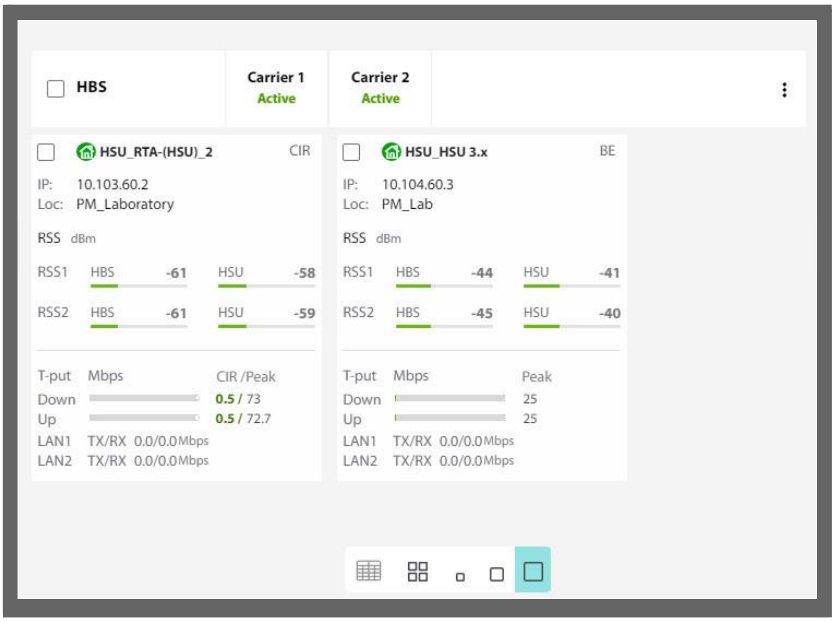
RSS dBm

RSS1 HBS -44 HSU -41

RSS2 HBS -45 HSU -40

Click on the large card option, and the information for the SUs will be displayed in large-sized cards with yet more information than the medium cards.

- Unit name, status
- Service category (CIR or BE)
- IP address
- Location
- RSS for each stream (RSS1 and RSS2), on both the HBS side and the SU side
- Throughput for the uplink and downlink
- CIR and Peak value (as per configuration)
- Tx/Rx ratio for each line (LAN1 and LAN2)
- Nomadic Level (if applicable)



□ HBS

Carrier 1 Active

Carrier 2 Active

□ HSU_RTA-(HSU)_2 CIR

IP: 10.103.60.2
Loc: PM_Laboratory

RSS dBm

RSS1 HBS -61 HSU -58
RSS2 HBS -61 HSU -59

T-put Mbps CIR /Peak
Down 0.5 / 73
Up 0.5 / 72.7
LAN1 TX/RX 0.0/0.0Mbps
LAN2 TX/RX 0.0/0.0Mbps

□ HSU_HSU 3.x BE

IP: 10.104.60.3
Loc: PM_Lab

RSS dBm

RSS1 HBS -44 HSU -41
RSS2 HBS -45 HSU -40

T-put Mbps Peak
Down 25
Up 25
LAN1 TX/RX 0.0/0.0Mbps
LAN2 TX/RX 0.0/0.0Mbps

2.3.35. Info Panel

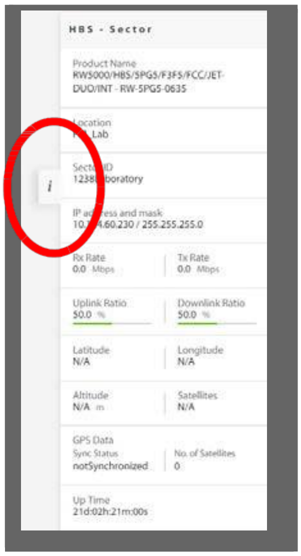
The info panel on the right pane of the user interface gives a brief overview of the sector, showing the following:

- HBS product name
- Location, Sector ID
- The present Rx and Tx Rates
- The present Uplink and Downlink ratios
- The HBS’s latitude, longitude, altitude (as per configuration) and if any satellites have been detected
- GPS data, including sync status and number of GPS satellites discovered

Scroll down, and you can see basic information about the link, which is displayed separately for each Carrier:

- Channel
- Channel Bandwidth
- Operational frequency
- Tx Power
- Service Type being used in the sector (CIR, BE, or mixed)
- CIR Resources being used, if any
- The HBS’s up time since last reset

To minimize the Right Pane, click on the minimize symbol:



HBS - Sector

Product Name
RW5000/HBS/5PG5/F3F5/FCC/JET-DUO/INT - RW-5PG5-0635

Location
[illegible] Lab

Secto[illegible]ID
1238[illegible]boratory

IP ad[illegible]ess and mask
10.[illegible]4.60.230 / 255.255.255.0

Rx Rate
0.0 Mbps

Tx Rate
0.0 Mbps

Uplink Ratio
50.0 %

Downlink Ratio
50.0 %

Latitude
N/A

Longitude
N/A

Altitude
N/A m

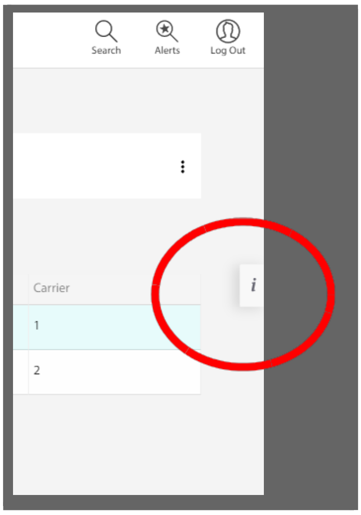
Satellites
N/A

GPS Data
Sync Status
notSynchronized

No. of Satellites
0

Up Time
21d:02h:21m:00s

- To restore the Right Pane, click on the minimize symbol again:



2.4. First-Time Use

When working with a RADWIN 5000 base station for the first time, carry out these tasks:

Update Connection Parameters - change the IP address of the RADWIN 5000 base station, and any other connection parameters in accordance with your radio plan.

Select operating band and activate the Base Station - this must be done for each carrier.

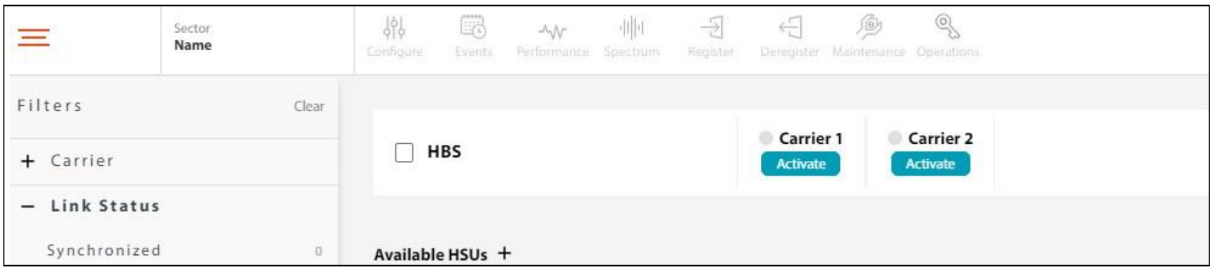
Register Subscriber Units - this must be done for each subscriber unit in each carrier.

Update Subscriber Unit Connection Parameters - change the IP address of each subscriber unit, and any other connection parameters in accordance with your radio plan.

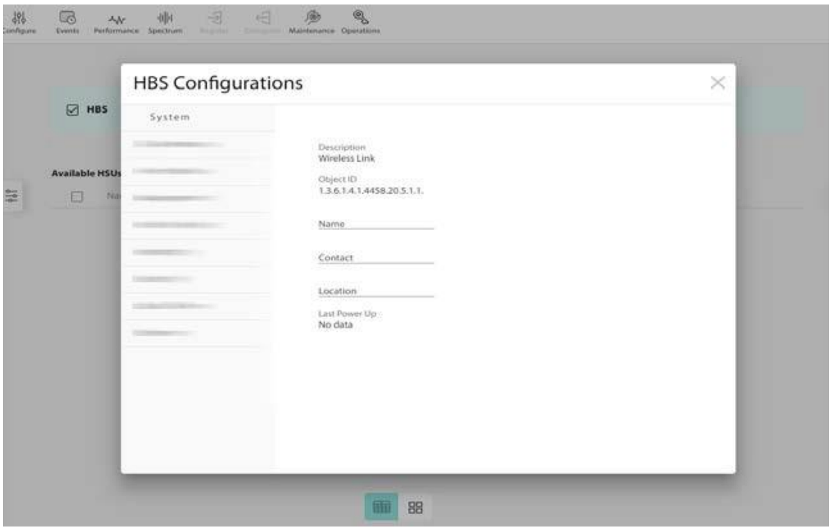
2.4.1. Update Connection Parameters

When first logging on to a new base station, we recommend that you change its IP address in accordance with your radio plan.

1. Connect the radio to the network and voltage via its PoE port[1].
2. Enter its IP address in a web browser (default value: 10.0.0.120).
3. Enter username **admin** and password **netwireless**.
4. Select the base station unit by placing a checkmark next to it, then click on **Configure.**



The **Configuration -> System** window will open.



Description
Wireless Link

Object ID
1.3.6.1.4.1.4458.20.5.1.1.

Name

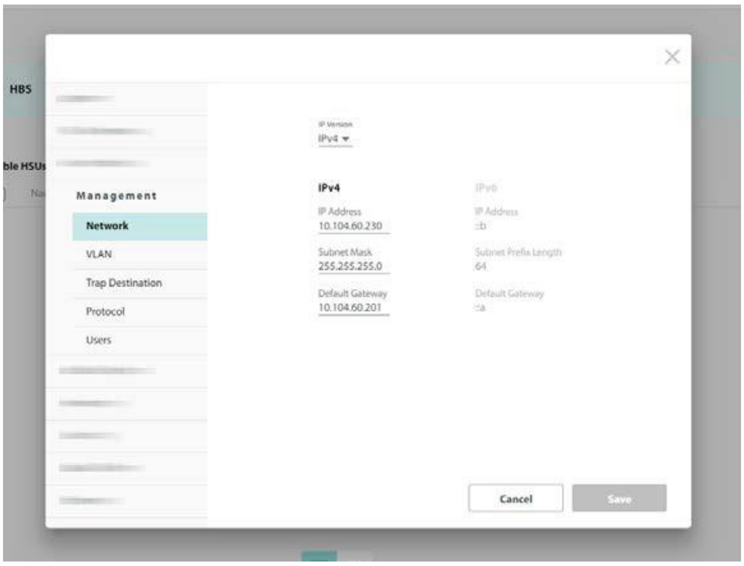
Contact

Location

Last Power Up
No data

Select **Management -> Network**:

[1] *Although you can use the SFP port for the network connection, you still need to connect power to the PoE port.*



IP Version: IPv4

IPv4

IP Address: 10.104.60.230

Subnet Mask: 255.255.255.0

Default Gateway: 10.104.60.201

IPv6

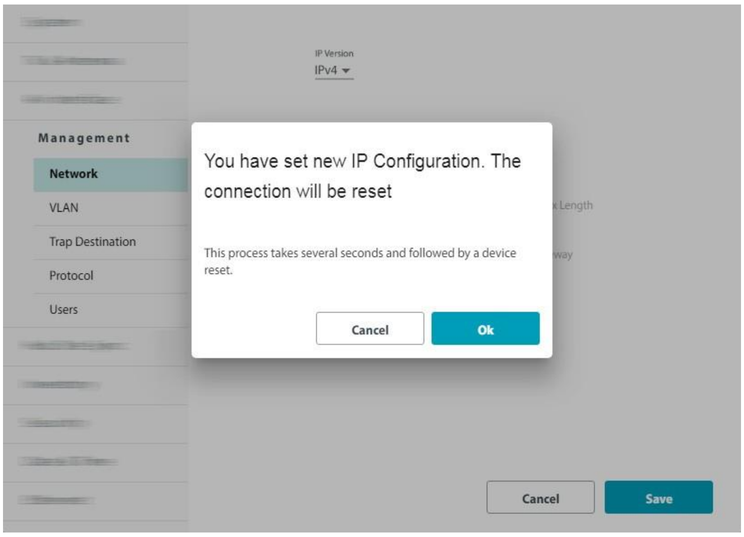
IP Address: ::b

Subnet Prefix Length: 64

Default Gateway: ::a

Enter the new IP address, Subnet Mask and Default Gateway in accordance with your radio plan, then click **Save**.

You will be warned that the device (HBS) will be reset. If all the values are correct, click **OK**.



IP Version: IPv4

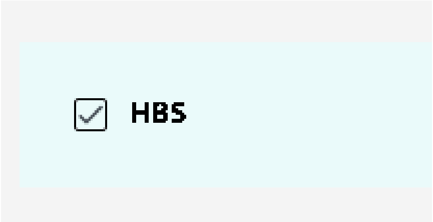
You have set new IP Configuration. The connection will be reset

This process takes several seconds and followed by a device reset.

Once the HBS is reset, log in again using the new IP address.

2.4.2. Select band and activate the carrier

1. In a web browser, enter the IP address of the HBS radio that is to be activated.
2. From the login page, enter username **admin** and password **netwireless**.
3. Select the HBS placing a checkmark next to its name:

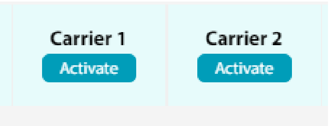


If your product has two carriers, you must activate the each carrier separately.

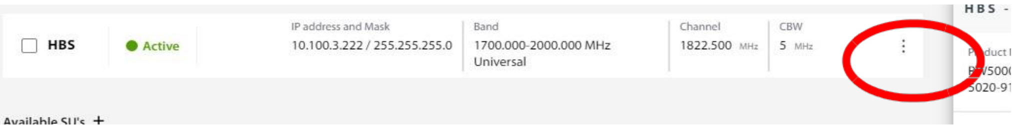
Note

For world-wide single PN products (Jet Air, Jet Air DUO), the country and channel must be configured before carrier activation is available. The text “**Band selection required**” will be displayed under the carrier light. Please see Change country and band for world-wide products for further information.

4. For the first carrier, click **Activate** under **Carrier 1** or **Carrier 2** (whichever you want to use).



- For a single-carrier product, click the far-right three-button icon:



IP address and Mask: 10.100.3.222 / 255.255.255.0

Band: 1700.000-2000.000 MHz Universal

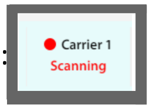
Channel: 1822.500 MHz

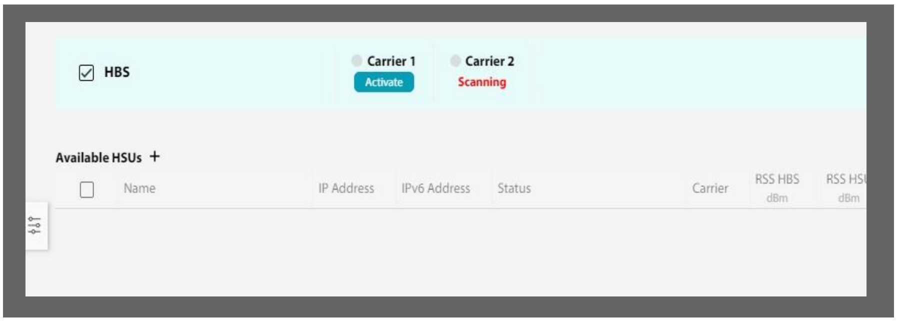
CBW: 5 MHz

5. Enter the Sector ID, Sector Name, and Location.

6. Once you are sure the values are correct, click **Activate**.

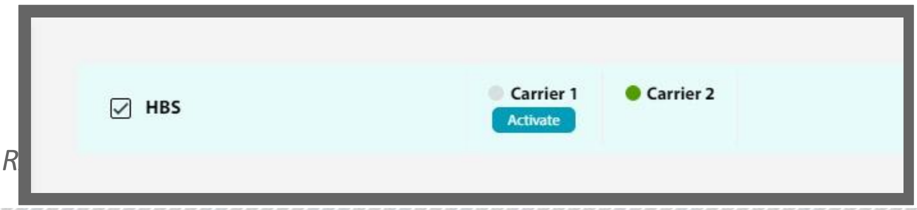
7. A “scanning” graphic will appear for a few moments:



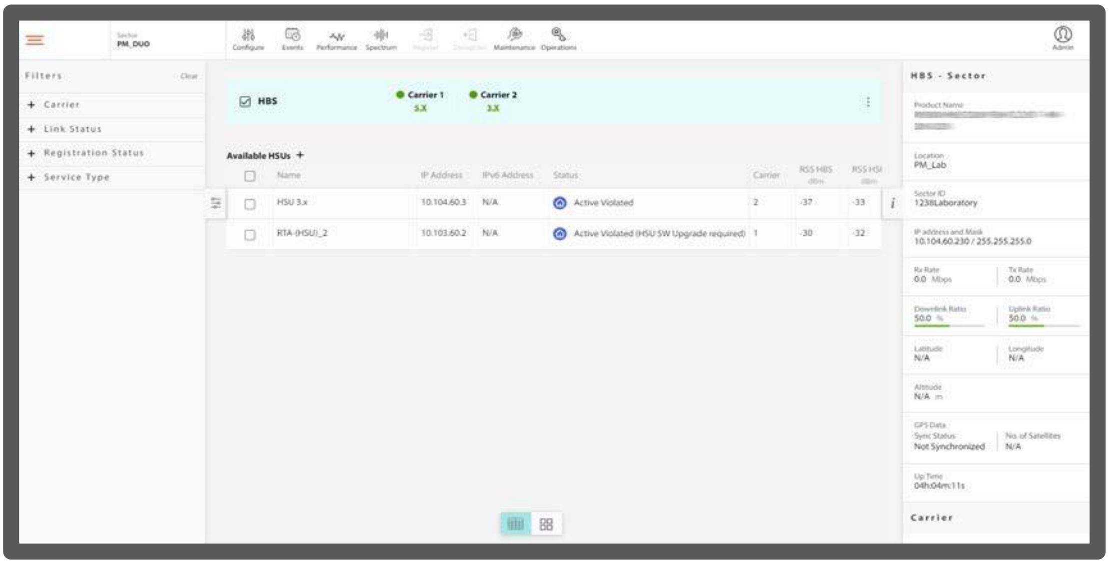


□	Name	IP Address	IPv6 Address	Status	Carrier	RSS HBS dBm	RSS HSU dBm

Then the carrier you are working with will be shown with a green bullet next to it, indicating that the carrier is Active. If your product has only one carrier, only that carrier will appear.



8. After you have repeated the above for the other carrier, the window will show that carrier as being active.



☑ HBS ● Carrier 1 5.X ● Carrier 2 3.X

Available HSUs +

□	Name	IP Address	IPv6 Address	Status	Carrier	RSS HBS dBm	RSS HSU dBm
□	HSU 3.x	10.104.60.3	N/A	Active Violated	2	-37	-33
□	RTA-(HSU)_2	10.103.60.2	N/A	Active Violated (HSU SW Upgrade required)	1	-30	-32

HBS - Sector

Product Name
[redacted]

Location
PM_Lab

Sector ID
1238Laboratory

IP address and Mask
10.104.60.230 / 255.255.255.0

Rx Rate 0.0 Mbps | Tx Rate 0.0 Mbps

Downlink Ratio 50.0 % | Uplink Ratio 50.0 %

Latitude N/A | Longitude N/A

Altitude
N/A m

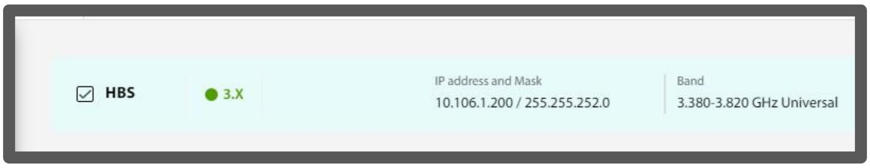
GPS Data
Sync Status Not Synchronized | No. of Satellites N/A

Up Time
04h:04m:11s

Carrier

Note that parameters that are common to both carriers will not appear when you run the activation wizard for the other carrier.

For single-carrier products, the band designation in green will appear:



☑ HBS ● 3.X

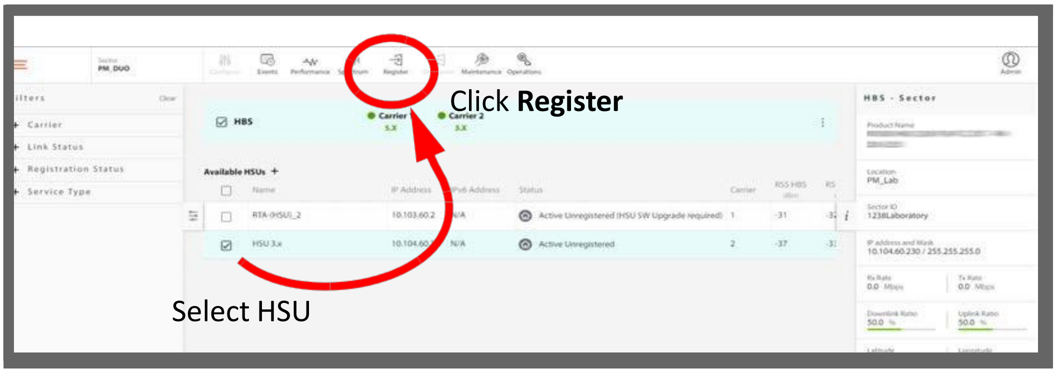
IP address and Mask
10.106.1.200 / 255.255.252.0

Band
3.380-3.820 GHz Universal

9. Carrier frequencies will be shown as Active, and any SUs that the HBS was able to contact are shown as well. However, for a first-time use, those SUs will be shown as un-registered. To work with them, you must register each one.

2.4.3. Register Subscriber Units

1. Select the SU you want to register by placing a checkmark next to it.



Click **Register**

☑ HBS ● Carrier 1 5.X ● Carrier 2 3.X

Available HSUs +

□	Name	IP Address	IPv6 Address	Status	Carrier	RSS HBS dBm	RS
□	RTA-(HSU)_2	10.103.60.2	N/A	Active Unregistered (HSU SW Upgrade required)	1	-31	-32
☑	HSU 3.x	10.104.60.3	N/A	Active Unregistered	2	-37	-31

Select HSU

HBS - Sector

Product Name
[redacted]

Location
PM_Lab

Sector ID
1238Laboratory

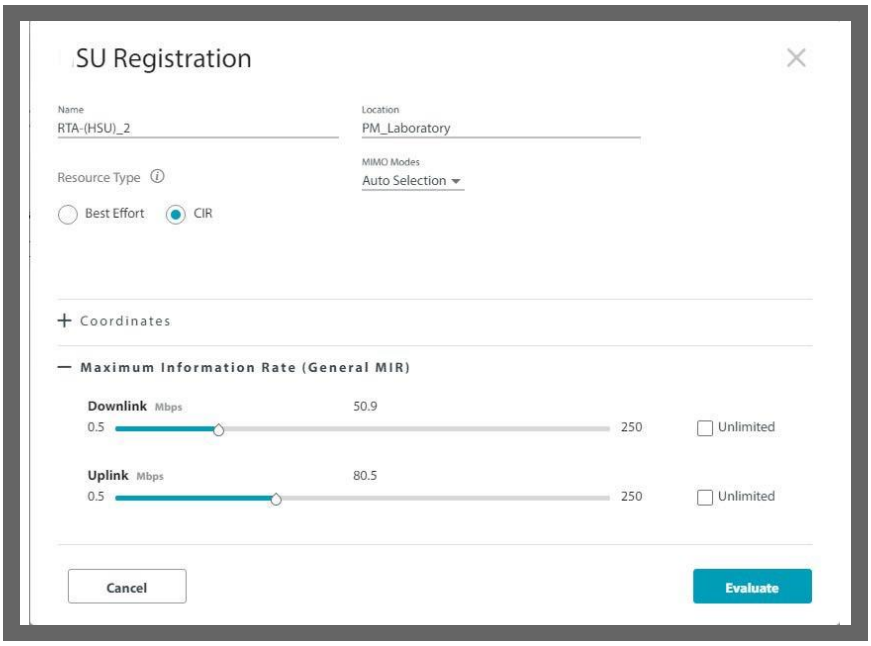
IP address and Mask
10.104.60.230 / 255.255.255.0

Rx Rate 0.0 Mbps | Tx Rate 0.0 Mbps

Downlink Ratio 50.0 % | Uplink Ratio 50.0 %

Latitude | Longitude

2. Click **Register**. You will see a window similar to the following:



SU Registration

Name: RTA-(HSU)_2

Location: PM_Laboratory

Resource Type: ○ Best Effort ● CIR

MIMO Modes: Auto Selection

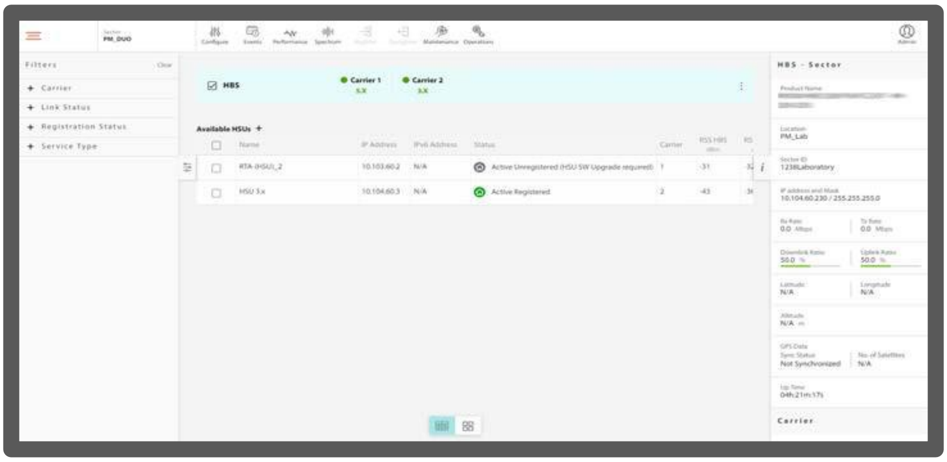
+ Coordinates

— Maximum Information Rate (General MIR)

Downlink Mbps: 50.9 (0.5 – 250) □ Unlimited

Uplink Mbps: 80.5 (0.5 – 250) □ Unlimited

3. You may edit or add the site’s Name, Location, and Coordinates.
4. Select the Resource Type for the SU. This can be CIR (Committed Information Rate), or BE (Best Effort):
    - BE grants the SU resources as they become available in the sector.
    - CIR grants the SU with a certain guaranteed percentage of resources. You set this percentage in the General MIR window.
5. Check a MIMO Mode for this SU:
    - Spatial Multiplexing (default) splits the data into two streams on transmission and recombines it on reception, providing maximum throughput.
    - Diversity transmits the same data from both antennas and checks for correctness on reception. This mode helps to ensure more reliable data transmission in a noisy environment, although throughput will be lower.
    - Auto Selection instructs the system to choose whichever mode is most efficient.
6. Optionally, you can choose the **Maximum Information Rate**. Use the sliders to set the maximum throughput rate you want for the specific SU in each direction: down link and up link. You can choose a value or click the Unlimited checkbox.
    - *If you chose the BE resource type in Step 4. above, continue to Step 7.*
    - *If you chose the CIR resource type in Step 4. above, continue to Step 8.*
7. If you chose the BE resource type in Step 4. above, click the Register button. In a few moments, the SU will be registered.



Sector PM_DUO

Filters Clear

- Carrier
- Link Status
- Registration Status
- Service Type

☑ HBS ● Carrier 1 5.X ● Carrier 2 5.X

Available HSUs +

□	Name	IP Address	IPv6 Address	Status	Carrier	RSS HBS dBm
□	RTA-(HSU)_2	10.103.60.2	N/A	Active Unregistered (HSU SW Upgrade required)	1	-31
□	HSU 5.x	10.104.60.3	N/A	Active Registered	2	-43

HBS - Sector

Product Name: [redacted]

Location: PM_Lab

Sector ID: 1238Laboratory

IP address and Mask: 10.104.60.230 / 255.255.255.0

Rx Rate: 0.0 Mbps | Tx Rate: 0.0 Mbps

Downlink Ratio: 50.0 % | Uplink Ratio: 50.0 %

Latitude: N/A | Longitude: N/A

Altitude: N/A m

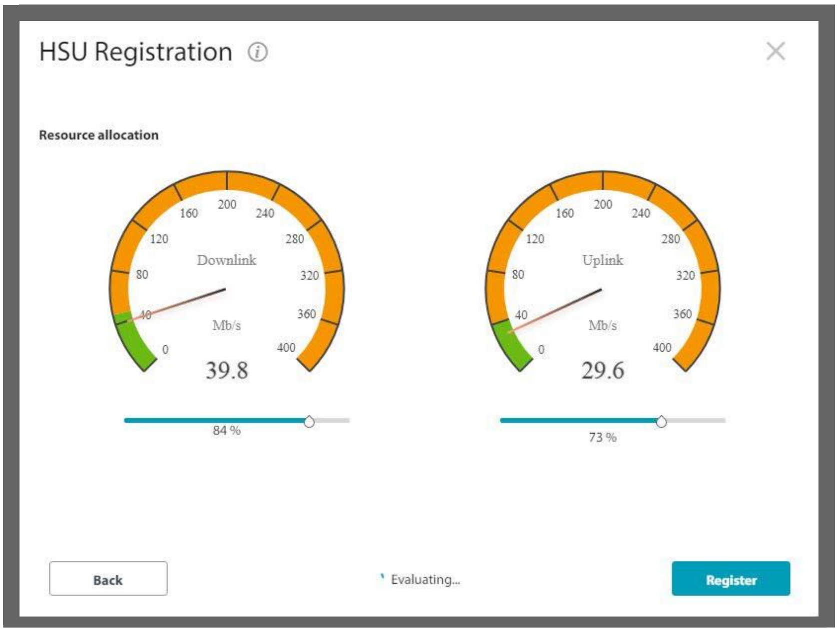
GPS Data: Sync Status: Not Synchronized | No. of Satellites: N/A

Up Time: 04h:21m:17s

Carrier

8. If you chose the CIR resource type above, choose the resource allocation (**General MIR**). Use the sliders to choose the percentage of resources to be allocated to the SU. This is the percentage of available resources in the sector. Obviously, you must make sure that the resource percentages of all the SUs in the sector do not add up to more than 100%. Once you have set the values, click **Evaluate.**

Evaluation dials will appear.



HSU Registration

Resource allocation

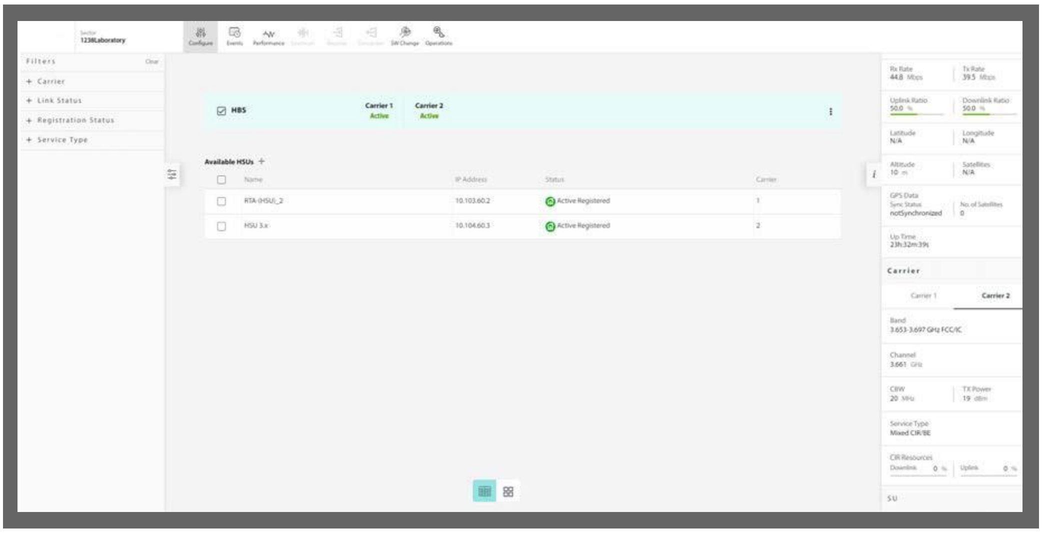
Downlink 39.8 Mb/s — 84 %

Uplink 29.6 Mb/s — 73 %

Evaluating...

9. When a stable value is reached, the **Register** button will become enabled.

10.Click **Register**.



☑ HBS — Carrier 1: Active — Carrier 2: Active

Available HSUs +

□	Name	IP Address	Status	Carrier
□	RTA-(HSU)_2	10.103.60.2	Active Registered	1
□	HSU 3.x	10.104.60.3	Active Registered	2

Rx Rate: 44.8 Mbps
Tx Rate: 39.5 Mbps
Uplink Ratio: 50.0 %
Downlink Ratio: 50.0 %
Latitude: N/A
Longitude: N/A
Altitude: 10 m
Satellites: N/A
GPS Data
Sync Status: notSynchronized
No. of Satellites: 0
Up Time: 23h:32m:39s

Carrier

Carrier 1 | Carrier 2

Band: 3.653-3.697 GHz FCC/IC
Channel: 3.661 GHz
CBW: 20 MHz
TX Power: 19 dBm
Service Type: Mixed CIR/BE
CIR Resources: Downlink 0 % | Uplink 0 %

SU

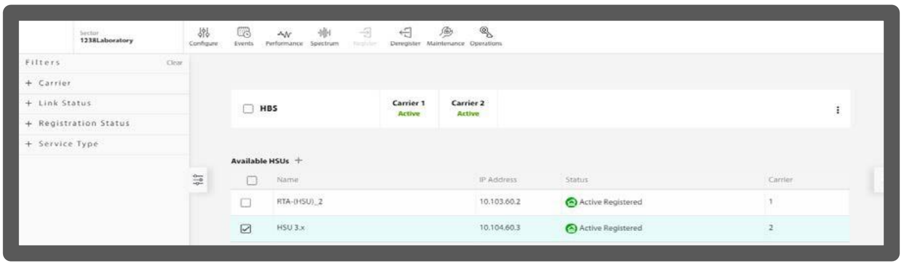
Caution

When working with the JET-DUO 5 GHz, since the carriers have the same Sector ID, the SU can sync to either Carrier 1 or Carrier 2. If the SU syncs to one carrier, and you wish it to sync to the other carrier, select "Suspend" for this unit, and select the time that this SU will be in suspend mode. The SU will lose synchronization from the carrier and will start scanning for other HBSs. Repeat this until the SU syncs to the correct carrier.

2.4.4. Update Subscriber Unit Connection Parameters

When first logging on to a new subscriber unit, you should change its IP address in accordance with your radio plan.

Select the subscriber unit by placing a checkmark next to it, then click on **Configure [Configure].**

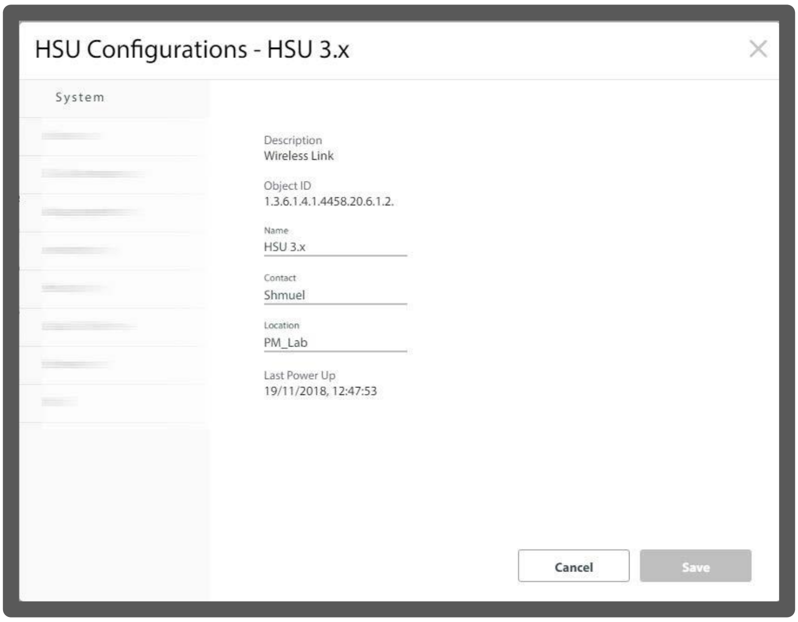


□ HBS — Carrier 1: Active — Carrier 2: Active

Available HSUs +

□	Name	IP Address	Status	Carrier
□	RTA-(HSU)_2	10.103.60.2	Active Registered	1
☑	HSU 3.x	10.104.60.3	Active Registered	2

The **Configuration -> System** window will appear.



HSU Configurations - HSU 3.x

Description
Wireless Link

Object ID
1.3.6.1.4.1.4458.20.6.1.2.

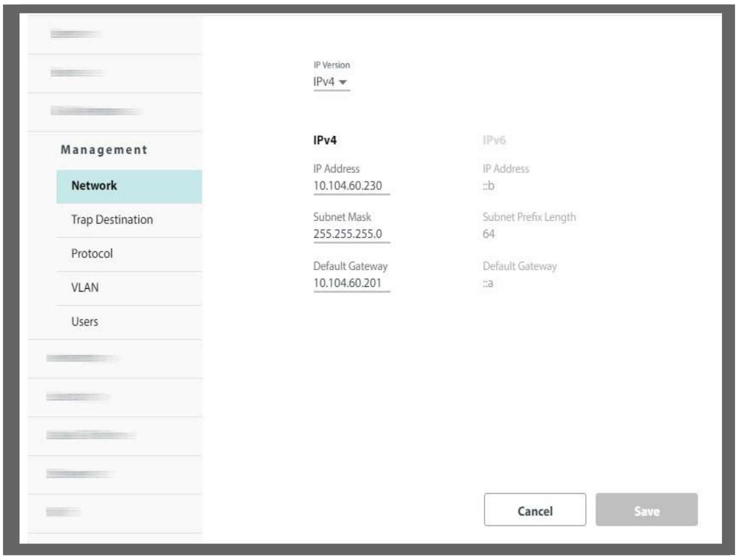
Name
HSU 3.x

Contact
Shmuel

Location
PM_Lab

Last Power Up
19/11/2018, 12:47:53

Select **Management -> Network**



IP Version
IPv4

IPv4

IP Address
10.104.60.230

Subnet Mask
255.255.255.0

Default Gateway
10.104.60.201

IPv6

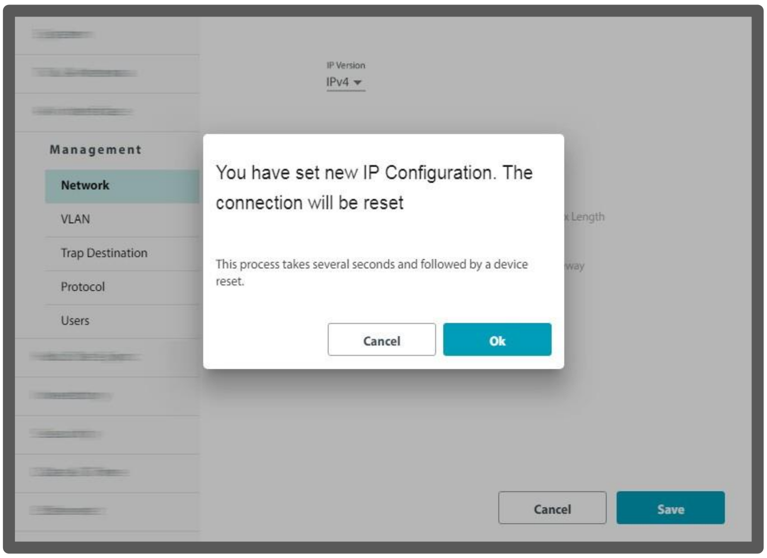
IP Address
::b

Subnet Prefix Length
64

Default Gateway
::a

Enter the new IP address, Subnet Mask, and Default Gateway in accordance with your radio plan, then click **Save**.

You will be warned that the unit will be reset. If all the values are correct, click **OK**.



You have set new IP Configuration. The connection will be reset

This process takes several seconds and followed by a device reset.

Once the unit is reset, the base station should synchronize with it shortly.

Chapter 3: Managing SU *PRO/ AIR* Units Directly

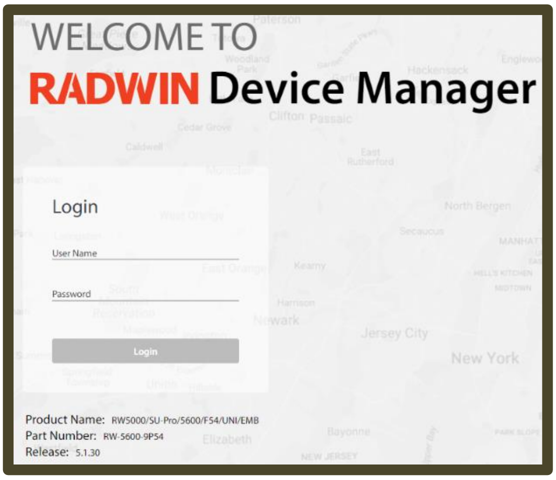
3.1. Scope of this Chapter

This chapter describes how to configure SU ***PRO/AIR*** units via its web interface.

3.2. Login

Access the web interface by connecting to the unit, either directly via RJ45 cable, or via the internet. We recommend using a PC or laptop. Enter the unit’s IP address in a web browser (default value: 10.0.0.120). A welcome message will appear.

Note - SU-Air/Pro products have a built-in WiFi AP for management only. For configuration and monitoring, you can connect to the radio via its WiFi AP. The ESSID of the radio is R [serial number of the unit] and the default password is wireless. Upon successful authentication, your WiFi client will get a DHCP IP address.
To login to the radio, enter the IP address of the WiFi AP in a web browser (default value: 192.168.1.1).


WELCOME TO

RADWIN Device Manager

Login

User Name

Password

Login

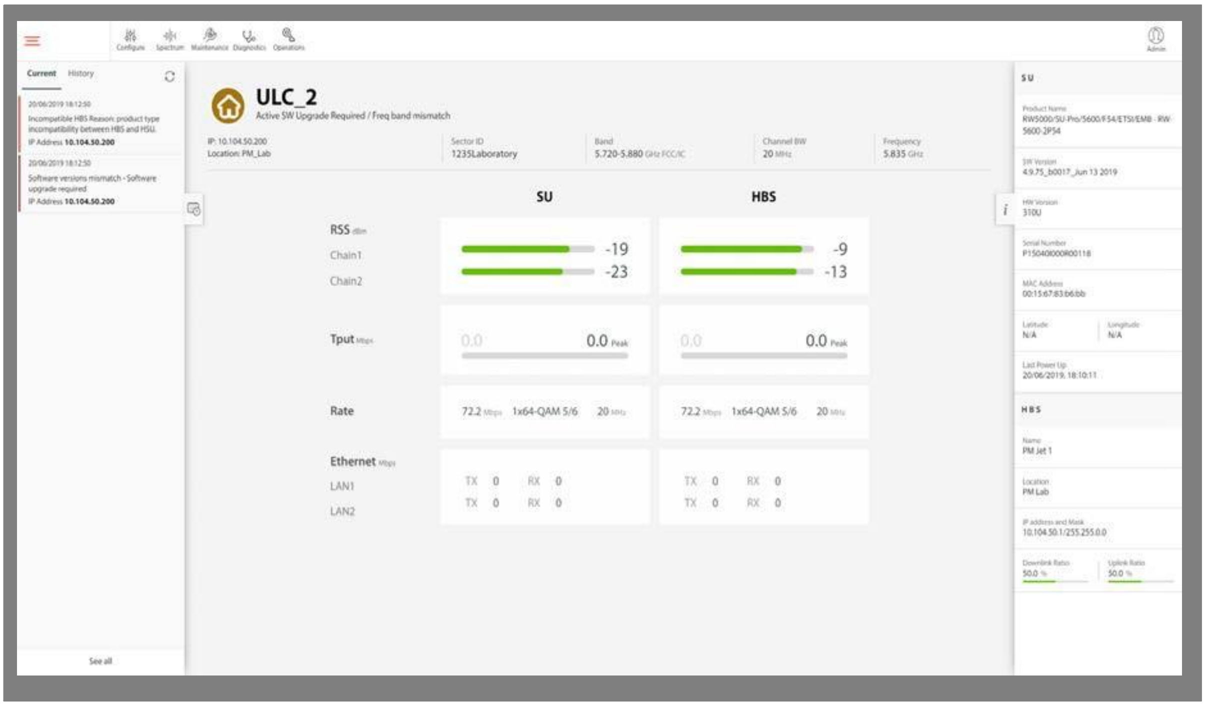
Product Name: RW5000/SU-Pro/5600/F54/UNI/EMB
Part Number: RW-5600-9P54
Release: 5.1.30

Enter the username and password then click **Login.**

Username: **admin**

Password: **netwireless**

The main window will appear.



Current History

20/06/2019 18:12:50
Incompatible HBS Reason: product type incompatibility between HBS and HSU.
IP Address **10.104.50.200**

20/06/2019 18:12:50
Software versions mismatch - Software upgrade required
IP Address **10.104.50.200**

See all

ULC_2
Active SW Upgrade Required / Freq band mismatch

IP: 10.104.50.200
Location: PM_Lab

Sector ID: 1235Laboratory
Band: 5.720-5.880 GHz FCC/IC
Channel BW: 20 MHz
Frequency: 5.835 GHz

	SU	HBS
RSS dBm		
Chain1	-19	-9
Chain2	-23	-13
Tput Mbps	0.0 0.0 Peak	0.0 0.0 Peak
Rate	72.2 Mbps 1x64-QAM 5/6 20 MHz	72.2 Mbps 1x64-QAM 5/6 20 MHz
Ethernet Mbps		
LAN1	TX 0 RX 0	TX 0 RX 0
LAN2	TX 0 RX 0	TX 0 RX 0

SU
Product Name: RW5000/SU-Pro/5600/F54/ETSI/EMB - RW-5600-2P54
SW Version: 4.9.75_b0017_Jun 13 2019
HW Version: 310U
Serial Number: P150400000R00118
MAC Address: 00:15:67:83:b6:bb
Latitude: N/A
Longitude: N/A
Last Power Up: 20/06/2019, 18:10:11

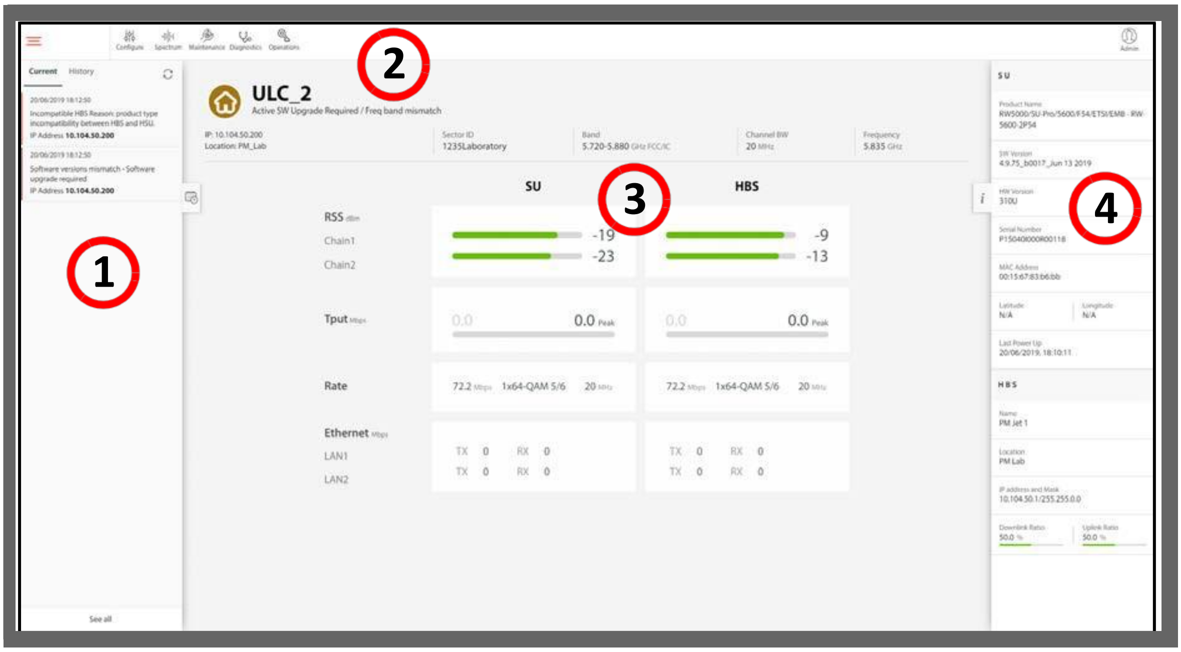
HBS
Name: PM Jet 1
Location: PM Lab
IP address and Mask: 10.104.50.1/255.255.0.0
Downlink Ratio: 50.0 %
Uplink Ratio: 50.0 %

Figure 3-1: SU ***PRO/AIR*** *Main/Overview Window*

Note – In SU-Pro, PtP or PtMP mode appears under the "Location" parameter. SU-Pro automatically changes the mode according to the type of base station (PtP or PtMP) it is synchronized with.

3.3. WebUI Overview

The WebUI shows the SU ***PRO/AIR*** unit and the base station to which it belongs.



Click on the section of the WebUI for which you want more information:

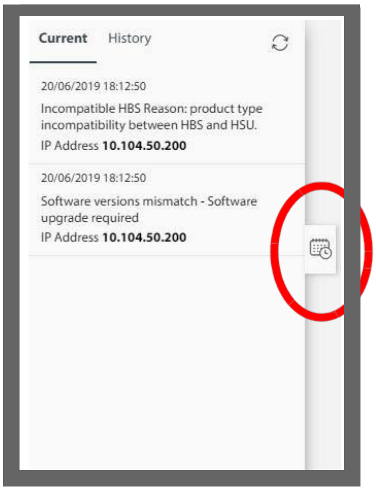
1	*History*	2	*Main icons*
3	*Radio List*	4	*Info Panel*

3.3.1. History

Here you can see the history of events.

Click on the **Current** tab to limit the list to recent events (from the last several hours), or on the **History** tab to see a comprehensive list of events.

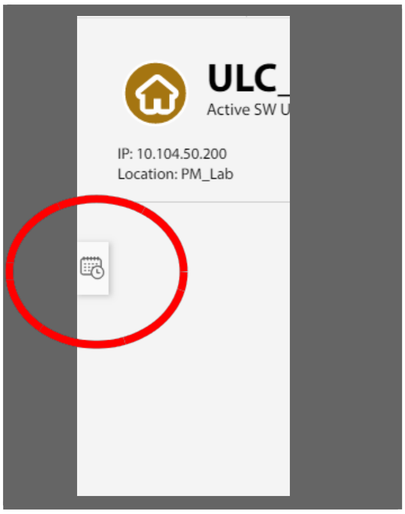
- To minimize the History list, click on the minimize symbol:



20/06/2019 18:12:50
Incompatible HBS Reason: product type incompatibility between HBS and HSU.
IP Address **10.104.50.200**

20/06/2019 18:12:50
Software versions mismatch - Software upgrade required
IP Address **10.104.50.200**

- To restore the History list, click on the minimize symbol again:

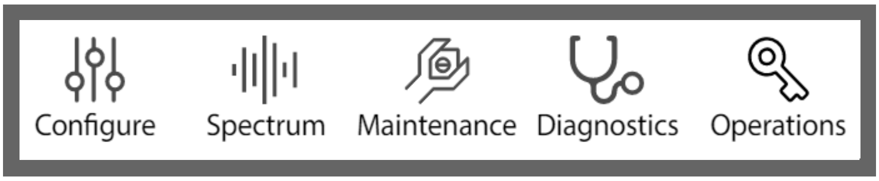


IP: 10.104.50.200
Location: PM_Lab

3.3.2. Main icons

Along the top edge of the WebUI, there are icons that allow you to carry out certain tasks for the radio units.

The applicable icons become enabled when you select the radio unit relevant for the task.



Configure	***Configure***	Set various parameters for the selected unit, including, but not limited to: • IP address, • frequency and bandwidth, • transmission power, • passwords, • NTP settings, and more
Spectrum	***Spectrum***	The Spectrum view utility provides spectral measurements, and is useful in assisting with diagnosing interference related problems prior to a full sector activation. It is operated per carrier.
Maintenance	***Maintenance***	Back up, upgrade or restore the software in the selected unit or units.
Diagnostics	***Diagnostics***	Shows radio signal strength (refer to this when carrying out antenna alignment) and allows a ping and trace, a speed test, creates diagnostics files, and enables sniffing of TCP/IP packets.
Operations	***Operations***	Resets, restores to factory default configuration, allows license-dependent upgrades and can activate the unit. SU-Pros that run release 5.1.10 and above support the option to change mode to PtP.
Admin	***User Profile Icon***	Click this icon to log out of the unit.

3.3.3. Configure

These are the configuration categories:

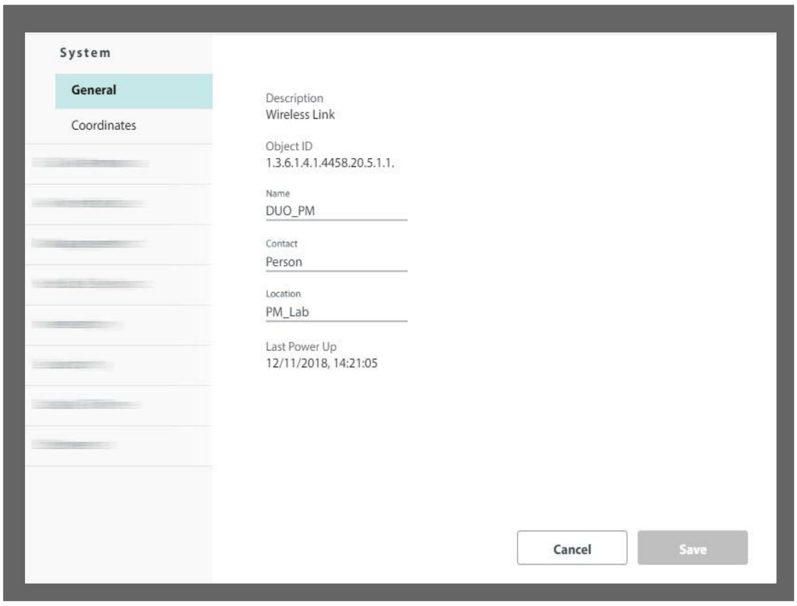
System	*Air Interface*	*Tx & Antenna*
Management	*Inventory*	*Security*
Date & Time	*Ethernet*	*WiFi*

Nomadic		

3.3.4. System

General

These items are convenience fields: **Description, Object ID, Name, Contact, Location,** and **Last Power Up**. Name and Location are typically entered during registration. If you make any changes, click **Save** to have them take effect.



Description
Wireless Link

Object ID
1.3.6.1.4.1.4458.20.5.1.1.

Name
DUO_PM

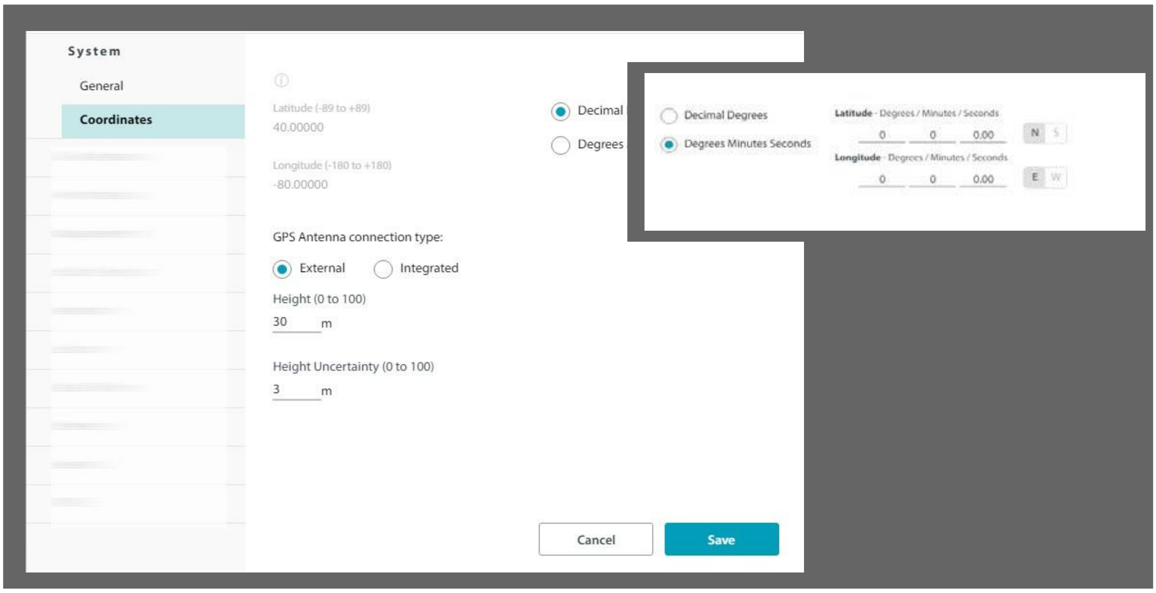
Contact
Person

Location
PM_Lab

Last Power Up
12/11/2018, 14:21:05

Coordinates

The coordinates (latitude and longitude) use either decimal degrees or degrees, minutes, and seconds. This is read-only.



Latitude (-89 to +89)
40.00000

Longitude (-180 to +180)
-80.00000

● Decimal
○ Degrees

○ Decimal Degrees
● Degrees Minutes Seconds

Latitude - Degrees / Minutes / Seconds
0 0 0.00 N S

Longitude - Degrees / Minutes / Seconds
0 0 0.00 E W

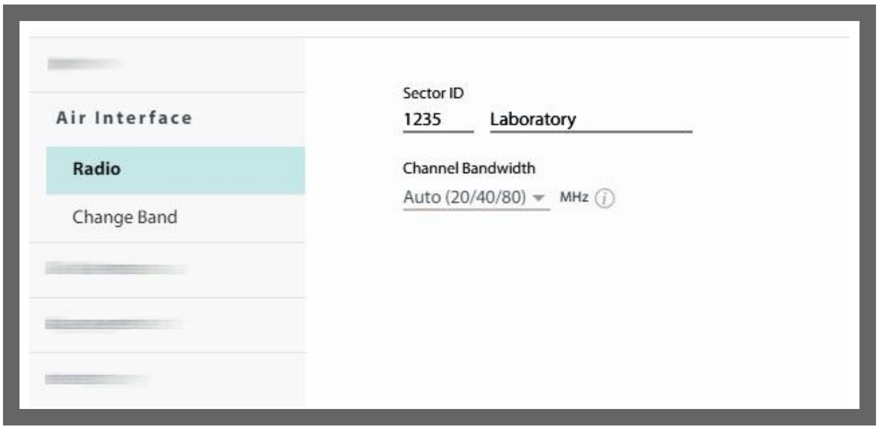
GPS Antenna connection type:
● External ○ Integrated

Height (0 to 100)
30 m

Height Uncertainty (0 to 100)
3 m

3.3.5. Air Interface

You can change the Sector ID, channel bandwidth, and frequency band. The Sector ID is important as it **must** be the same as that of the base station.

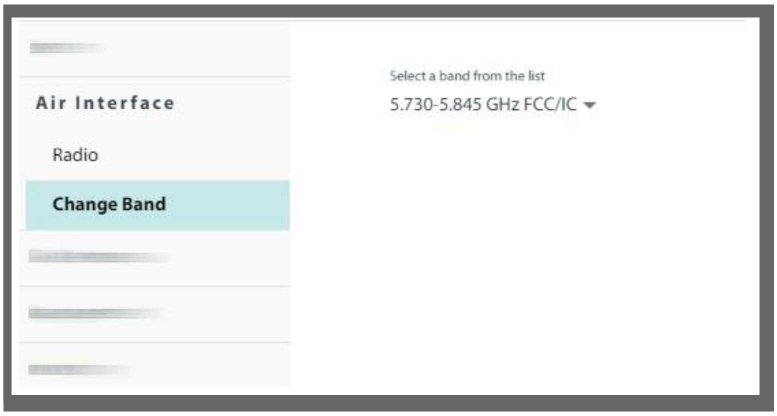


Sector ID: 1235 Laboratory

Channel Bandwidth: Auto (20/40/80) MHz

Radio

- Sector ID: Set the Sector ID here. This must be the same as the HBS to which the SU is to connect.
- Channel Bandwidth: Shows the channel bandwidth.



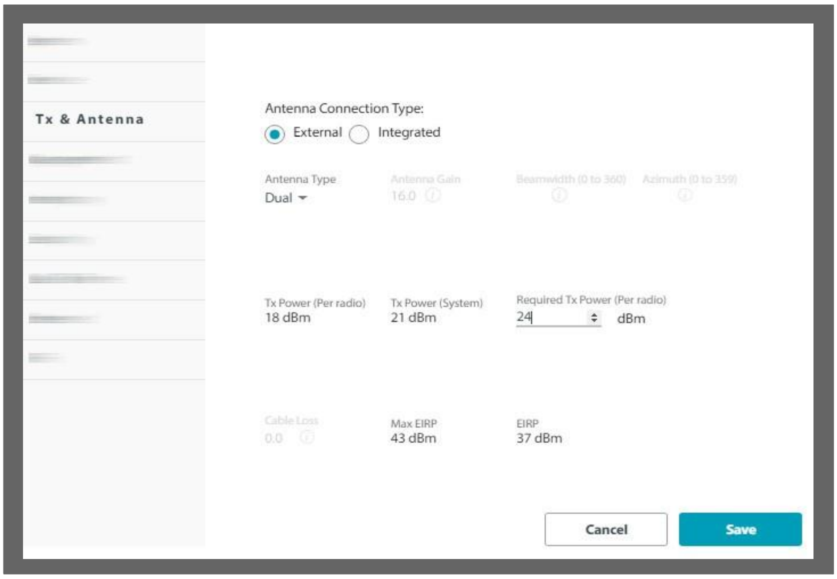
Select a band from the list: 5.730-5.845 GHz FCC/IC

Change Band

You can change the frequency band here. Only frequency bands allowed by your regulatory environment will appear.

3.3.6. Tx & Antenna

Changes made here may affect link quality. Antenna connection type is integrated.



Antenna Connection Type:
● External ○ Integrated

Antenna Type: Dual

Antenna Gain: 16.0

Beamwidth (0 to 360)

Azimuth (0 to 359)

Tx Power (Per radio): 18 dBm

Tx Power (System): 21 dBm

Required Tx Power (Per radio): 24 dBm

Cable Loss: 0.0

Max EIRP: 43 dBm

EIRP: 37 dBm

If you make any changes, click **Save** to have them take effect.

3.3.7. Management

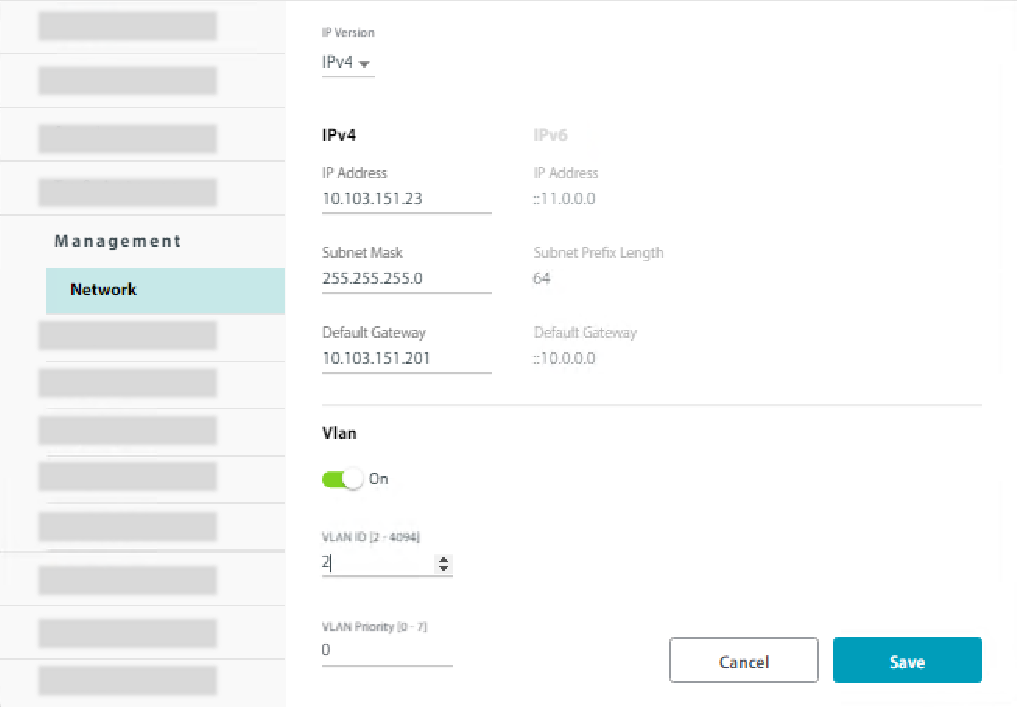
This category enables you to change the IP address, Subnet Mask, and Default Gateway of the selected device, configure the management VLAN, set trap destinations, change the management protocol and its authentication mode, set the IP address of a Syslog server, and add or remove user definitions.

Network

Configure management IP address

You may configure a link for IPv4, IPv6, or both. Using both IP versions is useful in conjunction with applications that do not fully support IPv6.

1. Choose what type of IP address to enter (IPv4, IPv6, or both).



IP Version
IPv4

IPv4

IP Address
10.103.151.23

Subnet Mask
255.255.255.0

Default Gateway
10.103.151.201

IPv6

IP Address
::11.0.0.0

Subnet Prefix Length
64

Default Gateway
::10.0.0.0

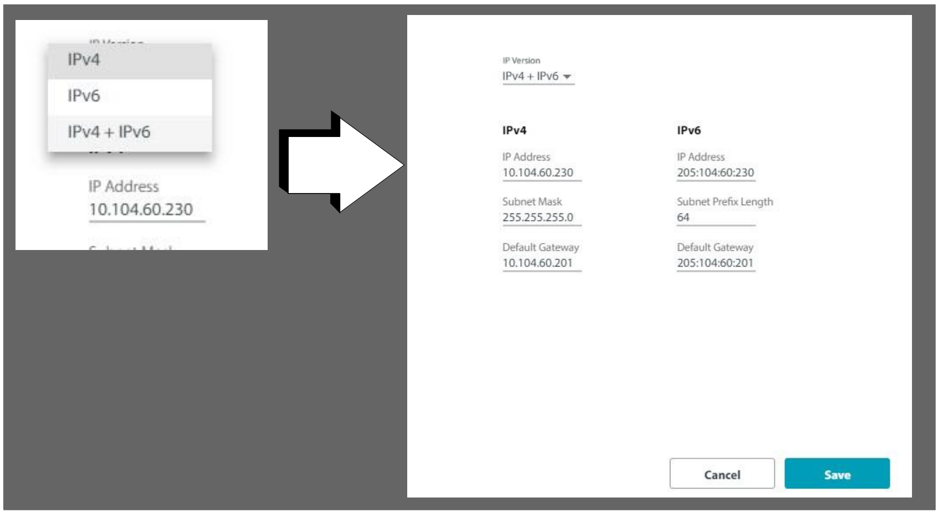
Vlan

On

VLAN ID [2 - 4094]
2

VLAN Priority [0 - 7]
0

Here, you can choose both, and enter the IPv6 addresses:



IP Address
10.104.60.230

IP Version
IPv4 + IPv6

IPv4

IP Address
10.104.60.230

Subnet Mask
255.255.255.0

Default Gateway
10.104.60.201

IPv6

IP Address
205:104:60:230

Subnet Prefix Length
64

Default Gateway
205:104:60:201

2. Enter the appropriate IP address or addresses, including the Subnet Mask and Default Gateway (for IPv4), and/or the Subnet Prefix Length and Default Gateway (for IPv6).
3. Click **Save**.
4. If you changed any value, you will see a warning message that a device reset will be done. To confirm, click **OK**.

Configure management VLAN

Configure the management VLAN here. To configure a VLAN for traffic, See VLAN.

The management VLAN enables the separation of user traffic from management traffic whenever such separation is required.

Caution

VLAN IDs are used by RADWIN products in three separate contexts:

Management VLAN, Traffic VLAN and HSSoE. It is recommended that you use different VLAN IDs for each context.

To enable VLAN for management:

1. Check ON in the VLAN checkbox.
2. Enter a VLAN ID. Its value should be between 2 and 4094.

   After entering the VLAN ID, only packets with the specified VLAN ID are processed for management purposes by the HBS/SU. This includes all the protocols supported by the radio (ICMP, SNMP, Telnet and NTP). Using VLAN for management traffic affects all types of management connections (local, network and over the air).
3. Enter a Priority number between 0 and 7.

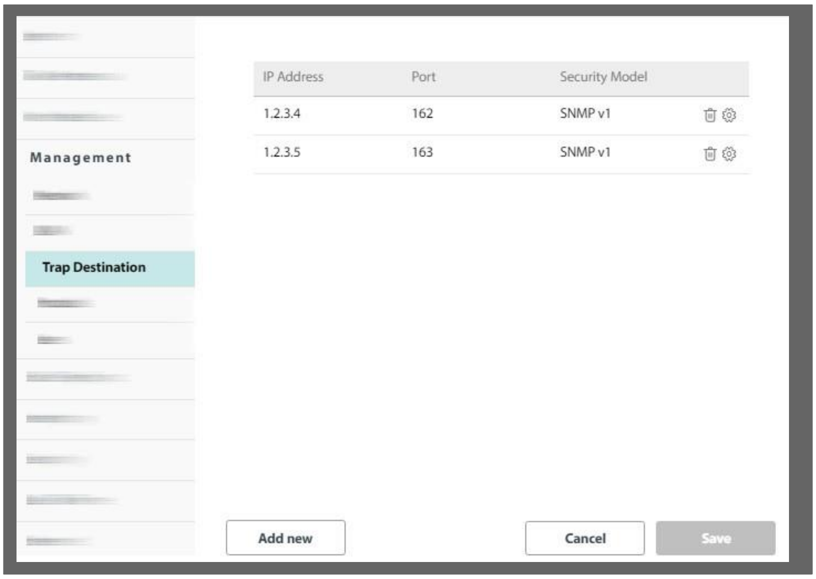
   The VLAN priority is used for the traffic sent from the radio to the managing computer.
4. Change the VLAN ID and Priority of the managing computer NIC to be the same as those of steps 2 and 3 respectively.
5. Click **Save**.

Lost or forgotten VLAN ID or IP Address (SU-Air/Pro)

If the VLAN ID or IP address of the SU unit is forgotten, you can reset the unit find the IP address using a sniffer (like Wireshark).
When the SU is reset, it sends a Gratuitous ARP packet toward the Ethernet interface which contains the management VLAN ID and IP address.
You can also reset the unit and locally access to it via the WiFi.

Trap Destinations

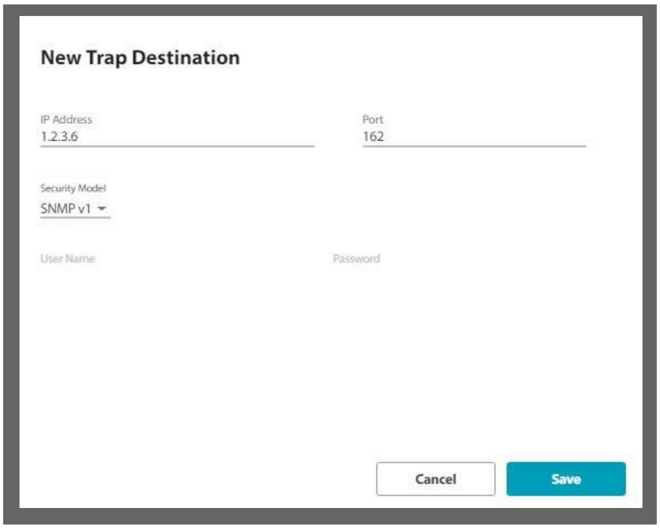
All traps are saved at each location you define.



IP Address	Port	Security Model
1.2.3.4	162	SNMP v1
1.2.3.5	163	SNMP v1

Ø **To set a new trap destination:**

1. Click **Add new.**
2. In the window that appears, enter the Trap Destination IP Address, Port, and Security Model (SNMP v1 or v3). If choosing SNMP v3, enter the username and password. The IP address can be the same as the managing computer. The events log will be stored at the address(es) chosen.



New Trap Destination

IP Address: 1.2.3.6

Port: 162

Security Model: SNMP v1

User Name

Password

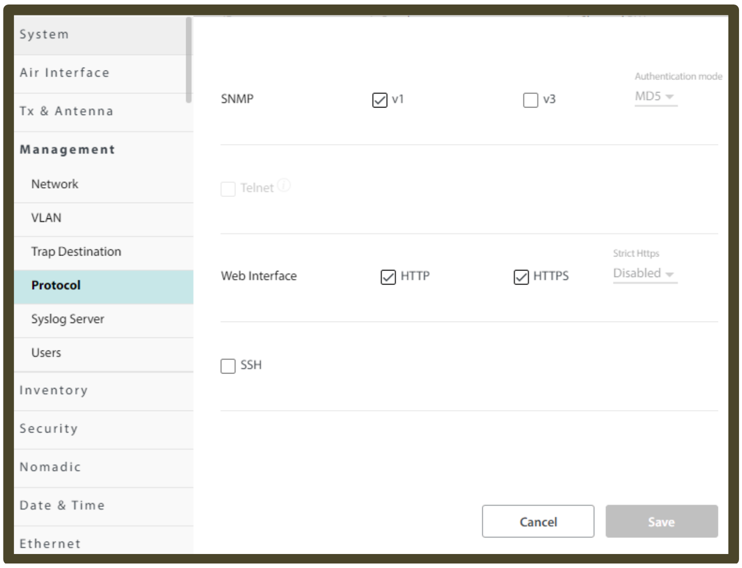
3. Once you are finished, click **Save** to have your changes take effect.

Ø **To change (edit or delete) a trap destination:**

1. To delete a trap destination, click the trash icon (🗑) on the same line as the IP address.
2. To edit a destination, click the configuration icon (⚙) on the same line as the IP address.
3. In the window that appears, change the parameters you wish to change (Trap Destination IP Address, Port, and/or Security Model). If choosing SNMP v3, enter the username and password. The IP address can be the same as the managing computer. The events log will be stored at the address(es) chosen.
4. Once you are finished, click **Save** to have your changes take effect.

Protocol

You can set the management protocol as well as the authentication mode.



SNMP ☑ v1 ☐ v3 Authentication mode MD5

☐ Telnet

Web Interface ☑ HTTP ☑ HTTPS Strict Https Disabled

☐ SSH

SNMP

SNMP support is permanently enabled. You may choose between SNMPv1, SNMPv3 or both.

You can leave the default authentication mode for SNMPv3 as MD5 (message digest algorithm), or change it to SHA1 (secure hash algorithm).

If you change these values here, you will be required to use them when you log in to the unit via the RADWIN Manager.

Web Interface

- The unit can be configured for HTTP, HTTPS, or both. To do this, place a checkmark in the box next to the protocol you want from the **Web Interface** line.
- The next time you log on to the unit's Web Interface, use the protocol you chose here.
- An admin user must be logged in with HTTPS to make changes in users.
- If you have selected HTTPS and log in with HTTP, then the unit will automatically use the secured model (HTTPS).
- If you choose Enabled under **Strict HTTPS**, then the next time you log in, you must do it via **https://IP Address**.

Once you are finished, click **Save** to have any changes take effect.

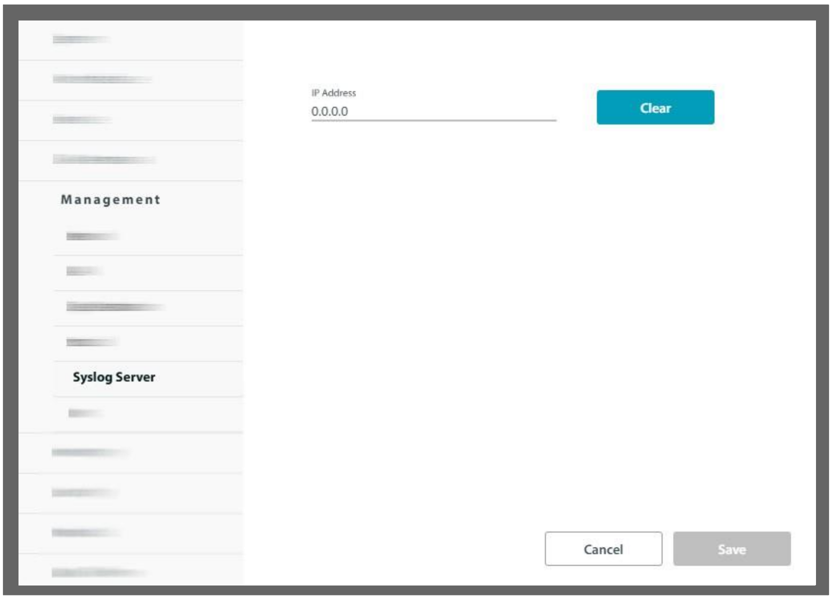
SSH

Turn SSH CLI on or off

For a list of supported CLI commands, See appendix

Syslog Server

This field shows the IP address of a Syslog server to which the specific radio unit sends Syslog messages. This is configured per individual unit.

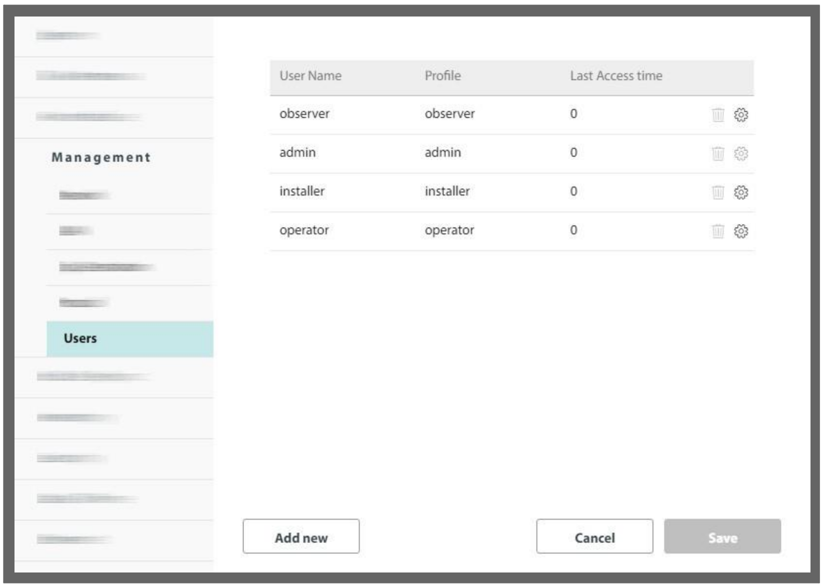


IP Address
0.0.0.0

- Enter the IP address of the Syslog server and click **Save**. It could be the IP address of the managing computer. The Syslog events will be stored at the address chosen.

Users

Here, an admin user can define users and assign them to a pre-defined category. The admin user must be logged in using HTTPS. Once you define a user, that person can use their username and password to log in.



User Name	Profile	Last Access time
observer	observer	0
admin	admin	0
installer	installer	0
operator	operator	0

Possible user profiles are as follows:

Profile	Default Password	Function
observer	netobserver	Read Only

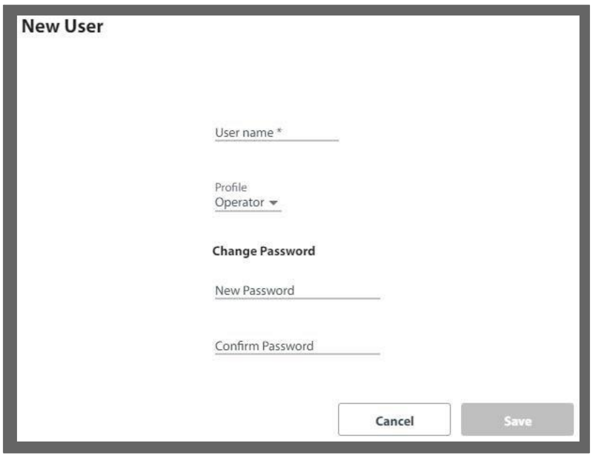
operator	netpublic	Can install and configure the sector, but cannot change the operating frequency or regulation.
installer	netinstaller	Functions as Operator, in addition to being able to change the operating frequency or regulation, antenna gain, and cable loss. Only an Installer can change the antenna gain and cable loss.
admin	netwireless	Functions as Operator, in addition to being able to change new users. Pre-defined users cannot be changed. Can change the operating frequency or regulation, and enhance the security mode.

Caution

To add or edit a user, you must be logged in via secure HTTP.
Do this by making sure that HTTPS is selected (from a selected unit, click the Configure icon, then from Management -> Protocol, select the HTTPS box). Then, log in using the same IP address as before, but add https:// before its address.

New user:

Click **Add new** and the New User window will open.



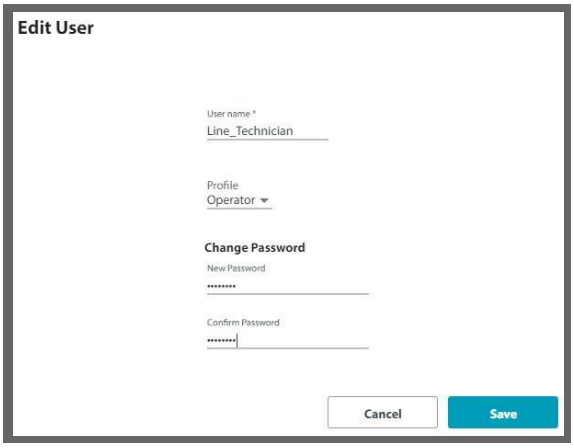
New User

Profile: Operator

1. Enter a convenient name for the new user.
2. Choose the profile for this user. The profile determines what the user can and cannot do.
3. Set the password for this user and confirm it.
4. Click **Save** to have your changes take effect.
5. You will see the new user in the Users list.

Edit user:

Click the configuration icon (⚙) and the Edit User window will open.


Edit User

User name *
Line_Technician

Profile
Operator ▾

Change Password

New Password
••••••••

Confirm Password
••••••••

1. Change the name, if needed.
2. Change the profile, if needed. This determines what the user can and cannot do.
3. Set the password for this user and confirm it. This must be done no matter what action you take here.
4. Click **Save** to have your changes take effect.
5. You will see the edited user in the Users list.

Remove user:

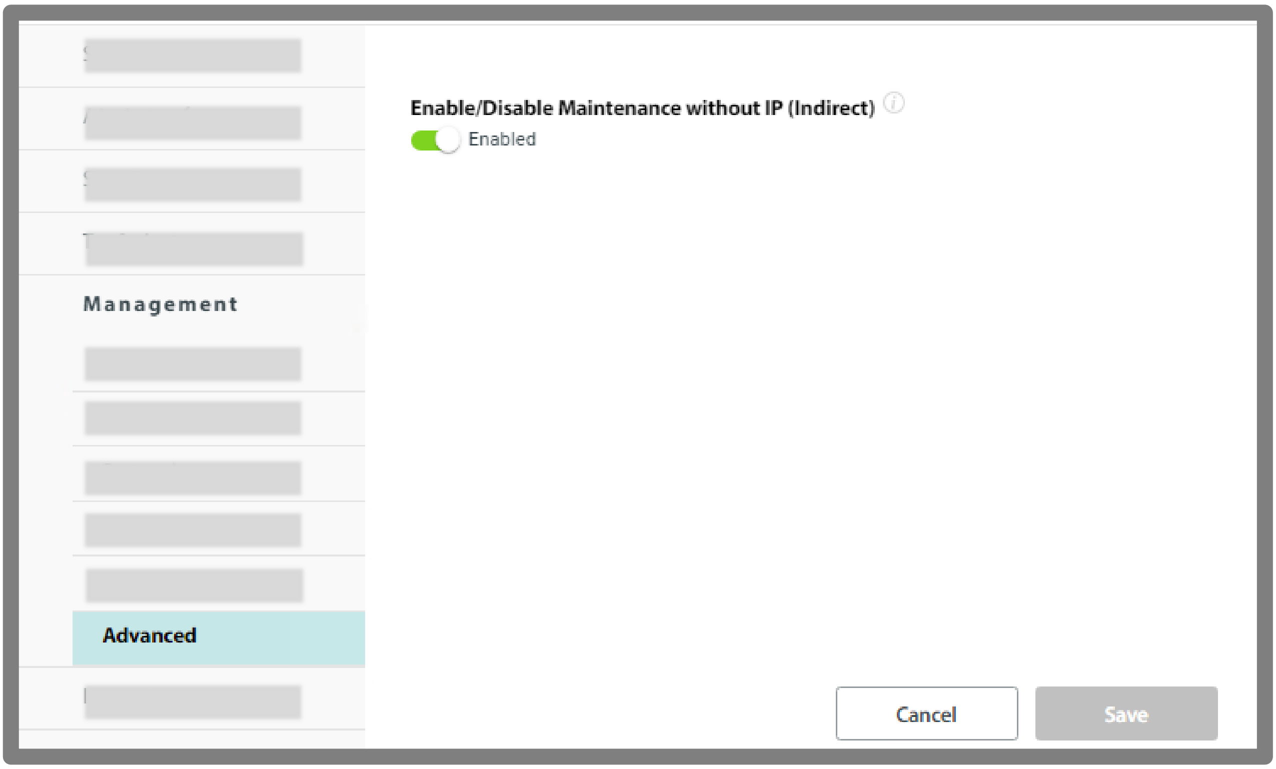
You cannot remove pre-defined users.

1. Click on the trash icon (🗑) to remove the user.
2. The user will be removed from the Users list.

Advanced

Enable / Disable maintenance without IP (indirect)

This option enables to perform SW upgrade or backup to SU devices via the BS without using the IP address of the SUs, meaning without having IP connection to the local IP address of the SU. If you don’t use SW upgrade or backup for SUs without having connection to their IPs, this option should be disable.

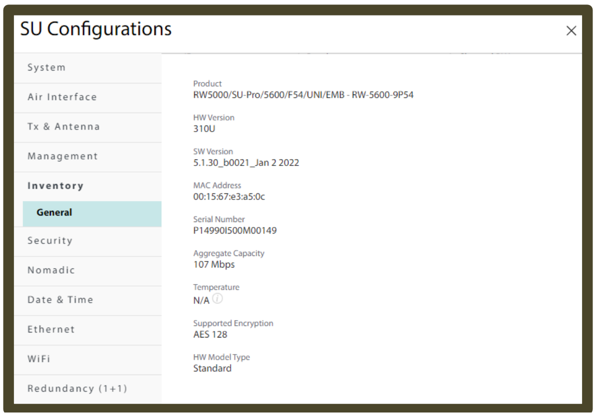


Enable/Disable Maintenance without IP (Indirect)
Enabled

3.3.8. Inventory

This shows the identification information for the selected unit: product version, hardware version and software version, mac address, serial number, aggregate capacity, the present temperature inside the unit, the unit's power consumption, supported encryption, and hardware mode type. Note that there is an indication of a special edition CBW for SUs with special hardware that don't support CBW of 10Mhz.

Note you cannot see the IP address here. Go to **Configure -> Management -> Network** to see the IP address of the selected unit.



Product
RW5000/SU-Pro/5600/F54/UNI/EMB - RW-5600-9P54

HW Version
310U

SW Version
5.1.30_b0021_Jan 2 2022

MAC Address
00:15:67:e3:a5:0c

Serial Number
P14990I500M00149

Aggregate Capacity
107 Mbps

Temperature
N/A

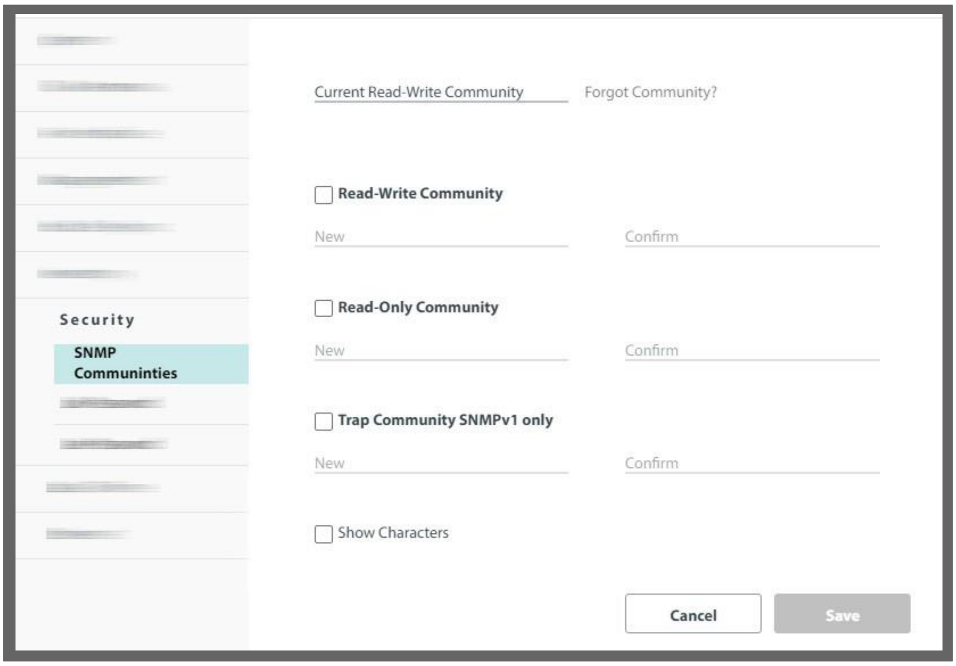
Supported Encryption
AES 128

HW Model Type
Standard

3.3.9. Security

The Security dialog enables you to change the SNMP Community strings.

You can also create an encrypted SNMP Community string value file, set the Security Mode, and change the present user password.



SNMP Communities

Each radio unit communicates with the managing computer using the SNMPv1 or SNMPv3 protocol. The SNMPv1 protocol defines three types of communities:

- Read-only for retrieving information from the radio unit.
- Read-write to configure and control the radio unit.
- Trap used by the radio unit to issue traps.

The read-write community strings and read-only community strings have a minimum of five alphanumeric characters. Changing the trap community is optional.

Editing SNMPv1 Community Strings

When editing these strings, both read-write and read-only communities must be defined.

Ø **To change a community string:**

1. Type the current read-write community in the **Current Read-Write Community** field (default is *netman*).
2. Click the check box next to the community whose string you wish to change.
3. Type the new community string and re-type to confirm. A community string must contain at least five and no more than 32 characters, excluding SPACE, TAB, and any of “>#@|*?;."
4. Click **Save** to have your changes take effect.

Security Mode

This is an enhanced version of the usual secured method of working, which offers extra protection against unauthorized access of the system.

It is performed on a unit-by-unit basis, and is independent of sector structure or hierarchy[1].

Implement this mode as follows:

1. Change the SNMP management interface to SNMPv3:

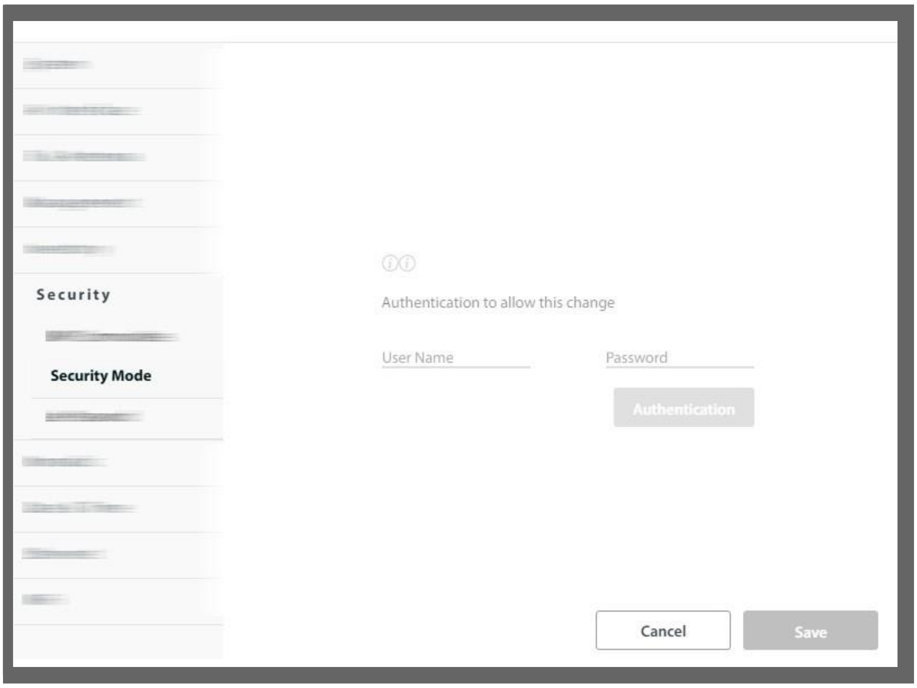
   Select **Configuration -> Management -> Protocol** (See Protoco)

   a. Choose the SNMPv3 radio button. Choose SNMPv3 only, not "V1 and V3".

   b. You can use either the MD5 or SHA1 authentication mode.

   c. Click **Save**. You will be asked to log in again. Make sure you have the proper SNMPv3 user name and password.

2. Select **Configuration** -> **Security** -> **Security Mode**.



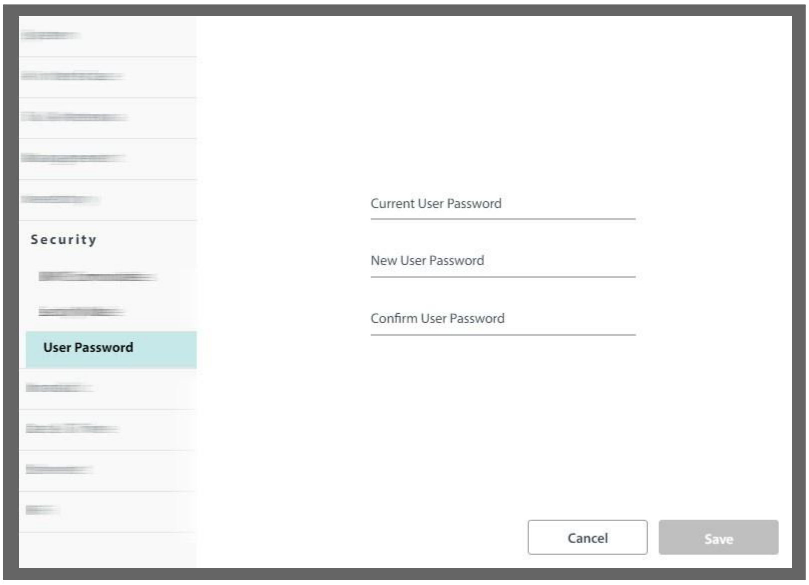
3. Enter the SNMPv3 username and password, and click **Authentication**.
4. Click **Save**.

User Password

Ø **To change the user password of the present user:**

1. Select **Security -> User Password**. The User Password dialog box opens.

[1] *If configuring a single unit for SNMPv3 and Enhanced Security, its counterpart must also be configured for SNMPv3, but it does not need to be configured with Enhanced Security.*



Current User Password

New User Password

Confirm User Password

2. Enter the current password.
3. Enter the new password.
4. Confirm the new password.
5. Click **Save**.

3.3.10. Nomadic

Note – Nomadic doesn't supported by SU-Air or SU in BE mode. Each nomadic SU is allocated to one of four HBS levels labelled A, B, C and D. Some operating parameters for each level (such as VLAN, MIR, QoS, resources, fixed rate, Spatial Multiplexing/Diversity antenna mode) can be different for each level, allowing for broad prioritization of services between different types of nomadic units. This requires that each nomadic SU be assigned a level to join a sector.

A nomadic SU may only send and receive service traffic while stationary. A nomadic SU detects that it is time to seek another HBS upon sync loss. Upon entering and stopping in a new sector, it may take several seconds to establish a sync with the sector HBS.

Note

Changing the VLAN, MIR, QoS, fixed rate, or Spatial Multiplexing/Diversity antenna mode for one configured SU at a given level changes all other SUs at that level.

If you add a new SU to a sector (by direct connection) at a given level, at sync time, it will acquire the existing parameters for that level.

1. To configure a nomadic HSU, you must first add a “framework” or placeholder for a Nomadic device from the HBS.
2. Configure the radio as a stationary SU as described in the other sections here, then do the following from the **Configure -> Nomadic** tab[1]:

[1] *If accessing the SU via the HBS, click Configure -> Nomadic -> Nomadic SU.*

a. Select the **Nomadic** radio button.

b. From the Device Level pull-down menu, select the level of the unit (A, B, C, or D).

c. Click **Save**.

d. A message will appear warning you that if the selected type is not defined in the base station, the SU will not be able to synchronize.

e. Once you are ready, click **OK**. The process will take several seconds, after which the SU will be reset.

Notes for units working in the UNI or ETSI (ie, non-FCC) regulatory environment:

For 5.x GHz and 3.x GHz units: You can select a threshold for scanning. Every 1MHz is checked. This threshold value is used as a jumping off point for a nomadic unit to scan for a base station. Any base station that has an RSS value higher is immediately locked on to. Base stations with values lower than this are placed in a list, and the best one is chosen.

For 3.x GHz units only: Since every 250kHz is checked, the scan for the best unit can take quite some time. To reduce this time, you can choose a channel from which to start the scan.

3.3.11. Date & Time

Here you can set the date and time of the selected unit, whether manually, based on local time or on an NTP Server.

The radio unit maintains a date and time. The date and time should be synchronized with any Network Time Protocol (NTP) version 3 compatible server.

During power-up, the radio attempts to configure the initial date and time using an NTP server. If the server IP address is not configured or is not reachable, a default time is set.

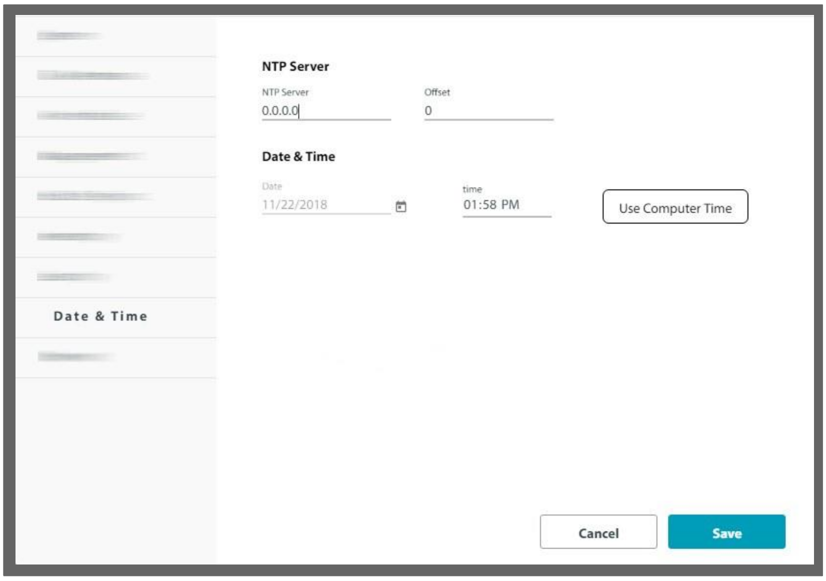
When configuring the NTP server IP address, you should also configure the offset from the Universal Coordinated Time (UTC). If there is no server available, you can either set the date and time, or you can set it to use the date and time from the managing computer. Note that manual settings are not recommended since they will be overridden by a reset, power up, or synchronization with an NTP server.

Note

The NTP uses UDP port 123. If a firewall is configured between the radio and the NTP server, this port must be opened.
It can take up to 8 minutes for the NTP to synchronize the radio date and time.

Ø **To set the date and time:**

1. Determine the IP address of the NTP server to be used.
2. Test it for connectivity using the command (Windows XP and 7), for example:
w32tm /stripchart /computer:216.218.192.202



NTP Server

NTP Server: 0.0.0.0

Offset: 0

Date & Time

Date: 11/22/2018

time: 01:58 PM

3. If entering an IP address for the NTP server, enter the new address.
4. Set your site **Offset** value in minutes ahead or behind GMT[1].
5. To manually set the date and time, click the calendar icon and choose the new date, then click the spinner next to Time to choose the time.
6. To set the time based on the time of the managing computer, click **Use Computer Time**.
7. Click **Save** to have your changes take effect.

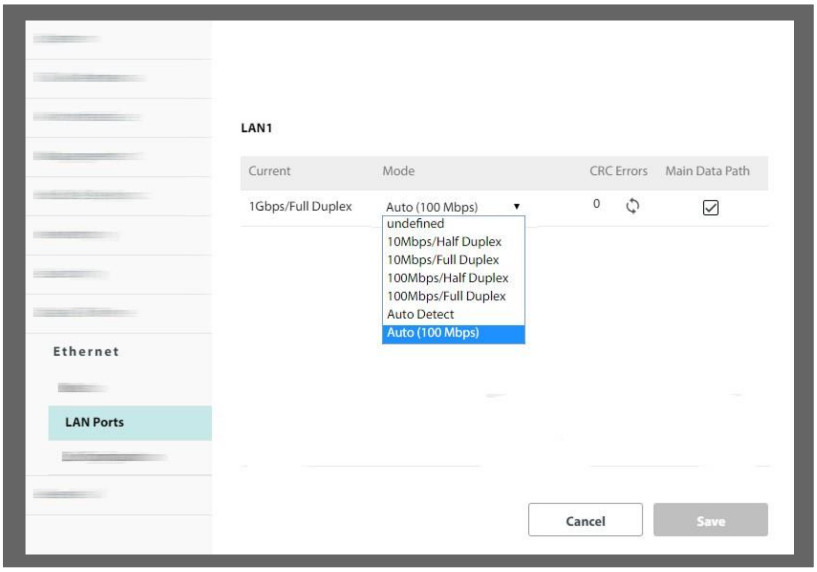
3.3.12. Ethernet

In this category, you can configure the input ports on the unit.

LAN Ports

- The input port (called here “LAN1”) is configurable for line speed and duplex mode (half or full duplex).
- An Auto Detect feature is provided, whereby the line speed and duplex mode are detected automatically using auto-negotiation. Use manual configurations when attached external equipment do not support auto-negotiation. The default setting is Auto Detect.
- The CRC Errors shows how many Cyclic Redundancy Check errors occurred since the last rest.

[1] *Greenwich Mean Time.*

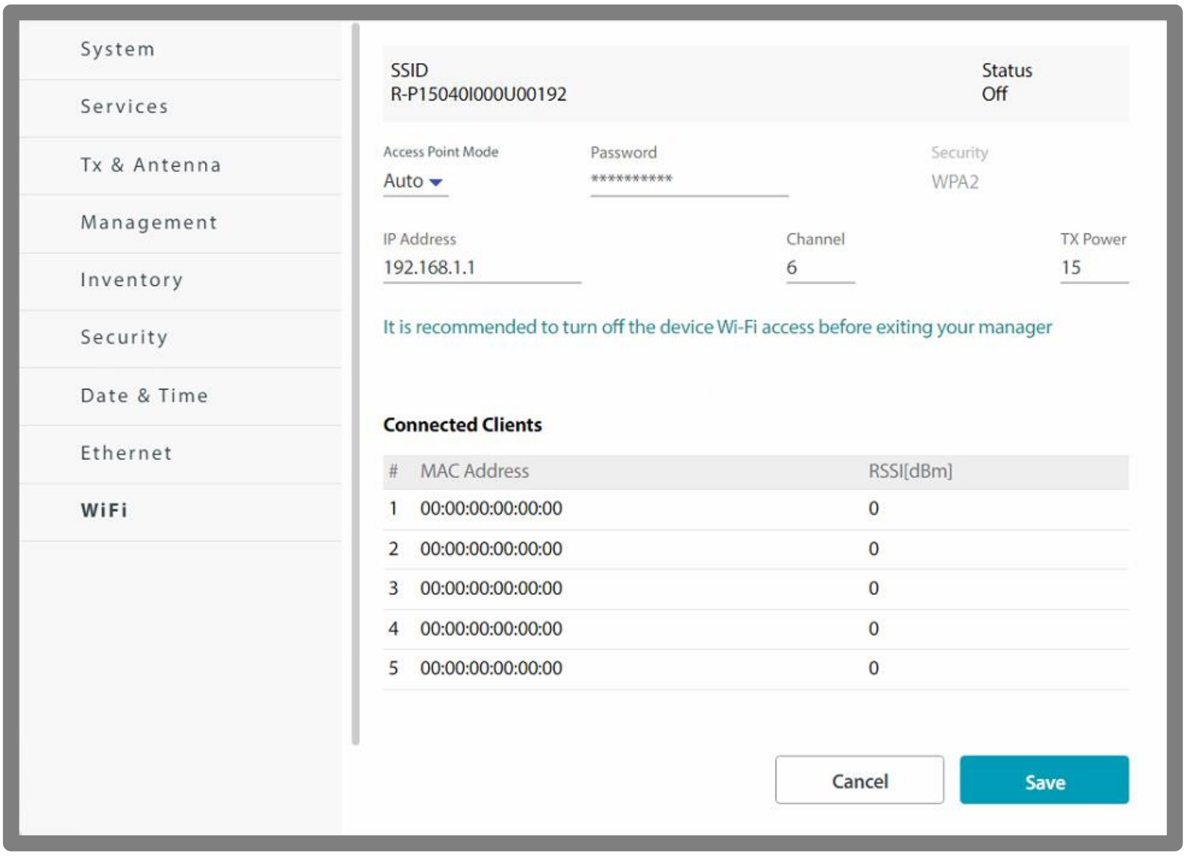


LAN1

Current	Mode	CRC Errors		Main Data Path
1Gbps/Full Duplex	Auto (100 Mbps) ▾	0	↻	☑

undefined
10Mbps/Half Duplex
10Mbps/Full Duplex
100Mbps/Half Duplex
100Mbps/Full Duplex
Auto Detect
Auto (100 Mbps)

3.3.13. WiFi



SSID
R-P15040I000U00192

Status
Off

Access Point Mode: Auto ▾

Password: **********

Security: WPA2

IP Address: 192.168.1.1

Channel: 6

TX Power: 15

It is recommended to turn off the device Wi-Fi access before exiting your manager

Connected Clients

#	MAC Address	RSSI[dBm]
1	00:00:00:00:00:00	0
2	00:00:00:00:00:00	0
3	00:00:00:00:00:00	0
4	00:00:00:00:00:00	0
5	00:00:00:00:00:00	0

The SSID status, Security method, and On status of the WiFi unit are displayed.

Access Point Mode:

- Auto: default. Turns on the wifi for 4 hours upon unit power on, and turns it off if no wifi client is connected within 4 hours.
- On: wifi always on
- Off: WiFi disabled

You can set the following WiFi parameters:

- password
  - Default password: “wireless”

- IP address
  - Default IP address is 192.168.1.1
  - Class C (/24) is always assumed
  - The WiFi access point will lease DHCP IP addresses in the same subnet
  - It is required to change the default IP to some other subnet in order to set the SU management IP in 192.168.1.x range
- channel
  - Default: channel 6
- Tx power
  - Default: 15 dBm. Possible range: 1 - 16dBm

Connected Clients: This area shows up to 5 clients that are connected to this unit, including their MAC addresses and signal strength (RSSI).

Note The SSID of the WiFi is R- [serial number of unit].

Click **Save** to have your changes take effect.

3.3.14. Spectrum

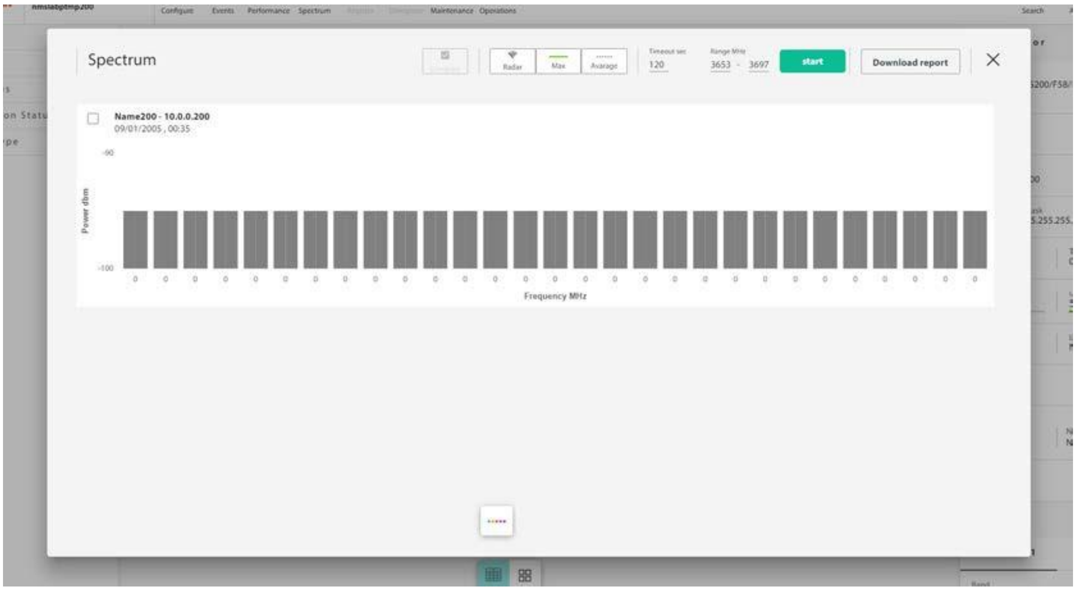
Spectrum

The Spectrum View utility is an RF survey tool that provides spectral measurement information on power vs. frequency. You can view real-time spectrum information, save results, and view historic spectrum scans. The data is stored in the radio unit itself.

The results of the Spectrum View utility are intended for use by RADWIN's Customer Service team to assist with diagnosing interference related problems.

We assume the reader knows about RF Spectrum Analysis so detailed theoretical explanations are not needed.

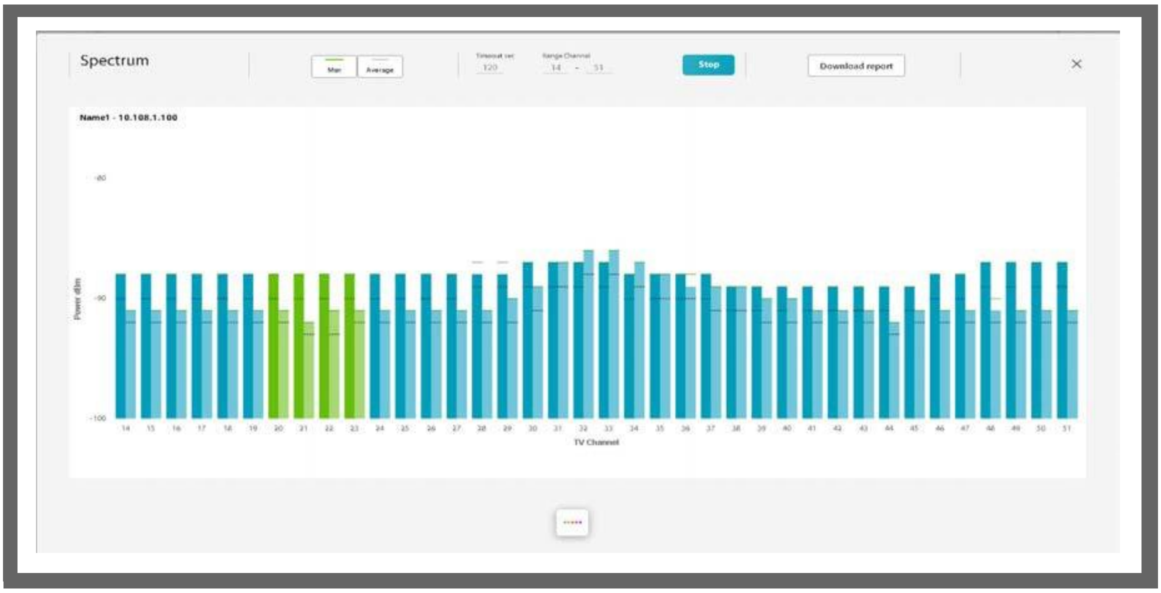
1. Click on the Spectrum View icon Spectrum . The Spectrum View window will appear.



A blank Spectrum View result display will appear, where all the bars are grey.

The name of the unit appears, together with its IP address, date and time.

2. To start a scan, first choose its **Timeout sec** time (top of window), which is the maximum analysis time per scan.
3. Select the frequency range (**Range MHz**, top of window). You can only select allowed frequencies.
4. Once you are ready, click **Start** to start the scan and see the results on screen. You will be warned that this is traffic-affecting. If this is acceptable, then click **Ye**s.



- Green bars relate to those frequencies as listed when you activated the HBS. Dark green is Antenna A and light green is Antenna B.
- If there are frequencies you did not choose when you activated the HBS, their bars appear blue.
- The frequencies the unit is working at has text that appears in blue.
- Green lines show the maximum power found for the indicated frequency range.
- Dotted lines show the average power found for the indicated frequency range.
- If a radar was detected, it's indicated by the brown icon; if not, that is indicated by the gray icon.

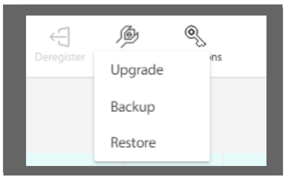
The key on the bottom of the window reviews these indications ( )

5. If you want to save the report, click **Download Report**, and select a location where to save the report file.

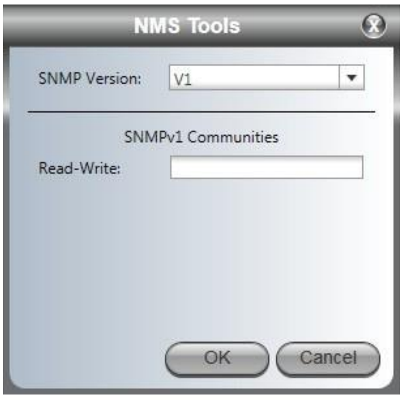
3.3.15. Maintenance

This allows you to upgrade, backup, or restore the target software.

Choose the action you want from the pull-down menu.



- Any of these actions requires the NMSTools.exe application. This is the RADWIN Manager, which must be installed on your computer[1]. When you choose any of these options, you will be asked if you want to open this application. Click **Open NMSTools.exe** to open the application.



SNMP Version: V1

SNMPv1 Communities

Read-Write:

- Enter the password **netwireless** and click **OK**. The RADWIN Manager will open to the Software Upgrade Tool. Continue according to the instructions found in the RADWIN 5000 *Configuration Guide*.
- Note: Upgrading HBS upgrades the whole sector, including any SUs connected.

[1] *See the Configuration Guide for the RADWIN Manager for more details.*

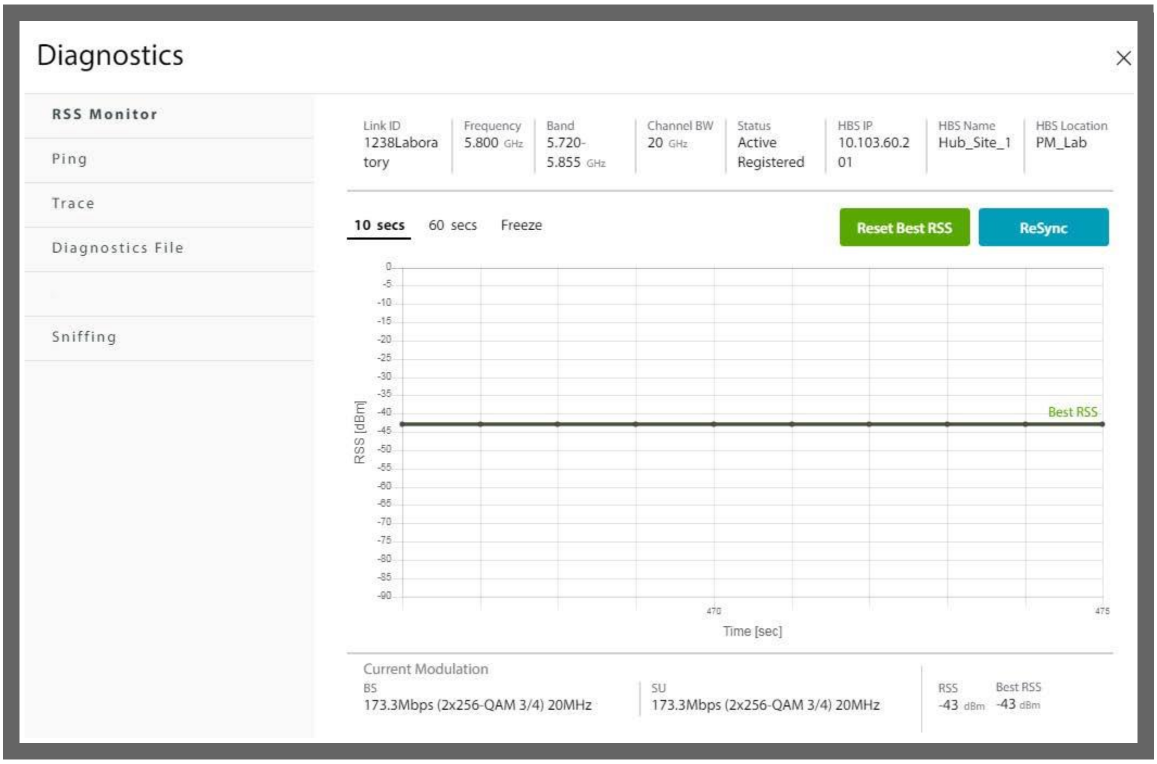
3.3.16. Diagnostics

This category provides various tools: Radio Signal Strength display, a ping and trace capability, diagnostic files (to be used by RADWIN professional services), Ethernet loop backs, and radio unit sniffing.

Click the icon to open the **Diagnostics** window.

RSS Monitor

- This shows the Radio Signal Strength of the selected item in real time.
- You can set the refresh rate at 10 secs or 60 secs, or you can freeze the display at any point in time.
- The display shows both the present RSS and the best RSS achieved till the present point in time.
- Click Reset Best RSS to reset the best RSS counter and click ReSync to re-synchronize the radio unit.
- Use this display when carrying out antenna alignment.



Link ID	Frequency	Band	Channel BW	Status	HBS IP	HBS Name	HBS Location
1238Laboratory	5.800 GHz	5.720-5.855 GHz	20 GHz	Active Registered	10.103.60.201	Hub_Site_1	PM_Lab

Current Modulation

BS	SU	RSS	Best RSS
173.3Mbps (2x256-QAM 3/4) 20MHz	173.3Mbps (2x256-QAM 3/4) 20MHz	-43 dBm	-43 dBm

Ping

This is a standard ping function that allows you to set the number of packets and the packet size sent in the ping action.

1. Enter the target IP address in the Target IP window.
2. Enter the number of packets to be sent in the ping action in the Packets

window, and the packet size to be sent in the Packet Size window.

3. When you are ready, click PING. The button will display Processing. Do not interrupt the process.

4. After a few moments or longer, depending on the size of the values you entered above, the ping results will be shown.

Trace

The ping action is a one-time action, and does not repeat indefinitely.

This is a trace route tool.

1. Enter the IP address of the target to which you want to carry out the trace.
2. When you are ready, click Trace. The button will display **Processing**. Do not interrupt the process.
3. The results will be shown on-screen.

Diagnostics File

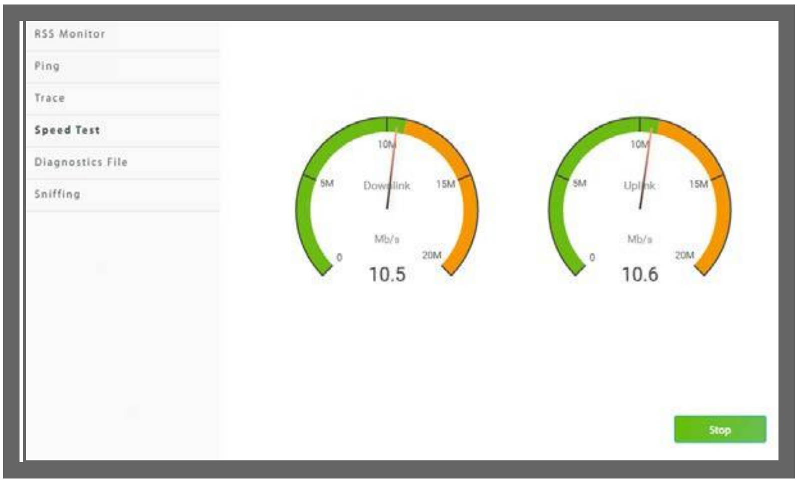
This creates a diagnostic file to be used by RADWIN professional services and support personnel to expedite assistance.

1. Select the items for which you want information. If an item is not selected, the diagnostic file will not contain information for that item. If no items are selected, the Diagnostics icon will become disabled.
2. Click **Generate Diagnostics File**. The diagnostics process will begin, and a button will appear with the option to stop the diagnostics action.
    - After a few seconds or minutes, a JSON file will be created, stored in the default downloads section of the managing computer.
    - The format of this file name is: **diagnostics-DATE TIME.json.**
3. Send this file to the RADWIN professional services team.

Speed Test

Speed Test actively tests current air interface throughput for a specific SU, by sending dedicated generated frames over the air in the downlink and uplink directions. The speed test results are graphically displayed in real-time. A speed test can only be performed on a registered SU.

- To carry out the speed test, click Start.
- To stop the speed test, click Stop.



Sniffing

- The Sniffing (or "sniffer") command captures and downloads management TCP/IP packets on the line between the managing computer and the selected radio device.
- You can select sniffing using full mode, or capture only the headers.
- Click **Start** to start the sniffing process. It will continue until you click **Stop**, or until the file reaches it maximum size (5MB).
- The process can be run in the background.
- Once you stop the process, click **Download** to download the *.pcap file.
- This *.pcap file is downloaded to the default download section of the managing computer. You can use an application, such as WinShark, to read this file.

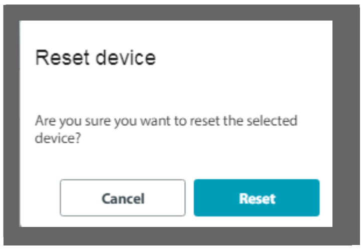
3.3.17. Operations

Operations

This icon allows you to perform a reset, restore the factory default settings, or to perform a license-dependent upgrade on the selected device.

Reset

When you choose Reset, you are asked to confirm. Reset is traffic-affecting. If you are sure, click **Reset**.

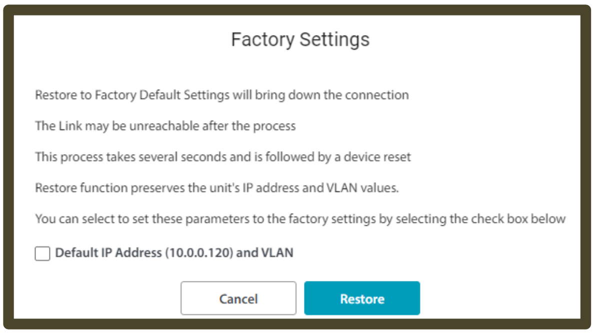

Reset device

Are you sure you want to reset the selected device?

Factory Default

When you choose Factory Default, you are asked to confirm. Since Factory Default involves a reset, it is traffic-affecting. You have an option to restore the default IP address (10.0.0.120) and the management VLAN by clicking the box next to Default IP address. If you do not click this box, the device will retain its previous IP address and management VLAN.

Once you are sure, click **Restore Defaults**. Otherwise, click **Cancel.**



Factory Settings

Restore to Factory Default Settings will bring down the connection

The Link may be unreachable after the process

This process takes several seconds and is followed by a device reset

Restore function preserves the unit's IP address and VLAN values.

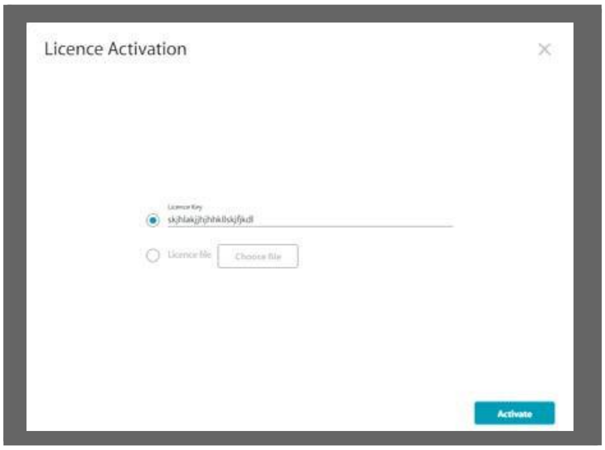
You can select to set these parameters to the factory settings by selecting the check box below

□ Default IP Address (10.0.0.120) and VLAN

Licenses

To carry out a license-dependent upgrade, you must first acquire a license key. Do this as follows:

1. Catalogue number: Contact your RADWIN representative and get the catalogue number for the upgrade you want. Purchase as many of these upgrades as you deem necessary.
2. PAKs: You will receive a list of Product Activation Keys (PAK) for each upgrade instance. A PAK number can be used on any compatible RADWIN product; they are not specific to any one given item of equipment.
3. Activate PAKs: Associate each PAK to a specific item of equipment - Access the License Key Application provided to you by your RADWIN representative and follow the instructions there to activate each PAK for the specific item of equipment you need to upgrade.
4. Get License Keys: The License Key Application will then give you a list of license keys. These numbers *are* unique for the specific upgrade and specific item of equipment. We recommend saving this list as a text file in a convenient location.
5. Select the device for which you want to apply a license-dependent upgrade.
6. Choose Operations -> License. The License Activation window will open.



Licence Activation

● Licence Key: skjhlakjjhjhhklskjfjkdl

○ Licence file

7. Enter the license code in the field, or click **License file**, then click **Choose file** to select where to save the license file.
8. Once you are ready, click **Activate**.
9. The unit will be reset, after which it will be upgraded using the new license.

3.3.18. User Profile Icon

Admin

Admin, Observer, Operator, Installer

The name of the user profile will appear on the icon. Click this icon to log out of the HBS.

3.3.19. 3.3.3 Radio List

The mid-section of the user interface shows the status of the connected unit, together with its base station.

The information for the subscriber unit will be displayed along the top edge of the window.

- Name of unit
- IP address
- Status
- Which carrier it is associated with (if relevant)
- Location
- Sector ID
- Frequency Band
- Channel BW
- Frequency of operation
- Range of unit (distance from base station)
- Tx/Rx ratio
- RSS for each stream (RSS1 and RSS2), on both the HBS side and the SU side
- Throughput for the uplink and downlink

Note

You can use the display of the RSS in real time as an aid during antenna alignment.

3.3.20. 3.3.4 Info Panel

The right pane of the user interface functions as an information panel, giving a brief overview of the sector, showing the following:

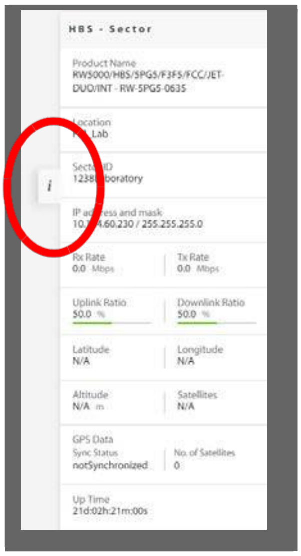
SU (above)

- Product name
- Software version of target (SW Version)
- Hardware version (HW Version)
- Serial Number
- MAC Address
- The unit’s latitude and longitude
- The unit’s up time since last reset

HBS (below)

- Product name
- Location
- Sector ID
- IP address and mask
- Rx rate and Tx rate
- Downlink ratio and Uplink ratio

To minimize the info panel, click on the minimize symbol:



HBS - Sector

Product Name
RW5000/HBS/5PG5/F3F5/FCC/JET-DUO/INT - RW-5PG5-0635

Location
[illegible] Lab

Sector ID
1238[illegible]boratory

IP address and mask
10.[illegible]4.60.230 / 255.255.255.0

Rx Rate	Tx Rate
0.0 Mbps	0.0 Mbps

Uplink Ratio	Downlink Ratio
50.0 %	50.0 %

Latitude	Longitude
N/A	N/A

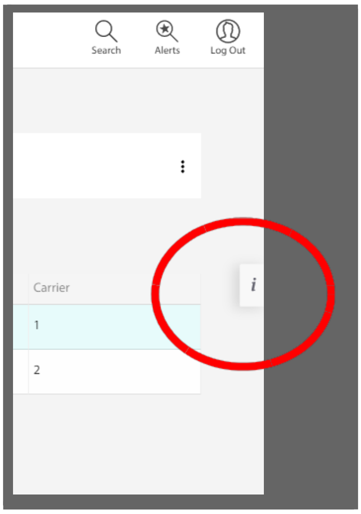
Altitude	Satellites
N/A m	N/A

GPS Data

Sync Status	No. of Satellites
notSynchronized	0

Up Time
21d:02h:21m:00s

- To restore the info panel, click on the minimize symbol again.



Appendix A: Terminology

Table A-1: Terminology (Sheet 1 of 5)

Term	Description
Assured throughput	Actual number of timeslots allocated to a radio unit.
ACS	Automatic Channel Selection - an option that instructs the radio to choose which frequency to use. Enabling or disabling this option has various ramifications, as shown in the documentation.
API	Application Program Interface
ATPC	Automatic Transmit Power Control
BE	Best Effort: A level of priority for traffic in which users receive dynamic resource allocations according to overall demand. They are not guaranteed resources. See also CIR.
BFD	Bidirectional Forwarding Detection - a network protocol used to detect faults between two forwarding engines connected by a link.
BS	Base Station: a radio that can transmit and receive to more than one point. See also HBS.
CIR	Committed Information Rate: A level of priority for traffic in which users receive a guaranteed percentage of resources in addition to dynamic resources, if available. See also BE.
CPE	Customer Premises Equipment
CSE	Customer Site Equipment
DBA	Dynamic Bandwidth Allocation - a method that allocates bandwidth between the various users of that same bandwidth in the network.

Term	Description
DBS	Dynamic Bandwidth Selection: When activating a base station, or when changing its bandwidth, if you choose the maximum value available for the bandwidth, the link may dynamically switch between the maximum value and values as low as 20MHz to ensure the best throughput.
DFS	Dynamic Frequency Selection - those products that have DFS enabled ensure that no radar signal is present in the selected frequency channel within the band being used. If a radar signal is detected, that frequency channel is evacuated and the product will not transmit on this channel.
DHCP	Dynamic Host Configuration Protocol - a protocol that automatically assigns IP addresses and other network configuration parameters.
Diversity	A technique by which the reliability of a radio link is increased using multiple transmitting and receiving antennas, transmitting the same signal on all antennas.
Downlink	Data traffic from an HBS to an HSU, or Data traffic from an RT-A to an RT-B
DUO	Dual Band base station
EIRP	Equivalent (or Effective) Isotropically Radiated Power - the power that an antenna must emit to produce the peak power density in the direction of a maximum antenna gain. In our cases, this is usually: System Tx Power + Antenna Gain - Cable Loss.
FAA	Federal Aviation Administration – a U.S. federal office that manages aviation regulations throughout the United States.
Fixed (HSU)	A “fixed” HSU remains in one location, as contrasted with a nomadic or mobile HSU, which does not remain in one location.
GHSS	GPS Hub Site Synchronization
GRE	Generic Routing Encapsulation - a communication protocol used to establish a direct, point-to-point connection between network nodes. GRE lets two peers share data they wouldn’t be able to share over the public network itself.
GRE Tunnel	A virtual point-to-point connection between two networks, using the GRE protocol to carry this out.
HBS	High capacity Base Station. Same as a BS.

Term	Description
HMU	High capacity Mobility (subscriber) Unit. Similar to an HSU, but can be mobile.
HSC	Hub Sync Client - when using Hub Site Synchronization, one unit is a master (generates the sync pulses), and the other units are clients.
HSM	Hub Sync Master - when using Hub Site Synchronization, one unit is a master (generates the sync pulses), and the other units are clients.
HSU	High capacity Subscriber Unit. Same as an SU.
IGMP	Internet Group Management Protocol
ISU	Integrated Synchronization Unit - a network device that provides a synchronization signal to underground HBSs.
LFF	Large Form-Factor
MD5	Message digest algorithm - an authentication type for SNMPv3 connections.
MDL	Multiple Device Learning
MIMO	Multiple In, Multiple Out – a technique by which the capacity of a radio link is increased using multiple transmitting and receiving antennas, transmitting a different signal on all antennas.
MIR	Maximum Information Rate
Mobile (HSU)	A “mobile” HSU can move from location to location and provide service while it moves or when it is stationary.
Nomadic (HSU)	A “nomadic” HSU move from location to location but can only provide service when it is stationary.
ODU	Outdoor Unit - a generic term for any radio, and can usually be exchanged for HBS or HSU.
PAWS	Protocol to Access White-Space - a protocol that allows geolocation TVWS databases to communicate with radios. PAWS specify how a master device obtains a schedule of available spectrums at its location. It also takes into consideration the security necessary to ensure the accuracy, privacy, and confidentiality of the device’s location.
PNAM	Predecessor Neighbor Advertisement Message
PPPoE	Point-to-Point Protocol over Ethernet

Term	Description
PtMP	Point to Multi-Point - link from an HBS to several HSUs
PtP	Point to Point
RADIUS	Remote Authentication Dial-In User Service
RSS	Radio Signal Strength
QAM	Quadrature Amplitude Modulation - the name of a family of digital modulation methods and a related family of analog modulation methods widely used in modern telecommunications to transmit information.
QoS	Quality of Service
SBM	Smart Bandwidth Management
Sector	A group of radios that consists of one HBS and several HSUs that communicate with the HBS.
SFF	Small Form-Factor
SHA1	Secure hash algorithm: an authentication type for SNMPv3 connections.
SLA	Service Level Agreement - the basic agreement between the service provider and its customer regarding certain aspects of the service provided. For example, what should be the data rate, throughput, jitter of the line, who should pay what fees, the mean time between failure (MTBF) of the equipment, and so forth.
SSM	Synchronization Status Message - provides traceability of synchronization signals, and is used in the Synchronous Ethernet standard of communication.
SU	Subscriber Unit - a radio that can transmit and receive to one point. See also HSU.
Sync E or SyncE	Synchronous Ethernet - a standard of communication for Ethernet that provides a synchronization signal to network elements that need such a signal.
TBS	Transportation Base Station - similar to an HBS or BS, but used with high-speed transportation applications.
TCO	Total Cost of Ownership

Term	Description
TDWR	Terminal Doppler Weather Radar - a type of radar station used in the U.S. and other countries for weather reporting. If a radio unit is installed close enough to one of these stations, the FCC requires that certain actions must be taken on the part of the customer. Regulations in other countries varies.
TMU	Transportation Mobile Unit. Similar to an SU
TSN	Time Sensitive Network
TVWS	TV (television) White Space - a method by which certain unused frequencies in the television spectrum are put to use for BWA purposes.
Uplink	Data traffic from an HSU to an HBS, or Data traffic from an RT-B to an RT-A
VMU	Vehicular Mobile Unit
WI	Web Interface - a web-based application that provides simple configuration capabilities for the radio units.
WISPA	Wireless Internet Service Provider Association - an organization that manages the registration of wireless devices that operate close to TDWR facilities run by the FAA.
VRRP	Virtual Router Redundancy Protocol - a networking protocol that provides automatic assignments of available IP routers to participating hosts.

Appendix B: About Antennas

B.1 Scope of this Appendix

This appendix provides some basic information and considerations regarding antennas and what you need to take into account when configuring antenna parameters.

B.2 Antenna Issues

The choice of Tx Power, antenna gain, and cable loss (between the radio and the antenna) determines the EIRP and is affected by such considerations as radio limitations and regulatory restrictions.

Before proceeding to antenna installation details, the following background information should be considered:

B.3 About Single and Dual Antennas

Each RADWIN radio is actually made of two radio transceivers (radios). The radios make use of algorithms that utilize both Spatial Multiplexing (also called MIMO) and Diversity, resulting in enhanced capacity, and range and link availability. The number of antennas (i.e. radios) used is determined by user configurations and by automatic system decisions, explained below.

3.3.21. B.3.1 Dual Antennas at the HBS and an SU

When using dual antennas at both sites (single bipolar antenna or two mo-unipolar antennas) you can choose between Spatial Multiplexing Mode and Diversity Mode.

Spatial Multiplexing Mode

Under this mode, the system doubles the link capacity. At the same time, it keeps the same rate and modulation per radio as was used with the single antenna, thus increasing capacity, range, and availability.

For example, with a dual antenna, RADWIN 5000 can transmit at modulation of 64QAM and FEC of 5/6 and get an air rate of 130 Mbps, compared to 65 Mbps with a single antenna.

To work in this mode, each antenna post must be connected to an antenna, the RSS level of both receivers should be balanced and a minimal separation between the antennas must be maintained. (For example, by using dual polarization antennas a cross polarization separation is attained).

Upon selecting Antenna Type as Dual, the RADWIN 5000 automatically selects this mode and doubles the air rates.

The RADWIN Manager indicates a case of unbalanced RSS between the two antennas in the HBS panels.

Diversity Mode

Diversity Mode uses two antennas to improve the quality and reliability of the link. Often, there is not a clear line-of-sight (LOS) between the transmitter and the receiver. Instead, the signal is reflected along multiple paths before finally being received.

Each such “bounce” can introduce phase shifts, time delays, attenuations, and even distortions that can destructively interfere with one another at the aperture of the receiving antenna. Antenna diversity is especially effective at mitigating these multi-path situations.

This is because multiple antennas afford a receiver with several recordings of the same signal. Each antenna will be exposed to a different interference environment. Thus, if one antenna is undergoing a deep fade, it is likely that another has a sufficient signal. Collectively, such a system can provide a robust link.

Antenna diversity requires antenna separation, which is possible by using a dual-polarization antenna or by two spatially separated antennas.

Use Diversity instead of Spatial Multiplexing in the following situations:

- When the system cannot operate in Spatial Multiplexing Mode.
- When one of the receivers has high interference compared to the second receiver (i.e. the system is “unbalanced”).
- When you achieve higher capacity in Diversity Mode than in Spatial Multiplexing Mode.
- When high robustness is of importance and the capacity of Diversity Mode is sufficient (up to 25 Mbps full duplex).

3.3.22. B.3.2 Single Antennas at Both Sites

By selecting a single antenna at the HBS and SU, the ODUs operate with a single radio that is connected to the ANT 1 connector. The second radio is automatically shut down.

3.3.23. B.3.3 Single at One Site, Dual Antennas at the Other

In this mode, one of the sites uses the ODU with a single antenna while the other site uses the ODU with a dual antenna.

The advantages in this mode - in comparison to using a single antenna in both sites - are double the total Tx Power and additional polarization and/or space diversity (depending on the polarization of installed antennas).

The air rates used in this mode are the same as when using single antennas in both sites. Table B-1 summarizes the situation: (SM =Spatial Multiplexing)

Table B-1: Spatial Multiplexing - Diversity Settings

Number of Antennas		Mode		Max Full Duplex Capacity
Site A	**Site B**	**Site A**	**Site B**	
2	**2**	Spatial Multiplexing	Spatial Multiplexing	50 Mbps
		Diversity	Diversity	25 Mbps
2	**1**	Diversity	Single	25 Mbps
1	**2**	Single	Diversity	25 Mbps
1	**1**	Single	Single	25 Mbps

Site A and B may be HBS or SU.

B.4 Considerations for Changing Antenna Parameters

Let:

max Available Tx Power denote the maximum Tx Power practically available from an ODU. (It appears as Tx Power per Radio).

maxRegEIRP denotes the maximum EIRP available by regulation. It will be determined by three factors:

- per band/regulation
- per channel bandwidth
- antenna gain

maxRegTxPower denotes the maximum regulatory Tx Power for the equipment, also having regarded the above three points.

Then, the following relationship must be satisfied:

$$\mathrm{maxAvailableTxPower} \leq \min(\mathrm{maxRegEIRP} - \mathrm{AntennaGain} + \mathrm{CableLoss},\ \mathrm{maxRegTxPower})$$

... (*)

The Tx Power (per radio) indicates the power of each radio inside the ODU and is used for Link Budget Calculations. The Tx Power (System) shows the total transmission power of the ODU and is used to calculate the EIRP according to regulations.

The inequality (*) above is always satisfied by the system in accordance with the relevant regulation.

Note

- The Max EIRP level will be automatically set according to the selected band and regulation.

The precise relationship between the items in inequality (*) is as follows: Required Tx Power (per radio) will be adjusted down to the lesser of the value entered and maxAvailableTxPower.

- Tx Power (system) is maxAvailableTxPower + 3 (for 2 radios).
- Max EIRP is maxRegEIRP.
- EIRP is maxAvailableTx Power + Antenna Gain - Cable Loss.

Appendix C: SSH CLI

From 5.1.30, the SSH protocol is supported by HBS and SUs web-based products (SU-Air/Pro,JET DUO, Multisector, NEO/NEO DUO). Users can enable or disable this protocol. The SSH login has the same user access privileges as the users who log in to the web UI (Admin, Operator, etc..). SSU supports auto completion of the command by using the tab key.

A SSH terminal can be used to configure and monitor the devices. To start a SSH session with the IP address of the ODU, use an SSH terminal. The username for the SSH session is **cli** (no password). Once the session is open, CLI prompt “login as” will appear, enter your credentials (same as for WEB GUI, default is admin/netwireless).

Below is the list of SSH commands

Command	Explanation
help	Show available commands
quit	Disconnect
logout	Disconnect
exit	Exit from current mode
history	Show a list of previously run commands
configure terminal	Configure from the terminal. Enable access to configure terminal modes and set the login timeout in seconds. Press exit to exit the config terminal mode
display inventory	Display device inventory information
display management	Display device management information
display link all, reg, unreg, <serial>, <mac>, <name>	Display Wireless link information [param: all, reg, unreg, <serial>, <mac>, <name>]. You can select to see information of all the connected SUs, registered SUs only, unregistered SUs only, or select a specific SU by writing its serial number, mac address, or name. Examples: **display link reg** **display link P17300I000K00160**
display ethernet	Display the ethernet & SFP status and information
display ntp	Display network time information
display bands	Display Wireless bands information
set ip <ipaddr> <subnetMask> <gateway>	Set the management IP, Subnet, and Default Gateway
set trap <index:1-10> <ipaddr> <port:1-65535>	Enable the ability to set the trap destination index number (up to 10), IP address and port number
set syslog <server ip>	The set Syslog server IP address <0.0.0.0> is used to disable the syslog server
set ntp <ntp-server> <offset-minutes>'	Set the NTP server of the offset time
set secID <sectorId>	Set the sector ID

set name <new name>	Set the name of the unit
set location <new location>	Set the location of the unit
set contact <new contact>	Set the contact information
set ethernet <port:LAN1> <mode:Auto,Auto_100,10H,10F,100H,100F>	Set the mode of the negotiation mode of Ethernet port
reboot	Reboot the unit
util ping [OPTIONS] IP (CTRL+C To Stop, 'util ping' for all options)	Enable the ability to check ping connectivity with a network device. The ping utility have a number of options for ping tests: ping [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface] [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos] [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline] [-W timeout] [hop1 ...] destination Example 1: send 10 pings and stop **util ping 20.0.0.150 ‘-c’ 10** Example 2: send pings in interval of 0.5 second (interval should be below 1) **util ping 20.0.0.150 ‘-i’ 0.5**
util traceroute [OPTIONS] IP [BYTES] (CTRL+C To Stop, 'util traceroute' for all options)	Enable the ability to perform traceroute tests
Link [param: <serial>, <mac>, <name>]	Enable SSH login remotely to the SU. Specify the required SU by its serial or mac or name. When login remotely is enabled, the name of the SU will appear in the CLI. Example of an SSH access to the SU is that its name is Alpha_IP_64 via the SSH of HBS with ip address 20.0.0.130 **admin@20.0.0.130(link-Alpha_IP_64)->**
display beamwidth	for products that support SDS (Jet DUO) Displays the current SDS beamwidth (45 / 60 / 90) Output example: Sector beamwidth on carrier 1 is 45 Sector beamwidth on carrier 2 is 45
set beamwidth <value>	for products that support SDS (Jet DUO) Sets the sector's SDS beamwidth (value can be 45 / 60 / 90) for both carriers Output example: Sector beamwidth is set to 60

Appendix D: Revision History

Table C-1: Revision History: RADWIN 5000 Configuration Guide for the Web UI

Release & Doc.Rev	Date	Description
Release 4.9.80,	Mar, 2020	• Initial release: Includes Web-configured units only, which means the JET units starting from HW ver.4, and the SU-PRO/AIR units
Release 5.0.50	Jun, 2020	• RADIUS AAA functions • 802.1x authentication • Nomadic functionality • Utilization feature • Quality detection feature • Bridge table • DHCP (Option 82)
DQ0266620/B.00 System Release 5.0.70	Sep, 2020	• Automated Carrier Switching • Sector Self Backhaul • Multi Sector
DQ0266620/B.01 System Release 5.0.70	Oct, 2020	• IGMP • Multi Sector - Connectorized
DQ0266620/B.02 System Release 5.1.10	Jun, 2021	• NEO, NEO DUO, and SU Connectorized • Carrier Switch can configure criteria separately
System Release 5.1.30	Feb, 2022	• Radius Authorization • Deregister preserved sector ID • Factory default preserved VLAN management • SSH
System Release 5.1.42	Sep, 2022	Release 5.1.42: • Enable / Disable upgrade /backup without IP • Self Registered SU Mode • allow SUs interconnections per HBS • Lost or forgotten VLAN ID or IP Address (SU-Air/Pro) • Management IP & Management VLAN at the same tab • RADWIN 5000L
System Release 5.1.44	Feb 2023	Added SDS option to Jet DUO
System Release 5.1.45	June 2023	Added world-wide single PN products – Jet Air and Jet Air DUO

User Handbook Notice

RADWIN 5000

This handbook contains information that is proprietary to RADWIN Ltd (RADWIN hereafter). No part of this publication may be reproduced in any form whatsoever without prior written approval by RADWIN.

Right, title and interest, all information, copyrights, patents, know-how, trade secrets and other intellectual property or other proprietary rights relating to this handbook and to the RADWIN products and any software components contained therein are proprietary products of RADWIN protected under international copyright law and shall be and remain solely with RADWIN.

The RADWIN name is a registered trademark of RADWIN. No right, license, or interest to such trademark is granted hereunder, and you agree that no such right, license, or interest shall be asserted by you with respect to such trademark.

You shall not copy, reverse compile or reverse assemble all or any portion of the Configuration Guide for the Web UI or any other RADWIN documentation or products. You are prohibited from, and shall not, directly or indirectly, develop, market, distribute, license, or sell any product that supports substantially similar functionality based or derived in any way from RADWIN products.Your undertaking in this paragraph shall survive the termination of this Agreement.

This Agreement is effective upon your opening of a RADWIN product package and shall continue until terminated. RADWIN may terminate this Agreement upon the breach by you of any term thereof. Upon such termination by RADWIN, you agree to return to RADWIN any RADWIN products and documentation and all copies and portions thereof.

For further information contact RADWIN at one of the addresses under Worldwide Contacts below or contact your local distributor.

Disclaimer

The parameters quoted in this document must be specifically confirmed in writing before they become applicable to any particular order or contract. RADWIN reserves the right to make alterations or amendments to the detail specification at its discretion. The publication of information in this document does not imply freedom from patent or other rights of RADWIN, or others.

Trademarks

WinLink 1000, RADWIN 2000, RADWIN 5000, RADWIN 6000, RADWIN 600 and FiberinMotion are trademarks of RADWIN Ltd.

Windows 2000, XP Pro, Vista, Windows 7 and Internet Explorer are trademarks of Microsoft Inc.
Mozilla and Firefox are trademarks of the Mozilla Foundation.

Other product names are trademarks of their respective manufacturers.

Last page of EndPage files

RADWIN